ONTAP System Manager docs

ONTAP System Manager

NetApp
April 21, 2020

Table of Contents

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 9.7 is the latest version of 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.

The most noticeable feature of ONTAP 9.7 is 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 9.7 System Manager that you should watch out for.

- **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.

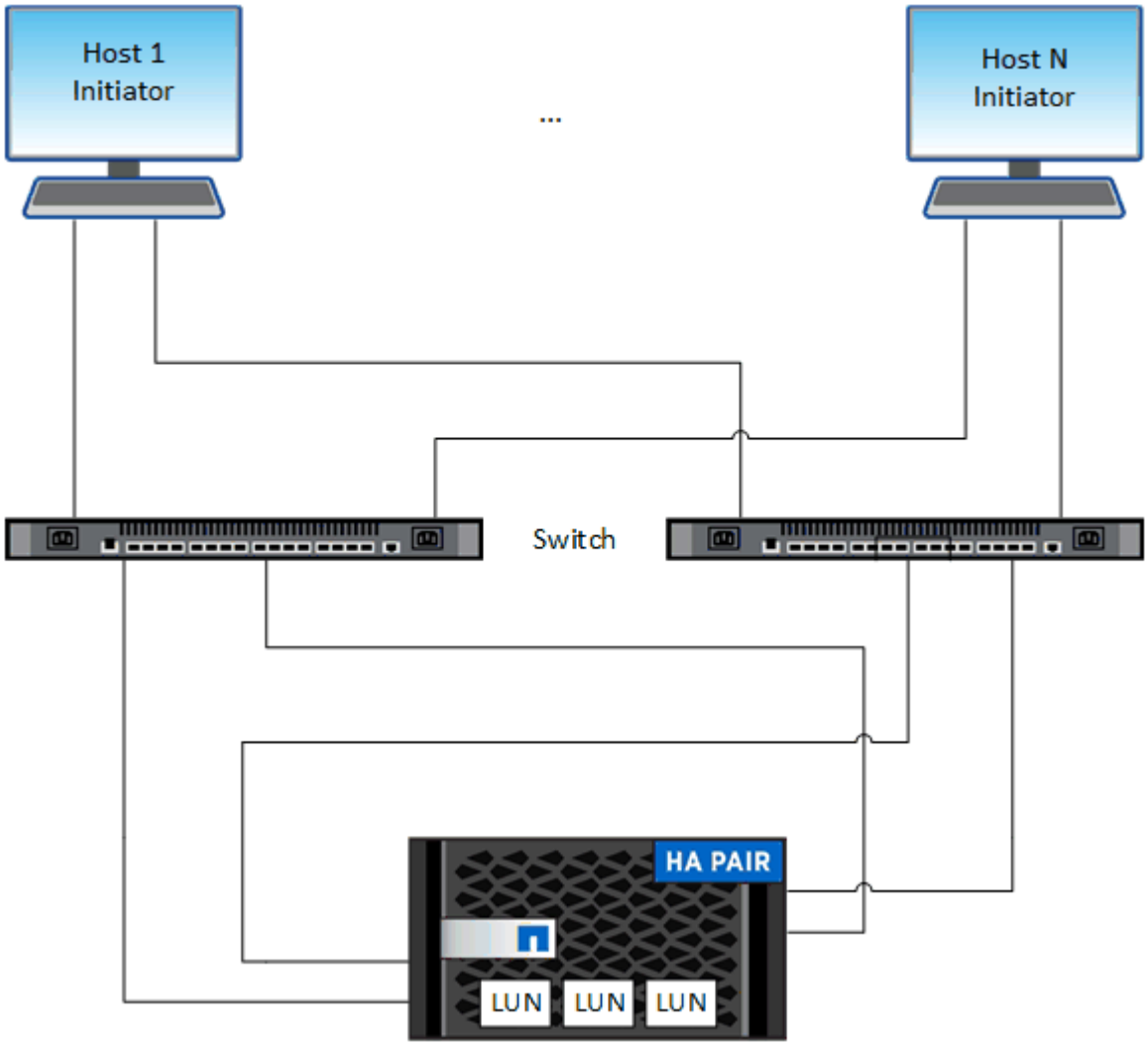
Steps

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 WWPs and iSCSI host node names and control which initiators have access to which LUNs.

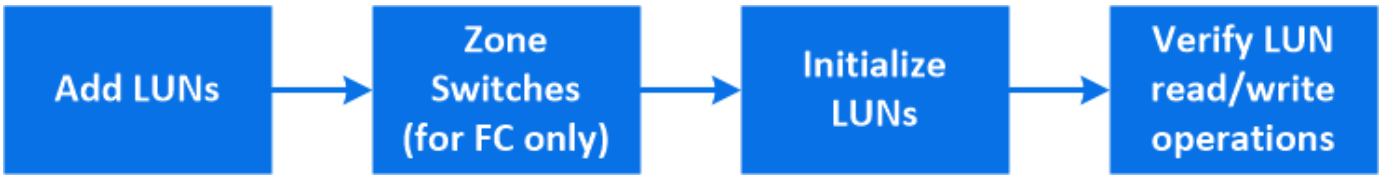
FC targets connect to the network through FC switches and host-side adapters and are identified by world-wide port names (WWPNs). iSCSI targets connect to the network through standard Ethernet network adapters (NICs), TCP offload engine (TOE) cards with software initiators, converged network adapters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



Steps

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

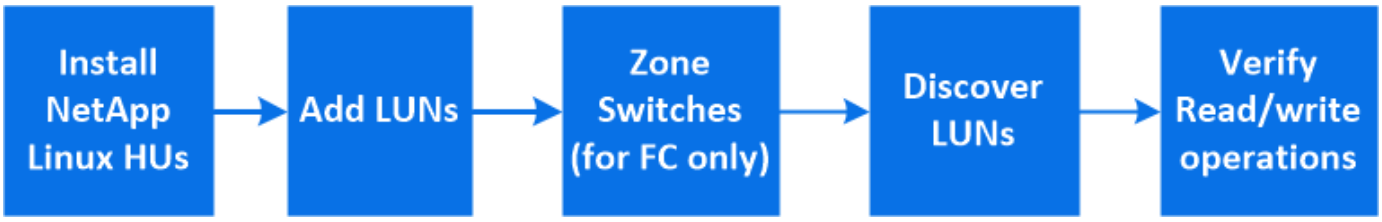
   If you need to create a new initiator group, click **More Options**.

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.



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**.

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:

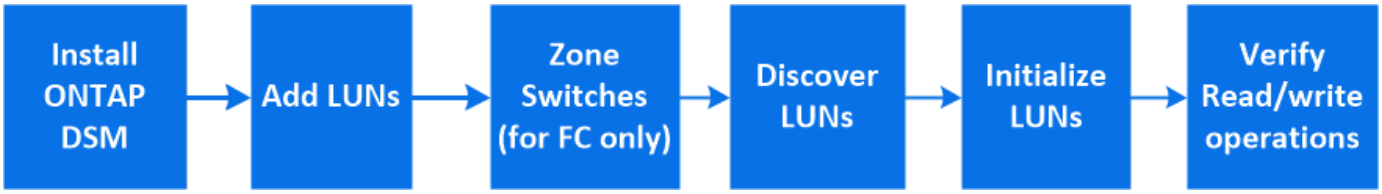
   ```
   /usr/bin/rescan-scsi-bus.sh
   ```

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.



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**.

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.

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.

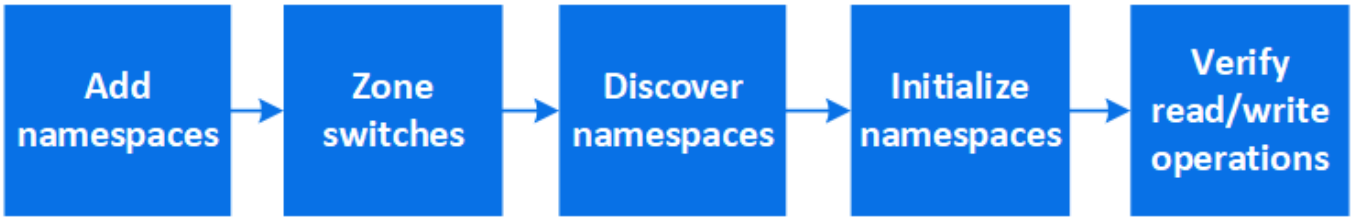
NVMe targets are connected to the network through a standard FC infrastructure using FC switches and host-side adapters.

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.



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**.

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

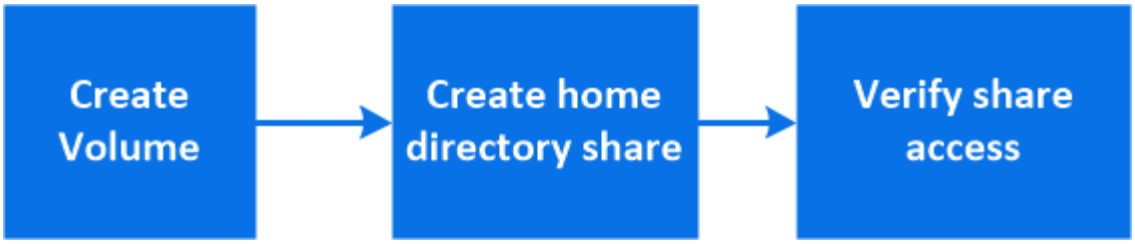
Create volumes to provide VMware datastores using the NFS protocol.

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. Create a new volume: click **Storage** > **Volumes** and then click **Add**.
2. Create a home directory share: click **Storage** > **Shares**, click **Add**, and select **Home Directory**.
3. 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_`
    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.

Steps

1. Create a new volume: click **Storage** > **Volumes** and then click **Add**.
    a. The default export policy grants full access to all users. You can add more restrictive rules to the export policy later.
2. Switch to a Linux system 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 might want to 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. Create or modify an export policy for a volume: click **Storage** > **Volumes**, click an NFS-enabled volume, click **More**, and then click **Edit Export Policy**.
2. 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.

Steps

1. Create a new volume: 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.

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 might want to 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.

Steps

1. Create a new volume: click **Storage** > **Volumes** and then click **Add**.
   a. Create an export policy: click **More Options** and check **Share via NFS**.

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

b. Create a share: check **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.

2. Switch to a Linux client 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.
3. 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 might want to 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. It is assumed that you have already 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 and configure Kerberos: click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, click → under Kerberos, click **Add** under Kerberos Realm, and complete the following sections:
   a. Add Kerberos Realm: enter configuration details depending on KDC vendor.
   b. Add Network Interface to Realm: click **Add** and select a network interface.
5. If desired, add mappings from Kerberos principal names to local user names.
   a. Click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click → under **Name Mapping**.
   b. 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, it is assumed that the LDAP configuration details required in your environment are available and that you are using a default ONTAP LDAP schema.

Steps

1. Configure the required service: click **Storage** > **Storage VMs**, select the storage VM, click **Settings**, and then click ⚙ for LDAP or NIS.
2. 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.

Steps

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

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.

Steps

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

3. Click **More Options** and then select **Add as cache for a remote volume**.

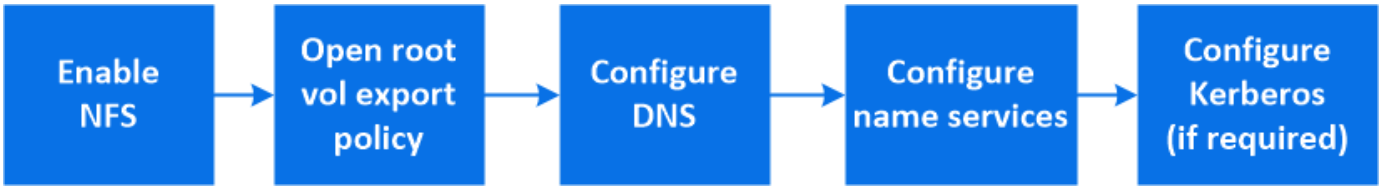
For any new data requests, the FlexCache volume requests the data from the remote volume and stores it. All the subsequent read requests for the data are then served directly from the FlexCache volume.

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.



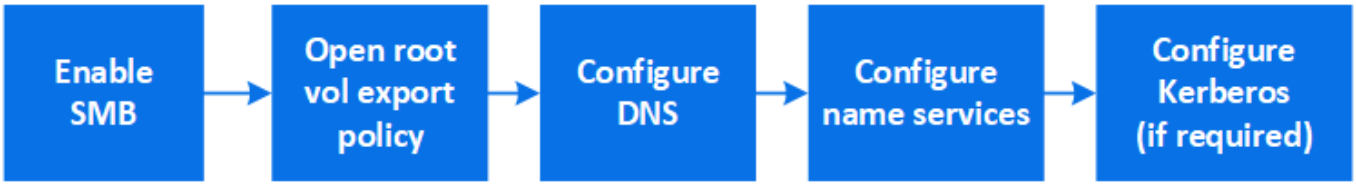
Steps

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.



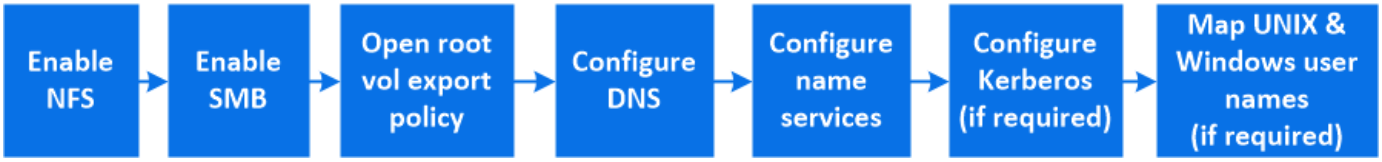
Steps

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.

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.

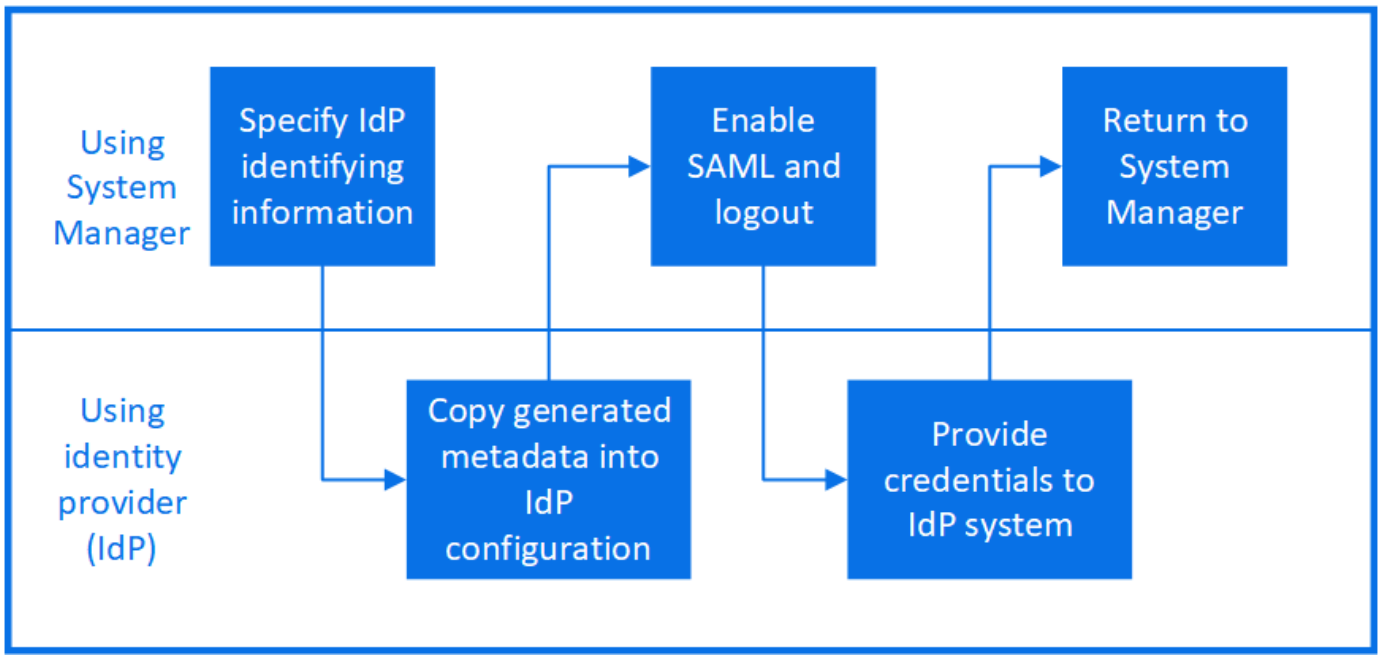
Set up multifactor authentication

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**.

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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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.

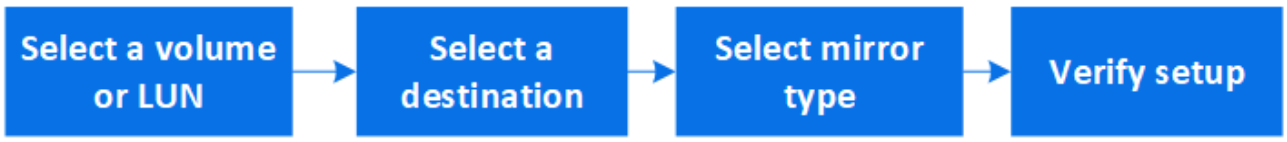
   Select the protection policy based on the type of data protection you need.

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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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.

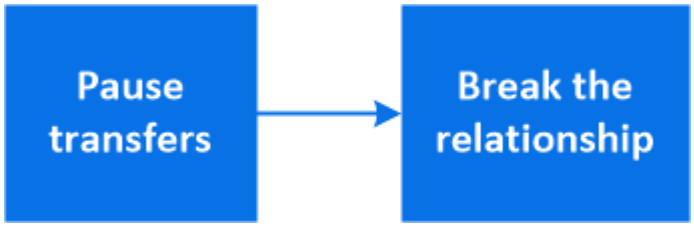


Steps

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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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.

= Restore from a SnapMirror destination to original source
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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.

= Roll back data to an earlier version from a vault
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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.

= Extend to the cloud

= Cloud overview
:toc: macro
:toclevels: 1

:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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 one of the following service providers:

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

= Tier data to cloud
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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.

You will need to use the CLI to set a volume tiering policy and to start tiering.

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 Primary**.

= Register a cluster with NDAS

:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

If you are using NetApp Data Availability Services (NDAS) to back up your data to the cloud or StorageGRID, you must first register the ONTAP cluster that contains the volumes to be protected. A registration key is generated automatically within the NDAS app and the key must be entered on the ONTAP cluster using System Manager.

Before registering the ONTAP cluster with NDAS, ONTAP cluster and SnapMirror requirements must be satisfied.

For more information, see Registering ONTAP target storage with NetApp Data Availability Services.

Steps

1. Click **Cluster** > **Settings**> **Cloud Registration**, then click ⚙.
2. Paste in the registration key from the NDAS app.
3. Verify the IPspace and click Register.

   If the status is unavailable or disconnected, you must reregister the ONTAP cluster with NDAS by using a new configuration key.

= View cluster performance

= Cluster performance overview
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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 any object or operation
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

You can search for various actions and objects in System Manager. Then, you can sort and filter the results.

NOTE

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

== 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.

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

Type of search	**Sample search string**	**Sample search results**
By object name	vol_	vol_lun_dest on storage VM: svm0 (Volume) /vol/vol…est1/lun on storage VM: svm0 (LUN) svm0:vol_lun_dest1 role: Destination (Relationship)
By location in interface	volume	Add Volume (Action) Protection – Overview (Page) Recover deleted volume (Help)
By actions	add	Add Volume (Action) Network – Overview (Page) Expand volumes and LUNs (Help)

Type of search	Sample search string	Sample search results
By help content	san	Storage – Overview (Page) SAN overview (Help) Provision SAN storage for databases (Help)

== Filtering

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

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.

= Monitor cluster performance using System Manager
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:

:icons: font
:linkattrs:
:imagesdir: ./media/

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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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

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

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

- Create a cluster, configure a network, and set up support details for the cluster.
- Configure and manage storage objects, such as disks, local tiers, volumes, qtrees, and quotas.
- Configure protocols, such as SMB/CIFS and NFS, and provision file sharing.
- Configure protocols such as FC, FCoE, NVMe, and iSCSI for block access.
- Create and configure network components, such as subnets, broadcast domains, data and

management interfaces, and interface groups.

- Set up and manage mirroring and vaulting relationships.
- Perform cluster management, storage node management, and storage virtual machine (storage VM) management operations.
- Create and configure storage VMs, manage storage objects associated with storage VMs, and manage storage VM services.
- Monitor and manage high-availability (HA) configurations in a cluster.
- Configure service processors to remotely log in, manage, monitor, and administer the node, regardless of the state of the node.

= Search, filter, and sort any object or operation
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

You can search for various actions and objects in System Manager. Then, you can sort and filter the results.

NOTE

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

== 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.

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

Type of search	Sample search string	Sample search results
By object name	vol_	vol_lun_dest on storage VM: svm0 (Volume) /vol/vol...est1/lun on storage VM: svm0 (LUN) svm0:vol_lun_dest1 role: Destination (Relationship)
By location in interface	volume	Add Volume (Action) Protection – Overview (Page) Recover deleted volume (Help)
By actions	add	Add Volume (Action) Network – Overview (Page) Expand volumes and LUNs (Help)
By help content	san	Storage – Overview (Page) SAN overview (Help) Provision SAN storage for databases (Help)

== Filtering

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

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.

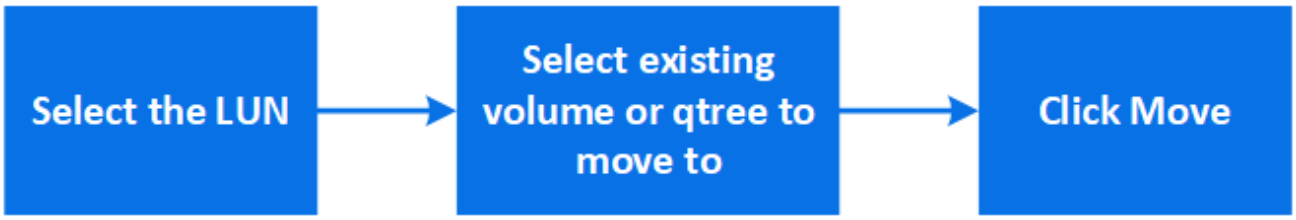
= Balance loads by moving LUNs
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:

:icons: font
:linkattrs:
:imagesdir: ./media/

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.

= Enable new features by adding license keys
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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.

= MetroCluster switchover and switchback
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

You can switchover from one MetroCluster site to the other to perform maintenance or recover from an issue.

Steps

1. Click **(Return to classic version)**.
2. Click **Configuration** > **MetroCluster**.

   System Manager verifies whether a negotiated switchover is possible.

3. 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.

4. Click **Switchover from Site B to Site A** to initiate the switchover process.
5. Click **Switch to the new experience**.

= Recover deleted volumes
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

If you have accidently deleted one or more FlexVol volumes, you can recover these 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.

Steps

1. Click **Storage** > **Volumes**.
2. Click **More** > **Show Deleted Volumes**.
3. Select the volumes and click the desired action.

Deleting a volume deletes the associated configurations of the volume. Recovering a volume does not reset all the configurations. You should 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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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.

= Clone volumes and LUNs for testing
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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.

NOTE

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.

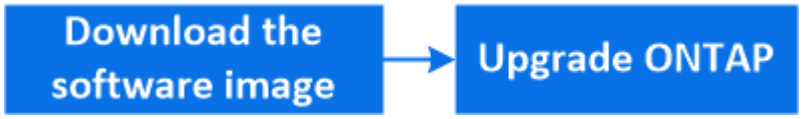
= Update ONTAP
:toc: macro
:toclevels: 1
:hardbreaks:

:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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**.

= Expand storage

= Increase the size of volumes and LUNs
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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.

Steps

1. To increase the size of a volume, click **Storage** > **Volumes**.

   To increase the size of a LUN, click **Storage** > **LUNs**.

2. Hover over the name of the volume or LUN you want to increase in size, click ⋮, and select **Edit**.

= Add disks to a local tier (Add capacity to aggregate)
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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

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

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.

= Rest API

= REST API log overview
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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


```
{
  "records": [
    {
      "svm": {
        "uuid": "19507946-e801-11e9-b984-00a0986ab770",
        "name": "SMQA",
        "_links": {
          "self": {
            "href": "/api/svm/svms/19507946-e801-11e9-b984-00a0986ab770"
          }
        }
      },
      "volume": {
        "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
        "name": "vol_vol_test2_dest_dest",
        "_links": {
          "self": {
            "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-00a0986abd71"
          }
        }
      },
      "id": 1,
      "name": "test2",
      "security_style": "mixed",
      "unix_permissions": 777,
      "export_policy": {
```

```
        "name": "default",
        "id": 12884901889,
        "_links": {
          "self": {
            "href": "/api/protocols/nfs/export-policies/12884901889"
          }
        }
      },
      "path": "/vol_vol_test2_dest_dest/test2",
      "_links": {
        "self": {
          "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-00a0986abd71/1"
        }
      }
    },
    ],
    "num_records": 1,
    "_links": {
      "self": {
        "href": "/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"
      }
    }
  }
```


= Getting more information
:toc: macro
:toclevels: 1
:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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

:hardbreaks:
:nofooter:
:icons: font
:linkattrs:
:imagesdir: ./media/

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