



# ONTAP System Manager docs

## ONTAP System Manager

NetApp

December 16, 2020

This PDF was generated from <https://docs.netapp.com/us-en/ontap/index.html> on December 16, 2020. Always check docs.netapp.com for the latest.



# Table of Contents

|                                                                                    |    |
|------------------------------------------------------------------------------------|----|
| ONTAP System Manager docs .....                                                    | 1  |
| Benefits of using ONTAP System Manager .....                                       | 1  |
| Key concepts .....                                                                 | 3  |
| Configure ONTAP on a new cluster .....                                             | 5  |
| Assign a node-management IP address .....                                          | 5  |
| Initialize the cluster .....                                                       | 6  |
| Create your local tier .....                                                       | 6  |
| Configure protocols .....                                                          | 6  |
| Provision Storage .....                                                            | 7  |
| Provision SAN storage .....                                                        | 8  |
| SAN Overview .....                                                                 | 8  |
| Provision SAN storage for VMware datastores .....                                  | 9  |
| Provision SAN storage for Linux servers .....                                      | 9  |
| Provision SAN storage for Windows servers .....                                    | 10 |
| SnapMirror Business Continuity .....                                               | 11 |
| Provision NVMe storage .....                                                       | 15 |
| NVMe overview .....                                                                | 15 |
| Provision NVMe storage for SUSE Linux .....                                        | 15 |
| Provision NAS storage .....                                                        | 17 |
| NAS overview .....                                                                 | 17 |
| Provision NAS storage for VMware datastores .....                                  | 17 |
| Provision NAS storage for home directories .....                                   | 17 |
| Provision NAS storage for Linux servers using NFS .....                            | 18 |
| Manage access using export policies .....                                          | 19 |
| Provision NAS storage for Windows servers using SMB/CIFS .....                     | 19 |
| Provision NAS storage for both Windows and Linux using both NFS and SMB/CIFS ..... | 20 |
| Secure client access with Kerberos .....                                           | 21 |
| Provide client access with name services .....                                     | 22 |
| Provision NAS storage for large file systems using FlexGroup volumes .....         | 23 |
| Monitor volume usage with ONTAP File System Analytics .....                        | 23 |
| Monitor NFS active clients .....                                                   | 25 |
| Improve performance for multiple clients with FlexCache .....                      | 26 |
| Enable NAS storage .....                                                           | 27 |
| Provision object storage .....                                                     | 30 |
| ONTAP S3 overview .....                                                            | 30 |
| Enable an S3 server on a storage .....                                             | 31 |

|                                                              |    |
|--------------------------------------------------------------|----|
| Provision buckets .....                                      | 31 |
| Add S3 users and groups .....                                | 32 |
| Manage user access to buckets .....                          | 33 |
| Manage user access to S3-enabled storage VMs .....           | 33 |
| Manage resources using quotas .....                          | 35 |
| Quota overview .....                                         | 35 |
| Set quotas to limit resource use .....                       | 35 |
| Maximize security .....                                      | 36 |
| Security overview .....                                      | 36 |
| Set up multifactor authentication .....                      | 36 |
| Control administrator access .....                           | 38 |
| Encrypt stored data using software-based encryption .....    | 39 |
| Encrypt stored data using self-encrypting drives .....       | 39 |
| Diagnose and correct file access issues .....                | 40 |
| Protect data .....                                           | 41 |
| Data protection overview .....                               | 41 |
| Configure Snapshot copies .....                              | 41 |
| Recover from Snapshot copies .....                           | 41 |
| Prepare for mirroring and vaulting .....                     | 42 |
| Configure mirrors and vaults .....                           | 42 |
| Serve data from a SnapMirror destination .....               | 43 |
| Resynchronize a protection relationship .....                | 44 |
| Restore a volume from an earlier Snapshot copy .....         | 44 |
| Restore to a new volume .....                                | 45 |
| Reverse Resynchronizing a Protection Relationship .....      | 45 |
| Reactivate a source storage VM .....                         | 45 |
| Resynchronize a destination storage VM .....                 | 46 |
| Extend to the cloud .....                                    | 47 |
| Cloud overview .....                                         | 47 |
| Tier data to cloud .....                                     | 47 |
| Tier data to local bucket .....                              | 48 |
| Create tags for tiering objects .....                        | 48 |
| Enable inactive data reporting .....                         | 48 |
| View cluster performance .....                               | 50 |
| Cluster performance overview .....                           | 50 |
| View performance on cluster dashboard .....                  | 50 |
| Identify hot volumes and other objects .....                 | 50 |
| Search, filter, and sort information in System Manager ..... | 51 |

|                                                              |    |
|--------------------------------------------------------------|----|
| Monitor cluster performance using System Manager .....       | 53 |
| Monitor cluster performance with Unified Manager .....       | 53 |
| Monitor cluster performance with Cloud Insights .....        | 54 |
| Day-to-day administration .....                              | 56 |
| Administration overview .....                                | 56 |
| Viewing and managing your network .....                      | 56 |
| Downloading network data for reporting .....                 | 57 |
| Search, filter, and sort information in System Manager ..... | 57 |
| Enable new features by adding license keys .....             | 60 |
| Reboot, shut down, take over, and give back nodes .....      | 60 |
| Troubleshoot hardware problems .....                         | 60 |
| Manage MetroCluster sites .....                              | 62 |
| Clone volumes and LUNs for testing .....                     | 72 |
| Modify QoS .....                                             | 73 |
| Update ONTAP .....                                           | 73 |
| Manage storage .....                                         | 75 |
| Rest API .....                                               | 82 |
| REST API log overview .....                                  | 82 |
| Accessing the REST API log .....                             | 82 |
| Getting more information .....                               | 85 |
| Legal notices .....                                          | 86 |
| Copyright .....                                              | 86 |
| Trademarks .....                                             | 86 |
| Patents .....                                                | 86 |
| Privacy policy .....                                         | 86 |

# ONTAP System Manager docs

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

Beginning with ONTAP 9.7, a totally redesigned ONTAP System Manager simplifies ONTAP management with an intuitive graphical user interface. The new dashboard shows key cluster status and performance on one screen.

The documentation for ONTAP System Manager is totally redesigned as well. Easy-to-navigate content is quick and easy to use. Watch embedded videos for quick overviews of major management tasks.

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



## Benefits of using ONTAP System Manager

- Fast, simple configuration  
Simplified workflows for ONTAP setup and management of common tasks.
- Smart defaults  
Enable you to create best-practice configurations based on proven deployments.
- Extensive administrative capabilities

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

- Integrated management

System Manager comes bundled with the ONTAP 9 platform, eliminating the need for a separate installation.

# Key concepts

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

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

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

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

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

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

- **Cluster** – that's the big picture. A cluster is made up of one or more nodes. Think of nodes as computers that specialize in data management and storage. You can add nodes to your cluster as your needs grow, or you can replace smaller nodes with bigger ones. All without interrupting access to your data, of course.
- **Snapshot copies** – these are instant copies of your data that you can use to undo a mistake, move or back up to cloud, mirror to another cluster, or even copy to tape. Without interruption to your clients. And who can afford downtime?
- **Data protection** - the protection features you use depend on what you need to protect against and how long you can wait to recover if something goes wrong. ONTAP offers synchronous and asynchronous mirroring and more.
- **HA pair** – speaking of avoiding downtime, the high-availability pair is the basic unit of an ONTAP cluster. It's made up of two partner nodes that can take over for each other. Say you want to upgrade to the latest version of ONTAP to get a great new data management feature. Just have the

partner take over a node's client load, upgrade that client, and then give the load back. Repeat for the partner node and you have just upgraded without any disruption.

- **Storage efficiency** – disks cost money (real money!), but storage efficiency lets you store more data in less space. And that saves real money and makes you a data hero. You can use any or all of ONTAP's compression, deduplication, and compaction features. We're sure you already know what compression is. Deduplication identifies multiple copies of the same data and replaces the duplicates with pointers to a single copy. Compaction puts multiple small files into a single block of storage, filling in what would otherwise be wasted space.
- **Security** – security is integral to ONTAP data management software. ONTAP helps you out in many ways, such as using multifactor authentication for administrators, encrypting data on disk and in flight, and using antivirus tools to protect Windows files.
- **Volumes** – are exactly what you think volumes are. They're containers to store files. You can export volumes to Linux clients, share volumes with Windows clients, or even do both at the same time with the same files.
- **LUNs** – the basic unit of SAN. That's Fibre Channel and iSCSI. In a SAN environment, ONTAP provides virtual disks to clients instead of files. Database administrators often want virtual disks that they can manage at a low level or apply a specialized file system to. Many ONTAP systems, but not all, can serve data to SAN clients.
- **NVMe namespaces** – the future of flash storage. The NVMe protocol is optimized for SSD-based storage, and it is really fast. NVMe is a flavor of SAN, but the basic unit of storage is called a *namespace* instead of a LUN.

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

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



# Configure ONTAP on a new cluster

You can quickly create a cluster and configure ONTAP software for your cluster. System Manager provides a simple and easy workflow for setting up the cluster and configuring storage.

Your system should already be installed and cabled according to the [Installation and Setup Instructions](#) that came with the system. Also, cluster network interfaces should be configured on each node of the cluster for intra-cluster communication.



## Assign a node-management IP address

### Windows System

You should connect your Windows computer to the same subnet as the controllers. This will automatically assign a node-management IP address to your system.

#### *Step*

1. From the Windows system, open the **Network** drive to discover the nodes.

2. Double-click the node to launch the cluster setup wizard.

## Other systems

You should configure the node-management IP address for one of the nodes in your cluster. You can use this node-management IP address to launch the cluster set up wizard.

See [Creating the cluster on the first node](#) for information about assigning a node-management IP address.

## Initialize the cluster

You initialize the cluster by setting an administrative password for the cluster and setting up the cluster management and node management networks. You can also configure services like a DNS server to resolve host names and an NTP server to synchronize time.

### *Steps*

1. On a web browser, enter the node-management IP address that you have configured: "https://node-management-IP"

System Manager automatically discovers the remaining nodes in the cluster.

2. Initialize the storage system by configuring the cluster management network and node management IP addresses for all the nodes.

## Create your local tier

Create local tiers from the available disks or SSDs in your nodes. System Manager automatically calculates the best tier configuration based on your hardware.

### *Steps*

1. Click **Dashboard** and then click **Prepare Storage**.

Accept the storage recommendation for your local tier.

## Configure protocols

Depending on the licenses enabled on your cluster, you can enable the desired protocols on your cluster. You then create network interfaces using which you can access the storage.

### *Steps*

1. Click **Dashboard** and then click **Configure Protocols**.
  - Enable iSCSI or FC for SAN access.
  - Enable NFS or SMB/CIFS for NAS access.

- Enable NVMe for FC-NVMe access.

## Provision Storage

You can now provision storage. The options you see depends on the licenses that are installed.

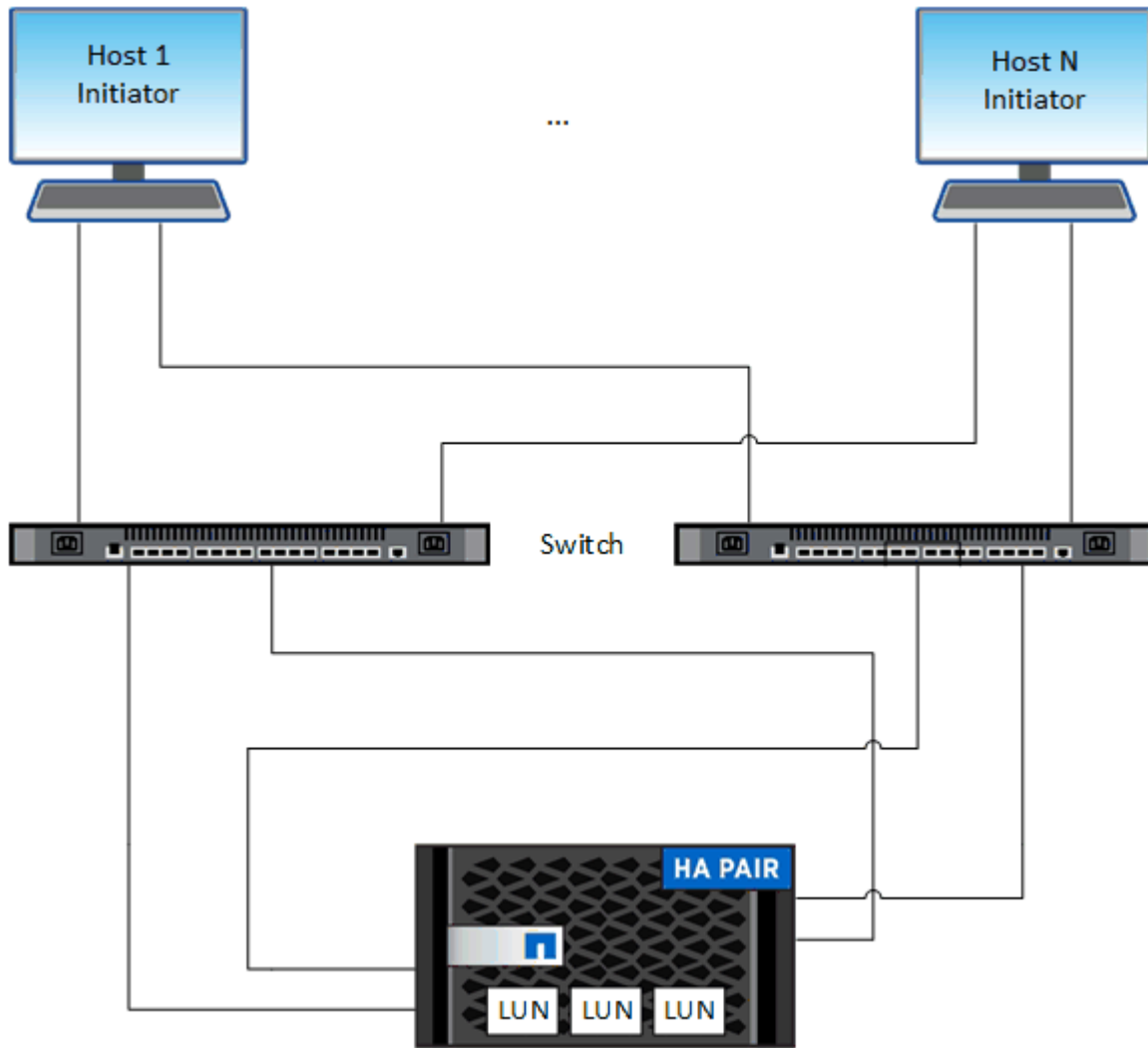
### *Steps*

1. Click **Dashboard** and then click **Provision Storage**.
  - To [provision SAN access](#), click **Add LUNs**.
  - To [provision NAS access](#), click **Add Volumes**.
  - To [provision NVMe storage](#), click **Add Namespaces**.

# Provision SAN storage

## SAN Overview

You can use the iSCSI and FC protocols to provide storage in a SAN environment.



With iSCSI and FC, storage targets are called LUNs (logical units) and are presented to hosts as standard block devices. You create LUNs and then map them to initiator groups (igroups). Initiator groups are tables of FC host WWPNs and iSCSI host node names and control which initiators have access to which LUNs.

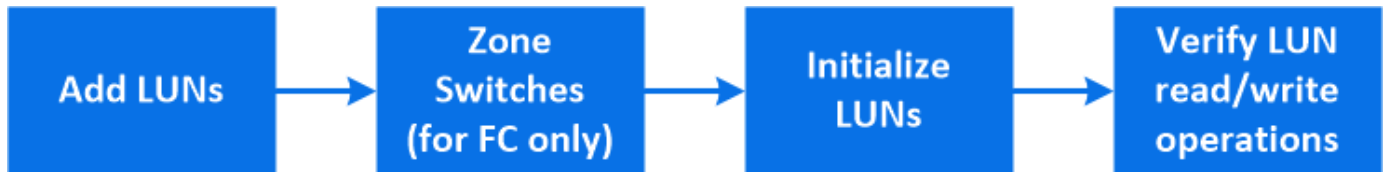
FC targets connect to the network through FC switches and host-side adapters and are identified by world-wide port names (WWPNs). iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters (CNAs) or dedicated host bus adapters (HBAs) and are identified by iSCSI qualified names (IQNs).

Learn more about [SAN](#).

# Provision SAN storage for VMware datastores

Create LUNs to provide storage for an ESXi host using the FC or iSCSI SAN protocol. LUNs appear as disks to the ESXi host.

This procedure creates new LUNs on an existing storage VM. Your FC or iSCSI protocol should already be set up.



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

## Steps

1. In ONTAP System Manager, click **Storage > LUNs** and then click **Add**.

If you need to create a new initiator group, click **More Options**.

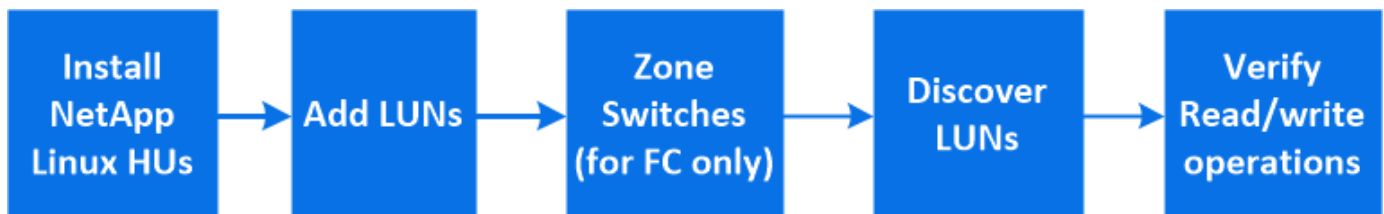
If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then select **Performance Service Level**.

2. For FC, zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
3. Use Virtual Storage Console (VSC) for VMware vSphere, to discover and initialize the LUN and to verify that the ESXi hosts can write and read data on the LUN.

# Provision SAN storage for Linux servers

Create LUNs to provide storage for a Linux server using the FC or iSCSI SAN protocol. LUNs appear to Linux as SCSI disk devices.

This procedure creates new LUNs on an existing storage VM. Your FC or iSCSI protocol should already be set up. You need to know the initiator identifiers (FC WWPN or iSCSI iqn) for your Linux server.





Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

### Steps

1. On your Linux server, install the [NetApp Linux Host Utilities](#) package.
2. In ONTAP System Manager, click **Storage > LUNs** and then click **Add**.

If you need to create a new initiator group, click **More Options**.

If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then select **Performance Service Level**.

3. For FC, zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
4. On your Linux server, discover the new LUNs:

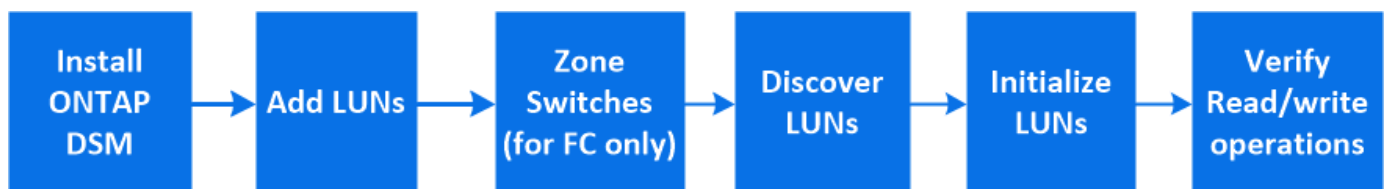
```
/usr/bin/rescan-scsi-bus.sh
```

5. Optionally partition the LUNs and create file systems.
6. Verify the Linux server can write and read data on the LUN.

## Provision SAN storage for Windows servers

Create LUNs to provide storage for a Windows server using the FC or iSCSI SAN protocol. LUNs appear as disks to the Windows host.

This procedure creates new LUNs on an existing storage VM. Your FC or iSCSI protocol should already be set up.



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

### Steps

1. On your Windows server, install Data ONTAP DSM for Windows MPIO.
2. In ONTAP System Manager, click **Storage > LUNs**, and then click **Add**.

If you need to create a new initiator group, click **More Options**.

If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then select **Performance Service Level**.

3. For FC, zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
4. On your Windows server, discover the new LUN.
5. Initialize the LUN and optionally format it with a file system.
6. Verify the Windows server can write and read data on the LUN.

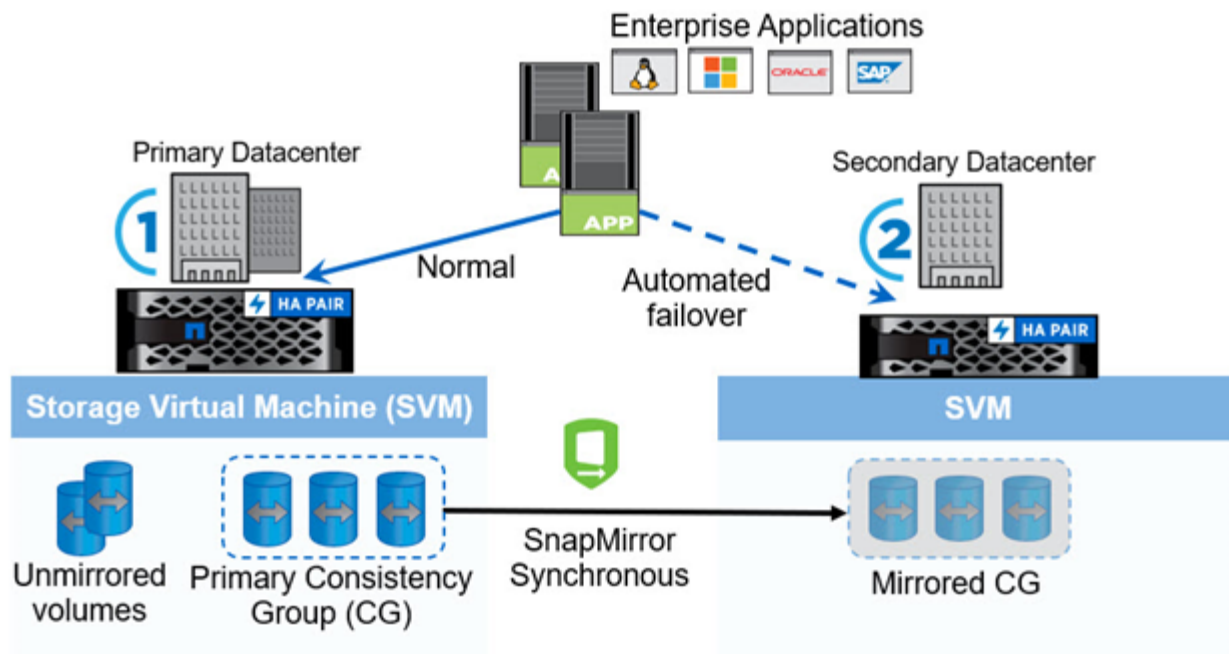
## SnapMirror Business Continuity

### SnapMirror Business Continuity overview

Starting in ONTAP 9.8, you can use System Manager to protect LUNs for transparent application failover, enabling applications to fail over automatically for business continuity when using two AFF clusters or two All SAN Array (ASA) clusters. Your clusters cannot be mixed; they must consist of two AFF clusters or two ASA clusters. Protection for business continuity supports iSCSI and FCP protocols.

The SnapMirror Business Continuity provides the following benefits:

- Automated failover of business-critical applications
- Simplified application management, using consistency groups for dependent write-order consistency
- The ability to test failover for each application
- Instantaneous creation of mirror clones without impacting application availability



## Requirements

SnapMirror Business Continuity has the following requirements:

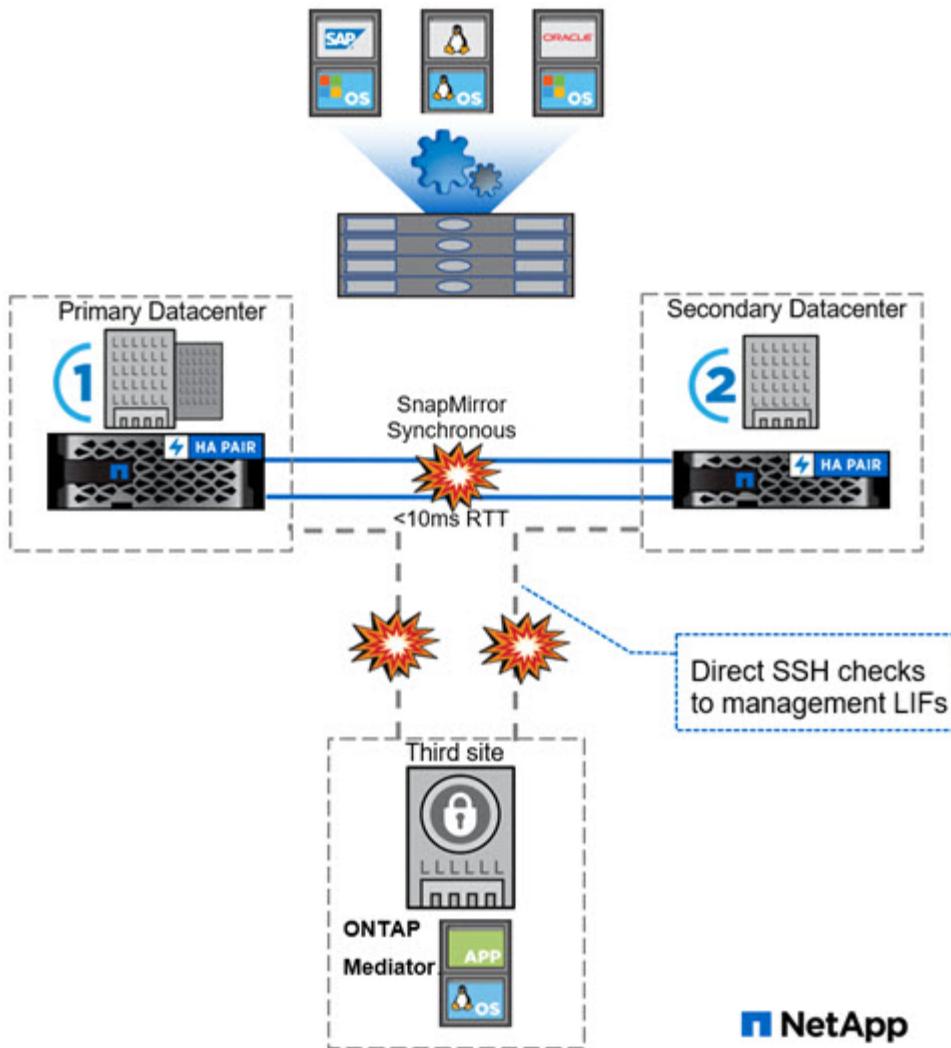
- 2-node HA cluster, only – both either AFF or ASA. No intermixing.
- A server or VM running RHEL 7.6 or 7.8 or CentOS 8.0 or 8.1 for installing ONTAP Mediator
- Data Protection or Premium bundle license

## Support

SnapMirror Business Continuity provides support for the following:

- Synchronous replication
- SAN protocol – FCP or iSCSI
- Up to 5 consistency groups, each with up to 12 volumes
- A total of 80 concurrent synchronous relationships per HA pair, including consistency groups





## Configure Mediator

Use System Manager to configure the Mediator server to be used for automated failover. You can also replace the self-signed SSL and CA with the third party validated SSL Certificate and CA if you have not already done so.

### Steps

1. Navigate to **Protection > Overview > Mediator > Configure**.
2. Click **Add**, and enter the following Mediator server information:
  - IPv4 address
  - Username
  - Password
  - Certificate

## Configure protection for business continuity

Configuring protection for business continuity involves selecting LUNs on the ONTAP source cluster and adding them to a consistency group. Open System Manager from a browser on the source cluster to begin configuring protection for business continuity.

### About this task

- LUNs must reside on the same storage VM.
- LUNs can reside on different volumes.
- The source and destination cluster cannot be the same.


### Steps

1. Choose the LUNs you want to protect and add them to a protection group: **Protection > Overview > Protect for Business Continuity > Protect LUNs**.
2. Select one or more LUNs to protect on the source cluster.
3. Select the destination cluster and SVM.
4. **Initialize relationship** is selected by default. Click **Save** to begin protection.
5. Go to **Dashboard > Performance** to verify IOPS activity for the LUNs.
6. On the destination cluster, use System Manager to verify that the protection for business continuity relationship is in sync: **Protection > Relationships**.

## Reestablish the original protection relationship after an unplanned failover

ONTAP uses the ONTAP Mediator to detect when a failure occurs on the primary storage system and executes automatic unplanned failover to the secondary storage system. You can use ONTAP System Manager to reverse the relationship and reestablish the original protection relationship when original source cluster is back online.

### Steps

1. Navigate to **Protection > Relationships** and wait for the relationship state to show “InSync.”
2. To resume operations on the original source cluster, click  and select **Failover**.

# Provision NVMe storage

## NVMe overview

You can use the non-volatile memory express (NVMe) protocol to provide storage in a SAN environment. The NVMe protocol is optimized for performance with solid state storage.

For NVMe, storage targets are called namespaces. An NVMe namespace is a quantity of non-volatile storage that can be formatted into logical blocks and presented to a host as a standard block device. You create namespaces and subsystems, and then map the namespaces to the subsystems, similar to the way LUNs are provisioned and mapped to igroups for FC and iSCSI.

NVMe targets are connected to the network through a standard FC infrastructure using FC switches and host-side adapters.

Learn more about [NVMe](#).

## Provision NVMe storage for SUSE Linux

Create namespaces to provide storage for a SUSE Linux server using the NVMe protocol. Namespaces appear to Linux as SCSI disk devices.

This procedure creates new namespaces on an existing storage VM. Your storage VM must be configured for NVME, and your FC transport should already be set up.



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

### Steps

1. In ONTAP System Manager, click **Storage** > **NVMe Namespaces** and then click **Add**.

If you need to create a new subsystem, click **More Options**.

If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then select **Performance Service Level**.

2. Zone your FC switches by WWPN. Use one zone per initiator and include all target ports in each zone.
3. On your Linux server, discover the new namespaces.
4. Initialize the namespace and optionally format it with a file system.
5. Verify the Linux server can write and read data on the namespace.

# Provision NAS storage

## NAS overview

ONTAP enables you to serve data to Linux and Windows clients simply, securely, and efficiently.

ONTAP System Manager supports workflows for:

- Initial configuration of clusters that you intend to use for NAS file services.
- Additional volume provisioning for changing storage needs.
- Configuration and maintenance for industry-standard authentication and security facilities.

Using ONTAP System Manager, you can manage NAS services at the component level:

- Protocols – NFS, SMB/CIFS, or both (NAS multiprotocol)
- Name services – DNS, LDAP, and NIS
- Name service switch
- Kerberos security
- Exports and shares
- Qtrees
- Name mapping of users and groups

If you need to learn more about ONTAP NAS features, you can review the *Concepts* guide and *Provisioning for NAS protocols* section in the [ONTAP 9 Documentation Center](#).

## Provision NAS storage for VMware datastores

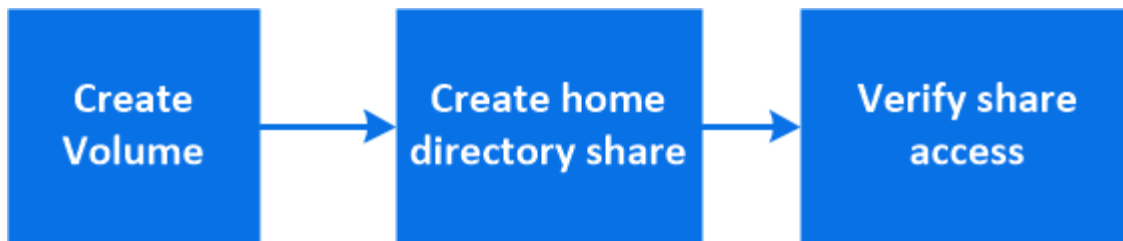
Create volumes to provide VMware datastores using the NFS protocol.

See the [NFS Configuration for ESXi using VSC Express Guide](#) for VMware datastore provisioning best practices.

## Provision NAS storage for home directories

Create volumes to provide storage for home directories using the SMB/CIFS protocol.

This procedure creates new volumes for home directories on an [existing SMB-enabled storage VM](#).



### Steps

1. In ONTAP System Manager, click **Storage** > **Volumes** and then click **Add**.
2. Click **Storage** > **Shares**, click **Add**, and select **Home Directory**.
3. On a Windows client, do the following to verify that the share is accessible.
  - a. In Windows Explorer, map a drive to the share in the following format:  
`\\_SMB_Server_Name__Share_Name_`  
  
If the share name was created with variables (%w, %d, or %u), be sure to test access with a resolved name.
  - b. On the newly created drive, create a test file, and then delete the file.

## Provision NAS storage for Linux servers using NFS

Create volumes to provide storage for Linux servers using the NFS protocol.

This procedure creates new volumes on an [existing NFS-enabled storage VM](#).



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

### Steps

1. In ONTAP System Manager, click **Storage** > **Volumes** and then click **Add**.

The default export policy grants full access to all users. You can add more restrictive rules to the export policy later.

If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then select **Performance Service Level**.

2. On a Linux client, do the following to verify access.
  - a. Create and mount the volume using the network interface of the storage VM.
  - b. On the newly mounted volume, create a test file, write text to it, and then delete the file.

After verifying access, you can [restrict client access with the volume's export policy](#) and set any desired UNIX ownership and permissions on the mounted volume.

# Manage access using export policies

Enable Linux client access to NFS servers by using export policies.

This procedure creates or modifies export policies for an [existing NFS-enabled storage VM](#).

## Steps

1. In ONTAP System Manager, Click **Storage > Volumes**.
2. Click an NFS-enabled volume and click **More**.
3. Click **Edit Export Policy** and then click **Select an existing policy** or **Add a new policy**.

# Provision NAS storage for Windows servers using SMB/CIFS

Create volumes to provide storage for Windows servers using the SMB/CIFS protocol.

This procedure creates new volumes on an [existing SMB-enabled storage VM](#).



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

## Steps

1. In ONTAP System Manager, click **Storage > Volumes** and then click **Add**.

The default share grants full access to all users. You can modify the Access Control List (ACL) later.

If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then select **Performance Service Level**.

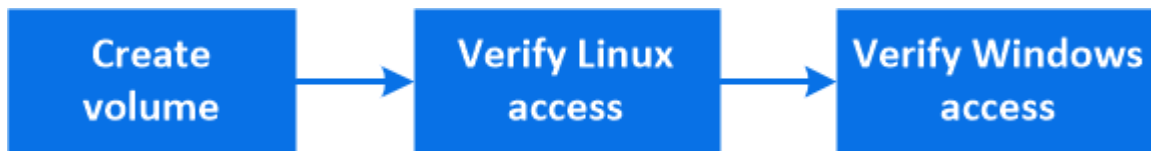
2. Switch to a Windows client to verify that the share is accessible.
  - a. In Windows Explorer, map a drive to the share in the following format:  
`\\_SMB_Server_Name__Share_Name_`
  - b. On the newly created drive, create a test file, write text to it, and then delete the file.

After verifying access, you can [restrict client access with the share ACL](#) and set any desired security properties on the mapped drive.

# Provision NAS storage for both Windows and Linux using both NFS and SMB/CIFS

Create volumes to provide storage for clients using either the NFS or SMB/CIFS protocol.

This procedure creates new volumes on an [existing storage VM enabled for both NFS and SMB protocols](#).



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

## Steps

1. In ONTAP System Manager, click **Storage > Volumes** and then click **Add**.

If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then select **Performance Service Level**.

2. Click **More Options** and select **Share via NFS**.

The default setting grants full access to all users. You can add more restrictive rules to the export policy later.

3. Select **Share via SMB/CIFS**.

The share is created with a default Access Control List (ACL) set to "Full Control" for the **Everyone** group. You can add restrictions to the ACL later.

4. On a Linux client, do the following to verify that the export is accessible.
  - a. Create and mount the volume using the network interface of the storage VM.
  - b. On the newly mounted volume, create a test file, write text to it, and then delete the file.
5. On a Windows client, do the following to verify that the share is accessible.
  - a. In Windows Explorer, map a drive to the share in the following format:  
`\\_SMB_Server_Name_\\Share_Name_`
  - b. On the newly created drive, create a test file, write text to it, and then delete the file.

After verifying access, you can [restrict client access with the volume's export policy](#), [restrict client access with the share ACL](#), and set any desired ownership and permissions on the exported and shared



volume.

## Secure client access with Kerberos

Enable Kerberos to secure storage access for NAS clients.

This procedure configures Kerberos on an existing storage VM enabled for [NFS](#) or [SMB](#).

Before beginning you should have configured DNS, NTP, and [LDAP](#) on the storage system.



### Steps

1. At the ONTAP command line, set UNIX permissions for the storage VM root volume.
  - a. Display the relevant permissions on the storage VM root volume: `volume show -volume root_vol_name-fields user,group,unix-permissions`

The root volume of the storage VM must have the following configuration:

| Name...          | Setting...   |
|------------------|--------------|
| UID              | root or ID 0 |
| GID              | root or ID 0 |
| UNIX permissions | 755          |

- b. If these values are not shown, use the `volume modify` command to update them.
2. Set user permissions for the storage VM root volume.
  - a. Display the local UNIX users: `vserver services name-service unix-user show -vserver vserver_name`

The storage VM should have the following UNIX users configured:

| User name | User ID | Primary group ID |
|-----------|---------|------------------|
| nfs       | 500     | 0                |
| root      | 0       | 0                |



**Note:** The NFS user is not required if a Kerberos-UNIX name mapping exists for the SPN of the NFS client user; see step 5.

- b. If these values are not shown, use the `vserver services name-service unix-user modify` command to update them.
3. Set group permissions for the storage VM root volume.

- a. Display the local UNIX groups: `vserver services name-service unix-group show -vserver vserver_name`

The storage VM should have the following UNIX groups configured:

| Group name | Group ID |
|------------|----------|
| daemon     | 1        |
| root       | 0        |

- b. If these values are not shown, use the `vserver services name-service unix-group modify` command to update them.
4. Switch to System Manager to configure Kerberos
5. In ONTAP System Manager, click **Storage** > **Storage VMs** and select the storage VM.
6. Click **Settings**.
7. Click  under Kerberos.
8. Click **Add** under Kerberos Realm, and complete the following sections:
  - Add Kerberos Realm  
  
Enter configuration details depending on KDC vendor.
  - Add Network Interface to Realm  
  
Click **Add** and select a network interface.
9. If desired, add mappings from Kerberos principal names to local user names.
  - a. Click **Storage** > **Storage VMs** and select the storage VM.
  - b. Click **Settings**, and then click  under **Name Mapping**.
  - c. Under **Kerberos to UNIX**, add patterns and replacements using regular expressions.

## Provide client access with name services



Enable ONTAP to look up host, user, group, or netgroup information using LDAP or NIS to authenticate NAS clients.

This procedure creates or modifies LDAP or NIS configurations on an existing storage VM enabled for [NFS](#) or [SMB](#).

For LDAP configurations, you should have the LDAP configuration details required in your environment and you should be using a default ONTAP LDAP schema.

### Steps

1. Configure the required service: click **Storage** > **Storage VMs**.

2. Select the storage VM, click **Settings**, and then click  for LDAP or NIS.
3. Include any changes in the name services switch: click  under Name Services Switch.

## Provision NAS storage for large file systems using FlexGroup volumes

A FlexGroup volume is a scalable NAS container that provides high performance along with automatic load distribution. FlexGroup volumes provide massive capacity (in petabytes), which considerably exceeds the FlexVol volume limits, without adding any management overhead.

ONTAP automatically selects the local tiers required for creating the FlexGroup volume.



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

### *Steps*

1. Click **Storage > Volumes**.
2. Click **Add**.
3. Click **More Options** and then select **Distribute volume data across the cluster**.

If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then select **Performance Service Level**.

## Monitor volume usage with ONTAP File System Analytics

### File System Analytics overview

File System Analytics is a framework for collecting and displaying data about the contents of a FlexGroup or FlexVol volume.

File system analytics presents detailed information at each level of the volume's file system hierarchy, allowing you to:

- Assess capacity usage and trends
- Monitor file and directory counts
- Evaluate file activity and history

In ONTAP 9.8 and later, file system analytics can be displayed using ONTAP System Manager. You can also use ONTAP REST APIs to access the data programmatically.



Enabling file system analytics is expected to have a performance impact. Do not enable analytics if maximal performance is required in your environment. You can also disable analytics if your testing shows that the performance impact is unacceptable. When you disable analytics, previously collected data is no longer displayed for that volume.

File system analytics is not available for the following volume types:

- SnapMirror destination volumes
- SnapLock volumes
- Volumes containing LUNs
- Volumes used for SMB/CIFS audit
- Volumes transitioned from 7-mode systems
- Node root volumes (/mroot)

## Enable File System Analytics

To collect and display usage data, you must enable file system analytics. You can do so using System Manager, the ONTAP CLI, or REST APIs.

You can enable file system analytics when you create a new volume, or when you upgrade a system with volumes to ONTAP 9.8 or later. After upgrading, be sure that all upgrade processes have completed before enabling analytics.

Depending on the size and contents of the volume, enabling analytics might take some time while ONTAP processes existing data in the volume. System Manager displays progress and presents analytics data when complete. If you need more precise information about initialization progress, you can use the ONTAP CLI command `volume analytics show`.

### Steps

1. Click **Storage > Volumes**, then select the desired volume.
2. Click **Explorer**, then click **Enable Analytics** or **Disable Analytics**.

## View file system activity

After File System Analytics is enabled, by default, you can view the root directory contents of a selected volume sorted by the spaced used in each subtree

Clicking on any file system object allows you to browse the file system and to display detailed

information about each object in a directory. Information about directories can also be displayed graphically. Over time, historical data is displayed for each subtree. Space used is not sorted if there are more than 3000 records.

The file system analytics **Explorer** screen consists of three areas:

- Tree view of directories and subdirectories; expandable list showing name, size, modify history, and access history.
- Files; showing name, size, and accessed time for the object selected in the directory list.
- Active and inactive data comparison for the object selected in the directory list.

Accessed time is shown by default. However, if the volume default has been altered from the CLI, by setting the `-atime-update` option to `false` with the `volume modify` command, only last modified time is shown. For example:

- The tree view will not display the **access history**.
- The files view will be altered.
- The active/inactive data view will be based on modified time (`mtime`).

Using these displays, you can examine the following:

- File system locations consuming the most space
- Detailed information about a directory tree, including file and subdirectory count within directories and subdirectories
- File system locations that contain old data (for example, scratch, temp, or log trees)

Keep the following points in mind when interpreting file system analytics output:

- File system analytics show where and when your data is in use, not how much data is being processed. For example, large space consumption by recently accessed or modified files does not necessarily indicate high system processing loads.
- The way that the **Volume Explorer** tab calculates space consumption for file system analytics might differ from other tools. In particular, there could be significant differences compared to the consumption reported in the **Volume Overview** if the volume has storage efficiency features enabled. This is because the **Volume Explorer** tab does not include efficiency savings.

### *Steps*

1. Click **Storage > Volumes**, select the desired volume, then click **Explorer**.

## Monitor NFS active clients

Beginning with ONTAP 9.8, System Manager shows which NFS client connections are active when NFS is licensed on a cluster.

This allows you to quickly verify which NFS clients are actively connect to a storage VM, which are connected but idle, and which are disconnected.

For each NFS client IP address, the **NFS Clients** display shows:

- \* Time of last access
- \* Network interface IP address
- \* NFS connection version
- \* Storage VM name

In addition, a list of NFS clients active in the last 48 hours is also shown in the **Storage>Volumes** display and a count of NFS clients is includes in the **Dashboard** display.

#### *Step*

1. Display NFS client activity: Click **Hosts > NFS Clients**.

## Improve performance for multiple clients with FlexCache

You can use FlexCache volumes to speed up access to data or to offload traffic from heavily accessed volumes. FlexCache volumes are ideal for read-intensive workloads, especially where clients need to access the same data repeatedly.

The FlexCache volume can be on the same cluster as or on a different cluster than that of the remote volume. If the remote volume is on a different cluster, you need to have already peered the clusters and storage VMs.



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.

#### *Steps*

1. Click **Storage > Volumes**.
2. Click **Add**.
3. Click **More Options** and then select **Add as cache for a remote volume**.

If you are running ONTAP 9.8 or later and you want to disable QoS or choose a custom QoS policy, click **More Options** and then select **Performance Service Level**.

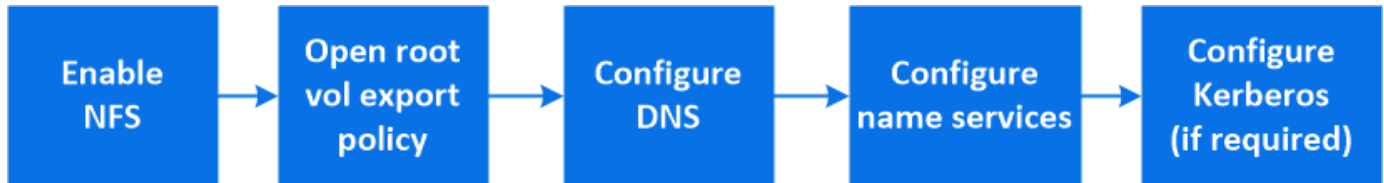
For any new data requests, the FlexCache volume requests the data from the remote volume and stores it. All the subsequent read requests for the data are then served directly from the FlexCache volume.

# Enable NAS storage






## Enable NAS storage for Linux servers using NFS

Modify storage VMs to enable NFS servers for serving data to Linux clients.

This procedure enables an existing storage VM. It is assumed that configuration details are available for any authentication or security services required in your environment.



### Steps

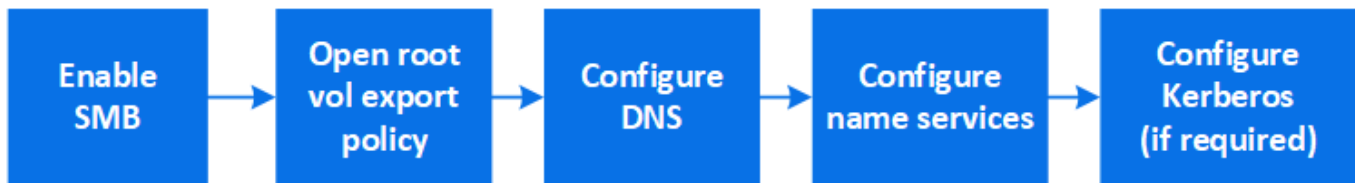
1. Enable NFS on an existing VM: click **Storage** > **Storage VMs**, select a storage VM, click **Settings**, and then click  under **NFS**.
2. Open the export policy of the storage VM root volume:
  - a. Click **Storage** > **Volumes**, select the root volume of the storage VM (which by default is *volume-name\_root*), and then click on the policy that is displayed under **Export Policy**.
  - b. Click **Add** to add a rule.
    - Client specification = *0.0.0.0/0*
    - Access protocols = NFS
    - Access details = UNIX Read-Only
3. Configure DNS for host-name resolution: click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click  under **DNS**.
4. Configure name services as required.
  - a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click for  LDAP or NIS.
  - b. Include any changes in the name services switch file: click  in the Name Services Switch tile.
5. Configure Kerberos if required:
  - a. Click **Storage** > **Storage VMs**, select the storage VM, and then click **Settings**.
  - b. Click  in the Kerberos tile and then click **Add**.

## Enable NAS storage for Windows servers using SMB/CIFS






Modify storage VMs to enable SMB servers for serving data to Windows clients.

This procedure enables an existing storage VM. It is assumed that configuration details are available

for any authentication or security services required in your environment.



### Steps

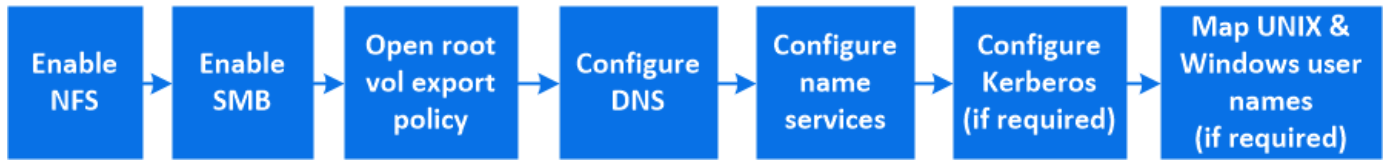
1. Enable SMB/CIFS on an existing VM: click **Storage** > **Storage VMs**, select a storage VM, click **Settings**, and then click  under **SMB/CIFS**.
2. Open the export policy of the storage VM root volume:
  - a. Click **Storage** > **Volumes**, select the root volume of the storage VM (which by default is *volume-name\_root*), and then click on the policy that is displayed under **Export Policy**.
  - b. Click **Add** to add a rule.
    - Client specification = **0.0.0.0/0**
    - Access protocols = SMB/CIFS
    - Access details = NTFS Read-Only
3. Configure DNS for host-name resolution:
  - a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click  under **DNS**.
  - b. Switch to the DNS server and map the SMB server.
    - Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.
    - If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data network interface.
4. Configure name services as required
  - a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click  under **LDAP** or **NIS**.
  - b. Include any changes in the name services switch file: click  under **Name Services Switch**.
5. Configure Kerberos if required:
  - a. Click **Storage** > **Storage VMs**, select the storage VM, and then click **Settings**.
  - b. Click  under **Kerberos** and then click **Add**.

## Enable NAS storage for both Windows and Linux using both NFS and SMB/CIFS








Modify storage VMs to enable NFS and SMB servers to serve data to Linux and Windows clients.



This procedure enables an existing storage VM. It is assumed that configuration details are available for any authentication or security services required in your environment.



### Steps

1. Enable NFS on an existing VM: click **Storage** > **Storage VMs**, select a storage VM, click **Settings**, and then click  under **NFS**.
2. Enable SMB/CIFS on an existing VM: click  under **SMB/CIFS**.
3. Open the export policy of the storage VM root volume:
  - a. Click **Storage** > **Volumes**, select the root volume of the storage VM (which by default is *volume-name\_root*), and then click on the policy that is displayed under **Export Policy**.
  - b. Click **Add** to add a rule.
    - Client specification = **0.0.0.0/0**
    - Access protocols = NFS
    - Access details = NFS Read-Only
4. Configure DNS for host-name resolution:
  - a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click  under **DNS**.
  - b. When DNS configuration is complete, switch to the DNS server and map the SMB server.
    - Create forward (A - Address record) and reverse (PTR - Pointer record) lookup entries to map the SMB server name to the IP address of the data network interface.
    - If you use NetBIOS aliases, create an alias canonical name (CNAME resource record) lookup entry to map each alias to the IP address of the SMB server's data network interface.
5. Configure name services as required:
  - a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click  for LDAP or NIS.
  - b. Include any changes in the name services switch file: click  under **Name Services Switch**.
6. Configure Kerberos if required: click  in the Kerberos tile and then click **Add**.
7. Map UNIX and Windows user names if required: click  under **Name Mapping** and then click **Add**.

You should use this procedure only if your site has Windows and UNIX user accounts that do not map implicitly, which is when the lowercase version of each Windows user name matches the UNIX user name. This procedure can be done using LDAP, NIS, or local users. If you have two sets of users that do not match, you should configure name mapping.

# Provision object storage

## ONTAP S3 overview

Beginning with ONTAP 9.8, you can enable an ONTAP Simple Storage Service (S3) object storage server in an ONTAP cluster.

System Manager supports two on-premises use case scenarios for serving S3 object storage:

- FabricPool tier to a bucket on local cluster (tier to a local bucket) or remote cluster (cloud tier).
- S3 client app access to a bucket on the local cluster or a remote cluster.

For more information about tiering, see [Cloud overview](#).



ONTAP S3 is appropriate if you want S3 capabilities on existing clusters without additional hardware and management. For deployments larger than 300TB, NetApp StorageGRID software continues to be the NetApp flagship solution for object storage. For more information, see the [StorageGRID documentation](#).

When you create an S3 bucket using System Manager, ONTAP configures a default performance service level that is the highest available on your system. For example, on an AFF system, the default setting would be **Extreme**. Performance service levels are predefined adaptive Quality of Service (QoS) policy groups. Instead of one of the default service levels, you can specify a custom QoS policy group or no policy group.

Predefined adaptive QoS policy groups are:

- **Extreme**: Used for applications that expect the lowest latency and highest performance.
- **Performance**: Used for applications with modest performance needs and latency.
- **Value**: Used for applications for which throughput and capacity are more important than latency.
- **Custom**: Specify a custom QoS policy or no QoS policy.

If you select **Use for tiering**, no performance service levels are selected, and the system tries to select low-cost media with optimal performance for the tiered data.

See also: [Using adaptive QoS policy groups](#).

ONTAP tries to provision this bucket on local tiers that have the most appropriate disks, satisfying the chosen service level. However, if you need to specify which disks to include in the bucket, consider configuring S3 object storage from the CLI by specifying the local tiers (aggregate). If you configure the S3 server from the CLI, you can still manage it with System Manager if desired. For more information, see [S3 Configuration Power Guide](#).

# Enable an S3 server on a storage

Add an S3 server to a new or existing storage VM for serving content to S3 clients.

An S3 server can coexist in a storage VM with other protocol servers, or you can create a new storage VM to isolate the namespace and workload.

## *Before you begin*

You should be prepared to enter an S3 server name (FQDN) and IP addresses for interface role Data.

If you are using an external-CA signed certificate, you will be prompted to enter it during this procedure; you also have the option to use a system-generated certificate.

## *Steps*

1. Enable S3 on a storage VM.

- a. Add a new storage VM: click **Storage** > **Storage VMs**, then click **Add**.

If this is a new system with no existing storage VMs: click **Dashboard** > **Configure Protocols**.

If you are adding an S3 server to an existing storage VM: click **Storage** > **Storage VMs**, select a storage VM, click **Settings**, and then click  under **S3**.

- b. Click **Enable S3**, then enter the S3 Server Name.

This will be the Fully Qualified Domain Name (FQDN) that clients will use.

- c. Select the certificate type.

Whether you select system-generated certificate or one of your own, it will be required for client access.

- d. Enter the network interfaces.

2. If you selected the system-generated certificate, you see the certificate information when the new storage VM creation is confirmed. Click **Download** and save it for client access.

- The secret key will not be displayed again.
- If you need the certificate information again: click **Storage** > **Storage VMs**, select the storage VM, and click **Settings**.

# Provision buckets

Add an S3 bucket for the new S3 object store or add additional buckets to an existing object store.


For remote client access, you must configure buckets in an S3-enabled storage VM. If you create a

bucket in a storage VM that is not S3-enabled, it will only be available for local tiering.



Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process or at a later time.


### Steps

1. Add a new bucket on an S3-enabled storage VM.
    - a. Click **Storage > Buckets**, then click **Add**.
    - b. Enter a name, select the storage VM, and enter a size.
      - If you click **Save** at this point, a bucket is created with these default settings:
        - No users are granted access to the bucket unless any group policies are already in effect.
- 
- You should not use the S3 root user to manage ONTAP object storage and share its permissions, because it has unlimited access to the object store. Instead, create a user or group with administrative privileges that you assign.
- A Quality of Service (performance) level that is the highest available for your system.
    - You can click **More Options** to configure user permissions and performance level when you configure the bucket, or you can modify these settings later.
      - You must have already created user and groups before using **More Options** to configure their permissions.
      - If you intend to use the S3 object store for FabricPool tiering, consider selecting **Use for tiering** (use low-cost media with optimal performance for the tiered data) rather than a performance service level.
  2. On S3 client apps – another ONTAP system or an external 3rd-party app – verify access to the new bucket by entering the following:
    - The S3 server CA certificate.
    - The user's access key and secret key.
    - The S3 server FQDN name and bucket name.

## Add S3 users and groups

Edit the storage VM to add users, and to add users to groups.

### Steps

1. Edit the storage VM: click **Storage > storage VMs**, click the storage VM, click **Settings** and then click  under S3.

2. Add a user: click **Users**, then click **Add**.
  - a. Enter a name and click **Save**.
  - b. Be sure to save the access key and secret key, they will be required for access from S3 clients.
3. If desired, add a group: click **Groups**, then click **Add**.
  - a. Enter a group name and select from a list of users.
  - b. You can select an existing group policy or add one now, or you can add a policy later.

## Manage user access to buckets

Edit the bucket to modify the list users with access to the bucket and specify their permissions.

User and group permissions can be granted when the bucket is created or as needed later. You can also modify the bucket capacity and QoS policy group assignment.

You must have already created users or groups before granting permissions.

### *Steps*

1. Edit the bucket: click **Storage > Buckets**, click the desired bucket, and then click **Edit**.

When adding or modifying permissions, you can specify the following parameters:

- Principal: the user or group to whom access is granted.
- Effect: allows or denies access to a user or group.
- Actions: permissible actions in the bucket for a given user or group.
- Resources: paths and names of objects within the bucket for which access is granted or denied.

The defaults ***bucketname*** and ***bucketname/\**** grant access to all objects in the bucket. You can also grant access to single objects; for example, ***bucketname/\*\_readme.txt***.

- Conditions (optional): expressions that are evaluated when access is attempted. For example, you can specify a list of IP addresses for which access will be allowed or denied.


## Manage user access to S3-enabled storage VMs

Edit the storage VM to add a policy that controls user and group access permissions to multiple buckets.

You can add a group policy to manage access to one or more buckets in an S3-enabled storage VM, rather than managing access permissions for individual buckets. Doing so simplifies management when buckets are added or when access needs change.

You must have already created users and at least one group before granting permissions in a policy.

## Steps

1. Edit the storage VM: click **Storage** > **storage VMs**, click the storage VM, click **Settings** and then click  under S3.
2. Add a user: click **Policies**, then click **Add**.
  - a. Enter a policy name and select from a list of groups.
  - b. Select an existing default policy or add a new one.

When adding or modifying a group policy, you can specify the following parameters:

- **Group**: the groups to whom access is granted.
- **Effect**: allows or denies access to one or more groups.
- **Actions**: permissible actions in one or more buckets for a given group.
- **Resources**: paths and names of objects within one or more buckets for which access is granted or denied.

For example:

- **\*** grants access to all buckets in the storage VM.
  - **bucketname** and **bucketname/\*** grant access to all objects in a specific bucket.
  - **bucketname/readme.txt** grants access to an object in a specific bucket.
- c. If desired, add statements to existing policies.

# Manage resources using quotas

## Quota overview

Quotas provide a way to restrict or track the disk space and number of files used by a user, group, or qtree. Quotas are applied to a specific volume or qtree.

You can use quotas to track and limit resource usage in volumes and provide notification when resource usage reaches specific levels.

Quotas can be soft or hard. Soft quotas cause ONTAP to send a notification when specified limits are exceeded, and hard quotas prevent a write operation from succeeding when specified limits are exceeded.

## Set quotas to limit resource use

Add quotas to limit the amount of disk space the quota target can use.

You can set a hard limit and a soft limit for a quota.

Hard quotas impose a hard limit on system resources; any operation that would result in exceeding the limit fails. Soft quotas send a warning message when resource usage reaches a certain level, but they do not affect data access operations, so you can take appropriate action before the quota is exceeded.

### *Steps*

1. Click **Storage > Quotas**.
2. Click **Add**.

# Maximize security

## Security overview

With System Manager, you use ONTAP standard methods to secure client and administrator access to storage and to protect against viruses. Advanced technologies are available for encryption of data at rest and for WORM storage.

### Client authentication and authorization

ONTAP authenticates a client machine and user by verifying their identities with a trusted source. ONTAP authorizes a user to access a file or directory by comparing the user's credentials with the permissions configured on the file or directory.

### Administrator authentication and RBAC

Administrators use local or remote login accounts to authenticate themselves to the cluster and storage VM. Role-Based Access Control (RBAC) determines the commands to which an administrator has access.

### Virus scanning

You can use integrated antivirus functionality on the storage system to protect data from being compromised by viruses or other malicious code. ONTAP virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

### Encryption

ONTAP offers both software- and hardware-based encryption technologies for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen.

### WORM storage

*SnapLock* is a high-performance compliance solution for organizations that use *write once, read many (WORM)* storage to retain critical files in unmodified form for regulatory and governance purposes.

## Set up multifactor authentication

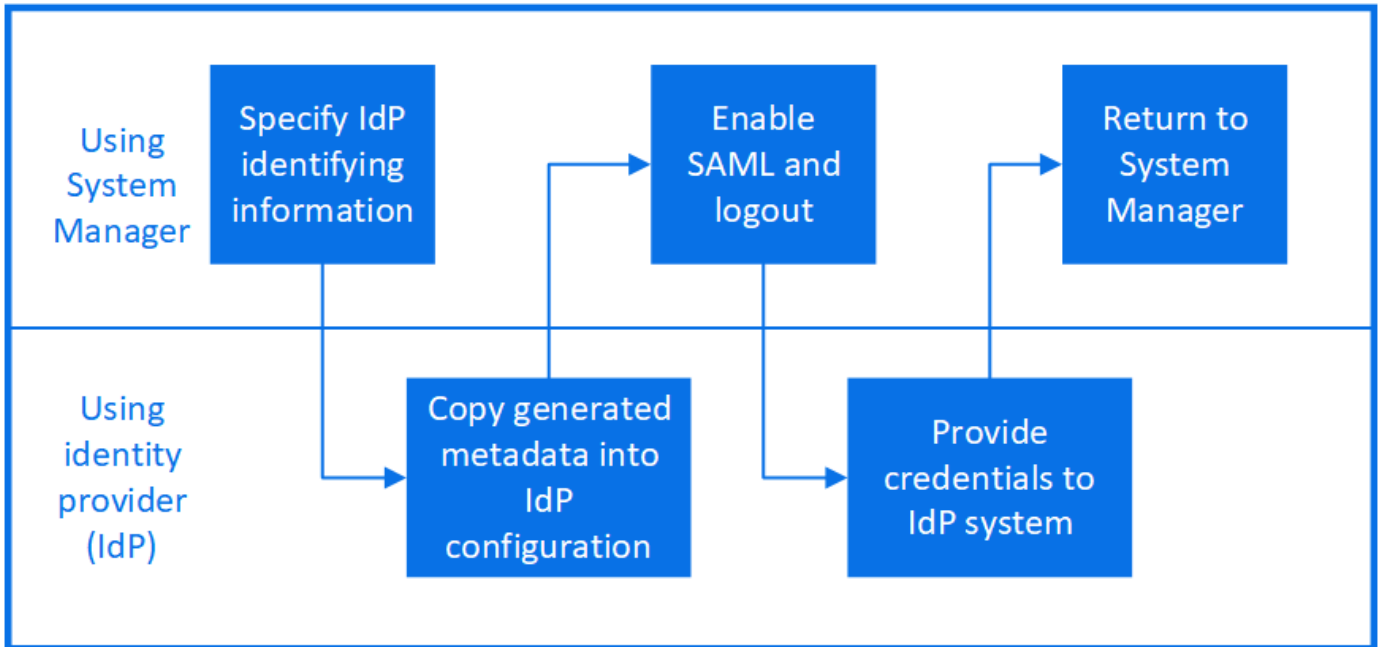
Security Assertion Markup Language (SAML) authentication allows users to log in to an application by using a secure identity provider (IdP).

In System Manager, in addition to standard ONTAP authentication, SAML-based authentication is provided as an option for multifactor authentication.




Security Assertion Markup Language (SAML) is an XML-based framework for authentication and authorization between two entities: a service provider and an identity provider.

## Enable SAML authentication



To enable SAML authentication, perform the following steps:

### Steps


1. Click **Cluster > Settings**.
2. Next to **SAML Authentication**, click .
3. Ensure there is a check in the **Enable SAML Authentication** checkbox.
4. Enter the URL of the IdP URI (including "https://").
5. Modify the host system address, if needed.
6. Ensure the correct certificate is being used:
  - If your system was mapped with only one certificate with type "server", then that certificate is considered the default and it isn't displayed.
  - If your system was mapped with multiple certificates as type "server", then one of the certificates is displayed. To select a different certificate, click **Change**.
7. Click **Save**. A confirmation window displays the metadata information, which has been automatically copied to your clipboard.
8. Go to the IdP system you specified and copy the metadata from your clipboard to update the system metadata.
9. Return to the confirmation window (in System Manager) and check the checkbox **I have configured the IdP with the host URI or metadata**.

10. Click **Logout** to enable SAML-based authentication. The IdP system will display an authentication screen.
11. In the IdP system, enter your SAML-based credentials. After your credentials are verified, you will be directed to the System Manager home page.

## Disable SAML authentication

To disable SAML authentication, perform the following steps:

### Steps

1. Click **Cluster > Settings**.
2. Under **SAML Authentication**, click the **Enabled** toggle button.
3. *Optional:* You can also click  next to **SAML Authentication**, and then uncheck the **Enable SAML Authentication** checkbox.

## Control administrator access

The role assigned to an administrator determines which functions the administrator can perform with System Manager. Predefined roles for cluster administrators and storage VM administrators are provided by System Manager. You assign the role when you create the administrator's account, or you can assign a different role later.

Depending on how you have enabled account access, you might need to perform any of the following:



- Associate a public key with a local account.
- Install a CA-signed server digital certificate.
- Configure AD, LDAP, or NIS access.

You can perform these tasks before or after enabling account access.

## Assigning a role to an administrator

Assign a role to an administrator, as follows:


### Steps

1. Click **Cluster > Settings**.
2. Click  next to **Users and Roles**.
3. Click  **Add** under **Users**.
4. Specify a user name, and select a role in the drop-down menu for **Role**.
5. Specify a login method and password for the user.

## Changing an administrator's role

Change the role for an administrator, as follows:

### *Steps*

1. Click **Cluster** > **Settings**.
2. Select the name of user whose role you want to change, then click the  that appears next to the user name.
3. Click **Edit**.
4. Select a role in the drop-down menu for **Role**.



## Encrypt stored data using software-based encryption

Use volume encryption to ensure that volume data cannot be read if the underlying device is repurposed, returned, misplaced, or stolen. Volume encryption does not require special disks; it works with all HDDs and SSDs.

Volume encryption requires a key manager. You can configure the Onboard Key Manager using ONTAP System Manager. You can also use an external key manager, but you need to first set it up using the ONTAP CLI.

After the key manager is configured, new volumes are encrypted by default.

### *Steps*

1. Click **Cluster** > **Settings**.
2. Under **Encryption**, click  to configure the Onboard Key Manager for the first time.
3. To encrypt existing volumes, click **Storage** > **Volumes**.
4. On the desired volume, click  and then click **Edit**.
5. Select **Enable encryption**.

## Encrypt stored data using self-encrypting drives



Use disk encryption to ensure that all data in a local tier cannot be read if the underlying device is repurposed, returned, misplaced, or stolen. Disk encryption requires special self-encrypting HDDs or SSDs.

Disk encryption requires a key manager. You can configure the onboard key manager using ONTAP System Manager. You can also use an external key manager, but you need to first set it up using the ONTAP CLI.

If ONTAP detects self-encrypting disks, it prompts you to configure the onboard key manager when you

create the local tier.


#### *Steps*

1. Under **Encryption**, click  to configure the onboard key manager.
2. If you see a message that disks need to be rekeyed, click , and then click **Rekey Disks**.

## Diagnose and correct file access issues

Starting with ONTAP 9.8, you can trace file access permissions with System Manager to diagnose why clients cannot access files.

#### *Steps*

1. In ONTAP System Manager, select **Storage > Storage VMs**.
2. Select the storage VM on which you want to perform a trace.
3. Click  **More**.
4. Click **Trace File Access**.
5. Provide the user name and client IP address, then click **Start Tracing**.

The trace results are displayed in a table. The **Reasons** column provides the reason why a file could not be accessed.

6. Click  in the left column of the results table to view the file access permissions.

# Protect data

## Data protection overview

Protect your data by creating and managing Snapshot copies, mirrors, vaults, and mirror-and-vault relationships.

*SnapMirror* is disaster recovery technology, designed for failover from primary storage to secondary storage at a geographically remote site. As its name implies, SnapMirror creates a replica, or mirror, of your working data in secondary storage from which you can continue to serve data in the event of a catastrophe at the primary site.




A *vault* is designed for disk-to-disk Snapshot copy replication for standards compliance and other governance-related purposes. In contrast to a SnapMirror relationship, in which the destination usually contains only the Snapshot copies currently in the source volume, a vault destination typically retains point-in-time Snapshot copies created over a much longer period.

## Configure Snapshot copies

You can create Snapshot copy policies to specify the maximum number of Snapshot copies that are automatically created and how frequently they are created. The policy specifies when to create Snapshot copies, how many copies to retain, and how to name them.

This procedure creates a Snapshot copy policy on the local cluster only.

### Steps

1. Click **Protection > Overview > Local Policy Settings**.
2. Under **Snapshot Policies**, click , and then click  **Add**.
3. Type the policy name, select the policy scope, and under **Schedules**, click  **Add** to enter the schedule details.

## Recover from Snapshot copies

You can recover a volume to an earlier point in time by restoring from a Snapshot copy.

This procedure restores a volume from a Snapshot copy.

### Steps

1. Click **Storage** and select a volume.

2. Under **Snapshot Copies**, click  next to the Snapshot copy you want to restore, and select **Restore**.

## Prepare for mirroring and vaulting

You can protect your data by replicating it to a remote cluster for data backup and disaster recovery purposes.




Several default protection policies are available. You must have created your protection policies if you want to use custom policies.



### Steps

1. In the local cluster, click **Protection > Overview**.
2. Expand **Intercluster Settings**. Click **Add Network Interfaces** and add intercluster network interfaces for the cluster.

Repeat this step on the remote cluster.

3. In the remote cluster, click **Protection > Overview**. Click  in the Cluster Peers section and click **Generate Passphrase**.
4. Copy the generated passphrase and paste it in the local cluster.
5. In the local cluster, under Cluster Peers, click **Peer Clusters** and peer the local and remote clusters.
6. Optionally, under Storage VM Peers, click  and then **Peer Storage VMs** to peer the storage VMs.
7. Click **Protect Volumes** to protect your volumes. To protect your LUNs, click **Storage > LUNs**, select a LUN to protect, and then click  **Protect**.

Select the protection policy based on the type of data protection you need.

8. To verify the volumes and LUNs are successfully protected from the local cluster, click **Storage > Volumes** or **Storage > LUNs** and, expand the volume/LUN view.

## Configure mirrors and vaults


Create a mirror and vault of a volume to protect data in case of a disaster and to have multiple archived versions of data to which you can roll back. Only the combined mirror-and-vault policy is supported. You cannot specify separate mirror

and vault policies.

This procedure creates a mirror-and-vault policy on a remote cluster. The source cluster and destination cluster use intercluster network interfaces for exchanging data. The procedure assumes the [intercluster network interfaces are created and the clusters containing the volumes are peered](#) (paired). You can also peer storage VMs for data protection; however, if storage VMs are not peered, but permissions are enabled, storage VMs are automatically peered when the protection relationship is created.



#### Steps


1. Select the volume or LUN to protect: click **Storage > Volumes** or **Storage > LUNs**, and then click the desired volume or LUN name.
2. Click  **Protect**.
3. Select the destination cluster and storage VM.
4. The asynchronous policy is selected by default. To select a synchronous policy, click **More Options**.
5. Click **Protect**.
6. Click the **SnapMirror (Local or Remote)** tab for the selected volume or LUN to verify that protection is set up correctly.

## Serve data from a SnapMirror destination

To serve data from a mirror destination when a source becomes unavailable, stop scheduled transfers to the destination, and then break the SnapMirror relationship to make the destination writable.



#### Steps

1. Select the desired protection relationship: click **Protection > Relationships**, and then click the desired volume name.
2. Click .
3. Stop scheduled transfers : click **Pause**.

4. Make the destination writable: click **Break**.
5. Go to the main **Relationships** page to verify that the relationship state displays as "broken off".

*Next steps:*


When the disabled source volume is available again, you should resynchronize the relationship to copy the current data to the original source volume. This process replaces the data on the original source volume.

## Resynchronize a protection relationship

When your original source volume is available again after a disaster, you can resynchronize data from the destination volume and reestablish the protection relationship.

This procedure replaces the data in the original source volume in an asynchronous relationship so that you can start serving data from the original source volume again and resume the original protection relationship.

*Steps*


1. Click **Protection** > **Relationships** and then click the broken off relationship you want to resynchronize.
2. Click  and then select **Resync**.
3. Under **Relationships**, monitor the resynchronization progress by checking the relationship state. The state changes to "Mirrored" when resynchronization is complete.

## Restore a volume from an earlier Snapshot copy

When data in a volume is lost or corrupted, you can roll back your data by restoring from an earlier Snapshot copy.

This procedure replaces the current data on the source volume with data from an earlier Snapshot copy version. You should perform this task on the destination cluster.

*Steps*

1. Click **Protection** > **Relationships**, and then click the source volume name.
2. Click  and then select **Restore**.
3. Under **Source**, the source volume is selected by default. Click **Other Volume** if you want to choose a different volume.
4. Under **Destination**, choose the Snapshot copy you want to restore.
5. If your source and destination are located on different clusters, on the remote cluster, click **Protection** > **Relationships** to monitor the restore progress.




## Restore to a new volume

Starting in System Manager 9.8, you can restore backed up data on the destination volume to a volume other than the original source.

When you restore to a different volume, you can select an existing volume, or you can create a new volume.

### *Steps*


1. Select the desired protection relationship: click **Protection** > **Relationships**.
2. Click  and click **Restore**.
3. Under **Relationships**, monitor the restore progress by viewing **Transfer Status** for the relationship.

## Reverse Resynchronizing a Protection Relationship

Starting in System Manager 9.8, you can perform a reverse resynchronization operation to delete an existing protection relationship and reverse the functions of the source and destination volumes. Then you use the destination volume to serve data while you repair or replace the source, update the source, and reestablish the original configuration of the systems.

When you perform a reverse resynch operation, any data on the source volume that is newer than the data in the common Snapshot copy is deleted.


### *Steps*

1. Select the desired protection relationship: click **Protection** > **Relationships**.
2. Click  and click **Reverse Resync**.
3. Under **Relationships**, monitor the reverse resynchronization progress by viewing **Transfer Status** for the relationship.

## Reactivate a source storage VM

Starting in System Manager 9.8, you can reactivate a source storage VM after a disaster. Reactivating the source storage VM stops the destination storage VM, and it reenables replication from the source to the destination.

### *Steps*

1. Select the desired protection relationship: click **Protection** > **Relationships**.
2. Click  and click **Reactivate Source Storage VM**.


3. Under **Relationships**, monitor the source reactivation progress by viewing **Transfer Status** for the protection relationship.

## Resynchronize a destination storage VM

You can resynchronize the data and configuration details from the source SVM to the destination SVM in a broken protection relationship and reestablish the relationship.

You perform the resync operation only from the destination of the original relationship. The resync deletes any data in the destination storage VM that is newer than the data in the source storage VM.

### *Steps*

1. Select the desired protection relationship: click **Protection** > **Relationships**.
2. Click  and click **Resync**.
3. Under **Relationships**, monitor the resynchronization progress by viewing **Transfer Status** for the relationship.

# Extend to the cloud

## Cloud overview

You can use FabricPool to automatically tier data depending on how frequently the data is accessed.

FabricPool is a hybrid storage solution that uses an all flash (all SSD) aggregate as the performance tier and an object store as the cloud tier. Using a FabricPool helps you reduce storage cost without compromising performance, efficiency, or protection.

The cloud tier can be located on NetApp StorageGRID or ONTAP S3 (beginning with ONTAP 9.8), or one of the following service providers:

- Alibaba cloud
- Amazon S3
- Google Cloud
- IBM cloud
- Microsoft Azure Blob Storage

## Tier data to cloud

Storing data in tiers can enhance the efficiency of your storage system. You can manage storage tiers by using FabricPool to store data in a tier, based on how frequently the data is accessed.

This procedure sets up an object store as the cloud tier for FabricPool. Keep in mind that once you attach to a local tier (aggr) the cloud tier cannot be unattached.

A FabricPool license is not required when using StorageGRID or ONTAP S3 as the cloud tier or when using Amazon S3, Google Cloud Storage, or Microsoft Azure Blob Storage as the cloud tier for Cloud Volumes for ONTAP. A FabricPool license is required for other cloud tier locations.

If you are tiering to ONTAP S3, there are additional requirements:

- \* There must be an entry for the remote ONTAP S3 server's hostname in the DNS server configured for the admin storage VM, including the S3 server's FQDN name and the IP addresses on its network interfaces.
- \* [Intercluster network interfaces](#) must be configured on both local and remote clusters, although cluster peering is not required.

You also have the option to create a volume tiering policy in System Manager.

### *Steps*

1. Click **Storage > Tiers > Add Cloud Tier** and select the object store provider you want to use.
2. If you want to create a cloud mirror, click **Add as FabricPool Mirror**.

## Tier data to local bucket


Beginning with ONTAP 9.8, you can tier data to local object storage using ONTAP S3.

Tiering data to a local bucket provides a simple alternative to moving data to a different local tier. This procedure uses an existing bucket on the local cluster, or you can let ONTAP automatically create a new storage VM and a new bucket.

Keep in mind that once you attach to a local tier (aggr) the cloud tier cannot be unattached.

An S3 license is required for this workflow, which creates a new S3 server and new bucket, or uses existing ones. A FabricPool license is not required for this workflow.

### *Step*

1. Tier data to a local bucket: click **Tiers**, select a tier, then click .
  - You have the option to create a new tier (ONTAP S3) or use an existing one.
  - You have the option to edit an existing volume tiering policy.

## Create tags for tiering objects

Starting in ONTAP 9.8, you can create object tags to help you classify and sort tiering objects for easier data management. You can set tags only on FabricPool volumes attached to StorageGRID. These tags are retained during a volume move.

### *Steps*

1. Navigate to **Storage > Tiers > Volumes**.
2. Locate the volume you want to tag and select **Click to enter tags**.


## Enable inactive data reporting

Starting in ONTAP 9.8, you can enable inactive data reporting to show how much inactive data can be tiered to the cloud.

You can enable inactive data reporting on HDD aggregates.

### *Steps*

1. Choose one of the following options:

- When you have existing HDD aggregates, navigate to **Storage** > **Tiers** and click  for the aggregate on which you want to enable inactive data reporting.
- When no cloud tiers are configured, navigate to **Dashboard** and click the **Enable inactive data reporting** link under **Capacity**.

# View cluster performance

## Cluster performance overview

ONTAP System Manager provides an easy interface that lets you create and manage clusters in your environment.

The System Manager Dashboard lets you determine the following information:

- **Health:** You can monitor the health of a cluster. Alerts are shown when problems arise.
- **Capacity:** System Manager shows you the available capacity on the cluster.
- **Performance:** You can monitor how well the cluster is performing, based on latency, IOPS, and throughput. The metrics are graphed every 15 seconds by hour, day, week, month, or year.
- **Network:** You can view how the network is configured with hosts and storage objects. You can view the number of ports that are available and the interfaces and storage VMs that are associated with them.

## View performance on cluster dashboard

Use the dashboard to make informed decisions about workloads you might want to add or move. You can also look at peak usage times to plan for potential changes.

The performance values refresh every 3 seconds and the performance graph refreshes every 15 seconds.

### *Steps*

1. Click **Dashboard**.
2. Under **Performance**, select the interval.

## Identify hot volumes and other objects

Accelerate your cluster performance by identifying the frequently accessed volumes (hot volumes) and data (hot objects).

### *Steps*

1. Click **Storage > Volumes**.
2. Filter the IOPS, latency, and throughput columns to view the frequently accessed volumes and data.

# Search, filter, and sort information in System Manager

You can search for various actions and objects in System Manager. You can also search table data for specific entries.

System Manager provides two types of searching:

- [Global searching](#)

When you enter a search argument in the field at the top of each page, System Manager searches throughout the interface to find matches. You can then sort and filter the results.

- [Table-grid searching](#)

Starting with ONTAP 9.8, when you enter a search argument in the field at the top of a table grid, System Manager searches only the columns and rows of that table to find matches.

## Global searching

At the top of each page in System Manager, you can use a global search field to search various objects and actions in the interface. For example, you can search for different objects by name, pages available in the navigator column (on the left side), various action items, like "Add Volume" or "Add License", and links to external help topics. You can also filter and sort the results.



For better results, perform searching, filtering, and sorting one minute after logging in and five minutes after creating, modifying, or deleting an object.

- [Getting search results](#)
- [Filtering search results](#)
- [Sorting search results](#)

## Getting search results

The search is not case-sensitive. You can enter a variety of text strings to find the page, actions, or topics you need. Up to 20 results are listed. If more results are found, you can click **Show more** to view all results. The following examples describe typical searches:

| Type of search | Sample search string | Sample search results                                                                                                                                      |
|----------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| By object name | vol_                 | vol_lun_dest on storage VM:<br>svm0 (Volume)<br>/vol/vol...est1/lun on storage VM:<br>svm0 (LUN)<br>svm0:vol_lun_dest1 role:<br>Destination (Relationship) |

| Type of search           | Sample search string | Sample search results                                                                          |
|--------------------------|----------------------|------------------------------------------------------------------------------------------------|
| By location in interface | volume               | Add Volume (Action)<br>Protection – Overview (Page)<br>Recover deleted volume (Help)           |
| By actions               | add                  | Add Volume (Action)<br>Network – Overview (Page)<br>Expand volumes and LUNs (Help)             |
| By help content          | san                  | Storage – Overview (Page)<br>SAN overview (Help)<br>Provision SAN storage for databases (Help) |


## Filtering search results

You can narrow the results with filters, as shown in the following examples:

| Filter               | Syntax                             | Sample search string |
|----------------------|------------------------------------|----------------------|
| By object type       | <type>:<objectName>                | volume:vol_2         |
| By object size       | <type><size-symbol><number><units> | luns<500mb           |
| By broken disks      | “broken disk” or “unhealthy disk”  | unhealthy disk       |
| By network interface | <IP address>                       | 172.22.108.21        |

## Sorting search results

When you view all the search results, they are sorted alphabetically. You can sort the results by clicking

 **Filter** and selecting how you want to sort the results.

## Table-grid searching

Starting with ONTAP 9.8, whenever System Manager displays information in a table-grid format, a search button appears at the top of the table.

When you click **Search**, a text field appears in which you can enter a search argument. System Manager searches the entire table and displays only the rows that contain text that matches your search argument.

You can use an asterisk ( \* ) as a "wildcard" character as a substitute for characters. For example, searching for **vol\*** might provide rows that contain the following:



- vol\_122\_D9
- vol\_lun\_dest1
- vol2866
- volspec1
- volum\_dest\_765
- volume
- volume\_new4
- volume9987

## Monitor cluster performance using System Manager

You can monitor cluster performance by viewing information about your system on the ONTAP System Manager Dashboard.

The Dashboard displays information about important alerts and notifications, the efficiency and capacity of storage tiers and volumes, the nodes that are available in a cluster, the status of the nodes in an HA pair, the most active applications and objects, and the performance metrics of a cluster or a node.

The Dashboard lets you determine the following information:

- **Health:** How healthy is the cluster?
- **Capacity:** What capacity is available on the cluster?
- **Performance:** How well is the cluster performing, based on latency, IOPS, and throughput?
- **Network:** How is the network configured with hosts and storage objects, such as ports, interfaces, and storage VMs?

In the Health and Capacity overviews, you can click  to view additional information and perform tasks.

In the Performance overview, you can view metrics based on the hour, the day, the week, the month, or the year.

In the Network overview, the number of each object in the network is displayed (for example, "8 NVMe/FC ports"). You can click on the numbers to view details about each network object.

## Monitor cluster performance with Unified Manager

With Active IQ Unified Manager, you can maximize availability and maintain control of your NetApp AFF and FAS storage infrastructure for improved

scalability, supportability, performance, and security.

Active IQ Unified Manager continuously monitors system health and send alerts, so your organization can free up IT staff resources. You can instantly view storage status from a single dashboard and quickly address issues through recommended actions.

Data management is simplified because you can discover, monitor, and receive notifications to proactively manage storage and quickly resolve issues. Admin efficiency is improved because you can monitor petabytes of data from a single dashboard and manage your data at scale.

With Active IQ Unified Manager, you can keep pace with fluctuating business demands, optimizing performance using performance data and advanced analytics. The reporting capabilities allow you to access standard reports or create custom operational reports to meet the specific needs of your business.

## **Monitor cluster performance with Cloud Insights**

NetApp Cloud Insights is a monitoring tool that gives you visibility into your complete infrastructure. With Cloud Insights, you can monitor, troubleshoot, and optimize all your resources including your public clouds and your private data centers.

### **Cloud Insights comes in two editions**

Cloud Insights Basic Edition is designed specifically to monitor and optimize your NetApp Data Fabric assets. It provides advanced analytics for the connections between all NetApp resources including HCI and All Flash FAS (AFF) within the environment free of charge.

Cloud Insights Standard Edition focuses not only on NetApp Data Fabric-enabled infrastructure components, but also on multi-vendor and multi-cloud environments. With its enriched capabilities, you can access support for over 100 services and resources.

In today's world, with resources in play from your on-premises data centers to multiple public clouds, it's crucial to have the complete picture from the application itself to the backend disk of the storage array. The additional support for application monitoring (like Kafka, MongoDB, and Nginx) gives you the information and knowledge you need to operate at the optimal level of utilization as well as with the perfect risk buffer.

Both editions (Basic and Standard) can integrate with NetApp Active IQ Unified Manager. Customers who use Active IQ Unified Manager will be able to see join information inside the Cloud Insights user interface. Notifications posted on Active IQ Unified Manager will not be overlooked and can now be correlated to events in Cloud Insights. In other words, you get the best of both worlds.

## **Monitor, troubleshoot, and optimize all your resources**

Cloud Insights helps you significantly reduce the time to resolve issues and prevent them from impacting end users. It also helps you reduce cloud infrastructure costs. Your exposure to insider threats is reduced by protecting your data with actionable intelligence.

Cloud Insights gives you visibility to your entire hybrid infrastructure in one place—from the public cloud to your data center. You can instantly create relevant dashboards that can be customized to your specific needs. You can also create targeted and conditional alerts that are specific and relevant to your organization's needs.

Advanced anomaly detection helps you proactively fix issues before they arise. You can view resource contention and degradation automatically to quickly restore impacted workloads. Troubleshooting goes more quickly with the automatically built hierarchy of relationships between the different components in your stack.

You can identify unused or abandoned resources across your environment, which helps you discover opportunities to right-size the infrastructure and optimize your entire spend.

Cloud Insights visualizes your system topology to gain an understanding of your Kubernetes architecture. You can monitor the health of your Kubernetes clusters, including which nodes are in trouble, and zoom in when you see a problem.

Cloud Insights helps you protect organizational data from being misused by malicious or compromised users through advanced machine learning and anomaly detection that gives you actionable intelligence on insider threats.

Cloud Insights helps you to visualize Kubernetes metrics so you can fully understand the relations between your pods, nodes, and clusters. You're able to assess the health of a cluster or a working pod, as well as the load it is currently processing—enabling you to take command of your K8S cluster and to control both the health and the cost of your deployment.

# Day-to-day administration

## Administration overview

ONTAP System Manager is a graphical management interface that enables you to use a web browser to manage storage systems and storage objects (such as disks, volumes, and storage tiers) and perform common management tasks related to storage systems.

Using the System Manager Dashboard, you can view at-a-glance information about important alerts and notifications, the efficiency and capacity of storage tiers and volumes, the nodes that are available in a cluster, the status of the nodes in an HA pair, the most active applications and objects, and the performance metrics of a cluster or a node.

With System Manager you can perform many common tasks, such as the following:

- Create a cluster, configure a network, and set up support details for the cluster.
- Configure and manage storage objects, such as disks, local tiers, volumes, qtrees, and quotas.
- Configure protocols, such as SMB/CIFS and NFS, and provision file sharing.
- Configure protocols such as FC, FCoE, NVMe, and iSCSI for block access.
- Create and configure network components, such as subnets, broadcast domains, data and management interfaces, and interface groups.
- Set up and manage mirroring and vaulting relationships.
- Perform cluster management, storage node management, and storage virtual machine (storage VM) management operations.
- Create and configure storage VMs, manage storage objects associated with storage VMs, and manage storage VM services.
- Monitor and manage high-availability (HA) configurations in a cluster.
- Configure service processors to remotely log in, manage, monitor, and administer the node, regardless of the state of the node.

## Viewing and managing your network

Starting with System Manager 9.8, you can display a graphic that shows the components and configuration of your network.

The graphic displays when you select **Network > Overview** or when you select  from the **Network** section of the Dashboard.


The following categories of components are shown in the graphic:

- Hosts
- Storage ports
- Network interfaces
- Storage VMs
- Data access components

Each section shows additional details that you can hover your mouse over or select to perform network management and configuration tasks.

## Examples

The following are some examples of the many ways you can interact with the graphic to view details about each component or initiate actions to manage your network:

- Click on a host to see its configuration: the ports, network interfaces, storage VMs, and data access components associated with it.
- Hover the mouse over the number of volumes in a storage VM to select a volume to view its details.
- Select an iSCSI interface to view its performance over the last week.
- Click on  next to a component to initiate actions to modify that component.
- Quickly determine where problems might occur in your network, indicated by an "X" next to unhealthy components.

## Downloading network data for reporting

Starting with System Manager 9.8, you can download the data that is displayed in System Manager about your network.

When you display information in a *List View*, you can click **Download**, and the list of objects displayed is downloaded.

- The list is downloaded in comma-separated values (CSV) format.
- Only the data in the visible columns is downloaded.
- The CSV filename is formatted with the object name and a time stamp.

## Search, filter, and sort information in System Manager

You can search for various actions and objects in System Manager. You can also search table data for specific entries.

System Manager provides two types of searching:

- [Global searching](#)

When you enter a search argument in the field at the top of each page, System Manager searches throughout the interface to find matches. You can then sort and filter the results.

- [Table-grid searching](#)

Starting with ONTAP 9.8, when you enter a search argument in the field at the top of a table grid, System Manager searches only the columns and rows of that table to find matches.

## Global searching

At the top of each page in System Manager, you can use a global search field to search various objects and actions in the interface. For example, you can search for different objects by name, pages available in the navigator column (on the left side), various action items, like "Add Volume" or "Add License", and links to external help topics. You can also filter and sort the results.



For better results, perform searching, filtering, and sorting one minute after logging in and five minutes after creating, modifying, or deleting an object.

- [Getting search results](#)
- [Filtering search results](#)
- [Sorting search results](#)

### Getting search results

The search is not case-sensitive. You can enter a variety of text strings to find the page, actions, or topics you need. Up to 20 results are listed. If more results are found, you can click **Show more** to view all results. The following examples describe typical searches:

| Type of search           | Sample search string | Sample search results                                                                                                                                      |
|--------------------------|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| By object name           | vol_                 | vol_lun_dest on storage VM:<br>svm0 (Volume)<br>/vol/vol...est1/lun on storage VM:<br>svm0 (LUN)<br>svm0:vol_lun_dest1 role:<br>Destination (Relationship) |
| By location in interface | volume               | Add Volume (Action)<br>Protection – Overview (Page)<br>Recover deleted volume (Help)                                                                       |

| Type of search  | Sample search string | Sample search results                                                                          |
|-----------------|----------------------|------------------------------------------------------------------------------------------------|
| By actions      | add                  | Add Volume (Action)<br>Network – Overview (Page)<br>Expand volumes and LUNs (Help)             |
| By help content | san                  | Storage – Overview (Page)<br>SAN overview (Help)<br>Provision SAN storage for databases (Help) |


## Filtering search results

You can narrow the results with filters, as shown in the following examples:

| Filter               | Syntax                             | Sample search string |
|----------------------|------------------------------------|----------------------|
| By object type       | <type>:<objectName>                | volume:vol_2         |
| By object size       | <type><size-symbol><number><units> | luns<500mb           |
| By broken disks      | “broken disk” or “unhealthy disk”  | unhealthy disk       |
| By network interface | <IP address>                       | 172.22.108.21        |

## Sorting search results

When you view all the search results, they are sorted alphabetically. You can sort the results by clicking

 **Filter** and selecting how you want to sort the results.

## Table-grid searching

Starting with ONTAP 9.8, whenever System Manager displays information in a table-grid format, a search button appears at the top of the table.

When you click **Search**, a text field appears in which you can enter a search argument. System Manager searches the entire table and displays only the rows that contain text that matches your search argument.

You can use an asterisk ( \* ) as a "wildcard" character as a substitute for characters. For example, searching for **vol1\*** might provide rows that contain the following:


- vol\_122\_D9
- vol\_lun\_dest1
- vol2866

- volspec1
- volum\_dest\_765
- volume
- volume\_new4
- volume9987

## Enable new features by adding license keys

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


### *Steps*

1. Click **Cluster** > **Settings**.
2. Under **License**, click .
3. Click **Add**.

## Reboot, shut down, take over, and give back nodes

You should switch a node's workload to its HA partner (takeover) before rebooting or shutting down the node.

### *Steps*

1. Click **Cluster** > **Overview**.
2. Under **Nodes**, click .
3. Click the node and select the desired action.

## Troubleshoot hardware problems

Starting with ONTAP 9.8, you can use System Manager to view the configuration of hardware on your network and troubleshoot problems that might arise.

### *Before you Start*

For ONTAP 9.8, System Manager provides a *preview* of the capability to view hardware configurations. The preview only shows a limited number of AFF models.

### *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 nodes](#)
- [Information about disk shelves](#)
- [Information about storage switches](#)

## Information about nodes

You can view the following:

### Nodes:

- Front and rear views are displayed.
- Models with an internal disk shelf also show the disk layout in the front view.
- For ONTAP 9.8, only platform models C190, A220, A300, A400, and A700 are shown.

### Ports:

- Console ports are not shown in this preview.
- 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 part numbers supported, then a generic graphic is displayed.

### FlashCache:

- Details about FlashCache are shown like an adapter card if slot information is available.

## Information about disk shelves

You can view the following:

### Disk shelves:

- Front and rear views are displayed.

### 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.
- For ONTAP 9.8, the following model can be viewed: X190100 (Cisco Nexus 3232).

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.

## Manage MetroCluster sites

Starting with ONTAP 9.8, you can use System Manager as a simplified interface for managing a configuration of a MetroCluster setup.

A MetroCluster configuration allows two clusters to mirror data to each other so if one cluster goes down, the data isn't lost.

Typically, an organization sets up the clusters in two separate geographical locations. An administrator at each location sets up a cluster and configures it. Then one of the administrators can set up the peering between the clusters so that they can share data.

The organization can also install an ONTAP Mediator in a third location. The ONTAP Mediator service monitors the status of each cluster. When one of the clusters detects that it cannot communicate with the partner cluster, it queries the monitor to determine if the error is a problem with the cluster system or with the network connection.

If the problem is with the network connection, the system administrator performs troubleshooting methods to correct the error and reconnect. If the partner cluster is down, the other cluster initiates a switchover process to control the data I/O for both clusters.

You can also perform a switchover to bring down one of the cluster systems for planned maintenance. The partner cluster handles all data I/O operations for both clusters until you bring up the cluster on which you performed maintenance and perform a switchback operation.

You can manage the following operations:

- [Set up an IP MetroCluster site](#)
- [Set up IP MetroCluster peering](#)
- [Configure an IP MetroCluster site](#)
- [Perform IP MetroCluster switchover and switchback](#)
- [Troubleshoot problems with IP MetroCluster configurations](#)
- [Upgrade ONTAP on MetroCluster clusters](#)

## Set up an IP MetroCluster site

Starting with ONTAP 9.8, you can use System Manager to set up an IP configuration of a MetroCluster site.

A MetroCluster site consists of two clusters. Typically, the clusters are located in different geographical locations.

### *Before you start*

- Your system should already be installed and cabled according to the [Installation and Setup Instructions](#) that came with the system.
- Cluster network interfaces should be configured on each node of each cluster for intra-cluster communication.



## Assign a node-management IP address

### Windows System

You should connect your Windows computer to the same subnet as the controllers. This will automatically assign a node-management IP address to your system.

#### *Steps*

1. From the Windows system, open the **Network** drive to discover the nodes.
2. Double-click the node to launch the cluster setup wizard.

### Other systems

You should configure the node-management IP address for one of the nodes in your cluster. You can use this node-management IP address to launch the cluster set up wizard.

See [Creating the cluster on the first node](#) for information about assigning a node-management IP address.

## Initialize and configure the cluster

You initialize the cluster by setting an administrative password for the cluster and setting up the cluster management and node management networks. You can also configure services like a DNS server to resolve host names and an NTP server to synchronize time.

#### *Steps*

1. On a web browser, enter the node-management IP address that you have configured: "https://node-management-IP"

System Manager automatically discovers the remaining nodes in the cluster.

2. In the **Initialize Storage System** window, perform the following:
  - a. Enter cluster management network configuration data.
  - b. Enter Node management IP addresses for all the nodes.
  - c. Provide domain name servers (DNS) details.
  - d. In the **Other** section, select the check box labeled **Use time service (NTP)** to add the time servers.

When you click **Submit**, wait for the cluster to be created and configured. Then, a validation process occurs.

#### *What's Next?*

After both clusters have been set up, initialized, and configured, perform the following procedure:

- [Set up IP MetroCluster peering](#)

## **Set up IP MetroCluster peering**

Starting with ONTAP 9.8, you can manage an IP configuration of a MetroCluster operation with System Manager. After setting up two clusters, you set up peering between them.

#### *Before you start*

You should have completed the following procedure to set up two clusters:

- [Set up an IP MetroCluster site](#)

Certain steps of this process are performed by different system administrators located at the geographical sites of each cluster. For the purposes of explaining this process, the clusters are called "Site A cluster" and "Site B cluster".

### **Performing the peering process from Site A**

This process is performed by a system administrator at Site A.

#### *Steps*

1. Log in to Site A cluster.
2. In System Manager, select **Dashboard** from the left navigation column to display the cluster overview.

The dashboard shows the details for this cluster (Site A). In the **MetroCluster** section, Site A cluster is shown on the left.

3. Click **Attach Partner Cluster**.
4. Enter the details of the network interfaces that allow the nodes in Site A cluster to communicate with the nodes in Site B cluster.
5. Click **Save and Continue**.
6. On the **Attach Partner Cluster** window, select **I do not have a passphrase**, which lets you generate a passphrase.
7. Copy the generated passphrase and share it with the system administrator at Site B.
8. Select **Close**.

### Performing the peering process from Site B

This process is performed by a system administrator at Site B.

#### *Steps*

1. Log in to Site B cluster.
2. In System Manager, select **Dashboard** to display the cluster overview.

The dashboard shows the details for this cluster (Site B). In the MetroCluster section, Site B cluster is shown on the left.

3. Click **Attach Partner Cluster** to start the peering process.
4. Enter the details of the network interfaces that allow the nodes in Site B cluster to communicate with the nodes in Site A cluster.
5. Click **Save and Continue**.
6. On the **Attach Partner Cluster** window, select **I have a passphrase**, which lets you enter the passphrase that you received from the system administrator at Site A.
7. Select **Peer** to complete the peering process.

#### *What's next?*

After the peering process is successfully completed, you configure the clusters. See [Configure an IP MetroCluster site](#).

### Configure an IP MetroCluster site

Starting with ONTAP 9.8, you can manage an IP configuration of a MetroCluster operation with System Manager. After setting up two clusters and peering them, you configure each cluster.

### *Before you start*

You should have completed the following procedures:

- [Set up an IP MetroCluster site](#)
- [Set up IP MetroCluster peering](#)

## **Configure the connection between clusters**

### *Steps*

1. Log in to System Manager on one of the sites, and select **Dashboard**.

In the **MetroCluster** section, the graphic shows the two clusters that you set up and peered for the MetroCluster sites. The cluster you are working from (local cluster) is shown on the left.

2. Click **Configure MetroCluster**. From this window, you can perform the following tasks:
  - a. The nodes for each cluster in the MetroCluster configuration are shown. Use the drop-down lists to select which nodes in the local cluster will be disaster recovery partners with which nodes in the remote cluster.
  - b. Click the check box if you want to configure an ONTAP Mediator service. See [Configure the ONTAP Mediator service](#).
  - c. If both clusters have a license to enable encryption, the **Encryption** section is displayed.

To enable encryption, enter a passphrase.

1. Click **Save** to configure the MetroCluster sites.

On the **Dashboard**, in the **MetroCluster** section, the graphic shows a check mark on the link between the two clusters, indicating a healthy connection.


## **Configure the ONTAP Mediator service**

The ONTAP Mediator service is typically installed at a geographic location separate from either location of the clusters. The clusters communicate regularly with the service to indicate that they are up and running. If one of the clusters in the MetroCluster configuration detects that the communication with its partner cluster is down, it checks with the ONTAP Mediator to determine if the partner cluster itself is down.

### *Before you start*

Both clusters at the MetroCluster sites should be up and peered.

### *Steps*

1. In System Manager 9.8, select **Cluster > Settings**.
2. In the **Mediator** section, click .
3. On the **Configure Mediator** window, click **Add+**.

4. Enter the configuration details for the ONTAP Mediator.

## Perform IP MetroCluster switchover and switchback

You can switch over control from one IP MetroCluster site to the other to perform maintenance or recover from an issue.



Switchover and switchback procedures are supported only for IP MetroCluster configurations.

### Overview of switchover and switchback

A switchover can occur in two instances:

- **A planned switchover**

This switchover is initiated by a system administrator using System Manager. The planned switchover allows a system administrator of a local cluster to switch control so that the data services of the remote cluster are handled by the local cluster. Then, a system administrator at the remote cluster location can perform maintenance on the remote cluster.

- **An unplanned switchover**

In some cases, when a MetroCluster cluster goes down or the connections between the clusters are down, ONTAP will automatically initiate a switchover procedure so that the cluster that is still running handles the data handling responsibilities of the down cluster.

At other times, when ONTAP cannot determine the status of one of the clusters, the system administrator of the site that is working initiates the switchover procedure to take control of the data handling responsibilities of the other site.

For any type of switchover procedure, the data servicing capability is returned to the cluster by using a *switchback* process.

You perform different switchover and switchback processes for ONTAP 9.7 and 9.8:

- [Use System Manager 9.7 for switchover and switchback](#)
- [Use System Manager 9.8 for switchover and switchback](#)

### Use System Manager 9.7 for switchover and switchback

#### *Steps*

1. Log in to System Manager 9.7.
2. Click **(Return to classic version)**.
3. Click **Configuration > MetroCluster**.




System Manager verifies whether a negotiated switchover is possible.

4. Perform one of the following substeps when the validation process has completed:
  - a. If validation fails, but Site B is up, then an error has occurred. For example, there might be a problem with a subsystem, or NVRAM mirroring might not be synchronized.
    - i. Fix the issue that is causing the error, click **Close**, and then start again at Step 2.
    - ii. Halt the Site B nodes, click **Close**, and then perform the steps in [Performing an unplanned switchover](#).
  - b. If validation fails, and Site B is down, then most likely there is a connection problem. Verify that Site B is really down, then perform the steps in [Performing an unplanned switchover](#).
5. Click **Switchover from Site B to Site A** to initiate the switchover process.
6. Click **Switch to the new experience**.

## Use System Manager 9.8 for switchover and switchback

### Perform a planned switchover (ONTAP 9.8)

#### Steps

1. Log in to System Manager 9.8.
2. Select **Dashboard**. In the **MetroCluster** section, the two clusters are shown with a connection.
3. In the local cluster (shown on the left), click , and select **Take control of remote site**.

After the switchover request is validated, control is transferred from the remote site to the local site, which performs data service requests for both clusters.

The remote cluster reboots, but the storage components are not active, and the cluster does not service data requests. It is now available for planned maintenance.



The remote cluster should not be used for data servicing until you perform a switchback.

### Perform an unplanned switchover (ONTAP 9.8)

An unplanned switchover might be initiated automatically by ONTAP. If ONTAP cannot determine if a switchback is needed, the system administrator of the MetroCluster site that is still running initiates the switchover with the following steps:

#### Steps

1. Log in to System Manager 9.8.
2. Select **Dashboard**.

In the **MetroCluster** section, the connection between the two clusters is shown with an "X" on it,

meaning a connection cannot be detected. Either the connections or the cluster is down.

3. In the local cluster (shown on the left), click , and select **Take control of remote site**.

After the switchover request is validated, control is transferred from the remote site to the local site, which performs data service requests for both clusters.

The cluster must be repaired before it is brought online again.



After the remote cluster is brought online again, it should not be used for data servicing until you perform a switchback.

## Perform a switchback (ONTAP 9.8)


### *Before you start*

Whether the remote cluster was down due to planned maintenance or due to a disaster, it should now be up and running and waiting for the switchback.

### *Steps*

1. On the local cluster, log in to System Manager 9.8.
2. Select **Dashboard**.

In the **MetroCluster** section, the two clusters are shown.

3. In the local cluster (shown on the left), click , and select **Take back control**.

The data is *healed* first, to ensure data is synchronized and mirrored between both clusters.

4. When the data healing is complete, click , and select **Initiate switchback**.

When the switchback is complete, both clusters are active and servicing data requests. Also, the data is being mirrored and synchronized between the clusters.

## Troubleshoot problems with IP MetroCluster configurations

Starting with ONTAP 9.8, System Manager monitors the health of IP MetroCluster configurations and helps you identify and correct problems that might occur.

### Overview of the MetroCluster Health Check

System Manager periodically checks the health of your IP MetroCluster configuration. When you view the MetroCluster section in the Dashboard, usually the message is "MetroCluster systems are healthy."

However, when a problem occurs, the message will show the number of events. You can click on that message and view the results of the health check for the following components:

- Node
- Network Interface
- Tier (Storage)
- Cluster
- Connection
- Volume
- Configuration Replication

The **Status** column identifies which components have problems, and the **Details** column suggests how to correct the problem.

## MetroCluster troubleshooting

### Steps

1. In System Manager, select **Dashboard**.
2. In the **MetroCluster** section, notice the message.
  - a. If the message indicates that your MetroCluster configuration is healthy, and the connections between the clusters and the ONTAP Mediator are healthy (shown with check marks), then you have no problems to correct.
  - b. If the message lists the number of events, or the connections have gone down (shown with an "X"), then continue to the next step.
3. Click the message that shows the number of events.

The MetroCluster Health Report displays.

4. Troubleshoot the problems that appear in the report using the suggestions in the **Details** column.
5. When all the problems have been corrected, click **Check MetroCluster Health**.



The MetroCluster Health Check uses an intensive amount of resources, so it is recommended that you perform all your troubleshooting tasks before running the check.

The MetroCluster Health Check runs in the background. You can work on other tasks while you wait for it to finish.

## Update ONTAP on MetroCluster clusters

You can use System Manager to upgrade both clusters in a MetroCluster configuration to a newer version of ONTAP. During the upgrade, the storage service remains online.

### *Before you start*

- Upload the ONTAP image using a local drive or from an HTTP server on both clusters of the MetroCluster configuration.

### *Steps*

1. Log in to System Manager.
2. Select **Cluster > Update**.

The **ONTAP Update** window displays a list of images that are available to upload.

3. Hover over any image name that you do *NOT* want to upload, and click the trash can icon.
4. Select the radio button next to the image name that you want to update, and click **Update**.
5. Wait for the system to validate the images.

When the images are successfully validated, the update process begins to install a new version of ONTAP on both clusters.

You can click **Pause** at any time to pause the updating process.

6. When the update process is completed, click **Relaunch System Manager**.

## Clone volumes and LUNs for testing

You can clone volumes and LUNs to create temporary, writable copies for testing. The clones reflect the current, point-in-time state of the data. You can also use clones to give additional users access to data without giving them access to production data.




The FlexClone license should be installed on the storage system.

### Cloning a volume

Create a clone of a volume, as follows:

#### *Steps*


1. Click **Storage > Volumes**.
2. Click  next to the name of the volume you want to clone.
3. Select **Clone** from the list.
4. Specify a name for the clone and complete the other selections.
5. Click **Clone** and verify that the volume clone appears in the list of volumes.

Alternatively, you can clone a volume from the **Overview** that displays when you view volume details.

## Cloning a LUN

Create a clone of a LUN, as follows:

### *Steps*

1. Click **Storage** > **LUNs**.
2. Click  next to the name of the LUN you want to clone.
3. Select **Clone** from the list.
4. Specify a name for the clone and complete the other selections.
5. Click **Clone** and verify that the LUN clone appears in the list of LUNs.


Alternatively, you can clone a LUN from the **Overview** that displays when you view LUN details.

When you create a LUN clone, System Manager automatically enables the deletion of the clone when space is needed.

## Modify QoS

Beginning in ONTAP 9.8, when you provision storage, QoS is enabled by default. You can disable QoS or choose a custom QoS policy during the provisioning process. You can also modify QoS after your storage has been provisioned.

### *Steps*

1. In ONTAP System Manager, click **Storage** and select **Volumes**.
2. Next to the volume for which you want to modify QoS, click  and select **Edit**.

## Update ONTAP

### Update ONTAP

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

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


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



### Steps

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

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

2. In ONTAP System Manager, click **Cluster > Overview**.
3. In the right corner of the Overview pane, click .
4. Click **ONTAP Update**.

## Update ONTAP on MetroCluster clusters

You can use System Manager to upgrade both clusters in a MetroCluster configuration to a newer version of ONTAP. During the upgrade, the storage service remains online.

### Before you start

- Upload the ONTAP image using a local drive or from an HTTP server on both clusters of the MetroCluster configuration.

### Steps

1. Log in to System Manager.
2. Select **Cluster > Update**.

The **ONTAP Update** window displays a list of images that are available to upload.

3. Hover over any image name that you do *NOT* want to upload, and click the trash can icon.
4. Select the radio button next to the image name that you want to update, and click **Update**.
5. Wait for the system to validate the images.

When the images are successfully validated, the update process begins to install a new version of ONTAP on both clusters.

You can click **Pause** at any time to pause the updating process.

6. When the update process is completed, click **Relaunch System Manager**.

## Update firmware

You can apply a firmware updated to supported devices in your cluster, such as disks, disk shelves, the Disk Qualification Package (DQP) the service processor (SP),


or the Baseboard Management Controller (BMC).



#### Steps

1. Copy the needed firmware update files from the NetApp support site.

You can copy the files to an HTTP or FTP server on your network or to a local folder.

2. In ONTAP System Manager, click **Cluster** > **Overview**.
3. In the right corner of the Overview pane, click  and select **ONTAP Update**.
4. Click **Firmware Update**, select **From Server** or **Local Client** and provide the server URL or the file location.

You can monitor or verify the update under **Firmware Update Summary**.

## Manage storage

### Expand storage

You can increase the size of your volume or LUN so that more space is available to your host. The size of a LUN cannot exceed the size of the containing volume.

- [Increase the size of a volume](#)
- [Increase the size of a LUN](#)


Also, you can add a LUN to an existing volume. The processes are different for using System Manager with ONTAP 9.7 or 9.8

- [Add a LUN to an existing volume \(ONTAP 9.7\)](#)
- [Add a LUN to an existing volume \(ONTAP 9.8\)](#)

Also, starting with ONTAP 9.8, you can use System Manager to add a LUN to an existing volume.

### Increase the size of a volume


#### Steps

1. Click **Storage** > **Volumes**.
2. Hover over the name of the volume you want to increase in size.
3. Click .

4. Select **Edit**.
5. Increase the capacity value.

### **Increase the size of a LUN**

#### *Steps*

1. Click **Storage > LUNs**.
2. Hover over the name of the LUN you want to increase in size.
3. Click .
4. Select **Edit**.
5. Increase the capacity value.

### **Add a LUN to an existing volume (ONTAP 9.7)**

To use System Manager with ONTAP 9.7 to add a LUN to an existing volume, you should switch to the Classical View first.

#### *Steps*

1. Log in to System Manager in ONTAP 9.7.
2. Click **Classical View**.
3. Select **Storage > LUNs > Create**
4. Specify the details to create the LUN.
5. Specify to which existing volume or qtree the LUN should be added.

### **Add a LUN to an existing volume (ONTAP 9.8)**

Starting with ONTAP 9.8, you can use System Manager to add a LUN to an existing volume that already has a least one LUN.

#### *Steps*

1. Click **Storage > LUNs**.
2. Click **Add+**.
3. Complete the fields in the **Add LUNs** window.
4. Select **More Options**.
5. Select the checkbox labeled **Group with related LUNs**.
6. In the drop-down field, select a LUN that exists on the volume to which you want to add another LUN.
7. Complete the rest of the fields. For **Host Mapping**, click one of the radio buttons:
  - **Existing initiator group** lets you select an existing group from a list.



- **New initiator group** lets you enter a new group in the field.

### **Add disks to a local tier (Add capacity to aggregate)**

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

#### *Steps*

1. Click **(Return to classic version)**.
2. Click **Hardware and Diagnostics > Aggregates**.
3. Select the aggregate to which you want to add capacity disks, and then click **Actions > Add Capacity**.

You should add disks that are of the same size as the other disks in the aggregate.

4. Click **Switch to the new experience**.
5. Click **Storage > Tiers** to verify the size of the new aggregate.

### **Add cache to a local tier**

Provision cache by converting an existing local tier (aggregate) to a Flash Pool aggregate by adding SSDs. Flash Pool aggregates enable you to deploy flash as high performance cache for your working data set while using lower-cost HDDs for less frequently accessed data.

#### *Steps*

1. Click **(Return to classic version)**.
2. Click **Hardware and Diagnostics > Aggregates**.
3. Select the aggregate, and then click **Actions > Add Cache**.

Select the cache source as storage pools or dedicated SSDs.

4. Click **Switch to the new experience**.
5. Click **Storage > Tiers** to verify the size of the new aggregate.

### **Add nodes to cluster**

You can increase the size and capabilities of your cluster by adding new nodes.

#### *Before you Start*

You should have already cabled the new nodes to the cluster.

There are separate processes for working with System Manager in ONTAP 9.7 or ONTAP 9.8.

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

#### Adding nodes to a cluster with System Manager 9.7

##### Steps

1. Click **(Return to classic version)**.
2. Click **Configurations > Cluster Expansion**.

System Manager automatically discovers the new nodes.

3. Click **Switch to the new experience**.
4. Click **Cluster > Overview** to view the new nodes.

#### Adding nodes to a cluster with System Manager 9.8

##### Steps

1. Select **Cluster > Overview**.

The new controllers are shown as nodes connected to the cluster network but are not in the cluster.

2. Click **Add**.
  - The nodes are added into the cluster.
  - Storage is allocated implicitly.


## Manage storage efficiency policies

Starting with ONTAP 9.8, you can use System Manager to enable, disable, add, edit, or delete efficiency policies for storage VMs on FAS systems.





This function is not available on AFF systems.

##### Steps

1. Select **Storage > Storage VMs**
2. Select the storage VM for which you want to manage efficiency policies.
3. On the **Settings** tab, select  in the **Efficiency Policy** section. The efficiency policies for that storage VM are displayed.

You can perform the following tasks:

- **Enable or disable** an efficiency policy by clicking the toggle button in the Status column.
- **Add** an efficiency policy by clicking on **Add+**.

- **Edit** an efficiency policy by clicking on  to the right of the policy name and selecting **Edit**.
- **Delete** an efficiency policy by clicking on  to the right of the policy name and selecting **Delete**.

## Recover deleted volumes

If you have accidentally deleted one or more FlexVol volumes, you can recover these volumes. Starting in System Manager 9.8, you can also recover FlexGroup volumes. You can also delete the volumes permanently by purging the volumes.

The volume retention time can be set on a storage VM level. By default, the volume retention time is set to 12 hours.

### Selecting deleted volumes

#### *Steps*

1. Click **Storage > Volumes**.
2. Click **More > Show Deleted Volumes**.
3. Select the volumes and click the desired action to recover or permanently delete the volumes.

### Resetting the volume configurations

Deleting a volume deletes the associated configurations of the volume. Recovering a volume does not reset all the configurations. Perform the following tasks manually after recovering a volume to bring the volume back to its original state:

#### *Steps*

1. Rename the volume.
2. Set up a junction path (NAS).
3. Create mappings for LUNs in the volume (SAN).
4. Associate a Snapshot policy and export policy with the volume.
5. Add new quota policy rules for the volume.
6. Add a QOS policy for the volume.

## Save storage space using compression, compaction, and deduplication

For volumes on non-AFF clusters, you can run deduplication, data compression, and data compaction together or independently to achieve optimal space savings.

- Deduplication eliminates duplicate data blocks.
- Data compression compresses the data blocks to reduce the amount of physical storage that is required.

- Data compaction stores more data in less space to increase storage efficiency.



These tasks are supported for volumes on non-AFF clusters. Beginning with ONTAP 9.2, all inline storage efficiency features, such as inline deduplication and inline compression, are enabled by default on AFF volumes.

### Steps

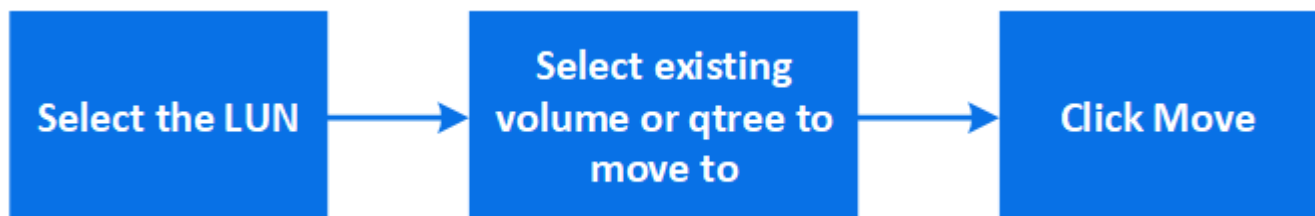
1. Click **Storage > Volumes**.
2. Next to the name of the volume for which you want to save storage, click **⋮**.
3. Click **Edit** and scroll to **Storage Efficiency**.
4. *Optional:* If you want to enable background deduplication, ensure the checkbox is checked.
5. *Optional:* If you want to enable background compression, specify the storage efficiency policy and ensure the checkbox is checked.
6. *Optional:* If you want to enable inline compression, ensure the checkbox is checked.

## Balance loads by moving LUNs

You can move a LUN to another volume within the storage VM to balance the load, or you can move it to a volume with a higher performance service level to improve performance.

### Move restrictions

- A LUN cannot be moved to a qtree within the same volume.
- A LUN created from a file using the CLI cannot be moved with System Manager.
- LUNs that are online and serving data cannot be moved.
- LUNs cannot be moved if the allocated space in the destination volume cannot contain the LUN (even if autogrow is enabled on the volume).
- LUNs on SnapLock volumes cannot be moved with System Manager.



### Steps

1. Click **Storage > LUNs**.
2. Select the LUN that you want to move and click **Move**.
3. Select an existing volume to which you want to move the LUN. If the volume contains qtrees, select

the qtree.



While the Move operation is in progress, the LUN is displayed on both the origin and destination volume.

## Balance loads by moving volumes to another tier

Starting with ONTAP 9.8, you can use System Manager to move a volume to another tier to balance the load.

### *Steps*

1. Click **Storage > Volumes**.
2. Select the volume or volumes that you want to move, and then click **Move**.
3. Select an existing tier (aggregate) to which you want to move the volume or volumes.

# Rest API

## REST API log overview

The REST API log captures the API calls that System Manager issues to ONTAP. You can use the log to understand the nature and sequence of the calls needed to perform the various ONTAP administrative tasks.

### How System Manager uses the REST API and API log

There are several ways that REST API calls are issued by System Manager to ONTAP.

#### When does System Manager issue API calls

Here are the most important examples of when System Manager issues ONTAP REST API calls.

#### Automatic page refresh

System Manager automatically issues API calls in the background to refresh the displayed information, such as on the dashboard page.

#### Display action by user

One or more API calls are issued when you display a specific storage resource or a collection of resources from the System Manager UI.

#### Update action by user

An API call is issued when you add, modify, or delete an ONTAP resource from the System Manager UI.

#### Reissuing an API call

You can also manually reissue an API call by clicking a log entry. This displays the raw JSON output from the call.

### Where to find more information

- [ONTAP 9 REST API Developers Guide](#)
- [NetApp DevNet: ONTAP RESTful API](#)

## Accessing the REST API log

You can access the log containing a record of the ONTAP REST API calls made by System Manager. When displaying the log, you can also reissue API calls and review the output.

## Steps

1. At the top of the page, click  to display the REST API log.

The most recent entries are displayed at the bottom of the page.

2. On the left, click **DASHBOARD** and observe the new entries being created for the API calls issued to refresh the page.
3. Click **STORAGE** and then click **Qtrees**.

This causes System Manager to issue a specific API call to retrieve a list of the Qtrees.

4. Locate the log entry describing the API call which has the form:

`GET /api/storage/qtrees`

You will see additional HTTP query parameters included with the entry, such as `max_records`.

5. Click the log entry to reissue the GET API call and display the raw JSON output.

## Example

```
1 {
2   "records": [
3     {
4       "svm": {
5         "uuid": "19507946-e801-11e9-b984-00a0986ab770",
6         "name": "SMQA",
7         "_links": {
8           "self": {
9             "href": "/api/svm/svms/19507946-e801-11e9-b984-00a0986ab770"
10          }
11        }
12      },
13      "volume": {
14        "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
15        "name": "vol_vol_test2_dest_dest",
16        "_links": {
17          "self": {
18            "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-00a0986abd71"
19          }
20        }
21      },
22      "id": 1,
23      "name": "test2",
24      "security_style": "mixed",
25      "unix_permissions": 777,
26      "export_policy": {
```

```
27     "name": "default",
28     "id": 12884901889,
29     "_links": {
30         "self": {
31             "href": "/api/protocols/nfs/export-policies/12884901889"
32         }
33     },
34     "path": "/vol_vol_test2_dest_dest/test2",
35     "_links": {
36         "self": {
37             "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-00a0986abd71/1"
38         }
39     }
40 },
41 ],
42 "num_records": 1,
43 "_links": {
44     "self": {
45         "href": "/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"
46     }
47 }
48 }
49 }
```



# Getting more information

You can get help and find more information through various resources, including videos, documentation, and forums.

- [NetApp TechCommTV](#) – more NetApp videos
- [ONTAP 9 Doc Center](#) – including Release Notes and documentation for previous versions of System Manager
- [ONTAP and ONTAP System Manager Documentation Resources](#) – including links to Technical Reports and Knowledgebase Articles
- [NetApp Community](#) – forums

# Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

## Copyright

<http://www.netapp.com/us/legal/copyright.aspx>

## Trademarks

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

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/us/media/patents-page.pdf>

## Privacy policy

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## Copyright Information

Copyright © 2020 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.