



# **Cluster administration**

## **ONTAP 9**

NetApp  
March 09, 2022

This PDF was generated from [https://docs.netapp.com/us-en/ontap/concept\\_administration\\_overview.html](https://docs.netapp.com/us-en/ontap/concept_administration_overview.html) on March 09, 2022. Always check docs.netapp.com for the latest.

# Table of Contents

- Cluster administration. . . . . 1
  - Cluster management with System Manager . . . . . 1
  - Cluster management with the CLI . . . . . 11
  - Disk and aggregate management with the CLI . . . . . 202
  - FabricPool tier management with System Manager . . . . . 267
  - FabricPool tier management with the CLI . . . . . 271
  - SVM data mobility . . . . . 316
  - High availability management . . . . . 322
  - Rest API management with System Manager . . . . . 342

# Cluster administration

## Cluster management with System Manager

### Administration overview with System Manager

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.

The procedures in this section help you manage your cluster with System Manager in ONTAP 9.7 and later releases.



If you are using the classic System Manager (available only in ONTAP 9.7 and earlier), refer to [System Manager Classic \(ONTAP 9.0 to 9.7\)](#)

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 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.

### System Manager terminology

System Manager uses different terminology than the CLI for some ONTAP key functionality.

- **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)*.
- **Pause** - an action that halts operations. Before ONTAP 9.8, you might have referred to *quiesce* in other versions of System Manager.


## Enable new features by adding license keys

Some ONTAP features are enabled by license keys. You can add license keys using System Manager.

Beginning with ONTAP 9.10.1, you use System Manager to install a NetApp License File to enable multiple licensed features all at once. Using a NetApp License File simplifies license installation because you no longer have to add separate feature license keys. You download the NetApp License File from the NetApp Support Site.

If you already have license keys for some features and you are upgrading to ONTAP 9.10.1, you can continue to use those license keys.

### Steps

1. Click **Cluster > Settings**.
2. Under **License**, click .
3. Click **Browse** to locate and select the NetApp License File you downloaded.
4. If you have license keys you want to add, select **Use 28-character license keys** and enter the keys.

## View and submit support cases

Beginning 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.

## Monitor risks

Beginning with ONTAP 9.10.0, you can use System Manager to monitor the risks reported by Active IQ Digital Advisor. Beginning with ONTAP 9.10.1, you can use System Manager to also acknowledge the risks.

NetApp Active IQ Digital Advisor reports opportunities to reduce risk and improve the performance and efficiency of your storage environment. With System Manager, you can learn about risks reported by Active IQ and receive actionable intelligence that helps you administer storage and achieve higher availability, improved security, and better storage performance.

### Link to your Active IQ account

To receive information about risks from Active IQ, you should first link to your Active IQ account from System Manager.

#### Steps

1. In System Manager, click **Cluster > Settings**.
2. Under **Active IQ Registration**, click **Register**.
3. Enter your credentials for Active IQ.
4. After your credentials are authenticated, click **Confirm to link Active IQ with System Manager**.

### View the number of risks

Beginning with ONTAP 9.10.0, you can view from the dashboard in System Manager the number of risks reported by Active IQ.

#### Before you begin

You must establish a connection from System Manager to your Active IQ account. Refer to [Link to your Active IQ account](#).

#### Steps

1. In System Manager, click **Dashboard**.
2. In the **Health** section, view the number of reported risks.



You can view more detailed information about each risk by clicking the message showing the number of risks. See [View details of risks](#).

### View details of risks

Beginning with ONTAP 9.10.0, you can view from System Manager how the risks reported by Active IQ are categorized by impact areas. You can also view detailed information about each reported risk, its potential impact on your system, and corrective actions you can take.

#### Before you begin

You must establish a connection from System Manager to your Active IQ account. Refer to [Link to your Active IQ account](#).

## Steps

1. Click **Events > All Events**.
2. In the **Overview** section, under **Active IQ Suggestions**, view the number of risks in each impact area category. The risk categories include:
  - Performance & efficiency
  - Availability & protection
  - Capacity
  - Configuration
  - Security
3. Click on the **Active IQ Suggestions** tab to view information about each risk, including the following:
  - Level of impact to your System
  - Category of the risk
  - Nodes that are affected
  - Type of mitigation needed
  - Corrective actions you can take

## Acknowledge risks

Beginning with ONTAP 9.10.1, you can use System Manager to acknowledge any of the open risks.

### Steps

1. In System Manager, display the list of risks by performing the procedure in [View details of risks](#).
2. Click on the risk name of an open risk that you want to acknowledge.
3. Enter information into the following fields:
  - Reminder (date)
  - Justification
  - Comments
4. Click **Acknowledge**.



After you acknowledge a risk, it takes a few minutes for the change to be reflected in the list of Active IQ suggestions.

## Unacknowledge risks

Beginning with ONTAP 9.10.1, you can use System Manager to unacknowledge any risk that was previously acknowledged.

### Steps

1. In System Manager, display the list of risks by performing the procedure in [View details of risks](#).
2. Click on the risk name of an acknowledged risk that you want to unacknowledge.
3. Enter information into the following fields:
  - Justification

- Comments

#### 4. Click **Unacknowledge**.



After you unacknowledge a risk, it takes a few minutes for the change to be reflected in the list of Active IQ suggestions.

## Gain insights to help optimize your system

Beginning with ONTAP 9.11.0, you can view insights in System Manager that help you optimize the capacity and security compliance of your system. Based on best practices, these insights are displayed on one page from which you can initiate immediate actions to optimize your system.

### View optimization insights

#### Steps

1. In System Manager, click **Insights** in the left-hand navigation column.

The **Insights** page shows groups of insights. Each group of insights might contain one or more insights. The following groups are displayed:

- Needs your attention
  - Remediate risks
  - Optimize your storage
2. (Optional) Filter the insights that are displayed by clicking either of these buttons in the upper-right corner of the page:

◦



Display the security-related insights.

◦



Display the capacity-related insights.

### Respond to insights to optimize your system

In System Manager, you can respond to insights by either dismissing them, exploring different ways to remediate the problems, or initiating the process to fix the problems.

#### Steps

1. In System Manager, click **Insights** in the left-hand navigation column.
2. Hover over an insight to reveal the buttons to perform the following actions:
  - **Dismiss:** Remove the insight from the view. To “undismiss” the insight, refer to [Customize the setting for insights](#).
  - **Explore:** Find out various ways to remediate the problem mentioned in the insight. This button appears only if there is more than one method of remediation.
  - **Fix:** Initiate the process of remediating the problem mentioned in the insight. You will be asked to confirm whether you want to take the action needed to apply the fix.




Some of these actions can be initiated from other pages in System Manager, but the **Insights** page helps you streamline your day-to-day tasks by allowing you to initiate these action from this one page.

## Customize the setting for insights

You can customize which insights you will notified about in System Manager.

### Steps

1. In System Manager, click **Insights** in the left-hand navigation column.
2. In the upper-right corner of the page, click .
3. On the **Settings** page, ensure there is a check in the check boxes next to the insights you want to be notified about. If you previously dismissed an insight, you can “undismiss” it by ensuring a check is in its check box.
4. Click **Save**.

## 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.

### Before you Start

For ONTAP 9.8, System Manager provides a *preview* of the capability to view AFF hardware configurations. Beginning 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:

<b>If your system is running...</b>	<b>Then you can use System Manager to view...</b>
-------------------------------------	---



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 use System Manager to 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.
- Beginning 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 use System Manager to 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.

Video of Hardware Visualization using System Manager in ONTAP 9.8

The hardware visualization feature enables users to quickly visualize hardware status and any potential connection issues.



Add disks to a local tier (Add capacity to an aggregate)

You can increase the size of an existing aggregate (local tier) by adding capacity disks.

The process you use to increase capacity depends on the version of ONTAP that you have installed:

If you have installed...	Then increase capacity with this process...
ONTAP 9.7 or earlier	<a href="#">Increase the capacity of an aggregate (ONTAP 9.7 or earlier)</a>
ONTAP 9.8 or later	<a href="#">Increase the capacity of a local tier (ONTAP 9.8 or later)</a>

### Increase the capacity of an aggregate (ONTAP 9.7 or earlier)

Using System Manager with ONTAP 9.7 or earlier, you can add capacity to an aggregate by adding capacity disks.

#### About this task

You perform this task only if you have installed ONTAP 9.7 or earlier. If you installed ONTAP 9.8 or later, refer to [Increase the capacity of a local tier \(ONTAP 9.8 or later\)](#).

#### 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.

### Increase the capacity of a local tier (ONTAP 9.8 or later)

Using System manager with ONTAP 9.8 or later, you can add capacity to a local tier by adding capacity disks.

#### About this task

You perform this task only if you have installed ONTAP 9.8 or later. If you installed an earlier version of ONTAP, refer to [Increase the capacity of an aggregate \(ONTAP 9.7 or earlier\)](#).

#### Steps

1. Click **Storage > Tiers**.
2. Click **:** next to the name of the local tier to which you want to add capacity.
3. Click **Add Capacity**.



If there are no spare disks that you can add, then the **Add Capacity** option is not shown, and you cannot increase the capacity of the local tier.

4. If the node contains multiple storage tiers, then select the number of disks you want to add to the local tier. Otherwise, if the node contains only a single storage tier, the added capacity is estimated automatically.
5. Click **Add**.
6. (Optional) The process takes some time to complete. If you want to run the process in the background, select **Run in Background**.


7. After the process completes, you can view the increased capacity amount in the local tier information at **Storage > Tiers**.

## Manage nodes

### 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.

### 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 \(ONTAP 9.7\)](#)
- [Adding nodes to a cluster with System Manager \(ONTAP 9.8\)](#)

#### Adding nodes to a cluster with System Manager (ONTAP 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 (ONTAP 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.

# Cluster management with the CLI

## Administration overview with the CLI

You can administer ONTAP systems with the command-line interface (CLI). You can use the ONTAP management interfaces, access the cluster, manage nodes, and much more.

You should use these procedures under the following circumstances:

- You want to understand the range of ONTAP administrator capabilities.
- You want to use the CLI, not System Manager or an automated scripting tool.

### Related information

For details about CLI syntax and usage, see the [ONTAP 9 manual page reference](#) documentation.

## Cluster and SVM administrators

### Cluster and SVM administrators

Cluster administrators administer the entire cluster and the storage virtual machines (SVMs, formerly known as Vservers) it contains. SVM administrators administer only their own data SVMs.

Cluster administrators can administer the entire cluster and its resources. They can also set up data SVMs and delegate SVM administration to SVM administrators. The specific capabilities that cluster administrators have depend on their access-control roles. By default, a cluster administrator with the “admin” account name or role name has all capabilities for managing the cluster and SVMs.

SVM administrators can administer only their own SVM storage and network resources, such as volumes, protocols, LIFs, and services. The specific capabilities that SVM administrators have depend on the access-control roles that are assigned by cluster administrators.



The ONTAP command-line interface (CLI) continues to use the term *Vserver* in the output, and `vserver` as a command or parameter name has not changed.

### What the cluster management server is

The cluster management server, also called an *adminSVM*, is a specialized storage virtual machine (SVM) implementation that presents the cluster as a single manageable entity. In addition to serving as the highest-level administrative domain, the cluster management server owns resources that do not logically belong with a data SVM.

The cluster management server is always available on the cluster. You can access the cluster management server through the console or cluster management LIF.

Upon failure of its home network port, the cluster management LIF automatically fails over to another node in the cluster. Depending on the connectivity characteristics of the management protocol you are using, you might or might not notice the failover. If you are using a connectionless protocol (for example, SNMP) or have a limited connection (for example, HTTP), you are not likely to notice the failover. However, if you are using a

long-term connection (for example, SSH), then you will have to reconnect to the cluster management server after the failover.

When you create a cluster, all of the characteristics of the cluster management LIF are configured, including its IP address, netmask, gateway, and port.

Unlike a data SVM or node SVM, a cluster management server does not have a root volume or host user volumes (though it can host system volumes). Furthermore, a cluster management server can only have LIFs of the cluster management type.

If you run the `vserver show` command, the cluster management server appears in the output listing for that command.

## Types of SVMs

A cluster consists of four types of SVMs, which help in managing the cluster and its resources and data access to the clients and applications.

A cluster contains the following types of SVMs:

- Admin SVM

The cluster setup process automatically creates the admin SVM for the cluster. The admin SVM represents the cluster.

- Node SVM

A node SVM is created when the node joins the cluster, and the node SVM represents the individual nodes of the cluster.

- System SVM (advanced)

A system SVM is automatically created for cluster-level communications in an IPspace.

- Data SVM

A data SVM represents the data serving SVMs. After the cluster setup, a cluster administrator must create data SVMs and add volumes to these SVMs to facilitate data access from the cluster.

A cluster must have at least one data SVM to serve data to its clients.



Unless otherwise specified, the term SVM refers to a data (data-serving) SVM.

In the CLI, SVMs are displayed as Vservers.

## ONTAP management interface basics

### Access the cluster by using the CLI (cluster administrators only)

#### Access the cluster by using the serial port

You can access the cluster directly from a console that is attached to a node's serial port.

#### Steps

1. At the console, press Enter.

The system responds with the login prompt.

2. At the login prompt, do one of the following:

To access the cluster with...	Enter the following account name...
The default cluster account	<b>admin</b>
An alternative administrative user account	<i>username</i>

The system responds with the password prompt.

3. Enter the password for the admin or administrative user account, and then press Enter.

### Access the cluster by using SSH

You can issue SSH requests to the cluster to perform administrative tasks. SSH is enabled by default.

#### What you'll need

- You must have a user account that is configured to use `ssh` as an access method.

The `-application` parameter of the `security login` commands specifies the access method for a user account. The `security login man` pages contain additional information.

- If you use an Active Directory (AD) domain user account to access the cluster, an authentication tunnel for the cluster must have been set up through a CIFS-enabled storage virtual machine (SVM), and your AD domain user account must also have been added to the cluster with `ssh` as an access method and `domain` as the authentication method.
- If you use IPv6 connections, IPv6 must already be configured and enabled on the cluster, and firewall policies must already be configured with IPv6 addresses.

The `network options ipv6 show` command displays whether IPv6 is enabled. The `system services firewall policy show` command displays firewall policies.

#### About this task

- You must use an OpenSSH 5.7 or later client.
- Only the SSH v2 protocol is supported; SSH v1 is not supported.
- ONTAP supports a maximum of 64 concurrent SSH sessions per node.

If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

If the rate of incoming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

- ONTAP supports only the AES and 3DES encryption algorithms (also known as *ciphers*) for SSH.

AES is supported with 128, 192, and 256 bits in key length. 3DES is 56 bits in key length as in the original

DES, but it is repeated three times.

- When FIPS mode is on, SSH clients should negotiate with Elliptic Curve Digital Signature Algorithm (ECDSA) public key algorithms for the connection to be successful.
- If you want to access the ONTAP CLI from a Windows host, you can use a third-party utility such as PuTTY.
- If you use a Windows AD user name to log in to ONTAP, you should use the same uppercase or lowercase letters that were used when the AD user name and domain name were created in ONTAP.

AD user names and domain names are not case-sensitive. However, ONTAP user names are case-sensitive. Case mismatch between the user name created in ONTAP and the user name created in AD results in a login failure.

- Beginning with ONTAP 9.3, you can enable SSH multifactor authentication for local administrator accounts.

When SSH multifactor authentication is enabled, users are authenticated by using a public key and a password.

- Beginning with ONTAP 9.4, you can enable SSH multifactor authentication for LDAP and NIS remote users.

## Steps

1. From an administration host, enter the `ssh` command in one of the following formats:

- **`ssh username@hostname_or_IP [command]`**
- **`ssh -l username hostname_or_IP [command]`**

If you are using an AD domain user account, you must specify *username* in the format of *domainname\AD\_accountname* (with double backslashes after the domain name) or "*domainname\AD\_accountname*" (enclosed in double quotation marks and with a single backslash after the domain name).

*hostname\_or\_IP* is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

*command* is not required for SSH-interactive sessions.

## Examples of SSH requests

The following examples show how the user account named "joe" can issue an SSH request to access a cluster whose cluster management LIF is 10.72.137.28:

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```



```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

The following examples show how the user account named “john” from the domain named “DOMAIN1” can issue an SSH request to access a cluster whose cluster management LIF is 10.72.137.28:

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

The following example shows how the user account named “joe” can issue an SSH MFA request to access a cluster whose cluster management LIF is 10.72.137.32:

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                Health  Eligibility
-----
node1                true   true
node2                true   true
2 entries were displayed.
```

## Related information

### SSH login security

Beginning with ONTAP 9.5, you can view information about previous logins, unsuccessful attempts to log in, and changes to your privileges since your last successful login.

Security-related information is displayed when you successfully log in as an SSH admin user. You are alerted about the following conditions:

- The last time your account name was logged in.
- The number of unsuccessful login attempts since the last successful login.
- Whether the role has changed since the last login (for example, if the admin account's role changed from "admin" to "backup.")
- Whether the add, modify, or delete capabilities of the role were modified since the last login.



If any of the information displayed is suspicious, you should immediately contact your security department.

To obtain this information when you login, the following prerequisites must be met:

- Your SSH user account must be provisioned in ONTAP.
- Your SSH security login must be created.
- Your login attempt must be successful.

### Restrictions and other considerations for SSH login security

The following restrictions and considerations apply to SSH login security information:

- The information is available only for SSH-based logins.
- For group-based admin accounts, such as LDAP/NIS and AD accounts, users can view the SSH login information if the group of which they are a member is provisioned as an admin account in ONTAP.

However, alerts about changes to the role of the user account cannot be displayed for these users. Also, users belonging to an AD group that has been provisioned as an admin account in ONTAP cannot view the count of unsuccessful login attempts that occurred since the last time they logged in.

- The information maintained for a user is deleted when the user account is deleted from ONTAP.
- The information is not displayed for connections to applications other than SSH.

### Examples of SSH login security information

The following examples demonstrate the type of information displayed after you login.

- This message is displayed after each successful login:

```
Last Login : 7/19/2018 06:11:32
```

- These messages are displayed if there have been unsuccessful attempts to login since the last successful

login:

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- These messages are displayed if there have been unsuccessful attempts to login and your privileges were modified since the last successful login:

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

### Enable Telnet or RSH access to the cluster

As a security best practice, Telnet and RSH are disabled in the predefined management firewall policy (`mgmt`). To enable the cluster to accept Telnet or RSH requests, you must create a new management firewall policy that has Telnet or RSH enabled, and then associate the new policy with the cluster management LIF.

#### About this task

ONTAP prevents you from changing predefined firewall policies, but you can create a new policy by cloning the predefined `mgmt` management firewall policy, and then enabling Telnet or RSH under the new policy. However, Telnet and RSH are not secure protocols, so you should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session.

Perform the following steps to enable Telnet or RSH access to the clusters:

#### Steps

1. Enter the advanced privilege mode:

```
set advanced
```

2. Enable a security protocol (RSH or Telnet):

```
security protocol modify -application security_protocol -enabled true
```

3. Create a new management firewall policy based on the `mgmt` management firewall policy:

```
system services firewall policy clone -policy mgmt -new-policy-name policy-name
```

4. Enable Telnet or RSH in the new management firewall policy:

```
system services firewall policy create -policy policy-name -service security_protocol -action allow -ip-list ip_address/netmask
```

To allow all IP addresses, you should specify `-ip-list 0.0.0.0/0`

5. Associate the new policy with the cluster management LIF:

```
network interface modify -vserver cluster_management_LIF -lif cluster_mgmt
-firewall-policy policy-name
```

### Access the cluster by using Telnet

You can issue Telnet requests to the cluster to perform administrative tasks. Telnet is disabled by default.

### What you'll need

The following conditions must be met before you can use Telnet to access the cluster:

- You must have a cluster local user account that is configured to use Telnet as an access method.

The `-application` parameter of the `security login` commands specifies the access method for a user account. For more information, see the `security login` man pages.

- Telnet must already be enabled in the management firewall policy that is used by the cluster or node management LIFs so that Telnet requests can go through the firewall.

By default, Telnet is disabled. The `system services firewall policy show` command with the `-service telnet` parameter displays whether Telnet has been enabled in a firewall policy. For more information, see the `system services firewall policy` man pages.

- If you use IPv6 connections, IPv6 must already be configured and enabled on the cluster, and firewall policies must already be configured with IPv6 addresses.

The `network options ipv6 show` command displays whether IPv6 is enabled. The `system services firewall policy show` command displays firewall policies.

### About this task

- Telnet is not a secure protocol.

You should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session.

- ONTAP supports a maximum of 50 concurrent Telnet sessions per node.

If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

If the rate of in-coming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

- If you want to access the ONTAP CLI from a Windows host, you can use a third-party utility such as PuTTY.

### Steps

1. From an administration host, enter the following command:

```
telnet hostname_or_IP
```

*hostname\_or\_IP* is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

### Example of a Telnet request

The following example shows how the user named “joe”, who has been set up with Telnet access, can issue a Telnet request to access a cluster whose cluster management LIF is 10.72.137.28:

```
admin_host$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>
```

### Access the cluster by using RSH

You can issue RSH requests to the cluster to perform administrative tasks. RSH is not a secure protocol and is disabled by default.

### What you'll need

The following conditions must be met before you can use RSH to access the cluster:

- You must have a cluster local user account that is configured to use RSH as an access method.

The `-application` parameter of the `security login` commands specifies the access method for a user account. For more information, see the `security login` man pages.

- RSH must already be enabled in the management firewall policy that is used by the cluster or node management LIFs so that RSH requests can go through the firewall.

By default, RSH is disabled. The `system services firewall policy show` command with the `-service rsh` parameter displays whether RSH has been enabled in a firewall policy. For more information, see the `system services firewall policy` man pages.

- If you use IPv6 connections, IPv6 must already be configured and enabled on the cluster, and firewall policies must already be configured with IPv6 addresses.

The `network options ipv6 show` command displays whether IPv6 is enabled. The `system services firewall policy show` command displays firewall policies.

### About this task

- RSH is not a secure protocol.

You should consider using SSH to access the cluster. SSH provides a secure remote shell and interactive network session.

- ONTAP supports a maximum of 50 concurrent RSH sessions per node.

If the cluster management LIF resides on the node, it shares this limit with the node management LIF.

If the rate of in-coming connections is higher than 10 per second, the service is temporarily disabled for 60 seconds.

## Steps

1. From an administration host, enter the following command:

```
rsh hostname_or_IP -l username:passwordcommand
```

*hostname\_or\_IP* is the host name or the IP address of the cluster management LIF or a node management LIF. Using the cluster management LIF is recommended. You can use an IPv4 or IPv6 address.

*command* is the command you want to execute over RSH.

## Example of an RSH request

The following example shows how the user named “joe”, who has been set up with RSH access, can issue an RSH request to run the `cluster show` command:

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show
```

Node	Health	Eligibility
node1	true	true
node2	true	true

2 entries were displayed.

```
admin_host$
```

## Use the ONTAP command-line interface

### Using the ONTAP command-line interface

The ONTAP command-line interface (CLI) provides a command-based view of the management interface. You enter commands at the storage system prompt, and command results are displayed in text.

The CLI command prompt is represented as `cluster_name::>`.

If you set the privilege level (that is, the `-privilege` parameter of the `set` command) to `advanced`, the prompt includes an asterisk (\*), for example:

```
cluster_name::*>
```

### About the different shells for CLI commands (cluster administrators only)

### About the different shells for CLI commands overview (cluster administrators only)

The cluster has three different shells for CLI commands, the *clustershell*, the *nodeshell*,

and the *systemshell*. The shells are for different purposes, and they each have a different command set.

- The clustershell is the native shell that is started automatically when you log in to the cluster.

It provides all the commands you need to configure and manage the cluster. The clustershell CLI help (triggered by `?` at the clustershell prompt) displays available clustershell commands. The `man command_name` command in the clustershell displays the man page for the specified clustershell command.

- The nodeshell is a special shell for commands that take effect only at the node level.

The nodeshell is accessible through the `system node run` command.

The nodeshell CLI help (triggered by `?` or `help` at the nodeshell prompt) displays available nodeshell commands. The `man command_name` command in the nodeshell displays the man page for the specified nodeshell command.

Many commonly used nodeshell commands and options are tunneled or aliased into the clustershell and can be executed also from the clustershell.

- The systemshell is a low-level shell that is used only for diagnostic and troubleshooting purposes.

The systemshell and the associated “diag” account are intended for low-level diagnostic purposes. Their access requires the diagnostic privilege level and is reserved only for technical support to perform troubleshooting tasks.

## Access of nodeshell commands and options in the clustershell

Nodeshell commands and options are accessible through the nodeshell:

```
system node run -node nodename
```

Many commonly used nodeshell commands and options are tunneled or aliased into the clustershell and can be executed also from the clustershell.

Nodeshell options that are supported in the clustershell can be accessed by using the `vserver options clustershell` command. To see these options, you can do one of the following:

- Query the clustershell CLI with `vserver options -vserver nodename_or_clustername -option-name?`
- Access the `vserver options` man page in the clustershell CLI with `man vserver options`

If you enter a nodeshell or legacy command or option in the clustershell, and the command or option has an equivalent clustershell command, ONTAP informs you of the clustershell command to use.

If you enter a nodeshell or legacy command or option that is not supported in the clustershell, ONTAP informs you of the “not supported” status for the command or option.

## Display available nodeshell commands

You can obtain a list of available nodeshell commands by using the CLI help from the

nodeshell.

### Steps

1. To access the nodeshell, enter the following command at the clustershell's system prompt:

```
system node run -node {nodename|local}
```

`local` is the node you used to access the cluster.



The `system node run` command has an alias command, `run`.

2. Enter the following command in the nodeshell to see the list of available nodeshell commands:

```
[commandname] help
```

*commandname* is the name of the command whose availability you want to display. If you do not include *commandname*, the CLI displays all available nodeshell commands.

You enter `exit` or type `Ctrl-d` to return to the clustershell CLI.

### Example of displaying available nodeshell commands

The following example accesses the nodeshell of a node named `node2` and displays information for the nodeshell command `environment`:

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
      [status] [shelf [<adapter>[.<shelf-number>]]] |
      [status] [shelf_log] |
      [status] [shelf_stats] |
      [status] [shelf_power_status] |
      [status] [chassis [all | list-sensors | Temperature | PSU 1 |
PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

### Methods of navigating CLI command directories

Commands in the CLI are organized into a hierarchy by command directories. You can run commands in the hierarchy either by entering the full command path or by navigating through the directory structure.

When using the CLI, you can access a command directory by typing the directory's name at the prompt and then pressing `Enter`. The directory name is then included in the prompt text to indicate that you are interacting with the appropriate command directory. To move deeper into the command hierarchy, you type the name of a command subdirectory followed by pressing `Enter`. The subdirectory name is then included in the prompt text and the context shifts to that subdirectory.



You can navigate through several command directories by entering the entire command. For example, you can display information about disk drives by entering the `storage disk show` command at the prompt. You can also run the command by navigating through one command directory at a time, as shown in the following example:

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

You can abbreviate commands by entering only the minimum number of letters in a command that makes the command unique to the current directory. For example, to abbreviate the command in the previous example, you can enter `st d sh`. You can also use the Tab key to expand abbreviated commands and to display a command's parameters, including default parameter values.

You can use the `top` command to go to the top level of the command hierarchy, and the `up` command or `..` command to go up one level in the command hierarchy.



Commands and command options preceded by an asterisk (\*) in the CLI can be executed only at the advanced privilege level or higher.

#### Rules for specifying values in the CLI

Most commands include one or more required or optional parameters. Many parameters require you to specify a value for them. A few rules exist for specifying values in the CLI.

- A value can be a number, a Boolean specifier, a selection from an enumerated list of predefined values, or a text string.

Some parameters can accept a comma-separated list of two or more values. Comma-separated lists of values do not need to be in quotation marks (" "). Whenever you specify text, a space, or a query character (when not meant as a query or text starting with a less-than or greater-than symbol), you must enclose the entity in quotation marks.

- The CLI interprets a question mark (" ? ") as the command to display help information for a particular command.
- Some text that you enter in the CLI, such as command names, parameters, and certain values, is not case-sensitive.

For example, when you enter parameter values for the `vserver cifs` commands, capitalization is ignored. However, most parameter values, such as the names of nodes, storage virtual machines (SVMs), aggregates, volumes, and logical interfaces, are case-sensitive.

- If you want to clear the value of a parameter that takes a string or a list, you specify an empty set of quotation marks (" ") or a dash ("-").
- The hash sign (" # "), also known as the pound sign, indicates a comment for a command-line input; if used, it should appear after the last parameter in a command line.

The CLI ignores the text between " # " and the end of the line.

In the following example, an SVM is created with a text comment. The SVM is then modified to delete the

comment:

```
cluster1::> vsserver create -vsserver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipspace ipspaceA -comment "My SVM"
cluster1::> vsserver modify -vsserver vs0 -comment ""
```

In the following example, a command-line comment that uses the “#” sign indicates what the command does.

```
cluster1::> security login create -vsserver vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

### Methods of viewing command history and reissuing commands

Each CLI session keeps a history of all commands issued in it. You can view the command history of the session that you are currently in. You can also reissue commands.

To view the command history, you can use the `history` command.

To reissue a command, you can use the `redo` command with one of the following arguments:

- A string that matches part of a previous command

For example, if the only `volume` command you have run is `volume show`, you can use the `redo volume` command to reexecute the command.

- The numeric ID of a previous command, as listed by the `history` command

For example, you can use the `redo 4` command to reissue the fourth command in the history list.

- A negative offset from the end of the history list

For example, you can use the `redo -2` command to reissue the command that you ran two commands ago.

For example, to redo the command that is third from the end of the command history, you would enter the following command:

```
cluster1::> redo -3
```

## Keyboard shortcuts for editing CLI commands

The command at the current command prompt is the active command. Using keyboard shortcuts enables you to edit the active command quickly. These keyboard shortcuts are similar to those of the UNIX tcsh shell and the Emacs editor.

The following table lists the keyboard shortcuts for editing CLI commands. “Ctrl-” indicates that you press and hold the Ctrl key while typing the character specified after it. “Esc-” indicates that you press and release the Esc key and then type the character specified after it.

If you want to...	Use the following keyboard shortcut...
Move the cursor back by one character	Ctrl-B
	Back arrow
Move the cursor forward by one character	Ctrl-F
	Forward arrow
Move the cursor back by one word	Esc-B
Move the cursor forward by one word	Esc-F
Move the cursor to the beginning of the line	Ctrl-A
Move the cursor to the end of the line	Ctrl-E
Remove the content of the command line from the beginning of the line to the cursor, and save it in the cut buffer. The cut buffer acts like temporary memory, similar to what is called a <i>clipboard</i> in some programs.	Ctrl-U
Remove the content of the command line from the cursor to the end of the line, and save it in the cut buffer	Ctrl-K
Remove the content of the command line from the cursor to the end of the following word, and save it in the cut buffer	Esc-D
Remove the word before the cursor, and save it in the cut buffer	Ctrl-W
Yank the content of the cut buffer, and push it into the command line at the cursor	Ctrl-Y

If you want to...	Use the following keyboard shortcut...
Delete the character before the cursor	Ctrl-H
	Backspace
Delete the character where the cursor is	Ctrl-D
Clear the line	Ctrl-C
Clear the screen	Ctrl-L
Replace the current content of the command line with the previous entry on the history list.  With each repetition of the keyboard shortcut, the history cursor moves to the previous entry.	Ctrl-P
	Esc-P
	Up arrow
Replace the current content of the command line with the next entry on the history list. With each repetition of the keyboard shortcut, the history cursor moves to the next entry.	Ctrl-N
	Esc-N
	Down arrow
Expand a partially entered command or list valid input from the current editing position	Tab
	Ctrl-I
Display context-sensitive help	?
Escape the special mapping for the question mark (“?”) character. For instance, to enter a question mark into a command’s argument, press Esc and then the “?” character.	Esc-?
Start TTY output	Ctrl-Q
Stop TTY output	Ctrl-S

#### Use of administrative privilege levels

ONTAP commands and parameters are defined at three privilege levels: *admin*, *advanced*, and *diagnostic*. The privilege levels reflect the skill levels required in performing the tasks.

- **admin**

Most commands and parameters are available at this level. They are used for common or routine tasks.

- **advanced**

Commands and parameters at this level are used infrequently, require advanced knowledge, and can cause problems if used inappropriately.

You use advanced commands or parameters only with the advice of support personnel.

- **diagnostic**

Diagnostic commands and parameters are potentially disruptive. They are used only by support personnel to diagnose and fix problems.

### Set the privilege level in the CLI

You can set the privilege level in the CLI by using the `set` command. Changes to privilege level settings apply only to the session you are in. They are not persistent across sessions.

#### Steps

1. To set the privilege level in the CLI, use the `set` command with the `-privilege` parameter.

#### Example of setting the privilege level

The following example sets the privilege level to advanced and then to admin:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by technical support.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

### Set display preferences in the CLI

You can set display preferences for a CLI session by using the `set` command and `rows` command. The preferences you set apply only to the session you are in. They are not persistent across sessions.

#### About this task

You can set the following CLI display preferences:

- The privilege level of the command session
- Whether confirmations are issued for potentially disruptive commands
- Whether `show` commands display all fields
- The character or characters to use as the field separator
- The default unit when reporting data sizes
- The number of rows the screen displays in the current CLI session before the interface pauses output

If the preferred number of rows is not specified, it is automatically adjusted based on the actual height of the terminal. If the actual height is undefined, the default number of rows is 24.

- The default storage virtual machine (SVM) or node
- Whether a continuing command should stop if it encounters an error

**Steps**

1. To set CLI display preferences, use the `set` command.

To set the number of rows the screen displays in the current CLI session, you can also use the `rows` command.

For more information, see the man pages for the `set` command and `rows` command.

**Example of setting display preferences in the CLI**

The following example sets a comma to be the field separator, sets GB as the default data-size unit, and sets the number of rows to 50:

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

**Methods of using query operators**

The management interface supports queries and UNIX-style patterns and wildcards to enable you to match multiple values in command-parameter arguments.

The following table describes the supported query operators:

Operator	Description
*	Wildcard that matches all entries.  For example, the command <code>volume show -volume *tmp*</code> displays a list of all volumes whose names include the string <code>tmp</code> .
!	NOT operator.  Indicates a value that is not to be matched; for example, <code>!vs0</code> indicates not to match the value <code>vs0</code> .
	OR operator.  Separates two values that are to be compared; for example, <code>vs0   vs2</code> matches either <code>vs0</code> or <code>vs2</code> . You can specify multiple OR statements; for example, <code>a   b*   *c*</code> matches the entry <code>a</code> , any entry that starts with <code>b</code> , and any entry that includes <code>c</code> .

Operator	Description
..	Range operator.  For example, <b>5..10</b> matches any value from 5 to 10, inclusive.
<	Less-than operator.  For example, <b>&lt;20</b> matches any value that is less than 20.
>	Greater-than operator.  For example, <b>&gt;5</b> matches any value that is greater than 5.
<=	Less-than-or-equal-to operator.  For example, <b>&lt;=5</b> matches any value that is less than or equal to 5.
>=	Greater-than-or-equal-to operator.  For example, <b>&gt;=5</b> matches any value that is greater than or equal to 5.
{query}	Extended query.  An extended query must be specified as the first argument after the command name, before any other parameters.  For example, the command <code>volume modify {-volume *tmp*} -state offline sets offline</code> all volumes whose names include the string <code>tmp</code> .

If you want to parse query characters as literals, you must enclose the characters in double quotes (for example, “^”, “.”, “\*”, or “\$”) for the correct results to be returned.

You can use multiple query operators in one command line. For example, the command `volume show -size >1GB -percent-used <50 -vserver !vs1` displays all volumes that are greater than 1 GB in size, less than 50% utilized, and not in the storage virtual machine (SVM) named “vs1”.

#### Methods of using extended queries

You can use extended queries to match and perform operations on objects that have specified values.

You specify extended queries by enclosing them within curly brackets ({}). An extended query must be specified as the first argument after the command name, before any other parameters. For example, to set offline all volumes whose names include the string `tmp`, you run the command in the following example:

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

Extended queries are generally useful only with `modify` and `delete` commands. They have no meaning in

create or show commands.

The combination of queries and modify operations is a useful tool. However, it can potentially cause confusion and errors if implemented incorrectly. For example, using the (advanced privilege) `system node image modify` command to set a node's default software image automatically sets the other software image not to be the default. The command in the following example is effectively a null operation:

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

This command sets the current default image as the non-default image, then sets the new default image (the previous non-default image) to the non-default image, resulting in the original default settings being retained. To perform the operation correctly, you can use the command as given in the following example:

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

#### Methods of customizing show command output by using fields

When you use the `-instance` parameter with a `show` command to display details, the output can be lengthy and include more information than you need. The `-fields` parameter of a `show` command enables you to display only the information you specify.

For example, running `volume show -instance` is likely to result in several screens of information. You can use `volume show -fields fieldname[,fieldname...]` to customize the output so that it includes only the specified field or fields (in addition to the default fields that are always displayed.) You can use `-fields ?` to display valid fields for a `show` command.

The following example shows the output difference between the `-instance` parameter and the `-fields` parameter:



```

cluster1::> volume show -instance

Vserver Name: cluster1-1
Volume Name: vol0
Aggregate Name: aggr0
Volume Size: 348.3GB
Volume Data Set ID: -
Volume Master Data Set ID: -
Volume State: online
Volume Type: RW
Volume Style: flex
...
Space Guarantee Style: volume
Space Guarantee in Effect: true
...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume  space-guarantee  space-guarantee-enabled
-----  -
cluster1-1 vol0    volume           true
cluster1-2 vol0    volume           true
vs1      root_vol
          volume           true
vs2      new_vol
          volume           true
vs2      root_vol
          volume           true
...
cluster1::>

```

### About positional parameters

You can take advantage of the positional parameter functionality of the ONTAP CLI to increase efficiency in command input. You can query a command to identify parameters that are positional for the command.

### What a positional parameter is

- A positional parameter is a parameter that does not require you to specify the parameter name before specifying the parameter value.
- A positional parameter can be interspersed with nonpositional parameters in the command input, as long as it observes its relative sequence with other positional parameters in the same command, as indicated in

the ***command\_name*** ? output.

- A positional parameter can be a required or optional parameter for a command.
- A parameter can be positional for one command but nonpositional for another.



Using the positional parameter functionality in scripts is not recommended, especially when the positional parameters are optional for the command or have optional parameters listed before them.

### Identify a positional parameter

You can identify a positional parameter in the ***command\_name*** ? command output. A positional parameter has square brackets surrounding its parameter name, in one of the following formats:

- `[-parameter_name] parameter_value` shows a required parameter that is positional.
- `[[ -parameter_name] parameter_value]` shows an optional parameter that is positional.

For example, when displayed as the following in the ***command\_name*** ? output, the parameter is positional for the command it appears in:

- `[-lif] <lif-name>`
- `[[ -lif] <lif-name>]`

However, when displayed as the following, the parameter is nonpositional for the command it appears in:

- `-lif <lif-name>`
- `[-lif <lif-name>]`

### Examples of using positional parameters

In the following example, the ***volume create*** ? output shows that three parameters are positional for the command: `-volume`, `-aggregate`, and `-size`.

```

cluster1::> volume create ?
    -vserver <vserver name>                Vserver Name
    [-volume] <volume name>                Volume Name
    [-aggregate] <aggregate name>          Aggregate Name
    [[-size] {<integer>[KB|MB|GB|TB|PB]]]  Volume Size
    [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                           Volume State (default: online)
    [ -type {RW|DP|DC} ]                   Volume Type (default: RW)
    [ -policy <text> ]                     Export Policy
    [ -user <user name> ]                 User ID
    ...
    [ -space-guarantee|-s {none|volume} ]   Space Guarantee Style (default:
volume)
    [ -percent-snapshot-space <percent> ]  Space Reserved for Snapshot
Copies
    ...

```

In the following example, the `volume create` command is specified without taking advantage of the positional parameter functionality:

```

cluster1::> volume create -vserver svm1 -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0

```

The following examples use the positional parameter functionality to increase the efficiency of the command input. The positional parameters are interspersed with nonpositional parameters in the `volume create` command, and the positional parameter values are specified without the parameter names. The positional parameters are specified in the same sequence indicated by the **volume create ?** output. That is, the value for `-volume` is specified before that of `-aggregate`, which is in turn specified before that of `-size`.

```

cluster1::> volume create vol2 aggr1 1g -vserver svm1 -percent-snapshot-space 0

```

```

cluster1::> volume create -vserver svm1 vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none

```

### Methods of accessing ONTAP man pages

ONTAP manual (man) pages explain how to use ONTAP commands. They are available at the command line and on the NetApp Support Site.

The `man command_name` command displays the manual page of the specified command. If you do not specify a command name, the manual page index is displayed. You can use the `man man` command to view information about the `man` command itself. You can exit a man page by entering **q**.

The [ONTAP 9 man pages](#) contains command references for the admin-level and advanced-level ONTAP commands.

## Manage CLI sessions (cluster administrators only)

### Manage records of CLI sessions

#### Manage records of CLI sessions overview

You can record a CLI session into a file with a specified name and size limit, then upload the file to an FTP or HTTP destination. You can also display or delete files in which you previously recorded CLI sessions.

A record of a CLI session ends when you stop the recording or end the CLI session, or when the file reaches the specified size limit. The default file size limit is 1 MB. The maximum file size limit is 2 GB.

Recording a CLI session is useful, for example, if you are troubleshooting an issue and want to save detailed information or if you want to create a permanent record of space usage at a specific point in time.

#### Record a CLI session

You can use the `system script start` and `system script stop` commands to record a CLI session.

##### Steps

1. To start recording the current CLI session into a file, use the `system script start` command.

For more information about using the `system script start` command, see the man page.

ONTAP starts recording your CLI session into the specified file.

2. Proceed with your CLI session.
3. To stop recording the session, use the `system script stop` command.

For more information about using the `system script stop` command, see the man page.

ONTAP stops recording your CLI session.

#### Commands for managing records of CLI sessions

You use the `system script` commands to manage records of CLI sessions.

If you want to...	Use this command...
Start recording the current CLI session in to a specified file	<code>system script start</code>
Stop recording the current CLI session	<code>system script stop</code>
Display information about records of CLI sessions	<code>system script show</code>

If you want to...	Use this command...
Upload a record of a CLI session to an FTP or HTTP destination	<code>system script upload</code>
Delete a record of a CLI session	<code>system script delete</code>

### Related information

[ONTAP 9 commands](#)

### Commands for managing the automatic timeout period of CLI sessions

The timeout value specifies how long a CLI session remains idle before being automatically terminated. The CLI timeout value is cluster-wide. That is, every node in a cluster uses the same CLI timeout value.

By default, the automatic timeout period of CLI sessions is 30 minutes.

You use the `system timeout` commands to manage the automatic timeout period of CLI sessions.

If you want to...	Use this command...
Display the automatic timeout period for CLI sessions	<code>system timeout show</code>
Modify the automatic timeout period for CLI sessions	<code>system timeout modify</code>

### Related information

[ONTAP 9 commands](#)

## Cluster access with System Manager

### Use System Manager to access a cluster

If you prefer to use a graphic interface instead of the command-line interface (CLI) for accessing and managing a cluster, you can do so by using System Manager, which is included with ONTAP as a web service, is enabled by default, and is accessible by using a browser.

### What you'll need

- You must have a cluster user account that is configured with the `admin` role and the `http`, `ontapi`, and `console` application types.
- You must have enabled cookies and site data in the browser.

### About this task

You can use a cluster management LIF or node management LIF to access System Manager. For uninterrupted access to System Manager, you should use a cluster management LIF.

### Steps

1. Point the web browser to the IP address of the cluster management LIF:

- If you are using IPv4: **`https://cluster-mgmt-LIF`**
- If you are using IPv6: **`https://[cluster-mgmt-LIF]`**



Only HTTPS is supported for browser access of System Manager.

If the cluster uses a self-signed digital certificate, the browser might display a warning indicating that the certificate is not trusted. You can either acknowledge the risk to continue the access or install a Certificate Authority (CA) signed digital certificate on the cluster for server authentication.

2. **Optional:** If you have configured an access banner by using the CLI, then read the message that is displayed in the **Warning** dialog box, and choose the required option to proceed.

This option is not supported on systems on which Security Assertion Markup Language (SAML) authentication is enabled.

- If you do not want to continue, click **Cancel**, and close the browser.
- If you want to continue, click **OK** to navigate to the System Manager login page.

3. Log in to System Manager by using your cluster administrator credentials.

## Related information

[Managing access to web services](#)

[Accessing a node's log, core dump, and MIB files by using a web browser](#)

## About System Manager

System Manager is a graphical management interface that enables you to manage storage systems and storage objects (such as disks, volumes, and aggregates) and perform common management tasks related to storage systems from a web browser. As a cluster administrator, you can use System Manager to administer the entire cluster and its resources.



System Manager is no longer available as an executable file and is now included with ONTAP software as a web service, enabled by default, and accessible by using a browser.



The name of System Manager has changed from previous versions. Versions 9.5 and earlier were named OnCommand System Manager. Versions 9.6 and later are now called System Manager.

System Manager enables you to 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, aggregates, volumes, qtrees, and quotas.
- Configure protocols such as 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 (SVM) management operations.
- Create and configure SVMs, manage storage objects associated with SVMs, and manage SVM services.
- Monitor and manage 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.

For more information about System Manager, see the [NetApp Support Site](#).

### Ways to manage access to System Manager

You can enable or disable a web browser's access to System Manager. You can also view the System Manager log.

You can control a web browser's access to System Manager by using `vserver services web modify -name sysmgr -vserver cluster_name -enabled [true|false]`.

System Manager logging is recorded in the `/mroot/etc/log/mlog/sysmgr.log` files of the node that hosts the cluster management LIF at the time System Manager is accessed. You can view the log files by using a browser. The System Manager log is also included in AutoSupport messages.

## Using the ONTAP command-line interface

The ONTAP command-line interface (CLI) provides a command-based view of the management interface. You enter commands at the storage system prompt, and command results are displayed in text.

The CLI command prompt is represented as `cluster_name::>`.

If you set the privilege level (that is, the `-privilege` parameter of the `set` command) to advanced, the prompt includes an asterisk (\*), for example:

```
cluster_name::*>
```

### About the different shells for CLI commands overview (cluster administrators only)

The cluster has three different shells for CLI commands, the *clustershell*, the *nodeshell*, and the *systemshell*. The shells are for different purposes, and they each have a different command set.

- The *clustershell* is the native shell that is started automatically when you log in to the cluster.

It provides all the commands you need to configure and manage the cluster. The *clustershell* CLI help (triggered by `?` at the *clustershell* prompt) displays available *clustershell* commands. The `man command_name` command in the *clustershell* displays the man page for the specified *clustershell* command.

- The *nodeshell* is a special shell for commands that take effect only at the node level.

The nodeshell is accessible through the `system node run` command.

The nodeshell CLI help (triggered by `?` or `help` at the nodeshell prompt) displays available nodeshell commands. The `man command_name` command in the nodeshell displays the man page for the specified nodeshell command.

Many commonly used nodeshell commands and options are tunneled or aliased into the clustershell and can be executed also from the clustershell.

- The systemshell is a low-level shell that is used only for diagnostic and troubleshooting purposes.

The systemshell and the associated “diag” account are intended for low-level diagnostic purposes. Their access requires the diagnostic privilege level and is reserved only for technical support to perform troubleshooting tasks.

### Access of nodeshell commands and options in the clustershell

Nodeshell commands and options are accessible through the nodeshell:

```
system node run -node nodename
```

Many commonly used nodeshell commands and options are tunneled or aliased into the clustershell and can be executed also from the clustershell.

Nodeshell options that are supported in the clustershell can be accessed by using the `vserver options clustershell` command. To see these options, you can do one of the following:

- Query the clustershell CLI with `vserver options -vserver nodename_or_clustername -option-name?`
- Access the `vserver options` man page in the clustershell CLI with `man vserver options`

If you enter a nodeshell or legacy command or option in the clustershell, and the command or option has an equivalent clustershell command, ONTAP informs you of the clustershell command to use.

If you enter a nodeshell or legacy command or option that is not supported in the clustershell, ONTAP informs you of the “not supported” status for the command or option.

### Display available nodeshell commands

You can obtain a list of available nodeshell commands by using the CLI help from the nodeshell.

#### Steps

1. To access the nodeshell, enter the following command at the clustershell’s system prompt:

```
system node run -node {nodename|local}
```

`local` is the node you used to access the cluster.



The `system node run` command has an alias command, `run`.



2. Enter the following command in the nodeshell to see the list of available nodeshell commands:

```
[commandname] help
```

*commandname* is the name of the command whose availability you want to display. If you do not include *commandname*, the CLI displays all available nodeshell commands.

You enter `exit` or type `Ctrl-d` to return to the clustershell CLI.

### Example of displaying available nodeshell commands

The following example accesses the nodeshell of a node named `node2` and displays information for the nodeshell command `environment`:

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
      [status] [shelf [<adapter>[.<shelf-number>]]] |
      [status] [shelf_log] |
      [status] [shelf_stats] |
      [status] [shelf_power_status] |
      [status] [chassis [all | list-sensors | Temperature | PSU 1 |
                        PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

### Methods of navigating CLI command directories

Commands in the CLI are organized into a hierarchy by command directories. You can run commands in the hierarchy either by entering the full command path or by navigating through the directory structure.

When using the CLI, you can access a command directory by typing the directory's name at the prompt and then pressing `Enter`. The directory name is then included in the prompt text to indicate that you are interacting with the appropriate command directory. To move deeper into the command hierarchy, you type the name of a command subdirectory followed by pressing `Enter`. The subdirectory name is then included in the prompt text and the context shifts to that subdirectory.

You can navigate through several command directories by entering the entire command. For example, you can display information about disk drives by entering the `storage disk show` command at the prompt. You can also run the command by navigating through one command directory at a time, as shown in the following example:

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

You can abbreviate commands by entering only the minimum number of letters in a command that makes the

command unique to the current directory. For example, to abbreviate the command in the previous example, you can enter `st d sh`. You can also use the Tab key to expand abbreviated commands and to display a command's parameters, including default parameter values.

You can use the `top` command to go to the top level of the command hierarchy, and the `up` command or `..` command to go up one level in the command hierarchy.



Commands and command options preceded by an asterisk (\*) in the CLI can be executed only at the advanced privilege level or higher.

## Rules for specifying values in the CLI

Most commands include one or more required or optional parameters. Many parameters require you to specify a value for them. A few rules exist for specifying values in the CLI.

- A value can be a number, a Boolean specifier, a selection from an enumerated list of predefined values, or a text string.

Some parameters can accept a comma-separated list of two or more values. Comma-separated lists of values do not need to be in quotation marks (" "). Whenever you specify text, a space, or a query character (when not meant as a query or text starting with a less-than or greater-than symbol), you must enclose the entity in quotation marks.

- The CLI interprets a question mark (" ? ") as the command to display help information for a particular command.
- Some text that you enter in the CLI, such as command names, parameters, and certain values, is not case-sensitive.

For example, when you enter parameter values for the `vserver cifs` commands, capitalization is ignored. However, most parameter values, such as the names of nodes, storage virtual machines (SVMs), aggregates, volumes, and logical interfaces, are case-sensitive.

- If you want to clear the value of a parameter that takes a string or a list, you specify an empty set of quotation marks (" ") or a dash ("-").
- The hash sign (" # "), also known as the pound sign, indicates a comment for a command-line input; if used, it should appear after the last parameter in a command line.

The CLI ignores the text between " # " and the end of the line.

In the following example, an SVM is created with a text comment. The SVM is then modified to delete the comment:

```
cluster1::> vserver create -vserver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipspace ipspaceA -comment "My SVM"
cluster1::> vserver modify -vserver vs0 -comment ""
```

In the following example, a command-line comment that uses the " # " sign indicates what the command does.

```
cluster1::> security login create -vserver vs0 -user-or-group-name new-  
admin  
-application ssh -authmethod password #This command creates a new user  
account
```

## Methods of viewing command history and reissuing commands

Each CLI session keeps a history of all commands issued in it. You can view the command history of the session that you are currently in. You can also reissue commands.

To view the command history, you can use the `history` command.

To reissue a command, you can use the `redo` command with one of the following arguments:

- A string that matches part of a previous command

For example, if the only `volume` command you have run is `volume show`, you can use the `redo volume` command to reexecute the command.

- The numeric ID of a previous command, as listed by the `history` command

For example, you can use the `redo 4` command to reissue the fourth command in the history list.

- A negative offset from the end of the history list

For example, you can use the `redo -2` command to reissue the command that you ran two commands ago.

For example, to redo the command that is third from the end of the command history, you would enter the following command:

```
cluster1::> redo -3
```

## Keyboard shortcuts for editing CLI commands

The command at the current command prompt is the active command. Using keyboard shortcuts enables you to edit the active command quickly. These keyboard shortcuts are similar to those of the UNIX `tcsh` shell and the Emacs editor.

The following table lists the keyboard shortcuts for editing CLI commands. “Ctrl-” indicates that you press and hold the Ctrl key while typing the character specified after it. “Esc-” indicates that you press and release the Esc key and then type the character specified after it.

If you want to...	Use the following keyboard shortcut...
Move the cursor back by one character	Ctrl-B
	Back arrow
Move the cursor forward by one character	Ctrl-F
	Forward arrow
Move the cursor back by one word	Esc-B
Move the cursor forward by one word	Esc-F
Move the cursor to the beginning of the line	Ctrl-A
Move the cursor to the end of the line	Ctrl-E
Remove the content of the command line from the beginning of the line to the cursor, and save it in the cut buffer. The cut buffer acts like temporary memory, similar to what is called a <i>clipboard</i> in some programs.	Ctrl-U
Remove the content of the command line from the cursor to the end of the line, and save it in the cut buffer	Ctrl-K
Remove the content of the command line from the cursor to the end of the following word, and save it in the cut buffer	Esc-D
Remove the word before the cursor, and save it in the cut buffer	Ctrl-W
Yank the content of the cut buffer, and push it into the command line at the cursor	Ctrl-Y
Delete the character before the cursor	Ctrl-H
	Backspace
Delete the character where the cursor is	Ctrl-D
Clear the line	Ctrl-C
Clear the screen	Ctrl-L

If you want to...	Use the following keyboard shortcut...
Replace the current content of the command line with the previous entry on the history list.  With each repetition of the keyboard shortcut, the history cursor moves to the previous entry.	Ctrl-P
	Esc-P
	Up arrow
Replace the current content of the command line with the next entry on the history list. With each repetition of the keyboard shortcut, the history cursor moves to the next entry.	Ctrl-N
	Esc-N
	Down arrow
Expand a partially entered command or list valid input from the current editing position	Tab
	Ctrl-I
Display context-sensitive help	?
Escape the special mapping for the question mark ("?",) character. For instance, to enter a question mark into a command's argument, press Esc and then the "?" character.	Esc-?
Start TTY output	Ctrl-Q
Stop TTY output	Ctrl-S

### Use of administrative privilege levels

ONTAP commands and parameters are defined at three privilege levels: *admin*, *advanced*, and *diagnostic*. The privilege levels reflect the skill levels required in performing the tasks.

- **admin**

Most commands and parameters are available at this level. They are used for common or routine tasks.

- **advanced**

Commands and parameters at this level are used infrequently, require advanced knowledge, and can cause problems if used inappropriately.

You use advanced commands or parameters only with the advice of support personnel.

- **diagnostic**

Diagnostic commands and parameters are potentially disruptive. They are used only by support personnel

to diagnose and fix problems.

## Set the privilege level in the CLI

You can set the privilege level in the CLI by using the `set` command. Changes to privilege level settings apply only to the session you are in. They are not persistent across sessions.

### Steps

1. To set the privilege level in the CLI, use the `set` command with the `-privilege` parameter.

### Example of setting the privilege level

The following example sets the privilege level to advanced and then to admin:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by technical support.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

## Set display preferences in the CLI

You can set display preferences for a CLI session by using the `set` command and `rows` command. The preferences you set apply only to the session you are in. They are not persistent across sessions.

### About this task

You can set the following CLI display preferences:

- The privilege level of the command session
- Whether confirmations are issued for potentially disruptive commands
- Whether `show` commands display all fields
- The character or characters to use as the field separator
- The default unit when reporting data sizes
- The number of rows the screen displays in the current CLI session before the interface pauses output

If the preferred number of rows is not specified, it is automatically adjusted based on the actual height of the terminal. If the actual height is undefined, the default number of rows is 24.

- The default storage virtual machine (SVM) or node
- Whether a continuing command should stop if it encounters an error

### Steps

1. To set CLI display preferences, use the `set` command.

To set the number of rows the screen displays in the current CLI session, you can also use the `rows`

command.

For more information, see the man pages for the `set` command and `rows` command.

### Example of setting display preferences in the CLI

The following example sets a comma to be the field separator, sets GB as the default data-size unit, and sets the number of rows to 50:

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

### Methods of using query operators

The management interface supports queries and UNIX-style patterns and wildcards to enable you to match multiple values in command-parameter arguments.

The following table describes the supported query operators:

Operator	Description
*	Wildcard that matches all entries.  For example, the command <code>volume show -volume *tmp*</code> displays a list of all volumes whose names include the string <code>tmp</code> .
!	NOT operator.  Indicates a value that is not to be matched; for example, <code>!vs0</code> indicates not to match the value <code>vs0</code> .
	OR operator.  Separates two values that are to be compared; for example, <code>vs0   vs2</code> matches either <code>vs0</code> or <code>vs2</code> . You can specify multiple OR statements; for example, <code>a   b*   *c*</code> matches the entry <code>a</code> , any entry that starts with <code>b</code> , and any entry that includes <code>c</code> .
..	Range operator.  For example, <code>5..10</code> matches any value from 5 to 10, inclusive.
<	Less-than operator.  For example, <code>&lt;20</code> matches any value that is less than 20.
>	Greater-than operator.  For example, <code>&gt;5</code> matches any value that is greater than 5.

Operator	Description
<=	Less-than-or-equal-to operator.  For example, <=5 matches any value that is less than or equal to 5.
>=	Greater-than-or-equal-to operator.  For example, >=5 matches any value that is greater than or equal to 5.
{query}	Extended query.  An extended query must be specified as the first argument after the command name, before any other parameters.  For example, the command <code>volume modify {-volume *tmp*} -state offline</code> sets offline all volumes whose names include the string <code>tmp</code> .

If you want to parse query characters as literals, you must enclose the characters in double quotes (for example, “^”, “.”, “\*”, or “\$”) for the correct results to be returned.

You can use multiple query operators in one command line. For example, the command `volume show -size >1GB -percent-used <50 -vserver !vs1` displays all volumes that are greater than 1 GB in size, less than 50% utilized, and not in the storage virtual machine (SVM) named “vs1”.

### Methods of using extended queries

You can use extended queries to match and perform operations on objects that have specified values.

You specify extended queries by enclosing them within curly brackets ({}). An extended query must be specified as the first argument after the command name, before any other parameters. For example, to set offline all volumes whose names include the string `tmp`, you run the command in the following example:

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

Extended queries are generally useful only with `modify` and `delete` commands. They have no meaning in `create` or `show` commands.

The combination of queries and modify operations is a useful tool. However, it can potentially cause confusion and errors if implemented incorrectly. For example, using the (advanced privilege) `system node image modify` command to set a node’s default software image automatically sets the other software image not to be the default. The command in the following example is effectively a null operation:

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

This command sets the current default image as the non-default image, then sets the new default image (the previous non-default image) to the non-default image, resulting in the original default settings being retained.



To perform the operation correctly, you can use the command as given in the following example:

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

### Methods of customizing show command output by using fields

When you use the `-instance` parameter with a `show` command to display details, the output can be lengthy and include more information than you need. The `-fields` parameter of a `show` command enables you to display only the information you specify.

For example, running `volume show -instance` is likely to result in several screens of information. You can use `volume show -fields fieldname[,fieldname...]` to customize the output so that it includes only the specified field or fields (in addition to the default fields that are always displayed.) You can use `-fields ?` to display valid fields for a `show` command.

The following example shows the output difference between the `-instance` parameter and the `-fields` parameter:

```

cluster1::> volume show -instance

Vserver Name: cluster1-1
Volume Name: vol0
Aggregate Name: aggr0
Volume Size: 348.3GB
Volume Data Set ID: -
Volume Master Data Set ID: -
Volume State: online
Volume Type: RW
Volume Style: flex
...
Space Guarantee Style: volume
Space Guarantee in Effect: true
...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume  space-guarantee  space-guarantee-enabled
-----  -
cluster1-1 vol0    volume           true
cluster1-2 vol0    volume           true
vs1      root_vol
          volume           true
vs2      new_vol
          volume           true
vs2      root_vol
          volume           true
...
cluster1::>

```

## About positional parameters

You can take advantage of the positional parameter functionality of the ONTAP CLI to increase efficiency in command input. You can query a command to identify parameters that are positional for the command.

### What a positional parameter is

- A positional parameter is a parameter that does not require you to specify the parameter name before specifying the parameter value.
- A positional parameter can be interspersed with nonpositional parameters in the command input, as long as it observes its relative sequence with other positional parameters in the same command, as indicated in

the ***command\_name*** ? output.

- A positional parameter can be a required or optional parameter for a command.
- A parameter can be positional for one command but nonpositional for another.



Using the positional parameter functionality in scripts is not recommended, especially when the positional parameters are optional for the command or have optional parameters listed before them.

### Identify a positional parameter

You can identify a positional parameter in the ***command\_name*** ? command output. A positional parameter has square brackets surrounding its parameter name, in one of the following formats:

- `[-parameter_name] parameter_value` shows a required parameter that is positional.
- `[[ -parameter_name] parameter_value]` shows an optional parameter that is positional.

For example, when displayed as the following in the ***command\_name*** ? output, the parameter is positional for the command it appears in:

- `[-lif] <lif-name>`
- `[[ -lif] <lif-name>]`

However, when displayed as the following, the parameter is nonpositional for the command it appears in:

- `-lif <lif-name>`
- `[-lif <lif-name>]`

### Examples of using positional parameters

In the following example, the ***volume create*** ? output shows that three parameters are positional for the command: `-volume`, `-aggregate`, and `-size`.

```

cluster1::> volume create ?
    -vserver <vserver name>                Vserver Name
    [-volume] <volume name>                Volume Name
    [-aggregate] <aggregate name>          Aggregate Name
    [[-size] {<integer>[KB|MB|GB|TB|PB]]]  Volume Size
    [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                           Volume State (default: online)
    [ -type {RW|DP|DC} ]                   Volume Type (default: RW)
    [ -policy <text> ]                     Export Policy
    [ -user <user name> ]                  User ID
    ...
    [ -space-guarantee|-s {none|volume} ]   Space Guarantee Style (default:
volume)
    [ -percent-snapshot-space <percent> ]   Space Reserved for Snapshot
Copies
    ...

```

In the following example, the `volume create` command is specified without taking advantage of the positional parameter functionality:

```

cluster1::> volume create -vserver svm1 -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0

```

The following examples use the positional parameter functionality to increase the efficiency of the command input. The positional parameters are interspersed with nonpositional parameters in the `volume create` command, and the positional parameter values are specified without the parameter names. The positional parameters are specified in the same sequence indicated by the **volume create ?** output. That is, the value for `-volume` is specified before that of `-aggregate`, which is in turn specified before that of `-size`.

```

cluster1::> volume create vol2 aggr1 1g -vserver svm1 -percent-snapshot-space 0

```

```

cluster1::> volume create -vserver svm1 vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none

```

## Methods of accessing ONTAP man pages

ONTAP manual (man) pages explain how to use ONTAP commands. They are available at the command line and on the NetApp Support Site.

The `man command_name` command displays the manual page of the specified command. If you do not specify a command name, the manual page index is displayed. You can use the `man man` command to view information about the `man` command itself. You can exit a man page by entering **q**.

The [ONTAP 9 man pages](#) contains command references for the admin-level and advanced-level ONTAP commands.

## Cluster management basics (cluster administrators only)

### Display information about the nodes in a cluster

You can display node names, whether the nodes are healthy, and whether they are eligible to participate in the cluster. At the advanced privilege level, you can also display whether a node holds epsilon.

#### Steps

1. To display information about the nodes in a cluster, use the `cluster show` command.

If you want the output to show whether a node holds epsilon, run the command at the advanced privilege level.

### Examples of displaying the nodes in a cluster

The following example displays information about all nodes in a four-node cluster:

```
cluster1::> cluster show
Node                Health  Eligibility
-----
node1               true   true
node2               true   true
node3               true   true
node4               true   true
```

The following example displays detailed information about the node named “node1” at the advanced privilege level:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

      Node: node1
Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
  Epsilon: false
Eligibility: true
      Health: true
```

### Display cluster attributes

You can display a cluster’s unique identifier (UUID), name, serial number, location, and contact information.

## Steps

1. To display a cluster's attributes, use the `cluster identity show` command.

## Example of displaying cluster attributes

The following example displays the name, serial number, location, and contact information of a cluster.

```
cluster1::> cluster identity show

Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
Cluster Name: cluster1
Cluster Serial Number: 1-80-123456
Cluster Location: Sunnyvale
Cluster Contact: jsmith@example.com
```

## Modify cluster attributes

You can modify a cluster's attributes, such as the cluster name, location, and contact information as needed.

### About this task

You cannot change a cluster's UUID, which is set when the cluster is created.

## Steps

1. To modify cluster attributes, use the `cluster identity modify` command.

The `-name` parameter specifies the name of the cluster. The `cluster identity modify man` page describes the rules for specifying the cluster's name.

The `-location` parameter specifies the location for the cluster.

The `-contact` parameter specifies the contact information such as a name or e-mail address.

## Example of renaming a cluster

The following command renames the current cluster ("cluster1") to "cluster2":

```
cluster1::> cluster identity modify -name cluster2
```

## Display the status of cluster replication rings

You can display the status of cluster replication rings to help you diagnose cluster-wide problems. If your cluster is experiencing problems, support personnel might ask you to perform this task to assist with troubleshooting efforts.

## Steps

1. To display the status of cluster replication rings, use the `cluster ring show` command at the advanced privilege level.

### Example of displaying cluster ring-replication status

The following example displays the status of the VLDB replication ring on a node named node0:

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
      Node: node0
    Unit Name: vldb
      Status: master
      Epoch: 5
Master Node: node0
  Local Node: node0
      DB Epoch: 5
DB Transaction: 56
  Number Online: 4
      RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412
```

### About quorum and epsilon

Quorum and epsilon are important measures of cluster health and function that together indicate how clusters address potential communications and connectivity challenges.

*Quorum* is a precondition for a fully functioning cluster. When a cluster is in quorum, a simple majority of nodes are healthy and can communicate with each other. When quorum is lost, the cluster loses the ability to accomplish normal cluster operations. Only one collection of nodes can have quorum at any one time because all of the nodes collectively share a single view of the data. Therefore, if two non-communicating nodes are permitted to modify the data in divergent ways, it is no longer possible to reconcile the data into a single data view.

Each node in the cluster participates in a voting protocol that elects one node *master*; each remaining node is a *secondary*. The master node is responsible for synchronizing information across the cluster. When quorum is formed, it is maintained by continual voting. If the master node goes offline and the cluster is still in quorum, a new master is elected by the nodes that remain online.

Because there is the possibility of a tie in a cluster that has an even number of nodes, one node has an extra fractional voting weight called *epsilon*. If the connectivity between two equal portions of a large cluster fails, the group of nodes containing epsilon maintains quorum, assuming that all of the nodes are healthy. For example, the following illustration shows a four-node cluster in which two of the nodes have failed. However, because one of the surviving nodes holds epsilon, the cluster remains in quorum even though there is not a simple majority of healthy nodes.



Epsilon is automatically assigned to the first node when the cluster is created. If the node that holds epsilon becomes unhealthy, takes over its high-availability partner, or is taken over by its high-availability partner, then epsilon is automatically reassigned to a healthy node in a different HA pair.

Taking a node offline can affect the ability of the cluster to remain in quorum. Therefore, ONTAP issues a warning message if you attempt an operation that will either take the cluster out of quorum or else put it one outage away from a loss of quorum. You can disable the quorum warning messages by using the `cluster quorum-service options modify` command at the advanced privilege level.

In general, assuming reliable connectivity among the nodes of the cluster, a larger cluster is more stable than a smaller cluster. The quorum requirement of a simple majority of half the nodes plus epsilon is easier to maintain in a cluster of 24 nodes than in a cluster of two nodes.

A two-node cluster presents some unique challenges for maintaining quorum. Two-node clusters use *cluster HA*, in which neither node holds epsilon; instead, both nodes are continuously polled to ensure that if one node fails, the other has full read-write access to data, as well as access to logical interfaces and management functions.

### What system volumes are

System volumes are FlexVol volumes that contain special metadata, such as metadata for file services audit logs. These volumes are visible in the cluster so that you can fully account for storage use in your cluster.

System volumes are owned by the cluster management server (also called the admin SVM), and they are created automatically when file services auditing is enabled.

You can view system volumes by using the `volume show` command, but most other volume operations are not permitted. For example, you cannot modify a system volume by using the `volume modify` command.

This example shows four system volumes on the admin SVM, which were automatically created when file services auditing was enabled for a data SVM in the cluster:



```
cluster1::> volume show -vserver cluster1
```

Vserver	Volume	Aggregate	State	Type	Size	Available
Used%						
-----	-----	-----	-----	-----	-----	-----
-----						
cluster1	MDV_aud_1d0131843d4811e296fc123478563412	aggr0	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_8be27f813d7311e296fc123478563412	root_vs0	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_9dc4ad503d7311e296fc123478563412	aggr1	online	RW	2GB	1.90GB
5%						
cluster1	MDV_aud_a4b887ac3d7311e296fc123478563412	aggr2	online	RW	2GB	1.90GB
5%						

4 entries were displayed.

## Manage nodes

### Display node attributes

You can display the attributes of one or more nodes in the cluster, for example, the name, owner, location, model number, serial number, how long the node has been running, health state, and eligibility to participate in a cluster.

### Steps

1. To display the attributes of a specified node or about all nodes in a cluster, use the `system node show` command.

### Example of displaying information about a node

The following example displays detailed information about node1:

```
cluster1::> system node show -node node1
Node: node1
Owner: Eng IT
Location: Lab 5
Model: model_number
Serial Number: 12345678
Asset Tag: -
Uptime: 23 days 04:42
NVRAM System ID: 118051205
System ID: 0118051205
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: true
Capacity Optimized: false
QLC Optimized: false
All-Flash Select Optimized: false
SAS2/SAS3 Mixed Stack Support: none
```

## Modify node attributes

You can modify the attributes of a node as required. The attributes that you can modify include the node's owner information, location information, asset tag, and eligibility to participate in the cluster.

### About this task

A node's eligibility to participate in the cluster can be modified at the advanced privilege level by using the `-eligibility` parameter of the `system node modify` or `cluster modify` command. If you set a node's eligibility to `false`, the node becomes inactive in the cluster.



You cannot modify node eligibility locally. It must be modified from a different node. Node eligibility also cannot be modified with a cluster HA configuration.



You should avoid setting a node's eligibility to `false`, except for situations such as restoring the node configuration or prolonged node maintenance. SAN and NAS data access to the node might be impacted when the node is ineligible.

### Steps

1. Use the `system node modify` command to modify a node's attributes.

### Example of modifying node attributes

The following command modifies the attributes of the "node1" node. The node's owner is set to "Joe Smith" and its asset tag is set to "js1234":

```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag js1234
```

## Rename a node

You can change a node's name as required.

### Steps

1. To rename a node, use the `system node rename` command.

The `-newname` parameter specifies the new name for the node. The `system node rename` man page describes the rules for specifying the node name.

If you want to rename multiple nodes in the cluster, you must run the command for each node individually.



Node name cannot be "all" because "all" is a system reserved name.

### Example of renaming a node

The following command renames node "node1" to "node1a":

```
cluster1::> system node rename -node node1 -newname node1a
```

## Add nodes to the cluster

After a cluster is created, you can expand it by adding nodes to it. You add only one node at a time.

### What you'll need

- If you are adding nodes to a multiple-node cluster, more than half of the existing nodes in the cluster must be healthy (indicated by `cluster show`).
- If you are adding nodes to a two-node switchless cluster, you must have installed and configured the cluster management and interconnect switches before adding additional nodes.

The switchless cluster functionality is supported only in a two-node cluster.

When a cluster contains or grows to more than two nodes, cluster HA is not required and is disabled automatically.

- If you are adding a second node to a single-node cluster, the second node must have been installed, and the cluster network must have been configured.
- If the cluster has the SP automatic configuration enabled, the subnet specified for the SP to use must have available resources for the joining node.

A node that joins the cluster uses the specified subnet to perform automatic configuration for the SP.

- You must have gathered the following information for the new node's node management LIF:
  - Port

- IP address
- Netmask
- Default gateway

### About this task

Nodes must be in even numbers so that they can form HA pairs. After you start to add a node to the cluster, you must complete the process. The node must be part of the cluster before you can start to add another node.

### Steps

1. Power on the node that you want to add to the cluster.

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

```
Welcome to node setup.
```

```
You can enter the following commands at any time:
```

```
"help" or "?" - if you want to have a question clarified,
```

```
"back" - if you want to change previously answered questions, and
```

```
"exit" or "quit" - if you want to quit the setup wizard.
```

```
Any changes you made before quitting will be saved.
```

```
To accept a default or omit a question, do not enter a value.
```

```
Enter the node management interface port [e0c]:
```

2. Exit the Node Setup wizard: `exit`

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

3. Log in to the admin account by using the `admin` user name.
4. Start the Cluster Setup wizard:

```
cluster setup
```

```
::> cluster setup
```

Welcome to the cluster setup wizard.

You can enter the following commands at any time:

"help" or "?" - if you want to have a question clarified,  
"back" - if you want to change previously answered questions, and  
"exit" or "quit" - if you want to quit the cluster setup wizard.  
Any changes you made before quitting will be saved.

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

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:



For more information on setting up a cluster using the setup GUI, see the [System Manager](#) online help.

5. Press Enter to use the CLI to complete this task. When prompted to create a new cluster or join an existing one, enter **join**.

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

6. Follow the prompts to set up the node and join it to the cluster:
  - To accept the default value for a prompt, press Enter.
  - To enter your own value for a prompt, enter the value, and then press Enter.
7. Repeat the preceding steps for each additional node that you want to add.

### After you finish

After adding nodes to the cluster, you should enable storage failover for each HA pair.

### Remove nodes from the cluster

You can remove unwanted nodes from a cluster, one node at a time. After you remove a node, you must also remove its failover partner. If you are removing a node, then its data becomes inaccessible or erased.

### What you'll need

- More than half of the nodes in the cluster must be healthy.
- All of the data on the node that you want to remove must have been evacuated.
- All intercluster LIFs must have been removed.



When you remove intercluster LIFs a warning is displayed that can be ignored.

You must not perform operations such as `cluster remove-node`, `cluster unjoin`, and `node rename` when an automated ONTAP upgrade is in progress.

### About this task

If you are running a mixed-version cluster, you can remove the last low-version node by using one of the advanced privilege commands beginning with ONTAP 9.3:

- ONTAP 9.3: `cluster unjoin -skip-last-low-version-node-check`
- ONTAP 9.4 and later: `cluster remove-node -skip-last-low-version-node-check`



You must make all of the system and user data from the disks that are connected to the node inaccessible to users before removing a node from the cluster. After removing a node from the cluster, if you need to join the node back to the same cluster, contact technical support for assistance about restoring data.

### Steps

1. Change the privilege level to advanced:

```
set -privilege advanced
```

2. If Storage Encryption is enabled on the cluster and the self-encrypting disks (SEDs) are operating you must set the data-id-key to 0x0.

- a. Set the data-id-key to 0x0:

```
storage encryption disk modify -disk \[disk_path_name\] -data-key-id 0x0
```

- b. Optional: If Storage Encryption is enabled and the SEDs are operating in the Federal Information Processing Standard (FIPS) compliance mode, in addition to setting the data-id-key you must also disable the FIPS compliance mode.

This enables the disks that are attached to the node to be sanitized and repurposed after the node is removed from the cluster.

- Display the SEDs that are currently in the FIPS compliance mode:

```
storage encryption disk show -fips
```

- Disable the FIPS compliance mode:

```
storage encryption disk modify disk [disk_path_name] -fips-key-id 0x0
```

- Verify that the modified SEDs are no longer in the FIPS compliance mode:

```
storage encryption disk show -fips
```

3. If the node you want to remove is the current master node, then enable another node in the cluster to be elected as the master node by changing the master node's cluster eligibility to `false`:

```
cluster modify -eligibility false
```

The master node is the node that holds processes such as “mgmt”, “vldb”, “vifmgr”, “bcomd”, and “crs”. The `cluster ring show` advanced command shows the current master node.

```
cluster::*> cluster modify -node node1 -eligibility false
```

4. Remove the node from the cluster:

For this ONTAP version...	Use this command...
ONTAP 9.3	<b>cluster unjoin</b>
ONTAP 9.4 and later	<b>cluster remove-node</b>

If you have a mixed version cluster and you are removing the last lower version node, use the `-skip -last-low-version-node-check` parameter with these commands.

The system informs you of the following:

- You must also remove the node's failover partner from the cluster.
- After the node is removed and before it can rejoin a cluster, you must use boot menu option (4) Clean configuration and initialize all disks or option (9) Configure Advanced Drive Partitioning to erase the node's configuration and initialize all disks.

A failure message is generated if you have conditions that you must address before removing the node. For example, the message might indicate that the node has shared resources that you must remove or that the node is in a cluster HA configuration or storage failover configuration that you must disable.

If the node is the quorum master, the cluster will briefly lose and then return to quorum. This quorum loss is temporary and does not affect any data operations.

5. If a failure message indicates error conditions, address those conditions and rerun the `cluster remove-node` or `cluster unjoin` command.

The node is automatically rebooted after it is successfully removed from the cluster.

6. If you are repurposing the node, erase the node configuration and initialize all disks:
  - a. During the boot process, press Ctrl-C to display the boot menu when prompted to do so.
  - b. Select the boot menu option **(4) Clean configuration and initialize all disks**.
7. Return to admin privilege level:

```
set -privilege admin
```

8. Repeat the preceding steps to remove the failover partner from the cluster.

## After you finish

If you removed nodes to have a single-node cluster, you should modify the cluster ports to serve data traffic by modifying the cluster ports to be data ports, and then creating data LIFs on the data ports.

## Access a node's log, core dump, and MIB files by using a web browser

The Service Processor Infrastructure (`spi`) web service is enabled by default to enable a web browser to access the log, core dump, and MIB files of a node in the cluster. The files remain accessible even when the node is down, provided that the node is taken over by its partner.

### What you'll need

- The cluster management LIF must be up.

You can use the management LIF of the cluster or a node to access the `spi` web service. However, using the cluster management LIF is recommended.

The `network interface show` command displays the status of all LIFs in the cluster.

- If your user account does not have the “admin” role (which has access to the `spi` web service by default), your access-control role must be granted access to the `spi` web service.

The `vserver services web access show` command shows what roles are granted access to which web services.

- If you are not using the “admin” user account (which includes the `http` access method by default), your user account must be set up with the `http` access method.

The `security login show` command shows user accounts' access and login methods and their access-control roles.

- If you want to use HTTPS for secure web access, SSL must be enabled and a digital certificate must be installed.

The `system services web show` command displays the configuration of the web protocol engine at the cluster level.

### About this task

The `spi` web service is enabled by default, and the service can be disabled manually (`vserver services web modify -vserver * -name spi -enabled false`).

The “admin” role is granted access to the `spi` web service by default, and the access can be disabled manually (`services web access delete -vserver cluster_name -name spi -role admin`).

### Steps

1. Point the web browser to the `spi` web service URL in one of the following formats:

- `http://cluster-mgmt-LIF/spi/`
- `https://cluster-mgmt-LIF/spi/`

`cluster-mgmt-LIF` is the IP address of the cluster management LIF.



2. When prompted by the browser, enter your user account and password.

After your account is authenticated, the browser displays links to the `/mroot/etc/log/`, `/mroot/etc/crash/`, and `/mroot/etc/mib/` directories of each node in the cluster.

## Access the system console of a node

If a node is hanging at the boot menu or the boot environment prompt, you can access it only through the system console (also called the *serial console*). You can access the system console of a node from an SSH connection to the node's SP or to the cluster.

### About this task

Both the SP and ONTAP offer commands that enable you to access the system console. However, from the SP, you can access only the system console of its own node. From the cluster, you can access the system console of any node in the cluster.

### Steps

1. Access the system console of a node:

If you are in the...	Enter this command...
SP CLI of the node	<code>system console</code>
ONTAP CLI	<code>system node run-console</code>

2. Log in to the system console when you are prompted to do so.
3. To exit the system console, press Ctrl-D.

### Examples of accessing the system console

The following example shows the result of entering the `system console` command at the "SP node2" prompt. The system console indicates that node2 is hanging at the boot environment prompt. The `boot_ontap` command is entered at the console to boot the node to ONTAP. Ctrl-D is then pressed to exit the console and return to the SP.

```
SP node2> system console
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap

...
*****
*                                     *
* Press Ctrl-C for Boot Menu.      *
*                                     *
*****
...

```

(Ctrl-D is pressed to exit the system console.)

```
Connection to 123.12.123.12 closed.  
SP node2>
```

The following example shows the result of entering the `system node run-console -node node2` command from ONTAP to access the system console of node2, which is hanging at the boot environment prompt. The `boot_ontap` command is entered at the console to boot node2 to ONTAP. Ctrl-D is then pressed to exit the console and return to ONTAP.

```
cluster1::> system node run-console -node node2  
Pressing Ctrl-D will end this session and any further sessions you might  
open on top of this session.  
Type Ctrl-D to exit.  
  
LOADER>  
LOADER> boot_ontap  
  
...  
*****  
*                                     *  
* Press Ctrl-C for Boot Menu. *  
*                                     *  
*****  
...  

```

(Ctrl-D is pressed to exit the system console.)

```
Connection to 123.12.123.12 closed.  
cluster1::>
```

## Rules governing node root volumes and root aggregates

### Rules governing node root volumes and root aggregates overview

A node's root volume contains special directories and files for that node. The root aggregate contains the root volume. A few rules govern a node's root volume and root aggregate.

A node's root volume is a FlexVol volume that is installed at the factory or by setup software. It is reserved for system files, log files, and core files. The directory name is `/mroot`, which is accessible only through the systemshell by technical support. The minimum size for a node's root volume depends on the platform model.

- The following rules govern the node's root volume:
  - Unless technical support instructs you to do so, do not modify the configuration or content of the root volume.

- Do not store user data in the root volume.

Storing user data in the root volume increases the storage giveback time between nodes in an HA pair.

- You can move the root volume to another aggregate.

#### [Relocate root volumes to new aggregates](#)

- The root aggregate is dedicated to the node's root volume only.

ONTAP prevents you from creating other volumes in the root aggregate.

## NetApp Hardware Universe

### Free up space on a node's root volume

A warning message appears when a node's root volume has become full or almost full. The node cannot operate properly when its root volume is full. You can free up space on a node's root volume by deleting core dump files, packet trace files, and root volume Snapshot copies.

#### Steps

1. Display the node's core dump files and their names by using the `system node coredump show` command.
2. Delete unwanted core dump files from the node by using the `system node coredump delete` command.
3. Access the nodeshell:

```
system node run -node nodename
```

*nodename* is the name of the node whose root volume space you want to free up.

4. Switch to the nodeshell advanced privilege level from the nodeshell:

```
priv set advanced
```

5. Display and delete the node's packet trace files through the nodeshell:

- a. Display all files in the node's root volume:

```
ls /etc
```

- b. If any packet trace files (`*.trc`) are in the node's root volume, delete them individually:

```
rm /etc/log/packet_traces/file_name.trc
```

6. Identify and delete the node's root volume Snapshot copies through the nodeshell:

- a. Identify the root volume name:

```
vol status
```

The root volume is indicated by the word "root" in the "Options" column of the `vol status` command

output.

In the following example, the root volume is `vol0`:

```
node1*> vol status
```

Volume	State	Status	Options
vol0	online	raid_dp, flex 64-bit	root, nvfail=on

b. Display root volume Snapshot copies:

```
snap list root_vol_name
```

c. Delete unwanted root volume Snapshot copies:

```
snap delete root_vol_name snapshot_name
```

7. Exit the nodeshell and return to the clustershell:

```
exit
```

### Relocate root volumes to new aggregates

The root replacement procedure migrates the current root aggregate to another set of disks without disruption.

#### About this task

Storage failover must be enabled to relocate root volumes. You can use the `storage failover modify -node nodename -enable true` command to enable failover.

You can change the location of the root volume to a new aggregate in the following scenarios:

- When the root aggregates are not on the disk you prefer
- When you want to rearrange the disks connected to the node
- When you are performing a shelf replacement of the EOS disk shelves

#### Steps

1. Set the privilege level to advanced:

```
set privilege advanced
```

2. Relocate the root aggregate:

```
system node migrate-root -node nodename -disklist disklist -raid-type raid-type
```

- **-node**

Specifies the node that owns the root aggregate that you want to migrate.

- **-disklist**

Specifies the list of disks on which the new root aggregate will be created. All disks must be spares and owned by the same node. The minimum number of disks required is dependent on the RAID type.

- **-raid-type**

Specifies the RAID type of the root aggregate. The default value is `raid-dp`.

### 3. Monitor the progress of the job:

```
job show -id jobid -instance
```

## Results

If all of the pre-checks are successful, the command starts a root volume replacement job and exits. Expect the node to restart.

## Start or stop a node

### Start or stop a node overview

You might need to start or stop a node for maintenance or troubleshooting reasons. You can do so from the ONTAP CLI, the boot environment prompt, or the SP CLI.

Using the SP CLI command `system power off` or `system power cycle` to turn off or power-cycle a node might cause an improper shutdown of the node (also called a *dirty shutdown*) and is not a substitute for a graceful shutdown using the ONTAP `system node halt` command.

### Reboot a node at the system prompt

You can reboot a node in normal mode from the system prompt. A node is configured to boot from the boot device, such as a PC CompactFlash card.

## Steps

1. If the cluster contains four or more nodes, verify that the node to be rebooted does not hold epsilon:
  - a. Set the privilege level to advanced:

```
set -privilege advanced
```

- b. Determine which node holds epsilon:

```
cluster show
```

The following example shows that “node1” holds epsilon:

```
cluster1::*> cluster show
Node           Health Eligibility  Epsilon
-----
node1          true  true        true
node2          true  true        false
node3          true  true        false
node4          true  true        false
4 entries were displayed.
```

- c. If the node to be rebooted holds epsilon, then remove epsilon from the node:

```
cluster modify -node node_name -epsilon false
```

- d. Assign epsilon to a different node that will remain up:

```
cluster modify -node node_name -epsilon true
```

- e. Return to the admin privilege level:

```
set -privilege admin
```

2. Use the `system node reboot` command to reboot the node.

If you do not specify the `-skip-lif-migration` parameter, the command attempts to migrate data and cluster management LIFs synchronously to another node prior to the reboot. If the LIF migration fails or times out, the rebooting process is aborted, and ONTAP displays an error to indicate the LIF migration failure.

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

The node begins the reboot process. The ONTAP login prompt appears, indicating that the reboot process is complete.

### Boot ONTAP at the boot environment prompt

You can boot the current release or the backup release of ONTAP when you are at the boot environment prompt of a node.

#### Steps

1. Access the boot environment prompt from the storage system prompt by using the `system node halt` command.

The storage system console displays the boot environment prompt.

2. At the boot environment prompt, enter one of the following commands:

To boot...	Enter...
The current release of ONTAP	boot_ontap
The ONTAP primary image from the boot device	boot_primary
The ONTAP backup image from the boot device	boot_backup

If you are unsure about which image to use, you should use `boot_ontap` in the first instance.

### Shut down a node

You can shut down a node if it becomes unresponsive or if support personnel direct you to do so as part of troubleshooting efforts.

#### Steps

1. If the cluster contains four or more nodes, verify that the node to be shut down does not hold epsilon:

- a. Set the privilege level to advanced:

```
set -privilege advanced
```

- b. Determine which node holds epsilon:

```
cluster show
```

The following example shows that “node1” holds epsilon:

```
cluster1::*> cluster show
Node           Health  Eligibility  Epsilon
-----
node1          true    true         true
node2          true    true         false
node3          true    true         false
node4          true    true         false
4 entries were displayed.
```

- c. If the node to be shut down holds epsilon, then remove epsilon from the node:

```
cluster modify -node node_name -epsilon false
```

- d. Assign epsilon to a different node that will remain up:

```
cluster modify -node node_name -epsilon true
```

- e. Return to the admin privilege level:

```
set -privilege admin
```

2. Use the `system node halt` command to shut down the node.

If you do not specify the `-skip-lif-migration` parameter, the command attempts to migrate data and cluster management LIFs synchronously to another node prior to the shutdown. If the LIF migration fails or times out, the shutdown process is aborted, and ONTAP displays an error to indicate the LIF migration failure.

You can manually trigger a core dump with the shutdown by using both the `-dump` parameter.

The following example shuts down the node named “node1” for hardware maintenance:

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

## Manage a node by using the boot menu

You can use the boot menu to correct configuration problems on a node, reset the admin password, initialize disks, reset the node configuration, and restore the node configuration information back to the boot device.



If an HA pair is using [encrypting SAS or NVMe drives \(SED, NSE, FIPS\)](#), you must follow the instructions in the topic [Returning a FIPS drive or SED to unprotected mode](#) for all drives within the HA pair prior to initializing the system (boot options 4 or 9). Failure to do this may result in future data loss if the drives are repurposed.

### Steps

1. Reboot the node to access the boot menu by using the `system node reboot` command at the system prompt.

The node begins the reboot process.

2. During the reboot process, press Ctrl-C to display the boot menu when prompted to do so.

The node displays the following options for the boot menu:

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning
Selection (1-9)?
```



Boot menu option (2) Boot without /etc/rc is obsolete and takes no effect on the system.



3. Select one of the following options by entering the corresponding number:

To...	Select...
Continue to boot the node in normal mode	1) Normal Boot
Change the password of the node, which is also the "admin" account password	3) Change Password
Initialize the node's disks and create a root volume for the node	<p>4) Clean configuration and initialize all disks</p> <div>  <p>This menu option erases all data on the disks of the node and resets your node configuration to the factory default settings.</p> </div> <p>Only select this menu item after the node has been removed from a cluster (unjoined) and is not joined to another cluster.</p> <p>For a node with internal or external disk shelves, the root volume on the internal disks is initialized. If there are no internal disk shelves, then the root volume on the external disks is initialized.</p> <p>For a system running FlexArray Virtualization with internal or external disk shelves, the array LUNs are not initialized. Any native disks on either internal or external shelves are initialized.</p> <p>For a system running FlexArray Virtualization with only array LUNS and no internal or external disk shelves, the root volume on the storage array LUNS are initialized, see <a href="#">Installing FlexArray</a>.</p> <p>If the node you want to initialize has disks that are partitioned for root-data partitioning, the disks must be unpartitioned before the node can be initialized, see <b>9) Configure Advanced Drive Partitioning</b> and <a href="#">Disks and aggregates management</a>.</p>
Perform aggregate and disk maintenance operations and obtain detailed aggregate and disk information.	<p>5) Maintenance mode boot</p> <p>You exit Maintenance mode by using the <code>halt</code> command.</p>
Restore the configuration information from the node's root volume to the boot device, such as a PC CompactFlash card	<p>6) Update flash from backup config</p> <p>ONTAP stores some node configuration information on the boot device. When the node reboots, the information on the boot device is automatically backed up onto the node's root volume. If the boot device becomes corrupted or needs to be replaced, you must use this menu option to restore the configuration information from the node's root volume back to the boot device.</p>

To...	Select...
Install new software on the node	<p>7) Install new software first</p> <p>If the ONTAP software on the boot device does not include support for the storage array that you want to use for the root volume, you can use this menu option to obtain a version of the software that supports your storage array and install it on the node.</p> <p>This menu option is only for installing a newer version of ONTAP software on a node that has no root volume installed. Do <i>not</i> use this menu option to upgrade ONTAP.</p>
Reboot the node	8) Reboot node
Unpartition all disks and remove their ownership information or clean the configuration and initialize the system with whole or partitioned disks	<p>9) Configure Advanced Drive Partitioning</p> <p>Beginning with ONTAP 9.2, the Advanced Drive Partitioning option provides additional management features for disks that are configured for root-data or root-data-data partitioning. The following options are available from Boot Option 9:</p> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p>(9a) Unpartition all disks and remove their ownership information.</p> <p>(9b) Clean configuration and initialize system with partitioned disks.</p> <p>(9c) Clean configuration and initialize system with whole disks.</p> <p>(9d) Reboot the node.</p> <p>(9e) Return to main boot menu.</p> </div>

## Manage a node remotely using the SP/BMC

### Manage a node remotely using the SP/BMC overview

You can manage a node remotely using an onboard controller, called a Service Processor (SP) or Baseboard Management Controller (BMC). This remote management controller is included in all current platform models. The controller stays operational regardless of the operating state of the node.

The following platforms support BMC instead of SP:

- FAS 8700
- FAS 8300
- FAS27x0
- AFF A800

- AFF A700s
- AFF A400
- AFF A320
- AFF A220
- AFF C190

## About the SP

The Service Processor (SP) is a remote management device that enables you to access, monitor, and troubleshoot a node remotely.

The key capabilities of the SP include the following:

- The SP enables you to access a node remotely to diagnose, shut down, power-cycle, or reboot the node, regardless of the state of the node controller.

The SP is powered by a standby voltage, which is available as long as the node has input power from at least one of its power supplies.

You can log in to the SP by using a Secure Shell client application from an administration host. You can then use the SP CLI to monitor and troubleshoot the node remotely. In addition, you can use the SP to access the serial console and run ONTAP commands remotely.

You can access the SP from the serial console or access the serial console from the SP. The SP enables you to open both an SP CLI session and a separate console session simultaneously.

For instance, when a temperature sensor becomes critically high or low, ONTAP triggers the SP to shut down the motherboard gracefully. The serial console becomes unresponsive, but you can still press Ctrl-G on the console to access the SP CLI. You can then use the `system power on` or `system power cycle` command from the SP to power on or power-cycle the node.

- The SP monitors environmental sensors and logs events to help you take timely and effective service actions.

The SP monitors environmental sensors such as the node temperatures, voltages, currents, and fan speeds. When an environmental sensor has reached an abnormal condition, the SP logs the abnormal readings, notifies ONTAP of the issue, and sends alerts and “down system” notifications as necessary through an AutoSupport message, regardless of whether the node can send AutoSupport messages.

The SP also logs events such as boot progress, Field Replaceable Unit (FRU) changes, events generated by ONTAP, and SP command history. You can manually invoke an AutoSupport message to include the SP log files that are collected from a specified node.

Other than generating these messages on behalf of a node that is down and attaching additional diagnostic information to AutoSupport messages, the SP has no effect on the AutoSupport functionality. The AutoSupport configuration settings and message content behavior are inherited from ONTAP.



The SP does not rely on the `-transport` parameter setting of the `system node autosupport modify` command to send notifications. The SP only uses the Simple Mail Transport Protocol (SMTP) and requires its host's AutoSupport configuration to include mail host information.

If SNMP is enabled, the SP generates SNMP traps to configured trap hosts for all “down system” events.

- The SP has a nonvolatile memory buffer that stores up to 4,000 events in a system event log (SEL) to help you diagnose issues.

The SEL stores each audit log entry as an audit event. It is stored in onboard flash memory on the SP. The event list from the SEL is automatically sent by the SP to specified recipients through an AutoSupport message.

The SEL contains the following information:

- Hardware events detected by the SP—for example, sensor status about power supplies, voltage, or other components
  - Errors detected by the SP—for example, a communication error, a fan failure, or a memory or CPU error
  - Critical software events sent to the SP by the node—for example, a panic, a communication failure, a boot failure, or a user-triggered “down system” as a result of issuing the `SP system reset` or `system power cycle` command
- The SP monitors the serial console regardless of whether administrators are logged in or connected to the console.

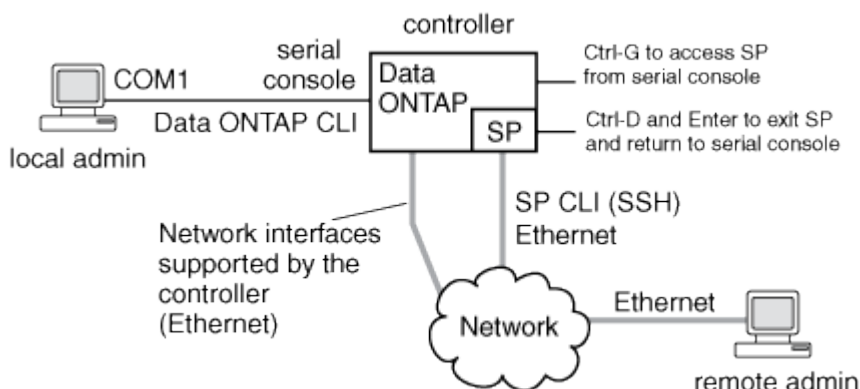
When messages are sent to the console, the SP stores them in the console log. The console log persists as long as the SP has power from either of the node power supplies. Because the SP operates with standby power, it remains available even when the node is power-cycled or turned off.

- Hardware-assisted takeover is available if the SP is configured.
- The SP API service enables ONTAP to communicate with the SP over the network.

The service enhances ONTAP management of the SP by supporting network-based functionality such as using the network interface for the SP firmware update, enabling a node to access another node’s SP functionality or system console, and uploading the SP log from another node.

You can modify the configuration of the SP API service by changing the port the service uses, renewing the SSL and SSH certificates that are used by the service for internal communication, or disabling the service entirely.

The following diagram illustrates access to ONTAP and the SP of a node. The SP interface is accessed through the Ethernet port (indicated by a wrench icon on the rear of the chassis):



## What the Baseboard Management Controller does

Beginning with ONTAP 9.1, on certain hardware platforms, software is customized to support a new onboard controller in called the Baseboard Management Controller (BMC). The BMC has command-line interface (CLI) commands you can use to manage the device remotely.

The BMC works similarly to the Service Processor (SP) and uses many of the same commands. The BMC allows you to do the following:

- Configure the BMC network settings.
- Access a node remotely and perform node management tasks such as diagnose, shut down, power-cycle, or reboot the node.

There are some differences between the SP and BMC:

- The BMC completely controls the environmental monitoring of power supply elements, cooling elements, temperature sensors, voltage sensors, and current sensors. The BMC reports sensor information to ONTAP through IPMI.
- Some of the high-availability (HA) and storage commands are different.
- The BMC does not send AutoSupport messages.

Automatic firmware updates are also available when running ONTAP 9.2 GA or later with the following requirements:

- BMC firmware revision 1.15 or later must be installed.



A manual update is required to upgrade BMC firmware from 1.12 to 1.15 or later.

- BMC automatically reboots after a firmware update is completed.



Node operations are not impacted during a BMC reboot.

## Configure the SP/BMC network

### Isolate management network traffic

It is a best practice to configure SP/BMC and the e0M management interface on a subnet dedicated to management traffic. Running data traffic over the management network can cause performance degradation and routing problems.

The management Ethernet port on most storage controllers (indicated by a wrench icon on the rear of the chassis) is connected to an internal Ethernet switch. The internal switch provides connectivity to SP/BMC and to the e0M management interface, which you can use to access the storage system via TCP/IP protocols like Telnet, SSH, and SNMP.



If you plan to use both the remote management device and e0M, you must configure them on the same IP subnet. Since these are low-bandwidth interfaces, the best practice is to configure SP/BMC and e0M on a subnet dedicated to management traffic.

If you cannot isolate management traffic, or if your dedicated management network is unusually large, you should try to keep the volume of network traffic as low as possible. Excessive ingress broadcast or multicast traffic may degrade SP/BMC performance.



Some storage controllers, such as the AFF A800, have two external ports, one for BMC and the other for e0M. For these controllers, there is no requirement to configure BMC and e0M on the same IP subnet.

### Considerations for the SP/BMC network configuration

You can enable cluster-level, automatic network configuration for the SP (recommended). You can also leave the SP automatic network configuration disabled (the default) and manage the SP network configuration manually at the node level. A few considerations exist for each case.



This topic applies to both the SP and the BMC.

The SP automatic network configuration enables the SP to use address resources (including the IP address, subnet mask, and gateway address) from the specified subnet to set up its network automatically. With the SP automatic network configuration, you do not need to manually assign IP addresses for the SP of each node. By default, the SP automatic network configuration is disabled; this is because enabling the configuration requires that the subnet to be used for the configuration be defined in the cluster first.

If you enable the SP automatic network configuration, the following scenarios and considerations apply:

- If the SP has never been configured, the SP network is configured automatically based on the subnet specified for the SP automatic network configuration.
- If the SP was previously configured manually, or if the existing SP network configuration is based on a different subnet, the SP network of all nodes in the cluster are reconfigured based on the subnet that you specify in the SP automatic network configuration.

The reconfiguration could result in the SP being assigned a different address, which might have an impact on your DNS configuration and its ability to resolve SP host names. As a result, you might need to update your DNS configuration.

- A node that joins the cluster uses the specified subnet to configure its SP network automatically.
- The `system service-processor network modify` command does not enable you to change the SP IP address.

When the SP automatic network configuration is enabled, the command only allows you to enable or disable the SP network interface.

- If the SP automatic network configuration was previously enabled, disabling the SP network interface results in the assigned address resource being released and returned to the subnet.
- If you disable the SP network interface and then reenabling it, the SP might be reconfigured with a different address.

If the SP automatic network configuration is disabled (the default), the following scenarios and considerations apply:

- If the SP has never been configured, SP IPv4 network configuration defaults to using IPv4 DHCP, and IPv6 is disabled.

A node that joins the cluster also uses IPv4 DHCP for its SP network configuration by default.

- The `system service-processor network modify` command enables you to configure a node's SP IP address.

A warning message appears when you attempt to manually configure the SP network with addresses that are allocated to a subnet. Ignoring the warning and proceeding with the manual address assignment might result in a scenario with duplicate addresses.

If the SP automatic network configuration is disabled after having been enabled previously, the following scenarios and considerations apply:

- If the SP automatic network configuration has the IPv4 address family disabled, the SP IPv4 network defaults to using DHCP, and the `system service-processor network modify` command enables you to modify the SP IPv4 configuration for individual nodes.
- If the SP automatic network configuration has the IPv6 address family disabled, the SP IPv6 network is also disabled, and the `system service-processor network modify` command enables you to enable and modify the SP IPv6 configuration for individual nodes.

### Enable the SP/BMC automatic network configuration

Enabling the SP to use automatic network configuration is preferred over manually configuring the SP network. Because the SP automatic network configuration is cluster wide, you do not need to manually manage the SP network for individual nodes.



This task applies to both the SP and the BMC.

- The subnet you want to use for the SP automatic network configuration must already be defined in the cluster and must have no resource conflicts with the SP network interface.

The `network subnet show` command displays subnet information for the cluster.

The parameter that forces subnet association (the `-force-update-lif-associations` parameter of the `network subnet` commands) is supported only on network LIFs and not on the SP network interface.

- If you want to use IPv6 connections for the SP, IPv6 must already be configured and enabled for ONTAP.

The `network options ipv6 show` command displays the current state of IPv6 settings for ONTAP.

## Steps

1. Specify the IPv4 or IPv6 address family and name for the subnet that you want the SP to use by using the `system service-processor network auto-configuration enable` command.
2. Display the SP automatic network configuration by using the `system service-processor network auto-configuration show` command.
3. If you subsequently want to disable or reenable the SP IPv4 or IPv6 network interface for all nodes that are in quorum, use the `system service-processor network modify` command with the `-address -family [IPv4|IPv6]` and `-enable [true|false]` parameters.

When the SP automatic network configuration is enabled, you cannot modify the SP IP address for a node that is in quorum. You can only enable or disable the SP IPv4 or IPv6 network interface.

If a node is out of quorum, you can modify the node's SP network configuration, including the SP IP address, by running `system service-processor network modify` from the node and confirming that you want to override the SP automatic network configuration for the node. However, when the node joins the quorum, the SP automatic reconfiguration takes place for the node based on the specified subnet.

## Configure the SP/BMC network manually

If you do not have automatic network configuration set up for the SP, you must manually configure a node's SP network for the SP to be accessible by using an IP address.

### What you'll need

If you want to use IPv6 connections for the SP, IPv6 must already be configured and enabled for ONTAP. The `network options ipv6` commands manage IPv6 settings for ONTAP.



This task applies to both the SP and the BMC.

You can configure the SP to use IPv4, IPv6, or both. The SP IPv4 configuration supports static and DHCP addressing, and the SP IPv6 configuration supports static addressing only.

If the SP automatic network configuration has been set up, you do not need to manually configure the SP network for individual nodes, and the `system service-processor network modify` command allows you to only enable or disable the SP network interface.

## Steps

1. Configure the SP network for a node by using the `system service-processor network modify` command.
  - The `-address-family` parameter specifies whether the IPv4 or IPv6 configuration of the SP is to be modified.



- The `-enable` parameter enables the network interface of the specified IP address family.
- The `-dhcp` parameter specifies whether to use the network configuration from the DHCP server or the network address that you provide.

You can enable DHCP (by setting `-dhcp` to `v4`) only if you are using IPv4. You cannot enable DHCP for IPv6 configurations.

- The `-ip-address` parameter specifies the public IP address for the SP.

A warning message appears when you attempt to manually configure the SP network with addresses that are allocated to a subnet. Ignoring the warning and proceeding with the manual address assignment might result in a duplicate address assignment.

- The `-netmask` parameter specifies the netmask for the SP (if using IPv4.)
- The `-prefix-length` parameter specifies the network prefix-length of the subnet mask for the SP (if using IPv6.)
- The `-gateway` parameter specifies the gateway IP address for the SP.

2. Configure the SP network for the remaining nodes in the cluster by repeating the step 1.
3. Display the SP network configuration and verify the SP setup status by using the `system service-processor network show` command with the `-instance` or `-field setup-status` parameters.

The SP setup status for a node can be one of the following:

- `not-setup` — Not configured
- `succeeded` — Configuration succeeded
- `in-progress` — Configuration in progress
- `failed` — Configuration failed

### Example of configuring the SP network

The following example configures the SP of a node to use IPv4, enables the SP, and displays the SP network configuration to verify the settings:

```

cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

Node: node1
Address Type: IPv4
Interface Enabled: true
Type of Device: SP
Status: online
Link Status: up
DHCP Status: none
IP Address: 192.168.123.98
MAC Address: ab:cd:ef:fe:ed:02
Netmask: 255.255.255.0
Prefix Length of Subnet Mask: -
Router Assigned IP Address: -
Link Local IP Address: -
Gateway IP Address: 192.168.123.1
Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
Subnet Name: -
Enable IPv6 Router Assigned Address: -
SP Network Setup Status: succeeded
SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>

```

## Modify the SP API service configuration

The SP API is a secure network API that enables ONTAP to communicate with the SP over the network. You can change the port used by the SP API service, renew the certificates the service uses for internal communication, or disable the service entirely. You need to modify the configuration only in rare situations.

### About this task

- The SP API service uses port 50000 by default.

You can change the port value if, for example, you are in a network setting where port 50000 is used for communication by another networking application, or you want to differentiate between traffic from other applications and traffic generated by the SP API service.

- The SSL and SSH certificates used by the SP API service are internal to the cluster and not distributed externally.

In the unlikely event that the certificates are compromised, you can renew them.

- The SP API service is enabled by default.

You only need to disable the SP API service in rare situations, such as in a private LAN where the SP is not configured or used and you want to disable the service.

If the SP API service is disabled, the API does not accept any incoming connections. In addition, functionality such as network-based SP firmware updates and network-based SP “down system” log collection becomes unavailable. The system switches to using the serial interface.

## Steps

1. Switch to the advanced privilege level by using the `set -privilege advanced` command.
2. Modify the SP API service configuration:

If you want to...	Use the following command...
Change the port used by the SP API service	<code>system service-processor api-service</code> modify with the <code>-port {49152..65535}</code> parameter
Renew the SSL and SSH certificates used by the SP API service for internal communication	<ul style="list-style-type: none"><li>• For ONTAP 9.5 or later use <code>system service-processor api-service renew-internal-certificate</code></li><li>• For ONTAP 9.4 and earlier use</li><li>• <code>system service-processor api-service renew-certificates</code></li></ul> <p>If no parameter is specified, only the host certificates (including the client and server certificates) are renewed.</p> <p>If the <code>-renew-all true</code> parameter is specified, both the host certificates and the root CA certificate are renewed.</p>
comm	
Disable or reenablen the SP API service	<code>system service-processor api-service</code> modify with the <code>-is-enabled {true false}</code> parameter

3. Display the SP API service configuration by using the `system service-processor api-service show` command.

## Methods of managing SP/BMC firmware updates

ONTAP includes an SP firmware image that is called the *baseline image*. If a new version of the SP firmware becomes subsequently available, you have the option to download it

and update the SP firmware to the downloaded version without upgrading the ONTAP version.



This topic applies to both the SP and the BMC.

ONTAP offers the following methods for managing SP firmware updates:

- The SP automatic update functionality is enabled by default, allowing the SP firmware to be automatically updated in the following scenarios:
  - When you upgrade to a new version of ONTAP

The ONTAP upgrade process automatically includes the SP firmware update, provided that the SP firmware version bundled with ONTAP is newer than the SP version running on the node.



ONTAP detects a failed SP automatic update and triggers a corrective action to retry the SP automatic update up to three times. If all three retries fail, you should contact technical support.

- When you download a version of the SP firmware from the NetApp Support Site and the downloaded version is newer than the one that the SP is currently running
- When you downgrade or revert to an earlier version of ONTAP

The SP firmware is automatically updated to the newest compatible version that is supported by the ONTAP version you reverted or downgraded to. A manual SP firmware update is not required.

You have the option to disable the SP automatic update functionality by using the `system service-processor image modify` command. However, it is recommended that you leave the functionality enabled. Disabling the functionality can result in suboptimal or nonqualified combinations between the ONTAP image and the SP firmware image.

- ONTAP enables you to trigger an SP update manually and specify how the update should take place by using the `system service-processor image update` command.

You can specify the following options:

- The SP firmware package to use (`-package`)

You can update the SP firmware to a downloaded package by specifying the package file name. The `advance system image package show` command displays all package files (including the files for the SP firmware package) that are available on a node.

- Whether to use the baseline SP firmware package for the SP update (`-baseline`)

You can update the SP firmware to the baseline version that is bundled with the currently running version of ONTAP.



If you use some of the more advanced update options or parameters, the BMC's configuration settings may be temporarily cleared. After reboot, it can take up to 10 minutes for ONTAP to restore the BMC configuration.

- ONTAP enables you to display the status for the latest SP firmware update triggered from ONTAP by using

the `system service-processor image update-progress show` command.

Any existing connection to the SP is terminated when the SP firmware is being updated. This is the case whether the SP firmware update is automatically or manually triggered.

#### Related information

[NetApp Downloads: System Firmware and Diagnostics](#)

#### When the SP/BMC uses the network interface for firmware updates

An SP firmware update that is triggered from ONTAP with the SP running version 1.5, 2.5, 3.1, or later supports using an IP-based file transfer mechanism over the SP network interface.



This topic applies to both the SP and the BMC.

An SP firmware update over the network interface is faster than an update over the serial interface. It reduces the maintenance window during which the SP firmware is being updated, and it is also nondisruptive to ONTAP operation. The SP versions that support this capability are included with ONTAP. They are also available on the NetApp Support Site and can be installed on controllers that are running a compatible version of ONTAP.

When you are running SP version 1.5, 2.5, 3.1, or later, the following firmware upgrade behaviors apply:

- An SP firmware update that is *automatically* triggered by ONTAP defaults to using the network interface for the update; however, the SP automatic update switches to using the serial interface for the firmware update if one of the following conditions occurs:
  - The SP network interface is not configured or not available.
  - The IP-based file transfer fails.
  - The SP API service is disabled.

Regardless of the SP version you are running, an SP firmware update triggered from the SP CLI always uses the SP network interface for the update.

#### Related information

[NetApp Downloads: System Firmware and Diagnostics](#)

#### Access the SP/BMC

##### Accounts that can access the SP

When you try to access the SP, you are prompted for credential. Cluster user accounts that are created with the `service-processor` application type have access to the SP CLI on any node of the cluster. SP user accounts are managed from ONTAP and authenticated by password.

User accounts for accessing the SP are managed from ONTAP instead of the SP CLI. A cluster user account of any role can access the SP if it is created with the `-application` parameter of the `security login create` command set to `service-processor` and the `-authmethod` parameter set to `password`. The SP supports only password authentication.

By default, the cluster user account named “admin” includes the `service-processor` application type and

has access to the SP.

ONTAP prevents you from creating user accounts with names that are reserved for the system (such as “root” and “naroot”). You cannot use a system-reserved name to access the cluster or the SP.

You can display current SP user accounts by using the `-application service-processor` parameter of the `security login show` command.

### Access the SP/BMC from an administration host

You can log in to the SP of a node from an administration host to perform node management tasks remotely.

#### What you'll need

The following conditions must be met:

- The administration host you use to access the SP must support SSHv2.
- Your user account must already be set up for accessing the SP.

To access the SP, your user account must have been created with the `-application` parameter of the `security login create` command set to `service-processor` and the `-authmethod` parameter set to `password`.



This task applies to both the SP and the BMC.

If the SP is configured to use an IPv4 or IPv6 address, and if five SSH login attempts from a host fail consecutively within 10 minutes, the SP rejects SSH login requests and suspends the communication with the IP address of the host for 15 minutes. The communication resumes after 15 minutes, and you can try to log in to the SP again.

ONTAP prevents you from creating or using system-reserved names (such as “root” and “naroot”) to access the cluster or the SP.

#### Steps

1. From the administration host, log in to the SP:

```
ssh username@SP_IP_address
```

2. When you are prompted, enter the password for `username`.

The SP prompt appears, indicating that you have access to the SP CLI.

#### Examples of SP access from an administration host

The following example shows how to log in to the SP with a user account `joe`, which has been set up to access the SP.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

The following examples show how to use the IPv6 global address or IPv6 router-advertised address to log in to the SP on a node that has SSH set up for IPv6 and the SP configured for IPv6.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

### Access the SP/BMC from the system console

You can access the SP from the system console (also called *serial console*) to perform monitoring or troubleshooting tasks.

#### About this task

This task applies to both the SP and the BMC.

#### Steps

1. Access the SP CLI from the system console by pressing Ctrl-G at the prompt.
2. Log in to the SP CLI when you are prompted.

The SP prompt appears, indicating that you have access to the SP CLI.

3. Exit the SP CLI and return to the system console by pressing Ctrl-D, and then press Enter.

#### Example of accessing the SP CLI from the system console

The following example shows the result of pressing Ctrl-G from the system console to access the SP CLI. The `help system power` command is entered at the SP prompt, followed by pressing Ctrl-D and then Enter to return to the system console.

```
cluster1::>
```

(Press Ctrl-G to access the SP CLI.)

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

(Press Ctrl-D and then Enter to return to the system console.)

```
cluster1::>
```

### Relationship among the SP CLI, SP console, and system console sessions

You can open an SP CLI session to manage a node remotely and open a separate SP console session to access the console of the node. The SP console session mirrors output displayed in a concurrent system console session. The SP and the system console have independent shell environments with independent login authentication.

Understanding how the SP CLI, SP console, and system console sessions are related helps you manage a node remotely. The following describes the relationship among the sessions:

- Only one administrator can log in to the SP CLI session at a time; however, the SP enables you to open both an SP CLI session and a separate SP console session simultaneously.

The SP CLI is indicated with the SP prompt (`SP>`). From an SP CLI session, you can use the SP `system console` command to initiate an SP console session. At the same time, you can start a separate SP CLI session through SSH. If you press Ctrl-D to exit from the SP console session, you automatically return to the SP CLI session. If an SP CLI session already exists, a message asks you whether to terminate the existing SP CLI session. If you enter “y”, the existing SP CLI session is terminated, enabling you to return from the SP console to the SP CLI. This action is recorded in the SP event log.

In an ONTAP CLI session that is connected through SSH, you can switch to the system console of a node by running the ONTAP `system node run-console` command from another node.

- For security reasons, the SP CLI session and the system console session have independent login authentication.

When you initiate an SP console session from the SP CLI (by using the SP `system console` command), you are prompted for the system console credential. When you access the SP CLI from a system console session (by pressing Ctrl-G), you are prompted for the SP CLI credential.

- The SP console session and the system console session have independent shell environments.

The SP console session mirrors output that is displayed in a concurrent system console session. However,



the concurrent system console session does not mirror the SP console session.

The SP console session does not mirror output of concurrent SSH sessions.

## Manage the IP addresses that can access the SP

By default, the SP accepts SSH connection requests from administration hosts of any IP addresses. You can configure the SP to accept SSH connection requests from only the administration hosts that have the IP addresses you specify. The changes you make apply to SSH access to the SP of any nodes in the cluster.

### Steps

1. Grant SP access to only the IP addresses you specify by using the `system service-processor ssh add-allowed-addresses` command with the `-allowed-addresses` parameter.

- The value of the `-allowed-addresses` parameter must be specified in the format of `address/netmask`, and multiple `address/netmask` pairs must be separated by commas, for example, `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.

Setting the `-allowed-addresses` parameter to `0.0.0.0/0, ::/0` enables all IP addresses to access the SP (the default).

- When you change the default by limiting SP access to only the IP addresses you specify, ONTAP prompts you to confirm that you want the specified IP addresses to replace the “allow all” default setting (`0.0.0.0/0, ::/0`).
  - The `system service-processor ssh show` command displays the IP addresses that can access the SP.
2. If you want to block a specified IP address from accessing the SP, use the `system service-processor ssh remove-allowed-addresses` command with the `-allowed-addresses` parameter.

If you block all IP addresses from accessing the SP, the SP becomes inaccessible from any administration hosts.

## Examples of managing the IP addresses that can access the SP

The following examples show the default setting for SSH access to the SP, change the default by limiting SP access to only the specified IP addresses, remove the specified IP addresses from the access list, and then restore SP access for all IP addresses:

```

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
      with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
      addresses will be denied access. To restore the "allow all"
default,
      use the "system service-processor ssh add-allowed-addresses
      -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
      {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

```

#### Use online help at the SP/BMC CLI

The online help displays the SP/BMC CLI commands and options.

#### About this task

This task applies to both the SP and the BMC.

#### Steps

1. To display help information for the SP/BMC commands, enter the following:

To access SP help...	To access BMC help...
Type <code>help</code> at the SP prompt.	Type <code>system</code> at the BMC prompt.

The following example shows the SP CLI online help.

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

The following example shows the BMC CLI online help.

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

2. To display help information for the option of an SP/BMC command, enter `help` before or after the SP/BMC command.

The following example shows the SP CLI online help for the SP `events` command.

```

SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events

```

The following example shows the BMC CLI online help for the BMC `system power` command.

```

BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>

```

#### Commands for managing a node remotely

You can manage a node remotely by accessing its SP and running SP CLI commands to perform node-management tasks. For several commonly performed remote node-management tasks, you can also use ONTAP commands from another node in the cluster. Some SP commands are platform-specific and might not be available on your platform.

If you want to...	Use this SP command...	Use this BMC command...	Or this ONTAP command ...
Display available SP commands or subcommands of a specified SP command	<code>help [command]</code>		
Display the current privilege level for the SP CLI	<code>priv show</code>		
Set the privilege level to access the specified mode for the SP CLI	<code>priv set {admin   advanced   diag}</code>		
Display system date and time	<code>date</code>		<code>date</code>

If you want to...	Use this SP command...	Use this BMC command...	Or this ONTAP command ...
Display events that are logged by the SP	<code>events {all   info   newest number   oldest number   search keyword}</code>		
Display SP status and network configuration information	<code>sp status [-v   -d]</code>  The <code>-v</code> option displays SP statistics in verbose form. The <code>-d</code> option adds the SP debug log to the display.	<code>bmc status [-v   -d]</code>  The <code>-v</code> option displays SP statistics in verbose form. The <code>-d</code> option adds the SP debug log to the display.	<code>system service-processor show</code>
Display the length of time the SP has been up and the average number of jobs in the run queue over the last 1, 5, and 15 minutes	<code>sp uptime</code>	<code>bmc uptime</code>	
Display system console logs	<code>system log</code>		
Display the SP log archives or the files in an archive	<code>sp log history show [-archive {latest   all   archive-name}] [-dump {all   file-name}]</code>	<code>bmc log history show [-archive {latest   all   archive-name}] [-dump {all   file-name}]</code>	
Display the power status for the controller of a node	<code>system power status</code>		<code>system node power show</code>
Display battery information	<code>system battery show</code>		
Display ACP information or the status for expander sensors	<code>system acp [show   sensors show]</code>		
List all system FRUs and their IDs	<code>system fru list</code>		
Display product information for the specified FRU	<code>system fru show fru_id</code>		

If you want to...	Use this SP command...	Use this BMC command...	Or this ONTAP command ...
Display the FRU data history log	<code>system fru log show</code> (advanced privilege level)		
Display the status for the environmental sensors, including their states and current values	<code>system sensors</code> or <code>system sensors show</code>		<code>system node environment sensors show</code>
Display the status and details for the specified sensor	<code>system sensors get sensor_name</code>  You can obtain <code>sensor_name</code> by using the <code>system sensors</code> or the <code>system sensors show</code> command.		
Display the SP firmware version information	<code>version</code>		<code>system service-processor image show</code>
Display the SP command history	<code>sp log audit</code> (advanced privilege level)	<code>bmc log audit</code>	
Display the SP debug information	<code>sp log debug</code> (advanced privilege level)	<code>bmc log debug</code> (advanced privilege level)	
Display the SP messages file	<code>sp log messages</code> (advanced privilege level)	<code>bmc log messages</code> (advanced privilege level)	
Display the settings for collecting system forensics on a watchdog reset event, display system forensics information collected during a watchdog reset event, or clear the collected system forensics information	<code>system forensics [show   log dump   log clear]</code>		
Log in to the system console	<code>system console</code>		<code>system node run-console</code>
	You should press Ctrl-D to exit the system console session.		

If you want to...	Use this SP command...	Use this BMC command...	Or this ONTAP command ...
Turn the node on or off, or perform a power-cycle (turning the power off and then back on)	<code>system power on</code>		<code>system node power on</code> (advanced privilege level)
	<code>system power off</code>		
	<code>system power cycle</code>		
	<p>The standby power stays on to keep the SP running without interruption. During the power-cycle, a brief pause occurs before power is turned back on.</p> <div>  <p>Using these commands to turn off or power-cycle the node might cause an improper shutdown of the node (also called a <i>dirty shutdown</i>) and is not a substitute for a graceful shutdown using the ONTAP <code>system node halt</code> command.</p> </div>		
Create a core dump and reset the node	<code>system core [-f]</code>  The <code>-f</code> option forces the creation of a core dump and the reset of the node.		<code>system node coredump trigger</code>  (advanced privilege level)
	<p>These commands have the same effect as pressing the Non-maskable Interrupt (NMI) button on a node, causing a dirty shutdown of the node and forcing a dump of the core files when halting the node. These commands are helpful when ONTAP on the node is hung or does not respond to commands such as <code>system node shutdown</code>. The generated core dump files are displayed in the output of the <code>system node coredump show</code> command. The SP stays operational as long as the input power to the node is not interrupted.</p>		
Reboot the node with an optionally specified BIOS firmware image (primary, backup, or current) to recover from issues such as a corrupted image of the node's boot device	<code>system reset {primary   backup   current}</code>		<code>system node reset with the -firmware {primary   backup   current} parameter</code> (advanced privilege level)  <code>system node reset</code>
	<div>  <p>This operation causes a dirty shutdown of the node.</p> </div> <p>If no BIOS firmware image is specified, the current image is used for the reboot. The SP stays operational as long as the input power to the node is not interrupted.</p>		

If you want to...	Use this SP command...	Use this BMC command...	Or this ONTAP command ...
Display the status of battery firmware automatic update, or enable or disable battery firmware automatic update upon next SP boot	<pre>system battery auto_update [status   enable   disable]</pre> <p>(advanced privilege level)</p>		
Compare the current battery firmware image against a specified firmware image	<pre>system battery verify [image_URL]</pre> <p>(advanced privilege level)</p> <p>If image_URL is not specified, the default battery firmware image is used for comparison.</p>		
Update the battery firmware from the image at the specified location	<pre>system battery flash image_URL</pre> <p>(advanced privilege level)</p> <p>You use this command if the automatic battery firmware upgrade process has failed for some reason.</p>		
Update the SP firmware by using the image at the specified location	<pre>sp update image_URL</pre> <p>image_URL must not exceed 200 characters.</p>	<pre>bmc update image_URL</pre> <p>image_URL must not exceed 200 characters.</p>	<pre>system service- processor image update</pre>
Reboot the SP	<pre>sp reboot</pre>		<pre>system service- processor reboot-sp</pre>
	<div>  <p>You should avoid booting the SP from the backup image. Booting from the backup image is reserved for troubleshooting and recovery purposes only. It might require that the SP automatic firmware update be disabled, which is not a recommended setting. You should contact technical support before attempting to boot the SP from the backup image.</p> </div>		



If you want to...	Use this SP command...	Use this BMC command...	Or this ONTAP command ...
Erase the NVRAM flash content	<pre>system nvram flash clear (advanced privilege level)</pre> <p>This command cannot be initiated when the controller power is off (system power off).</p>		
Exit the SP CLI	<code>exit</code>		

#### About the threshold-based SP sensor readings and status values of the system sensors command output

Threshold-based sensors take periodic readings of a variety of system components. The SP compares the reading of a threshold-based sensor against its preset threshold limits that define a component's acceptable operating conditions.

Based on the sensor reading, the SP displays the sensor state to help you monitor the condition of the component.

Examples of threshold-based sensors include sensors for the system temperatures, voltages, currents, and fan speeds. The specific list of threshold-based sensors depends on the platform.

Threshold-based sensors have the following thresholds, displayed in the output of the SP `system sensors` command:

- Lower critical (LCR)
- Lower noncritical (LNC)
- Upper noncritical (UNC)
- Upper critical (UCR)

A sensor reading between LNC and LCR or between UNC and UCR means that the component is showing signs of a problem and a system failure might occur as a result. Therefore, you should plan for component service soon.

A sensor reading below LCR or above UCR means that the component is malfunctioning and a system failure is about to occur. Therefore, the component requires immediate attention.

The following diagram illustrates the severity ranges that are specified by the thresholds:



You can find the reading of a threshold-based sensor under the `Current` column in the `system sensors`

command output. The `system sensors get sensor_name` command displays additional details for the specified sensor. As the reading of a threshold-based sensor crosses the noncritical and critical threshold ranges, the sensor reports a problem of increasing severity. When the reading exceeds a threshold limit, the sensor's status in the `system sensors` command output changes from `ok` to `nc` (noncritical) or `cr` (critical) depending on the exceeded threshold, and an event message is logged in the SEL event log.

Some threshold-based sensors do not have all four threshold levels. For those sensors, the missing thresholds show `na` as their limits in the `system sensors` command output, indicating that the particular sensor has no limit or severity concern for the given threshold and the SP does not monitor the sensor for that threshold.

### **Example of the system sensors command output**

The following example shows some of the information displayed by the `system sensors` command in the SP CLI:

```
SP node1> system sensors
```

Sensor Name	Current	Unit	Status	LCR	LNC
UNC	UCR				
-----+-----+-----+-----+-----+					
-----+-----+-----					
CPU0_Temp_Margin	-55.000	degrees C	ok	na	na
-5.000	0.000				
CPU1_Temp_Margin	-56.000	degrees C	ok	na	na
-5.000	0.000				
In_Flow_Temp	32.000	degrees C	ok	0.000	10.000
42.000	52.000				
Out_Flow_Temp	38.000	degrees C	ok	0.000	10.000
59.000	68.000				
CPU1_Error	0x0	discrete	0x0180	na	na
na	na				
CPU1_Therm_Trip	0x0	discrete	0x0180	na	na
na	na				
CPU1_Hot	0x0	discrete	0x0180	na	na
na	na				
IO_Mid1_Temp	30.000	degrees C	ok	0.000	10.000
55.000	64.000				
IO_Mid2_Temp	30.000	degrees C	ok	0.000	10.000
55.000	64.000				
CPU_VTT	1.106	Volts	ok	1.028	1.048
1.154	1.174				
CPU0_VCC	1.154	Volts	ok	0.834	0.844
1.348	1.368				
3.3V	3.323	Volts	ok	3.053	3.116
3.466	3.546				
5V	5.002	Volts	ok	4.368	4.465
5.490	5.636				
STBY_1.8V	1.794	Volts	ok	1.678	1.707
1.892	1.911				
...					

#### Example of the system sensors sensor\_name command output for a threshold-based sensor

The following example shows the result of entering `system sensors get sensor_name` in the SP CLI for the threshold-based sensor 5V:

```

SP node1> system sensors get 5V

Locating sensor record...
Sensor ID           : 5V (0x13)
Entity ID           : 7.97
Sensor Type (Analog) : Voltage
Sensor Reading       : 5.002 (+/- 0) Volts
Status               : ok
Lower Non-Recoverable : na
Lower Critical        : 4.246
Lower Non-Critical    : 4.490
Upper Non-Critical    : 5.490
Upper Critical        : 5.758
Upper Non-Recoverable : na
Assertion Events      :
Assertions Enabled    : lnc- lcr- ucr+
Deassertions Enabled : lnc- lcr- ucr+

```

#### About the discrete SP sensor status values of the system sensors command output

Discrete sensors do not have thresholds. Their readings, displayed under the `Current` column in the SP CLI `system sensors` command output, do not carry actual meanings and thus are ignored by the SP. The `Status` column in the `system sensors` command output displays the status values of discrete sensors in hexadecimal format.

Examples of discrete sensors include sensors for the fan, power supply unit (PSU) fault, and system fault. The specific list of discrete sensors depends on the platform.

You can use the SP CLI `system sensors get sensor_name` command for help with interpreting the status values for most discrete sensors. The following examples show the results of entering `system sensors get sensor_name` for the discrete sensors `CPU0_Error` and `IO_Slot1_Present`:

```

SP node1> system sensors get CPU0_Error
Locating sensor record...
Sensor ID           : CPU0_Error (0x67)
Entity ID           : 7.97
Sensor Type (Discrete): Temperature
States Asserted      : Digital State
                      [State Deasserted]

```

```

SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID           : IO_Slot1_Present (0x74)
Entity ID           : 11.97
Sensor Type (Discrete): Add-in Card
States Asserted      : Availability State
                      [Device Present]

```

Although the `system sensors get sensor_name` command displays the status information for most discrete sensors, it does not provide status information for the `System_FW_Status`, `System_Watchdog`, `PSU1_Input_Type`, and `PSU2_Input_Type` discrete sensors. You can use the following information to interpret these sensors' status values.

### System\_FW\_Status

The `System_FW_Status` sensor's condition appears in the form of `0xAABB`. You can combine the information of `AA` and `BB` to determine the condition of the sensor.

`AA` can have one of the following values:

Values	Condition of the sensor
01	System firmware error
02	System firmware hang
04	System firmware progress

`BB` can have one of the following values:

Values	Condition of the sensor
00	System software has properly shut down
01	Memory initialization in progress
02	NVMEM initialization in progress (when NVMEM is present)
04	Restoring memory controller hub (MCH) values (when NVMEM is present)
05	User has entered Setup
13	Booting the operating system or LOADER

Values	Condition of the sensor
1F	BIOS is starting up
20	LOADER is running
21	LOADER is programming the primary BIOS firmware. You must not power down the system.
22	LOADER is programming the alternate BIOS firmware. You must not power down the system.
2F	ONTAP is running
60	SP has powered off the system
61	SP has powered on the system
62	SP has reset the system
63	SP watchdog power cycle
64	SP watchdog cold reset

For instance, the System\_FW\_Status sensor status 0x042F means "system firmware progress (04), ONTAP is running (2F)."

### System\_Watchdog

The System\_Watchdog sensor can have one of the following conditions:

- **0x0080**

The state of this sensor has not changed

Values	Condition of the sensor
0x0081	Timer interrupt
0x0180	Timer expired
0x0280	Hard reset
0x0480	Power down
0x0880	Power cycle

For instance, the System\_Watchdog sensor status 0x0880 means a watchdog timeout occurs and causes a system power cycle.

### PSU1\_Input\_Type and PSU2\_Input\_Type

For direct current (DC) power supplies, the PSU1\_Input\_Type and PSU2\_Input\_Type sensors do not apply. For alternating current (AC) power supplies, the sensors' status can have one of the following values:

Values	Condition of the sensor
0x01 xx	220V PSU type
0x02 xx	110V PSU type

For instance, the PSU1\_Input\_Type sensor status 0x0280 means that the sensor reports that the PSU type is 110V.

### Commands for managing the SP from ONTAP

ONTAP provides commands for managing the SP, including the SP network configuration, SP firmware image, SSH access to the SP, and general SP administration.

### Commands for managing the SP network configuration

If you want to...	Run this ONTAP command...
Enable the SP automatic network configuration for the SP to use the IPv4 or IPv6 address family of the specified subnet	<code>system service-processor network auto-configuration enable</code>
Disable the SP automatic network configuration for the IPv4 or IPv6 address family of the subnet specified for the SP	<code>system service-processor network auto-configuration disable</code>
Display the SP automatic network configuration	<code>system service-processor network auto-configuration show</code>

If you want to...	Run this ONTAP command...
<p>Manually configure the SP network for a node, including the following:</p> <ul style="list-style-type: none"> <li>• The IP address family (IPv4 or IPv6)</li> <li>• Whether the network interface of the specified IP address family should be enabled</li> <li>• If you are using IPv4, whether to use the network configuration from the DHCP server or the network address that you specify</li> <li>• The public IP address for the SP</li> <li>• The netmask for the SP (if using IPv4)</li> <li>• The network prefix-length of the subnet mask for the SP (if using IPv6)</li> <li>• The gateway IP address for the SP</li> </ul>	<pre>system service-processor network modify</pre>
<p>Display the SP network configuration, including the following:</p> <ul style="list-style-type: none"> <li>• The configured address family (IPv4 or IPv6) and whether it is enabled</li> <li>• The remote management device type</li> <li>• The current SP status and link status</li> <li>• Network configuration, such as IP address, MAC address, netmask, prefix-length of subnet mask, router-assigned IP address, link local IP address, and gateway IP address</li> <li>• The time the SP was last updated</li> <li>• The name of the subnet used for SP automatic configuration</li> <li>• Whether the IPv6 router-assigned IP address is enabled</li> <li>• SP network setup status</li> <li>• Reason for the SP network setup failure</li> </ul>	<pre>system service-processor network show</pre> <p>Displaying complete SP network details requires the <code>-instance</code> parameter.</p>
<p>Modify the SP API service configuration, including the following:</p> <ul style="list-style-type: none"> <li>• Changing the port used by the SP API service</li> <li>• Enabling or disabling the SP API service</li> </ul>	<pre>system service-processor api-service modify</pre> <p>(advanced privilege level)</p>



If you want to...	Run this ONTAP command...
Display the SP API service configuration	<pre>system service-processor api-service show</pre> <p>(advanced privilege level)</p>
Renew the SSL and SSH certificates used by the SP API service for internal communication	<ul style="list-style-type: none"> <li>• For ONTAP 9.5 or later: <pre>system service-processor api-service renew-internal-certificates</pre></li> <li>• For ONTAP 9.4 or earlier: <pre>system service-processor api-service renew-certificates</pre></li> </ul> <p>(advanced privilege level)</p>

### Commands for managing the SP firmware image

If you want to...	Run this ONTAP command...
Display the details of the currently installed SP firmware image, including the following: <ul style="list-style-type: none"> <li>• The remote management device type</li> <li>• The image (primary or backup) that the SP is booted from, its status, and firmware version</li> <li>• Whether the firmware automatic update is enabled and the last update status</li> </ul>	<pre>system service-processor image show</pre> <p>The <code>-is-current</code> parameter indicates the image (primary or backup) that the SP is currently booted from, not if the installed firmware version is most current.</p>
Enable or disable the SP automatic firmware update	<pre>system service-processor image modify</pre> <p>By default, the SP firmware is automatically updated with the update of ONTAP or when a new version of the SP firmware is manually downloaded. Disabling the automatic update is not recommended because doing so can result in suboptimal or nonqualified combinations between the ONTAP image and the SP firmware image.</p>

If you want to...	Run this ONTAP command...
Manually download an SP firmware image on a node	<pre>system node image get</pre> <div>  <p>Before you run the <code>system node image</code> commands, you must set the privilege level to advanced (<code>set -privilege advanced</code>), entering <b>y</b> when prompted to continue.</p> </div> <p>The SP firmware image is packaged with ONTAP. You do not need to download the SP firmware manually, unless you want to use an SP firmware version that is different from the one packaged with ONTAP.</p>
Display the status for the latest SP firmware update triggered from ONTAP, including the following information: <ul style="list-style-type: none"> <li>• The start and end time for the latest SP firmware update</li> <li>• Whether an update is in progress and the percentage that is complete</li> </ul>	<pre>system service-processor image update-progress show</pre>

### Commands for managing SSH access to the SP

If you want to...	Run this ONTAP command...
Grant SP access to only the specified IP addresses	<pre>system service-processor ssh add-allowed-addresses</pre>
Block the specified IP addresses from accessing the SP	<pre>system service-processor ssh remove-allowed-addresses</pre>
Display the IP addresses that can access the SP	<pre>system service-processor ssh show</pre>

### Commands for general SP administration

If you want to...	Run this ONTAP command...
<p>Display general SP information, including the following:</p> <ul style="list-style-type: none"> <li>• The remote management device type</li> <li>• The current SP status</li> <li>• Whether the SP network is configured</li> <li>• Network information, such as the public IP address and the MAC address</li> <li>• The SP firmware version and Intelligent Platform Management Interface (IPMI) version</li> <li>• Whether the SP firmware automatic update is enabled</li> </ul>	<pre>system service-processor show</pre> <p>Displaying complete SP information requires the <code>-instance</code> parameter.</p>
<p>Reboot the SP on a node and optionally specify the SP firmware image (primary or backup) to use</p>	<pre>system service-processor reboot-sp</pre> <div>  <p>You should avoid booting the SP from the backup image. Booting from the backup image is reserved for troubleshooting and recovery purposes only. It might require that the SP automatic firmware update be disabled, which is not a recommended setting. You should contact Technical Support before attempting to boot the SP from the backup image.</p> </div>
<p>Generate and send an AutoSupport message that includes the SP log files collected from a specified node</p>	<pre>system node autosupport invoke-spllog</pre>
<p>Display the allocation map of the collected SP log files in the cluster, including the sequence numbers for the SP log files that reside in each collecting node</p>	<pre>system service-processor log show-allocations</pre>

## Related information

[ONTAP 9 commands](#)

## ONTAP commands for BMC management

These ONTAP commands are supported on the Baseboard Management Controller (BMC).

The BMC uses some of the same commands as the Service Processor (SP). The following SP commands are supported on the BMC.

If you want to...	Use this command
Display the BMC information	<code>system service-processor show</code>
Display/modify the BMC network configuration	<code>system service-processor network show/modify</code>
Reset the BMC	<code>system service-processor reboot-sp</code>
Display/modify the details of the currently installed BMC firmware image	<code>system service-processor image show/modify</code>
Update BMC firmware	<code>system service-processor image update</code>
Display the status for the latest BMC firmware update	<code>system service-processor image update-progress show</code>
Enable the automatic network configuration for the BMC to use an IPv4 or IPv6 address on the specified subnet	<code>system service-processor network auto-configuration enable</code>
Disable the automatic network configuration for an IPv4 or IPv6 address on the subnet specified for the BMC	<code>system service-processor network auto-configuration disable</code>
Display the BMC automatic network configuration	<code>system service-processor network auto-configuration show</code>

For commands that are not supported by the BMC firmware, the following error message is returned.

```
::> Error: Command not supported on this platform.
```

#### BMC CLI commands

You can log into the BMC using SSH. The following commands are supported from the BMC command line.

Command	Function
<code>system</code>	Display a list of all commands.
<code>system console</code>	Connect to the system's console. Use <code>Ctrl+D</code> to exit the session.
<code>system core</code>	Dump the system core and reset.

Command	Function
system power cycle	Power the system off, then on.
system power off	Power the system off.
system power on	Power the system on.
system power status	Print system power status.
system reset	Reset the system.
system log	Print system console logs
system fru show [id]	Dump all/selected field replaceable unit (FRU) info.

## Manage audit logging for management activities

### Changes to audit logging in ONTAP 9

Beginning with ONTAP 9, the `command-history.log` file is replaced by `audit.log`, and the `mgwd.log` file no longer contains audit information. If you are upgrading to ONTAP 9, you should review any scripts or tools that refer to the legacy files and their contents.

After upgrade to ONTAP 9, existing `command-history.log` files are preserved. They are rotated out (deleted) as new `audit.log` files are rotated in (created).

Tools and scripts that check the `command-history.log` file might continue to work, because a soft link from `command-history.log` to `audit.log` is created at upgrade. However, tools and scripts that check the `mgwd.log` file will fail, because that file no longer contains audit information.

In addition, audit logs in ONTAP 9 and later no longer include the following entries because they are not considered useful and cause unnecessary logging activity:

- Internal commands run by ONTAP (that is, where `username=root`)
- Command aliases (separately from the command they point to)

Beginning with ONTAP 9, you can transmit the audit logs securely to external destinations using the TCP and TLS protocols.

### How ONTAP implements audit logging

Management activities recorded in the audit log are included in standard AutoSupport reports, and certain logging activities are included in EMS messages. You can also forward the audit log to destinations that you specify, and you can display audit log files by using the CLI or a web browser.

ONTAP logs management activities that are performed on the cluster, for example, what request was issued, the user who triggered the request, the user's access method, and the time of the request.

The management activities can be one of the following types:

- Set requests, which typically apply to non-display commands or operations
  - These requests are issued when you run a `create`, `modify`, or `delete` command, for instance.
  - Set requests are logged by default.
- Get requests, which retrieve information and display it in the management interface
  - These requests are issued when you run a `show` command, for instance.
  - Get requests are not logged by default, but you can use the `security audit modify` command to control whether get requests sent from the ONTAP CLI (`-cli`) or from the ONTAP APIs (`-ontapi`) are logged in the file.

ONTAP records management activities in the `/mroot/etc/log/mlog/audit.log` file of a node. Commands from the three shells for CLI commands—the `clustershell`, the `nodeshell`, and the non-interactive `systemshell` (interactive `systemshell` commands are not logged)—as well as API commands are logged here. Audit logs include timestamps to show whether all nodes in a cluster are time synchronized.

The `audit.log` file is sent by the AutoSupport tool to the specified recipients. You can also forward the content securely to external destinations that you specify; for example, a Splunk or a syslog server.

The `audit.log` file is rotated daily. The rotation also occurs when it reaches 100 MB in size, and the previous 48 copies are preserved (with a maximum total of 49 files). When the audit file performs its daily rotation, no EMS message is generated. If the audit file rotates because its file size limit is exceeded, an EMS message is generated.

You can use the `security audit log show` command to display audit entries for individual nodes or merged from multiple nodes in the cluster. You can also display the content of the `/mroot/etc/log/mlog` directory on a single node by using a web browser.

## Forward the audit log to a destination

You can forward the audit log to a maximum of 10 destinations that you specify by using the `cluster log-forwarding create` command. For example, you can forward the log to a Splunk or syslog server for monitoring, analysis, or backup purposes.

### About this task

If the `cluster log-forwarding create` command cannot ping the destination host to verify connectivity, the command fails with an error. Although not recommended, using the `-force` parameter with the command bypasses the connectivity verification.

You can configure transmission security options when forwarding log files:

- Protocols for sending messages to the destination

You can select one of the following `-protocol` values:

- `udp-unencrypted`: User Datagram Protocol with no security (default)
- `tcp-unencrypted`: Transmission Control Protocol with no security

- tcp-encrypted: Transmission Control Protocol with Transport Layer Security (TLS)

- Verification of destination server identity

When you set the `-verify-server` parameter to `true`, the identity of the log forwarding destination is verified by validating its certificate. You can set the value to `true` only when you select the `tcp-encrypted` value in the `-protocol` field.

## Steps

1. For each destination that you want to forward the audit log to, specify the destination IP address or host name and any security options.

```
cluster1::> cluster log-forwarding create -destination 192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination 192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

2. Verify that the destination records are correct by using the `cluster log-forwarding show` command.

```
cluster1::> cluster log-forwarding show
```

Destination Host	Port	Protocol	Verify Server	Syslog Facility
192.168.123.96	514	udp-unencrypted	false	user
192.168.123.98	514	tcp-encrypted	true	user

2 entries were displayed.

## Related information

[ONTAP 9 commands](#)

## Commands for managing audit settings for management activities

You use the `security audit` commands to manage which management activities are logged in the `audit.log` file. You use the `cluster log-forwarding` commands to manage destinations for forwarding the audit log to.

If you want to...	Use this command...
Specify that get requests from the ONTAP CLI or APIs should be recorded in the audit log (the <code>audit.log</code> file), in addition to default set requests	<code>security audit modify</code>
Display the settings of the audit log	<code>security audit show</code>

If you want to...	Use this command...
Display audit entries merged from multiple nodes in the cluster	<code>security audit log show</code>
Specify a forwarding destination for the audit log and security measures for its transmission	<code>cluster log-forwarding create</code>
Modify a destination for the audit log	<code>cluster log-forwarding modify</code>
Delete a destination for the audit log	<code>cluster log-forwarding delete</code>
Show the configured destinations for the audit log	<code>cluster log-forwarding show</code>

### Related information

[ONTAP 9 commands](#)

## Manage the cluster time (cluster administrators only)

Problems can occur when the cluster time is inaccurate. Although ONTAP enables you to manually set the time zone, date, and time on the cluster, you should configure the Network Time Protocol (NTP) servers to synchronize the cluster time.

Beginning with ONTAP 9.5, you can configure your NTP server with symmetric authentication.

NTP is always enabled. However, configuration is still required for the cluster to synchronize with an external time source. ONTAP enables you to manage the cluster's NTP configuration in the following ways:

- You can associate a maximum of 10 external NTP servers with the cluster (`cluster time-service ntp server create`).
  - For redundancy and quality of time service, you should associate at least three external NTP servers with the cluster.
  - You can specify an NTP server by using its IPv4 or IPv6 address or fully qualified host name.
  - You can manually specify the NTP version (v3 or v4) to use.

By default, ONTAP automatically selects the NTP version that is supported for a given external NTP server.

If the NTP version you specify is not supported for the NTP server, time exchange cannot take place.

- At the advanced privilege level, you can specify an external NTP server that is associated with the cluster to be the primary time source for correcting and adjusting the cluster time.
- You can display the NTP servers that are associated with the cluster (`cluster time-service ntp server show`).
- You can modify the cluster's NTP configuration (`cluster time-service ntp server modify`).
- You can disassociate the cluster from an external NTP server (`cluster time-service ntp server delete`).



- At the advanced privilege level, you can reset the configuration by clearing all external NTP servers' association with the cluster (`cluster time-service ntp server reset`).

A node that joins a cluster automatically adopts the NTP configuration of the cluster.

In addition to using NTP, ONTAP also enables you to manually manage the cluster time. This capability is helpful when you need to correct erroneous time (for example, a node's time has become significantly incorrect after a reboot). In that case, you can specify an approximate time for the cluster until NTP can synchronize with an external time server. The time you manually set takes effect across all nodes in the cluster.

You can manually manage the cluster time in the following ways:

- You can set or modify the time zone, date, and time on the cluster (`cluster date modify`).
- You can display the current time zone, date, and time settings of the cluster (`cluster date show`).



Job schedules do not adjust to manual cluster date and time changes. These jobs are scheduled to run based on the current cluster time when the job was created or when the job most recently ran. Therefore, if you manually change the cluster date or time, you must use the `job show` and `job history show` commands to verify that all scheduled jobs are queued and completed according to your requirements.



## Commands for managing the cluster time

You use the `cluster time-service ntp server` commands to manage the NTP servers for the cluster. You use the `cluster date` commands to manage the cluster time manually.

Beginning with ONTAP 9.5, you can configure your NTP server with symmetric authentication.

The following commands enable you to manage the NTP servers for the cluster:

If you want to...	Use this command...
Associate the cluster with an external NTP server without symmetric authentication	<code>cluster time-service ntp server create -server server_name</code>
Associate the cluster with an external NTP server with symmetric authentication Available in ONTAP 9.5 or later	<code>cluster time-service ntp server create -server server_ip_address -key-id key_id</code> <div>  The <code>key_id</code> must refer to an existing shared key configured with 'cluster time-service ntp key'. </div>
Enable symmetric authentication for an existing NTP server An existing NTP server can be modified to enable authentication by adding the required key-id.  Available in ONTAP 9.5 or later	<code>cluster time-service ntp server modify -server server_name -key-id key_id</code>

If you want to...	Use this command...
Disable symmetric authentication	<code>cluster time-service ntp server modify -server server_name -authentication disabled</code>
Configure a shared NTP key	<pre>cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value</pre> <div>  <p>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</p> </div>
Display information about the NTP servers that are associated with the cluster	<code>cluster time-service ntp server show</code>
Modify the configuration of an external NTP server that is associated with the cluster	<code>cluster time-service ntp server modify</code>
Dissociate an NTP server from the cluster	<code>cluster time-service ntp server delete</code>
Reset the configuration by clearing all external NTP servers' association with the cluster	<pre>cluster time-service ntp server reset</pre> <div>  <p>This command requires the advanced privilege level.</p> </div>

The following commands enable you to manage the cluster time manually:

If you want to...	Use this command...
Set or modify the time zone, date, and time	<code>cluster date modify</code>
Display the time zone, date, and time settings for the cluster	<code>cluster date show</code>

#### Related information

[ONTAP 9 commands](#)

## Manage the banner and MOTD

### Manage the banner and MOTD overview

ONTAP enables you to configure a login banner or a message of the day (MOTD) to communicate administrative information to CLI users of the cluster or storage virtual machine (SVM).

A banner is displayed in a console session (for cluster access only) or an SSH session (for cluster or SVM access) before a user is prompted for authentication such as a password. For example, you can use the banner to display a warning message such as the following to someone who attempts to log in to the system:

```
$ ssh admin@cluster1-01
```

```
This system is for authorized users only. Your IP Address has been logged.
```

```
Password:
```

An MOTD is displayed in a console session (for cluster access only) or an SSH session (for cluster or SVM access) after a user is authenticated but before the clustershell prompt appears. For example, you can use the MOTD to display a welcome or informational message such as the following that only authenticated users will see:

```
$ ssh admin@cluster1-01
```

```
Password:
```

```
Greetings. This system is running ONTAP 9.0.
```

```
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015  
from 10.72.137.28.
```

You can create or modify the content of the banner or MOTD by using the `security login banner modify` or `security login motd modify` command, respectively, in the following ways:

- You can use the CLI interactively or noninteractively to specify the text to use for the banner or MOTD.

The interactive mode, launched when the command is used without the `-message` or `-uri` parameter, enables you to use newlines (also known as end of lines) in the message.

The noninteractive mode, which uses the `-message` parameter to specify the message string, does not support newlines.

- You can upload content from an FTP or HTTP location to use for the banner or MOTD.
- You can configure the MOTD to display dynamic content.

Examples of what you can configure the MOTD to display dynamically include the following:

- Cluster name, node name, or SVM name
- Cluster date and time
- Name of the user logging in
- Last login for the user on any node in the cluster
- Login device name or IP address
- Operating system name
- Software release version

- Effective cluster version string

The `security login motd modify` man page describes the escape sequences that you can use to enable the MOTD to display dynamically generated content.

The banner does not support dynamic content.

You can manage the banner and MOTD at the cluster or SVM level:

- The following facts apply to the banner:
  - The banner configured for the cluster is also used for all SVMs that do not have a banner message defined.
  - An SVM-level banner can be configured for each SVM.

If a cluster-level banner has been configured, it is overridden by the SVM-level banner for the given SVM.

- The following facts apply to the MOTD:
  - By default, the MOTD configured for the cluster is also enabled for all SVMs.
  - Additionally, an SVM-level MOTD can be configured for each SVM.

In this case, users logging in to the SVM will see two MOTDs, one defined at the cluster level and the other at the SVM level.

- The cluster-level MOTD can be enabled or disabled on a per-SVM basis by the cluster administrator.

If the cluster administrator disables the cluster-level MOTD for an SVM, a user logging in to the SVM does not see the cluster-level MOTD.

## Create a banner

You can create a banner to display a message to someone who attempts to access the cluster or SVM. The banner is displayed in a console session (for cluster access only) or an SSH session (for cluster or SVM access) before a user is prompted for authentication.

### Steps

1. Use the `security login banner modify` command to create a banner for the cluster or SVM:

If you want to...	Then...
Specify a message that is a single line	Use the <code>-message "text"</code> parameter to specify the text.
Include newlines (also known as end of lines) in the message	Use the command without the <code>-message</code> or <code>-uri</code> parameter to launch the interactive mode for editing the banner.
Upload content from a location to use for the banner	Use the <code>-uri</code> parameter to specify the content's FTP or HTTP location.

The maximum size for a banner is 2,048 bytes, including newlines.

A banner created by using the `-uri` parameter is static. It is not automatically refreshed to reflect subsequent changes of the source content.

The banner created for the cluster is displayed also for all SVMs that do not have an existing banner. Any subsequently created banner for an SVM overrides the cluster-level banner for that SVM. Specifying the `-message` parameter with a hyphen within double quotes ("`-`") for the SVM resets the SVM to use the cluster-level banner.

2. Verify that the banner has been created by displaying it with the `security login banner show` command.

Specifying the `-message` parameter with an empty string ("`''`") displays banners that have no content.

Specifying the `-message` parameter with "`-`" displays all (admin or data) SVMs that do not have a banner configured.

### Examples of creating banners

The following example uses the noninteractive mode to create a banner for the "cluster1" cluster:

```
cluster1::> security login banner modify -message "Authorized users only!"  
  
cluster1::>
```

The following example uses the interactive mode to create a banner for the "svm1" SVM:

```
cluster1::> security login banner modify -vserver svm1  
  
Enter the message of the day for Vserver "svm1".  
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to  
abort.  
0          1          2          3          4          5          6          7  
8  
12345678901234567890123456789012345678901234567890123456789012345678901234  
567890  
The svm1 SVM is reserved for authorized users only!  
  
cluster1::>
```

The following example displays the banners that have been created:

```

cluster1::> security login banner show
Vserver: cluster1
Message
-----
---
Authorized users only!

Vserver: svm1
Message
-----
---
The svm1 SVM is reserved for authorized users only!

2 entries were displayed.

cluster1::>

```

## Related information

[Managing the banner](#)

## Managing the banner

You can manage the banner at the cluster or SVM level. The banner configured for the cluster is also used for all SVMs that do not have a banner message defined. A subsequently created banner for an SVM overrides the cluster banner for that SVM.

### Choices

- Manage the banner at the cluster level:

If you want to...	Then...
Create a banner to display for all CLI login sessions	Set a cluster-level banner: <pre> security login banner modify -vserver cluster_name { [-message "text"]   [ -uri ftp_or_http_addr] } </pre>
Remove the banner for all (cluster and SVM) logins	Set the banner to an empty string (""): <pre> security login banner modify -vserver * -message "" </pre>

If you want to...	Then...
Override a banner created by an SVM administrator	Modify the SVM banner message:  <pre>security login banner modify -vserver svm_name { [-message "text"]   [-uri ftp_or_http_addr] }</pre>

- Manage the banner at the SVM level:

Specifying `-vserver svm_name` is not required in the SVM context.

If you want to...	Then...
Override the banner supplied by the cluster administrator with a different banner for the SVM	Create a banner for the SVM:  <pre>security login banner modify -vserver svm_name { [-message "text"]   [-uri ftp_or_http_addr] }</pre>
Suppress the banner supplied by the cluster administrator so that no banner is displayed for the SVM	Set the SVM banner to an empty string for the SVM:  <pre>security login banner modify -vserver svm_name -message ""</pre>
Use the cluster-level banner when the SVM currently uses an SVM-level banner	Set the SVM banner to "-":  <pre>security login banner modify -vserver svm_name -message "-"</pre>

## Create an MOTD

You can create a message of the day (MOTD) to communicate information to authenticated CLI users. The MOTD is displayed in a console session (for cluster access only) or an SSH session (for cluster or SVM access) after a user is authenticated but before the clustershell prompt appears.

### Steps

1. Use the `security login motd modify` command to create an MOTD for the cluster or SVM:

If you want to...	Then...
Specify a message that is a single line	Use the <code>-message "text"</code> parameter to specify the text.
Include newlines (also known as end of lines)	Use the command without the <code>-message</code> or <code>-uri</code> parameter to launch the interactive mode for editing the MOTD.

If you want to...	Then...
Upload content from a location to use for the MOTD	Use the <code>-uri</code> parameter to specify the content's FTP or HTTP location.

The maximum size for an MOTD is 2,048 bytes, including newlines.

The `security login motd modify` man page describes the escape sequences that you can use to enable the MOTD to display dynamically generated content.

An MOTD created by using the `-uri` parameter is static. It is not automatically refreshed to reflect subsequent changes of the source content.

An MOTD created for the cluster is displayed also for all SVM logins by default, along with an SVM-level MOTD that you can create separately for a given SVM. Setting the `-is-cluster-message-enabled` parameter to `false` for an SVM prevents the cluster-level MOTD from being displayed for that SVM.

2. Verify that the MOTD has been created by displaying it with the `security login motd show` command.

Specifying the `-message` parameter with an empty string (`""`) displays MOTDs that are not configured or have no content.

See the [security login motd modify](#) command man page for a list of parameters to use to enable the MOTD to display dynamically generated content. Be sure to check the man page specific to your ONTAP version.

## Examples of creating MOTDs

The following example uses the noninteractive mode to create an MOTD for the "cluster1" cluster:

```
cluster1::> security login motd modify -message "Greetings!"
```

The following example uses the interactive mode to create an MOTD for the "svm1" SVM that uses escape sequences to display dynamically generated content:

```
cluster1::> security login motd modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0          1          2          3          4          5          6          7
8
1234567890123456789012345678901234567890123456789012345678901234
567890
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.
```

The following example displays the MOTDs that have been created:



```

cluster1::> security login motd show
Vserver: cluster1
Is the Cluster MOTD Displayed?: true
Message
-----
---
Greetings!

Vserver: svm1
Is the Cluster MOTD Displayed?: true
Message
-----
---
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.

2 entries were displayed.

```


## Manage the MOTD

You can manage the message of the day (MOTD) at the cluster or SVM level. By default, the MOTD configured for the cluster is also enabled for all SVMs. Additionally, an SVM-level MOTD can be configured for each SVM. The cluster-level MOTD can be enabled or disabled for each SVM by the cluster administrator.

### Choices

- Manage the MOTD at the cluster level:

If you want to...	Then...
Create an MOTD for all logins when there is no existing MOTD	Set a cluster-level MOTD:  <pre>security login motd modify -vserver cluster_name { [-message "text"]   [- uri ftp_or_http_addr] }</pre>
Change the MOTD for all logins when no SVM-level MOTDs are configured	Modify the cluster-level MOTD:  <pre>security login motd modify -vserver cluster_name { [-message "text"] }   [-uri ftp_or_http_addr] }</pre>
Remove the MOTD for all logins when no SVM-level MOTDs are configured	Set the cluster-level MOTD to an empty string (""): <pre>security login motd modify -vserver cluster_name -message ""</pre>

If you want to...	Then...
Have every SVM display the cluster-level MOTD instead of using the SVM-level MOTD	<p>Set a cluster-level MOTD, then set all SVM-level MOTDs to an empty string with the cluster-level MOTD enabled:</p> <ol style="list-style-type: none"> <li>1. <code>security login motd modify -vserver <i>cluster_name</i> { [-message "text"]   [-uri <i>ftp_or_http_addr</i>] }</code></li> <li>2. <code>security login motd modify { -vserver !"cluster_name" } -message "" -is-cluster-message-enabled true</code></li> </ol>
Have an MOTD displayed for only selected SVMs, and use no cluster-level MOTD	<p>Set the cluster-level MOTD to an empty string, then set SVM-level MOTDs for selected SVMs:</p> <ol style="list-style-type: none"> <li>1. <code>security login motd modify -vserver <i>cluster_name</i> -message ""</code></li> <li>2. <code>security login motd modify -vserver <i>svm_name</i> { [-message "text"]   [-uri <i>ftp_or_http_addr</i>] }</code></li> </ol> <p>You can repeat this step for each SVM as needed.</p>
Use the same SVM-level MOTD for all (data and admin) SVMs	<p>Set the cluster and all SVMs to use the same MOTD:</p> <pre>security login motd modify -vserver * { [-message "text"]   [-uri <i>ftp_or_http_addr</i>] }</pre> <div data-bbox="873 1371 927 1423">  </div> <p>If you use the interactive mode, the CLI prompts you to enter the MOTD individually for the cluster and each SVM. You can paste the same MOTD into each instance when you are prompted to.</p>
Have a cluster-level MOTD optionally available to all SVMs, but do not want the MOTD displayed for cluster logins	<p>Set a cluster-level MOTD, but disable its display for the cluster:</p> <pre>security login motd modify -vserver <i>cluster_name</i> { [-message "text"]   [-uri <i>ftp_or_http_addr</i>] } -is-cluster -message-enabled false</pre>

If you want to...	Then...
Remove all MOTDs at the cluster and SVM levels when only some SVMs have both cluster-level and SVM-level MOTDs	Set the cluster and all SVMs to use an empty string for the MOTD:  <b>security login motd modify -vserver * -message ""</b>
Modify the MOTD only for the SVMs that have a non-empty string, when other SVMs use an empty string, and when a different MOTD is used at the cluster level	Use extended queries to modify the MOTD selectively:  <b>security login motd modify { -vserver !"cluster_name" -message !"" } { [-message "text"]   [-uri ftp_or_http_addr] }</b>
Display all MOTDs that contain specific text (for example, "January" followed by "2015") anywhere in a single or multiline message, even if the text is split across different lines	Use a query to display MOTDs:  <b>security login motd show -message *"January"*"2015"*</b>
Interactively create an MOTD that includes multiple and consecutive newlines (also known as end of lines, or EOLs)	In the interactive mode, press the space bar followed by Enter to create a blank line without terminating the input for the MOTD.

- Manage the MOTD at the SVM level:

Specifying `-vserver svm_name` is not required in the SVM context.

If you want to...	Then...
Use a different SVM-level MOTD, when the SVM already has an existing SVM-level MOTD	Modify the SVM-level MOTD:  <b>security login motd modify -vserver svm_name { [-message "text"]   [-uri ftp_or_http_addr] }</b>
Use only the cluster-level MOTD for the SVM, when the SVM already has an SVM-level MOTD	Set the SVM-level MOTD to an empty string, then have the cluster administrator enable the cluster-level MOTD for the SVM:  <ol style="list-style-type: none"> <li>1. <b>security login motd modify -vserver svm_name -message ""</b></li> <li>2. (For the cluster administrator) <b>security login motd modify -vserver svm_name -is-cluster-message-enabled true</b></li> </ol>

If you want to...	Then...
Not have the SVM display any MOTD, when both the cluster-level and SVM-level MOTDs are currently displayed for the SVM	<p>Set the SVM-level MOTD to an empty string, then have the cluster administrator disable the cluster-level MOTD for the SVM:</p> <ol style="list-style-type: none"> <li>1. <code>security login motd modify -vserver <i>svm_name</i> -message ""</code></li> <li>2. (For the cluster administrator) <code>security login motd modify -vserver <i>svm_name</i> -is-cluster-message-enabled false</code></li> </ol>

## Manage licenses (cluster administrators only)

### Manage licenses overview (cluster administrators only)

A license is a record of one or more software entitlements. In ONTAP 8.2 through ONTAP 9.9.1, license keys are delivered as 28-character strings, and there is one key per ONTAP feature. A new license key format called a NetApp License File (NLF) was introduced in ONTAP 9.2 for cluster-wide features only, such as FabricPool.

Beginning with ONTAP 9.10.1, all license are delivered as NLFs. NLF licenses can enable one or more ONTAP features, depending on your purchase. You can retrieve NLF licenses from the NetApp Support Site by searching for the system (controller) serial number.

You can find licenses for your initial or add-on software orders at the NetApp Support Site under **My Support > Software Licenses** (login required). If you cannot locate your license keys from the Software Licenses page, contact your sales or support representative.

ONTAP enables you to manage feature licenses in the following ways:

- Display information about installed licenses (`system license show`)
- Display the packages that require licenses and their current license status on the cluster (`system license status show`)
- Delete a license from the cluster or a node whose serial number you specify (`system license delete`)
- Display or remove expired or unused licenses (`system license clean-up`)

ONTAP enables you to monitor feature usage and license entitlement risk in the following ways:

- Display a summary of feature usage in the cluster on a per-node basis (`system feature-usage show-summary`)

The summary includes counter information such as the number of weeks a feature was in use and the last date and time the feature was used.

- Display feature usage status in the cluster on a per-node and per-week basis (`system feature-usage show-history`)

The feature usage status can be `not-used`, `configured`, or `in-use`. If the usage information is not

available, the status shows `not-available`.

- Display the status of license entitlement risk for each license package (`system license entitlement-risk show`)

The risk status can be `low`, `medium`, `high`, `unlicensed`, or `unknown`. The risk status is also included in the AutoSupport message. License entitlement risk does not apply to the base license package.

The license entitlement risk is evaluated by using a number of factors, which might include but are not limited to the following:

- Each package's licensing state
- The type of each license, its expiry status, and the uniformity of the licenses across the cluster
- Usage for the features associated with the license package

If the evaluation process determines that the cluster has a license entitlement risk, the command output also suggests a corrective action.



Note: ONTAP 9.10.1 also supports 28-character license keys using System Manager or the CLI. However, if an NLF license is installed for a feature, you cannot install a 28-character license key over the NLF license for the same feature. For information about installing NLFs or license keys using System Manager, see “Enable new features.”

## Related information

[What are Data ONTAP 8.2 and 8.3 licensing overview and references?](#)

[How to verify Data ONTAP Software Entitlements and related License Keys using the Support Site](#)

[FAQ: Licensing updates in Data ONTAP 9.2](#)

[NetApp: Data ONTAP Entitlement Risk Status](#)

## License types and licensed method

Understanding license types and the licensed method helps you manage the licenses in a cluster.

### License types

A package can have one or more of the following license types installed in the cluster. The `system license show` command displays the installed license type or types for a package.

- Standard license (`license`)

A standard license is a node-locked license. It is issued for a node with a specific system serial number (also known as a *controller serial number*). A standard license is valid only for the node that has the matching serial number.

Installing a standard, node-locked license entitles a node to the licensed functionality. For the cluster to use licensed functionality, at least one node must be licensed for the functionality. It might be out of compliance to use licensed functionality on a node that does not have an entitlement for the functionality.

- Site license (`site`)

A site license is not tied to a specific system serial number. When you install a site license, all nodes in the cluster are entitled to the licensed functionality. The `system license show` command displays site licenses under the cluster serial number.

If your cluster has a site license and you remove a node from the cluster, the node does not carry the site license with it, and it is no longer entitled to the licensed functionality. If you add a node to a cluster that has a site license, the node is automatically entitled to the functionality granted by the site license.

- Evaluation license (demo)

An evaluation license is a temporary license that expires after a certain period of time (indicated by the `system license show` command). It enables you to try certain software functionality without purchasing an entitlement. It is a cluster-wide license, and it is not tied to a specific serial number of a node.

If your cluster has an evaluation license for a package and you remove a node from the cluster, the node does not carry the evaluation license with it.

### Licensed method

It is possible to install both a cluster-wide license (the `site` or `demo` type) and a node-locked license (the `license` type) for a package. Therefore, an installed package can have multiple license types in the cluster. However, to the cluster, there is only one *licensed method* for a package. The `licensed method` field of the `system license status show` command displays the entitlement that is being used for a package. The command determines the licensed method as follows:

- If a package has only one license type installed in the cluster, the installed license type is the licensed method.
- If a package does not have any licenses installed in the cluster, the licensed method is `none`.
- If a package has multiple license types installed in the cluster, the licensed method is determined in the following priority order of the license type--`site`, `license`, and `demo`.



For example:

- If you have a site license, a standard license, and an evaluation license for a package, the licensed method for the package in the cluster is `site`.
- If you have a standard license and an evaluation license for a package, the licensed method for the package in the cluster is `license`.
- If you have only an evaluation license for a package, the licensed method for the package in the cluster is `demo`.

### Commands for managing licenses

You use the `system license` commands to manage feature licenses for the cluster. You use the `system feature-usage` commands to monitor feature usage.

If you want to...	Use this command...
Add one or more licenses	<code>system license add</code>

If you want to...	Use this command...
<p>Display information about installed licenses, for example:</p> <ul style="list-style-type: none"> <li>• License package name and description</li> <li>• License type (site, license, or demo)</li> <li>• Expiration date, if applicable</li> <li>• The cluster or nodes that a package is licensed for</li> <li>• Whether the license was installed prior to Data ONTAP 8.2 (legacy)</li> <li>• Customer ID</li> </ul>	<pre>system license show</pre> <div>  <p>Some information is displayed only when you use the <code>-instance</code> parameter.</p> </div>
<p>Display all packages that require licenses and their current license status, including the following:</p> <ul style="list-style-type: none"> <li>• The package name</li> <li>• The licensed method</li> <li>• The expiration date, if applicable</li> </ul>	<pre>system license status show</pre>
<p>Delete the license of a package from the cluster or a node whose serial number you specify</p>	<pre>system license delete</pre>
<p>Display or remove expired or unused licenses</p>	<pre>system license clean-up</pre>
<p>Display summary of feature usage in the cluster on a per-node basis</p>	<pre>system feature-usage show-summary</pre>
<p>Display feature usage status in the cluster on a per-node and per-week basis</p>	<pre>system feature-usage show-history</pre>
<p>Display the status of license entitlement risk for each license package</p>	<pre>system license entitlement-risk show</pre> <div>  <p>Some information is displayed only when you use the <code>-detail</code> and <code>-instance</code> parameters.</p> </div>

## Related information

[ONTAP 9 commands](#)

## Manage jobs and schedules

### Job categories

There are three categories of jobs that you can manage: server-affiliated, cluster-

affiliated, and private.

A job can be in any of the following categories:

- **Server-Affiliated jobs**

These jobs are queued by the management framework to a specific node to be run.

- **Cluster-Affiliated jobs**

These jobs are queued by the management framework to any node in the cluster to be run.

- **Private jobs**

These jobs are specific to a node and do not use the replicated database (RDB) or any other cluster mechanism. The commands that manage private jobs require the advanced privilege level or higher.

### Commands for managing jobs

Jobs are placed into a job queue and run in the background when resources are available. If a job is consuming too many cluster resources, you can stop it or pause it until there is less demand on the cluster. You can also monitor and restart jobs.

When you enter a command that invokes a job, typically, the command informs you that the job has been queued and then returns to the CLI command prompt. However, some commands instead report job progress and do not return to the CLI command prompt until the job has been completed. In these cases, you can press Ctrl-C to move the job to the background.

If you want to...	Use this command...
Display information about all jobs	<code>job show</code>
Display information about jobs on a per-node basis	<code>job show bynode</code>
Display information about cluster-affiliated jobs	<code>job show-cluster</code>
Display information about completed jobs	<code>job show-completed</code>
Display information about job history	<code>job history show</code>  Up to 25,000 job records are stored for each node in the cluster. Consequently, attempting to display the full job history could take a long time. To avoid potentially long wait times, you should display jobs by node, storage virtual machine (SVM), or record ID.
Display the list of private jobs	<code>job private show</code> (advanced privilege level)



If you want to...	Use this command...
Display information about completed private jobs	<code>job private show-completed</code> (advanced privilege level)
Display information about the initialization state for job managers	<code>job initstate show</code> (advanced privilege level)
Monitor the progress of a job	<code>job watch-progress</code>
Monitor the progress of a private job	<code>job private watch-progress</code> (advanced privilege level)
Pause a job	<code>job pause</code>
Pause a private job	<code>job private pause</code> (advanced privilege level)
Resume a paused job	<code>job resume</code>
Resume a paused private job	<code>job private resume</code> (advanced privilege level)
Stop a job	<code>job stop</code>
Stop a private job	<code>job private stop</code> (advanced privilege level)
Delete a job	<code>job delete</code>
Delete a private job	<code>job private delete</code> (advanced privilege level)
Disassociate a cluster-affiliated job with an unavailable node that owns it, so that another node can take ownership of that job	<code>job unclaim</code> (advanced privilege level)



You can use the `event log show` command to determine the outcome of a completed job.

## Related information

[ONTAP 9 commands](#)

## Commands for managing job schedules

Many tasks—for instance, volume Snapshot copies—can be configured to run on specified schedules. Schedules that run at specific times are called *cron* schedules (similar to UNIX `cron` schedules). Schedules that run at intervals are called *interval* schedules. You use the `job schedule` commands to manage job schedules.

Job schedules do not adjust to manual changes to the cluster date and time. These jobs are scheduled to run based on the current cluster time when the job was created or when the job most recently ran. Therefore, if you manually change the cluster date or time, you should use the `job show` and `job history show` commands to verify that all scheduled jobs are queued and completed according to your requirements.

If the cluster is part of a MetroCluster configuration, then the job schedules on both clusters must be identical. Therefore, if you create, modify, or delete a job schedule, you must perform the same operation on the remote cluster.

If you want to...	Use this command...
Display information about all schedules	<code>job schedule show</code>
Display the list of jobs by schedule	<code>job schedule show-jobs</code>
Display information about cron schedules	<code>job schedule cron show</code>
Display information about interval schedules	<code>job schedule interval show</code>
Create a cron schedule <sup>1</sup>	<code>job schedule cron create</code>
Create an interval schedule	<code>job schedule interval create</code>  You must specify at least one of the following parameters: <code>-days</code> , <code>-hours</code> , <code>-minutes</code> , or <code>-seconds</code> .
Modify a cron schedule	<code>job schedule cron modify</code>
Modify an interval schedule	<code>job schedule interval modify</code>
Delete a schedule	<code>job schedule delete</code>
Delete a cron schedule	<code>job schedule cron delete</code>
Delete an interval schedule	<code>job schedule interval delete</code>

<sup>1</sup>Beginning with ONTAP 9.10.1, when you create a job schedule by using the `job schedule cron create` command, you can include the Vserver for your job schedule.

#### Related information

[ONTAP 9 commands](#)

## Back up and restore cluster configurations (cluster administrators only)

## What configuration backup files are

Configuration backup files are archive files (.7z) that contain information for all configurable options that are necessary for the cluster, and the nodes within it, to operate properly.

These files store the local configuration of each node, plus the cluster-wide replicated configuration. You use configuration backup files to back up and restore the configuration of your cluster.

There are two types of configuration backup files:

- **Node configuration backup file**

Each healthy node in the cluster includes a node configuration backup file, which contains all of the configuration information and metadata necessary for the node to operate healthy in the cluster.

- **Cluster configuration backup file**

These files include an archive of all of the node configuration backup files in the cluster, plus the replicated cluster configuration information (the replicated database, or RDB file). Cluster configuration backup files enable you to restore the configuration of the entire cluster, or of any node in the cluster. The cluster configuration backup schedules create these files automatically and store them on several nodes in the cluster.



Configuration backup files contain configuration information only. They do not include any user data. For information about restoring user data, see [Data Protection](#).

## Manage configuration backups

### How the node and cluster configurations are backed up automatically

Three separate schedules automatically create cluster and node configuration backup files and replicate them among the nodes in the cluster.

The configuration backup files are automatically created according to the following schedules:

- Every 8 hours
- Daily
- Weekly



At each of these times, a node configuration backup file is created on each healthy node in the cluster. All of these node configuration backup files are then collected in a single cluster configuration backup file along with the replicated cluster configuration and saved on one or more nodes in the cluster.

For single-node clusters (including Data ONTAP Edge systems), you can specify the configuration backup destination during software setup. After setup, those settings can be modified using ONTAP commands.

### Commands for managing configuration backup schedules

You can use the `system configuration backup settings` commands to manage configuration backup schedules.

These commands are available at the advanced privilege level.

If you want to...	Use this command...
<p>Change the settings for a configuration backup schedule:</p> <ul style="list-style-type: none"><li>• Specify a remote URL (HTTP, HTTPS, FTP, FTPS, or TFTP ) where the configuration backup files will be uploaded in addition to the default locations in the cluster</li><li>• Specify a user name to be used to log in to the remote URL</li><li>• Set the number of backups to keep for each configuration backup schedule</li></ul>	<p><code>system configuration backup settings modify</code></p> <p>When you use HTTPS in the remote URL, use the <code>-validate-certification</code> option to enable or disable digital certificate validation. Certificate validation is disabled by default.</p> <div><p>The web server to which you are uploading the configuration backup file must have PUT operations enabled for HTTP and POST operations enabled for HTTPS. For more information, see your web server's documentation.</p></div>
<p>Set the password to be used to log in to the remote URL</p>	<p><code>system configuration backup settings set-password</code></p>
<p>View the settings for the configuration backup schedule</p>	<p><code>system configuration backup settings show</code></p> <div><p>You set the <code>-instance</code> parameter to view the user name and the number of backups to keep for each schedule.</p></div>

#### Commands for managing configuration backup files

You use the `system configuration backup` commands to manage cluster and node configuration backup files.

These commands are available at the advanced privilege level.

If you want to...	Use this command...
<p>Create a new node or cluster configuration backup file</p>	<p><code>system configuration backup create</code></p>
<p>Copy a configuration backup file from a node to another node in the cluster</p>	<p><code>system configuration backup copy</code></p>

If you want to...	Use this command...
<p>Upload a configuration backup file from a node in the cluster to a remote URL (FTP, HTTP, HTTPS, TFTP, or FTPS)</p>	<p><code>system configuration backup upload</code></p> <p>When you use HTTPS in the remote URL, use the <code>-validate-certification</code> option to enable or disable digital certificate validation. Certificate validation is disabled by default.</p> <div data-bbox="850 569 902 625">  </div> <p>The web server to which you are uploading the configuration backup file must have PUT operations enabled for HTTP and POST operations enabled for HTTPS. Some web servers might require the installation of an additional module. For more information, see your web server's documentation. Supported URL formats vary by ONTAP release. See the command line help for your ONTAP version.</p>
<p>Download a configuration backup file from a remote URL to a node in the cluster, and, if specified, validate the digital certificate</p>	<p><code>system configuration backup download</code></p> <p>When you use HTTPS in the remote URL, use the <code>-validate-certification</code> option to enable or disable digital certificate validation. Certificate validation is disabled by default.</p>
<p>Rename a configuration backup file on a node in the cluster</p>	<p><code>system configuration backup rename</code></p>
<p>View the node and cluster configuration backup files for one or more nodes in the cluster</p>	<p><code>system configuration backup show</code></p>
<p>Delete a configuration backup file on a node</p>	<p><code>system configuration backup delete</code></p> <div data-bbox="850 1493 902 1549">  </div> <p>This command deletes the configuration backup file on the specified node only. If the configuration backup file also exists on other nodes in the cluster, it remains on those nodes.</p>

## Recovering a node configuration

### Find a configuration backup file to use for recovering a node

You use a configuration backup file located at a remote URL or on a node in the cluster to recover a node configuration.

### About this task

You can use either a cluster or node configuration backup file to restore a node configuration.

### Step

1. Make the configuration backup file available to the node for which you need to restore the configuration.

If the configuration backup file is located...	Then...
At a remote URL	Use the <code>system configuration backup download</code> command at the advanced privilege level to download it to the recovering node.
On a node in the cluster	<ol style="list-style-type: none"><li>a. Use the <code>system configuration backup show</code> command at the advanced privilege level to view the list of configuration backup files available in the cluster that contains the recovering node's configuration.</li><li>b. If the configuration backup file you identify does not exist on the recovering node, then use the <code>system configuration backup copy</code> command to copy it to the recovering node.</li></ol>

If you previously re-created the cluster, you should choose a configuration backup file that was created after the cluster recreation. If you must use a configuration backup file that was created prior to the cluster recreation, then after recovering the node, you must re-create the cluster again.

### Restore the node configuration using a configuration backup file

You restore the node configuration using the configuration backup file that you identified and made available to the recovering node.

### About this task

You should only perform this task to recover from a disaster that resulted in the loss of the node's local configuration files.

### Steps

1. If the node is healthy, then at the advanced privilege level of a different node, use the `cluster modify` command with the `-node` and `-eligibility` parameters to mark it ineligible and isolate it from the cluster.

If the node is not healthy, then you should skip this step.

This example modifies node2 to be ineligible to participate in the cluster so that its configuration can be restored:

```
cluster1::*> cluster modify -node node2 -eligibility false
```

2. Use the `system configuration recovery node restore` command at the advanced privilege level to restore the node's configuration from a configuration backup file.

If the node lost its identity, including its name, then you should use the `-nodename-in-backup` parameter to specify the node name in the configuration backup file.

This example restores the node's configuration using one of the configuration backup files stored on the node:

```
cluster1::*> system configuration recovery node restore -backup
cluster1.8hour.2011-02-22.18_15_00.7z
```

```
Warning: This command overwrites local configuration files with
files contained in the specified backup file. Use this
command only to recover from a disaster that resulted
in the loss of the local configuration files.
The node will reboot after restoring the local configuration.
Do you want to continue? {y|n}: y
```

The configuration is restored, and the node reboots.

3. If you marked the node ineligible, then use the `system configuration recovery cluster sync` command to mark the node as eligible and synchronize it with the cluster.
4. If you are operating in a SAN environment, use the `system node reboot` command to reboot the node and reestablish SAN quorum.

### After you finish

If you previously re-created the cluster, and if you are restoring the node configuration by using a configuration backup file that was created prior to that cluster re-creation, then you must re-create the cluster again.

## Recover a cluster configuration

### Find a configuration to use for recovering a cluster

You use the configuration from either a node in the cluster or a cluster configuration backup file to recover a cluster.

### Steps

1. Choose a type of configuration to recover the cluster.

- A node in the cluster

If the cluster consists of more than one node, and one of the nodes has a cluster configuration from when the cluster was in the desired configuration, then you can recover the cluster using the configuration stored on that node.

In most cases, the node containing the replication ring with the most recent transaction ID is the best node to use for restoring the cluster configuration. The `cluster ring show` command at the advanced privilege level enables you to view a list of the replicated rings available on each node in the cluster.

- A cluster configuration backup file

If you cannot identify a node with the correct cluster configuration, or if the cluster consists of a single

node, then you can use a cluster configuration backup file to recover the cluster.

Recovering a cluster from a configuration backup file might require the use of diagnostic tools to resolve discrepancies between the backup and the cluster configuration present on the recovering node. Therefore, if you use a configuration backup file, you should plan to contact technical support.

2. If you chose to use a cluster configuration backup file, then make the file available to the node you plan to use to recover the cluster.

If the configuration backup file is located...	Then...
At a remote URL	Use the <code>system configuration backup download</code> command at the advanced privilege level to download it to the recovering node.
On a node in the cluster	<ol style="list-style-type: none"><li>a. Use the <code>system configuration backup show</code> command at the advanced privilege level to find a cluster configuration backup file that was created when the cluster was in the desired configuration.</li><li>b. If the cluster configuration backup file is not located on the node you plan to use to recover the cluster, then use the <code>system configuration backup copy</code> command to copy it to the recovering node.</li></ol>

### Restore a cluster configuration from an existing configuration

To restore a cluster configuration from an existing configuration after a cluster failure, you re-create the cluster using the cluster configuration that you chose and made available to the recovering node, and then rejoin each additional node to the new cluster.

#### About this task

You should only perform this task to recover from a disaster that resulted in the loss of the cluster's configuration.



If you are re-creating the cluster from a configuration backup file, you must contact technical support to resolve any discrepancies between the configuration backup file and the configuration present in the cluster.

#### Steps

1. Disable storage failover for each HA pair:

```
storage failover modify -node node_name -enabled false
```

You only need to disable storage failover once for each HA pair. When you disable storage failover for a node, storage failover is also disabled on the node's partner.

2. Halt each node except for the recovering node:

```
system node halt -node node_name -reason "text"
```



```
cluster1::*> system node halt -node node0 -reason "recovering cluster"

Warning: Are you sure you want to halt the node? {y|n}: y
```

3. Set the privilege level to advanced:

```
set -privilege advanced
```

4. On the recovering node, use the **system configuration recovery cluster recreate** command to re-create the cluster.

This example re-creates the cluster using the configuration information stored on the recovering node:

```
cluster1::*> configuration recovery cluster recreate -from node

Warning: This command will destroy your existing cluster. It will
        rebuild a new single-node cluster consisting of this node
        and its current configuration. This feature should only be
        used to recover from a disaster. Do not perform any other
        recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

A new cluster is created on the recovering node.

5. If you are re-creating the cluster from a configuration backup file, verify that the cluster recovery is still in progress:

```
system configuration recovery cluster show
```

You do not need to verify the cluster recovery state if you are re-creating the cluster from a healthy node.

```
cluster1::*> system configuration recovery cluster show
Recovery Status: in-progress
Is Recovery Status Persisted: false
```

6. Boot each node that needs to be rejoined to the re-created cluster.

You must reboot the nodes one at a time.

7. For each node that needs to be joined to the re-created cluster, do the following:

- a. From a healthy node on the re-created cluster, rejoin the target node:

```
system configuration recovery cluster rejoin -node node_name
```

This example rejoins the “node2” target node to the re-created cluster:

```
cluster1::*> system configuration recovery cluster rejoin -node node2

Warning: This command will rejoin node "node2" into the local
cluster, potentially overwriting critical cluster
configuration files. This command should only be used
to recover from a disaster. Do not perform any other
recovery operations while this operation is in progress.
This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

The target node reboots and then joins the cluster.

- b. Verify that the target node is healthy and has formed quorum with the rest of the nodes in the cluster:

```
cluster show -eligibility true
```

The target node must rejoin the re-created cluster before you can rejoin another node.

```
cluster1::*> cluster show -eligibility true
Node           Health  Eligibility  Epsilon
-----
node0           true    true         false
node1           true    true         false
2 entries were displayed.
```

8. If you re-created the cluster from a configuration backup file, set the recovery status to be complete:

```
system configuration recovery cluster modify -recovery-status complete
```

9. Return to the admin privilege level:

```
set -privilege admin
```

10. If the cluster consists of only two nodes, use the **cluster ha modify** command to reenoble cluster HA.

11. Use the **storage failover modify** command to reenoble storage failover for each HA pair.

### After you finish

If the cluster has SnapMirror peer relationships, then you also need to re-create those relationships. For more information, see [Data Protection](#).

### Synchronize a node with the cluster

If cluster-wide quorum exists, but one or more nodes are out of sync with the cluster, then you must synchronize the node to restore the replicated database (RDB) on the node and bring it into quorum.

### Step

1. From a healthy node, use the `system configuration recovery cluster sync` command at the advanced privilege level to synchronize the node that is out of sync with the cluster configuration.

This example synchronizes a node (*node2*) with the rest of the cluster:

```
cluster1::*> system configuration recovery cluster sync -node node2
```

Warning: This command will synchronize node "node2" with the cluster configuration, potentially overwriting critical cluster configuration files on the node. This feature should only be used to recover from a disaster. Do not perform any other recovery operations while this operation is in progress. This command will cause all the cluster applications on node "node2" to restart, interrupting administrative CLI and Web interface on that node.

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

All cluster applications on node "node2" will be restarted. Verify that the cluster applications go online.

## Result

The RDB is replicated to the node, and the node becomes eligible to participate in the cluster.

## Manage core dumps (cluster administrators only)

When a node panics, a core dump occurs and the system creates a core dump file that technical support can use to troubleshoot the problem. You can configure or display core dump attributes. You can also save, display, segment, upload, or delete a core dump file.

You can manage core dumps in the following ways:

- Configuring core dumps and displaying the configuration settings
- Displaying basic information, the status, and attributes of core dumps

Core dump files and reports are stored in the `/mroot/etc/crash/` directory of a node. You can display the directory content by using the `system node coredump` commands or a web browser.

- Saving the core dump content and uploading the saved file to a specified location or to technical support

ONTAP prevents you from initiating the saving of a core dump file during a takeover, an aggregate relocation, or a giveback.


- Deleting core dump files that are no longer needed



AFF A220, AFF A800, FAS2720, FAS2750, and later systems store core dumps on their boot device. When NetApp Volume Encryption (NVE) or NetApp Storage Encryption (NSE) is enabled on these systems, the core dump is also encrypted.

## Commands for managing core dumps

You use the `system node coredump config` commands to manage the configuration of core dumps, the `system node coredump` commands to manage the core dump files, and the `system node coredump reports` commands to manage application core reports.

If you want to...	Use this command...
Configure core dumps	<code>system node coredump config modify</code>
Display the configuration settings for core dumps	<code>system node coredump config show</code>
Display basic information about core dumps	<code>system node coredump show</code>
Manually trigger a core dump when you reboot a node	<code>system node reboot</code> with both the <code>-dump</code> and <code>-skip-lif-migration</code> parameters
Manually trigger a core dump when you shut down a node	<code>system node halt</code> with both the <code>-dump</code> and <code>-skip-lif-migration</code> parameters
Save a specified core dump	<code>system node coredump save</code>
Save all unsaved core dumps that are on a specified node	<code>system node coredump save-all</code>
Generate and send an AutoSupport message with a core dump file you specify	<code>system node autosupport invoke-core-upload</code> <div> The <code>-uri</code> optional parameter specifies an alternate destination for the AutoSupport message.</div>
Display status information about core dumps	<code>system node coredump status</code>
Delete a specified core dump	<code>system node coredump delete</code>
Delete all unsaved core dumps or all saved core files on a node	<code>system node coredump delete-all</code>
Display application core dump reports	<code>system node coredump reports show</code>
Delete an application core dump report	<code>system node coredump reports delete</code>

### Related information

## Monitor a storage system

### Use AutoSupport and Active IQ Digital Advisor

The AutoSupport component of ONTAP collects telemetry and sends it for analysis. Active IQ Digital Advisor analyzes the data from AutoSupport and provides proactive care and optimization. Using artificial intelligence, Active IQ can identify potential problems and help you resolve them before they impact your business.

Active IQ enables you to optimize your data infrastructure across your global hybrid cloud by delivering actionable predictive analytics and proactive support through a cloud-based portal and mobile app. Data-driven insights and recommendations from Active IQ are available to all NetApp customers with an active SupportEdge contract (features vary by product and support tier).

Here are some things you can do with Active IQ:

- Plan upgrades. Active IQ identifies issues in your environment that can be resolved by upgrading to a newer version of ONTAP and the Upgrade Advisor component helps you plan for a successful upgrade.
- View system wellness. Your Active IQ dashboard reports any issues with wellness and helps you correct those issues. Monitor system capacity to make sure you never run out of storage space. View support cases for your system.
- Manage performance. Active IQ shows system performance over a longer period than you can see in System Manager. Identify configuration and system issues that are impacting your performance.
- Maximize efficiency. View storage efficiency metrics and identify ways to store more data in less space.
- View inventory and configuration. Active IQ displays complete inventory and software and hardware configuration information. See when service contracts are expiring and renew them to ensure you remain supported.

### Related information

[NetApp Documentation: Active IQ Digital Advisor](#)

[Launch Active IQ](#)

[SupportEdge Services](#)

### Manage AutoSupport settings with System Manager

You can use System Manager to view and edit the settings for your AutoSupport account.

You can perform the following procedures:

- [View AutoSupport settings](#)
- [Generate and send AutoSupport data](#)
- [Test the connection to AutoSupport](#)
- [Enable or disable AutoSupport](#)
- [Suppress the generation of support cases](#)
- [Resume the generation of support cases](#)

- [Edit AutoSupport settings](#)

### View AutoSupport settings


You can use System Manager to view the settings for your AutoSupport account.

#### Steps

1. In System Manager, click **Cluster > Settings**.

In the **AutoSupport** section, the following information is displayed:

- Status
- Transport protocol
- Proxy server
- From email address


2. In the **AutoSupport** section, click , then click **More Options**.

Additional information is displayed about the AutoSupport connection and email settings. Also, the transfer history of messages is listed.

### Generate and send AutoSupport data

In System Manager, you can initiate the generation of AutoSupport messages and choose from which cluster node or nodes the data is collected.

#### Steps

1. In System Manager, click **Cluster > Settings**.
2. In the **AutoSupport** section, click , then click **Generate and Send**.
3. Enter a subject.
4. Click the check box under **Collect Data From** to specify the nodes from which to collect the data.

### Test the connection to AutoSupport

From System Manager, you can send a test message to verify the connection to AutoSupport.


#### Steps

1. In System Manager, click **Cluster > Settings**.
2. In the **AutoSupport** section, click , then click **Test Connectivity**.
3. Enter a subject for the message.

### Enable or disable AutoSupport

In System Manager, you can disable the ability of AutoSupport to monitor the health of your storage system and send you notification messages. You can enable AutoSupport again after it has been disabled.

#### Steps

1. Click **Cluster > Settings**.
2. In the **AutoSupport** section, click , then click **Disable**.

3. If want to enable AutoSupport again, in the **AutoSupport** section, click , then click **Enable**.

### Suppress the generation of support cases


Beginning with ONTAP 9.10.1, you can use System Manager to send a request to AutoSupport to suppress the generation of support cases.

#### About this task

To suppress the generation of support cases, you specify the nodes and number of hours for which you want the suppression to occur.

Suppressing support cases can be especially helpful if you do not want AutoSupport to create automated cases while you are performing maintenance on your systems.


#### Steps

1. Click **Cluster > Settings**.
2. In the **AutoSupport** section, click , then click **Suppress Support Case Generation**.
3. Enter the number of hours that you want the suppression to occur.
4. Select the nodes for which you want the suppression to occur.

### Resume the generation of support cases

Beginning with ONTAP 9.10.1, you can use System Manager to resume the generation of support cases from AutoSupport if it has been suppressed.



#### Steps

1. Click **Cluster > Settings**.
2. In the **AutoSupport** section, click , then click **Resume Support Case Generation**.
3. Select the nodes for which you want the generation to resume.

### Edit AutoSupport settings

You can use System Manager to modify the connection and email settings for your AutoSupport account.

#### Steps

1. Click **Cluster > Settings**.
2. In the **AutoSupport** section, click , then click **More Options**.
3. In the **Connections** section or the **Email** section, click  **Edit** to modify the setting for either section.

### Manage AutoSupport with the CLI

#### Manage AutoSupport overview

AutoSupport is a mechanism that proactively monitors the health of your system and automatically sends messages to NetApp technical support, your internal support organization, and a support partner. Although AutoSupport messages to technical support are enabled by default, you must set the correct options and have a valid mail host to have messages sent to your internal support organization.

Only the cluster administrator can perform AutoSupport management. The storage virtual machine (SVM)

administrator has no access to AutoSupport.

AutoSupport is enabled by default when you configure your storage system for the first time. AutoSupport begins sending messages to technical support 24 hours after AutoSupport is enabled. You can shorten the 24-hour period by upgrading or reverting the system, modifying the AutoSupport configuration, or changing the system time to be something other than a 24-hour period.



You can disable AutoSupport at any time, but you should leave it enabled. Enabling AutoSupport can significantly help speed problem determination and resolution should a problem occur on your storage system. By default, the system collects AutoSupport information and stores it locally, even if you disable AutoSupport.

For more information about AutoSupport, see the NetApp Support Site.

**Related information**

- [NetApp Support](#)
- [Learn more about the AutoSupport commands in the ONTAP CLI](#)

**When and where AutoSupport messages are sent**

AutoSupport sends messages to different recipients, depending on the type of message. Learning when and where AutoSupport sends messages can help you understand messages that you receive through email or view on the Active IQ (formerly known as My AutoSupport) web site.

Unless specified otherwise, settings in the following tables are parameters of the `system node autosupport modify` command.

**Event-triggered messages**

When events occur on the system that require corrective action, AutoSupport automatically sends an event-triggered message.

When the message is sent	Where the message is sent
AutoSupport responds to a trigger event in the EMS	Addresses specified in <code>-to</code> and <code>-noteto</code> . (Only critical, service-affecting events are sent.)  Addresses specified in <code>-partner-address</code>  Technical support, if <code>-support</code> is set to <code>enable</code>

**Scheduled messages**

AutoSupport automatically sends several messages on a regular schedule.



When the message is sent	Where the message is sent
Daily (by default, sent between 12:00 a.m. and 1:00 a.m. as a log message)	Addresses specified in <code>-partner-address</code>  Technical support, if <code>-support</code> is set to <code>enable</code>
Daily (by default, sent between 12:00 a.m. and 1:00 a.m. as a performance message), if the <code>-perf</code> parameter is set to <code>true</code>	Addresses specified in <code>-partner-address`</code>  Technical support, if <code>-support</code> is set to <code>enable</code>
Weekly (by default, sent Sunday between 12:00 a.m. and 1:00 a.m.)	Addresses specified in <code>-partner-address</code>  Technical support, if <code>-support</code> is set to <code>enable</code>

## Manually triggered messages

You can manually initiate or resend an AutoSupport message.

When the message is sent	Where the message is sent
You manually initiate a message using the <code>system node autosupport invoke</code> command	<p>If a URI is specified using the <code>-uri</code> parameter in the <code>system node autosupport invoke</code> command, the message is sent to that URI.</p> <p>If <code>-uri</code> is omitted, the message is sent to the addresses specified in <code>-to</code> and <code>-partner-address</code>. The message is also sent to technical support if <code>-support</code> is set to <code>enable</code>.</p>
You manually initiate a message using the <code>system node autosupport invoke-core-upload</code> command	<p>If a URI is specified using the <code>-uri</code> parameter in the <code>system node autosupport invoke-core-upload</code> command, the message is sent to that URI, and the core dump file is uploaded to the URI.</p> <p>If <code>-uri</code> is omitted in the <code>system node autosupport invoke-core-upload</code> command, the message is sent to technical support, and the core dump file is uploaded to the technical support site.</p> <p>Both scenarios require that <code>-support</code> is set to <code>enable</code> and <code>-transport</code> is set to <code>https</code> or <code>http</code>.</p> <p>Due to the large size of core dump files, the message is not sent to the addresses specified in the <code>-to</code> and <code>-partner-addresses</code> parameters.</p>

When the message is sent	Where the message is sent
You manually initiate a message using the <code>system node autosupport invoke-performance-archive</code> command	<p>If a URI is specified using the <code>-uri</code> parameter in the <code>system node autosupport invoke-performance-archive</code> command, the message is sent to that URI, and the performance archive file is uploaded to the URI.</p> <p>If <code>-uri</code> is omitted in the <code>system node autosupport invoke-performance-archive</code>, the message is sent to technical support, and the performance archive file is uploaded to the technical support site.</p> <p>Both scenarios require that <code>-support</code> is set to <code>enable</code> and <code>-transport</code> is set to <code>https</code> or <code>http</code>.</p> <p>Due to the large size of performance archive files, the message is not sent to the addresses specified in the <code>-to</code> and <code>-partner-addresses</code> parameters.</p>
You manually resend a past message using the <code>system node autosupport history retransmit</code> command	Only to the URI that you specify in the <code>-uri</code> parameter of the <code>system node autosupport history retransmit</code> command

### Messages triggered by technical support

Technical support can request messages from AutoSupport using the AutoSupport OnDemand feature.

When the message is sent	Where the message is sent
When AutoSupport obtains delivery instructions to generate new AutoSupport messages	<p>Addresses specified in <code>-partner-address</code></p> <p>Technical support, if <code>-support</code> is set to <code>enable</code> and <code>-transport</code> is set to <code>https</code></p>
When AutoSupport obtains delivery instructions to resend past AutoSupport messages	Technical support, if <code>-support</code> is set to <code>enable</code> and <code>-transport</code> is set to <code>https</code>
When AutoSupport obtains delivery instructions to generate new AutoSupport messages that upload core dump or performance archive files	Technical support, if <code>-support</code> is set to <code>enable</code> and <code>-transport</code> is set to <code>https</code> . The core dump or performance archive file is uploaded to the technical support site.

### How AutoSupport creates and sends event-triggered messages

AutoSupport creates event-triggered AutoSupport messages when the EMS processes a trigger event. An event-triggered AutoSupport message alerts recipients to problems that require corrective action and contains only information that is relevant to the problem. You

can customize what content to include and who receives the messages.

AutoSupport uses the following process to create and send event-triggered AutoSupport messages:

1. When the EMS processes a trigger event, EMS sends AutoSupport a request.

A trigger event is an EMS event with an AutoSupport destination and a name that begins with a `callhome.` prefix.

2. AutoSupport creates an event-triggered AutoSupport message.

AutoSupport collects basic and troubleshooting information from subsystems that are associated with the trigger to create a message that includes only information that is relevant to the trigger event.

A default set of subsystems is associated with each trigger. However, you can choose to associate additional subsystems with a trigger by using the `system node autosupport trigger modify` command.

3. AutoSupport sends the event-triggered AutoSupport message to the recipients defined by the `system node autosupport modify` command with the `-to`, `-noteto`, `-partner-address`, and `-support` parameters.

You can enable and disable delivery of AutoSupport messages for specific triggers by using the `system node autosupport trigger modify` command with the `-to` and `-noteto` parameters.

### Example of data sent for a specific event

The `storage shelf PSU failed` EMS event triggers a message that contains basic data from the Mandatory, Log Files, Storage, RAID, HA, Platform, and Networking subsystems and troubleshooting data from the Mandatory, Log Files, and Storage subsystems.

You decide that you want to include data about NFS in any AutoSupport messages sent in response to a future `storage shelf PSU failed` event. You enter the following command to enable troubleshooting-level data for NFS for the `callhome.shlf.ps.fault` event:

```
cluster1::\>
system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Note that the `callhome.` prefix is dropped from the `callhome.shlf.ps.fault` event when you use the `system node autosupport trigger` commands, or when referenced by AutoSupport and EMS events in the CLI.

### Types of AutoSupport messages and their content

AutoSupport messages contain status information about supported subsystems. Learning what AutoSupport messages contain can help you interpret or respond to messages that you receive in email or view on the Active IQ (formerly known as My AutoSupport) web site.

Type of message	Type of data the message contains
Event-triggered	Files containing context-sensitive data about the specific subsystem where the event occurred
Daily	Log files
Performance	Performance data sampled during the previous 24 hours
Weekly	Configuration and status data
Triggered by the <code>system node autosupport invoke</code> command	<p>Depends on the value specified in the <code>-type</code> parameter:</p> <ul style="list-style-type: none"> <li>• <code>test</code> sends a user-triggered message with some basic data.</li> </ul> <p>This message also triggers an automated email response from technical support to any specified email addresses, using the <code>-to</code> option, so that you can confirm that AutoSupport messages are being received.</p> <ul style="list-style-type: none"> <li>• <code>performance</code> sends performance data.</li> <li>• <code>all</code> sends a user-triggered message with a complete set of data similar to the weekly message, including troubleshooting data from each subsystem.</li> </ul> <p>Technical support typically requests this message.</p>
Triggered by the <code>system node autosupport invoke-core-upload</code> command	Core dump files for a node
Triggered by the <code>system node autosupport invoke-performance-archive</code> command	Performance archive files for a specified period of time

Type of message	Type of data the message contains
Triggered by AutoSupport OnDemand	<p>AutoSupport OnDemand can request new messages or past messages:</p> <ul style="list-style-type: none"> <li>• New messages, depending on the type of AutoSupport collection, can be <code>test</code>, <code>all</code>, or <code>performance</code>.</li> <li>• Past messages depend on the type of message that is resent.</li> </ul> <p>AutoSupport OnDemand can request new messages that upload the following files to the NetApp Support Site at <a href="https://mysupport.netapp.com">mysupport.netapp.com</a>:</p> <ul style="list-style-type: none"> <li>• Core dump</li> <li>• Performance archive</li> </ul>

### What AutoSupport subsystems are

Each subsystem provides basic and troubleshooting information that AutoSupport uses for its messages. Each subsystem is also associated with trigger events that allow AutoSupport to collect from subsystems only information that is relevant to the trigger event.

AutoSupport collects context-sensitive content. You can view information about subsystems and trigger events by using the `system node autosupport trigger show` command.

### AutoSupport size and time budgets

AutoSupport collects information, organized by subsystem, and enforces a size and time budget on content for each subsystem. As storage systems grow, AutoSupport budgets provide control over the AutoSupport payload, which in turn provides scalable delivery of AutoSupport data.

AutoSupport stops collecting information and truncates the AutoSupport content if the subsystem content exceeds its size or time budget. If the content cannot be truncated easily (for example, binary files), AutoSupport omits the content.

You should modify the default size and time budgets only with guidance from technical support. You can also review the default size and time budgets of the subsystems by using the `autosupport manifest show` command.

### Files sent in event-triggered AutoSupport messages

Event-triggered AutoSupport messages only contain basic and troubleshooting information from subsystems that are associated with the event that caused AutoSupport to generate the message. The specific data helps NetApp support and support partners troubleshoot the problem.

AutoSupport uses the following criteria to control content in event-triggered AutoSupport messages:

- Which subsystems are included
- Data is grouped into subsystems, including common subsystems, such as Log Files, and specific subsystems, such as RAID. Each event triggers a message that contains only the data from specific subsystems.
- The detail level of each included subsystem
- Data for each included subsystem is provided at a basic or troubleshooting level.

You can view all possible events and determine which subsystems are included in messages about each event using the `system node autosupport trigger show` command with the `-instance` parameter.

In addition to the subsystems that are included by default for each event, you can add additional subsystems at either a basic or a troubleshooting level using the `system node autosupport trigger modify` command.

**Log files sent in AutoSupport messages**

AutoSupport messages can contain several key log files that enable technical support staff to review recent system activity.

All types of AutoSupport messages might include the following log files when the Log Files subsystem is enabled:

Log file	Amount of data included from the file
<ul style="list-style-type: none"><li>• Log files from the <code>/mroot/etc/log/mlog/</code> directory</li><li>• The MESSAGES log file</li></ul>	<p>Only new lines added to the logs since the last AutoSupport message up to a specified maximum. This ensures that AutoSupport messages have unique, relevant—not overlapping—data.</p> <p>(Log files from partners are the exception; for partners, the maximum allowed data is included.)</p>
<ul style="list-style-type: none"><li>• Log files from the <code>/mroot/etc/log/shelflog/</code> directory</li><li>• Log files from the <code>/mroot/etc/log/acp/</code> directory</li><li>• Event Management System (EMS) log data</li></ul>	<p>The most recent lines of data up to a specified maximum.</p>

The content of AutoSupport messages can change between releases of ONTAP.

**Files sent in weekly AutoSupport messages**

Weekly AutoSupport messages contain additional configuration and status data that is useful to track changes in your system over time.

The following information is sent in weekly AutoSupport messages:

- Basic information about every subsystem
- Contents of selected `/mroot/etc` directory files
- Log files
- Output of commands that provide system information
- Additional information, including replicated database (RDB) information, service statistics, and more

#### **How AutoSupport OnDemand obtains delivery instructions from technical support**

AutoSupport OnDemand periodically communicates with technical support to obtain delivery instructions for sending, resending, and declining AutoSupport messages as well as uploading large files to the NetApp support site. AutoSupport OnDemand enables AutoSupport messages to be sent on-demand instead of waiting for the weekly AutoSupport job to run.

AutoSupport OnDemand consists of the following components:

- AutoSupport OnDemand client that runs on each node
- AutoSupport OnDemand service that resides in technical support

The AutoSupport OnDemand client periodically polls the AutoSupport OnDemand service to obtain delivery instructions from technical support. For example, technical support can use the AutoSupport OnDemand service to request that a new AutoSupport message be generated. When the AutoSupport OnDemand client polls the AutoSupport OnDemand service, the client obtains the delivery instructions and sends the new AutoSupport message on-demand as requested.

AutoSupport OnDemand is enabled by default. However, AutoSupport OnDemand relies on some AutoSupport settings to continue communicating with technical support. AutoSupport OnDemand automatically communicates with technical support when the following requirements are met:

- AutoSupport is enabled.
- AutoSupport is configured to send messages to technical support.
- AutoSupport is configured to use the HTTPS transport protocol.

The AutoSupport OnDemand client sends HTTPS requests to the same technical support location to which AutoSupport messages are sent. The AutoSupport OnDemand client does not accept incoming connections.



AutoSupport OnDemand uses the “autosupport” user account to communicate with technical support. ONTAP prevents you from deleting this account.

If you want to have AutoSupport OnDemand disabled, but keep AutoSupport enabled and configured to send messages to technical support by using the HTTPS transport protocol, contact technical support.

The following illustration shows how AutoSupport OnDemand sends HTTPS requests to technical support to obtain delivery instructions.



The delivery instructions can include requests for AutoSupport to do the following:

- Generate new AutoSupport messages.

Technical support might request new AutoSupport messages to help triage issues.

- Generate new AutoSupport messages that upload core dump files or performance archive files to the NetApp support site.

Technical support might request core dump or performance archive files to help triage issues.

- Retransmit previously generated AutoSupport messages.

This request automatically happens if a message was not received due to a delivery failure.

- Disable delivery of AutoSupport messages for specific trigger events.

Technical support might disable delivery of data that is not used.

### Structure of AutoSupport messages sent by email

When an AutoSupport message is sent by email, the message has a standard subject, a brief body, and a large attachment in 7z file format that contains the data.



If AutoSupport is configured to hide private data, certain information, such as the hostname, is omitted or masked in the header, subject, body, and attachments.

### Subject

The subject line of messages sent by the AutoSupport mechanism contains a text string that identifies the reason for the notification. The format of the subject line is as follows:

HA Group Notification from *System\_Name* (*Message*) *Severity*

- *System\_Name* is either the hostname or the system ID, depending on the AutoSupport configuration

### Body

The body of the AutoSupport message contains the following information:

- Date and timestamp of the message
- Version of ONTAP on the node that generated the message



- System ID, serial number, and hostname of the node that generated the message
- AutoSupport sequence number
- SNMP contact name and location, if specified
- System ID and hostname of the HA partner node

### Attached files

The key information in an AutoSupport message is contained in files that are compressed into a 7z file called `body.7z` and attached to the message.

The files contained in the attachment are specific to the type of AutoSupport message.

### AutoSupport severity types

AutoSupport messages have severity types that help you understand the purpose of each message—for example, to draw immediate attention to an emergency problem, or only to provide information.

Messages have one of the following severities:

- **Alert:** Alert messages indicate that a next-higher level event might occur if you do not take some action.  
You must take an action against alert messages within 24 hours.
- **Emergency:** Emergency messages are displayed when a disruption has occurred.  
You must take an action against emergency messages immediately.
- **Error:** Error conditions indicate what might happen if you ignore.
- **Notice:** Normal but significant condition.
- **Info:** Informational message provides details about the issue, which you can ignore.
- **Debug:** Debug-level messages provide instructions you should perform.

If your internal support organization receives AutoSupport messages through email, the severity appears in the subject line of the email message.

### Requirements for using AutoSupport

You should use HTTPS for delivery of AutoSupport messages to provide the best security and to support all of the latest AutoSupport features. Although AutoSupport supports HTTP and SMTP for delivery of AutoSupport messages, HTTPS is recommended.

### Supported protocols

All of these protocols run on IPv4 or IPv6, based on the address family to which the name resolves.

Protocol and port	Description
HTTPS on port 443	<p>This is the default protocol. You should use this whenever possible.</p> <p>This protocol supports AutoSupport OnDemand and uploads of large files.</p> <p>The certificate from the remote server is validated against the root certificate, unless you disable validation.</p> <p>The delivery uses an HTTP PUT request. With PUT, if the request fails during transmission, the request restarts where it stopped. If the server receiving the request does not support PUT, the delivery uses an HTTP POST request.</p>
HTTP on port 80	<p>This protocol is preferred over SMTP.</p> <p>This protocol supports uploads of large files, but not AutoSupport OnDemand.</p> <p>The delivery uses an HTTP PUT request. With PUT, if the request fails during transmission, the request restarts where it stopped. If the server receiving the request does not support PUT, the delivery uses an HTTP POST request.</p>
SMTP on port 25 or another port	<p>You should use this protocol only if the network connection does not allow HTTPS or HTTP.</p> <p>The default port value is 25, but you can configure AutoSupport to use a different port.</p> <p>Keep the following limitations in mind when using SMTP:</p> <ul style="list-style-type: none"> <li>• AutoSupport OnDemand and uploads of large files are not supported.</li> <li>• Data is not encrypted.</li> </ul> <p>SMTP sends data in clear text, making text in the AutoSupport message easy to intercept and read.</p> <ul style="list-style-type: none"> <li>• Limitations on message length and line length can be introduced.</li> </ul>

If you configure AutoSupport with specific email addresses for your internal support organization, or a support partner organization, those messages are always sent by SMTP.

For example, if you use the recommended protocol to send messages to technical support and you also want to send messages to your internal support organization, your messages will be transported using both HTTPS

and SMTP, respectively.

AutoSupport limits the maximum file size for each protocol. The default setting for HTTP and HTTPS transfers is 25 MB. The default setting for SMTP transfers is 5 MB. If the size of the AutoSupport message exceeds the configured limit, AutoSupport delivers as much of the message as possible. You can edit the maximum size by modifying AutoSupport configuration. See the `system node autosupport modify` man page for more information.



AutoSupport automatically overrides the maximum file size limit for the HTTPS and HTTP protocols when you generate and send AutoSupport messages that upload core dump or performance archive files to the NetApp support site or a specified URI. The automatic override applies only when you upload files by using the `system node autosupport invoke-core-upload` or the `system node autosupport invoke-performance-archive` commands.

## Configuration requirements

Depending on your network configuration, use of HTTP or HTTPS protocols may require additional configuration of a proxy URL. If you use HTTP or HTTPS to send AutoSupport messages to technical support and you have a proxy, you must identify the URL for that proxy. If the proxy uses a port other than the default port, which is 3128, you can specify the port for that proxy. You can also specify a user name and password for proxy authentication.

If you use SMTP to send AutoSupport messages either to your internal support organization or to technical support, you must configure an external mail server. The storage system does not function as a mail server; it requires an external mail server at your site to send mail. The mail server must be a host that listens on the SMTP port (25) or another port, and it must be configured to send and receive 8-bit Multipurpose Internet Mail Extensions (MIME) encoding. Example mail hosts include a UNIX host running an SMTP server such as the sendmail program and a Windows server running the Microsoft Exchange server. You can have one or more mail hosts.

## Set up AutoSupport

You can control whether and how AutoSupport information is sent to technical support and your internal support organization, and then test that the configuration is correct.

### About this task

In ONTAP 9.5 and later releases, you can enable AutoSupport and modify its configuration on all nodes of the cluster simultaneously. When a new node joins the cluster, the node inherits the AutoSupport cluster configuration automatically. You do not have to update the configuration on each node separately.



Beginning with ONTAP 9.5, the scope of the `system node autosupport modify` command is cluster-wide. The AutoSupport configuration is modified on all nodes in the cluster, even when the `-node` option is specified. The option is ignored, but it has been retained for CLI backward compatibility.

In ONTAP 9.4 and earlier releases, the scope of the "system node autosupport modify" command is specific to the node. The AutoSupport configuration should be modified on each node in your cluster.

By default, AutoSupport is enabled on each node to send messages to technical support by using the HTTPS transport protocol.

Steps

1. Ensure that AutoSupport is enabled:

```
system node autosupport modify -state enable
```

2. If you want technical support to receive AutoSupport messages, use the following command:

```
system node autosupport modify -support enable
```

You must enable this option if you want to enable AutoSupport to work with AutoSupport OnDemand or if you want to upload large files, such as core dump and performance archive files, to technical support or a specified URL.

3. If technical support is enabled to receive AutoSupport messages, specify which transport protocol to use for the messages.

You can choose from the following options:

If you want to...	Then set the following parameters of the <code>system node autosupport modify</code> command...
Use the default HTTPS protocol	<p>a. Set <code>-transport</code> to <code>https</code>.</p> <p>b. If you use a proxy, set <code>-proxy-url</code> to the URL of your proxy. This configuration supports communication with AutoSupport OnDemand and uploads of large files.</p>
Use HTTP that is preferred over SMTP	<p>a. Set <code>-transport</code> to <code>http</code>.</p> <p>b. If you use a proxy, set <code>-proxy-url</code> to the URL of your proxy. This configuration supports uploads of large files, but not AutoSupport OnDemand.</p>
Use SMTP	<p>Set <code>-transport</code> to <code>smtp</code>.</p> <p>This configuration does not support AutoSupport OnDemand or uploads of large files.</p>

4. If you want your internal support organization or a support partner to receive AutoSupport messages, perform the following actions:
- a. Identify the recipients in your organization by setting the following parameters of the `system node autosupport modify` command:

Set this parameter...	To this...
-----------------------	------------

<code>-to</code>	Up to five comma-separated individual email addresses or distribution lists in your internal support organization that will receive key AutoSupport messages
<code>-noteto</code>	Up to five comma-separated individual email addresses or distribution lists in your internal support organization that will receive a shortened version of key AutoSupport messages designed for cell phones and other mobile devices
<code>-partner-address</code>	Up to five comma-separated individual email addresses or distribution lists in your support partner organization that will receive all AutoSupport messages

- b. Check that addresses are correctly configured by listing the destinations using the `system node autosupport destinations show` command.
5. If you are sending messages to your internal support organization or you chose SMTP transport for messages to technical support, configure SMTP by setting the following parameters of the `system node autosupport modify` command:

- Set `-mail-hosts` to one or more mail hosts, separated by commas.

You can set a maximum of five.

You can configure a port value for each mail host by specifying a colon and port number after the mail host name: for example, `mymailhost.example.com:5678`, where 5678 is the port for the mail host.

- Set `-from` to the email address that sends the AutoSupport message.

6. Configure DNS.
7. (Optional) Add command options if you want to change specific settings:

If you want to do this...	Then set the following parameters of the <code>system node autosupport modify</code> command...
Hide private data by removing, masking, or encoding sensitive data in the messages	Set <code>-remove-private-data</code> to <code>true</code> . If you change from <code>false</code> to <code>true</code> , all AutoSupport history and all associated files are deleted.
Stop sending performance data in periodic AutoSupport messages	Set <code>-perf</code> to <code>false</code> .

8. Check the overall configuration by using the `system node autosupport show` command with the `-node` parameter.
9. Verify the AutoSupport operation by using the `system node autosupport check show` command.

If any problems are reported, use the `system node autosupport check show-details` command to view more information.

10. Test that AutoSupport messages are being sent and received:

- a. Use the `system node autosupport invoke` command with the `-type` parameter set to `test`.

```
cluster1::> system node autosupport invoke -type test -node node1
```

- b. Confirm that NetApp is receiving your AutoSupport messages:

```
system node autosupport history show -node local
```

The status of the latest outgoing AutoSupport message should eventually change to `sent-successful` for all appropriate protocol destinations.

- c. (Optional) Confirm that the AutoSupport message is being sent to your internal support organization or to your support partner by checking the email of any address that you configured for the `-to`, `-noteto`, or `-partner-address` parameters of the `system node autosupport modify` command.

### Upload core dump files

When a core dump file is saved, an event message is generated. If the AutoSupport service is enabled and configured to send messages to NetApp support, an AutoSupport message is transmitted, and an automated email acknowledgement is sent to you.

### What you'll need

- You must have set up AutoSupport with the following settings:
  - AutoSupport is enabled on the node.
  - AutoSupport is configured to send messages to technical support.
  - AutoSupport is configured to use the HTTP or HTTPS transport protocol.

The SMTP transport protocol is not supported when sending messages that include large files, such as core dump files.

### About this task

You can also upload the core dump file through the AutoSupport service over HTTPS by using the `system node autosupport invoke-core-upload` command, if requested by NetApp support.

### [How to upload a file to NetApp](#)

### Steps

1. View the core dump files for a node by using the `system node coredump show` command.

In the following example, core dump files are displayed for the local node:

```
cluster1::> system node coredump show -node local
Node:Type Core Name Saved Panic Time
-----
node:kernel
core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
```

2. Generate an AutoSupport message and upload a core dump file by using the `system node autosupport invoke-core-upload` command.

In the following example, an AutoSupport message is generated and sent to the default location, which is technical support, and the core dump file is uploaded to the default location, which is the NetApp support site:

```
cluster1::> system node autosupport invoke-core-upload -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

In the following example, an AutoSupport message is generated and sent to the location specified in the URI, and the core dump file is uploaded to the URI:

```
cluster1::> system node autosupport invoke-core-upload -uri
https://files.company.com -core-filename
core.4073000068.2013-09-11.15_05_01.nz -node local
```

### Upload performance archive files

You can generate and send an AutoSupport message that contains a performance archive. By default, NetApp technical support receives the AutoSupport message, and the performance archive is uploaded to the NetApp support site. You can specify an alternate destination for the message and upload.

#### What you'll need

- You must have set up AutoSupport with the following settings:
  - AutoSupport is enabled on the node.
  - AutoSupport is configured to send messages to technical support.
  - AutoSupport is configured to use the HTTP or HTTPS transport protocol.

The SMTP transport protocol is not supported when sending messages that include large files, such as performance archive files.

#### About this task

You must specify a start date for the performance archive data that you want to upload. Most storage systems retain performance archives for two weeks, enabling you to specify a start date up to two weeks ago. For example, if today is January 15, you can specify a start date of January 2. If you need help identifying the start

date for the performance archive that you want to upload, contact technical support.

**Step**

1. Generate an AutoSupport message and upload the performance archive file by using the `system node autosupport invoke-performance-archive` command.

In the following example, 4 hours of performance archive files from January 12, 2015 are added to an AutoSupport message and uploaded to the default location, which is the NetApp support site:

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h
```

In the following example, 4 hours of performance archive files from January 12, 2015 are added to an AutoSupport message and uploaded to the location specified by the URI:

```
cluster1::> system node autosupport invoke-performance-archive -node
local -start-date 1/12/2015 13:42:09 -duration 4h -uri
https://files.company.com
```

**Get AutoSupport message descriptions**

The descriptions of the AutoSupport messages that you receive are available through the online AutoSupport Message Matrices page.

**Steps**

1. Go to the AutoSupport Message Matrices page.  
  
[support.netapp.com/NOW/knowledge/docs/olio/autosupport/matrices/](https://support.netapp.com/NOW/knowledge/docs/olio/autosupport/matrices/)
2. On the AutoSupport Message Matrices page under Select a Release, select your version of ONTAP, and then click **View Matrix**.

The Syslog Translator page appears with all AutoSupport message descriptions listed alphabetically by subject line.

**Commands for managing AutoSupport**

You use the `system node autosupport` commands to change or view AutoSupport configuration, display information about previous AutoSupport messages, and send, resend or cancel an AutoSupport message.

**Configure AutoSupport**

If you want to...	Use this command...
Control whether any AutoSupport messages are sent	<code>system node autosupport modify with the -state parameter</code>



If you want to...	Use this command...
Control whether AutoSupport messages are sent to technical support	<code>system node autosupport modify with the -support parameter</code>
Set up AutoSupport or modify the configuration of AutoSupport	<code>system node autosupport modify</code>
Enable and disable AutoSupport messages to your internal support organization for individual trigger events, and specify additional subsystem reports to include in messages sent in response to individual trigger events	<code>system node autosupport trigger modify</code>

### Display information about the AutoSupport configuration

If you want to...	Use this command...
Display the AutoSupport configuration	<code>system node autosupport show with the -node parameter</code>
View a summary of all addresses and URLs that receive AutoSupport messages	<code>system node autosupport destinations show</code>
Display which AutoSupport messages are sent to your internal support organization for individual trigger events	<code>system node autosupport trigger show</code>
Display status of AutoSupport configuration as well as delivery to various destinations	<code>system node autosupport check show</code>
Display detailed status of AutoSupport configuration as well as delivery to various destinations	<code>system node autosupport check show-details</code>

### Display information about past AutoSupport messages

If you want to...	Use this command...
Display information about one or more of the 50 most recent AutoSupport messages	<code>system node autosupport history show</code>
Display information about recent AutoSupport messages generated to upload core dump or performance archive files to the technical support site or a specified URI	<code>system node autosupport history show-upload-details</code>

If you want to...	Use this command...
View the information in the AutoSupport messages including the name and size of each file collected for the message along with any errors	<code>system node autosupport manifest show</code>

## Send, resend, or cancel AutoSupport messages

If you want to...	Use this command...
Retransmit a locally stored AutoSupport message, identified by its AutoSupport sequence number <div>  <p>If you retransmit an AutoSupport message, and if support already received that message, the support system will not create a duplicate case. If, on the other hand, support did not receive that message, then the AutoSupport system will analyze the message and create a case, if necessary.</p> </div>	<code>system node autosupport history retransmit</code>
Generate and send an AutoSupport message—for example, for testing purposes	<code>system node autosupport invoke</code> <div>  <p>Use the <code>-force</code> parameter to send a message even if AutoSupport is disabled. Use the <code>-uri</code> parameter to send the message to the destination you specify instead of the configured destination.</p> </div>
Cancel an AutoSupport message	<code>system node autosupport history cancel</code>

## Related information

[ONTAP 9 commands](#)

### Information included in the AutoSupport manifest

The AutoSupport manifest provides you with a detailed view of the files collected for each AutoSupport message. The AutoSupport manifest also includes information about collection errors when AutoSupport cannot collect the files it needs.

The AutoSupport manifest includes the following information:

- Sequence number of the AutoSupport message
- Which files AutoSupport included in the AutoSupport message
- Size of each file, in bytes

- Status of the AutoSupport manifest collection
- Error description, if AutoSupport failed to collect one or more files

You can view the AutoSupport manifest by using the `system node autosupport manifest show` command.

The AutoSupport manifest is included with every AutoSupport message and presented in XML format, which means that you can either use a generic XML viewer to read it or view it using the Active IQ (formerly known as My AutoSupport) portal.

#### AutoSupport case suppression during scheduled maintenance windows

AutoSupport case suppression enables you to stop unnecessary cases from being created by AutoSupport messages that are triggered during scheduled maintenance windows.

To suppress AutoSupport cases, you must manually invoke an AutoSupport message with a specially formatted text string: `MAINT=xh`. `x` is the duration of the maintenance window in units of hours.

#### Related information

[How to suppress automatic case creation during scheduled maintenance windows](#)

#### Troubleshoot AutoSupport

##### Troubleshoot AutoSupport when messages are not received

If the system does not send the AutoSupport message, you can determine whether that is because AutoSupport cannot generate the message or cannot deliver the message.

#### Steps

1. Check delivery status of the messages by using the `system node autosupport history show` command.
2. Read the status.

This status	Means
initializing	The collection process is starting. If this state is temporary, all is well. However, if this state persists, there is an issue.
collection-failed	AutoSupport cannot create the AutoSupport content in the spool directory. You can view what AutoSupport is trying to collect by entering the <code>system node autosupport history show -detail</code> command.
collection-in-progress	AutoSupport is collecting AutoSupport content. You can view what AutoSupport is collecting by entering the <code>system node autosupport manifest show</code> command.
queued	AutoSupport messages are queued for delivery, but not yet delivered.

This status	Means
transmitting	AutoSupport is currently delivering messages.
sent-successful	AutoSupport successfully delivered the message. You can find out where AutoSupport delivered the message by entering the <code>system node autosupport history show -delivery</code> command.
ignore	AutoSupport has no destinations for the message. You can view the delivery details by entering the <code>system node autosupport history show -delivery</code> command.
re-queued	AutoSupport tried to deliver messages, but the attempt failed. As a result, AutoSupport placed the messages back in the delivery queue for another attempt. You can view the error by entering the <code>system node autosupport history show</code> command.
transmission-failed	AutoSupport failed to deliver the message the specified number of times and stopped trying to deliver the message. You can view the error by entering the <code>system node autosupport history show</code> command.
ondemand-ignore	The AutoSupport message was processed successfully, but the AutoSupport OnDemand service chose to ignore it.

3. Perform one of the following actions:

For this status	Do this
initializing or collection-failed	Contact technical support because AutoSupport cannot generate the message.
ignore, re-queued, or transmission failed	Check that destinations are correctly configured for SMTP, HTTP, or HTTPS because AutoSupport cannot deliver the message.

## Troubleshoot AutoSupport message delivery over HTTP or HTTPS

If the system does not send the expected AutoSupport message and you are using HTTP or HTTPS, or the Automatic Update feature is not working, you can check a number of settings to resolve the problem.

### What you'll need

You should have confirmed basic network connectivity and DNS lookup:

- Your node management LIF must be up for operational and administrative status.
- You must be able to ping a functioning host on the same subnet from the cluster management LIF (not a LIF on any of the nodes).

- You must be able to ping a functioning host outside the subnet from the cluster management LIF.
- You must be able to ping a functioning host outside the subnet from the cluster management LIF using the name of the host (not the IP address).

### About this task

These steps are for cases when you have determined that AutoSupport can generate the message, but cannot deliver the message over HTTP or HTTPS.

If you encounter errors or cannot complete a step in this procedure, determine and address the problem before proceeding to the next step.

### Steps

1. Display the detailed status of the AutoSupport subsystem:

```
system node autosupport check show-details
```

This includes verifying connectivity to AutoSupport destinations by sending test messages and providing a list of possible errors in your AutoSupport configuration settings.

2. Verify the status of the node management LIF:

```
network interface show -home-node local -role node-mgmt -fields
vserver, lif, status-oper, status-admin, address, role
```

The status-oper and status-admin fields should return “up”.

3. Record the SVM name, the LIF name, and the LIF IP address for later use.
4. Ensure that DNS is enabled and configured correctly:

```
vserver services name-service dns show
```

5. Address any errors returned by the AutoSupport message:

```
system node autosupport history show -node * -fields node, seq-
num, destination, last-update, status, error
```

If the error refers to a problem with the digital certificate, contact technical support.

6. Confirm that the cluster can access both the servers it needs and the Internet successfully:

a. `network traceroute -lif node-management_LIF -destination DNS server`

b. `network traceroute -lif node_management_LIF -destination support.netapp.com`



The address `support.netapp.com` itself does not respond to ping/traceroute, but the per-hop information is valuable.

c. `system node autosupport show -fields proxy-url`

d. `network traceroute -node node_management_LIF -destination proxy_url`

If any of these routes are not functioning, try the same route from a functioning host on the same subnet as the cluster, using the “traceroute” or “tracert” utility found on most third-party network clients. This assists you in determining whether the issue is in your network configuration or your cluster configuration.

7. If you are using HTTPS for your AutoSupport transport protocol, ensure that HTTPS traffic can exit your network:

- a. Configure a web client on the same subnet as the cluster management LIF.

Ensure that all configuration parameters are the same values as for the AutoSupport configuration, including using the same proxy server, user name, password, and port.

- b. Access `https://support.netapp.com` with the web client.

The access should be successful. If not, ensure that all firewalls are configured correctly to allow HTTPS and DNS traffic, and that the proxy server is configured correctly. For more information on configuring static name resolution for `support.netapp.com`, see the article [How would a HOST entry be added in ONTAP for support.netapp.com?](#).

8. Beginning with ONTAP 9.10.1, if you enabled the Automatic Update feature, ensure you have HTTPS connectivity to the following additional URLs:

- `https://support-sg-emea.netapp.com`
- `https://support-sg-naeast.netapp.com`
- `https://support-sg-nawest.netapp.com`

## Troubleshoot AutoSupport message delivery over SMTP

If the system cannot deliver AutoSupport messages over SMTP, you can check a number of settings to resolve the problem.

### What you'll need

You should have confirmed basic network connectivity and DNS lookup:

- Your node management LIF must be up for operational and administrative status.
- You must be able to ping a functioning host on the same subnet from the cluster management LIF (not a LIF on any of the nodes).
- You must be able to ping a functioning host outside the subnet from the cluster management LIF.
- You must be able to ping a functioning host outside the subnet from the cluster management LIF using the name of the host (not the IP address).

### About this task

These steps are for cases when you have determined that AutoSupport can generate the message, but cannot deliver the message over SMTP.

If you encounter errors or cannot complete a step in this procedure, determine and address the problem before proceeding to the next step.

All commands are entered at the ONTAP command-line interface, unless otherwise specified.

### Steps

1. Verify the status of the node management LIF:

```
network interface show -home-node local -role node-mgmt -fields
vserver,lif,status-oper,status-admin,address,role
```

The `status-oper` and `status-admin` fields should return up.

- Record the SVM name, the LIF name, and the LIF IP address for later use.
- Ensure that DNS is enabled and configured correctly:

```
vserver services name-service dns show
```

- Display all of the servers configured to be used by AutoSupport:

```
system node autosupport show -fields mail-hosts
```

Record all server names displayed.

- For each server displayed by the previous step, and `support.netapp.com`, ensure that the server or URL can be reached by the node:

```
network traceroute -node local -destination server_name
```

If any of these routes is not functioning, try the same route from a functioning host on the same subnet as the cluster, using the “traceroute” or “tracert” utility found on most third-party network clients. This assists you in determining whether the issue is in your network configuration or your cluster configuration.

- Log in to the host designated as the mail host, and ensure that it can serve SMTP requests:

```
netstat -aAn|grep 25
```

25 is the listener SMTP port number.

A message similar to the following text is displayed:

```
ff64878c tcp          0      0 *.25    *.*    LISTEN.
```

- From some other host, open a Telnet session with the SMTP port of the mail host:

```
telnet mailhost 25
```

A message similar to the following text is displayed:

```
220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
10:49:04 PST
```

- At the telnet prompt, ensure that a message can be relayed from your mail host:

```
HELO domain_name
```

```
MAIL FROM: your_email_address
```

```
RCPT TO: autosupport@netapp.com
```

`domain_name` is the domain name of your network.

If an error is returned saying that relaying is denied, relaying is not enabled on the mail host. Contact your system administrator.

9. At the telnet prompt, send a test message:

**DATA**

**SUBJECT: TESTING**

**THIS IS A TEST**

.



Ensure that you enter the last period (.) on a line by itself. The period indicates to the mail host that the message is complete.

If an error is returned, your mail host is not configured correctly. Contact your system administrator.

10. From the ONTAP command-line interface, send an AutoSupport test message to a trusted email address that you have access to:

```
system node autosupport invoke -node local -type test
```

11. Find the sequence number of the attempt:

```
system node autosupport history show -node local -destination smtp
```

Find the sequence number for your attempt based on the timestamp. It is probably the most recent attempt.

12. Display the error for your test message attempt:

```
system node autosupport history show -node local -seq-num seq_num -fields error
```

If the error displayed is `Login denied`, your SMTP server is not accepting send requests from the cluster management LIF. If you do not want to change to using HTTPS as your transport protocol, contact your site network administrator to configure the SMTP gateways to address this issue.

If this test succeeds but the same message sent to `mailto:autosupport@netapp.com` does not, ensure that SMTP relay is enabled on all of your SMTP mail hosts, or use HTTPS as a transport protocol.

If even the message to the locally administered email account does not succeed, confirm that your SMTP servers are configured to forward attachments with both of these characteristics:

- The “7z” suffix
- The “application/x-7x-compressed” MIME type.

## Troubleshoot the AutoSupport subsystem

The `system node check show` commands can be used to verify and troubleshoot any issues related to the AutoSupport configuration and delivery.

### Step



1. Use the following commands to display the status of the AutoSupport subsystem.

Use this command...	To do this...
<b>system node autosupport check show</b>	Display overall status of the AutoSupport subsystem, such as the status of AutoSupport HTTP or HTTPS destination, AutoSupport SMTP destinations, AutoSupport OnDemand Server, and AutoSupport configuration
<b>system node autosupport check show-details</b>	Display detailed status of the AutoSupport subsystem, such as detailed descriptions of errors and the corrective actions

## Monitor the health of your system

### Monitor the health of your system overview

Health monitors proactively monitor certain critical conditions in your cluster and raise alerts if they detect a fault or risk. If there are active alerts, the system health status reports a degraded status for the cluster. The alerts include the information that you need to respond to degraded system health.

If the status is degraded, you can view details about the problem, including the probable cause and recommended recovery actions. After you resolve the problem, the system health status automatically returns to OK.

The system health status reflects multiple separate health monitors. A degraded status in an individual health monitor causes a degraded status for the overall system health.

For details on how ONTAP supports cluster switches for system health monitoring in your cluster, you can refer to the *Hardware Universe*.

### [Supported switches in the Hardware Universe](#)

For details on the causes of Cluster Switch Health Monitor (CSHM) AutoSupport messages, and the necessary actions required to resolve these alerts, you can refer to the Knowledgebase article.

### [AutoSupport Message: Health Monitor Process CSHM](#)

### How health monitoring works

Individual health monitors have a set of policies that trigger alerts when certain conditions occur. Understanding how health monitoring works can help you respond to problems and control future alerts.

Health monitoring consists of the following components:

- Individual health monitors for specific subsystems, each of which has its own health status

For example, the Storage subsystem has a node connectivity health monitor.

- An overall system health monitor that consolidates the health status of the individual health monitors

A degraded status in any single subsystem results in a degraded status for the entire system. If no subsystems have alerts, the overall system status is OK.

Each health monitor is made up of the following key elements:

- Alerts that the health monitor can potentially raise

Each alert has a definition, which includes details such as the severity of the alert and its probable cause.

- Health policies that identify when each alert is triggered

Each health policy has a rule expression, which is the exact condition or change that triggers the alert.

A health monitor continuously monitors and validates the resources in its subsystem for condition or state changes. When a condition or state change matches a rule expression in a health policy, the health monitor raises an alert. An alert causes the subsystem's health status and the overall system health status to become degraded.

#### **Ways to respond to system health alerts**

When a system health alert occurs, you can acknowledge it, learn more about it, repair the underlying condition, and prevent it from occurring again.

When a health monitor raises an alert, you can respond in any of the following ways:

- Get information about the alert, which includes the affected resource, alert severity, probable cause, possible effect, and corrective actions.
- Get detailed information about the alert, such as the time when the alert was raised and whether anyone else has acknowledged the alert already.
- Get health-related information about the state of the affected resource or subsystem, such as a specific shelf or disk.
- Acknowledge the alert to indicate that someone is working on the problem, and identify yourself as the "Acknowledger."
- Resolve the problem by taking the corrective actions provided in the alert, such as fixing cabling to resolve a connectivity problem.
- Delete the alert, if the system did not automatically clear it.
- Suppress an alert to prevent it from affecting the health status of a subsystem.

Suppressing is useful when you understand a problem. After you suppress an alert, it can still occur, but the subsystem health displays as "ok-with-suppressed." when the suppressed alert occurs.

#### **System health alert customization**

You can control which alerts a health monitor generates by enabling and disabling the system health policies that define when alerts are triggered. This enables you to customize the health monitoring system for your particular environment.

You can learn the name of a policy either by displaying detailed information about a generated alert or by

displaying policy definitions for a specific health monitor, node, or alert ID.

Disabling health policies is different from suppressing alerts. When you suppress an alert, it does not affect the subsystem's health status, but the alert can still occur.

If you disable a policy, the condition or state that is defined in its policy rule expression no longer triggers an alert.

### **Example of an alert that you want to disable**

For example, suppose an alert occurs that is not useful to you. You use the `system health alert show -instance` command to obtain the Policy ID for the alert. You use the policy ID in the `system health policy definition show` command to view information about the policy. After reviewing the rule expression and other information about the policy, you decide to disable the policy. You use the `system health policy definition modify` command to disable the policy.

### **How health alerts trigger AutoSupport messages and events**

System health alerts trigger AutoSupport messages and events in the Event Management System (EMS), enabling you to monitor the health of the system using AutoSupport messages and the EMS in addition to using the health monitoring system directly.

Your system sends an AutoSupport message within five minutes of an alert. The AutoSupport message includes all alerts generated since the previous AutoSupport message, except for alerts that duplicate an alert for the same resource and probable cause within the previous week.

Some alerts do not trigger AutoSupport messages. An alert does not trigger an AutoSupport message if its health policy disables the sending of AutoSupport messages. For example, a health policy might disable AutoSupport messages by default because AutoSupport already generates a message when the problem occurs. You can configure policies to not trigger AutoSupport messages by using the `system health policy definition modify` command.

You can view a list of all of the alert-triggered AutoSupport messages sent in the previous week using the `system health autosupport trigger history show` command.

Alerts also trigger the generation of events to the EMS. An event is generated each time an alert is created and each time an alert is cleared.

### **Available cluster health monitors**

There are several health monitors that monitor different parts of a cluster. Health monitors help you to recover from errors within ONTAP systems by detecting events, sending alerts to you, and deleting events as they clear.

Health monitor name (identifier)	Subsystem name (identifier)	Purpose
Cluster switch(cluster-switch)	Switch (Switch-Health)	<p>Monitors cluster network switches and management network switches for temperature, utilization, interface configuration, redundancy (cluster network switches only), and fan and power supply operation. The cluster switch health monitor communicates with switches through SNMP. SNMPv2c is the default setting.</p> <div>  <p>Beginning with ONTAP 9.2, this monitor can detect and report when a cluster switch has rebooted since the last polling period.</p> </div>
MetroCluster Fabric	Switch	Monitors the MetroCluster configuration back-end fabric topology and detects misconfigurations such as incorrect cabling and zoning, and ISL failures.
MetroCluster Health	Interconnect, RAID, and storage	Monitors FC-VI adapters, FC initiator adapters, left-behind aggregates and disks, and inter-cluster ports
Node connectivity(node-connect)	CIFS nondisruptive operations (CIFS-NDO)	Monitors SMB connections for nondisruptive operations to Hyper-V applications.
	Storage (SAS-connect)	Monitors shelves, disks, and adapters at the node level for appropriate paths and connections.
System	not applicable	Aggregates information from other health monitors.
System connectivity (system-connect)	Storage (SAS-connect)	Monitors shelves at the cluster level for appropriate paths to two HA clustered nodes.

## Receive system health alerts automatically

You can manually view system health alerts by using the `system health alert show` command. However, you should subscribe to specific Event Management System (EMS) messages to automatically receive notifications when a health monitor generates an alert.

### About this task

The following procedure shows you how to set up notifications for all `hm.alert.raised` messages and all `hm.alert.cleared` messages.

All `hm.alert.raised` messages and all `hm.alert.cleared` messages include an SNMP trap. The names of the SNMP traps are `HealthMonitorAlertRaised` and `HealthMonitorAlertCleared`. For information about SNMP traps, see the *Network Management Guide*.

### Steps

1. Use the `event destination create` command to define the destination to which you want to send the EMS messages.

```
cluster1::> event destination create -name health_alerts -mail  
admin@example.com
```

2. Use the `event route add-destinations` command to route the `hm.alert.raised` message and the `hm.alert.cleared` message to a destination.

```
cluster1::> event route add-destinations -messagename hm.alert*  
-destinations health_alerts
```

### Related information

[Network management](#)

## Respond to degraded system health

When your system's health status is degraded, you can show alerts, read about the probable cause and corrective actions, show information about the degraded subsystem, and resolve the problem. Suppressed alerts are also shown so that you can modify them and see whether they have been acknowledged.

### About this task

You can discover that an alert was generated by viewing an AutoSupport message or an EMS event, or by using the `system health` commands.

### Steps

1. Use the `system health alert show` command to view the alerts that are compromising the system's health.
2. Read the alert's probable cause, possible effect, and corrective actions to determine whether you can resolve the problem or need more information.

3. If you need more information, use the `system health alert show -instance` command to view additional information available for the alert.
4. Use the `system health alert modify` command with the `-acknowledge` parameter to indicate that you are working on a specific alert.
5. Take corrective action to resolve the problem as described by the `Corrective Actions` field in the alert.

The corrective actions might include rebooting the system.

When the problem is resolved, the alert is automatically cleared. If the subsystem has no other alerts, the health of the subsystem changes to `OK`. If the health of all subsystems is `OK`, the overall system health status changes to `OK`.

6. Use the `system health status show` command to confirm that the system health status is `OK`.

If the system health status is not `OK`, repeat this procedure.

#### Example of responding to degraded system health

By reviewing a specific example of degraded system health caused by a shelf that lacks two paths to a node, you can see what the CLI displays when you respond to an alert.

After starting ONTAP, you check the system health and you discover that the status is degraded:

```
cluster1::>system health status show
Status
-----
degraded
```

You show alerts to find out where the problem is, and see that shelf 2 does not have two paths to node1:

```
cluster1::>system health alert show
```

```
Node: node1
```

```
Resource: Shelf ID 2
```

```
Severity: Major
```

```
Indication Time: Mon Nov 10 16:48:12 2013
```

```
Probable Cause: Disk shelf 2 does not have two paths to controller  
node1.
```

```
Possible Effect: Access to disk shelf 2 via controller node1 will be  
lost with a single hardware component failure (e.g.  
cable, HBA, or IOM failure).
```

```
Corrective Actions: 1. Halt controller node1 and all controllers attached  
to disk shelf 2.
```

```
2. Connect disk shelf 2 to controller node1 via two  
paths following the rules in the Universal SAS and ACP Cabling Guide.
```

```
3. Reboot the halted controllers.
```

```
4. Contact support personnel if the alert persists.
```

You display details about the alert to get more information, including the alert ID:

```

cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
    Node: node1
    Monitor: node-connect
    Alert ID: DualPathToDiskShelf_Alert
    Alerting Resource: 50:05:0c:c1:02:00:0f:02
    Subsystem: SAS-connect
    Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
    Probable Cause: Connection_establishment_error
    Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
    Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
    hardware component failure (e.g. cable, HBA, or IOM failure).
    Acknowledge: false
    Suppress: false
    Policy: DualPathToDiskShelf_Policy
    Acknowledger: -
    Suppressor: -
    Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
    Alerting Resource Name: Shelf ID 2

```

You acknowledge the alert to indicate that you are working on it.

```

cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true

```

You fix the cabling between shelf 2 and node1, and then reboot the system. Then you check system health again, and see that the status is OK:



```
cluster1::>system health status show
Status
-----
OK
```

### Configure discovery of cluster and management network switches

The cluster switch health monitor automatically attempts to discover your cluster and management network switches using the Cisco Discovery Protocol (CDP). You must configure the health monitor if it cannot automatically discover a switch or if you do not want to use CDP for automatic discovery.

#### About this task

The `system cluster-switch show` command lists the switches that the health monitor discovered. If you do not see a switch that you expected to see in that list, then the health monitor cannot automatically discover it.

#### Steps

1. If you want to use CDP for automatic discovery, do the following; otherwise, go to step 2:

- a. Ensure that the Cisco Discovery Protocol (CDP) is enabled on your switches.

Refer to your switch documentation for instructions.

- b. Run the following command on each node in the cluster to verify whether CDP is enabled or disabled:

```
run -node node_name -command options cdpd.enable
```

If CDP is enabled, go to step d. If CDP is disabled, go to step c.

- c. Run the following command to enable CDP:

```
run -node node_name -command options cdpd.enable on
```

Wait five minutes before you go to the next step.

- d. Use the `system cluster-switch show` command to verify whether ONTAP can now automatically discover the switches.

2. If the health monitor cannot automatically discover a switch, use the `system cluster-switch create` command to configure discovery of the switch:

```
cluster1::> system cluster-switch create -device switch1 -address
192.0.2.250 -snmp-version SNMPv2c -community cshml! -model NX5020 -type
cluster-network
```

Wait five minutes before you go to the next step.

3. Use the `system cluster-switch show` command to verify that ONTAP can discover the switch for which you added information.

**After you finish**

Verify that the health monitor can monitor your switches.


**Verify the monitoring of cluster and management network switches**

The cluster switch health monitor automatically attempts to monitor the switches that it discovers; however, monitoring might not happen automatically if the switches are not configured correctly. You should verify that the health monitor is properly configured to monitor your switches.

**Steps**

- 1. Use the `system health cluster-switch show` command to identify the switches that the cluster switch health monitor discovered.

If the `Model` column displays the value `OTHER`, then ONTAP cannot monitor the switch. ONTAP sets the value to `OTHER` if a switch that it automatically discovers is not supported for health monitoring.



If a switch does not display in the command output, then you must configure discovery of the switch.

- 2. Upgrade to the latest supported switch software and reference the configuration file (RCF) from the NetApp Support Site.

[Cisco Ethernet Switch page](#)

The community string in the switch's RCF must match the community string that the health monitor is configured to use. By default, the health monitor uses the community string `cshml!`.

If you need to change information about a switch that the cluster monitors, you can modify the community string that the health monitor uses by using the `system health cluster-switch modify` command.

- 3. Verify that the switch's management port is connected to the management network.

This connection is required to perform SNMP queries.

**Commands for monitoring the health of your system**

You can use the `system health` commands to display information about the health of system resources, to respond to alerts, and to configure future alerts. Using the CLI commands enables you to view in-depth information about how health monitoring is configured. The man pages for the commands contain more information.

**Display the status of system health**

If you want to...	Use this command...
Display the health status of the system, which reflects the overall status of individual health monitors	<code>system health status show</code>

If you want to...	Use this command...
Display the health status of subsystems for which health monitoring is available	<code>system health subsystem show</code>

## Display the status of node connectivity

If you want to...	Use this command...
Display details about connectivity from the node to the storage shelf, including port information, HBA port speed, I/O throughput, and the rate of I/O operations per second	<code>storage shelf show -connectivity</code>  Use the <code>-instance</code> parameter to display detailed information about each shelf.
Display information about drives and array LUNs, including the usable space, shelf and bay numbers, and owning node name	<code>storage disk show</code>  Use the <code>-instance</code> parameter to display detailed information about each drive.
Display detailed information about storage shelf ports, including port type, speed, and status	<code>storage port show</code>  Use the <code>-instance</code> parameter to display detailed information about each adapter.

## Manage the discovery of cluster and management network switches

If you want to...	Use this command...
Display the switches that the cluster monitors	<code>system cluster-switch show</code>
Display the switches that the cluster currently monitors, including switches that you deleted (shown in the Reason column in the command output), and configuration information that you need for network access to the cluster and management network switches.  This command is available at the advanced privilege level.	<code>system cluster-switch show-all</code>
Configure discovery of an undiscovered switch	<code>system cluster-switch create</code>
Modify information about a switch that the cluster monitors (for example, device name, IP address, SNMP version, and community string)	<code>system cluster-switch modify</code>
Disable monitoring of a switch	<code>system cluster-switch modify -disable -monitoring</code>

If you want to...	Use this command...
Display the interval in which the health monitor polls switches to gather information	<code>system cluster-switch polling-interval show</code>
Modify the interval in which the health monitor polls switches to gather information.  This command is available at the advanced privilege level.	<code>system cluster-switch polling-interval modify</code>
Disable discovery and monitoring of a switch and delete switch configuration information	<code>system cluster-switch delete</code>
Permanently remove the switch configuration information which is stored in the database (doing so reenables automatic discovery of the switch)	<code>system cluster-switch delete -force</code>
Enable automatic logging to send with AutoSupport messages.  This command is available at the advanced privilege level.	<code>system cluster-switch log</code>

## Respond to generated alerts

If you want to...	Use this command...
Display information about generated alerts, such as the resource and node where the alert was triggered, and the alert's severity and probable cause	<code>system health alert show</code>
Display information about each generated alert	<code>system health alert show -instance</code>
Indicate that someone is working on an alert	<code>system health alert modify</code>
Acknowledge an alert	<code>system health alert modify -acknowledge</code>
Suppress a subsequent alert so that it does not affect the health status of a subsystem	<code>system health alert modify -suppress</code>
Delete an alert that was not automatically cleared	<code>system health alert delete</code>
Display information about the AutoSupport messages that alerts triggered within the last week, for example, to determine whether an alert triggered an AutoSupport message	<code>system health autosupport trigger history show</code>

## Configure future alerts

If you want to...	Use this command...
Enable or disable the policy that controls whether a specific resource state raises a specific alert	<code>system health policy definition modify</code>

## Display information about how health monitoring is configured

If you want to...	Use this command...
Display information about health monitors, such as their nodes, names, subsystems, and status	<code>system health config show</code>   Use the <code>-instance</code> parameter to display detailed information about each health monitor.
Display information about the alerts that a health monitor can potentially generate	<code>system health alert definition show</code>   Use the <code>-instance</code> parameter to display detailed information about each alert definition.
Display information about health monitor policies, which determine when alerts are raised	<code>system health policy definition show</code>   Use the <code>-instance</code> parameter to display detailed information about each policy. Use other parameters to filter the list of alerts—for example, by policy status (enabled or not), health monitor, alert, and so on.

## Downgrade software versions between minor releases

When downgrading a cluster from Data ONTAP 8.2.1 to Data ONTAP 8.2, ONTAP clears the history of deleted switches. It also sets the `Model` column to `OTHER` if a switch that it automatically discovers is not supported for health monitoring.

If you want to...	Use this command...
Downgrade the software version command	<code>system cluster-switch prepare-to-downgrade</code>

## Display environmental information

Sensors help you monitor the environmental components of your system. The information you can display about environmental sensors include their type, name, state, value, and threshold warnings.

## Step

1. To display information about environmental sensors, use the `system node environment sensors show` command.

## Manage access to web services

### Manage access to web services overview

A web service is an application that users can access by using HTTP or HTTPS. The cluster administrator can set up the web protocol engine, configure SSL, enable a web service, and enable users of a role to access a web service.

Beginning with ONTAP 9.6, the following web services are supported:

- Service Processor Infrastructure (`spi`)

This service makes a node's log, core dump, and MIB files available for HTTP or HTTPS access through the cluster management LIF or a node management LIF. The default setting is `enabled`.

Upon a request to access a node's log files or core dump files, the `spi` web service automatically creates a mount point from a node to another node's root volume where the files reside. You do not need to manually create the mount point. `

- ONTAP APIs (`ontapi`)

This service enables you to run ONTAP APIs to execute administrative functions with a remote program. The default setting is `enabled`.

This service might be required for some external management tools. For example, if you use System Manager, you should leave this service enabled.

- Data ONTAP Discovery (`disco`)

This service enables off-box management applications to discover the cluster in the network. The default setting is `enabled`.

- Support Diagnostics (`supdiag`)

This service controls access to a privileged environment on the system to assist problem analysis and resolution. The default setting is `disabled`. You should enable this service only when directed by technical support.

- System Manager (`sysmgr`)

This service controls the availability of System Manager, which is included with ONTAP. The default setting is `enabled`. This service is supported only on the cluster.

- Firmware Baseboard Management Controller (BMC) Update (`FW_BMC`)

This service enables you to download BMC firmware files. The default setting is `enabled`.

- ONTAP Documentation (`docs`)

This service provides access to the ONTAP documentation. The default setting is `enabled`.

- ONTAP RESTful APIs (`docs_api`)

This service provides access to the ONTAP RESTful API documentation. The default setting is `enabled`.

- File Upload and Download (`fud`)

This service offers file upload and download. The default setting is `enabled`.

- ONTAP Messaging (`ontapmsg`)

This service supports a publish and subscribe interface allowing you to subscribe to events. The default setting is `enabled`.

- ONTAP Portal (`portal`)

This service implements the gateway into a virtual server. The default setting is `enabled`.

- ONTAP Restful Interface (`rest`)

This service supports a RESTful interface that is used to remotely manage all elements of the cluster infrastructure. The default setting is `enabled`.

- Security Assertion Markup Language (SAML) Service Provider Support (`saml`)

This service provides resources to support the SAML service provider. The default setting is `enabled`.

- SAML Service Provider (`saml-sp`)

This service offers services such as SP metadata and the assertion consumer service to the service provider. The default setting is `enabled`.

- Configuration Backup Files (`backups`)

This service enables you to download configuration backup files. The default setting is `enabled`.

- ONTAP Security (`security`)

This service supports CSRF token management. The default setting is `enabled`.

Beginning with ONTAP 9.7, the following additional services are supported:

- Configuration Backup Files (`backups`)

This service enables you to download configuration backup files. The default setting is `enabled`.

- ONTAP Security (`security`)

This service supports CSRF token management for enhanced authentication. The default setting is `enabled`.

## Manage the web protocol engine

You can configure the web protocol engine on the cluster to control whether web access is allowed and what SSL versions can be used. You can also display the configuration settings for the web protocol engine.

You can manage the web protocol engine at the cluster level in the following ways:

- You can specify whether remote clients can use HTTP or HTTPS to access web service content by using the `system services web modify` command with the `-external` parameter.
- You can specify whether SSLv3 should be used for secure web access by using the `security config modify` command with the `-supported-protocol` parameter.

By default, SSLv3 is disabled. Transport Layer Security 1.0 (TLSv1.0) is enabled and it can be disabled if needed.

- You can enable Federal Information Processing Standard (FIPS) 140-2 compliance mode for cluster-wide control plane web service interfaces.



By default, FIPS 140-2 compliance mode is disabled.

- **When FIPS 140-2 compliance mode is disabled**

You can enable FIPS 140-2 compliance mode by setting the `is-fips-enabled` parameter to `true` for the `security config modify` command, and then using the `security config show` command to confirm the online status.

- **When FIPS 140-2 compliance mode is enabled**

Both TLSv1 and SSLv3 are disabled and only TLSv1.1 and TLSv1.2 remain enabled. ONTAP prevents you from enabling both TLSv1 and SSLv3 when FIPS 140-2 compliance mode is enabled. If you enable FIPS 140-2 compliance mode and then subsequently disable it, TLSv1 and SSLv3 remain disabled, but either TLSv1.2 or both TLSv1.1 and TLSv1.2 are enabled depending on the previous configuration.

- You can display the configuration of cluster-wide security by using the `system security config show` command.

If the firewall is enabled, the firewall policy for the logical interface (LIF) to be used for web services must be set up to allow HTTP or HTTPS access.

If you use HTTPS for web service access, SSL for the cluster or storage virtual machine (SVM) that offers the web service must also be enabled, and you must provide a digital certificate for the cluster or SVM.

In MetroCluster configurations, the setting changes you make for the web protocol engine on a cluster are not replicated on the partner cluster.

## Commands for managing the web protocol engine

You use the `system services web` commands to manage the web protocol engine. You use the `system services firewall policy create` and `network interface modify` commands to allow web access requests to go through the firewall.



If you want to...	Use this command...
Configure the web protocol engine at the cluster level: <ul style="list-style-type: none"> <li>• Enable or disable the web protocol engine for the cluster</li> <li>• Enable or disable SSLv3 for the cluster</li> <li>• Enable or disable FIPS 140-2 compliance for secure web services (HTTPS)</li> </ul>	<code>system services web modify</code>
Display the configuration of the web protocol engine at the cluster level, determine whether the web protocols are functional throughout the cluster, and display whether FIPS 140-2 compliance is enabled and online	<code>system services web show</code>
Display the configuration of the web protocol engine at the node level and the activity of web service handling for the nodes in the cluster	<code>system services web node show</code>
Create a firewall policy or add HTTP or HTTPS protocol service to an existing firewall policy to allow web access requests to go through firewall	<code>system services firewall policy create</code>  Setting the <code>-service</code> parameter to <code>http</code> or <code>https</code> enables web access requests to go through firewall.
Associate a firewall policy with a LIF	<code>network interface modify</code>  You can use the <code>-firewall-policy</code> parameter to modify the firewall policy of a LIF.

## Configure SAML authentication for web services

### Configure SAML authentication

Beginning with ONTAP 9.3, you can configure Security Assertion Markup Language (SAML) authentication for web services. When SAML authentication is configured and enabled, users are authenticated by an external Identity Provider (IdP) instead of the directory service providers such as Active Directory and LDAP.

### What you'll need

- You must have configured the IdP for SAML authentication.
- You must have the IdP URI.

### About this task

- SAML authentication applies only to the `http` and `ontapi` applications.

The `http` and `ontapi` applications are used by the following web services: Service Processor Infrastructure, ONTAP APIs, or System Manager.

- SAML authentication is applicable only for accessing the admin SVM.

## Steps

1. Create a SAML configuration so that ONTAP can access the IdP metadata:

```
security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name
```

`idp_uri` is the FTP or HTTP address of the IdP host from where the IdP metadata can be downloaded.

`ontap_host_name` is the host name or IP address of the SAML service provider host, which in this case is the ONTAP system. By default, the IP address of the cluster-management LIF is used.

You can optionally provide the ONTAP server certificate information. By default, the ONTAP web server certificate information is used.

```
cluster_12::> security saml-sp create -idp-uri
https://scspr0235321001.gdl.englab.netapp.com/idp/shibboleth -verify
-metadata-server false
```

Warning: This restarts the web server. Any HTTP/S connections that are active

will be disrupted.

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

[Job 179] Job succeeded: Access the SAML SP metadata using the URL:  
https://10.63.56.150/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server domain to ensure that users are the same for different authentication methods. See the "security login show" command for the Data ONTAP user configuration.

The URL to access the ONTAP host metadata is displayed.

2. From the IdP host, configure the IdP with the ONTAP host metadata.

For more information about configuring the IdP, see the IdP documentation.

3. Enable SAML configuration:

```
security saml-sp modify -is-enabled true
```

Any existing user that accesses the `http` or `ontapi` application is automatically configured for SAML authentication.

4. If you want to create users for the `http` or `ontapi` application after SAML is configured, specify SAML as the authentication method for the new users.

- a. Create a login method for new users with SAML authentication:

+

```
security login create -user-or-group-name user_name -application [http |
```

```
ontapi] -authentication-method saml -vserver svm_name
```

```
cluster_12::> security login create -user-or-group-name admin1  
-application http -authentication-method saml -vserver cluster_12
```

b. Verify that the user entry is created:

```
security login show
```

```
cluster_12::> security login show
```

```
Vserver: cluster_12
```

```
Second
```

```
User/Group
```

```
Authentication
```

```
Acct
```

```
Authentication
```

```
Name
```

```
Application
```

```
Method
```

```
Role Name
```

```
Locked
```

```
Method
```

```
-----  
-----  
-----  
-----  
-----
```

admin	console	password	admin	no	none
admin	http	password	admin	no	none
admin	http	saml	admin	-	none
admin	ontapi	password	admin	no	none
admin	ontapi	saml	admin	-	none
admin	service-processor				
		password	admin	no	none
admin	ssh	password	admin	no	none
admin1	http	password	backup	no	none
**admin1	http	saml	backup	-	
none**					

## Related information

[ONTAP 9 commands](#)

### Disable SAML authentication

You can disable SAML authentication when you want to stop authenticating web users by using an external Identity Provider (IdP). When SAML authentication is disabled, the configured directory service providers such as Active Directory and LDAP are used for authentication.

### What you'll need

You must be logged in from the console.

## Steps

1. Disable SAML authentication:

```
security saml-sp modify -is-enabled false
```

2. If you no longer want to use SAML authentication or if you want to modify the IdP, delete the SAML configuration:

```
security saml-sp delete
```

## Troubleshoot issues with SAML configuration

If configuring Security Assertion Markup Language (SAML) authentication fails, you can manually repair each node on which the SAML configuration failed and recover from the failure. During the repair process, the web server is restarted and any active HTTP connections or HTTPS connections are disrupted.

### About this task

When you configure SAML authentication, ONTAP applies SAML configuration on a per-node basis. When you enable SAML authentication, ONTAP automatically tries to repair each node if there are configuration issues. If there are issues with SAML configuration on any node, you can disable SAML authentication and then reenabling SAML authentication. There can be situations when SAML configuration fails to apply on one or more nodes even after you reenabling SAML authentication. You can identify the node on which SAML configuration has failed and then manually repair that node.

## Steps

1. Log in to the advanced privilege level:

```
set -privilege advanced
```

2. Identify the node on which SAML configuration failed:

```
security saml-sp status show -instance
```

```
cluster_12::~*> security saml-sp status show -instance

Node: node1
Update Status: config-success
Database Epoch: 9
Database Transaction Count: 997
Error Text:
SAML Service Provider Enabled: false
ID of SAML Config Job: 179

Node: node2
Update Status: config-failed
Database Epoch: 9
Database Transaction Count: 997
Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
ID of SAML Config Job: 180
2 entries were displayed.
```

### 3. Repair the SAML configuration on the failed node:

**security saml-sp repair -node *node\_name***

```
cluster_12::~*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

The web server is restarted and any active HTTP connections or HTTPS connections are disrupted.

### 4. Verify that SAML is successfully configured on all of the nodes:

**security saml-sp status show -instance**

```
cluster_12::*> security saml-sp status show -instance
```

```

                Node: node1
            Update Status: config-success
        Database Epoch: 9
    Database Transaction Count: 997
        Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                Node: node2
            Update Status: **config-success**
        Database Epoch: 9
    Database Transaction Count: 997
        Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

## Manage web services

### Manage web services overview

You can enable or disable a web service for the cluster or a storage virtual machine (SVM), display the settings for web services, and control whether users of a role can access a web service.

You can manage web services for the cluster or an SVM in the following ways:

- Enabling or disabling a specific web service
- Specifying whether access to a web service is restricted to only encrypted HTTP (SSL)
- Displaying the availability of web services
- Allowing or disallowing users of a role to access a web service
- Displaying the roles that are permitted to access a web service

For a user to access a web service, all of the following conditions must be met:

- The user must be authenticated.

For instance, a web service might prompt for a user name and password. The user's response must match a valid account.

- The user must be set up with the correct access method.

Authentication only succeeds for users with the correct access method for the given web service. For the ONTAP API web service (`ontapi`), users must have the `ontapi` access method. For all other web services, users must have the `http` access method.



You use the `security login` commands to manage users' access methods and authentication methods.

- The web service must be configured to allow the user's access-control role.



You use the `vserver services web access` commands to control a role's access to a web service.

If a firewall is enabled, the firewall policy for the LIF to be used for web services must be set up to allow HTTP or HTTPS.

If you use HTTPS for web service access, SSL for the cluster or SVM that offers the web service must also be enabled, and you must provide a digital certificate for the cluster or SVM.

### Commands for managing web services

You use the `vserver services web` commands to manage the availability of web services for the cluster or a storage virtual machine (SVM). You use the `vserver services web access` commands to control a role's access to a web service.

If you want to...	Use this command...
Configure a web service for the cluster or anSVM: <ul style="list-style-type: none"> <li>• Enable or disable a web service</li> <li>• Specify whether only HTTPS can be used for accessing a web service</li> </ul>	<code>vserver services web modify</code>
Display the configuration and availability of web services for the cluster or anSVM	<code>vserver services web show</code>
Authorize a role to access a web service on the cluster or anSVM	<code>vserver services web access create</code>
Display the roles that are authorized to access web services on the cluster or anSVM	<code>vserver services web access show</code>
Prevent a role from accessing a web service on the cluster or anSVM	<code>vserver services web access delete</code>

### Related information

[ONTAP 9 commands](#)

### Commands for managing mount points on the nodes

The `spi` web service automatically creates a mount point from one node to another node's root volume upon a request to access the node's log files or core files. Although you do not need to manually manage mount points, you can do so by using the `system`

node root-mount commands.

If you want to...	Use this command...
Manually create a mount point from one node to another node's root volume	<code>system node root-mount create</code> Only a single mount point can exist from one node to another.
Display existing mount points on the nodes in the cluster, including the time a mount point was created and its current state	<code>system node root-mount show</code>
Delete a mount point from one node to another node's root volume and force connections to the mount point to close	<code>system node root-mount delete</code>

### Related information

[ONTAP 9 commands](#)

## Manage SSL

The SSL protocol improves the security of web access by using a digital certificate to establish an encrypted connection between a web server and a browser.

You can manage SSL for the cluster or a storage virtual machine (SVM) in the following ways:

- Enabling SSL
- Generating and installing a digital certificate and associating it with the cluster or SVM
- Displaying the SSL configuration to see whether SSL has been enabled, and, if available, the SSL certificate name
- Setting up firewall policies for the cluster or SVM, so that web access requests can go through
- Defining which SSL versions can be used
- Restricting access to only HTTPS requests for a web service

### Commands for managing SSL

You use the `security ssl` commands to manage the SSL protocol for the cluster or a storage virtual machine (SVM).

If you want to...	Use this command...
Enable SSL for the cluster or an SVM, and associate a digital certificate with it	<code>security ssl modify</code>
Display the SSL configuration and certificate name for the cluster or an SVM	<code>security ssl show</code>



## Configure access to web services

Configuring access to web services allows authorized users to use HTTP or HTTPS to access the service content on the cluster or a storage virtual machine (SVM).

### Steps

1. If a firewall is enabled, ensure that HTTP or HTTPS access is set up in the firewall policy for the LIF that will be used for web services:



You can check whether a firewall is enabled by using the `system services firewall show` command.

- a. To verify that HTTP or HTTPS is set up in the firewall policy, use the `system services firewall policy show` command.

You set the `-service` parameter of the `system services firewall policy create` command to `http` or `https` to enable the policy to support web access.

- b. To verify that the firewall policy supporting HTTP or HTTPS is associated with the LIF that provides web services, use the `network interface show` command with the `-firewall-policy` parameter.

You use the `network interface modify` command with the `-firewall-policy` parameter to put the firewall policy into effect for a LIF.

2. To configure the cluster-level web protocol engine and make web service content accessible, use the `system services web modify` command.
3. If you plan to use secure web services (HTTPS), enable SSL and provide digital certificate information for the cluster or SVM by using the `security ssl modify` command.
4. To enable a web service for the cluster or SVM, use the `vserver services web modify` command.

You must repeat this step for each service that you want to enable for the cluster or SVM.

5. To authorize a role to access web services on the cluster or SVM, use the `vserver services web access create` command.

The role that you grant access must already exist. You can display existing roles by using the `security login role show` command or create new roles by using the `security login role create` command.

6. For a role that has been authorized to access a web service, ensure that its users are also configured with the correct access method by checking the output of the `security login show` command.

To access the ONTAP API web service (`ontapi`), a user must be configured with the `ontapi` access method. To access all other web services, a user must be configured with the `http` access method.



You use the `security login create` command to add an access method for a user.

## Troubleshoot web service access problems

Configuration errors cause web service access problems to occur. You can address the errors by ensuring that the LIF, firewall policy, web protocol engine, web services, digital certificates, and user access authorization are all configured correctly.

The following table helps you identify and address web service configuration errors:

This access problem...	Occurs because of this configuration error...	To address the error...
Your web browser returns an unable to connect or failure to establish a connection error when you try to access a web service.	Your LIF might be configured incorrectly.	<p>Ensure that you can ping the LIF that provides the web service.</p> <div>  <p>You use the <code>network ping</code> command to ping a LIF. For information about network configuration, see the <i>Network Management Guide</i>.</p> </div>
	Your firewall might be configured incorrectly.	<p>Ensure that a firewall policy is set up to support HTTP or HTTPS and that the policy is assigned to the LIF that provides the web service.</p> <div>  <p>You use the <code>system services firewall policy</code> commands to manage firewall policies. You use the <code>network interface modify</code> command with the <code>-firewall -policy</code> parameter to associate a policy with a LIF.</p> </div>
	Your web protocol engine might be disabled.	<p>Ensure that the web protocol engine is enabled so that web services are accessible.</p> <div>  <p>You use the <code>system services web</code> commands to manage the web protocol engine for the cluster.</p> </div>

This access problem...	Occurs because of this configuration error...	To address the error...
Your web browser returns a <code>not found</code> error when you try to access a web service.	The web service might be disabled.	<p>Ensure that each web service that you want to allow access to is enabled individually.</p> <div data-bbox="1166 331 1485 562">  <p>You use the <code>vserver services web modify</code> command to enable a web service for access.</p> </div>
The web browser fails to log in to a web service with a user's account name and password.	The user cannot be authenticated, the access method is not correct, or the user is not authorized to access the web service.	<p>Ensure that the user account exists and is configured with the correct access method and authentication method. Also, ensure that the user's role is authorized to access the web service.</p> <div data-bbox="1166 848 1485 1625">  <p>You use the <code>security login</code> commands to manage user accounts and their access methods and authentication methods. Accessing the ONTAP API web service requires the <code>ontapi</code> access method. Accessing all other web services requires the <code>http</code> access method. You use the <code>vserver services web access</code> commands to manage a role's access to a web service.</p> </div>

This access problem...	Occurs because of this configuration error...	To address the error...
<p>You connect to your web service with HTTPS, and your web browser indicates that your connection is interrupted.</p>	<p>You might not have SSL enabled on the cluster or storage virtual machine (SVM) that provides the web service.</p>	<p>Ensure that the cluster or SVM has SSL enabled and that the digital certificate is valid.</p> <div data-bbox="1076 516 1133 569">  </div> <p>You use the <code>security ssl</code> commands to manage SSL configuration for HTTP servers and the <code>security certificate show</code> command to display digital certificate information.</p>
<p>You connect to your web service with HTTPS, and your web browser indicates that the connection is untrusted.</p>	<p>You might be using a self-signed digital certificate.</p>	<p>Ensure that the digital certificate associated with the cluster or SVM is signed by a trusted CA.</p> <div data-bbox="1076 1293 1133 1346">  </div> <p>You use the <code>security certificate generate-csr</code> command to generate a digital certificate signing request and the <code>security certificate install</code> command to install a CA-signed digital certificate. You use the <code>security ssl</code> commands to manage the SSL configuration for the cluster or SVM that provides the web service.</p>

## Verify the identity of remote servers using certificates

### Verify the identity of remote servers using certificates overview

ONTAP supports security certificate features to verify the identity of remote servers.

ONTAP software enables secure connections using these digital certificate features and protocols:

- Online Certificate Status Protocol (OCSP) validates the status of digital certificate requests from ONTAP services using SSL and Transport Layer Security (TLS) connections. This feature is disabled by default.
- A default set of trusted root certificates is included with ONTAP software.
- Key Management Interoperability Protocol (KMIP) certificates enable mutual authentication of a cluster and a KMIP server.

**Verify digital certificates are valid using OCSP**

Beginning with ONTAP 9.2, Online Certificate Status Protocol (OCSP) enables ONTAP applications that use Transport Layer Security (TLS) communications to receive digital certificate status when OCSP is enabled. You can enable or disable OCSP certificate status checks for specific applications at any time. By default, OCSP certificate status checking is disabled.

**What you’ll need**

These commands must be performed at the advanced privilege level.

**About this task**

OCSP supports the following applications:

- AutoSupport
- Event Management System (EMS)
- LDAP over TLS
- Key Management Interoperability Protocol (KMIP)
- Audit Logging
- FabricPool

**Steps**

1. Set the privilege level to advanced: `set -privilege advanced`.
2. To enable or disable OCSP certificate status checks for specific ONTAP applications, use the appropriate command.

If you want OCSP certificate status checks for some applications to be...	Use the command...
Enabled	<code>security config ocsp enable -app app name</code>
Disabled	<code>security config ocsp disable -app app name</code>

The following command enables OCSP support for AutoSupport and EMS.

```
cluster::*> security config ocsd enable -app asup,ems
```

When OCSd is enabled, the application receives one of the following responses:

- Good - the certificate is valid and communication proceeds.
- Revoked - the certificate is permanently deemed as not trustworthy by its issuing Certificate Authority and communication fails to proceed.
- Unknown - the server does not have any status information about the certificate and communication fails to proceed.
- OCSd server information is missing in the certificate - the server acts as if OCSd is disabled and continues with TLS communication, but no status check occurs.
- No response from OCSd server - the application fails to proceed.

3. To enable or disable OCSd certificate status checks for all applications using TLS communications, use the appropriate command.

If you want OCSd certificate status checks for all applications to be...	Use the command...
Enabled	<pre>security config ocsd enable  -app all</pre>
Disabled	<pre>security config ocsd disable  -app all</pre>

When enabled, all applications receive a signed response signifying that the specified certificate is good, revoked, or unknown. In the case of a revoked certificate, the application will fail to proceed. If the application fails to receive a response from the OCSd server or if the server is unreachable, the application will fail to proceed.

4. Use the `security config ocsd show` command to display all the applications that support OCSd and their support status.

```
cluster::*> security config ocsf show
Application                                OCSP Enabled?
-----
autosupport                               false
audit_log                                 false
fabricpool                                false
ems                                         false
kmip                                        false
ldap_ad                                   true
ldap_nis_namemap                           true

7 entries were displayed.
```

## View default certificates for TLS-based applications

Beginning with ONTAP 9.2, ONTAP provides a default set of trusted root certificates for ONTAP applications using Transport Layer Security (TLS).

### What you'll need

The default certificates are installed only on the admin SVM during its creation, or during an upgrade to ONTAP 9.2.

### About this task

The current applications that act as a client and require certificate validation are AutoSupport, EMS, LDAP, Audit Logging, FabricPool, and KMIP.

When certificates expire, an EMS message is invoked that requests the user to delete the certificates. The default certificates can only be deleted at the advanced privilege level.



Deleting the default certificates may result in some ONTAP applications not functioning as expected (for example, AutoSupport and Audit Logging).

### Step

1. You can view the default certificates that are installed on the admin SVM by using the security certificate show command:

```
security certificate show -vserver -type server-ca
```



```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver      Serial Number  Common Name                                     Type
-----
fas2552-2n-abc-3
01           AACertificateServices
server-ca
Certificate Authority: AAA Certificate Services
Expiration Date: Sun Dec 31 18:59:59 2028
```

## Mutually authenticating the cluster and a KMIP server

### Mutually authenticating the cluster and a KMIP server overview

Mutually authenticating the cluster and an external key manager such as a Key Management Interoperability Protocol (KMIP) server enables the key manager to communicate with the cluster by using KMIP over SSL. You do so when an application or certain functionality (for example, the Storage Encryption functionality) requires secure keys to provide secure data access.

### Generate a certificate signing request for the cluster

You can use the `security certificate generate-csr` command to generate a certificate signing request (CSR). After processing your request, the certificate authority (CA) sends you the signed digital certificate.

### What you'll need

You must be a cluster administrator or SVM administrator to perform this task.

### Steps

1. Generate a CSR:

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

For complete command syntax, see the man pages.

The following command creates a CSR with a 2,048-bit private key generated by the SHA256 hashing function for use by the Software group in the IT department of a company whose custom common name is `server1.companyname.com`, located in Sunnyvale, California, USA. The email address of the SVM contact administrator is `web@example.com`. The system displays the CSR and the private key in the output.

```

cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGx1LmNvbTELMakGA1UEBhMCVVMx
CTAHBgNVBAgtADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxtAHBgNVBAStADEPMA0G
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3alwoUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC Power Guide
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgpV+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.

```

2. Copy the certificate request from the CSR output, and then send it in electronic form (such as email) to a trusted third-party CA for signing.

After processing your request, the CA sends you the signed digital certificate. You should keep a copy of the private key and the CA-signed digital certificate.

#### Install a CA-signed server certificate for the cluster

To enable an SSL server to authenticate the cluster or storage virtual machine (SVM) as an SSL client, you install a digital certificate with the client type on the cluster or SVM. Then you provide the client-ca certificate to the SSL server administrator for installation on the server.

#### What you'll need

You must have already installed the root certificate of the SSL server on the cluster or SVM with the `server-ca` certificate type.

#### Steps

1. To use a self-signed digital certificate for client authentication, use the `security certificate create`

command with the `type client` parameter.

2. To use a CA-signed digital certificate for client authentication, complete the following steps:
  - a. Generate a digital certificate signing request (CSR) by using the `security certificate generate-csr` command.

ONTAP displays the CSR output, which includes a certificate request and private key, and reminds you to copy the output to a file for future reference.

- b. Send the certificate request from the CSR output in an electronic form (such as email) to a trusted CA for signing.

You should keep a copy of the private key and the CA-signed certificate for future reference.

After processing your request, the CA sends you the signed digital certificate.

- c. Install the CA-signed certificate by using the `security certificate install` command with the `-type client` parameter.
  - d. Enter the certificate and the private key when you are prompted, and then press **Enter**.
  - e. Enter any additional root or intermediate certificates when you are prompted, and then press **Enter**.

You install an intermediate certificate on the cluster or SVM if a certificate chain that begins at the trusted root CA, and ends with the SSL certificate issued to you, is missing the intermediate certificates. An intermediate certificate is a subordinate certificate issued by the trusted root specifically to issue end-entity server certificates. The result is a certificate chain that begins at the trusted root CA, goes through the intermediate certificate, and ends with the SSL certificate issued to you.

3. Provide the `client-ca` certificate of the cluster or SVM to the administrator of the SSL server for installation on the server.

The `security certificate show` command with the `-instance` and `-type client-ca` parameters displays the `client-ca` certificate information.

#### Install a CA-signed client certificate for the KMIP server

The certificate subtype of Key Management Interoperability Protocol (KMIP) (the `-subtype kmip-cert` parameter), along with the `client` and `server-ca` types, specifies that the certificate is used for mutually authenticating the cluster and an external key manager, such as a KMIP server.

#### About this task

Install a KMIP certificate to authenticate a KMIP server as an SSL server to the cluster.

#### Steps

1. Use the `security certificate install` command with the `-type server-ca` and `-subtype kmip-cert` parameters to install a KMIP certificate for the KMIP server.
2. When you are prompted, enter the certificate, and then press Enter.

ONTAP reminds you to keep a copy of the certificate for future reference.

```
cluster1::> security certificate install -type server-ca -subtype kmip-  
cert  
-vserver cluster1  
  
Please enter Certificate: Press <Enter> when done  
-----BEGIN CERTIFICATE-----  
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG  
2JhucwNhkcV8sEVAbkSdjbCxlRhLQ2pRdKkkirWmnWXbj9T/UWZyB2oK0z5XqcJ  
2HUw19JlYDln1khVdWk/kfVIC0dpImmClr7JyDiGSnoscx1IaU5rfGW/D/xwzoiQ  
...  
-----END CERTIFICATE-----  
  
You should keep a copy of the CA-signed digital certificate for future  
reference.  
  
cluster1::>
```

## Disk and aggregate management with the CLI

### Disks and aggregates overview

You can manage ONTAP physical storage using the CLI. You can create, expand, and manage aggregates, work with Flash Pool aggregates, manage disks, and manage RAID policies.

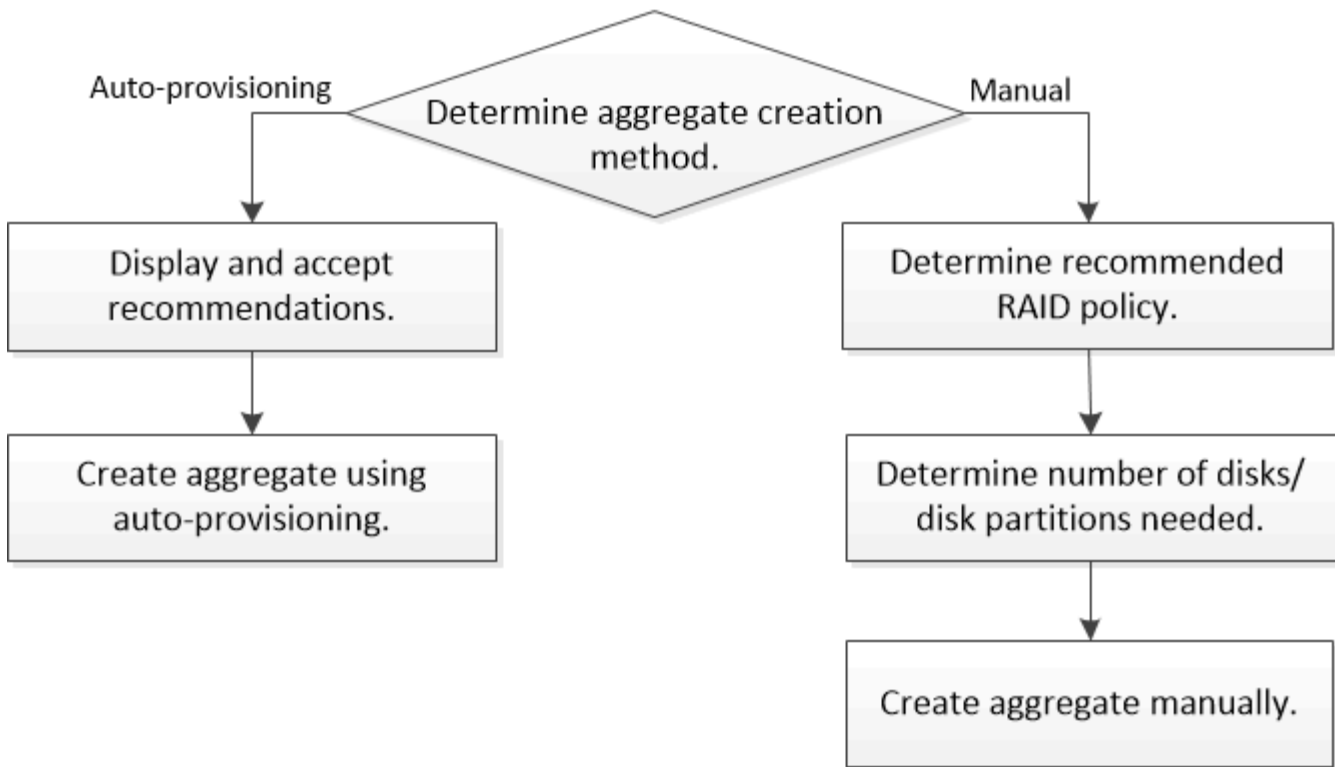
You perform these tasks if the following are true:

- You want to use the command-line interface (CLI), not System Manager or an automated scripting tool.
- You want to use best practices, not explore every available option.
- You have a MetroCluster configuration and you are following the procedures in the [MetroCluster](#) documentation for initial configuration and guidelines for aggregates and disk management.

### Aggregate creation

#### Aggregate creation workflow

Creating aggregates provides storage to volumes on your system. Beginning with ONTAP 9.2, you can let ONTAP recommend aggregate configurations for your system (auto-provision). If the auto-provision method is not available or appropriate in your environment, you can configure aggregates manually.



### Decide which aggregate creation method to use

Although aggregate creation with auto-provision is a best practice in ONTAP 9.2 and later, you must determine whether it is supported in your environment. If it is not, you must make decisions about RAID policy and disk configuration, and then create the aggregates manually.

When you create an aggregate using the `storage aggregate auto-provision` command, ONTAP analyzes available spare disks in the cluster and generates a recommendation about how spare disks should be used to create aggregates according to best practices. ONTAP displays the summary of recommended aggregates including their names and usable size, and then prompts you to decide whether the aggregates should be created as recommended.

In many cases, the recommended aggregate layout in the auto-provision display will be optimal for your environment. However, if your cluster is running ONTAP 9.1 or earlier, or your environment includes the following configurations, you must use the manual aggregate configuration method.

- Aggregates using third-party array LUNs
- Virtual disks with Cloud Volumes ONTAP or ONTAP Select
- MetroCluster
- SyncMirror
- MSATA disks
- FlashPool aggregates
- Multiple disk types or sizes are connected to the node

In addition, if any of the following disk conditions are present, they must be addressed before using the auto-provision method:

- Missing disks
- Fluctuation in spare disk numbers
- Unassigned disks
- Non-zeroed spares
- Disks undergoing maintenance testing

The `storage aggregate auto-provision man` page contains more information about these requirements.

## Related information

[ONTAP 9 commands](#)

## Create aggregates with auto-provision

If the auto-provision method is appropriate in your environment, you run the `storage aggregate auto-provision` to generate aggregate layout recommendations. You can then create aggregates after reviewing and approving ONTAP recommendations.

### What you'll need

ONTAP 9.2 or later must be running on your cluster.

### About this task

The default summary generated with the `storage aggregate auto-provision` command lists the recommended aggregates to be created, including names and usable size. You can view the list and determine whether you want to create the recommended aggregates when prompted.

You can also display a detailed summary by using the `-verbose` option, which displays the following reports:

- Per node summary of new aggregates to create, discovered spares, and remaining spare disks and partitions after aggregate creation
- New data aggregates to create with counts of disks and partitions to be used
- RAID group layout showing how spare disks and partitions will be used in new data aggregates to be created
- Details about spare disks and partitions remaining after aggregate creation

If you are familiar with the auto-provision method and your environment is correctly prepared, you can use the `-skip-confirmation` option to create the recommended aggregate without display and confirmation. The `storage aggregate auto-provision` command is not affected by the CLI session `-confirmations` setting.

The `storage aggregate auto-provision man` page contains more information about the aggregate layout recommendations.

## Steps

1. Run the `storage aggregate auto-provision` command with the desired display options.
  - no options: Display standard summary
  - `-verbose` option: Display detailed summary

◦ `-skip-confirmation` option: Create recommended aggregates without display or confirmation

2. After reviewing the display of recommended aggregates, respond to the prompt to create the recommended aggregates.

```
Do you want to create recommended aggregates? {y|n}:y
```

```
Info: Creating node1_SSD_1 ...
```

```
      Creating node2_SSD_1 ...
```

## Related information

[ONTAP 9 commands](#)

## Default RAID policies for aggregates

Either RAID-DP or RAID-TEC is the default RAID policy for all new aggregates. The RAID policy determines the parity protection you have in the event of a disk failure.

RAID-DP provides double-parity protection in the event of a single or double disk failure. RAID-DP is the default RAID policy for the following aggregate types:

- All flash aggregates
- Flash Pool aggregates
- Performance hard disk drive (HDD) aggregates

A new RAID policy called RAID-TEC is available. RAID-TEC is supported on all disk types and all platforms, including AFF. Aggregates that contain larger disks have a higher possibility of concurrent disk failures. RAID-TEC helps to mitigate this risk by providing triple-parity protection so that your data can survive up to three simultaneous disk failures. RAID-TEC is the default RAID policy for capacity HDD aggregates with disks that are 6 TB or larger.

## Determine the number of disks or disk partitions required for an aggregate

You must have enough disks or disk partitions in your aggregate to meet system and business requirements. You should also have the recommended number of hot spare disks or hot spare disk partitions to minimize the potential of data loss.

Root-data partitioning is enabled by default on certain configurations. Systems with root-data partitioning enabled use disk partitions to create aggregates. Systems that do not have root-data partitioning enabled use unpartitioned disks.

You must have enough disks or disk partitions to meet the minimum number required for your RAID policy and enough to meet your minimum capacity requirements.



In ONTAP, the usable space of the drive is less than the physical capacity of the drive. You can find the usable space of a specific drive and the minimum number of disks or disk partitions required for each RAID policy in *Hardware Universe*. You can also use the `storage aggregate show-spare-disks` command to find the usable space of a specific disk.

In addition to the number of disks or disk partitions necessary to create your RAID group and meet your capacity requirements, you should also have the minimum number of hot spare disks or hot spare disk partitions recommended for your aggregate:

- For all flash aggregates, you should have a minimum of one hot spare disk or disk partition.



The AFF C190 defaults to no spare drive. This exception is fully supported.

- For non-flash homogenous aggregates, you should have a minimum of two hot spare disks or disk partitions.
- For SSD storage pools, you should have a minimum of one hot spare disk for each HA pair.
- For Flash Pool aggregates, you should have a minimum of two spare disks for each HA pair. You can find more information on the supported RAID policies for Flash Pool aggregates in the [Hardware Universe](#).
- To support the use of the Maintenance Center and to avoid issues caused by multiple concurrent disk failures, you should have a minimum of four hot spares in multi-disk carriers.

### Related information

[NetApp Hardware Universe](#)

[NetApp Technical Report 3838: Storage Subsystem Configuration Guide](#)

### Create aggregates manually

Before you create aggregates manually, you should review disk configuration options and simulate creation. Then you can issue the `storage aggregate create` and verify the results.

### What you'll need

You must have determined the number of disks and the number of hot spare disks you need in the aggregate.

### About this task

If root-data-data partitioning is enabled and you have 24 solid state drives (SSDs) or fewer in your configuration, it is recommended that your data partitions be assigned to different nodes.

The procedure for creating aggregates on systems with root-data partitioning and root-data-data partitioning enabled is the same as the procedure for creating aggregates on systems using unpartitioned disks. If root-data partitioning is enabled on your system, you should use the number of disk partitions for the `-diskcount` option. For root-data-data partitioning, the `-diskcount` option specifies the count of disks to use.



When creating multiple aggregates for use with FlexGroups, aggregates should be as close in size as possible.

The `storage aggregate create man` page contains more information about aggregate creation options and requirements.

### Steps

1. View the list of spare disk partitions to verify that you have enough to create your aggregate:

```
storage aggregate show-spare-disks -original-owner node_name
```



Data partitions are displayed under `Local Data Usable`. A root partition cannot be used as a spare.

2. Simulate the creation of the aggregate:

```
storage aggregate create -aggregate aggregate_name -node node_name -raidtype  
raid_dp -diskcount number_of_disks_or_partitions -simulate true
```

3. If any warnings are displayed from the simulated command, adjust the command and repeat the simulation.

4. Create the aggregate:

```
storage aggregate create -aggregate aggr_name -node node_name -raidtype  
raid_dp -diskcount number_of_disks_or_partitions
```

5. Display the aggregate to verify that it was created:

```
storage aggregate show-status aggregate_name
```

### Related information

[ONTAP 9 commands](#)

## Aggregate expansion

### Aggregate expansion workflow

Expanding an aggregate involves identifying the aggregate to expand, determining how much new storage is needed, installing new disks, assigning disk ownership, and creating new a RAID group if needed.



### Add drives to a node or shelf

You add drives to a node or shelf to increase the number of hot spares or to add space to an aggregate.

#### About this task

The drive you want to add must be supported by your platform.

[NetApp Hardware Universe](#)

The minimum number of drives you should add in a single procedure is six. Adding a single drive might reduce performance.

#### Steps

1. Check the NetApp Support Site for newer drive and shelf firmware and Disk Qualification Package files.

If your node or shelf does not have the latest versions, update them before installing the new drive.

Drive firmware is automatically updated (nondisruptively) on new drives that do not have current firmware versions.

2. Properly ground yourself.
3. Gently remove the bezel from the front of the platform.
4. Identify the correct slot for the new drive.



The correct slots for adding drives vary depending on the platform model and ONTAP version. In some cases you need to add drives to specific slots in sequence. For example, in an AFF A800 you add the drives at specific intervals leaving clusters of empty slots. Whereas, in an AFF A220 you add new drives to the next empty slots running from the outside towards the middle of the shelf.

See the [NetApp Hardware Universe](#) to identify the correct slots for your configuration.

5. Insert the new drive:
  - a. With the cam handle in the open position, use both hands to insert the new drive.
  - b. Push until the drive stops.
  - c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place. Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.
6. Verify that the drive's activity LED (green) is illuminated.

When the drive's activity LED is solid, it means that the drive has power. When the drive's activity LED is blinking, it means that the drive has power and I/O is in progress. If the drive firmware is automatically updating, the LED blinks.

7. To add another drive, repeat Steps 4 through 6.

The new drives are not recognized until they are assigned to a node. You can assign the new drives manually, or you can wait for ONTAP to automatically assign the new drives if your node follows the rules for drive autoassignment.

8. After the new drives have all been recognized, verify their addition and their ownership information:

```
storage aggregate show-spare-disks
```

You should see the new drives, owned by the correct node.

9. Zero the newly added drives:

```
storage disk zerospares
```

Drives that have been used previously in an ONTAP aggregate must be zeroed before they can be added to another aggregate. Zeroing the drives now can prevent delays in case you need to quickly increase the size of an aggregate. The drive zeroing command runs in the background and can take hours to complete, depending on the size of the non-zeroed drives in the node.

## Results

The new drives are ready to be added to an aggregate, placed onto the list of hot spares, or you can create a

new aggregate.

## Manually assigning disk ownership

Disks must be owned by a node before they can be used in an aggregate. If your cluster is not configured to use automatic disk ownership assignment, you must assign ownership manually. You cannot reassign ownership of a disk that is in use in an aggregate.

### Steps

1. Display all unowned disks:

```
storage disk show -container-type unassigned
```

2. Assign each disk:

```
storage disk assign -disk disk_name -owner owner_name
```

You can use the wildcard character to assign more than one disk at once. If you are reassigning a spare disk that is already owned by a different node, you must use the `-force` option

## Fast zeroing of drives

Beginning with ONTAP 9.4, you can automatically and quickly zero drives (both SSDs and HDDs) before provisioning without experiencing long wait times..

For systems that are freshly installed with ONTAP 9.4 or later or systems that are reinitialized with ONTAP 9.4 or later, drive zeroing takes place automatically and is complete in seconds.

If you need to manually zero a drive, you can use one of the following methods:

- Use the `storage disk zerospares` command.

Admin privileges are required to use this command.

- From the boot menu select one of the following options:
  - (4) Clean configuration and initialize all disks
  - (9a) Unpartition all disks and remove their ownership information
  - (9b) Clean configuration and initialize node with whole disks

The fast zeroing enhancement does not support systems upgraded from a release earlier than ONTAP 9.4.

If any node on the cluster contains an aggregate with fast-zeroed drives, then you cannot revert the cluster to ONTAP 9.2 or earlier.

## Expand aggregates

You can add disks to an aggregate so that it can provide more storage to its associated volumes. The procedure for adding partitioned disks to an aggregate is similar to the procedure for adding unpartitioned disks.

## What you'll need

You must know what the RAID group size is for the aggregate you are adding the storage to.

## About this task

When you expand an aggregate, you should be aware of whether you are adding partition or unpartitioned disks to the aggregate. When you add unpartitioned drives to an existing aggregate, the size of the existing RAID groups is inherited by the new RAID group, which can affect the number of parity disks required. If an unpartitioned disk is added to a RAID group composed of partitioned disks, the new disk is partitioned, leaving an unused spare partition.

When you provision partitions, you must ensure that you do not leave the node without a drive with both partitions as spare. If you do, and the node experiences a controller disruption, valuable information about the problem (the core file) might not be available to provide to the technical support.



Do not use the `disklist` command to expand your aggregates. This could cause partition misalignment.

## Steps

1. Show the available spare storage on the system that owns the aggregate:

```
storage aggregate show-spare-disks -original-owner node_name
```

You can use the `-is-disk-shared` parameter to show only partitioned drives or only unpartitioned drives.

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2 -is
-disk-shared true
```

Original Owner: cl1-s2

Pool0

Shared HDD Spares

				Local	
Local				Data	
Root Physical					
Disk			Type	RPM	Checksum Usable
Usable	Size	Status			
-----					
1.0.1			BSAS	7200	block 753.8GB
73.89GB	828.0GB	zeroed			
1.0.2			BSAS	7200	block 753.8GB
0B	828.0GB	zeroed			
1.0.3			BSAS	7200	block 753.8GB
0B	828.0GB	zeroed			
1.0.4			BSAS	7200	block 753.8GB
0B	828.0GB	zeroed			
1.0.8			BSAS	7200	block 753.8GB
0B	828.0GB	zeroed			
1.0.9			BSAS	7200	block 753.8GB
0B	828.0GB	zeroed			
1.0.10			BSAS	7200	block 0B
73.89GB	828.0GB	zeroed			
2 entries were displayed.					

## 2. Show the current RAID groups for the aggregate:

```
storage aggregate show-status aggr_name
```



`-checksumstyle` parameter.

If you are adding disks to a Flash Pool aggregate, you must use the `-disktype` parameter to specify the disk type.

You can use the `-disksize` parameter to specify a size of the disks to add. Only disks with approximately the specified size are selected for addition to the aggregate.

```
cl1-s2::> storage aggregate add-disks -aggregate data_1 -raidgroup new  
-diskcount 5
```

5. Verify that the storage was added successfully:

```
storage aggregate show-status -aggregate aggr_name
```



```

cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
Aggregate: data_1 (online, raid_dp) (block checksums)
Plex: /data_1/plex0 (online, normal, active, pool0)
RAID Group /data_1/plex0/rg0 (normal, block checksums)

Physical
Position Disk                               Pool Type    RPM    Size
Size Status
-----
-----
shared    1.0.10                               0    BSAS    7200    753.8GB
828.0GB (normal)
shared    1.0.5                               0    BSAS    7200    753.8GB
828.0GB (normal)
shared    1.0.6                               0    BSAS    7200    753.8GB
828.0GB (normal)
shared    1.0.11                              0    BSAS    7200    753.8GB
828.0GB (normal)
shared    1.0.0                               0    BSAS    7200    753.8GB
828.0GB (normal)
shared    1.0.2                               0    BSAS    7200    753.8GB
828.0GB (normal)
shared    1.0.3                               0    BSAS    7200    753.8GB
828.0GB (normal)
shared    1.0.4                               0    BSAS    7200    753.8GB
828.0GB (normal)
shared    1.0.8                               0    BSAS    7200    753.8GB
828.0GB (normal)
shared    1.0.9                               0    BSAS    7200    753.8GB
828.0GB (normal)
10 entries were displayed.

```

6. Verify that the node still has at least one drive with both the root partition and the data partition as spare:

```
storage aggregate show-spare-disks -original-owner node_name
```

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2 -is
-disk-shared true
```

Original Owner: cl1-s2

Pool0

Shared HDD Spares

			Local			
					Data	
Root Physical						
Disk	Type	RPM	Checksum	Usable		
Usable	Size	Status				
-----						
1.0.1	BSAS	7200	block	753.8GB		
73.89GB	828.0GB	zeroed				
1.0.10	BSAS	7200	block	0B		
73.89GB	828.0GB	zeroed				
2 entries were displayed.						

## Managing aggregates

### RAID protection levels for disks

ONTAP supports three levels of RAID protection for aggregates. Your level of RAID protection determines the number of parity disks available for data recovery in the event of disk failures.

With RAID protection, if there is a data disk failure in a RAID group, ONTAP can replace the failed disk with a spare disk and use parity data to reconstruct the data of the failed disk.

- RAID4

With RAID4 protection, ONTAP can use one spare disk to replace and reconstruct the data from one failed disk within the RAID group.

- RAID-DP

With RAID-DP protection, ONTAP can use up to two spare disks to replace and reconstruct the data from up to two simultaneously failed disks within the RAID group.

- RAID-TEC

With RAID-TEC protection, ONTAP can use up to three spare disks to replace and reconstruct the data from up to three simultaneously failed disks within the RAID group.

### Related information

[NetApp Technical Report 3437: Storage Subsystem Resiliency Guide](#)

## Determine the number of disks or disk partitions required for an aggregate

You must have enough disks or disk partitions in your aggregate to meet system and business requirements. You should also have the recommended number of hot spare disks or hot spare disk partitions to minimize the potential of data loss.

Root-data partitioning is enabled by default on certain configurations. Systems with root-data partitioning enabled use disk partitions to create aggregates. Systems that do not have root-data partitioning enabled use unpartitioned disks.

You must have enough disks or disk partitions to meet the minimum number required for your RAID policy and enough to meet your minimum capacity requirements.



In ONTAP, the usable space of the drive is less than the physical capacity of the drive. You can find the usable space of a specific drive and the minimum number of disks or disk partitions required for each RAID policy in *Hardware Universe*. You can also use the `storage aggregate show-spare-disks` command to find the usable space of a specific disk.

In addition to the number of disks or disk partitions necessary to create your RAID group and meet your capacity requirements, you should also have the minimum number of hot spare disks or hot spare disk partitions recommended for your aggregate:

- For all flash aggregates, you should have a minimum of one hot spare disk or disk partition.



The AFF C190 defaults to no spare drive. This exception is fully supported.

- For non-flash homogenous aggregates, you should have a minimum of two hot spare disks or disk partitions.
- For SSD storage pools, you should have a minimum of one hot spare disk for each HA pair.
- For Flash Pool aggregates, you should have a minimum of two spare disks for each HA pair. You can find more information on the supported RAID policies for Flash Pool aggregates in the [Hardware Universe](#).
- To support the use of the Maintenance Center and to avoid issues caused by multiple concurrent disk failures, you should have a minimum of four hot spares in multi-disk carriers.

### Related information

[NetApp Hardware Universe](#)

[NetApp Technical Report 3838: Storage Subsystem Configuration Guide](#)

### Correct misaligned spare partitions

When you add partitioned disks to an aggregate, you must leave a disk with both the root and data partition available as spare for every node. If you do not and your node experiences a disruption, ONTAP cannot dump the core to the spare data partition.

### What you'll need

You must have both a spare data partition and a spare root partition on the same type of disk owned by the same node.

### Steps

1. Display the spare partitions for the node:

```
storage aggregate show-spare-disks -original-owner node_name
```

Note which disk has a spare data partition (spare\_data) and which disk has a spare root partition (spare\_root). The spare partition will show a non-zero value under the Local Data Usable or Local Root Usable column.

2. Replace the disk with a spare data partition with the disk with the spare root partition:

```
storage disk replace -disk spare_data -replacement spare_root -action start
```

You can copy the data in either direction; however, copying the root partition takes less time to complete.

3. Monitor the progress of the disk replacement:

```
storage aggregate show-status -aggregate aggr_name
```

4. After the replacement operation is complete, display the spares again to confirm that you have a full spare disk:

```
storage aggregate show-spare-disks -original-owner node_name
```

You should see a spare disk with usable space under both Local Data Usable and Local Root Usable.

### Example

You display your spare partitions for node c1-01 and see that your spare partitions are not aligned:

```
c1::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
Pool0
  Shared HDD Spares
```

Physical Disk Size	Type	RPM	Checksum	Local Data Usable	Local Root Usable
1.0.1 828.0GB	BSAS	7200	block	753.8GB	0B
1.0.10 828.0GB	BSAS	7200	block	0B	73.89GB

You start the disk replacement job:

```
c1::> storage disk replace -disk 1.0.1 -replacement 1.0.10 -action start
```

While you are waiting for the replacement operation to finish, you display the progress of the operation:

```
c1::> storage aggregate show-status -aggregate aggr0_1

Owner Node: c1-01
Aggregate: aggr0_1 (online, raid_dp) (block checksums)
Plex: /aggr0_1/plex0 (online, normal, active, pool0)
RAID Group /aggr0_1/plex0/rg0 (normal, block checksums)

Physical
Size Status
-----
shared 1.0.1 828.0GB (replacing, copy in progress)
shared 1.0.10 828.0GB (copy 63% completed)
shared 1.0.0 828.0GB (normal)
shared 1.0.11 828.0GB (normal)
shared 1.0.6 828.0GB (normal)
shared 1.0.5 828.0GB (normal)

Pool Type RPM Usable Size
-----
0 BSAS 7200 73.89GB
0 BSAS 7200 73.89GB
0 BSAS 7200 73.89GB
0 BSAS 7200 73.89GB
0 BSAS 7200 73.89GB
0 BSAS 7200 73.89GB
```

After the replacement operation is complete, you confirm that you have a full spare disk:

```
ie2220::> storage aggregate show-spare-disks -original-owner c1-01
```

Original Owner: c1-01

Pool0

Shared HDD Spares

Physical Disk Size	Type	RPM	Checksum	Local Data Usable	Local Root Usable
1.0.1 828.0GB	BSAS	7200	block	753.8GB	73.89GB

### Determine drive and RAID group information for an aggregate

Some aggregate administration tasks require that you know what types of drives compose the aggregate, their size, checksum, and status, whether they are shared with other aggregates, and the size and composition of the RAID groups.

#### Step

1. Show the drives for the aggregate, by RAID group:

```
storage aggregate show-status aggr_name
```

The drives are displayed for each RAID group in the aggregate.

You can see the RAID type of the drive (data, parity, dparity) in the `Position` column. If the `Position` column displays `shared`, then the drive is shared: if it is an HDD, it is a partitioned disk; if it is an SSD, it is part of a storage pool.

### Example: A Flash Pool aggregate using an SSD storage pool and data partitions

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)
Usable
Physical
Position Disk                               Pool Type    RPM    Size
Size Status
-----
shared 2.0.1                                0 SAS      10000 472.9GB
547.1GB (normal)
shared 2.0.3                                0 SAS      10000 472.9GB
547.1GB (normal)
shared 2.0.5                                0 SAS      10000 472.9GB
547.1GB (normal)
shared 2.0.7                                0 SAS      10000 472.9GB
547.1GB (normal)
shared 2.0.9                                0 SAS      10000 472.9GB
547.1GB (normal)
shared 2.0.11                               0 SAS      10000 472.9GB
547.1GB (normal)

RAID Group /nodeA_flashpool_1/plex0/rg1 (normal, block checksums,
raid4) (Storage Pool: SmallSP)
Usable
Physical
Position Disk                               Pool Type    RPM    Size
Size Status
-----
shared 2.0.13                               0 SSD        - 186.2GB
745.2GB (normal)
shared 2.0.12                               0 SSD        - 186.2GB
745.2GB (normal)
8 entries were displayed.
```

### Relocate aggregate ownership within an HA pair

#### Relocate aggregate ownership

You can change the ownership of aggregates among the nodes in an HA pair without

interrupting service from the aggregates.

Both nodes in an HA pair are physically connected to each other's disks or array LUNs. Each disk or array LUN is owned by one of the nodes. Although ownership of disks temporarily changes when a takeover occurs, the aggregate relocation operations either permanently (for example, if done for load balancing) or temporarily (for example, if done as part of takeover) change the ownership of all disks or array LUNs within an aggregate from one node to the other. The ownership changes without any data-copy processes or physical movement of the disks or array LUNs.

### About this task

- Because volume count limits are validated programmatically during aggregate relocation operations, it is not necessary to check for this manually.

If the volume count exceeds the supported limit, the aggregate relocation operation fails with a relevant error message.

- You should not initiate aggregate relocation when system-level operations are in progress on either the source or the destination node; likewise, you should not start these operations during the aggregate relocation.

These operations can include the following:

- Takeover
- Giveback
- Shutdown
- Another aggregate relocation operation
- Disk ownership changes
- Aggregate or volume configuration operations
- Storage controller replacement
- ONTAP upgrade
- ONTAP revert
- If you have a MetroCluster configuration, you should not initiate aggregate relocation while disaster recovery operations (*switchover*, *healing*, or *switchback*) are in progress.
- If you have a MetroCluster configuration and initiate aggregate relocation on a switched-over aggregate, the operation might fail because it exceeds the DR partner's volume limit count.
- You should not initiate aggregate relocation on aggregates that are corrupt or undergoing maintenance.
- Before initiating the aggregate relocation, you should save any core dumps on the source and destination nodes.

### Steps

1. View the aggregates on the node to confirm which aggregates to move and ensure they are online and in good condition:

```
storage aggregate show -node source-node
```

The following command shows six aggregates on the four nodes in the cluster. All aggregates are online. Node1 and Node3 form an HA pair and Node2 and Node4 form an HA pair.



```
cluster::> storage aggregate show
```

Aggregate	Size	Available	Used%	State	#Vols	Nodes	RAID	Status
aggr_0	239.0GB	11.13GB	95%	online	1	node1	raid_dp,	normal
aggr_1	239.0GB	11.13GB	95%	online	1	node1	raid_dp,	normal
aggr_2	239.0GB	11.13GB	95%	online	1	node2	raid_dp,	normal
aggr_3	239.0GB	11.13GB	95%	online	1	node2	raid_dp,	normal
aggr_4	239.0GB	238.9GB	0%	online	5	node3	raid_dp,	normal
aggr_5	239.0GB	239.0GB	0%	online	4	node4	raid_dp,	normal

6 entries were displayed.

## 2. Issue the command to start the aggregate relocation:

```
storage aggregate relocation start -aggregate-list aggregate-1, aggregate-2...
-node source-node -destination destination-node
```

The following command moves the aggregates `aggr_1` and `aggr_2` from Node1 to Node3. Node3 is Node1's HA partner. The aggregates can be moved only within the HA pair.

```
cluster::> storage aggregate relocation start -aggregate-list aggr_1,
aggr_2 -node node1 -destination node3
Run the storage aggregate relocation show command to check relocation
status.
node1::storage aggregate>
```

## 3. Monitor the progress of the aggregate relocation with the `storage aggregate relocation show` command:

```
storage aggregate relocation show -node source-node
```

The following command shows the progress of the aggregates that are being moved to Node3:

```
cluster::> storage aggregate relocation show -node node1
Source Aggregate      Destination      Relocation Status
-----
node1
      aggr_1         node3           In progress, module: wafl
      aggr_2         node3           Not attempted yet
2 entries were displayed.
node1::storage aggregate>
```

When the relocation is complete, the output of this command shows each aggregate with a relocation status of Done.

### Commands for aggregate relocation

There are specific ONTAP commands for relocating aggregate ownership within an HA pair.

If you want to...	Use this command...
Start the aggregate relocation process	<code>storage aggregate relocation start</code>
Monitor the aggregate relocation process	<code>storage aggregate relocation show</code>

### Related information

[ONTAP 9 commands](#)

## Assigning aggregates to SVMs

If you assign one or more aggregates to a storage virtual machine (SVM, formerly known as Vserver), then you can use only those aggregates to contain volumes for that SVM. Assigning aggregates to your SVMs is particularly important in a multi-tenancy environment.

### What you'll need

The SVM and the aggregates you want to assign to that SVM must already exist.

### About this task

Assigning aggregates to your SVMs helps you keep your SVMs isolated from each other; this is especially important in a multi-tenancy environment..

### Steps

1. Check the list of aggregates already assigned to the SVM:

```
vserver show -fields aggr-list
```

The aggregates currently assigned to the SVM are displayed. If there are no aggregates assigned, "-" is displayed.

2. Add or remove assigned aggregates, depending on your requirements:

If you want to...	Use this command...
Assign additional aggregates	<code>vserver add-aggregates</code>
Unassign aggregates	<code>vserver remove-aggregates</code>

The listed aggregates are assigned to or removed from the SVM. If the SVM already has volumes that use an aggregate that is not assigned to the SVM, a warning message is displayed, but the command is completed successfully. Any aggregates that were already assigned to the SVM and that were not named in the command are unaffected.

### Example

In the following example, the aggregates `aggr1` and `aggr2` are assigned to SVM `svm1`:

```
vserver add-aggregates -vserver svm1 -aggregates aggr1,aggr2
```

### Determine space usage in an aggregate

You can view space usage by all volumes in one or more aggregates with the `aggregate show-space` command. This helps you see which volumes are consuming the most space in their containing aggregates so that you can take actions to free more space.

The used space in an aggregate is directly affected by the space used in the FlexVol volumes it contains. Measures that you take to increase space in a volume also affect space in the aggregate.

The following rows are included in the `aggregate show-space` command output:

- Volume Footprints

The total of all volume footprints within the aggregate. It includes all of the space that is used or reserved by all data and metadata of all volumes in the containing aggregate.

- Aggregate Metadata

The total file system metadata required by the aggregate, such as allocation bitmaps and inode files.

- Snapshot Reserve

The amount of space reserved for aggregate Snapshot copies, based on volume size. It is considered used space and is not available to volume or aggregate data or metadata.

- Snapshot Reserve Unusable

The amount of space originally allocated for aggregate Snapshot reserve that is unavailable for aggregate Snapshot copies because it is being used by volumes associated with the aggregate. Can occur only for aggregates with a non-zero aggregate Snapshot reserve.

- Total Used

The sum of all space used or reserved in the aggregate by volumes, metadata, or Snapshot copies.

- **Total Physical Used**

The amount of space being used for data now (rather than being reserved for future use). Includes space used by aggregate Snapshot copies.

The following example shows the `aggregate show-space` command output for an aggregate whose Snapshot reserve is 5%. If the Snapshot reserve was 0, the row would not be displayed.

```
cluster1::> storage aggregate show-space
```

Aggregate : wqa\_gx106\_aggr1

Feature	Used	Used%
-----	-----	-----
Volume Footprints	101.0MB	0%
Aggregate Metadata	300KB	0%
Snapshot Reserve	5.98GB	5%
Total Used	6.07GB	5%
Total Physical Used	34.82KB	0%

## Determine which volumes reside on an aggregate

You might need to determine which volumes reside on an aggregate before performing operations on the aggregate, such as relocating it or taking it offline.

### Steps

1. To display the volumes that reside on an aggregate, enter

```
volume show -aggregate aggregate_name
```

All volumes that reside on the specified aggregate are displayed.

## How you can determine and control a volume's space usage in the aggregate

You can determine which FlexVol volumes are using the most space in the aggregate and specifically which features within the volume. The `volume show-footprint` command provides information about a volume's footprint, or its space usage within the containing aggregate.

The `volume show-footprint` command shows details about the space usage of each volume in an aggregate, including offline volumes. This command bridges the gap between the output of the `volume show-space` and `aggregate show-space` commands. All percentages are calculated as a percent of aggregate size.

The following example shows the `volume show-footprint` command output for a volume called testvol:

```
cluster1::> volume show-footprint testvol
```

```
Vserver : thevs
Volume  : testvol
```

Feature	Used	Used%
-----	-----	-----
Volume Data Footprint	120.6MB	4%
Volume Guarantee	1.88GB	71%
Flexible Volume Metadata	11.38MB	0%
Delayed Frees	1.36MB	0%
Total Footprint	2.01GB	76%

The following table explains some of the key rows of the output of the `volume show-footprint` command and what you can do to try to decrease space usage by that feature:

Row/feature name	Description/contents of row	Some ways to decrease
Volume Data Footprint	The total amount of space used in the containing aggregate by a volume's data in the active file system and the space used by the volume's Snapshot copies. This row does not include reserved space.	<ul style="list-style-type: none"> <li>• Deleting data from the volume.</li> <li>• Deleting Snapshot copies from the volume.</li> </ul>
Volume Guarantee	The amount of space reserved by the volume in the aggregate for future writes. The amount of space reserved depends on the guarantee type of the volume.	Changing the type of guarantee for the volume to <code>none</code> .
Flexible Volume Metadata	The total amount of space used in the aggregate by the volume's metadata files.	No direct method to control.
Delayed Frees	Blocks that ONTAP used for performance and cannot be immediately freed. For SnapMirror destinations, this row has a value of 0 and is not displayed.	No direct method to control.
File Operation Metadata	The total amount of space reserved for file operation metadata.	No direct method to control.
Total Footprint	The total amount of space that the volume uses in the aggregate. It is the sum of all of the rows.	Any of the methods used to decrease space used by a volume.

## Related information

[NetApp Technical Report 3483: Thin Provisioning in a NetApp SAN or IP SAN Enterprise Environment](#)

## Methods to create space in an aggregate

If an aggregate runs out of free space, various problems can result that range from loss of data to disabling a volume's guarantee. There are multiple ways to make more space in an aggregate.

All of the methods have various consequences. Prior to taking any action, you should read the relevant section in the documentation.

The following are some common ways to make space in an aggregate, in order of least to most consequences:

- Add disks to the aggregate.
- Move some volumes to another aggregate with available space.
- Shrink the size of volume-guaranteed volumes in the aggregate.

You can do this manually or with the `autoshrink` option of the `autosize` capability.

- Change volume guarantee types to `none` on volumes that are using large amounts of space (large volume-guaranteed volumes with large reserved files) so that the volumes take up less space in the aggregate.

A volume with a guarantee type of `none` has a smaller footprint in the aggregate than a volume with a guarantee type of `volume`.

- Delete unneeded volume Snapshot copies if the volume's guarantee type is `none`.
- Delete unneeded volumes.
- Enable space-saving features, such as deduplication or compression.
- (Temporarily) disable features that are using a large amount of metadata .

## Commands for managing aggregates

You use the `storage aggregate` command to manage your aggregates.

If you want to...	Use this command...
Display the size of the cache for all Flash Pool aggregates	<code>storage aggregate show -fields hybrid-cache-size-total -hybrid-cache-size -total &gt;0</code>
Display disk information and status for an aggregate	<code>storage aggregate show-status</code>
Display spare disks by node	<code>storage aggregate show-spare-disks</code>
Display the root aggregates in the cluster	<code>storage aggregate show -has-mroot true</code>

If you want to...	Use this command...
Display basic information and status for aggregates	<code>storage aggregate show</code>
Display the type of storage used in an aggregate	<code>storage aggregate show -fields storage-type</code>
Bring an aggregate online	<code>storage aggregate online</code>
Delete an aggregate	<code>storage aggregate delete</code>
Put an aggregate into the restricted state	<code>storage aggregate restrict</code>
Rename an aggregate	<code>storage aggregate rename</code>
Take an aggregate offline	<code>storage aggregate offline</code>
Change the RAID type for an aggregate	<code>storage aggregate modify -raidtype</code>

#### Related information

[ONTAP 9 commands](#)

## Work with Flash Pool aggregates

### Flash Pool caching policies and SSD partitioning

#### How Flash Pool aggregate caching policies work

Caching policies for the volumes in a Flash Pool aggregate let you deploy flash as high performance cache for your working data set while using lower-cost HDDs for less frequently accessed data. If you are providing cache to two or more Flash Pool aggregates, you should use Flash Pool SSD partitioning to share SSDs across the aggregates in the Flash Pool.

Caching policies are applied to volumes that reside in Flash Pool aggregates. You should understand how caching policies work before changing them.

In most cases, the default caching policy of `auto` is the best caching policy to use. The caching policy should be changed only if a different policy provides better performance for your workload. Configuring the wrong caching policy can severely degrade volume performance; the performance degradation could increase gradually over time.

Caching policies combine a read caching policy and a write caching policy. The policy name concatenates the names of the read caching policy and the write caching policy, separated by a hyphen. If there is no hyphen in the policy name, the write caching policy is “none”, except for the `auto` policy.

Read caching policies optimize for future read performance by placing a copy of the data in the cache in addition to the stored data on HDDs. For read caching policies that insert data into the cache for write

operations, the cache operates as a *write-through* cache.

Data inserted into the cache by using the write caching policy exists only in cache; there is no copy in HDDs. Flash Pool cache is RAID protected. Enabling write caching makes data from write operations available for reads from cache immediately, while deferring writing the data to HDDs until it ages out of the cache.

You can change the caching policy for a volume that resides on a Flash Pool aggregate by using the `-caching-policy` parameter with the `volume create` command. When you create a volume on a Flash Pool aggregate, by default, the `auto` caching policy is assigned to the volume.

If you move a volume from a Flash Pool aggregate to a single-tier aggregate, it loses its caching policy; if you later move it back to a Flash Pool aggregate, it is assigned the default caching policy of `auto`. If you move a volume between two Flash Pool aggregates, the caching policy is preserved.

#### **How Flash Pool SSD partitioning works for Flash Pool aggregates using storage pools**

If you are providing cache to two or more Flash Pool aggregates, you should use Flash Pool Solid-State Drive (SSD) partitioning. Flash Pool SSD partitioning allows SSDs to be shared by all the aggregates using the Flash Pool. This spreads the cost of parity over multiple aggregates, increases SSD cache allocation flexibility, and maximizes SSD performance.

For an SSD to be used in a Flash Pool aggregate, the SSD must be placed in a storage pool. You cannot use SSDs that have been partitioned for root-data partitioning in a storage pool. After the SSD is placed in the storage pool, the SSD can no longer be managed as a stand-alone disk and cannot be removed from the storage pool unless you destroy the aggregates associated with the Flash Pool and you destroy the storage pool.

SSD storage pools are divided into four equal allocation units. SSDs added to the storage pool are divided into four partitions and one partition is assigned to each of the four allocation units. The SSDs in the storage pool must be owned by the same HA pair. By default, two allocation units are assigned to each node in the HA pair. Allocation units must be owned by the node that owns the aggregate it is serving. If more Flash cache is required for aggregates on one of the nodes, the default number of allocation units can be shifted to decrease the number on one node and increase the number on the partner node.

You can use only one spare SSD for a storage pool. If the storage pool provides allocation units to Flash Pool aggregates owned by both nodes in the HA pair, then the spare SSD can be owned by either node. However, if the storage pool provides allocation units only to Flash Pool aggregates owned by one of the nodes in the HA pair, then the SSD spare must be owned by that same node.

The following illustration is an example of Flash Pool SSD partitioning. The SSD storage pool provides cache to two Flash Pool aggregates:





Storage pool SP1 is composed of five SSDs and a hot spare SSD. Two of the storage pool's allocation units are allocated to Flash Pool FP1, and two are allocated to Flash Pool FP2. FP1 has a cache RAID type of RAID4. Therefore, the allocation units provided to FP1 contain only one partition designated for parity. FP2 has a cache RAID type of RAID-DP. Therefore, the allocation units provided to FP2 include a parity partition and a double-parity partition.

In this example, two allocation units are allocated to each Flash Pool aggregate. However, if one Flash Pool aggregate required a larger cache, you could allocate three of the allocation units to that Flash Pool aggregate, and only one to the other.

### Determine Flash Pool candidacy and optimal cache size

Before converting an existing aggregate to a Flash Pool aggregate, you can determine whether the aggregate is I/O bound, and what would be the best Flash Pool cache size for your workload and budget. You can also check whether the cache of an existing Flash Pool aggregate is sized correctly.

#### What you'll need

You should know approximately when the aggregate you are analyzing experiences its peak load.

#### Steps

1. Enter advanced mode:

```
set advanced
```

2. If you need to determine whether an existing aggregate would be a good candidate for conversion to a Flash Pool aggregate, determine how busy the disks in the aggregate are during a period of peak load, and how that is affecting latency:

```
statistics show-periodic -object disk:raid_group -instance raid_group_name
```

```
-counter disk_busy|user_read_latency -interval 1 -iterations 60
```

You can decide whether reducing latency by adding Flash Pool cache makes sense for this aggregate.

The following command shows the statistics for the first RAID group of the aggregate “aggr1”:

```
statistics show-periodic -object disk:raid_group -instance /aggr1/plex0/rg0  
-counter disk_busy|user_read_latency -interval 1 -iterations 60
```

### 3. Start Automated Workload Analyzer (AWA):

```
storage automated-working-set-analyzer start -node node_name -aggregate  
aggr_name
```

AWA begins collecting workload data for the volumes associated with the specified aggregate.

### 4. Exit advanced mode:

```
set admin
```

Allow AWA to run until one or more intervals of peak load have occurred. AWA collects workload statistics for the volumes associated with the specified aggregate, and analyzes data for up to one rolling week in duration. Running AWA for more than one week will report only on data collected from the most recent week. Cache size estimates are based on the highest loads seen during the data collection period; the load does not need to be high for the entire data collection period.

### 5. Enter advanced mode:

```
set advanced
```

### 6. Display the workload analysis:

```
storage automated-working-set-analyzer show -node node_name
```

### 7. Stop AWA:

```
storage automated-working-set-analyzer stop node_name
```

All workload data is flushed and is no longer available for analysis.

### 8. Exit advanced mode:

```
set admin
```

## Create a Flash Pool aggregate using physical SSDs

You create a Flash Pool aggregate by enabling the feature on an existing aggregate composed of HDD RAID groups, and then adding one or more SSD RAID groups to that aggregate. This results in two sets of RAID groups for that aggregate: SSD RAID groups (the SSD cache) and HDD RAID groups.

### What you’ll need

- You must have identified a valid aggregate composed of HDDs to convert to a Flash Pool aggregate.

- You must have determined write-caching eligibility of the volumes associated with the aggregate, and completed any required steps to resolve eligibility issues.
- You must have determined the SSDs you will be adding, and these SSDs must be owned by the node on which you are creating the Flash Pool aggregate.
- You must have determined the checksum types of both the SSDs you are adding and the HDDs already in the aggregate.
- You must have determined the number of SSDs you are adding and the optimal RAID group size for the SSD RAID groups.

Using fewer RAID groups in the SSD cache reduces the number of parity disks required, but larger RAID groups require RAID-DP.

- You must have determined the RAID level you want to use for the SSD cache.
- You must have determined the maximum cache size for your system and determined that adding SSD cache to your aggregate will not cause you to exceed it.
- You must have familiarized yourself with the configuration requirements for Flash Pool aggregates.

### About this task

After you add an SSD cache to an aggregate to create a Flash Pool aggregate, you cannot remove the SSD cache to convert the aggregate back to its original configuration.

By default, the RAID level of the SSD cache is the same as the RAID level of the HDD RAID groups. You can override this default selection by specifying the `raidtype` option when you add the first SSD RAID groups.

### Steps

1. Mark the aggregate as eligible to become a Flash Pool aggregate:

```
storage aggregate modify -aggregate aggr_name -hybrid-enabled true
```

If this step does not succeed, determine write-caching eligibility for the target aggregate.

2. Add the SSDs to the aggregate by using the `storage aggregate add` command.

You can specify the SSDs by ID or by using the `diskcount` and `disktype` parameters.

If the HDDs and the SSDs do not have the same checksum type, or if the aggregate is a mixed-checksum aggregate, then you must use the `checksumstyle` parameter to specify the checksum type of the disks you are adding to the aggregate.

You can specify a different RAID type for the SSD cache by using the `raidtype` parameter.

If you want the cache RAID group size to be different from the default for the RAID type you are using, you should change it now, by using the `-cache-raid-group-size` parameter.

## Create a Flash Pool aggregate using SSD storage pools

### Determine whether a Flash Pool aggregate is using an SSD storage pool

You can configure a Flash Pool aggregate by adding one or more allocation units from an SSD storage pool to an existing HDD aggregate.

You manage Flash Pool aggregates differently when they use SSD storage pools to provide their cache than when they use discrete SSDs.

### Step

1. Display the aggregate's drives by RAID group:

```
storage aggregate show-status aggr_name
```

If the aggregate is using one or more SSD storage pools, the value for the `Position` column for the SSD RAID groups is displayed as `Shared`, and the name of the storage pool is displayed next to the RAID group name.

### Create an SSD storage pool

You can create solid state drive (SSD) storage pools to provide SSD cache for two to four Flash Pool aggregates.

### About this task

- You must supply a disk list when creating or adding disks to a storage pool.

Storage pools do not support a `diskcount` parameter.

- The SSDs used in the storage pool should be the same size.

### Steps

1. Determine the names of the available spare SSDs:

```
storage aggregate show-spare-disks -disk-type SSD
```

The SSDs used in a storage pool can be owned by either node of an HA pair.

2. Create the storage pool:

```
storage pool create -storage-pool sp_name -disk-list disk1,disk2,...
```

3. **Optional:** Verify the newly created storage pool:

```
storage pool show -storage-pool sp_name
```

### Results

After the SSDs are placed into the storage pool, they no longer appear as spares on the cluster, even though the storage provided by the storage pool has not yet been allocated to any Flash Pool caches. You cannot add SSDs to a RAID group as discrete drives; their storage can be provisioned only by using the allocation units of the storage pool to which they belong.

### Create a Flash Pool aggregate using SSD storage pool allocation units

You can configure a Flash Pool aggregate by adding one or more allocation units from an SSD storage pool to an existing HDD aggregate.

### What you'll need

- You must have identified a valid aggregate composed of HDDs to convert to a Flash Pool aggregate.
- You must have determined write-caching eligibility of the volumes associated with the aggregate, and completed any required steps to resolve eligibility issues.
- You must have created an SSD storage pool to provide the SSD cache to this Flash Pool aggregate.

Any allocation unit from the storage pool that you want to use must be owned by the same node that owns the Flash Pool aggregate.

- You must have determined how much cache you want to add to the aggregate.

You add cache to the aggregate by allocation units. You can increase the size of the allocation units later by adding SSDs to the storage pool if there is room.

- You must have determined the RAID type you want to use for the SSD cache.

After you add a cache to the aggregate from SSD storage pools, you cannot change the RAID type of the cache RAID groups.

- You must have determined the maximum cache size for your system and determined that adding SSD cache to your aggregate will not cause you to exceed it.

You can see the amount of cache that will be added to the total cache size by using the `storage pool show` command.

- You must have familiarized yourself with the configuration requirements for Flash Pool aggregates.

### About this task

If you want the RAID type of the cache to be different from that of the HDD RAID groups, you must specify the cache RAID type when you add the SSD capacity. After you add the SSD capacity to the aggregate, you can no longer change the RAID type of the cache.

After you add an SSD cache to an aggregate to create a Flash Pool aggregate, you cannot remove the SSD cache to convert the aggregate back to its original configuration.

### Steps

1. Mark the aggregate as eligible to become a Flash Pool aggregate:

```
storage aggregate modify -aggregate aggr_name -hybrid-enabled true
```

If this step does not succeed, determine write-caching eligibility for the target aggregate.

2. Show the available SSD storage pool allocation units:

```
storage pool show-available-capacity
```

3. Add the SSD capacity to the aggregate:

```
storage aggregate add aggr_name -storage-pool sp_name -allocation-units  
number_of_units
```

If you want the RAID type of the cache to be different from that of the HDD RAID groups, you must change it when you enter this command by using the `raidtype` parameter.

You do not need to specify a new RAID group; ONTAP automatically puts the SSD cache into separate RAID groups from the HDD RAID groups.

You cannot set the RAID group size of the cache; it is determined by the number of SSDs in the storage pool.

The cache is added to the aggregate and the aggregate is now a Flash Pool aggregate. Each allocation unit added to the aggregate becomes its own RAID group.

4. Confirm the presence and size of the SSD cache:

```
storage aggregate show aggr_name
```

The size of the cache is listed under `Total Hybrid Cache Size`.

## Related information

[NetApp Technical Report 4070: Flash Pool Design and Implementation Guide](#)

### Determine the impact to cache size of adding SSDs to an SSD storage pool

If adding SSDs to a storage pool causes your platform model's cache limit to be exceeded, ONTAP does not allocate the newly added capacity to any Flash Pool aggregates. This can result in some or all of the newly added capacity being unavailable for use.

#### About this task

When you add SSDs to an SSD storage pool that has allocation units already allocated to Flash Pool aggregates, you increase the cache size of each of those aggregates and the total cache on the system. If none of the storage pool's allocation units have been allocated, adding SSDs to that storage pool does not affect the SSD cache size until one or more allocation units are allocated to a cache.

#### Steps

1. Determine the usable size of the SSDs you are adding to the storage pool:

```
storage disk show disk_name -fields usable-size
```

2. Determine how many allocation units remain unallocated for the storage pool:

```
storage pool show-available-capacity sp_name
```

All unallocated allocation units in the storage pool are displayed.

3. Calculate the amount of cache that will be added by applying the following formula:

$(4 - \text{number of unallocated allocation units}) \times 25\% \times \text{usable size} \times \text{number of SSDs}$

### Add SSDs to an SSD storage pool

When you add solid state drives (SSDs) to an SSD storage pool, you increase the storage pool's physical and usable sizes and allocation unit size. The larger allocation unit size also affects allocation units that have already been allocated to Flash Pool aggregates.

## What you'll need

You must have determined that this operation will not cause you to exceed the cache limit for your HA pair. ONTAP does not prevent you from exceeding the cache limit when you add SSDs to an SSD storage pool, and doing so can render the newly added storage capacity unavailable for use.

## About this task

When you add SSDs to an existing SSD storage pool, the SSDs must be owned by one node or the other of the same HA pair that already owned the existing SSDs in the storage pool. You can add SSDs that are owned by either node of the HA pair.

The SSD you add to the storage pool must be the same size as disk currently used in the storage pool.

## Steps

1. **Optional:** View the current allocation unit size and available storage for the storage pool:

```
storage pool show -instance sp_name
```

2. Find available SSDs:

```
storage disk show -container-type spare -type SSD
```

3. Add the SSDs to the storage pool:

```
storage pool add -storage-pool sp_name -disk-list disk1,disk2...
```

The system displays which Flash Pool aggregates will have their size increased by this operation and by how much, and prompts you to confirm the operation.

## Commands for managing SSD storage pools

ONTAP provides the `storage pool` command for managing SSD storage pools.

If you want to...	Use this command...
Display how much storage a storage pool is providing to which aggregates	<code>storage pool show-aggregate</code>
Display how much cache would be added to the overall cache capacity for both RAID types (allocation unit data size)	<code>storage pool show -instance</code>
Display the disks in a storage pool	<code>storage pool show-disks</code>
Display the unallocated allocation units for a storage pool	<code>storage pool show-available-capacity</code>
Change the ownership of one or more allocation units of a storage pool from one HA partner to the other	<code>storage pool reassign</code>

## Related information

**Determine whether to modify the caching policy of Flash Pool aggregates****Determine whether to modify the caching policy of Flash Pool aggregates overview**

You can assign cache-retention policies to volumes in Flash Pool aggregates to determine how long the volume data remains in the Flash Pool cache. However, in some cases changing the cache-retention policy might not impact the amount of time the volume's data remains in the cache.

**About this task**

If your data meets any of the following conditions, changing your cache-retention policy might not have an impact:

- Your workload is sequential.
- Your workload does not reread the random blocks cached in the solid state drives (SSDs).
- The cache size of the volume is too small.

The following steps check for these conditions. The task must be done in advanced privilege mode.

**Steps**

1. View the workload volume:

```
statistics start -object workload_volume
```

2. Determine the workload pattern of the volume:

```
statistics show -object workload_volume -instance volume-workload -counter sequential_reads
```

3. Determine the hit rate of the volume:

```
statistics show -object waf1_hya_vvol -instance volume -counter read_ops_replaced_ppercent|wc_write_blks_overwritten_percent
```

4. Determine the Cacheable Read and Project Cache Alloc of the volume:

```
system node run -node node_name waf1 awa start aggr_name
```

5. Display the AWA summary:

```
system node run -node node_name waf1 awa print aggr_name
```

6. Compare the volume's hit rate to the Cacheable Read.

If the hit rate of the volume is greater than the Cacheable Read, then your workload does not reread random blocks cached in the SSDs.

7. Compare the volume's current cache size to the Project Cache Alloc.

If the current cache size of the volume is greater than the Project Cache Alloc, then the size of your



volume cache is too small.

### Modify caching policies of Flash Pool aggregates

You should modify the caching policy of a volume only if a different caching policy is expected to provide better performance. You can modify the caching policy of a volume on a Flash Pool aggregate.

#### What you'll need

You must determine whether you want to modify your caching policy.

#### About this task

In most cases, the default caching policy of `auto` is the best caching policy that you can use. The caching policy should be changed only if a different policy provides better performance for your workload. Configuring the wrong caching policy can severely degrade volume performance; the performance degradation could increase gradually over time. You should use caution when modifying caching policies. If you experience performance issues with a volume for which the caching policy has been changed, you should return the caching policy to `auto`.

#### Step

1. Modify the volume's caching policy:

```
volume modify -volume volume_name -caching-policy policy_name
```

#### Example

The following example modifies the caching policy of a volume named "vol2" to the policy `none`:

```
volume modify -volume vol2 -caching-policy none
```

### Set the cache-retention policy for Flash Pool aggregates

You can assign cache-retention policies to volumes in Flash Pool aggregates. Data in volumes with a high cache-retention policy remains in cache longer and data in volumes with a low cache-retention policy is removed sooner. This increases performance of your critical workloads by making high priority information accessible at a faster rate for a longer period of time.

#### What you'll need

You should know whether your system has any conditions that might prevent the cache-retention policy from having an impact on how long your data remains in cache.

#### About this task

The task must be done in advanced privilege mode.

#### Steps

1. Change the privilege setting to advanced:

```
set -privilege advanced
```

2. Verify the volume's cache-retention policy:

By default the cache retention policy is `normal`.

3. Set the cache-retention policy:

ONTAP Version	Command
ONTAP 9.0, 9.1	<pre>priority hybrid-cache set volume_name read-cache=read_cache_value write- cache=write_cache_value cache- retention- priority=cache_retention_policy</pre> <p>Set <code>cache_retention_policy</code> to <code>high</code> for data that you want to remain in cache longer. Set <code>cache_retention_policy</code> to <code>low</code> for data that you want to remove from cache sooner.</p>
ONTAP 9.2 or later	<pre>volume modify -volume volume_name -vserver vservers_name -caching-policy policy_name.</pre>

4. Verify that the volume's cache-retention policy is changed to the option you selected.

5. Return the privilege setting to admin:

```
set -privilege admin
```

## Managing disks

### 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

## **How hot spare disks work**

A hot spare disk is a disk that is assigned to a storage system and is ready for use, but is not in use by a RAID group and does not hold any data.

If a disk failure occurs within a RAID group, the hot spare disk is automatically assigned to the RAID group to replace the failed disks. The data of the failed disk is reconstructed on the hot spare replacement disk in the background from the RAID parity disk. The reconstruction activity is logged in the `/etc/message` file and an AutoSupport message is sent.

If the available hot spare disk is not the same size as the failed disk, a disk of the next larger size is chosen and then downsized to match the size of the disk that it is replacing.

## **How low spare warnings can help you manage your spare disks**

By default, warnings are issued to the console and logs if you have fewer than one hot spare drive that matches the attributes of each drive in your storage system. You can change the threshold value for these warning messages to ensure that your system adheres to best practices.

You should set the `min_spare_count` RAID option to 2 to ensure that you always have the minimum recommended number of spare disks. You can use the `storage raid-options modify -node nodename -name option_name -value 2` to set the option.

## **Display disk and partition ownership**

You can view disk ownership to determine which node controls the storage. You can also view the partition ownership on systems that use shared disks.

### **Steps**

1. Display the ownership of physical disks using the `storage disk show -ownership` command:

```
cluster::> storage disk show -ownership
```

Disk	Aggregate	Home	Owner	DR	Home	Home ID	Owner ID	DR
Home ID	Reserver	Pool						
1.0.0	aggr0_2	node2	node2	-		2014941509	2014941509	-
2014941509	Pool10							
1.0.1	aggr0_2	node2	node2	-		2014941509	2014941509	-
2014941509	Pool10							
1.0.2	aggr0_1	node1	node1	-		2014941219	2014941219	-
2014941219	Pool10							
1.0.3	-	node1	node1	-		2014941219	2014941219	-
2014941219	Pool10							
...								

2. If you have a system that uses shared disks, display the partition ownership using the `storage disk show -partition-ownership` command:

```
cluster::> storage disk show -partition-ownership
```

		Root			Data		
Container	Container						
Disk	Aggregate	Root	Owner	Owner ID	Data	Owner	Owner ID
Owner ID							
1.0.0	-	node1	1886742616	node1	1886742616	node1	1886742616
1886742616							
1.0.1	-	node1	1886742616	node1	1886742616	node1	1886742616
1886742616							
1.0.2	-	node2	1886742657	node2	1886742657	node2	1886742657
1886742657							
1.0.3	-	node2	1886742657	node2	1886742657	node2	1886742657
1886742657							
...							

## Manually assign ownership of partitioned disks

### Manually assign ownership of partitioned disks overview

You can set the ownership of the container disk or the partitions manually or by using auto-assignment—just as you do for unpartitioned disks.



If a container disk fails in a half-populated shelf and is replaced, ONTAP will not auto-assign ownership. In this case, any assignment of new disks will need to be done manually. To make auto-assign work on half-populated shelves, place disks equally on lower half and 6 on far right bays to begin with. That is, 6 disks from bays 0-5 and 6 disks from bays 18-23. After the container disk is assigned in an ADP-configured system, ONTAP's software will handle any partitioning and partition assignments that are required, without user intervention.

### Manually assign disks with root-data partitioning

For root-data partitioning there are three owned entities (the container disk and the two partitions) collectively owned by the HA pair.

#### About this task

The container disk and the two partitions do not all need to be owned by the same node in the HA pair as long as they are all owned by one of the nodes in the HA pair. However, when you use a partition in an aggregate, it must be owned by the same node that owns the aggregate.

#### Steps

1. Display the current ownership for the partitioned disk:

```
storage disk show -disk disk_name -partition-ownership
```

2. Set the CLI privilege level to advanced:

```
set -privilege advanced
```

3. Enter the appropriate command, depending on which ownership entity you want to assign ownership for:

If you want to assign ownership for the...	Use this command...
Container disk	<pre>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i></pre>
Data partition	<pre>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -data true</pre>
Root partition	<pre>storage disk assign -disk <i>disk_name</i> -owner <i>owner_name</i> -root true</pre>

If any of the ownership entities are already owned, then you must include the `-force` option.

### Manually assign disks with root-data-data partitioning

For root-data-data partitioning there are four owned entities (the container disk and the three partitions) collectively owned by the HA pair.

#### About this task

Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.

Parameters must be used in the `disk assign` command to assign the proper partition of a root-data-data partitioned disk. You cannot use these parameters with disks that are part of a storage pool. The default value is false.

- The `[-data1 [true]]` parameter assigns the `data1` partition of a root-data1-data2 partitioned disk.
- The `[-data2 [true]]` parameter assigns the `data2` partition of a root-data1-data2 partitioned disk.

**Steps**

1. Display the current ownership for the partitioned disk:

```
storage disk show -disk disk_name -partition-ownership
```

2. Set the CLI privilege level to advanced:

```
set -privilege advanced
```

3. Enter the appropriate command, depending on which ownership entity you want to assign ownership for:

If you want to assign ownership for the...	Use this command...
Container disk	<code>storage disk assign -disk disk_name -owner owner_name</code>
Data1 partition	<code>storage disk assign -disk disk_name -owner owner_name-data1 true</code>
Data2 partition	<code>storage disk assign -disk disk_name -owner owner_name-data2 true</code>
Root partition	<code>storage disk assign -disk disk_name -owner owner_name -root true</code>

If any of the ownership entities are already owned, then you must include the `-force` option.

**Additional root-data partitioning management options**

Beginning with ONTAP 9.2, a new root-data partitioning option is available from the Boot Menu that provides additional management features for disks that are configured for root-data partitioning.

The following management features are available under the Boot Menu Option 9.

- Unpartition all disks and remove their ownership information

This option is useful if your system is configured for root-data partitioning and you need to reinitialize it with a different configuration.

- Clean configuration and initialize node with partitioned disks

This option is useful for the following:

- Your system is not configured for root-data partitioning and you would like to configure it for root-data partitioning
- Your system is incorrectly configured for root-data partitioning and you need to correct it
- You have an AFF platform or a FAS platform with only SSDs attached that is configured for the previous version of root-data partitioning and you want to upgrade it to the newer version of root-data partitioning to gain increased storage efficiency
- Clean configuration and initialize node with whole disks

This option is useful if you need to:

- Unpartition existing partitions
- Remove local disk ownership
- Reinitialize your system with whole disks using RAID-DP

### Configure automatic assignment of disk ownership

You can configure ONTAP to automatically assign disk ownership according to a disk's stack, shelf, or bay. If configured, automatic disk ownership assignments occur 10 minutes after system initialization and every five minutes during normal system operation.

#### What you'll need

- Your system must adhere to the requirements for automatic disk ownership.
- If you have multiple stacks or shelves that must have different ownership, one disk must have been manually assigned on each stack or shelf so that automatic ownership assignment works on each stack or shelf.
- Use the `bay autoassign-policy` only for entry level platforms. If you try to use the `bay autoassign-policy` for a non-entry level platform, it will fail.

#### About this task

The behavior of the `default` automatic assignment policy depends on the system model. For entry level models, the `default` policy is equivalent to the `bay` policy. For all other systems, it is equivalent to the `stack` policy.

#### Steps

1. Configure automatic disk assignment:

```
storage disk option modify -autoassign-policy autoassign_policy -node
node_name
```

- Use `stack` as the `autoassign_policy` to configure automatic ownership at the stack or loop level.
- Use `shelf` as the `autoassign_policy` to configure automatic ownership at the shelf level.
- Use `bay` as the `autoassign_policy` to configure automatic ownership at the bay level.

2. Verify the automatic assignment settings for the disks:

```
storage disk option show
```

```
cluster1::> storage disk option show
```

Node	BKg. FW. Upd.	Auto Copy	Auto Assign	Auto Assign Policy
-----	-----	-----	-----	-----
cluster1-1	on	on	on	default
cluster1-2	on	on	on	default

### Which disk autoassignment policy to use

You can typically use the default autoassignment policy, which is equivalent to the `stack` policy for most systems, and to the `bay` policy for entry-level systems (AFF A2xx, FAS2xxx). However, for some configurations, you might need to change the autoassignment policy.

You must select the appropriate autoassignment based on your configuration:

If you are using...	Then use this autoassignment policy...
Stand-alone entry-level system	<code>stack</code>
Entry-level systems in an HA configuration with a single, shared shelf	<code>bay</code>
Entry-level systems in an HA configuration with one stack of two or more shelves	<code>shelf</code>
MetroCluster configurations with one stack per node, two or more shelves	<code>shelf</code>
All other configurations	<code>stack</code>

### Remove a failed disk

A disk that is completely failed is no longer counted by ONTAP as a usable disk, and you can immediately disconnect the disk from the disk shelf. However, you should leave a partially failed disk connected long enough for the Rapid RAID Recovery process to complete.

#### About this task

If you are removing a disk because it has failed or because it is producing excessive error messages, you should not use the disk again in this or any other storage system.

#### Steps

1. Find the disk ID of the failed disk:



```
storage disk show -broken
```

If the disk does not appear in the list of failed disks, it might be partially failed, with a Rapid RAID Recovery in process. In this case, you should wait until the disk is present in the list of failed disks (which means that the Rapid RAID Recovery process is complete) before removing the disk.

2. Determine the physical location of the disk you want to remove: +

```
storage disk set-led -action on -disk disk_name 2
```

The fault LED on the face of the disk is lit.

3. Remove the disk from the disk shelf, following the instructions in the hardware guide for your disk shelf model.

## Remove ownership from a disk

ONTAP writes disk ownership information to the disk. Before you remove a spare disk or its shelf from a node, you should remove its ownership information so that it can be properly integrated into another node.

### What you'll need

The disk you want to remove ownership from must meet the following requirements:

- It must be a spare disk.

You cannot remove ownership from a disk that is being used in an aggregate.

- It cannot be in the maintenance center.
- It cannot be undergoing sanitization.
- It cannot be failed.

It is not necessary to remove ownership from a failed disk.

### About this task

If you have automatic disk assignment enabled, ONTAP could automatically reassign ownership before you remove the disk from the node. For this reason, you disable automatic ownership assignment until the disk is removed, and then reenable it.

### Steps

1. If disk ownership automatic assignment is on, turn it off:

```
storage disk option modify -node node_name -autoassign off
```

2. If needed, repeat the previous step for the node's HA partner.
3. Remove the software ownership information from the disk:

```
storage disk removeowner disk_name
```

To remove ownership information from multiple disks, use a comma-separated list:

```
storage disk removeowner sys1:0a.23,sys1:0a.24,sys1:0a.25
```

4. If the disk is partitioned for root-data partitioning, remove ownership from the partitions by entering both of the following commands:

```
storage disk removeowner -disk disk_name -root true
```

```
storage disk removeowner -disk disk_name -data true
```

Both partitions are no longer owned by any node.

5. If you turned off disk ownership automatic assignment previously, turn it on after the disk has been removed or reassigned:

```
storage disk option modify -node node_name -autoassign on
```

6. If needed, repeat the previous step for the node's HA partner.

## Disk sanitization

### Disk sanitization overview

Disk sanitization is the process of physically obliterating data by overwriting disks or SSDs with specified byte patterns or random data so that recovery of the original data becomes impossible. Using the sanitization process ensures that no one can recover the data on the disks.

This functionality is available through the nodeshell in all ONTAP 9 releases, and starting with ONTAP 9.6 in maintenance mode.

The disk sanitization process uses three successive default or user-specified byte overwrite patterns for up to seven cycles per operation. The random overwrite pattern is repeated for each cycle.

Depending on the disk capacity, the patterns, and the number of cycles, the process can take several hours. Sanitization runs in the background. You can start, stop, and display the status of the sanitization process. The sanitization process contains two phases:

1. Formatting phase

The operation performed for the formatting phase depends on the class of disk being sanitized, as shown in the following table:

Disk class	Formatting phase
Capacity HDDs	Skipped
Performance HDDs	SCSI format operation
SSDs	SCSI sanitize operation

2. Pattern overwrite phase

The specified overwrite patterns are repeated for the specified number of cycles.

When the sanitization process is complete, the specified disks are in a sanitized state. They are not returned to spare status automatically. You must return the sanitized disks to the spare pool before the newly sanitized

disks are available to be added to another aggregate.

#### **When disk sanitization cannot be performed**

Disk sanitization is not supported for all disk types. In addition, there are circumstances in which disk sanitization cannot be performed.

- It is not supported on all SSD part numbers.

For information about which SSD part numbers support disk sanitization, see the [Hardware Universe](#).

- It is not supported in takeover mode for systems in an HA pair.
- It cannot be performed on disks that were failed due to readability or writability problems.
- It does not perform its formatting phase on ATA drives.
- If you are using the random pattern, it cannot be performed on more than 100 disks at one time.
- It is not supported on array LUNs.
- If you sanitize both SES disks in the same ESH shelf at the same time, you see errors on the console about access to that shelf, and shelf warnings are not reported for the duration of the sanitization.

However, data access to that shelf is not interrupted.

#### **What happens if disk sanitization is interrupted**

If disk sanitization is interrupted by user intervention or an unexpected event such as a power outage, ONTAP takes action to return the disks that were being sanitized to a known state, but you must also take action before the sanitization process can finish.

Disk sanitization is a long-running operation. If the sanitization process is interrupted by power failure, system panic, or manual intervention, the sanitization process must be repeated from the beginning. The disk is not designated as sanitized.

If the formatting phase of disk sanitization is interrupted, ONTAP must recover any disks that were corrupted by the interruption. After a system reboot and once every hour, ONTAP checks for any sanitization target disk that did not complete the formatting phase of its sanitization. If any such disks are found, ONTAP recovers them. The recovery method depends on the type of the disk. After a disk is recovered, you can rerun the sanitization process on that disk; for HDDs, you can use the `-s` option to specify that the formatting phase is not repeated again.

#### **Tips for creating and backing up aggregates containing data to be sanitized**

If you are creating or backing up aggregates to contain data that might need to be sanitized, following some simple guidelines will reduce the time it takes to sanitize your data.

- Make sure your aggregates containing sensitive data are not larger than they need to be.

If they are larger than needed, sanitization requires more time, disk space, and bandwidth.

- When you back up aggregates containing sensitive data, avoid backing them up to aggregates that also contain large amounts of nonsensitive data.

This reduces the resources required to move nonsensitive data before sanitizing sensitive data.

## Sanitize a disk

Sanitizing a disk allows you to remove data from a disk or a set of disks on decommissioned or inoperable systems so that the data can never be recovered.

Two methods are available to sanitize disks:

- Using maintenance mode commands in ONTAP 9.6 and later releases.
- Using nodeshell commands in all ONTAP 9 releases.

### Maintenance mode method

Starting with ONTAP 9.6, you can perform disk sanitization in maintenance mode.

#### What you'll need

- The disks cannot be self-encrypting disks (SED).

You must use the `storage encryption disk sanitize` command to sanitize an SED.

#### [Encryption of data at rest](#)

### Steps

1. Boot into maintenance mode.
2. If the disks you want to sanitize are partitioned, unpartition each disk:

```
disk unpartition disk_name
```

3. Sanitize the specified disks:

```
disk sanitize start [-p pattern1|-r [-p pattern2|-r [-p pattern3|-r]]] [-c cycle_count] disk_list
```



Do not turn off power to the node, disrupt the storage connectivity, or remove target disks while sanitizing. If sanitizing is interrupted during the formatting phase, the formatting phase must be restarted and allowed to finish before the disks are sanitized and ready to be returned to the spare pool. If you need to abort the sanitization process, you can do so by using the `disk sanitize abort` command. If the specified disks are undergoing the formatting phase of sanitization, the abort does not occur until the phase is complete.

`-p pattern1 -p pattern2 -p pattern3` specifies a cycle of one to three user-defined hex byte overwrite patterns that can be applied in succession to the disks being sanitized. The default pattern is three passes, using 0x55 for the first pass, 0xaa for the second pass, and 0x3c for the third pass.

`-r` replaces a patterned overwrite with a random overwrite for any or all of the passes.

`-c cycle_count` specifies the number of times that the specified overwrite patterns are applied. The default value is one cycle. The maximum value is seven cycles.

`disk_list` specifies a space-separated list of the IDs of the spare disks to be sanitized.

4. If desired, check the status of the disk sanitization process:

```
disk sanitize status [disk_list]
```

5. After the sanitization process is complete, return the disks to spare status for each disk:

```
disk sanitize release disk_name
```

6. Exit maintenance mode.

## Nodeshell method

When disk sanitization is enabled using nodeshell commands, it disables some low-level ONTAP commands. After disk sanitization is enabled on a node, it cannot be disabled.

### What you'll need

- The disks must be spare disks; they must be owned by a node, but not used in an aggregate.

If the disks are partitioned, neither partition can be in use in an aggregate.

- The disks cannot be self-encrypting disks (SED).

You must use the `storage encryption disk sanitize` command to sanitize an SED.

### Encryption of data at rest

- The disks cannot be part of a storage pool.

## Steps

1. Enter the nodeshell for the node that owns the disks you want to sanitize:

```
system node run -node node_name
```

2. Enable disk sanitization:

```
options licensed_feature.disk_sanitization.enable on
```

You are asked to confirm the command because it is irreversible.

3. Switch to the nodeshell advanced privilege level:

```
priv set advanced
```

4. If the disks you want to sanitize are partitioned, unpartition each disk:

```
disk unpartition disk_name
```

5. Sanitize the specified disks:

```
disk sanitize start [-p pattern1|-r [-p pattern2|-r [-p pattern3|-r]]] [-c  
cycle_count] disk_list
```



Do not turn off power to the node, disrupt the storage connectivity, or remove target disks while sanitizing. If sanitizing is interrupted during the formatting phase, the formatting phase must be restarted and allowed to finish before the disks are sanitized and ready to be returned to the spare pool.

If you need to abort the sanitization process, you can do so by using the `disk sanitize abort` command. If the specified disks are undergoing the formatting phase of sanitization, the abort does not occur until the phase is complete.

`-p pattern1 -p pattern2 -p pattern3` specifies a cycle of one to three user-defined hex byte overwrite patterns that can be applied in succession to the disks being sanitized. The default pattern is three passes, using 0x55 for the first pass, 0xaa for the second pass, and 0x3c for the third pass.

`-r` replaces a patterned overwrite with a random overwrite for any or all of the passes.

`-c cycle_count` specifies the number of times that the specified overwrite patterns are applied.

The default value is one cycle. The maximum value is seven cycles.

`disk_list` specifies a space-separated list of the IDs of the spare disks to be sanitized.

6. If you want to check the status of the disk sanitization process:

```
disk sanitize status [disk_list]
```

7. After the sanitization process is complete, return the disks to spare status:

```
disk sanitize release disk_name
```

8. Return to the nodeshell admin privilege level:

```
priv set admin
```

9. Return to the ONTAP CLI:

```
exit
```

10. Determine whether all of the disks were returned to spare status:

```
storage aggregate show-spare-disks
```

If...	Then...
All of the sanitized disks are listed as spares	You are done. The disks are sanitized and in spare status.

Some of the sanitized disks are not listed as spares

Complete the following steps:

a. Enter advanced privilege mode:

```
set -privilege advanced
```

b. Assign the unassigned sanitized disks to the appropriate node for each disk:

```
storage disk assign -disk disk_name -owner  
node_name
```

c. Return the disks to spare status for each disk:

```
storage disk unfail -disk disk_name -s -q
```

d. Return to administrative mode:

```
+set -privilege admin
```

## Result

The specified disks are sanitized and designated as hot spares. The serial numbers of the sanitized disks are written to `/etc/log/sanitized_disks`.

## Set up an active-passive configuration on nodes using root-data partitioning

When an HA pair is configured to use root-data partitioning by the factory, ownership of the data partitions is split between both nodes in the pair, for use in an active-active configuration. If you want to use the HA pair in an active-passive configuration, you must update partition ownership before creating your data aggregate.

### What you'll need

- You should have decided which node will be the active node and which node will be the passive node.
- Storage failover must be configured on the HA pair.

### About this task

This task is performed on two nodes: Node A and Node B.

All commands are input at the clustershell.

This procedure is designed for nodes for which no data aggregate has been created from the partitioned disks.

### Steps

1. View the current ownership of the data partitions:

```
storage aggregate show-spare-disks
```

You can see that half of the data partitions are owned by one node and half are owned by the other node. All of the data partitions should be spare.

```
cluster1::> storage aggregate show-spare-disks
```

Original Owner: cluster1-01

Pool0

Partitioned Spares

Local

Local

Data

Root Physical

Disk	Type	RPM	Checksum	Usable
Usable      Size				

-----	-----	-----	-----	-----
1.0.0	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.1	BSAS	7200	block	753.8GB
73.89GB 828.0GB				
1.0.5	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.6	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.10	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.11	BSAS	7200	block	753.8GB
0B 828.0GB				

Original Owner: cluster1-02

Pool0

Partitioned Spares

Local

Local

Data

Root Physical

Disk	Type	RPM	Checksum	Usable
Usable      Size				

-----	-----	-----	-----	-----
1.0.2	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.3	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.4	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.7	BSAS	7200	block	753.8GB
0B 828.0GB				
1.0.8	BSAS	7200	block	753.8GB
73.89GB 828.0GB				



```

1.0.9          BSAS      7200 block      753.8GB
0B  828.0GB
12 entries were displayed.

```

## 2. Enter the advanced privilege level:

```
set advanced
```

## 3. For each data partition owned by the node that will be the passive node, assign it to the active node:

```
storage disk assign -force -data true -owner active_node_name -disk disk_name
```

You do not need to include the partition as part of the disk name.

You would enter a command similar to the following example for each data partition you need to reassign:

```
storage disk assign -force -data true -owner cluster1-01 -disk 1.0.3
```

## 4. Confirm that all of the partitions are assigned to the active node.

```

cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
Pool0
Partitioned Spares

Local
Local
Data
Root Physical
Disk
Usable      Size      Type      RPM Checksum      Usable
-----
-----
1.0.0          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.1          BSAS      7200 block      753.8GB
73.89GB  828.0GB
1.0.2          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.3          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.4          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.5          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.6          BSAS      7200 block      753.8GB
0B  828.0GB

```

```

1.0.7          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.8          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.9          BSAS      7200 block      753.8GB
0B  828.0GB
1.0.10         BSAS      7200 block      753.8GB
0B  828.0GB
1.0.11         BSAS      7200 block      753.8GB
0B  828.0GB

Original Owner: cluster1-02
Pool0
Partitioned Spares

Local
Local
Data
Root Physical
Disk
Usable      Size      Type      RPM Checksum      Usable
-----
1.0.8          BSAS      7200 block      0B
73.89GB  828.0GB
13 entries were displayed.

```

Note that cluster1-02 still owns a spare root partition.

##### 5. Return to administrative privilege:

```
set admin
```

##### 6. Create your data aggregate, leaving at least one data partition as spare:

```
storage aggregate create new_aggr_name -diskcount number_of_partitions -node
active_node_name
```

The data aggregate is created and is owned by the active node.

### Set up an active-passive configuration on nodes using root-data-data partitioning

When an HA pair is configured to use root-data-data partitioning by the factory, ownership of the data partitions is split between both nodes in the pair, for use in an active-active configuration. If you want to use the HA pair in an active-passive configuration, you must update partition ownership before creating your data aggregate.

#### What you'll need

- You should have decided which node will be the active node and which node will be the passive node.
- Storage failover must be configured on the HA pair.

### About this task

This task is performed on two nodes: Node A and Node B.

All commands are input at the clustershell.

This procedure is designed for nodes for which no data aggregate has been created from the partitioned disks.

### Steps

1. View the current ownership of the data partitions:

```
storage aggregate show-spare-disks -original-owner passive_node_name -fields
local-usable-data1-size, local-usable-data2-size
```

You should see that half of the data partitions are owned by one node and half are owned by the other node. All of the data partitions should be spare.

2. Enter the advanced privilege level:

```
set advanced
```

3. For each data1 partition owned by the node that will be the passive node, assign it to the active node:

```
storage disk assign -force -data1 -owner active_node_name -disk disk_name
```

You do not need to include the partition as part of the disk name

4. For each data2 partition owned by the node that will be the passive node, assign it to the active node:

```
storage disk assign -force -data2 -owner active_node_name -disk disk_name
```

You do not need to include the partition as part of the disk name

5. Confirm that all of the partitions are assigned to the active node:

```
storage aggregate show-spare-disks
```

```
cluster1::*> storage aggregate show-spare-disks
```

```
Original Owner: cluster1-01
```

```
Pool0
```

```
Partitioned Spares
```

```
Local
```

```
Local
```

```
Data
```

```
Root Physical
```

```
Disk
```

```
Type
```

```
RPM Checksum
```

```
Usable
```

```
Usable      Size
```

```
-----
```

```

-----
 1.0.0          BSAS      7200 block      753.8GB
0B  828.0GB
 1.0.1          BSAS      7200 block      753.8GB
73.89GB  828.0GB
 1.0.2          BSAS      7200 block      753.8GB
0B  828.0GB
 1.0.3          BSAS      7200 block      753.8GB
0B  828.0GB
 1.0.4          BSAS      7200 block      753.8GB
0B  828.0GB
 1.0.5          BSAS      7200 block      753.8GB
0B  828.0GB
 1.0.6          BSAS      7200 block      753.8GB
0B  828.0GB
 1.0.7          BSAS      7200 block      753.8GB
0B  828.0GB
 1.0.8          BSAS      7200 block      753.8GB
0B  828.0GB
 1.0.9          BSAS      7200 block      753.8GB
0B  828.0GB
 1.0.10         BSAS      7200 block      753.8GB
0B  828.0GB
 1.0.11         BSAS      7200 block      753.8GB
0B  828.0GB

```

Original Owner: cluster1-02

Pool0

Partitioned Spares

Local

Local

Data

Root Physical

Disk	Type	RPM	Checksum	Usable
Usable      Size				

```

-----
-----

```

```

 1.0.8          BSAS      7200 block      0B
73.89GB  828.0GB

```

13 entries were displayed.

Note that cluster1-02 still owns a spare root partition.

## 6. Return to administrative privilege:

```
set admin
```

7. Create your data aggregate, leaving at least one data partition as spare:

```
storage aggregate create new_aggr_name -diskcount number_of_partitions -node  
active_node_name
```

The data aggregate is created and is owned by the active node.

8. Alternatively, you can use ONTAP's recommend aggregate layout which includes best practices for RAID group layout and spare counts:

```
storage aggregate auto-provision
```

## Commands for managing disks

You can use the `storage disk` and `storage aggregate` commands to manage your disks.

If you want to...	Use this command...
Display a list of spare disks, including partitioned disks, by owner	<code>storage aggregate show-spare-disks</code>
Display the disk RAID type, current usage, and RAID group by aggregate	<code>storage aggregate show-status</code>
Display the RAID type, current usage, aggregate, and RAID group, including spares, for physical disks	<code>storage disk show -raid</code>
Display a list of failed disks	<code>storage disk show -broken</code>
Display the pre-cluster (nodescope) drive name for a disk	<code>storage disk show -primary-paths</code> (advanced)
Illuminate the LED for a particular disk or shelf	<code>storage disk set-led</code>
Display the checksum type for a specific disk	<code>storage disk show -fields checksum- compatibility</code>
Display the checksum type for all spare disks	<code>storage disk show -fields checksum- compatibility -container-type spare</code>
Display disk connectivity and placement information	<code>storage disk show -fields disk,primary- port,secondary-name,secondary- port,shelf,bay</code>
Display the pre-cluster disk names for specific disks	<code>storage disk show -disk diskname -fields diskpathnames</code>

Display the list of disks in the maintenance center	<code>storage disk show -maintenance</code>
Display SSD wear life	<code>storage disk show -ssd-wear</code>
Unpartition a shared disk	<code>storage disk unpartition</code> (available at diagnostic level)
Zero all non-zeroed disks	<code>storage disk zerospares</code>
Stop an ongoing sanitization process on one or more specified disks	<code>system node run -node nodename -command disk sanitize</code>
Display storage encryption disk information	<code>storage encryption disk show</code>
Retrieve authentication keys from all linked key management servers	<code>security key-manager restore</code>

#### Related information

[ONTAP 9 commands](#)

#### Commands for displaying space usage information

You use the `storage aggregate` and `volume` commands to see how space is being used in your aggregates and volumes and their Snapshot copies.

To display information about...	Use this command...
Aggregates, including details about used and available space percentages, Snapshot reserve size, and other space usage information	<code>storage aggregate show storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve</code>
How disks and RAID groups are used in an aggregate, and RAID status	<code>storage aggregate show-status</code>
The amount of disk space that would be reclaimed if you deleted a specific Snapshot copy	<code>volume snapshot compute-reclaimable</code>
The amount of space used by a volume	<code>volume show -fields size,used,available,percent-used volume show-space</code>
The amount of space used by a volume in the containing aggregate	<code>volume show-footprint</code>

#### Related information

[ONTAP 9 commands](#)

## Commands for displaying information about storage shelves

You use the `storage shelf show` command to display configuration and error information for your disk shelves.

If you want to display...	Use this command...
General information about shelf configuration and hardware status	<code>storage shelf show</code>
Detailed information for a specific shelf, including stack ID	<code>storage shelf show -shelf</code>
Unresolved, customer actionable, errors by shelf	<code>storage shelf show -errors</code>
Bay information	<code>storage shelf show -bay</code>
Connectivity information	<code>storage shelf show -connectivity</code>
Cooling information, including temperature sensors and cooling fans	<code>storage shelf show -cooling</code>
Information about I/O modules	<code>storage shelf show -module</code>
Port information	<code>storage shelf show -port</code>
Power information, including PSUs (power supply units), current sensors, and voltage sensors	<code>storage shelf show -power</code>

### Related information

[ONTAP 9 commands](#)

## Managing RAID groups

### Convert from RAID-DP to RAID-TEC

If you want the added protection of triple-parity, you can convert from RAID-DP to RAID-TEC. RAID-TEC is recommended if the size of the disks used in your aggregate is greater than 4 TiB.

#### What you'll need

The aggregate that is to be converted must have a minimum of six disks.

#### About this task

Hard disk drive (HDD) aggregates can be converted from RAID-DP to RAID-TEC. This includes HDD tiers in Flash Pool aggregates.

#### Steps

1. Verify that the aggregate is online and has a minimum of six disks:

```
storage aggregate show-status -aggregate aggregate_name
```

2. Convert the aggregate from RAID-DP to RAID-TEC:

```
storage aggregate modify -aggregate aggregate_name -raidtype raid_tec
```

3. Verify that the aggregate RAID policy is RAID-TEC:

```
storage aggregate show aggregate_name
```

## Convert RAID-TEC to RAID-DP

If you reduce the size of your aggregate and no longer need triple parity, you can convert your RAID policy from RAID-TEC to RAID-DP and reduce the number of disks you need for RAID parity.

### What you'll need

The maximum RAID group size for RAID-TEC is larger than the maximum RAID group size for RAID-DP. If the largest RAID-TEC group size is not within the RAID-DP limits, you cannot convert to RAID-DP.

### Steps

1. Verify that the aggregate is online and has a minimum of six disks:

```
storage aggregate show-status -aggregate aggregate_name
```

2. Convert the aggregate from RAID-TEC to RAID-DP:

```
storage aggregate modify -aggregate aggregate_name -raidtype raid_dp
```

3. Verify that the aggregate RAID policy is RAID-DP:

```
storage aggregate show aggregate_name
```

## Considerations for sizing RAID groups

Configuring an optimum RAID group size requires a trade-off of factors. You must decide which factors—speed of RAID rebuild, assurance against risk of data loss due to drive failure, optimizing I/O performance, and maximizing data storage space—are most important for the aggregate that you are configuring.

When you create larger RAID groups, you maximize the space available for data storage for the same amount of storage used for parity (also known as the “parity tax”). On the other hand, when a disk fails in a larger RAID group, reconstruction time is increased, impacting performance for a longer period of time. In addition, having more disks in a RAID group increases the probability of a multiple disk failure within the same RAID group.

### HDD or array LUN RAID groups

You should follow these guidelines when sizing your RAID groups composed of HDDs or array LUNs:



- All RAID groups in an aggregate should have the same number of disks.

While you can have up to 50% less or more than the number of disks in different raid groups on one aggregate, this might lead to performance bottlenecks in some cases, so is best avoided.

- The recommended range of RAID group disk numbers is between 12 and 20.

The reliability of performance disks can support a RAID group size of up to 28, if needed.

- If you can satisfy the first two guidelines with multiple RAID group disk numbers, you should choose the larger number of disks.

### **SSD RAID groups in Flash Pool aggregates**

The SSD RAID group size can be different from the RAID group size for the HDD RAID groups in a Flash Pool aggregate. Usually, you should ensure that you have only one SSD RAID group for a Flash Pool aggregate, to minimize the number of SSDs required for parity.

### **SSD RAID groups in SSD aggregates**

You should follow these guidelines when sizing your RAID groups composed of SSDs:

- All RAID groups in an aggregate should have a similar number of drives.

The RAID groups do not have to be exactly the same size, but you should avoid having any RAID group that is less than one half the size of other RAID groups in the same aggregate when possible.

- For RAID-DP, the recommended range of RAID group size is between 20 and 28.

### **Customize the size of your RAID groups**

You can customize the size of your RAID groups to ensure that your RAID group sizes are appropriate for the amount of storage you plan to include for an aggregate.

#### **About this task**

For standard aggregates, you change the size of RAID groups on a per-aggregate basis. For Flash Pool aggregates, you can change the RAID group size for the SSD RAID groups and the HDD RAID groups independently.

The following list outlines some facts about changing the RAID group size:

- By default, if the number of disks or array LUNs in the most recently created RAID group is less than the new RAID group size, disks or array LUNs will be added to the most recently created RAID group until it reaches the new size.
- All other existing RAID groups in that aggregate remain the same size, unless you explicitly add disks to them.
- You can never cause a RAID group to become larger than the current maximum RAID group size for the aggregate.
- You cannot decrease the size of already created RAID groups.
- The new size applies to all RAID groups in that aggregate (or, in the case of a Flash Pool aggregate, all RAID groups for the affected RAID group type—SSD or HDD).

### **Steps**

1. Use the applicable command:

If you want to...	Enter the following command...
Change the maximum RAID group size for the SSD RAID groups of a Flash Pool aggregate	<code>storage aggregate modify -aggregate aggr_name -cache-raid-group-size size</code>
Change the maximum size of any other RAID groups	<code>storage aggregate modify -aggregate aggr_name -maxraidspace size</code>

## Examples

The following command changes the maximum RAID group size of the aggregate `n1_a4` to 20 disks or array LUNs:

```
storage aggregate modify -aggregate n1_a4 -maxraidspace 20
```

The following command changes the maximum RAID group size of the SSD cache RAID groups of the Flash Pool aggregate `n1_cache_a2` to 24:

```
storage aggregate modify -aggregate n1_cache_a2 -cache-raid-group-size 24
```

## Mirrored and unmirrored aggregates

### Mirrored and unmirrored aggregates

You can use an optional feature called *SyncMirror* to synchronously mirror aggregate data in copies, or *plexes*, stored in different RAID groups. Plexes ensure against data loss if more disks fail than the RAID type protects against, or if there is a loss of connectivity to RAID group disks.

### How unmirrored aggregates work

Unless you are using *SyncMirror*, all of your aggregates are unmirrored. Unmirrored aggregates have only one *plex* (copy of their data), which contains all of the RAID groups belonging to that aggregate.

The following diagram shows an unmirrored aggregate composed of disks, with its one plex. The aggregate has four RAID groups: `rg0`, `rg1`, `rg2`, and `rg3`. Each RAID group has 6 data disks, one parity disk, and one *dparity* (double parity) disk. All disks used by the aggregate come from the same pool, `pool0`.



The following diagram shows an unmirrored aggregate with array LUNs, with its one plex. It has two RAID groups, rg0 and rg1. All array LUNs used by the aggregate come from the same pool, pool0.



### How mirrored aggregates work

Mirrored aggregates have two *plexes* (copies of their data), which use the SyncMirror functionality to duplicate the data to provide redundancy.

When a mirrored aggregate is created (or when a second plex is added to an existing unmirrored aggregate), ONTAP copies the data in the original plex (plex0) to the new plex (plex1). The plexes are physically separated (each plex has its own RAID groups and its own pool), and the plexes are updated simultaneously. This provides added protection against data loss if more disks fail than the RAID level of the aggregate protects

against or there is a loss of connectivity, because the unaffected plex continues to serve data while you fix the cause of the failure. After the plex that had a problem is fixed, the two plexes resynchronize and reestablish the mirror relationship.

The disks and array LUNs on the system are divided into two pools: pool0 and pool1. Plex0 gets its storage from pool0 and plex1 gets its storage from pool1.

The following diagram shows an aggregate composed of disks with the SyncMirror functionality enabled and implemented. A second plex has been created for the aggregate, plex1. The data in plex1 is a copy of the data in plex0, and the RAID groups are also identical. The 32 spare disks are allocated to pool0 or pool1, 16 disks for each pool.



The following diagram shows an aggregate composed of array LUNs with the SyncMirror functionality enabled and implemented. A second plex has been created for the aggregate, plex1. Plex1 is a copy of plex0, and the RAID groups are also identical.



# FabricPool tier management with System Manager

## FabricPool tier management overview with System Manager

The topics in this section show you how to configure and manage a FabricPool cloud tier with System Manager in ONTAP 9.7 and later releases.

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

### Tier Data and Lower Costs Use Case video



### Add a connection to the cloud

Beginning 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 with ONTAP 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.

Starting August 21, 2021, a new Cloud Tiering BYOL licensing was introduced for tiering configurations that are supported within Cloud Manager using the Cloud Tiering service. [Learn more about installing a FabricPool license](#).

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.



## Install a FabricPool license

The FabricPool license you might have used in the past is changing and is being retained only for configurations that aren't supported within Cloud Manager. Starting August 21, 2021, a new Cloud Tiering BYOL licensing was introduced for tiering configurations that are supported within Cloud Manager using the Cloud Tiering service.

[Learn more about the new Cloud Tiering BYOL licensing.](#)

Configurations that are supported by Cloud Manager must use the Digital Wallet page in Cloud Manager to license tiering for ONTAP clusters. This requires you to set up a Cloud Manager account and set up tiering for the particular object storage provider you plan to use. Cloud Manager currently supports tiering to the following object storage: Amazon S3, Azure Blob storage, Google Cloud Storage, S3-compatible object storage, and StorageGRID.

[Learn more about the Cloud tiering service.](#)

You can download and activate a FabricPool license using System Manager if you have one of the configurations that is not supported within Cloud Manager:

- ONTAP installations in the GovCloud or in Dark Sites
- ONTAP cluster in a MetroCluster configuration
- ONTAP clusters using FabricPool Mirror functionality
- ONTAP clusters that are tiering data to IBM Cloud Object Storage or Alibaba Cloud Object Storage

The FabricPool license is a cluster-wide license. It includes an entitled usage limit that you purchase for object storage that is associated with FabricPool in the cluster. The usage across the cluster must not exceed the

capacity of the entitled usage limit. If you need to increase the usage limit of the license, you should contact your sales representative.

FabricPool licenses are available in perpetual or term-based, 1- or 3- year, formats.

A term-based FabricPool license with 10 TB of free capacity is available for first time FabricPool orders for existing clusters configurations not supported within Cloud Manager. Free capacity is not available with perpetual licenses.

A license is not required if you use NetApp StorageGRID or ONTAP S3 for the cloud tier. Cloud Volumes ONTAP does not require a FabricPool license, regardless of the provider you are using.

This task is supported only by uploading the license file to the cluster using System Manager.

### Steps

1. Download the NetApp License File (NLF) for the FabricPool license from the [NetApp Support Site](#).
2. Perform the following actions using System Manager to upload the FabricPool license to the cluster:
  - a. In the **Cluster Settings** pane, on the **Licenses** card, click .
  - b. On the **License** page, click  **Add**.
  - c. In the **Add License** dialog box, click **Browse** to select the NLF you downloaded, and then click **Add** to upload the file to the cluster.

## 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

Beginning with ONTAP 9.8, you can use System Manager to 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

Beginning with ONTAP 9.8, you use System Manager to 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**.

## FabricPool tier management with the CLI

### FabricPool tier management with the CLI overview

You can configure and manage data in storage tiers using FabricPool, depending on how frequently you access the data.

Storing data in tiers can enhance the efficiency of your storage system. Beginning with ONTAP 9.2, you can manage storage tiers by using FabricPool. It enables you to store data in a tier, based on whether the data is frequently accessed.

Perform these tasks if the following are true:

- You want to use the command-line interface (CLI), not System Manager or an automated scripting tool.
- You want to use best practices, not explore every available option.

### Related information

See also the [NetApp Cloud Tiering](#) documentation.

## Benefits of storage tiers by using FabricPool

Configuring an aggregate to use FabricPool enables you to use storage tiers. You can efficiently balance the performance and cost of your storage system, monitor and optimize the space utilization, and perform policy-based data movement between storage tiers.

- You can optimize storage performance and reduce storage cost by storing data in a tier based on whether the data is frequently accessed.
  - Frequently accessed (“hot”) data is stored in the *performance tier*.

The performance tier uses high-performance primary storage, such as an all flash (all SSD) aggregate of the storage system.

- Infrequently accessed (“cold”) data is stored in the *cloud tier*, also known as the *capacity tier*.

The cloud tier uses an object store that is less costly and does not require high performance.

- You have the flexibility in specifying the tier in which data should be stored.

You can specify one of the supported tiering policy options at the volume level. The options enable you to efficiently move data across tiers as data becomes hot or cold.

#### Types of FabricPool tiering policies

- You can choose one of the supported object stores to use as the cloud tier for FabricPool.
- You can monitor the space utilization in a FabricPool-enabled aggregate.
- You can see how much data in a volume is inactive by using inactive data reporting.
- You can reduce the on-premise footprint of the storage system.

You save physical space when you use a cloud-based object store for the cloud tier.

## Considerations and requirements for using FabricPool

You should familiarize yourself with a few considerations and requirements about using FabricPool.

### General considerations and requirements

- You must be running ONTAP 9.2 at the minimum to use FabricPool.
- You must be running ONTAP 9.4 or later releases for the following FabricPool functionality:
  - The `auto` tiering policy

#### Types of FabricPool tiering policies

- Specifying the tiering minimum cooling period
- Inactive data reporting
- Using Microsoft Azure Blob Storage for the cloud as the cloud tier for FabricPool
- Using FabricPool with ONTAP Select
- You must be running ONTAP 9.5 or later releases for the following FabricPool functionality:
  - Specifying the tiering fullness threshold
  - Using IBM Cloud Object Storage as the cloud tier for FabricPool
  - NetApp Volume Encryption (NVE) of the cloud tier, enabled by default.
- You must be running ONTAP 9.6 or later releases for the following FabricPool functionality:
  - The `all` tiering policy
  - Inactive data reporting enabled manually on HDD aggregates
  - Inactive data reporting enabled automatically for SSD aggregates when you upgrade to ONTAP 9.6 and at time aggregate is created, except on low end systems with less than 4 CPU, less than 6 GB of RAM, or when WAFL-buffer-cache size is less than 3 GB.

ONTAP monitors system load, and if the load remains high for 4 continuous minutes, IDR is disabled, and is not automatically enabled. You can reenabling IDR manually, however, manually enabled IDR is not automatically disabled.

- Using Alibaba Cloud Object Storage as the cloud tier for FabricPool
- Using Google Cloud Platform as the cloud tier for FabricPool
- Volume move without cloud tier data copy
- You must be running ONTAP 9.7 or later releases for the following FabricPool functionality:
  - Non transparent HTTP and HTTPS proxy to provide access to only whitelisted access points, and to provide auditing and reporting capabilities.
  - FabricPool mirroring to tier cold data to two object stores simultaneously
  - FabricPool mirrors on MetroCluster configurations
  - NDMP dump and restore enabled by default on FabricPool attached aggregates.



If the backup application uses a protocol other than NDMP, such as NFS or SMB, all data being backed up in the performance tier becomes hot and can affect tiering of that data to the cloud tier. Non-NDMP reads can cause data migration from the cloud tier back to the performance tier.

### NDMP Backup and Restore Support for FabricPool

- You must be running ONTAP 9.8 or later for the following FabricPool functionality:
  - Cloud migration control to enable you to override the default tiering policy
  - Promoting data to the performance tier
  - FabricPool with SnapLock Enterprise
  - Minimum cooling period maximum of 183 days
  - Object tagging using user-created custom tags
  - FabricPools on HDD platforms and aggregates

HDD FabricPools are supported with SAS, FSAS, BSAS and MSATA disks only on systems with 6 or more CPU cores, including the following models:

- FAS9000
- FAS8700
- FAS8300
- FAS8200
- FAS8080
- FAS8060
- FAS8040
- FAS2750
- FAS2720
- FAS2650
- FAS2620

Check [Hardware Universe](#) for the latest supported models.

- FabricPool is supported on all platforms capable of running ONTAP 9.2 except for the following:

- FAS8020
- FAS2554
- FAS2552
- FAS2520

- FabricPool supports the following aggregate types:

- On AFF systems, you can use only all flash (all SSD) aggregates for FabricPool.

You cannot use Flash Pool aggregates (which contain both SSDs and HDDs).

- On FAS systems, you can use either all flash (all SSD) or HDD aggregates for FabricPool.
- On Cloud Volumes ONTAP and ONTAP Select, you can use either SSD or HDD aggregates for FabricPool.

However, using SSD aggregates is recommended.

- FabricPool supports using the following object stores as the cloud tier:

- NetApp StorageGRID 10.3 or later
- NetApp ONTAP S3 (ONTAP 9.8 and later)
- Alibaba Cloud Object Storage
- Amazon Web Services Simple Storage Service (AWS S3)
- Google Cloud Storage
- IBM Cloud Object Storage
- Microsoft Azure Blob Storage for the cloud

- The object store “bucket” (container) you plan to use must have already been set up, must have at least 10 GB of storage space, and must not be renamed.
- HA pairs that use FabricPool require intercluster LIFs to communicate with the object store.
- You cannot detach an object store bucket from the FabricPool configuration after it is attached.
- If you use throughput floors (QoS Min), the tiering policy on the volumes must be set to `none` before the aggregate can be attached to FabricPool.

Other tiering policies prevent the aggregate from being attached to FabricPool.

- You should follow the best practice guidelines for using FabricPool in specific scenarios.

[NetApp Technical Report 4598: FabricPool Best Practices in ONTAP 9](#)

## **Additional considerations when using Cloud Volumes ONTAP**

Cloud Volumes ONTAP does not require a FabricPool license, regardless of the object store provider you are using.

## **Additional considerations for using StorageGRID with FabricPool**

- You need to install a CA certificate for StorageGRID, unless you explicitly disable certificate checking.
- You must not enable StorageGRID object versioning on the object store bucket.

- A FabricPool license is not required.
- If a StorageGRID node is deployed in a virtual machine with storage assigned from a NetApp AFF system, confirm that the volume does not have a FabricPool tiering policy enabled.

Disabling FabricPool tiering for volumes used with StorageGRID nodes simplifies troubleshooting and storage operations.



Never use FabricPool to tier any data related to StorageGRID back to StorageGRID itself. Tiering StorageGRID data back to StorageGRID increases troubleshooting and operational complexity.

### Additional considerations for using Alibaba Cloud Object Storage with FabricPool

- You might need a FabricPool license.

Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool. If you need additional capacity on an AFF system, if you use Alibaba Cloud Object Storage on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

- On AFF and FAS systems and ONTAP Select, FabricPool supports the following Alibaba Object Storage Service classes:
  - Alibaba Object Storage Service Standard
  - Alibaba Object Storage Service Infrequent Access

[Alibaba Cloud: Introduction to storage classes](#)

Contact your NetApp sales representative for information about storage classes not listed.

### Additional considerations for using AWS S3 with FabricPool

- You might need a FabricPool license.
  - Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool.

If you need additional capacity on an AFF system, if you use AWS S3 on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

If you order FabricPool for the first time for an existing cluster, a FabricPool license with 10 TB of free capacity is available.

- The LIF that ONTAP uses to connect with the AWS S3 object server must be on a 10 Gbps port.
- On AFF and FAS systems and ONTAP Select, FabricPool supports the following Amazon S3 storage classes:
  - Amazon S3 Standard
  - Amazon S3 Standard - Infrequent Access (Standard - IA)
  - Amazon S3 One Zone - Infrequent Access (One Zone - IA)
  - Amazon S3 Intelligent-Tiering
  - Amazon Commercial Cloud Services

Contact your sales representative for information about storage classes not listed.

- On Cloud Volumes ONTAP, FabricPool supports tiering from General Purpose SSD (gp2) and Throughput Optimized HDD (st1) volumes of Amazon Elastic Block Store (EBS).

### **Additional considerations for using Google Cloud Storage with FabricPool**

- You might need a FabricPool license.

Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool. If you need additional capacity on an AFF system, if you use Google Cloud Storage on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

- The LIF that ONTAP uses to connect with the Google Cloud Storage object server must be on a 10 Gbps port.
- On AFF and FAS systems and ONTAP Select, FabricPool supports the following Google Cloud Object storage classes:
  - Google Cloud Multi-Regional
  - Google Cloud Regional
  - Google Cloud Nearline
  - Google Cloud Coldline

[Google Cloud: Storage Classes](#)

### **Additional considerations for using IBM Cloud Object Storage with FabricPool**

- You might need a FabricPool license.

Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool. If you need additional capacity on an AFF system, if you use IBM Cloud Object Storage on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

If you order FabricPool for the first time for an existing cluster, a FabricPool license with 10 TB of free capacity is available.

- The LIF that ONTAP uses to connect with the IBM Cloud object server must be on a 10 Gbps port.

### **Additional considerations for using Microsoft Azure Blob Storage with FabricPool**

- You might need a FabricPool license.

Newly ordered AFF systems come with 10 TB of free capacity for using FabricPool. If you need additional capacity on an AFF system, if you use Azure Blob Storage on a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

If you order FabricPool for the first time for an existing cluster, a FabricPool license with 10 TB of free capacity is available.

- A FabricPool license is not required if you are using Azure Blob Storage with Cloud Volumes ONTAP.
- The LIF that ONTAP uses to connect with the Azure Blob Storage object server must be on a 10 Gbps port.

- FabricPool currently does not support Azure Stack, which is on-premises Azure services.
- At the account level in Microsoft Azure Blob Storage, FabricPool supports only hot and cool storage tiers.

FabricPool does not support blob-level tiering. It also does not support tiering to Azure's archive storage tier.

### **Additional considerations for tiering data accessed by SAN protocols**

When tiering data that is accessed by SAN protocols, NetApp recommends using private clouds, like StorageGRID, due to connectivity considerations.

### **Functionality or features not supported by FabricPool**

- Object stores with WORM enabled and object versioning enabled.
- Information lifecycle management (ILM) policies that are applied to object store buckets

ILM typically includes various movement and deletion policies. These policies can be disruptive to the data in the cloud tier of FabricPool. Using FabricPool with ILM policies that are configured on object stores can result in data loss.

- 7-Mode data transition using the ONTAP CLI commands or the 7-Mode Transition Tool
- FlexArray Virtualization
- RAID SyncMirror, except in a MetroCluster configuration
- SnapLock volumes when using ONTAP 9.7 and earlier releases
- Tape backup using SMTape for FabricPool-enabled aggregates
- The Auto Balance functionality
- Volumes using a space guarantee other than `none`

FabricPool does not support attaching a cloud tier to an aggregate that contains volumes using a space guarantee other than `none`. For example, a volume using a space guarantee of `volume (-space -guarantee volume)` is not supported.

- Clusters with DP\_Optimized license
- Flash Pool aggregates

### **About FabricPool tiering policies**

FabricPool tiering policies enable you to move data efficiently across tiers as data becomes hot or cold. Understanding the tiering policies helps you select the right policy that suits your storage management needs.

### **Types of FabricPool tiering policies**

FabricPool tiering policies determine when or whether the user data blocks of a volume in FabricPool are moved to the cloud tier, based on the volume “temperature” of hot (active) or cold (inactive). The volume “temperature” increases when it is accessed frequently and decreases when it is not. Some tiering policies have an associated tiering minimum cooling period, which sets the time that user data in a volume of FabricPool must remain inactive for the data to be considered “cold” and moved to the cloud tier.

The FabricPool tiering policy is specified at the volume level. Four options are available:

- The `snapshot-only` tiering policy (the default) moves user data blocks of the volume Snapshot copies that are not associated with the active file system to the cloud tier.

The tiering minimum cooling period is 2 days. You can modify the default setting for the tiering minimum cooling period with the `-tiering-minimum-cooling-days` parameter in the advanced privilege level of the `volume create` and `volume modify` commands. Valid values are 2 to 183 days using ONTAP 9.8 and later. If you are using a version of ONTAP earlier than 9.8, valid values are 2 to 63 days.

- The `auto` tiering policy, supported only on ONTAP 9.4 and later releases, moves cold user data blocks in both the Snapshot copies and the active file system to the cloud tier.

The default tiering minimum cooling period is 31 days and applies to the entire volume, for both the active file system and the Snapshot copies.

You can modify the default setting for the tiering minimum cooling period with the `-tiering-minimum-cooling-days` parameter in the advanced privilege level of the `volume create` and `volume modify` commands. Valid values are 2 to 183 days.

- The `all` tiering policy, supported only on ONTAP 9.6 and later, moves all user data blocks in both the active file system and Snapshot copies to the cloud tier. It replaces the `backup` tiering policy.

The tiering minimum cooling period does not apply because the data moves the cloud tier as soon as the tiering scan runs, and you cannot modify the setting.

- The `none` tiering policy keeps data of a volume in the performance tier, preventing it from being moved to the cloud tier.

The tiering minimum cooling period does not apply because the data never moves to the cloud tier, and you cannot modify the setting.

The `volume show` command output shows the tiering policy of a volume. A volume that has never been used with FabricPool shows the `none` tiering policy in the output.

### What happens when you modify the tiering policy of a volume in FabricPool

You can modify the tiering policy of a volume by performing a `volume modify` operation. You must understand how changing the tiering policy might affect how long it takes for data to become cold and be moved to the cloud tier.

- Changing the tiering policy from `snapshot-only` or `none` to `auto` causes ONTAP to send user data blocks in the active file system that are already cold to the cloud tier, even if those user data blocks were not previously eligible for the cloud tier.
- Changing the tiering policy to `all` from another policy causes ONTAP to move all user blocks in the active file system and in the Snapshot copies to the cloud tier the next time the tiering scan runs.

Moving blocks back to the performance tier is not allowed.

- Changing the tiering policy from `auto` to `snapshot-only` or `none` does not cause active file system blocks that are already moved to the cloud tier to be moved back to the performance tier.

Volume reads are needed for the data to be moved back to the performance tier.



- Any time you change the tiering policy on a volume, the tiering minimum cooling period is reset to the default value for the policy.

### What happens to the tiering policy when you move a volume

- Unless you explicitly specify a different tiering policy, a volume retains its original tiering policy when it is moved in and out of a FabricPool-enabled aggregate.

However, the tiering policy takes effect only when the volume is in a FabricPool-enabled aggregate.

- The existing value of the `-tiering-minimum-cooling-days` parameter for a volume moves with the volume unless you specify a different tiering policy for the destination.

If you specify a different tiering policy, then the volume uses the default tiering minimum cooling period for that policy. This is the case whether the destination is FabricPool or not.

- You can move a volume across aggregates and at the same time modify the tiering policy.
- You should pay special attention when a `volume move` operation involves the `auto` tiering policy.

Assuming that both the source and the destination are FabricPool-enabled aggregates, the following table summarizes the outcome of a `volume move` operation that involves policy changes related to `auto`:

When you move a volume that has a tiering policy of...	And you change the tiering policy with the move to...	Then after the volume move...
<code>all</code>	<code>auto</code>	All data is moved to the performance tier.
<code>snapshot-only</code> , <code>none</code> , or <code>auto</code>	<code>auto</code>	Data blocks are moved to the same tier of the destination as they previously were on the source.
<code>auto</code> or <code>all</code>	<code>snapshot-only</code>	All data is moved to the performance tier.
<code>auto</code>	<code>all</code>	All user data is moved to the cloud tier.
<code>snapshot-only</code> , <code>auto</code> or <code>all</code>	<code>none</code>	All data is kept at the performance tier.

### What happens to the tiering policy when you clone a volume

- Beginning with ONTAP 9.8, a clone volume always inherits both the tiering policy and the cloud retrieval policy from the parent volume.

In releases earlier than ONTAP 9.8, a clone inherits the tiering policy from the parent except when the parent has the `all` tiering policy.

- If the parent volume has the `never` cloud retrieval policy, its clone volume must have either the `never`

cloud retrieval policy or the `all` tiering policy, and a corresponding cloud retrieval policy `default`.

- The parent volume cloud retrieval policy cannot be changed to `never` unless all its clone volumes have a cloud retrieval policy `never`.

When you clone volumes, keep the following best practices in mind:

- The `-tiering-policy` option and `tiering-minimum-cooling-days` option of the clone only controls the tiering behavior of blocks unique to the clone. Therefore, we recommend using tiering settings on the parent FlexVol that are either move the same amount of data or move less data than any of the clones
- The cloud retrieval policy on the parent FlexVol should either move the same amount of data or should move more data than the retrieval policy of any of the clones

## How tiering policies work with cloud migration

FabricPool cloud data retrieval is controlled by tiering policies that determine data retrieval from the cloud tier to performance tier based on the read pattern. Read patterns can be either sequential or random.

The following table lists the tiering policies and the cloud data retrieval rules for each policy.

Tiering policy	Retrieval behavior
<code>none</code>	Sequential and random reads
<code>snapshot-only</code>	Sequential and random reads
<code>auto</code>	Random reads
<code>all</code>	No data retrieval

Beginning with ONTAP 9.8, the cloud migration control `cloud-retrieval-policy` option overrides the default cloud migration or retrieval behavior controlled by the tiering policy.

The following table lists the supported cloud retrieval policies and their retrieval behavior.

Cloud retrieval policy	Retrieval behavior
<code>default</code>	Tiering policy decides what data should be pulled back, so there is no change to cloud data retrieval with “ <code>default</code> ,” <code>cloud-retrieval-policy</code> . This policy is the default value for any volume regardless of the hosted aggregate type.
<code>on-read</code>	All client-driven data read is pulled from cloud tier to performance tier.
<code>never</code>	No client-driven data is pulled from cloud tier to performance tier

promote

- For tiering policy “none,” all cloud data is pulled from the cloud tier to the performance tier
- For tiering policy “snapshot-only,” AFS data is pulled.

## FabricPool management workflow

You can use the FabricPool workflow diagram to help you plan the configuration and management tasks.



## Configure FabricPool

### Prepare for FabricPool configuration

#### Prepare for FabricPool configuration overview

Configuring FabricPool helps you manage which storage tier (the local performance tier or the cloud tier) data should be stored based on whether the data is frequently accessed.

The preparation required for FabricPool configuration depends on the object store you use as the cloud tier.

#### Install a FabricPool license

Newly ordered AFF systems come with a free 10 TB capacity term-based license for using non-NetApp object stores (AWS S3, Azure Blob Storage, IBM Cloud Object Storage, Alibaba Cloud Object Storage, or Google Cloud Storage) with FabricPool, if you select it. If you need additional capacity on an AFF system, if you plan to use non-NetApp

object stores with a non-AFF system, or if you upgrade from an existing cluster, you need a FabricPool license.

About this task

The FabricPool license is a cluster-wide license. It includes an entitled usage limit that you purchase for the AWS S3, Azure Blob Storage, or IBM Cloud Object Storage, Alibaba Cloud Object Storage, or Google Cloud Storage cloud tier that is associated with FabricPool in the cluster. The usage across the cluster must not exceed the capacity of the entitled usage limit. If you need to increase the usage limit of the license, you should contact your sales representative.

FabricPool licenses are available in perpetual or term-based, 1- or 3- year, formats.

A term-based FabricPool license with 10 TB of free capacity is available for first time FabricPool orders for existing clusters. Free capacity is not available with perpetual licenses.

A license is not required if you use NetApp StorageGRID or ONTAP S3 for the cloud tier. Cloud Volumes ONTAP does not require a FabricPool license, regardless of the provider you are using.

This task is supported only by uploading the license file to the cluster using System Manager.

Steps

- 1. Download the NetApp License File (NLF) for the FabricPool license from the NetApp Support Site.

[NetApp Support](#)

- 2. Use System Manager to upload the FabricPool license to the cluster:
  - a. Depending on the ONTAP release running on your storage system, perform the following action:

If you are running...	Perform the following action:
ONTAP 9.4 or earlier	Click <b>Configuration &gt; Licenses</b> .
ONTAP 9.5 or later	Click <b>Configuration &gt; Cluster &gt; Licenses</b> .

- b. In the **Cluster Settings** pane, click **Licenses**.
    - c. In the **Packages** window, click **Add**.
    - d. In the **Add License Packages** dialog box, click **Choose Files** to select the NLF you downloaded, and then click **Add** to upload the file to the cluster.

Related information

[ONTAP FabricPool \(FP\) Licensing Overview](#)

[NetApp Software License Search](#)

Install a FabricPool license (video)

This video shows a quick overview of using System Manager to install a FabricPool license for non-NetApp object stores such as AWS S3.

[NetApp video: Installing a FabricPool license](#)

## Related information

[NetApp TechComm TV: FabricPool playlist](#)

### Install a CA certificate if you use StorageGRID

Unless you plan to disable certificate checking for StorageGRID, you must install a StorageGRID CA certificate on the cluster so that ONTAP can authenticate with StorageGRID as the object store for FabricPool.

#### About this task

ONTAP 9.4 and later releases enable you to disable certificate checking for StorageGRID.

#### Steps

1. Contact your StorageGRID administrator to obtain the StorageGRID system's CA certificate.
2. Use the `security certificate install` command with the `-type server-ca` parameter to install the StorageGRID CA certificate on the cluster.

The fully qualified domain name (FQDN) you enter must match the custom common name on the StorageGRID CA certificate.

## Related information

[StorageGRID Resources](#)

### Install a CA certificate if you use ONTAP S3

Unless you plan to disable certificate checking for ONTAP S3, you must install a ONTAP S3 CA certificate on the cluster so that ONTAP can authenticate with ONTAP S3 as the object store for FabricPool.

#### Steps

1. Obtain the ONTAP S3 system's CA certificate.
2. Use the `security certificate install` command with the `-type server-ca` parameter to install the ONTAP S3 CA certificate on the cluster.

The fully qualified domain name (FQDN) you enter must match the custom common name on the ONTAP S3 CA certificate.

## Related information

[S3 configuration](#)

### Set up an object store as the cloud tier for FabricPool

#### Set up an object store as the cloud tier for FabricPool

Setting up FabricPool involves specifying the configuration information of the object store (StorageGRID, ONTAP S3, Alibaba Cloud Object Storage, AWS S3, Google Cloud Storage Platform, IBM Cloud Object Storage, or Microsoft Azure Blob Storage for the cloud) that you plan to use as the cloud tier for FabricPool.

## Specify the StorageGRID configuration information

If you are running ONTAP 9.2 or later, you can set up StorageGRID as the cloud tier for FabricPool. When tiering data that is accessed by SAN protocols, NetApp recommends using private clouds, like StorageGRID, due to connectivity considerations.

### About this task

Load balancing is enabled for StorageGRID in ONTAP 9.8 and later. When the server's hostname resolves to more than one IP address, ONTAP establishes client connections with all the IP addresses returned (up to a maximum of 16 IP addresses). The IP addresses are picked up in a round-robin method when connections are established.

### Steps

1. Specify the StorageGRID configuration information by using the `storage aggregate object-store config create` command with the `-provider-type SGWS` parameter.

- The `storage aggregate object-store config create` command fails if ONTAP cannot access StorageGRID with the provided information.
- You use the `-access-key` parameter to specify the access key for authorizing requests to the StorageGRID object store.
- You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the StorageGRID object store.
- If the StorageGRID password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in StorageGRID without interruption.

- Setting the `-is-certificate-validation-enabled` parameter to `false` disables certificate checking for StorageGRID.

```
cluster1::> storage aggregate object-store config create
-object-store-name mySGWS -provider-type SGWS -server mySGWSserver
-container-name mySGWScontainer -access-key mySGWSkey
-secret-password mySGWSpass
```

2. Display and verify the StorageGRID configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the StorageGRID configuration information for FabricPool.

## Attach StorageGRID as a FabricPool cloud tier (video)

This video shows a quick overview of using System Manager to attach a StorageGRID bucket to ONTAP aggregates with FabricPool.

[NetApp video: Attaching StorageGRID Webscale as a FabricPool external capacity tier](#)

### Related information

## Set up ONTAP S3 as the cloud tier

If you are running ONTAP 9.8 or later, you can set up ONTAP S3 as the cloud tier for FabricPool.

### What you'll need

You must have the ONTAP S3 server name and the IP address of its associated LIFs on the remote cluster.

There must be intercluster LIFs on both local and remote clusters.

### Creating intercluster LIFs for remote FabricPool tiering

#### About this task

Load balancing is enabled for ONTAP S3 servers in ONTAP 9.8 and later. When the server's hostname resolves to more than one IP address, ONTAP establishes client connections with all the IP addresses returned (up to a maximum of 16 IP addresses). The IP addresses are picked up in a round-robin method when connections are established.

#### Steps

1. Add entries for the S3 server and LIFs to your DNS server.

Option	Description
If you use an external DNS server	Give the S3 server name and IP addresses to the DNS server administrator.
If you use your local system's DNS hosts table	Enter the following command:  <pre>dns host create -vserver svm_name -address ip_address -hostname s3_server_name</pre>

2. Specify the ONTAP S3 configuration information by using the `storage aggregate object-store config create` command with the `-provider-type ONTAP_S3` parameter.
  - The `storage aggregate object-store config create` command fails if the local ONTAP system cannot access the ONTAP S3 server with the information provided.
  - You use the `-access-key` parameter to specify the access key for authorizing requests to the ONTAP S3 server.
  - You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the ONTAP S3 server.
  - If the ONTAP S3 server password is changed, you should immediately update the corresponding password stored in the local ONTAP system.

Doing so enables access to the data in the ONTAP S3 object store without interruption.

- Setting the `-is-certificate-validation-enabled` parameter to `false` disables certificate checking for ONTAP S3.

```
cluster1::> storage aggregate object-store config create
-object-store-name myS3 -provider-type ONTAP_S3 -server myS3server
-container-name myS3container -access-key myS3key
-secret-password myS3pass
```

3. Display and verify the ONTAP\_S3 configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the ONTAP\_S3 configuration information for FabricPool.

### Set up Alibaba Cloud Object Storage as the cloud tier

If you are running ONTAP 9.6 or later, you can set up Alibaba Cloud Object Storage as the cloud tier for FabricPool.

#### Steps

1. Specify the Alibaba Cloud Object Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type AliCloud` parameter.
  - The `storage aggregate object-store config create` command fails if ONTAP cannot access Alibaba Cloud Object Storage with the provided information.
  - You use the `-access-key` parameter to specify the access key for authorizing requests to the Alibaba Cloud Object Storage object store.
  - If the Alibaba Cloud Object Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in Alibaba Cloud Object Storage without interruption.

```
storage aggregate object-store config create my_ali_oss_store_1
-provider-type AliCloud -server oss-us-east-1.aliyuncs.com
-container-name my-ali-oss-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Display and verify the Alibaba Cloud Object Storage configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the Alibaba Cloud Object Storage configuration information for FabricPool.

### Set up AWS S3 as the cloud tier

If you are running ONTAP 9.2 or later, you can set up AWS S3 as the cloud tier for FabricPool. If you are running ONTAP 9.5 or later, you can set up AWS Commercial Cloud Services (C2S) for FabricPool.

#### Steps



1. Specify the AWS S3 configuration information by using the `storage aggregate object-store config create` command with the `-provider-type AWS_S3` parameter.

- You use the `-auth-type CAP` parameter to obtain credentials for C2S access.

When you use the `-auth-type CAP` parameter, you must use the `-cap-url` parameter to specify the full URL to request temporary credentials for C2S access.

- The `storage aggregate object-store config create` command fails if ONTAP cannot access AWS S3 with the provided information.
- You use the `-access-key` parameter to specify the access key for authorizing requests to the AWS S3 object store.
- You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the AWS S3 object store.
- If the AWS S3 password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in AWS S3 without interruption.

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

```
cluster1::> storage aggregate object-store config create -object
-store-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap
-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&r
ole=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-
bucket
```

2. Display and verify the AWS S3 configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the AWS S3 configuration information for FabricPool.

## Set up AWS S3 as the cloud tier

If you are running ONTAP 9.2 or later, you can set up AWS S3 as the cloud tier for FabricPool. If you are running ONTAP 9.5 or later, you can set up AWS Commercial Cloud Services (C2S) for FabricPool.

### Steps

1. Specify the AWS S3 configuration information by using the `storage aggregate object-store config create` command with the `-provider-type AWS_S3` parameter.

- You use the `-auth-type CAP` parameter to obtain credentials for C2S access.

When you use the `-auth-type CAP` parameter, you must use the `-cap-url` parameter to specify the full URL to request temporary credentials for C2S access.

- The `storage aggregate object-store config create` command fails if ONTAP cannot access AWS S3 with the provided information.
- You use the `-access-key` parameter to specify the access key for authorizing requests to the AWS S3 object store.
- You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the AWS S3 object store.
- If the AWS S3 password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in AWS S3 without interruption.

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

```
cluster1::> storage aggregate object-store config create -object
-store-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap
-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&r
ole=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-
bucket
```

2. Display and verify the AWS S3 configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the AWS S3 configuration information for FabricPool.

### Attach AWS S3 as a FabricPool cloud tier (video)

This video shows a quick overview of using System Manager to attach an AWS S3 bucket to ONTAP aggregates with FabricPool.

[NetApp video: Attaching Amazon S3 as a FabricPool external capacity tier](#)

### Related information

[NetApp TechComm TV: FabricPool playlist](#)

## Set up Google Cloud Storage as the cloud tier

If you are running ONTAP 9.6 or later, you can set up Google Cloud Storage as the cloud tier for FabricPool.

### Steps

1. Specify the Google Cloud Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type GoogleCloud` parameter.
  - The `storage aggregate object-store config create` command fails if ONTAP cannot access Google Cloud Storage with the provided information.
  - You use the `-access-key` parameter to specify the access key for authorizing requests to the Google Cloud Storage object store.
  - If the Google Cloud Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in Google Cloud Storage without interruption.

```
storage aggregate object-store config create my_gcp_store_1 -provider
-type GoogleCloud -container-name my-gcp-bucket1 -access-key
GOOGAUZZUV2USCFGHGQ511I8
```

2. Display and verify the Google Cloud Storage configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the Google Cloud Storage configuration information for FabricPool.

## Set up IBM Cloud Object Storage as the cloud tier

If you are running ONTAP 9.5 or later, you can set up IBM Cloud Object Storage as the cloud tier for FabricPool.

### Steps

1. Specify the IBM Cloud Object Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type IBM_COS` parameter.
  - The `storage aggregate object-store config create` command fails if ONTAP cannot access IBM Cloud Object Storage with the provided information.
  - You use the `-access-key` parameter to specify the access key for authorizing requests to the IBM Cloud Object Storage object store.
  - You use the `-secret-password` parameter to specify the password (secret access key) for authenticating requests to the IBM Cloud Object Storage object store.
  - If the IBM Cloud Object Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in IBM Cloud Object Storage without interruption.

```
storage aggregate object-store config create
-object-store-name MyIBM -provider-type IBM_COS
-server s3.us-east.objectstorage.softlayer.net
-container-name my-ibm-cos-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. Display and verify the IBM Cloud Object Storage configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the IBM Cloud Object Storage configuration information for FabricPool.

## Set up Azure Blob Storage for the cloud as the cloud tier

If you are running ONTAP 9.4 or later, you can set up Azure Blob Storage for the cloud as the cloud tier for FabricPool.

### About this task

FabricPool currently does not support Azure Stack, which is on-premises Azure services.

### Steps

1. Specify the Azure Blob Storage configuration information by using the `storage aggregate object-store config create` command with the `-provider-type Azure_Cloud` parameter.
  - The `storage aggregate object-store config create` command fails if ONTAP cannot access Azure Blob Storage with the provided information.
  - You use the `-azure-account` parameter to specify the Azure Blob Storage account.
  - You use the `-azure-private-key` parameter to specify the access key for authenticating requests to Azure Blob Storage.
  - If the Azure Blob Storage password is changed, you should update the corresponding password stored in ONTAP immediately.

Doing so enables ONTAP to access the data in Azure Blob Storage without interruption.

```
cluster1::> storage aggregate object-store config create
-object-store-name MyAzure -provider-type Azure_Cloud
-server blob.core.windows.net -container-name myAzureContainer
-azure-account myAzureAcct -azure-private-key myAzureKey
```

2. Display and verify the Azure Blob Storage configuration information by using the `storage aggregate object-store config show` command.

The `storage aggregate object-store config modify` command enables you to modify the Azure Blob Storage configuration information for FabricPool.

## Set up object stores for FabricPool in a MetroCluster configuration

If you are running ONTAP 9.7 or later, you can set up a mirrored FabricPool on a MetroCluster configuration to tier cold data to object stores in two different fault zones.

### What you'll need

- The MetroCluster configuration is set up and properly configured.
- Two object stores are set up on the appropriate MetroCluster sites.
- Containers are configured on each of the object stores.
- IP spaces are created or identified on the two MetroCluster configurations and their names match.

### About this task

- FabricPool in MetroCluster requires that the underlying mirrored aggregate and the associated object store configuration must be owned by the same MetroCluster configuration.
- You cannot attach an aggregate to an object store that is created in the remote MetroCluster site.
- You must create object store configurations on the MetroCluster configuration that owns the aggregate.

### Step

1. Specify the object store configuration information on each MetroCluster site by using the `storage object-store config create` command.

In this example, FabricPool is required on only one cluster in the MetroCluster configuration. Two object store configurations are created for that cluster, one for each object store bucket.

```
storage aggregate
  object-store config create -object-store-name mccl-ostore-config-s1
-provider-type SGWS -server
  <SGWS-server-1> -container-name <SGWS-bucket-1> -access-key <key>
-secret-password <password> -encrypt
  <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
  <IPSpace>
```

```
storage aggregate object-store config create -object-store-name mccl-
ostore-config-s2
  -provider-type SGWS -server <SGWS-server-2> -container-name <SGWS-
bucket-2> -access-key <key> -secret-password <password> -encrypt
  <true|false> -provider <provider-type>
  -is-ssl-enabled <true|false> ipspace <IPSpace>
```

This example sets up FabricPool on the second cluster in the MetroCluster configuration.

```
storage aggregate
  object-store config create -object-store-name mcc2-ostore-config-s1
  -provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-3> -access-key <key>
  -secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
  ipspace
    <IPSpace>
```

```
storage aggregate
  object-store config create -object-store-name mcc2-ostore-config-s2
  -provider-type SGWS -server
    <SGWS-server-2> -container-name <SGWS-bucket-4> -access-key <key>
  -secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
  ipspace
    <IPSpace>
```

### Attach the cloud tier to an aggregate

After setting up an object store as the cloud tier, you specify the aggregate to use by attaching it to FabricPool. In ONTAP 9.5 and later, you can also attach aggregates that contain qualified FlexGroup volume constituents.

### What you'll need

When you use the ONTAP CLI to set up an aggregate for FabricPool, the aggregate must already exist.



When you use System Manager to set up an aggregate for FabricPool, you can create the aggregate and set it up to use for FabricPool at the same time.

### Steps

1. **Optional:** To see how much data in a volume is inactive, follow the steps in [Determining how much data in a volume is inactive by using inactive data reporting](#).

Seeing how much data in a volume is inactive can help you decide which aggregate to use for FabricPool.

2. Attach the object store to an aggregate by using the `storage aggregate object-store attach` command.

If the aggregate has never been used with FabricPool and it contains existing volumes, then the volumes are assigned the default `snapshot-only` tiering policy.

```
cluster1::> storage aggregate object-store attach -aggregate myaggr
-object-store-name Amazon01B1
```

You can use the `allow-flexgroup true` option to attach aggregates that contain FlexGroup volume constituents.

3. Display the object store information and verify that the attached object store is available by using the `storage aggregate object-store show` command.

```
cluster1::> storage aggregate object-store show
```

Aggregate	Object Store Name	Availability State
-----	-----	-----
myaggr	Amazon01B1	available

## Manage FabricPool

### Manage FabricPool overview

To help you with your storage tiering needs, ONTAP enables you to display how much data in a volume is inactive, add or move volumes to FabricPool, monitor the space utilization for FabricPool, or modify a volume's tiering policy or tiering minimum cooling period.

### Determine how much data in a volume is inactive by using inactive data reporting

Seeing how much data in a volume is inactive enables you to make good use of storage tiers. Information in inactive data reporting helps you decide which aggregate to use for FabricPool, whether to move a volume in to or out of FabricPool, or whether to modify the tiering policy of a volume.

### What you'll need

You must be running ONTAP 9.4 or later to use the inactive data reporting functionality.

### About this task

- Inactive data reporting is not supported on some aggregates.

You cannot enable inactive data reporting when FabricPool cannot be enabled, including the following instances:

- Root aggregates
- MetroCluster aggregates running ONTAP versions earlier than 9.7
- Flash Pool (hybrid aggregates, or SnapLock aggregates)
- Inactive data reporting is enabled by default on all SSD aggregates in ONTAP 9.6.
- Inactive data reporting is enabled by default on FabricPool aggregate in ONTAP 9.4 and ONTAP 9.5.
- You can enable inactive data reporting on non-FabricPool aggregates using the ONTAP CLI, including HDD aggregates, beginning with ONTAP 9.6.

### Steps

1. If the aggregate for which you want to see inactive data reporting is not used in FabricPool, enable inactive data reporting for the aggregate by using the `storage aggregate modify` command with the `-is-inactive-data-reporting-enabled true` parameter.

```
cluster1::> storage aggregate modify -aggregate aggr1 -is-inactive-data-reporting-enabled true
```

You need to explicitly enable the inactive data reporting functionality on an aggregate that is not used for FabricPool.

You cannot and do not need to enable inactive data reporting on a FabricPool-enabled aggregate because the aggregate already comes with inactive data reporting. The `-is-inactive-data-reporting-enabled` parameter does not work on FabricPool-enabled aggregates.

The `-fields is-inactive-data-reporting-enabled` parameter of the `storage aggregate show` command shows whether inactive data reporting is enabled on an aggregate.

2. To display how much data is inactive on a volume, use the `volume show` command with the `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` parameter.

```
cluster1::> volume show -fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent

vserver volume performance-tier-inactive-user-data performance-tier-inactive-user-data-percent
-----
vsim1    vol0    0B                                0%
vs1      vs1rv1 0B                                0%
vs1      vv1    10.34MB                       0%
vs1      vv2    10.38MB                       0%
4 entries were displayed.
```

- The `performance-tier-inactive-user-data` field displays how much user data stored in the aggregate is inactive.
- The `performance-tier-inactive-user-data-percent` field displays what percent of the data is inactive across the active file system and Snapshot copies.
- For an aggregate that is not used for FabricPool, it takes 31 days after you enable inactive data reporting for ONTAP to display inactive data for the entire volume, regardless of whether a tiering policy has been set or what the tiering policy is.

Until the period is reached, the output shows “-” for the amount of inactive data instead of a value.

- On a volume that is part of FabricPool, what ONTAP reports as inactive depends on the tiering policy that is set on a volume.
  - For the `auto` tiering policy, ONTAP reports the inactive amount of the entire volume for the period



specified by the `-tiering-minimum-cooling-days` parameter in the advanced privilege level of the `volume create` or `volume modify` command.

If no value is set for `-tiering-minimum-cooling-days`, then ONTAP uses the default value (31 days).

- For the `snapshot-only` tiering policy, ONTAP reports the amount of the active file system that is inactive for at least 31 days.
- For the `none` tiering policy, ONTAP reports the amount of the entire volume that is inactive for at least 31 days.
- For the `all` tiering policy, inactive data reporting is not supported.

## Add or move volumes to FabricPool as needed

### Create a volume for FabricPool

You can add volumes to FabricPool by creating new volumes directly in the FabricPool-enabled aggregate or by moving existing volumes from another aggregate to the FabricPool-enabled aggregate.

When you create a volume for FabricPool, you have the option to specify a tiering policy. If no tiering policy is specified, the created volume uses the default `snapshot-only` tiering policy. For a volume with the `snapshot-only` or `auto` tiering policy, you can also specify the tiering minimum cooling period.

### What you'll need

- Setting a volume to use the `auto` tiering policy or specifying the tiering minimum cooling period requires ONTAP 9.4 or later.
- Using FlexGroup volumes requires ONTAP 9.5 or later.
- Setting a volume to use the `all` tiering policy requires ONTAP 9.6 or later.
- Setting a volume to use the `-cloud-retrieval-policy` parameter requires ONTAP 9.8 or later.

### Steps

1. Create a new volume for FabricPool by using the `volume create` command.
  - The `-tiering-policy` optional parameter enables you to specify the tiering policy for the volume.

You can specify one of the following tiering policies:

- `snapshot-only` (default)
- `auto`
- `all`
- `backup` (deprecated)
- `none`

### [Types of FabricPool tiering policies](#)

- The `-cloud-retrieval-policy` optional parameter enables cluster administrators with the advanced privilege level to override the default cloud migration or retrieval behavior controlled by the

tiering policy.

You can specify one of the following cloud retrieval policies:

- `default`

The tiering policy determines what data is pulled back, so there is no change to cloud data retrieval with `default` cloud-retrieval-policy. This means the behavior is the same as in pre-ONTAP 9.8 releases:

- If the tiering policy is `none` or `snapshot-only`, then “default” means that any client-driven data read is pulled from the cloud tier to performance tier.
- If the tiering policy is `auto`, then any client-driven random read is pulled but not sequential reads.
- If the tiering policy is `all` then no client-driven data is pulled from the cloud tier.

- `on-read`

All client-driven data reads are pulled from the cloud tier to performance tier.

- `never`

No client-driven data is pulled from the cloud tier to performance tier

- `promote`

- For tiering policy `none`, all cloud data is pulled from the cloud tier to the performance tier
- For tiering policy `snapshot-only`, all active filesystem data is pulled from the cloud tier to the performance tier.

- The `-tiering-minimum-cooling-days` optional parameter in the advanced privilege level enables you to specify the tiering minimum cooling period for a volume that uses the `snapshot-only` or `auto` tiering policy.

Beginning with ONTAP 9.8, you can specify a value between 2 and 183 for the tiering minimum cooling days. If you are using a version of ONTAP earlier than 9.8, you can specify a value between 2 and 63 for the tiering minimum cooling days.

### Example of creating a volume for FabricPool

The following example creates a volume called “myvol1” in the “myFabricPool” FabricPool-enabled aggregate. The tiering policy is set to `auto` and the tiering minimum cooling period is set to 45 days:

```
cluster1::*> volume create -vserver myVS -aggregate myFabricPool
-volume myvol1 -tiering-policy auto -tiering-minimum-cooling-days 45
```

### Related information

[FlexGroup volumes management](#)

### Move a volume to FabricPool

When you move a volume to FabricPool, you have the option to specify or change the

tiering policy for the volume with the move. Beginning with ONTAP 9.8, when you move a non-FabricPool volume with inactive data reporting enabled, FabricPool uses a heat map to read tierable blocks, and moves cold data to the capacity tier on the FabricPool destination.

### What you'll need

You must understand how changing the tiering policy might affect how long it takes for data to become cold and be moved to the cloud tier.

### What happens to the tiering policy when you move a volume

#### About this task

If a non-FabricPool volume has inactive data reporting enabled, when you move a volume with tiering-policy `auto` or `snapshot-only` to a FabricPool, FabricPool reads the temperature tierable blocks from a heat map file and uses that temperature to move the cold data directly to the capacity tier on the FabricPool destination.

You should not use the `-tiering-policy` option on volume move if you are using ONTAP 9.8 and you want FabricPools to use inactive data reporting information to move data directly to the capacity tier. Using this option causes FabricPools to ignore the temperature data and instead follow the move behavior of releases prior to ONTAP 9.8.

#### Step

1. Use the `volume move start` command to move a volume to FabricPool.

The `-tiering-policy` optional parameter enables you to specify the tiering policy for the volume.

You can specify one of the following tiering policies:

- `snapshot-only` (default)
- `auto`
- `all`
- `none`

### Types of FabricPool tiering policies

#### Example of moving a volume to FabricPool

The following example moves a volume named "myvol2" of the "vs1" SVM to the "dest\_FabricPool" FabricPool-enabled aggregate. The volume is explicitly set to use the `none` tiering policy:

```
cluster1::> volume move start -vserver vs1 -volume myvol2  
-destination-aggregate dest_FabricPool -tiering-policy none
```

### Object tagging using user-created custom tags

#### Object tagging using user-created custom tags overview

Beginning with ONTAP 9.8, FabricPool supports object tagging using user-created custom tags to enable you to classify and sort objects for easier management. If you are

a user with the admin privilege level, you can create new object tags, and modify, delete, and view existing tags.

#### Assign a new tag during volume creation

You can create a new object tag when you want to assign one or more tags to new objects that are tiered from a new volume you create.

#### About this task

- A maximum of 4 tags per volume is allowed
- Each object tag must be a key-value pair separated by an equal sign ("")
- Multiple tags must be separated by a comma ("")
- Each tag value can contain a maximum of 127 characters
- Each tag key must start with either an alphabetic character or an underscore.

Keys must contain only alphanumeric characters and underscores, and the maximum number of characters allowed is 127.

#### Step

1. Use the `volume create` command with the `-tiering-object-tags` option to create a new volume with the specified tags. You can specify multiple tags in comma-separated pairs:

```
volume create [ -vserver <vserver name> ] -volume <volume_name> -tiering
-object-tags <key1=value1> [
    ,<key2=value2>,<key3=value3>,<key4=value4> ]
```

The following example creates a volume named `fp_volume1` with three object tags.

```
vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=abc,content=data
```

#### Modify an existing tag

You can change the name of a tag, replace tags on existing objects in the object store, or add a different tag to new objects that you plan to add later.

#### About this task

Using the `volume modify` command with the `-tiering-object-tags` option replaces existing tags with the new value you provide.

#### Step

1. Use the `volume modify` command with the `-tiering-object-tags` option to modify an existing tag.

```
volume modify [ -vserver <vserver name> ] -volume <volume_name> -tiering
-object-tags <key1=value1> [ ,<key2=value2> ,
<key3=value3>,<key4=value4> ]
```

The following example changes the name of the existing tag type=abc to type=xyz.

```
vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=xyz,content=data
```

### Delete a tag

You can delete object tags when you no longer want them set on a volume or on objects in the object store.

#### Step

1. Use the `volume modify` command with the `-tiering-object-tags` option followed by an empty value (`""`) to delete an existing tag.

The following example deletes the existing tags on `fp_volume1`.

```
vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags ""
```

### View existing tags on a volume

You can view the existing tags on a volume to see what tags are available before appending new tags to the list.

#### Step

1. Use the `volume show` command with the `-tiering-object-tags` option to view existing tags on a volume.

```
volume show [ -vserver <vserver name> ] -volume <volume_name> -fields
-tiering-object-tags
```

### Check object tagging status on FabricPool volumes

You can check if tagging is complete on one or more FabricPool volumes.

#### Step

1. Use the `vol show` command with the `-fieldsneeds-object-retagging` option to see if tagging is in progress, if it has completed, or if tagging is not set.

```
vol show -fields needs-object-retagging [ -instance | -volume <volume
name>]
```

One of the following values is displayed:

- `true` — the object tagging scanner has not yet to run or needs to run again for this volume
- `false` — the object tagging scanner has completed tagging for this volume
- `<->` — the object tagging scanner is not applicable for this volume. This happens for volumes that are not residing on FabricPools.

## Monitor the space utilization for FabricPool

You need to know how much data is stored in the performance and cloud tiers for FabricPool. That information helps you determine whether you need to change the tiering policy of a volume, increase the FabricPool licensed usage limit, or increase the storage space of the cloud tier.

### Steps

1. Monitor the space utilization for FabricPool-enabled aggregates by using one of the following commands to display the information:

If you want to display...	Then use this command:
The used size of the cloud tier in an aggregate	<code>storage aggregate show</code> with the <code>-instance</code> parameter
Details of space utilization within an aggregate, including the object store's referenced capacity	<code>storage aggregate show-space</code> with the <code>-instance</code> parameter
Space utilization of the object stores that are attached to the aggregates, including how much license space is being used	<code>storage aggregate object-store show-space</code>
A list of volumes in an aggregate and the footprints of their data and metadata	<code>volume show-footprint</code>

In addition to using CLI commands, you can use Active IQ Unified Manager (formerly OnCommand Unified Manager), along with FabricPool Advisor, which is supported on ONTAP 9.4 and later clusters, or System Manager to monitor the space utilization.

The following example shows ways of displaying space utilization and related information for FabricPool:

```
cluster1::> storage aggregate show-space -instance
```

```
Aggregate: MyFabricPool
...
Aggregate Display Name:
MyFabricPool
...
Total Object Store Logical Referenced
Capacity: -
Object Store Logical Referenced Capacity
Percentage: -
...
Object Store
Size: -
Object Store Space Saved by Storage
Efficiency: -
Object Store Space Saved by Storage Efficiency
Percentage: -
Total Logical Used
Size: -
Logical Used
Percentage: -
Logical Unreferenced
Capacity: -
Logical Unreferenced
Percentage: -
```

```
cluster1::> storage aggregate show -instance
```

```
Aggregate: MyFabricPool
...
Composite: true
Capacity Tier Used Size:
...
```

```
cluster1::> volume show-footprint
```

```
Vserver : vs1
```

```
Volume : rootvol
```

Feature	Used	Used%
Volume Footprint	KB	%
Volume Guarantee	MB	%
Flexible Volume Metadata	KB	%
Delayed Frees	KB	%
Total Footprint	MB	%

```
Vserver : vs1
```

```
Volume : vol
```

Feature	Used	Used%
Volume Footprint	KB	%
Footprint in Performance Tier	KB	%
Footprint in Amazon01	KB	%
Flexible Volume Metadata	MB	%
Delayed Frees	KB	%
Total Footprint	MB	%
...		

2. Take one of the following actions as needed:

If you want to...	Then...
Change the tiering policy of a volume	Follow the procedure in <a href="#">Managing storage tiering by modifying a volume's tiering policy or tiering minimum cooling period</a> .
Increase the FabricPool licensed usage limit	Contact your NetApp or partner sales representative.  <a href="#">NetApp Support</a>
Increase the storage space of the cloud tier	Contact the provider of the object store that you use for the cloud tier.

### Manage storage tiering by modifying a volume's tiering policy or tiering minimum cooling period

You can change the tiering policy of a volume to control whether data is moved to the cloud tier when it becomes inactive (*cold*). For a volume with the `snapshot-only` or



`auto` tiering policy, you can also specify the tiering minimum cooling period that user data must remain inactive before it is moved to the cloud tier.

### What you'll need

Changing a volume to the `auto` tiering policy or modifying the tiering minimum cooling period requires ONTAP 9.4 or later.

### About this task

Changing the tiering policy of a volume changes only the subsequent tiering behavior for the volume. It does not retroactively move data to the cloud tier.

Changing the tiering policy might affect how long it takes for data to become cold and be moved to the cloud tier.

### What happens when you modify the tiering policy of a volume in FabricPool

#### Steps

1. Modify the tiering policy for an existing volume by using the `volume modify` command with the `-tiering-policy` parameter:

You can specify one of the following tiering policies:

- `snapshot-only` (default)
- `auto`
- `all`
- `none`

#### Types of FabricPool tiering policies

2. If the volume uses the `snapshot-only` or `auto` tiering policy and you want to modify the tiering minimum cooling period, use the `volume modify` command with the `-tiering-minimum-cooling-days` optional parameter in the advanced privilege level.

You can specify a value between 2 and 183 for the tiering minimum cooling days. If you are using a version of ONTAP earlier than 9.8, you can specify a value between 2 and 63 for the tiering minimum cooling days.

### Example of modifying the tiering policy and the tiering minimum cooling period of a volume

The following example changes the tiering policy of the volume “myvol” in the SVM “vs1” to `auto` and the tiering minimum cooling period to 45 days:

```
cluster1::> volume modify -vserver vs1 -volume myvol  
-tiering-policy auto -tiering-minimum-cooling-days 45
```

### Archive volumes with FabricPool (video)

This video shows a quick overview of using System Manager to archive a volume to a cloud tier with FabricPool.

## Related information

[NetApp TechComm TV: FabricPool playlist](#)

### Use cloud migration controls to override a volume's default tiering policy

You can change a volume's default tiering policy for controlling user data retrieval from the cloud tier to performance tier by using the `-cloud-retrieval-policy` option introduced in ONTAP 9.8.

#### What you'll need

- Modifying a volume using the `-cloud-retrieval-policy` option requires ONTAP 9.8 or later.
- You must have the advanced privilege level to perform this operation.
- You should understand the behavior of tiering policies with `-cloud-retrieval-policy`.

[How tiering policies work with cloud migration](#)

#### Step

1. Modify the tiering policy behavior for an existing volume by using the `volume modify` command with the `-cloud-retrieval-policy` option:

```
volume create -volume <volume_name> -vserver <vserver_name> - tiering-  
policy <policy_name> -cloud-retrieval-policy
```

```
vol modify -volume fp_volume4 -vserver vs0 -cloud-retrieval-policy  
promote
```

### Promote data to the performance tier

#### Promote data to the performance tier overview

Beginning with ONTAP 9.8, if you are a cluster administrator at the advanced privilege level, you can proactively promote data to the performance tier from the cloud tier using a combination of the `tiering-policy` and the `cloud-retrieval-policy` setting.

#### About this task

You might do this if you want to stop using FabricPool on a volume, or if you have a `snapshot-only` tiering policy and you want to bring restored Snapshot copy data back to the performance tier.

#### Promote all data from a FabricPool volume to the performance tier

You can proactively retrieve all data on a FabricPool volume in the Cloud and promote it to the performance tier.

### Step

1. Use the `volume modify` command to set `tiering-policy` to `none` and `cloud-retrieval-policy` to `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy none -cloud-retrieval-policy promote
```

### Promote file system data to the performance tier

You can proactively retrieve active file system data from a restored Snapshot copy in the cloud tier and promote it to the performance tier.

### Step

1. Use the `volume modify` command to set `tiering-policy` to `snapshot-only` and `cloud-retrieval-policy` to `promote`.

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy snapshot-only cloud-retrieval-policy promote
```

### Check the status of a performance tier promotion

You can check the status of performance tier promotion to determine when the operation is complete.

### Step

1. Use the `volume object-store` command with the `tiering` option to check the status of the performance tier promotion.

```
volume object-store tiering show [ -instance | -fields <fieldname>, ...
] [ -vserver <vserver name> ] *Vserver
[[-volume] <volume name>] *Volume [ -node <nodename> ] *Node Name [ -vol
-dsid <integer> ] *Volume DSID
[ -aggregate <aggregate name> ] *Aggregate Name
```

```

volume object-store tiering show v1 -instance

Vserver: vs1
Volume: v1
Node Name: node1
Volume DSID: 1023
Aggregate Name: a1
State: ready
Previous Run Status: completed
Aborted Exception Status: -
Time Scanner Last Finished: Mon Jan 13 20:27:30 2020
Scanner Percent Complete: -
Scanner Current VBN: -
Scanner Max VBNs: -
Time Waiting Scan will be scheduled: -
Tiering Policy: snapshot-only
Estimated Space Needed for Promotion: -
Time Scan Started: -
Estimated Time Remaining for scan to complete: -
Cloud Retrieve Policy: promote

```

### Trigger scheduled migration and tiering

You can trigger a tiering scan request at any time when you prefer not to wait for the default tiering scan.

#### Step

1. Use the `volume object-store` command with the `trigger` option to request migration and tiering.

```

volume object-store tiering trigger [ -vserver <vserver name> ] *VServer
Name [-volume] <volume name> *Volume Name

```

## Manage FabricPool mirrors

### Manage FabricPool mirrors overview

To ensure data is accessible in data stores in the event of a disaster, and to enable you to replace a data store, you can configure a FabricPool mirror by adding a second data store to synchronously tier data to two data stores . You can add a second data store to new or existing FabricPool configurations, monitor the mirror status, display FabricPool mirror details, promote a mirror, and remove a mirror. You must be running ONTAP 9.7 or later.

## Create a FabricPool mirror

To create a FabricPool mirror, you attach two object stores to a single FabricPool. You can create a FabricPool mirror either by attaching a second object store to an existing, single object store FabricPool configuration, or you can create a new, single object store FabricPool configuration and then attach a second object store to it. You can also create FabricPool mirrors on MetroCluster configurations.

### What you'll need

- You must have already created the two object stores using the `storage aggregate object-store config` command.
- If you are creating FabricPool mirrors on MetroCluster configurations:
  - You must have already set up and configured the MetroCluster
  - You must have created the object store configurations on the selected cluster.

If you are creating FabricPool mirrors on both clusters in a MetroCluster configuration, you must have created object store configurations on both of the clusters.

- If you are not using on premises object stores for MetroCluster configurations, you should ensure that one of the following scenarios exists:
  - Object stores are in different availability zones
  - Object stores are configured to keep copies of objects in multiple availability zones

[Setting up object stores for FabricPool in a MetroCluster configuration](#)

### About this task

The object store you use for the FabricPool mirror must be different from the primary object store.

The procedure for creating a FabricPool mirror is the same for both MetroCluster and non-MetroCluster configurations.

### Steps

1. If you are not using an existing FabricPool configuration, create a new one by attaching an object store to an aggregate using the `storage aggregate object-store attach` command.

This example creates a new FabricPool by attaching an object store to an aggregate.

```
cluster1::> storage aggregate object-store attach -aggregate aggr1 -name my-store-1
```

2. Attach a second object store to the aggregate using the `storage aggregate object-store mirror` command.

This example attaches a second object store to an aggregate to create a FabricPool mirror.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name
my-store-2
```

## Monitor FabricPool mirror resync status

When you replace a primary object store with a mirror, you might have to wait for the mirror to resync with the primary data store.

### About this task

If the FabricPool mirror is in sync, no entries are displayed.

### Step

1. Monitor mirror resync status using the `storage aggregate object-store show-resync-status` command.

```
aggregate1::> storage aggregate object-store show-resync-status
-aggregate aggr1
```

Aggregate	Primary	Mirror	Complete Percentage
-----	-----	-----	-----
aggr1	my-store-1	my-store-2	40%

## Display FabricPool mirror details

You can display details about a FabricPool mirror to see what object stores are in the configuration and whether the object store mirror is in sync with the primary object store.

### Step

1. Display information about a FabricPool mirror using the `storage aggregate object-store show` command.

This example displays the details about the primary and mirror object stores in a FabricPool mirror.

```
cluster1::> storage aggregate object-store show
```

Aggregate	Object Store Name	Availability	Mirror Type
-----	-----	-----	-----
aggr1	my-store-1	available	primary
	my-store-2	available	mirror

This example displays details about the FabricPool mirror, including whether the mirror is degraded due to a resync operation.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
aggr1	my-store-1	primary	-
	my-store-2	mirror	false

### Promote a FabricPool mirror

You can reassign the object store mirror as the primary object store by promoting it. When the object store mirror becomes the primary, the original primary automatically becomes the mirror.

#### What you'll need

- The FabricPool mirror must be in sync
- The object store must be operational

#### About this task

You can replace the original object store with an object store from a different cloud provider. For instance, your original mirror might be an AWS object store, but you can replace it with an Azure object store.

#### Step

1. Promote an object store mirror by using the `storage aggregate object-store modify -aggregate` command.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name my-store-2 -mirror-type primary
```

### Remove a FabricPool mirror

You can remove a FabricPool mirror if you no longer need to replicate an object store.

#### What you'll need

The primary object store must be operational, otherwise, the command fails.

#### Step

1. Remove an object store mirror in a FabricPool by using the `storage aggregate object-store unmirror -aggregate` command.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

## Replace an existing object store using a FabricPool mirror

You can use FabricPool mirror technology to replace one object store with another one. The new object store does not have to use the same cloud provider as the original object store.

### About this task

You can replace the original object store with an object store that uses a different cloud provider. For instance, your original object store might use AWS as the cloud provider, but you can replace it with an object store that uses Azure as the cloud provider, and vice versa. However, the new object store must retain the same object size as the original.

### Steps

1. Create a FabricPool mirror by adding a new object store to an existing FabricPool using the `storage aggregate object-store mirror` command.

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name my-AZURE-store
```

2. Monitor the mirror resync status using the `storage aggregate object-store show-resync-status` command.

```
cluster1::> storage aggregate object-store show-resync-status -aggregate aggr1
```

Aggregate	Primary	Mirror	Complete Percentage
-----	-----	-----	-----
aggr1	my-AWS-store	my-AZURE-store	40%

3. Verify the mirror is in sync using the `storage aggregate object-store> show -fields mirror-type,is-mirror-degraded` command.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-mirror-degraded
```



aggregate	object-store-name	mirror-type	is-mirror-degraded
-----	-----	-----	-----
aggr1	my-AWS-store	primary	-
	my-AZURE-store	mirror	false

4. Swap the primary object store with the mirror object store using the `storage aggregate object-store modify` command.

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name
my-AZURE-store -mirror-type primary
```

5. Display details about the FabricPool mirror using the `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` command.

This example displays the information about the FabricPool mirror, including whether the mirror is degraded (not in sync).

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-
mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
-----	-----	-----	-----
aggr1	my-AZURE-store	primary	-
	my-AWS-store	mirror	false

6. Remove the FabricPool mirror using the `storage aggregate object-store unmirror` command.

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

7. Verify that the FabricPool is back in a single object store configuration using the `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` command.

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
-----	-----	-----	-----
aggr1	my-AZURE-store	primary	-

## Replace a FabricPool mirror on a MetroCluster configuration

If one of the object stores in a FabricPool mirror is destroyed or becomes permanently unavailable on a MetroCluster configuration, you can make the object store the mirror if it is not the mirror already, remove the damaged object store from FabricPool mirror, and then add a new object store mirror to the FabricPool.

### Steps

1. If the damaged object store is not already the mirror, make the object store the mirror with the `storage aggregate object-store modify` command.

```
storage aggregate object-store modify -aggregate -aggregate fp_aggr1_A01
-name mccl_ostore1 -mirror-type mirror
```

2. Remove the object store mirror from the FabricPool by using the `storage aggregate object-store unmirror` command.

```
storage aggregate object-store unmirror -aggregate <aggregate name>
-name mccl_ostore1
```

3. You can force tiering to resume on the primary data store after you remove the mirror data store by using the `storage aggregate object-store modify` with the `-force-tiering-on-metrocluster true` option.

The absence of a mirror interferes with the replication requirements of a MetroCluster configuration.

```
storage aggregate object-store modify -aggregate <aggregate name> -name
mccl_ostore1 -force-tiering-on-metrocluster true
```

4. Create a replacement object store by using the `storage aggregate object-store config create` command.

```
storage aggregate object-store config create -object-store-name
mccl_ostore3 -cluster clusterA -provider-type SGWS -server <SGWS-server-
1> -container-name <SGWS-bucket-1> -access-key <key> -secret-password
<password> -encrypt <true|false> -provider <provider-type> -is-ssl
-enabled <true|false> ipspace <IPSpace>
```

5. Add the object store mirror to the FabricPool mirror using the `storage aggregate object-store mirror` command.

```
storage aggregate object-store mirror -aggregate aggr1 -name
mcc1_ostore3-mc
```

6. Display the object store information using the `storage aggregate object-store show` command.

```
storage aggregate object-store show -fields mirror-type,is-mirror-
degraded
```

aggregate	object-store-name	mirror-type	is-mirror-degraded
-----	-----	-----	-----
aggr1	mcc1_ostore1-mc	primary	-
	mcc1_ostore3-mc	mirror	true

7. Monitor the mirror resync status using the `storage aggregate object-store show-resync-status` command.

```
storage aggregate object-store show-resync-status -aggregate aggr1
```

Aggregate	Primary	Mirror	Complete Percentage
-----	-----	-----	-----
aggr1	mcc1_ostore1-mc	mcc1_ostore3-mc	40%

## Commands for managing aggregates with FabricPool

You use the `storage aggregate object-store` commands to manage object stores for FabricPool. You use the `storage aggregate` commands to manage aggregates for FabricPool. You use the `volume` commands to manage volumes for FabricPool.

If you want to...	Use this command:
Define the configuration for an object store so that ONTAP can access it	<code>storage aggregate object-store config create</code>
Modify object store configuration attributes	<code>storage aggregate object-store config modify</code>
Rename an existing object store configuration	<code>storage aggregate object-store config rename</code>

Delete the configuration of an object store	<code>storage aggregate object-store config delete</code>
Display a list of object store configurations	<code>storage aggregate object-store config show</code>
Attach a second object store to a new or existing FabricPool as a mirror	<code>storage aggregate object-store mirror</code> with the <code>-aggregate</code> and <code>-name</code> parameter in the admin privilege level
Remove an object store mirror from an existing FabricPool mirror	<code>storage aggregate object-store unmirror</code> with the <code>-aggregate</code> and <code>-name</code> parameter in the admin privilege level
Monitor FabricPool mirror resync status	<code>storage aggregate object-store show-resync-status</code>
Display FabricPool mirror details	<code>storage aggregate object-store show</code>
Promote an object store mirror to replace a primary object store in a FabricPool mirror configuration	<code>storage aggregate object-store modify</code> with the <code>-aggregate</code> parameter in the admin privilege level
Test the latency and performance of an object store without attaching the object store to an aggregate	<code>storage aggregate object-store profiler start</code> with the <code>-object-store-name</code> and <code>-node</code> parameter in the advanced privilege level
Monitor the object store profiler status	<code>storage aggregate object-store profiler show</code> with the <code>-object-store-name</code> and <code>-node</code> parameter in the advanced privilege level
Abort the object store profiler when it is running	<code>storage aggregate object-store profiler abort</code> with the <code>-object-store-name</code> and <code>-node</code> parameter in the advanced privilege level
Attach an object store to an aggregate for using FabricPool	<code>storage aggregate object-store attach</code>
Attach an object store to an aggregate that contains a FlexGroup volume for using FabricPool	<code>storage aggregate object-store attach</code> with the <code>allow-flexgroup true</code>
Display details of the object stores that are attached to FabricPool-enabled aggregates	<code>storage aggregate object-store show</code>

Display the aggregate fullness threshold used by the tiering scan	<code>storage aggregate object-store show</code> with the <code>-fields tiering-fullness-threshold</code> parameter in the advanced privilege level
Display space utilization of the object stores that are attached to FabricPool-enabled aggregates	<code>storage aggregate object-store show-space</code>
Enable inactive data reporting on an aggregate that is not used for FabricPool	<code>storage aggregate modify</code> with the <code>-is -inactive-data-reporting-enabled true</code> parameter
Display whether inactive data reporting is enabled on an aggregate	<code>storage aggregate show</code> with the <code>-fields is-inactive-data-reporting-enabled</code> parameter
Display information about how much user data is cold within an aggregate	<code>storage aggregate show-space</code> with the <code>-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent</code> parameter
<p>Create a volume for FabricPool, including specifying the following:</p> <ul style="list-style-type: none"> <li>• The tiering policy</li> <li>• The tiering minimum cooling period (for the <code>snapshot-only</code> or <code>auto</code> tiering policy)</li> </ul>	<p><code>volume create</code></p> <ul style="list-style-type: none"> <li>• You use the <code>-tiering-policy</code> parameter to specify the tiering policy.</li> <li>• You use the <code>-tiering-minimum-cooling -days</code> parameter in the advanced privilege level to specify the tiering minimum cooling period.</li> </ul>
<p>Modify a volume for FabricPool, including modifying the following:</p> <ul style="list-style-type: none"> <li>• The tiering policy</li> <li>• The tiering minimum cooling period (for the <code>snapshot-only</code> or <code>auto</code> tiering policy)</li> </ul>	<p><code>volume modify</code></p> <ul style="list-style-type: none"> <li>• You use the <code>-tiering-policy</code> parameter to specify the tiering policy.</li> <li>• You use the <code>-tiering-minimum-cooling -days</code> parameter in the advanced privilege level to specify the tiering minimum cooling period.</li> </ul>
<p>Display FabricPool information related to a volume, including the following:</p> <ul style="list-style-type: none"> <li>• The tiering minimum cooling period</li> <li>• How much user data is cold</li> </ul>	<p><code>volume show</code></p> <ul style="list-style-type: none"> <li>• You use the <code>-fields tiering-minimum-cooling-days</code> parameter in the advanced privilege level to display the tiering minimum cooling period.</li> <li>• You use the <code>-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent</code> parameter to display how much user data is cold.</li> </ul>

Move a volume in to or out of FabricPool	<code>volume move start</code> You use the <code>-tiering -policy</code> optional parameter to specify the tiering policy for the volume.
Modify the threshold for reclaiming unreferenced space (the defragmentation threshold) for FabricPool	<code>storage aggregate object-store modify</code> with the <code>-unreclaimed-space-threshold</code> parameter in the advanced privilege level
Modify the threshold for the percent full the aggregate becomes before the tiering scan begins tiering data for FabricPool  FabricPool continues to tier cold data to a cloud tier until the local tier reaches 98% capacity.	<code>storage aggregate object-store modify</code> with the <code>-tiering-fullness-threshold</code> parameter in the advanced privilege level
Display the threshold for reclaiming unreferenced space for FabricPool	<code>storage aggregate object-store show</code> or <code>storage aggregate object-store show-space</code> command with the <code>-unreclaimed-space -threshold</code> parameter in the advanced privilege level

## SVM data mobility

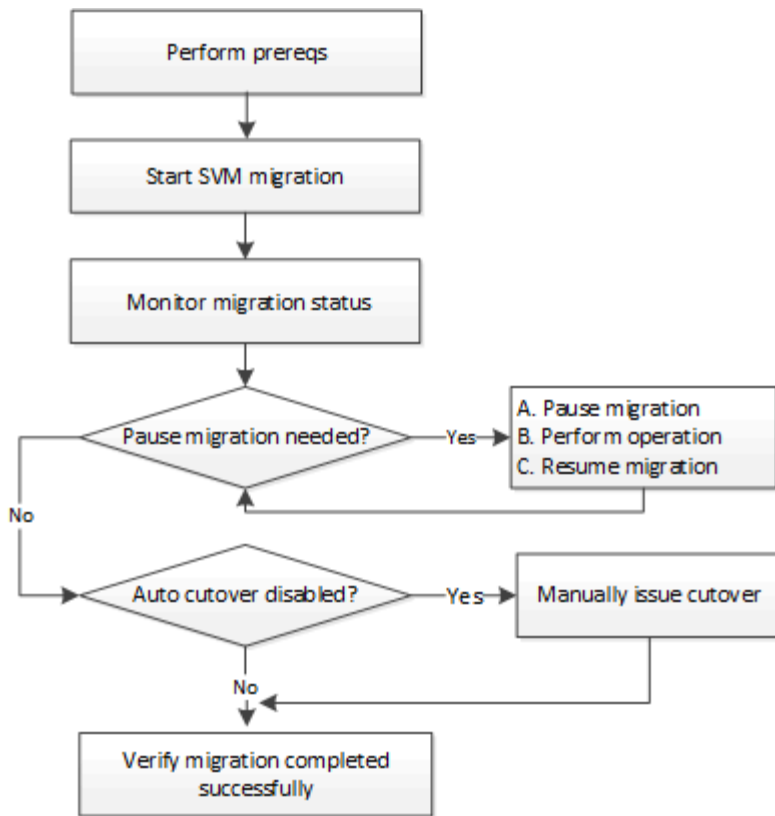
### SVM data mobility overview

Beginning with ONTAP 9.10.1, cluster administrators can non-disruptively relocate an SVM from a source cluster to a destination cluster to manage capacity and load balancing, or to enable equipment upgrades or data center consolidations. The feature is supported only on AFF arrays in ONTAP 9.10.1. iSCSI workloads are not supported.

The SVM's name and UUID remain unchanged after migration, as well as the data LIF name, IP address, and object names, such as the volume name. The UUID of the objects in the SVM will be different.

### SVM migration workflow

The diagram depicts the typical workflow for an SVM migration. You start an SVM migration from the destination cluster. You can monitor the migration from either the source or the destination. You can perform a manual cutover or an automatic cutover. An automatic cutover is performed by default.



## Supported configurations

The following configurations are supported:

- AFF arrays only
- Only two node clusters on the source and on the destination
- Migrate within data centers and a maximum network latency of 2ms

## Prerequisites

- You are a cluster administrator
- The source and destination clusters are peered to each other
- The source and destination clusters have the Data Protection Bundle license installed
- All nodes in the source cluster must be running ONTAP 9.10.1 or later
- All nodes in the source cluster must be running the same ONTAP version
- The destination cluster is at the same or newer effective cluster version (ECV) as the source cluster
- The source and destination clusters are in the same L2 network and must be in the same VLAN
- The source SVM contains fewer than the maximum number of supported data volumes for the release.

In ONTAP 9.10.1, the maximum number of data volumes supported is 100.

- Sufficient space for volume placement is available on the destination
- Onboard Key Manager must be configured on the destination if the source SVM has encrypted volumes

## Conflicting operations

You should check for operations that can conflict with an SVM migration:

- No failover operations are in progress
- WAFLIRON cannot be running
- Fingerprint is not in progress
- SMTape is not in progress
- Vol move, rehost, clone, create, convert or analytics are not running

## Supported features

The following features are supported with ONTAP 9.10.1:

- NFS v3, NFS v4.1, and NFS v4.2 protocols
- NetApp Volume Encryption

## Unsupported features

The following features are not supported with SVM migration:

- iSCSI workloads
- IPv6 LIFs
- SVM migration when the source cluster's Onboard Key Manager (OKM) has Common Criteria (CC) mode enabled
- SVM peering, SnapMirror, data protection volume
- SAN, NVMe over fiber, CIFS, VSCAN, NFS v4.0, vStorage, S3 replication
- Auditing
- NDMP
- VIP/BGP LIF
- IPsec policy
- Anti-ransomware
- Qtree, Quota
- SVM-DR
- External Key Manager at the destination cluster
- SnapMirror
- SnapLock
- FlexGroups
- FlexCache
- FabricPools
- Flash Pool aggregates
- MetroCluster
- System Manager



- Virtual Storage Console for VMware vSphere (VSC is part of the [ONTAP Tools for VMware vSphere virtual appliance](#) beginning with VSC 7.0.)
- Volume clones
- FAS arrays
- Load-sharing mirrors
- Cloud Volumes ONTAP

## Migrate an SVM

After an SVM migration has completed, clients are cut over to the destination cluster automatically and the unnecessary SVM is removed from the source cluster. Automatic cutover and automatic source cleanup are enabled by default. If necessary, you can disable client auto-cutover to suspend the migration before cutover occurs and you can also disable automatic source SVM cleanup.

- You can use the `-auto-cutover false` option to suspend the migration when automatic client cutover normally occurs and then manually perform the cutover later.

### [Manually cutover clients after SVM migration](#)

- You can use the advance privilege `-auto-source-cleanup false` option to disable the removal of the source SVM after cutover and then trigger source cleanup manually later, after cutover.

### [Manually remove source SVM after cutover](#)

## Migrate an SVM with automatic cutover enabled

By default, clients are cut over to the destination cluster automatically when the migration is complete, and the unnecessary SVM is removed from the source cluster.

### Steps

1. From the destination cluster, run the migration prechecks:

```
dest_cluster> vservers migrate start -vservers <vservers name> -source-cluster
<cluster name> -check-only true
```

2. From the destination cluster, start the SVM migration:

```
dest_cluster> vservers migrate start -vservers <vservers name> -source-cluster
<cluster name>
```

3. Check the migration status:

```
dest_cluster> vservers migrate show
```

The status displays `migrate-complete` when the SVM migration is finished.

## Migrate an SVM with automatic client cutover disabled

You can use the `-auto-cutover false` option to suspend the migration when automatic client cutover normally occurs and then manually perform the cutover later. See “Manually cut over clients after SVM migration.”

### Steps

1. From the destination cluster, run the migration prechecks:

```
dest_cluster> vserver migrate start -vserver <vserver name> -source-cluster  
<cluster name> -check-only true
```

2. From the destination cluster, start the SVM migration:

```
dest_cluster> vserver migrate start -vserver <vserver name> -source-cluster  
<cluster name> -auto-cutover false
```

3. Check the migration status:

```
dest_cluster> vserver migrate show
```

The status displays ready-for-cutover when SVM migration completes the asynchronous data transfers, and it is ready for cutover operation.

## Migrate an SVM with source cleanup disabled

You can use the advance privilege `-auto-source-cleanup false` option to disable the removal of the source SVM after cutover and then trigger source cleanup manually later, after cutover. See “Manually clean up source after cutover.”

### Steps

1. From the destination cluster, run the migration prechecks:

```
dest_cluster*> vserver migrate start -vserver <vserver name> -source-cluster  
<cluster name> -check-only true
```

2. From the destination cluster, start the SVM migration:

```
dest_cluster*> vserver migrate start -vserver <vserver name> -source-cluster  
<cluster name> -auto-source-cleanup false
```

3. Check the migration status:

```
dest_cluster*> vserver migrate show
```

The status displays ready-for-source-cleanup when SVM migration cutover is complete, and it is ready to remove the SVM on the source cluster.

## Monitor volume migration

In addition to monitoring the overall SVM migration, you can monitor the migration status of the volumes the SVM contains.

### Steps

1. Check volume migration status:

```
dest_clust> vserver migrate show-volume
```

## Pause and resume SVM migration

You might want to pause an SVM migration before the migration cutover begins. You can pause an SVM migration using the `vserver migrate pause` command.

### Pause migration

You can pause an SVM migration before client cutover starts by using the `vserver migrate pause` command.

#### Steps

1. From the destination cluster, pause the migration:

```
dest_cluster> vserver migrate pause -vserver <vserver name>
```

### Resume migrations

When you're ready to resume a paused SVM migration or when an SVM migration fails, you can use the `vserver migrate resume` command.

#### Step

1. Resume SVM migration:

```
dest_cluster> vserver migrate resume
```

2. Verify that the SVM migration has resumed, and monitor the progress:

```
dest_cluster> vserver migrate show
```

## Cancel an SVM migration

If you need to cancel an SVM migration before it completes, you can use the `vserver migrate abort` command. You can cancel an SVM migration only when the operation is in the paused or failed state. You cannot cancel an SVM migration when the status is "cutover-started" or after cutover is complete. You cannot use the `abort` option when an SVM migration is in progress.

#### Steps

1. Check the migration status:

```
dest_cluster> vserver migrate show -vserver <vserver name>
```

2. Cancel the migration:

```
dest_cluster> vserver migrate abort -vserver <vserver name>
```

Check the progress of the cancel operation:

```
dest_cluster> vserver migrate show
```

The migration status shows migrate-aborting while the cancel operation is in progress. When the cancel operation completes, the migration status shows nothing.

## Manually cut over clients after SVM migration

By default, client cutover to the destination cluster is performed automatically after the SVM migration reaches "ready-for-cutover" state. If you choose to disable automatic client cutover, you need to perform the client cutover manually.

### Steps

1. Manually execute client cutover:

```
dest_cluster> vserver migrate cutover -vserver <vserver name>
```

2. Check the status of the cutover operation:

```
dest_cluster> vserver migrate show
```

## Manually remove source SVM after client cutover

If you performed the SVM migration with source cleanup disabled, you can remove the source SVM manually after client cutover is complete.

### Steps

1. Verify they status is ready for source cleanup:

```
dest_cluster> vserver migrate show
```

2. Clean up the source:

```
dest_cluster> vserver migrate source-cleanup -vserver <vserver_name>
```

# High availability management

## High Availability management overview

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.
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 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...
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.  The default setting is true.	<code>storage failover modify -node <i>nodename</i> -auto-giveback true</code>
Disable automatic giveback. The default setting is true.  <b>Note:</b> Setting this parameter to false does not disable automatic giveback after takeover on panic; automatic giveback after takeover on panic must be disabled by setting the <code>-auto-giveback-after-panic</code> parameter to false.	<code>storage failover modify -node <i>nodename</i> -auto-giveback false</code>

Disable automatic giveback after takeover on panic (this setting is enabled by default).	<code>storage failover modify -node <i>nodename</i> -auto-giveback-after-panic false</code>
Delay automatic giveback for a specified number of seconds (the default is 600). This option determines the minimum time that a node remains in takeover before performing an automatic giveback.	<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
<code>-auto-giveback <i>true</i>   <i>false</i></code>	<i>true</i>
<code>-delay-seconds <i>integer</i> (seconds)</code>	600
<code>-onreboot <i>true</i>   <i>false</i></code>	<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?
<code>-onreboot <i>true</i></code>	reboot command	Yes
<code>-auto-giveback <i>true</i></code>	halt command, or power cycle operation issued from the Service Processor	Yes
<code>-onreboot <i>true</i></code>	reboot command	Yes
<code>-auto-giveback <i>false</i></code>	halt command, or power cycle operation issued from the Service Processor	Yes
<code>-onreboot <i>false</i></code>	reboot command	N/A In this case, takeover does not occur
<code>-auto-giveback <i>true</i></code>	halt command, or power cycle operation issued from the Service Processor	Yes

<code>-onreboot false</code>	reboot command	No
<code>-auto-giveback false</code>	halt command, or power cycle operation issued from the Service Processor	No

The `-auto-giveback` parameter controls giveback after panic and all other automatic takeovers. 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`.

The `-onreboot` parameter applies to reboots and halt commands issued from ONTAP. 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.



Be aware that takeover can occur for other reasons in the event of a node panic. For example, if a node panics but the panic packet is not received by its partner, the partner might perform a heartbeat loss takeover. In this case, giveback would not be controlled by the `-auto-giveback-after-panic` parameter but would instead be controlled by the `-onfailure` parameter.

storage failover parameters used	Does automatic giveback occur after panic?
<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

-onpanic true -auto-giveback false -auto-giveback-after-panic true	Yes
-onpanic true -auto-giveback false -auto-giveback-after-panic false	No
-onpanic false If -onpanic is set to false, takeover/giveback does not occur, regardless of the value set for -auto-giveback or -auto-giveback-after-panic	No

If you modify the default settings, the `-onpanic` parameter can override automatic giveback, as shown in the table above.



- 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`, a takeover does not occur and clients experience a disruption in ONTAP data services. Therefore, automatic giveback cannot occur, even if the `-auto-giveback-after-panic` parameter is set to `true`.



- Takeover might occur for other reasons during node panic. In such cases, giveback is not controlled by the `auto-giveback-after-panic` setting.
- 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.

## Manual takeover commands

You can perform a takeover manually when maintenance is required on the partner, and in other similar situations. Depending on the state of the partner, the command you use to perform the takeover varies.

If you want to...	Use this command...
Take over the partner node	<code>storage failover takeover</code>
Monitor the progress of the takeover as the partner's aggregates are moved to the node doing the takeover	<code>storage failover show-takeover</code>

Display the storage failover status for all nodes in the cluster	<code>storage failover show</code>
Take over the partner node without migrating LIFs	<code>storage failover takeover -skip-lif -migration-before-takeover true</code>
Take over the partner node even if there is a disk mismatch	<code>storage failover takeover -skip-lif -migration-before-takeover true</code>
Take over the partner node even if there is an ONTAP version mismatch  <b>Note:</b> This option is only used during the nondisruptive ONTAP upgrade process.	<code>storage failover takeover -option allow -version-mismatch</code>
Take over the partner node without performing aggregate relocation	<code>storage failover takeover -bypass -optimization true</code>
Take over the partner node before the partner has time to close its storage resources gracefully	<code>storage failover takeover -option immediate</code>

Before you issue the storage failover command with the immediate option, you must migrate the data LIFs to another node by using the following command: `network interface migrate-all -node node`



If you specify the `storage failover takeover -option immediate` command without first migrating the data LIFs, data LIF migration from the node is significantly delayed even if the `skip-lif-migration-before-takeover` option is not specified.

Similarly, if you specify the immediate option, negotiated takeover optimization is bypassed even if the `bypass-optimization` option is set to *false*.

## Moving epsilon for certain manually initiated takeovers

You should move epsilon if you expect that any manually initiated takeovers could result in your storage system being one unexpected node failure away from a cluster-wide loss of quorum.

### About this task

To perform planned maintenance, you must take over one of the nodes in an HA pair. Cluster-wide quorum must be maintained to prevent unplanned client data disruptions for the remaining nodes. In some instances, performing the takeover can result in a cluster that is one unexpected node failure away from cluster-wide loss of quorum.

This can occur if the node being taken over holds epsilon or if the node with epsilon is not healthy. To maintain a more resilient cluster, you can transfer epsilon to a healthy node that is not being taken over.

Typically, this would be the HA partner.

Only healthy and eligible nodes participate in quorum voting. To maintain cluster-wide quorum, more than  $N/2$  votes are required (where  $N$  represents the sum of healthy, eligible, online nodes). In clusters with an even number of online nodes, epsilon adds additional voting weight toward maintaining quorum for the node to which it is assigned.



Although cluster formation voting can be modified by using the `cluster modify -eligibility false` command, you should avoid this except for situations such as restoring the node configuration or prolonged node maintenance. If you set a node as ineligible, it stops serving SAN data until the node is reset to eligible and rebooted. NAS data access to the node might also be affected when the node is ineligible.

## Steps

1. Verify the cluster state and confirm that epsilon is held by a healthy node that is not being taken over:
  - a. Change to the advanced privilege level, confirming that you want to continue when the advanced mode prompt appears (\*>):

```
set -privilege advanced
```

- b. Determine which node holds epsilon:

```
cluster show
```

In the following example, Node1 holds epsilon:

Node	Health	Eligibility	Epsilon
Node1	true	true	true
Node2	true	true	false

If the node you want to take over does not hold epsilon, proceed to Step 4.

2. Remove epsilon from the node that you want to take over:

```
cluster modify -node Node1 -epsilon false
```

3. Assign epsilon to the partner node (in this example, Node2):

```
cluster modify -node Node2 -epsilon true
```

4. Perform the takeover operation:

```
storage failover takeover -ofnode node_name
```

5. Return to the admin privilege level:

```
set -privilege admin
```

## Manual giveback commands

You can perform a normal giveback, a giveback in which you terminate processes on the partner node, or a forced giveback.



Prior to performing a giveback, you must remove the failed drives in the taken-over system as described in [Disks and aggregates management](#).

## If giveback is interrupted

If the takeover node experiences a failure or a power outage during the giveback process, that process stops and the takeover node returns to takeover mode until the failure is repaired or the power is restored.

However, this depends upon the stage of giveback in which the failure occurred. If the node encountered failure or a power outage during partial giveback state (after it has given back the root aggregate), it will not return to takeover mode. Instead, the node returns to partial-giveback mode. If this occurs, complete the process by repeating the giveback operation.

## If giveback is vetoed

If giveback is vetoed, you must check the EMS messages to determine the cause. Depending on the reason or reasons, you can decide whether you can safely override the vetoes.

The `storage failover show-giveback` command displays the giveback progress and shows which subsystem vetoed the giveback, if any. Soft vetoes can be overridden, while hard vetoes cannot be, even if forced. The following tables summarize the soft vetoes that should not be overridden, along with recommended workarounds.

You can review the EMS details for any giveback vetoes by using the following command:

```
event log show -node * -event gb*
```

## Giveback of the root aggregate

These vetoes do not apply to aggregate relocation operations:

Vetoing subsystem module	Workaround
vfiler_low_level	<p>Terminate the SMB sessions causing the veto, or shutdown the SMB application that established the open sessions.</p> <p>Overriding this veto might cause the application using SMB to disconnect abruptly and lose data.</p>
Disk Check	<p>All failed or bypassed disks should be removed before attempting giveback. If disks are sanitizing, you should wait until the operation completes.</p> <p>Overriding this veto might cause an outage caused by aggregates or volumes going offline due to reservation conflicts or inaccessible disks.</p>

## Giveback of the SFO aggregates

These vetoes do not apply to aggregate relocation operations:

Vetoing subsystem module	Workaround
--------------------------	------------



Lock Manager	<p>Gracefully shutdown the SMB applications that have open files, or move those volumes to a different aggregate.</p> <p>Overriding this veto results in loss of SMB lock state, causing disruption and data loss.</p>
Lock Manager NDO	<p>Wait until the locks are mirrored.</p> <p>Overriding this veto causes disruption to Microsoft Hyper-V virtual machines.</p>
RAID	<p>Check the EMS messages to determine the cause of the veto:</p> <p>If the veto is due to nvfile, bring the offline volumes and aggregates online.</p> <p>If disk add or disk ownership reassignment operations are in progress, wait until they complete.</p> <p>If the veto is due to an aggregate name or UUID conflict, troubleshoot and resolve the issue.</p> <p>If the veto is due to mirror resync, mirror verify, or offline disks, the veto can be overridden and the operation restarts after giveback.</p>
Disk Inventory	<p>Troubleshoot to identify and resolve the cause of the problem.</p> <p>The destination node might be unable to see disks belonging to an aggregate being migrated.</p> <p>Inaccessible disks can result in inaccessible aggregates or volumes.</p>
Volume Move Operation	<p>Troubleshoot to identify and resolve the cause of the problem.</p> <p>This veto prevents the volume move operation from aborting during the important cutover phase. If the job is aborted during cutover, the volume might become inaccessible.</p>

### Commands for performing a manual giveback

You can manually initiate a giveback on a node in an HA pair to return storage to the original owner after completing maintenance or resolving any issues that caused the takeover.

If you want to...	Use this command...
Give back storage to a partner node	<code>storage failover giveback -ofnode nodename</code>

Give back storage even if the partner is not in the waiting for giveback mode	<pre>storage failover giveback -ofnode nodename -require-partner-waiting false</pre> <p>Do not use this option unless a longer client outage is acceptable.</p>
Give back storage even if processes are vetoing the giveback operation (force the giveback)	<pre>storage failover giveback -ofnode nodename -override-vetoes true</pre> <p>Use of this option can potentially lead to longer client outage, or aggregates and volumes not coming online after the giveback.</p>
Give back only the CFO aggregates (the root aggregate)	<pre>storage failover giveback -ofnode nodename  -only-cfo-aggregates true</pre>
Monitor the progress of giveback after you issue the giveback command	<pre>storage failover show-giveback</pre>

## Testing takeover and giveback

After you configure all aspects of your HA pair, you need to verify that it is operating as expected in maintaining uninterrupted access to both nodes' storage during takeover and giveback operations. Throughout the takeover process, the local (or takeover) node should continue serving the data normally provided by the partner node. During giveback, control and delivery of the partner's storage should return to the partner node.

### Steps

1. Check the cabling on the HA interconnect cables to make sure that they are secure.
2. Verify that you can create and retrieve files on both nodes for each licensed protocol.
3. Enter the following command:

```
storage failover takeover -ofnode partnernode
```

See the man page for command details.

4. Enter either of the following commands to confirm that takeover occurred:

```
storage failover show-takeover
```

```
storage failover show
```

If you have the `storage failover` command's `-auto-giveback` option enabled:

Node	Partner	Takeover Possible	State Description
------	---------	-------------------	-------------------

node 1	node 2	-	Waiting for giveback
node 2	node 1	false	In takeover, Auto giveback will be initiated in number of seconds

If you have the `storage failover` command's `-auto-giveback` option disabled:

Node	Partner	Takeover Possible	State Description
node 1	node 2	-	Waiting for giveback
node 2	node 1	false	In takeover

5. Display all the disks that belong to the partner node (Node2) that the takeover node (Node1) can detect:

```
storage disk show -home node2 -ownership
```

The following command displays all disks belonging to Node2 that Node1 can detect:

```
cluster::> storage disk show -home node2 -ownership
```

Disk	Aggregate	Home	Owner	DR Home	Home ID	Owner ID	DR Home ID	Reserve r	Pool
1.0.2	-	node2	node2	-	4078312453	4078312453	-	4078312452	Pool0
1.0.3	-	node2	node2	-	4078312453	4078312453	-	4078312452	Pool0

6. Confirm that the takeover node (Node1) controls the partner node's (Node2) aggregates:

```
aggr show -fields home-id,home-name,is-home
```

aggregate	home-id	home-name	is-home
aggr0_1	2014942045	node1	true
aggr0_2	4078312453	node2	false
aggr1_1	2014942045	node1	true
aggr1_2	4078312453	node2	false

During takeover, the "is-home" value of the partner node's aggregates is false.

7. Give back the partner node's data service after it displays the "Waiting for giveback" message:

```
storage failover giveback -ofnode partnernode
```

8. Enter either of the following commands to observe the progress of the giveback operation:

```
storage failover show-giveback
```

```
storage failover show
```

9. Proceed, depending on whether you saw the message that giveback was completed successfully:

If takeover and giveback...	Then...
Are completed successfully	Repeat Step 2 through Step 8 on the partner node.
Fail	Correct the takeover or giveback failure and then repeat this procedure.

## 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 <code>ha</code> 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"> <li>• Run the <code>storage failover show-giveback</code> command for more information.</li> </ul>
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.

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.	<p>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.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>
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.	<p>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.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>
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.	<p>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.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>
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.	<p>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.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>

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"> <li>• Run the <code>storage failover show-giveback</code> command for more information.</li> </ul>
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.

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.	Storage failover is not possible. The HA mode option is configured as non_ha. <ul style="list-style-type: none"> <li>You must reboot the node to use all of its NVRAM.</li> </ul>
Non-HA mode. Reboot node to activate HA.	Storage failover is not possible. <ul style="list-style-type: none"> <li>The node must be rebooted to enable HA capability.</li> </ul>
Non-HA mode.	Storage failover is not possible. The HA mode option is configured as non_ha. <ul style="list-style-type: none"> <li>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.</li> </ul>

## 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.

## Rest API management with System Manager

### Rest API management with System Manager

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 Automation docs](#)

## 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-
00a0986abd71/1"
39         }
40       }
41     },
42   ],

```

```
43     "num_records": 1,  
44     "_links": {  
45         "self": {  
46             "href":  
             "/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"  
47         }  
48     }  
49 }
```

## Copyright Information

Copyright © 2022 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.