ONTAP System Manager Classic documentation

System Manager Classic

NetApp
June 22, 2024

This PDF was generated from https://docs.netapp.com/us-en/ontap-system-manager-classic/index.html on June 22, 2024. Always check docs.netapp.com for the latest.

Table of Contents

ONTAP System Manager Classic documentation . . . 1
Provision NAS storage . . . 2
NFS configuration . . . 2
NFS configuration for ESXi using VSC . . . 26
SMB/CIFS and NFS multiprotocol configuration . . . 40
SMB/CIFS configuration . . . 63
Provision SAN storage . . . 79
FC configuration for ESXi using VSC . . . 79
FC configuration for Red Hat Enterprise Linux . . . 91
FC configuration for Windows . . . 111
iSCSI configuration for ESXi using VSC . . . 127
iSCSI configuration for Red Hat Enterprise Linux . . . 141
iSCSI configuration for Windows . . . 160
Data protection and disaster recovery . . . 177
Cluster and SVM peering configuration . . . 177
Volume disaster recovery . . . 187
Volume disaster recovery preparation . . . 199
Volume backup using SnapVault . . . 208
Volume restore management using SnapVault . . . 216
Cluster administration . . . 222
Cluster administration . . . 222
Volume move management . . . 244
SNMP configuration . . . 251
Cluster management using System Manager 9.6 and 9.7 . . . 258
Cluster management using System Manager 9.6 and 9.7 . . . 258
Legal notices . . . 636
Copyright . . . 636
Trademarks . . . 636
Patents . . . 636
Privacy policy . . . 636
Open source . . . 636

ONTAP System Manager Classic documentation

Provision NAS storage

NFS configuration

NFS configuration overview

You can quickly set up NFS access to a new volume on either a new or existing storage virtual machine (SVM) using the ONTAP System Manager classic interface (ONTAP 9.7 and earlier).

Use this procedure if you want to configure access to a volume in the following way:

- NFS access will be through NFSv3, not NFSv4 or NFSv4.1.
- You want to use best practices, not explore every available option.
- Your data network uses the default IPspace, the default broadcast domain, and the default failover group.

  If your data network is flat, using these default objects ensures that LIFs will fail over correctly in the event of a link failure. If you are not using the default objects, you should refer to Network Management Documentation for information on how to configure LIF path failover.

- UNIX file permissions will be used to secure the new volume.
- LDAP, if used, is provided by Active Directory.

If you want details about the range of ONTAP NFS protocol capabilities, consult the NFS reference overview.

Other ways to do this in ONTAP

To perform these tasks with…	Refer to…
The redesigned System Manager (available with ONTAP 9.7 and later)	Provision NAS storage for Linux servers using NFS
The ONTAP command line interface	NFS configuration overview with the CLI

NFS configuration workflow

Configuring NFS involves optionally creating an aggregate and then choosing a workflow that is specific to your goal—creating a new NFS-enabled SVM, configuring NFS access to an existing SVM, or simply adding an NFS volume to an existing SVM that is already fully configured for NFS access.

Create an aggregate

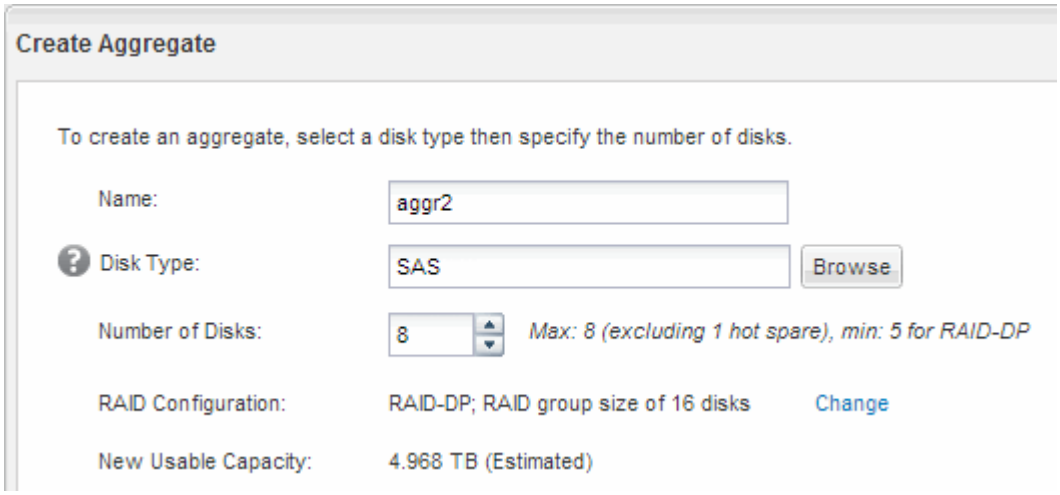
If you do not want to use an existing aggregate, you can create a new aggregate to provide physical storage to the volume which you are provisioning.

About this task

If you have an existing aggregate that you want to use for the new volume, you can skip this procedure.

Steps

1. Enter the URL `https://IP-address-of-cluster-management-LIF` in a web browser and log in to System Manager using your cluster administrator credential.
2. Navigate to the **Aggregates** window.
3. Click **Create.**
4. Follow the instructions on the screen to create the aggregate using the default RAID-DP configuration, and then click **Create**.



Results

The aggregate is created with the specified configuration and added to the list of aggregates in the Aggregates window.

Decide where to provision the new volume

Before you create a new NFS volume, you must decide whether to place it in an existing storage virtual machine (SVM), and, if so, how much configuration the SVM requires. This decision determines your workflow.

Procedure

- If you want to provision a volume on a new SVM, create a new NFS-enabled SVM.

  Creating a new NFS-enabled SVM

  You must choose this option if NFS is not enabled on an existing SVM.

- If you want to provision a volume on an existing SVM on which NFS is enabled but not configured, configure NFS access on the existing SVM.

  Configuring NFS access on an existing SVM

  This is the case if you did not follow this procedure to create the SVM while configuring a different protocol.

- If you want to provision a volume on an existing SVM that is fully configured for NFS access, add an NFS volume to the NFS-enabled SVM.

  Adding an NFS volume to an NFS-enabled SVM

Create a new NFS-enabled SVM

Setting up an NFS-enabled SVM involves creating the new SVM with an NFS volume and export, opening the default export policy of the SVM root volume and then verifying NFS access from a UNIX administration host. You can then configure NFS client access.

Create a new SVM with an NFS volume and export

You can use a wizard that guides you through the process of creating the storage virtual machine (SVM), configuring Domain Name System (DNS), creating a data logical interface (LIF), enabling NFS, optionally configuring NIS, and then creating and exporting a volume.

Before you begin

- Your network must be configured and the relevant physical ports must be connected to the network.
- You must know which of the following networking components the SVM will use:
  - The node and the specific port on that node where the data logical interface (LIF) will be created
  - The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
  - NIS information, if your site uses NIS for name services or name mapping
- The subnet must be routable to all external servers required for services such as Network Information Service (NIS), Lightweight Directory Access Protocol (LDAP), Active Directory (AD), and DNS.
- Any external firewalls must be appropriately configured to allow access to network services.
- The time on the AD domain controllers, clients, and SVM must be synchronized to within five minutes of each other.

Steps

1. Navigate to the **SVMs** window.
2. Click **Create.**
3. In the **Storage Virtual Machine (SVM) Setup** dialog box, create the SVM:

   a. Specify a unique name for the SVM.

      The name must either be a fully qualified domain name (FQDN) or follow another convention that ensures unique names across a cluster.

   b. Select all the protocols that you have licenses for and that you will eventually use on the SVM, even if you do not want to configure all the protocols immediately.

      If CIFS access is required eventually, you must select **CIFS** now so that CIFS and NFS clients can share the same data LIF.

   c. Keep the default language setting, C.UTF-8.

      If you support international character display in both NFS and SMB/CIFS clients, consider using the **UTF8MB4** language code, which is available beginning with ONTAP 9.5.

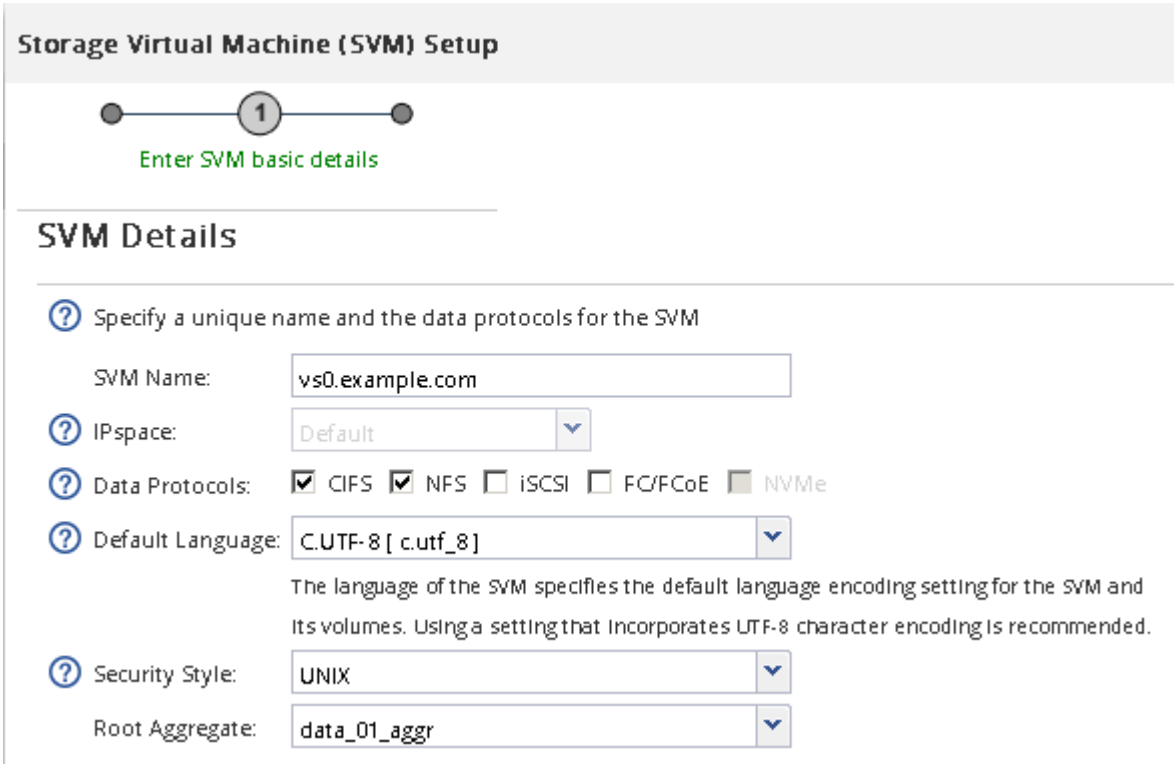
This language is inherited by the volume that you create later, and a volume's language cannot be changed.

d. **Optional**: If you enabled the CIFS protocol, change the security style to **UNIX**.

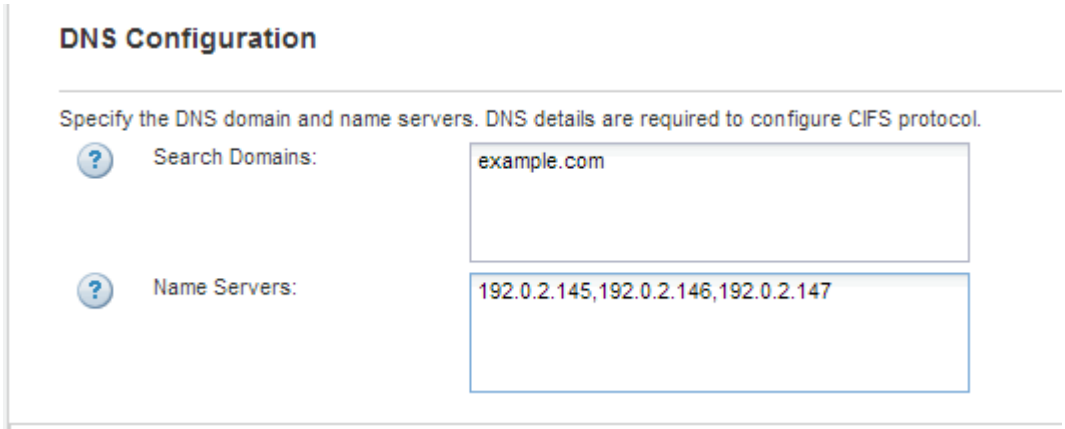
Selecting the CIFS protocol sets the security style to NTFS by default.

e. **Optional**: Select the root aggregate to contain the SVM root volume.

The aggregate that you select for the root volume does not determine the location of the data volume. The aggregate for the data volume is selected automatically when you provision storage in a later step.



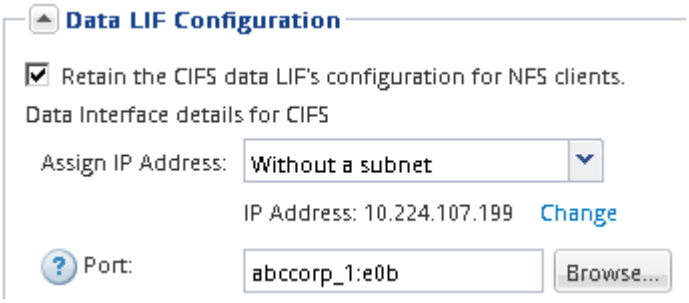
f. In the **DNS Configuration** area, ensure that the default DNS search domain and name servers are the ones that you want to use for this SVM.



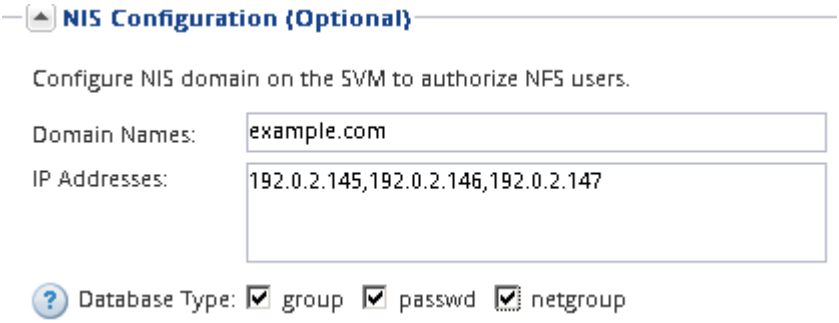
g. Click **Submit & Continue**.

The SVM is created, but protocols are not yet configured.

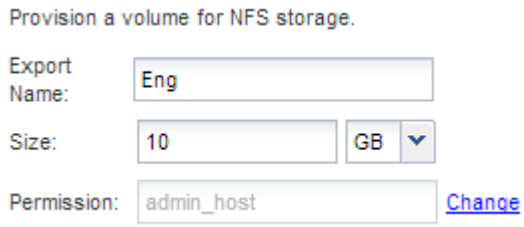
4. In the **Data LIF Configuration** section of the **Configure CIFS/NFS protocol** page, specify the details of the LIF that clients will use to access data:
   a. Assign an IP address to the LIF automatically from a subnet you specify or manually enter the address.
   b. Click **Browse** and select a node and port that will be associated with the LIF.



5. If the **NIS Configuration** area is collapsed, expand it.
6. If your site uses NIS for name services or name mapping, specify the domain and IP addresses of the NIS servers.

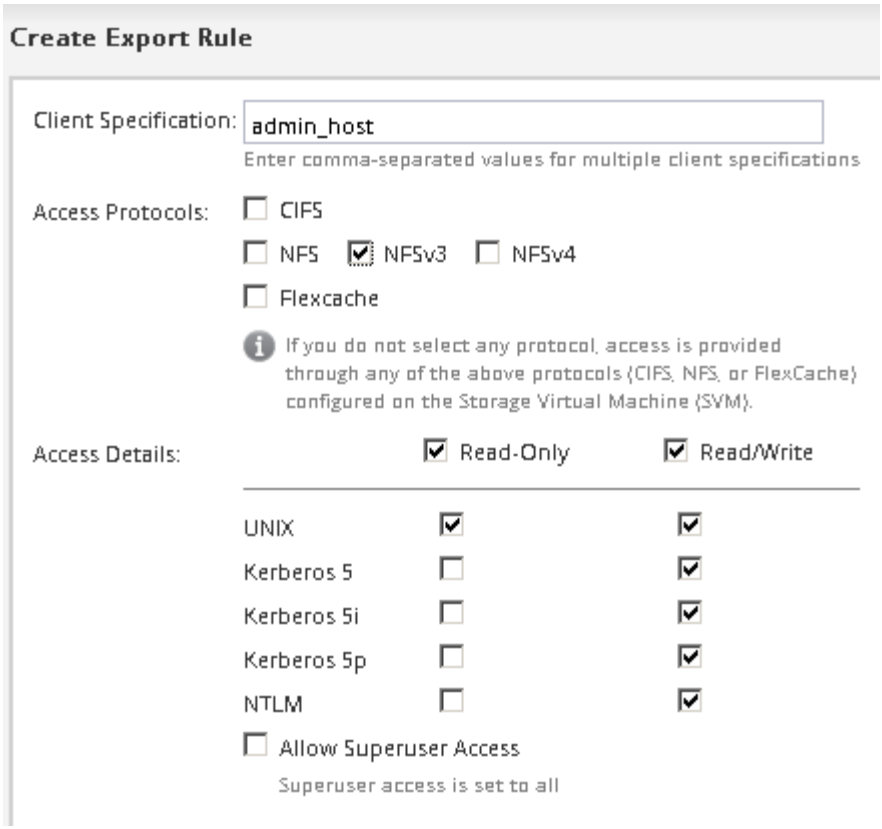


7. Create and export a volume for NFS access:
   a. For **Export Name**, type a name that will be both the export name and the beginning of the volume name.
   b. Specify a size for the volume that will contain the files.



   You do not have to specify the aggregate for the volume because it is automatically located on the aggregate with the most available space.

   c. In the **Permission** field, click **Change**, and specify an export rule that gives NFSv3 access to a UNIX administration host, including Superuser access.



You can create a 10 GB volume named Eng, export it as Eng, and add a rule that gives the “admin_host” client full access to the export, including Superuser access.

8. Click **Submit & Continue**.

   The following objects are created:

   - A data LIF named after the SVM with the suffix “_nfs_lif1”
   - An NFS server
   - A volume that is located on the aggregate with the most available space and has a name that matches the name of the export and ends in the suffix “_NFS_volume”
   - An export for the volume
   - An export policy with the same name as the export

9. For all other protocol configuration pages that are displayed, click **Skip** and configure the protocol later.
10. When the **SVM Administration** page is displayed, configure or defer configuring a separate administrator for this SVM:
    - Click **Skip** and configure an administrator later if required.
    - Enter the requested information and then click **Submit & Continue**.
11. Review the **Summary** page, record any information you might require later and then click **OK**.

    NFS clients need to know the IP address of the data LIF.

Results

A new SVM is created with an NFS server containing a new volume that is exported for an administrator.

Open the export policy of the SVM root volume (Create a new NFS-enabled SVM)

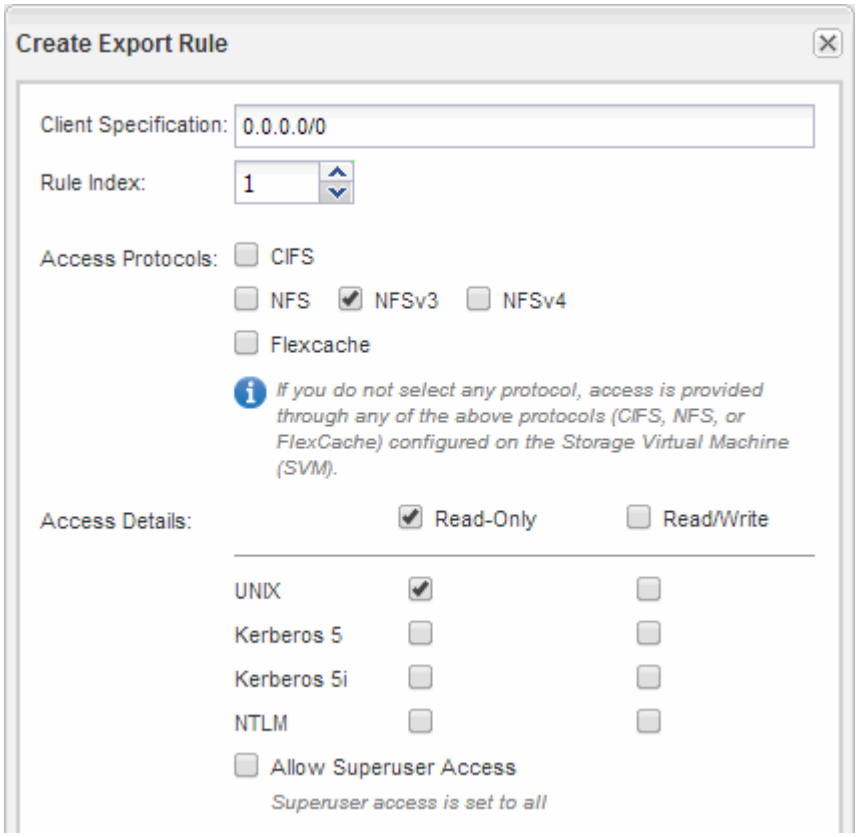
You must add a rule to the default export policy to allow all clients access through NFSv3. Without such a rule, all NFS clients are denied access to the storage virtual machine (SVM) and its volumes.

About this task

You should specify all NFS access as the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes.

Steps

1. Navigate to the **SVMs** window.
2. Click the **SVM Settings** tab.
3. In the **Policies** pane, click **Export Policies**.
4. Select the export policy named **default**, which is applied to the SVM root volume.
5. In the lower pane, click **Add**.
6. In the **Create Export Rule** dialog box, create a rule that opens access to all clients for NFS clients:
   a. In the **Client Specification** field, enter `0.0.0.0/0` so that the rule applies to all clients.
   b. Retain the default value as **1** for the rule index.
   c. Select **NFSv3**.
   d. Clear all the check boxes except the **UNIX** check box under **Read-Only**.
   e. Click **OK**.



Results

NFSv3 clients can now access any volumes created on the SVM.

Configure LDAP (Create a new NFS-enabled SVM)

If you want the storage virtual machine (SVM) to get user information from Active Directory-based Lightweight Directory Access Protocol (LDAP), you must create an LDAP client, enable it for the SVM, and give LDAP priority over other sources of user information.

Before you begin

- The LDAP configuration must be using Active Directory (AD).

  If you use another type of LDAP, you must use the command-line interface (CLI) and other documentation to configure LDAP. For more information, see Overview of using LDAP.

- You must know the AD domain and servers, as well as the following binding information: the authentication level, the Bind user and password, the base DN, and the LDAP port.

Steps

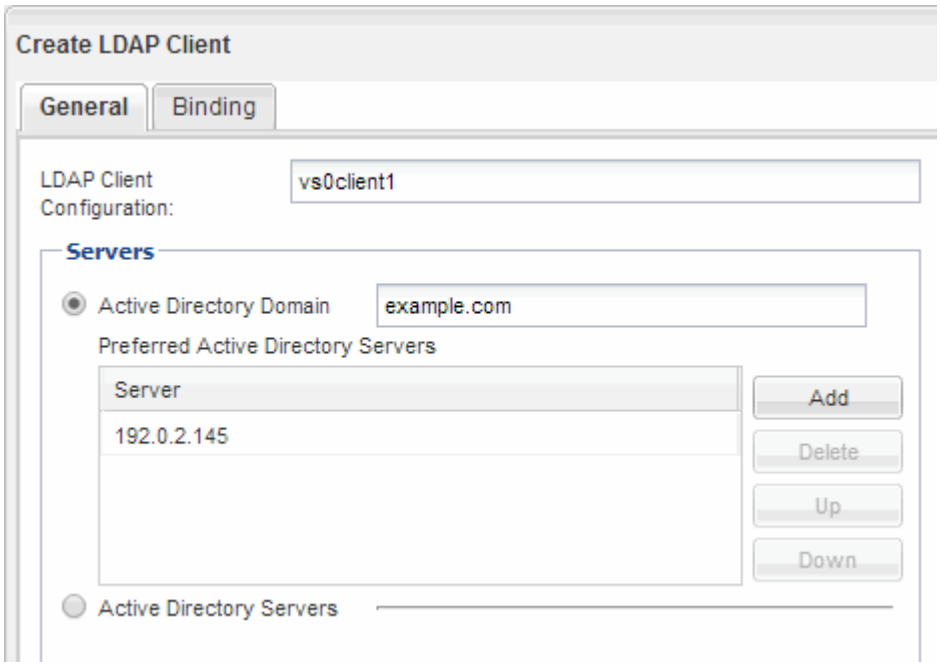
1. Navigate to the **SVMs** window.
2. Select the required SVM
3. Click the **SVM Settings** tab.
4. Set up an LDAP client for the SVM to use:

   a. In the **Services** pane, click **LDAP Client**.

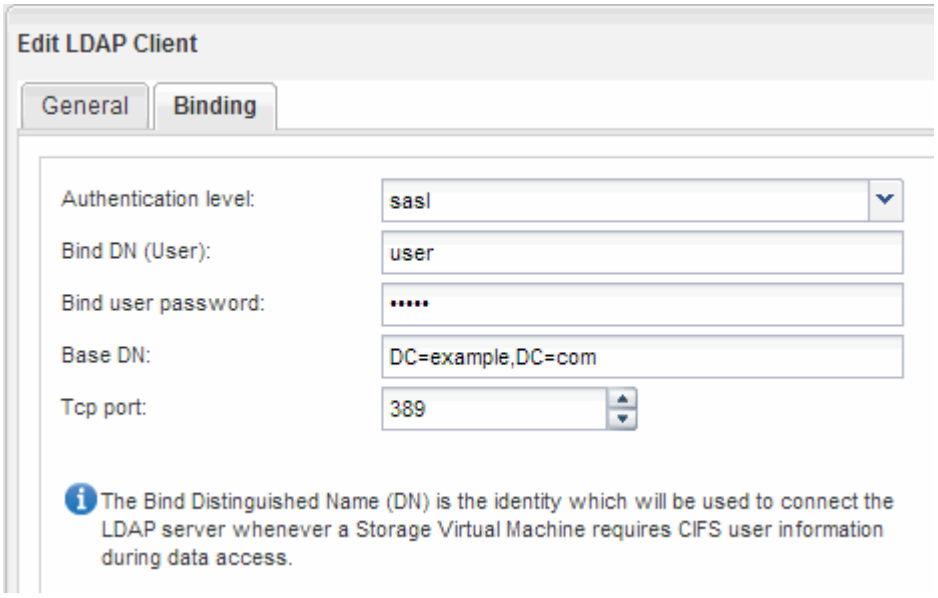
   b. In the **LDAP Client Configuration** window, click **Add**.

   c. In the **General** tab of the **Create LDAP Client** window, type the name of the LDAP client configuration, such as `vs0client1`.

   d. Add either the AD domain or the AD servers.



e. Click **Binding**, and specify the authentication level, the Bind user and password, the base DN, and the port.



f. Click **Save and Close**.

A new client is created and available for the SVM to use.

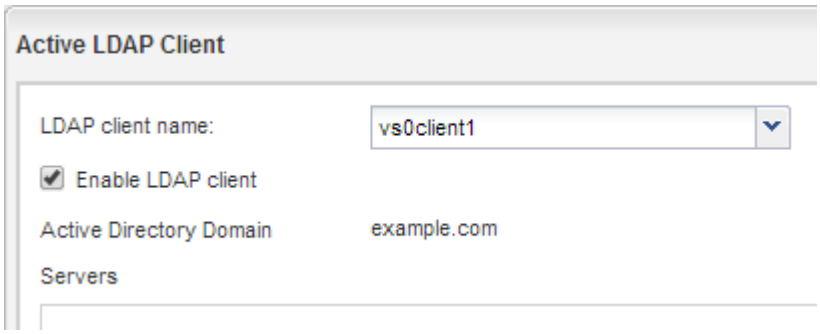
5. Enable the new LDAP client for the SVM:

   a. In the navigation pane, click **LDAP Configuration**.

   b. Click **Edit**.

   c. Ensure that the client you just created is selected in **LDAP client name**.

   d. Select **Enable LDAP client**, and click **OK**.



The SVM uses the new LDAP client.

6. Give LDAP priority over other sources of user information, such as Network Information Service (NIS) and local users and groups:

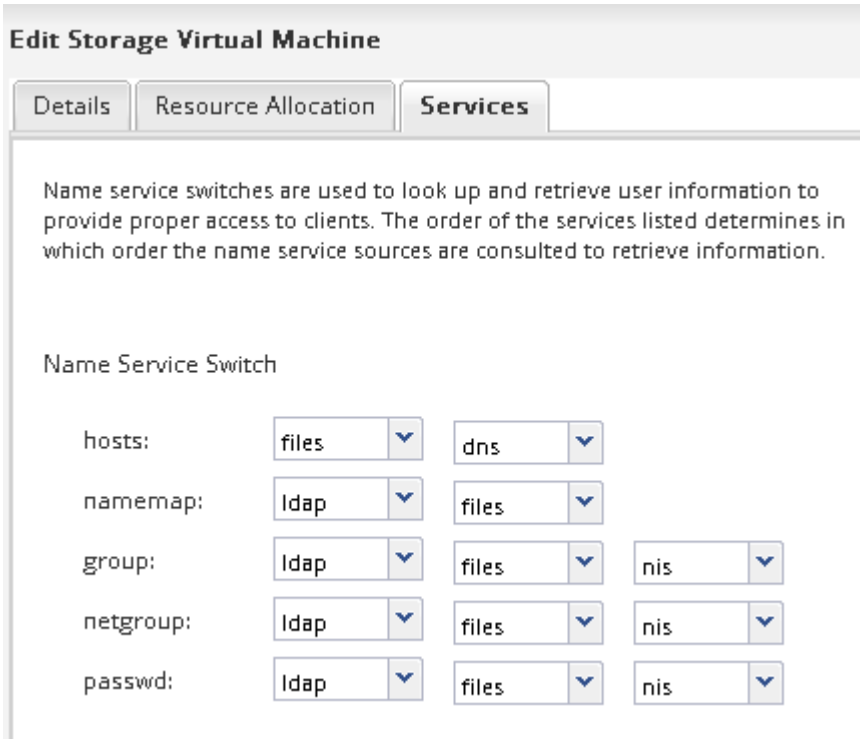
   a. Navigate to the **SVMs** window.

   b. Select the SVM and click **Edit**.

   c. Click the **Services** tab.

   d. Under **Name Service Switch**, specify **LDAP** as the preferred name service switch source for the database types.

e. Click **Save and Close**.



LDAP is the primary source of user information for name services and name mapping on this SVM.

Verify NFS access from a UNIX administration host

After you configure NFS access to storage virtual machine (SVM), you should verify the configuration by logging in to an NFS administration host and reading data from and writing data to the SVM.

Before you begin

- The client system must have an IP address that is allowed by the export rule you specified earlier.
- You must have the login information for the root user.

Steps

1. Log in as the root user to the client system.
2. Enter `cd /mnt/` to change the directory to the mount folder.
3. Create and mount a new folder using the IP address of the SVM:
   a. Enter `mkdir /mnt/folder` to create a new folder.
   b. Enter `mount -t nfs -o nfsvers=3,hard IPAddress:/volume_name /mnt/folder` to mount the volume at this new directory.
   c. Enter `cd folder` to change the directory to the new folder.

   The following commands create a folder named test1, mount the vol1 volume at the 192.0.2.130 IP address on the test1 mount folder, and change to the new test1 directory:

```
host# mkdir /mnt/test1
host# mount -t nfs -o nfsvers=3,hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

4. Create a new file, verify that it exists, and write text to it:

   a. Enter `touch filename` to create a test file.

   b. Enter `ls -l filename` to verify that the file exists.

   c. Enter `cat >filename`, type some text, and then press Ctrl+D to write text to the test file.

   d. Enter `cat filename` to display the content of the test file.

   e. Enter `rm filename` to remove the test file.

   f. Enter `cd ..` to return to the parent directory.

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

Results

You have confirmed that you have enabled NFS access to the SVM.

Configure and verify NFS client access (Create a new NFS-enabled SVM)

When you are ready, you can give select clients access to the share by setting UNIX file permissions on a UNIX administration host and adding an export rule in System Manager. Then you should test that the affected users or groups can access the volume.

Steps

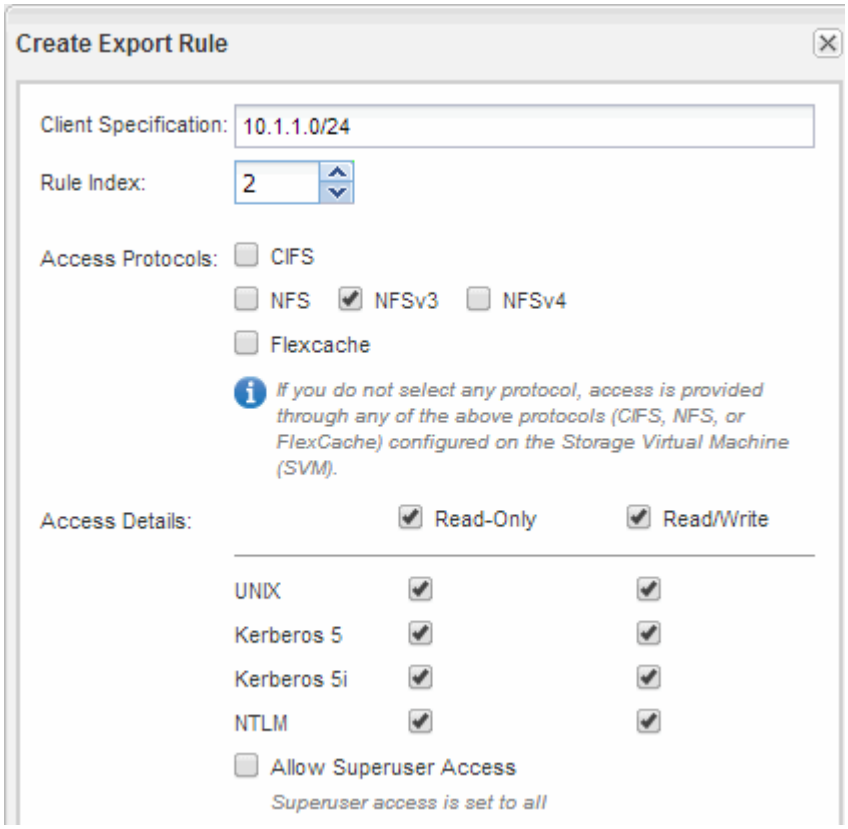
1. Decide which clients and users or groups will be given access to the share.
2. On a UNIX administration host, use the root user to set UNIX ownership and permissions on the volume.
3. In System Manager, add rules to the export policy to permit NFS clients to access the share.
   a. Select the storage virtual machine (SVM), and click **SVM Settings**.
   b. In the **Policies** pane, click **Export Policies**.
   c. Select the export policy with the same name as the volume.
   d. In the **Export Rules** tab, click **Add**, and specify a set of clients.
   e. Select **2** for the **Rule Index** so that this rule executes after the rule that allows access to the

administration host.

f. Select **NFSv3**.

g. Specify the access details that you want, and click **OK.**

You can give full read/write access to clients by typing the subnet `10.1.1.0/24` as the **Client Specification**, and selecting all the access check boxes except **Allow Superuser Access**.



4. On a UNIX client, log in as one of the users who now has access to the volume, and verify that you can mount the volume and create a file.

Configure NFS access to an existing SVM

Adding access for NFS clients to an existing SVM involves adding NFS configurations to the SVM, opening the export policy of the SVM root volume, optionally configuring LDAP, and verifying NFS access from a UNIX administration host. You can then configure NFS client access.

Add NFS access to an existing SVM

Adding NFS access to an existing SVM involves creating a data LIF, optionally configuring NIS, provisioning a volume, exporting the volume, and configuring the export policy.

Before you begin

- You must know which of the following networking components the SVM will use:
  - The node and the specific port on that node where the data logical interface (LIF) will be created

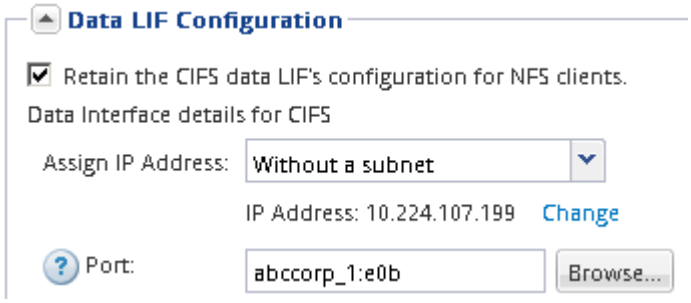
    - The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
- Any external firewalls must be appropriately configured to allow access to network services.
- The NFS protocol must be allowed on the SVM.

For more information, see the Network management documentation.

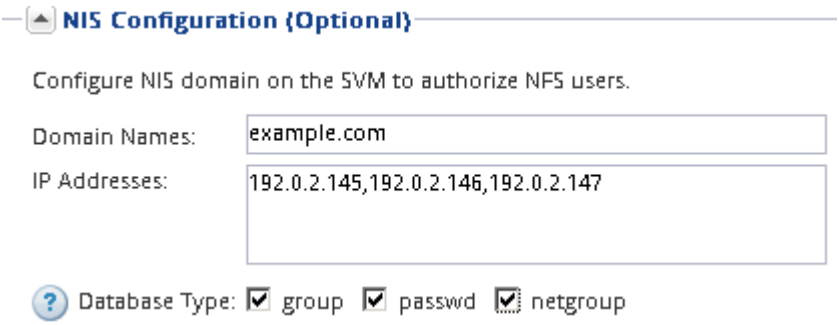
Steps

1. Navigate to the area where you can configure the protocols of the SVM:
    a. Select the SVM that you want to configure.
    b. In the **Details** pane, next to **Protocols**, click **NFS**.

2. In the **Configure NFS protocol** dialog box, create a data LIF.
    a. Assign an IP address to the LIF automatically from a subnet you specify or manually enter the address.
    b. Click **Browse** and select a node and port that will be associated with the LIF.

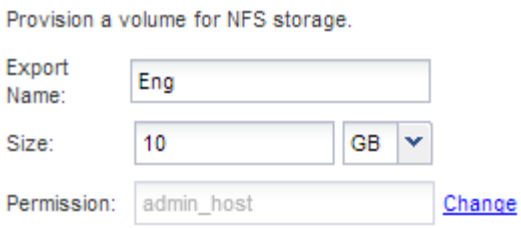


3. If your site uses NIS for name services or name mapping, specify the domain and IP addresses of the NIS servers and select the database types for which you want to add the NIS name service source.



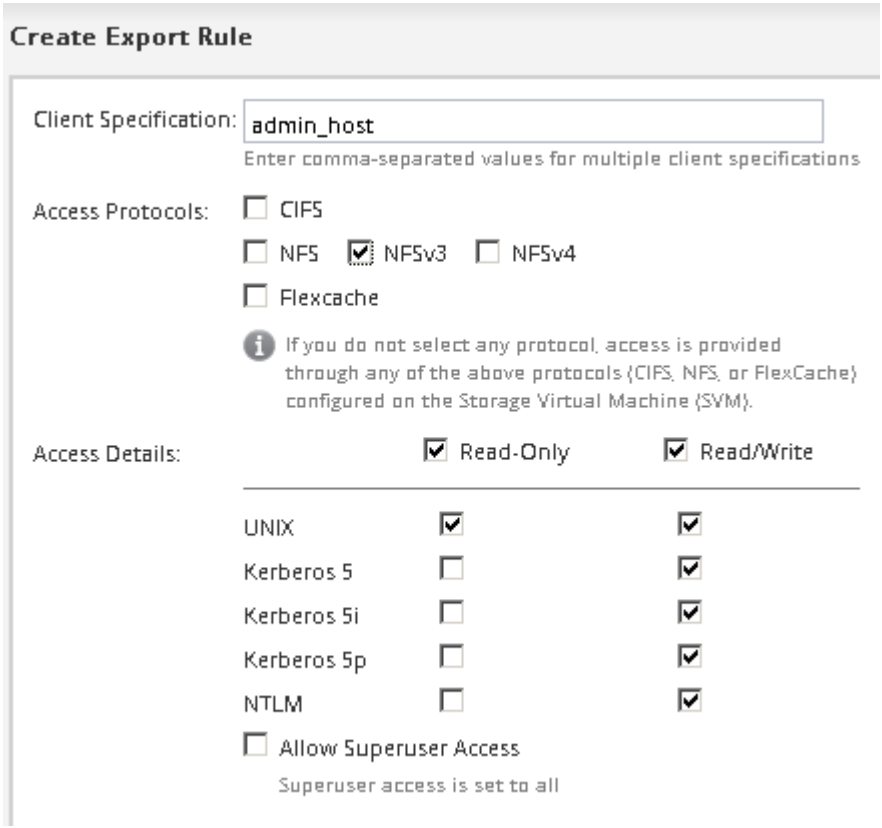
    If NIS services are not available, do not attempt to configure it. Improperly configured NIS services can cause datastore access issues.

4. Create and export a volume for NFS access:
    a. For **Export Name**, type a name that will be both the export name and the beginning of the volume name.
    b. Specify a size for the volume that will contain the files.



You do not have to specify the aggregate for the volume because it is automatically located on the aggregate with the most available space.

c. In the **Permission** field, click **Change**, and specify an export rule that gives NFSv3 access to a UNIX administration host, including Superuser access.



You can create a 10 GB volume named Eng, export it as Eng, and add a rule that gives the “admin_host” client full access to the export, including Superuser access.

5. Click **Submit & Close**, and then click **OK**.

Open the export policy of the SVM root volume (Configure NFS access to an existing SVM)

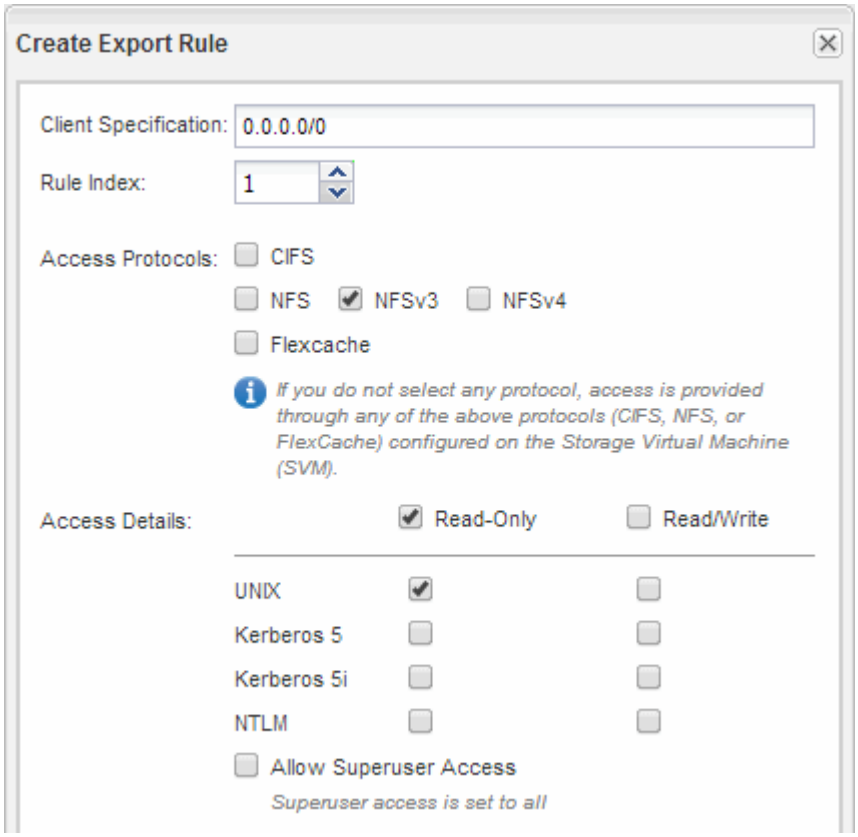
You must add a rule to the default export policy to allow all clients access through NFSv3. Without such a rule, all NFS clients are denied access to the storage virtual machine (SVM) and its volumes.

About this task

You should specify all NFS access as the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes.

Steps

1. Navigate to the **SVMs** window.
2. Click the **SVM Settings** tab.
3. In the **Policies** pane, click **Export Policies**.
4. Select the export policy named **default**, which is applied to the SVM root volume.
5. In the lower pane, click **Add**.
6. In the **Create Export Rule** dialog box, create a rule that opens access to all clients for NFS clients:
   a. In the **Client Specification** field, enter `0.0.0.0/0` so that the rule applies to all clients.
   b. Retain the default value as **1** for the rule index.
   c. Select **NFSv3**.
   d. Clear all the check boxes except the **UNIX** check box under **Read-Only**.
   e. Click **OK**.



Results

NFSv3 clients can now access any volumes created on the SVM.

Configure LDAP (Configure NFS access to an existing SVM)

If you want the storage virtual machine (SVM) to get user information from Active Directory-based Lightweight Directory Access Protocol (LDAP), you must create an LDAP client, enable it for the SVM, and give LDAP priority over other sources of user information.

Before you begin

- The LDAP configuration must be using Active Directory (AD).

  If you use another type of LDAP, you must use the command-line interface (CLI) and other documentation to configure LDAP. For more information, see Overview of using LDAP.

- You must know the AD domain and servers, as well as the following binding information: the authentication level, the Bind user and password, the base DN, and the LDAP port.

Steps

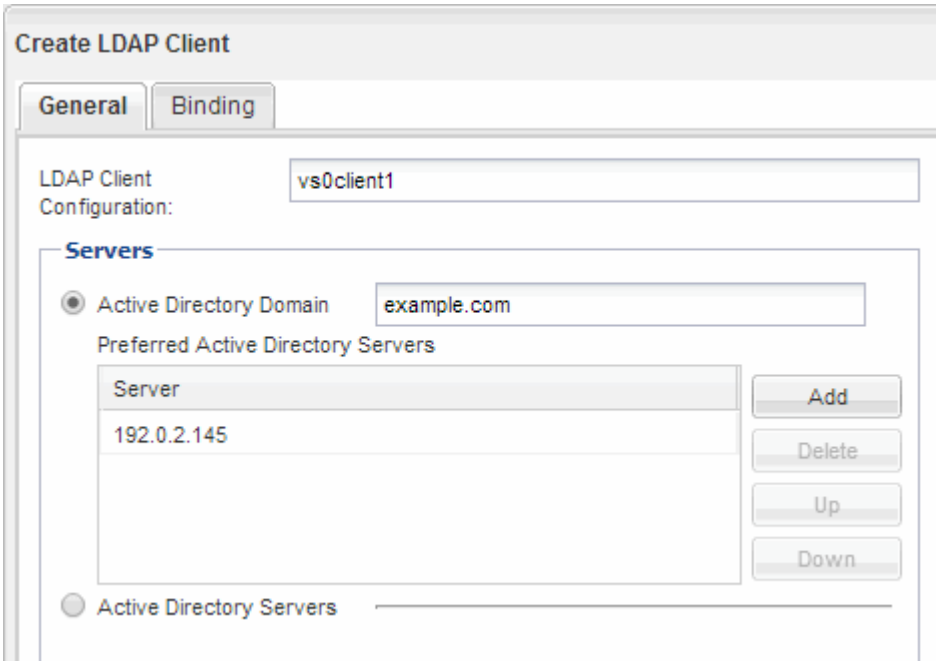
1. Navigate to the **SVMs** window.
2. Select the required SVM
3. Click the **SVM Settings** tab.
4. Set up an LDAP client for the SVM to use:

   a. In the **Services** pane, click **LDAP Client**.

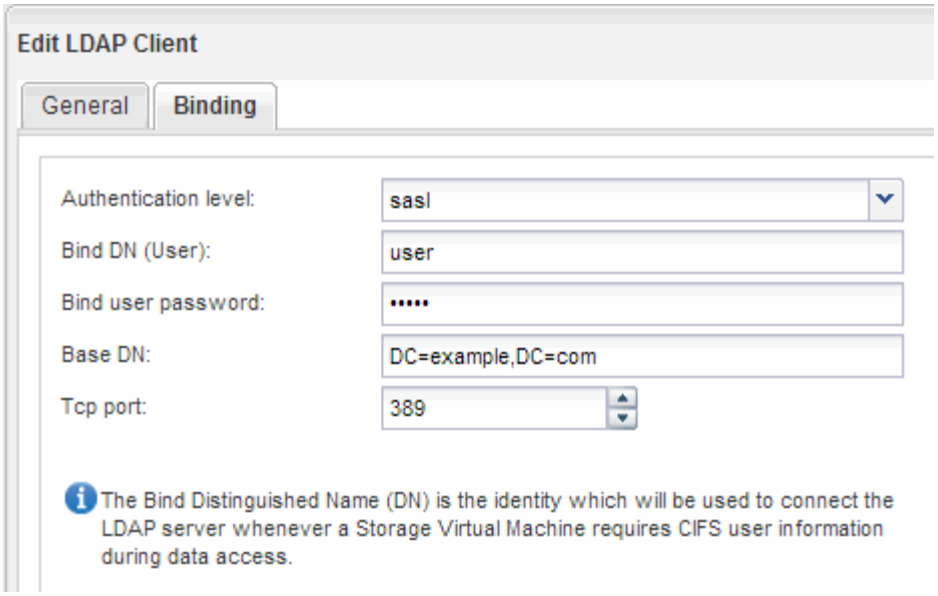
   b. In the **LDAP Client Configuration** window, click **Add**.

   c. In the **General** tab of the **Create LDAP Client** window, type the name of the LDAP client configuration, such as `vs0client1`.

   d. Add either the AD domain or the AD servers.



   e. Click **Binding**, and specify the authentication level, the Bind user and password, the base DN, and the port.



f. Click **Save and Close**.

A new client is created and available for the SVM to use.

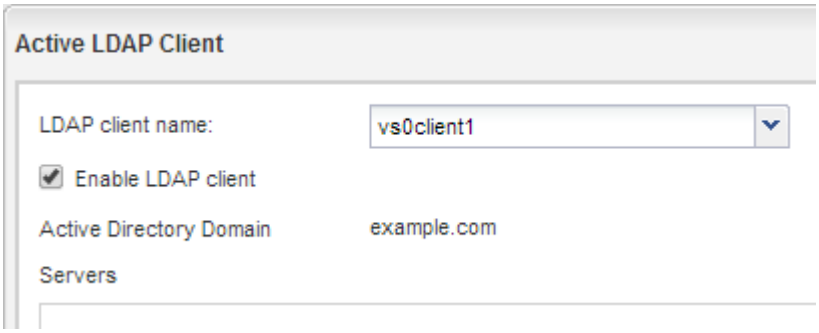
5. Enable the new LDAP client for the SVM:

   a. In the navigation pane, click **LDAP Configuration**.

   b. Click **Edit**.

   c. Ensure that the client you just created is selected in **LDAP client name**.

   d. Select **Enable LDAP client**, and click **OK**.



The SVM uses the new LDAP client.

6. Give LDAP priority over other sources of user information, such as Network Information Service (NIS) and local users and groups:

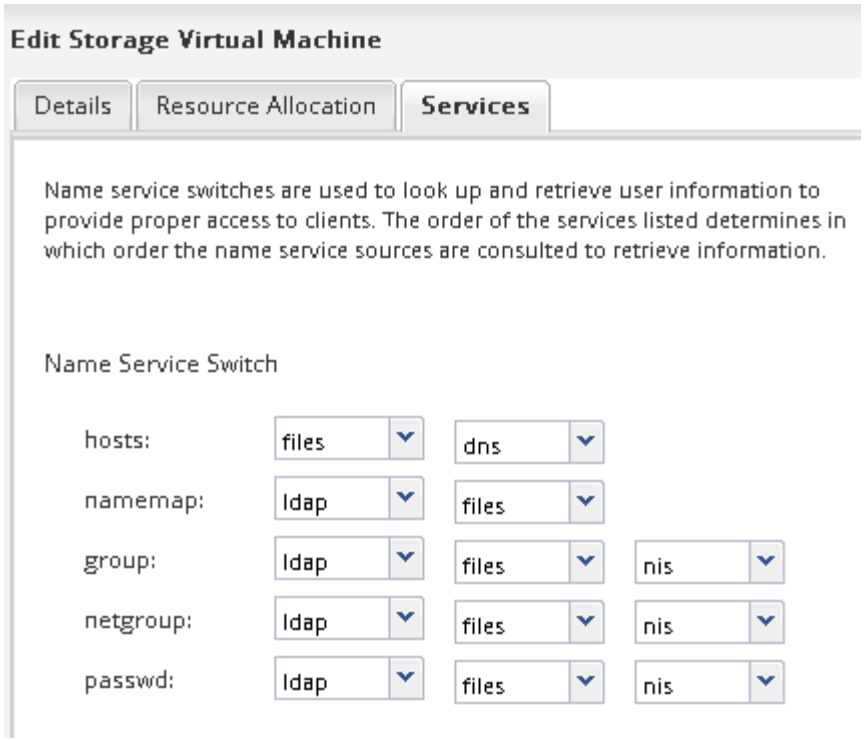
   a. Navigate to the **SVMs** window.

   b. Select the SVM and click **Edit**.

   c. Click the **Services** tab.

   d. Under **Name Service Switch**, specify **LDAP** as the preferred name service switch source for the database types.

   e. Click **Save and Close**.



+
LDAP is the primary source of user information for name services and name mapping on this SVM.

Verify NFS access from a UNIX administration host

After you configure NFS access to storage virtual machine (SVM), you should verify the configuration by logging in to an NFS administration host and reading data from and writing data to the SVM.

Before you begin

- The client system must have an IP address that is allowed by the export rule you specified earlier.
- You must have the login information for the root user.

Steps

1. Log in as the root user to the client system.
2. Enter `cd /mnt/` to change the directory to the mount folder.
3. Create and mount a new folder using the IP address of the SVM:
   a. Enter `mkdir /mnt/folder` to create a new folder.
   b. Enter `mount -t nfs -o nfsvers=3,hard IPAddress:/volume_name /mnt/folder` to mount the volume at this new directory.
   c. Enter `cd folder` to change the directory to the new folder.

      The following commands create a folder named test1, mount the vol1 volume at the 192.0.2.130 IP address on the test1 mount folder, and change to the new test1 directory:

```
host# mkdir /mnt/test1
host# mount -t nfs -o nfsvers=3,hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

4. Create a new file, verify that it exists, and write text to it:

   a. Enter `touch filename` to create a test file.

   b. Enter `ls -l filename` to verify that the file exists.

   c. Enter `cat >filename`, type some text, and then press Ctrl+D to write text to the test file.

   d. Enter `cat filename` to display the content of the test file.

   e. Enter `rm filename` to remove the test file.

   f. Enter `cd ..` to return to the parent directory.

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

Results

You have confirmed that you have enabled NFS access to the SVM.

Configure and verify NFS client access (Configure NFS access to an existing SVM)

When you are ready, you can give select clients access to the share by setting UNIX file permissions on a UNIX administration host and adding an export rule in System Manager. Then you should test that the affected users or groups can access the volume.

Steps

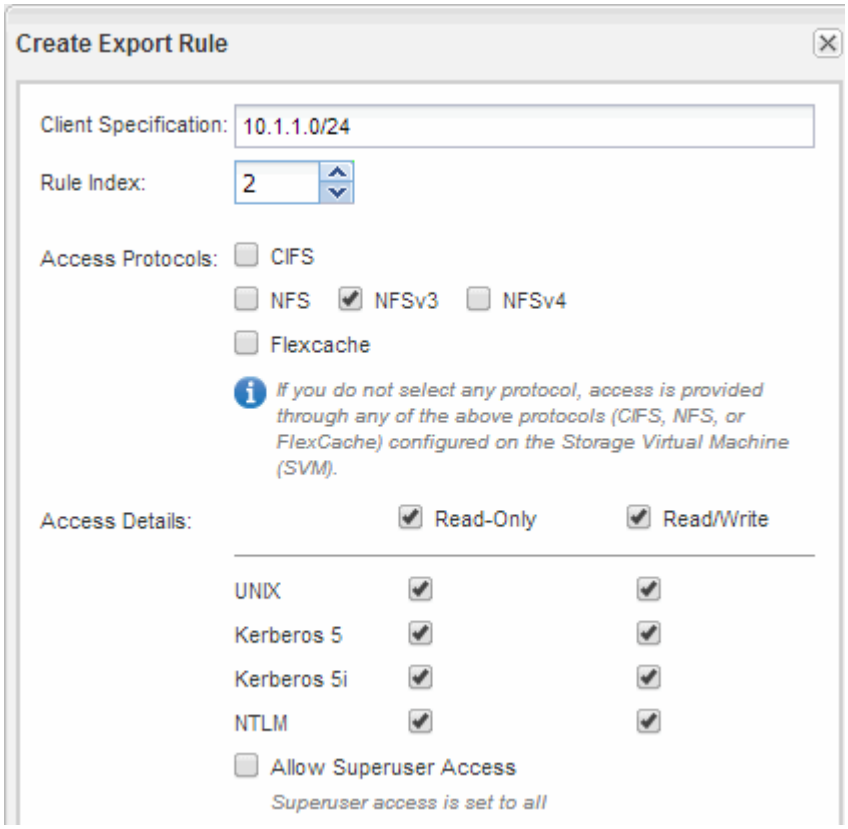
1. Decide which clients and users or groups will be given access to the share.
2. On a UNIX administration host, use the root user to set UNIX ownership and permissions on the volume.
3. In System Manager, add rules to the export policy to permit NFS clients to access the share.
   a. Select the storage virtual machine (SVM), and click **SVM Settings**.
   b. In the **Policies** pane, click **Export Policies**.
   c. Select the export policy with the same name as the volume.
   d. In the **Export Rules** tab, click **Add**, and specify a set of clients.
   e. Select **2** for the **Rule Index** so that this rule executes after the rule that allows access to the

administration host.

f. Select **NFSv3**.

g. Specify the access details that you want, and click **OK.**

You can give full read/write access to clients by typing the subnet `10.1.1.0/24` as the **Client Specification**, and selecting all the access check boxes except **Allow Superuser Access**.



4. On a UNIX client, log in as one of the users who now has access to the volume, and verify that you can mount the volume and create a file.

Add an NFS volume to an NFS-enabled SVM

Adding an NFS volume to an NFS-enabled SVM involves creating and configuring a volume, creating an export policy, and verifying access from a UNIX administration host. You can then configure NFS client access.

Before you begin

NFS must be completely set up on the SVM.

Create and configure a volume

You must create a FlexVol volume to contain your data. You can optionally change the volume's default security style, which is inherited from the security style of the root volume. You can also optionally change the volume's default location in the namespace, which is at the root volume of the storage virtual machine (SVM).

Steps

1. Navigate to the **Volumes** window.
2. Click **Create** > **Create FlexVol**.

   The Create Volume dialog box is displayed.

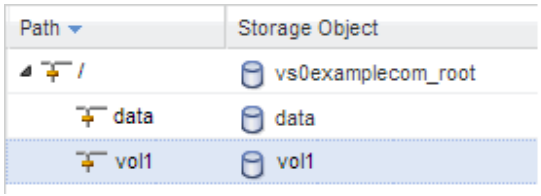
3. If you want to change the default name, which ends in a date and time stamp, specify a new name, such as `vol1`.
4. Select an aggregate for the volume.
5. Specify the size of the volume.
6. Click **Create**.

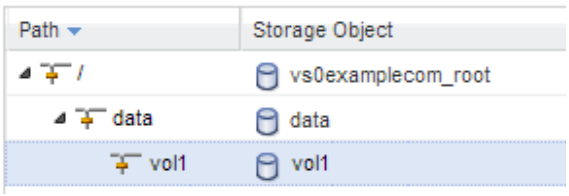
   Any new volume created in System Manager is mounted by default at the root volume using the volume name as the junction name. NFS clients use the junction path and the junction name when mounting the volume.

7. If you do not want the volume to be located at the root of the SVM, modify the place of the new volume in the existing namespace:

   a. Navigate to the **Namespace** window.
   b. Select the **SVM** from the drop-down menu.
   c. Click **Mount**.
   d. In the **Mount Volume** dialog box, specify the volume, the name of its junction path, and the junction path on which you want the volume mounted.
   e. Verify the new junction path in the **Namespace** window.

      If you want to organize certain volumes under a main volume named “data”, you can move the new volume “vol1” from the root volume to the “data” volume.



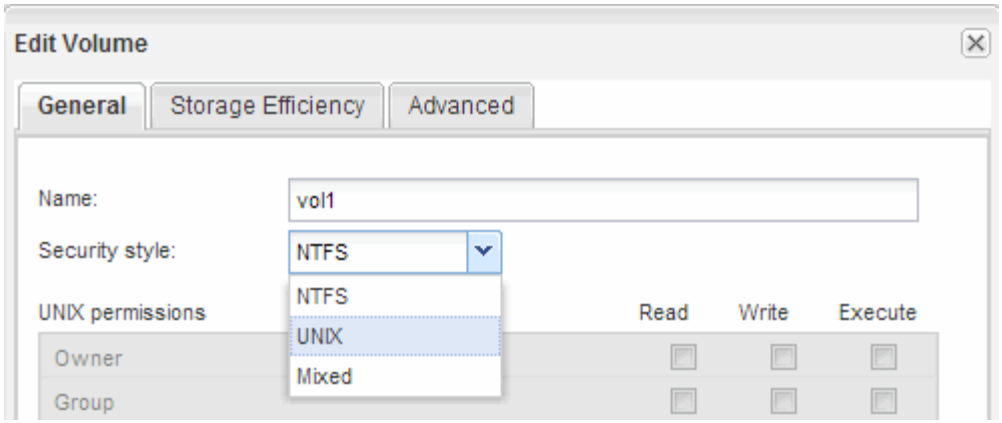


8. Review the volume’s security style and change it, if necessary:

   a. In the **Volume** window, select the volume you just created, and click **Edit**.

      The Edit Volume dialog box is displayed, showing the volume’s current security style, which is inherited from the security style of the SVM root volume.

   b. Make sure the security style is UNIX.

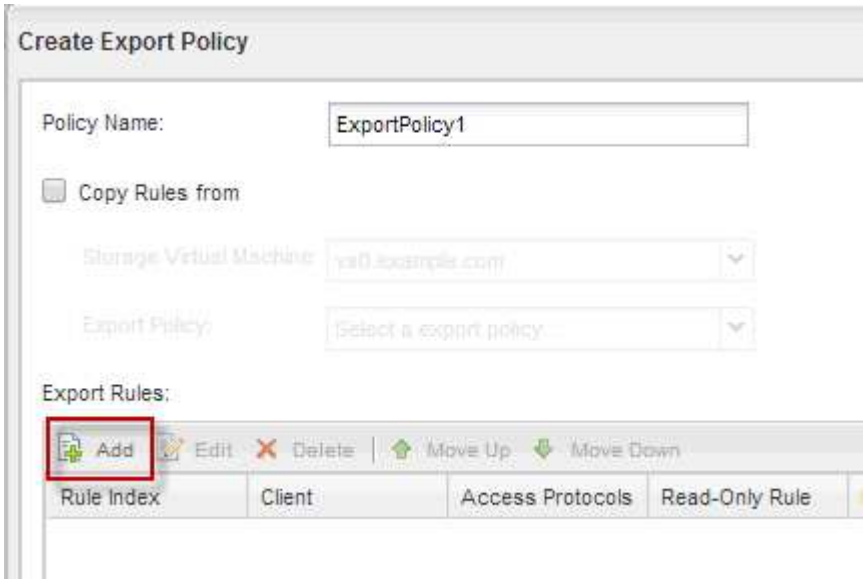


Create an export policy for the volume

Before any NFS clients can access a volume, you must create an export policy for the volume, add a rule that permits access by an administration host, and apply the new export policy to the volume.

Steps

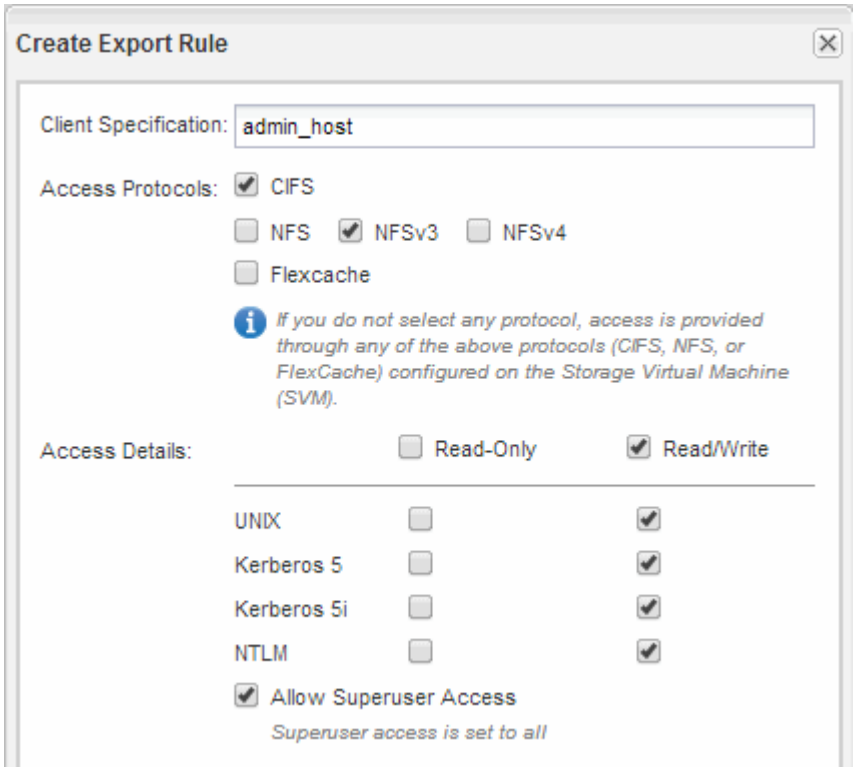
1. Navigate to the **SVMs** window.
2. Click the **SVM Settings** tab.
3. Create a new export policy:
   a. In the **Policies** pane, click **Export Policies** and then click **Create**.
   b. In the **Create Export Policy** window, specify a policy name.
   c. Under **Export Rules**, click **Add** to add a rule to the new policy.



4. In the **Create Export Rule** dialog box, create a rule that allows an administrator full access to the export through all protocols:
   a. Specify the IP address or client name, such as admin_host, from which the exported volume will be administered.

b. Select **NFSv3**.

c. Ensure that all **Read/Write** access details are selected, as well as **Allow Superuser Access**.



d. Click **OK** and then click **Create**.

The new export policy is created, along with its new rule.

5. Apply the new export policy to the new volume so that the administrator host can access the volume:
   a. Navigate to the **Namespace** window.
   b. Select the volume and click **Change Export Policy**.
   c. Select the new policy and click **Change**.

Related information

Verifying NFS access from a UNIX administration host

Verify NFS access from a UNIX administration host

After you configure NFS access to storage virtual machine (SVM), you should verify the configuration by logging in to an NFS administration host and reading data from and writing data to the SVM.

Before you begin

- The client system must have an IP address that is allowed by the export rule you specified earlier.
- You must have the login information for the root user.

Steps

1. Log in as the root user to the client system.

2. Enter `cd /mnt/` to change the directory to the mount folder.
3. Create and mount a new folder using the IP address of the SVM:
   a. Enter `mkdir /mnt/folder` to create a new folder.
   b. Enter `mount -t nfs -o nfsvers=3,hard IPAddress:/volume_name /mnt/folder` to mount the volume at this new directory.
   c. Enter `cd folder` to change the directory to the new folder.

      The following commands create a folder named test1, mount the vol1 volume at the 192.0.2.130 IP address on the test1 mount folder, and change to the new test1 directory:

```
host# mkdir /mnt/test1
host# mount -t nfs -o nfsvers=3,hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

4. Create a new file, verify that it exists, and write text to it:
   a. Enter `touch filename` to create a test file.
   b. Enter `ls -l filename` to verify that the file exists.
   c. Enter `cat >filename`, type some text, and then press Ctrl+D to write text to the test file.
   d. Enter `cat filename` to display the content of the test file.
   e. Enter `rm filename` to remove the test file.
   f. Enter `cd ..` to return to the parent directory.

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

Results

You have confirmed that you have enabled NFS access to the SVM.

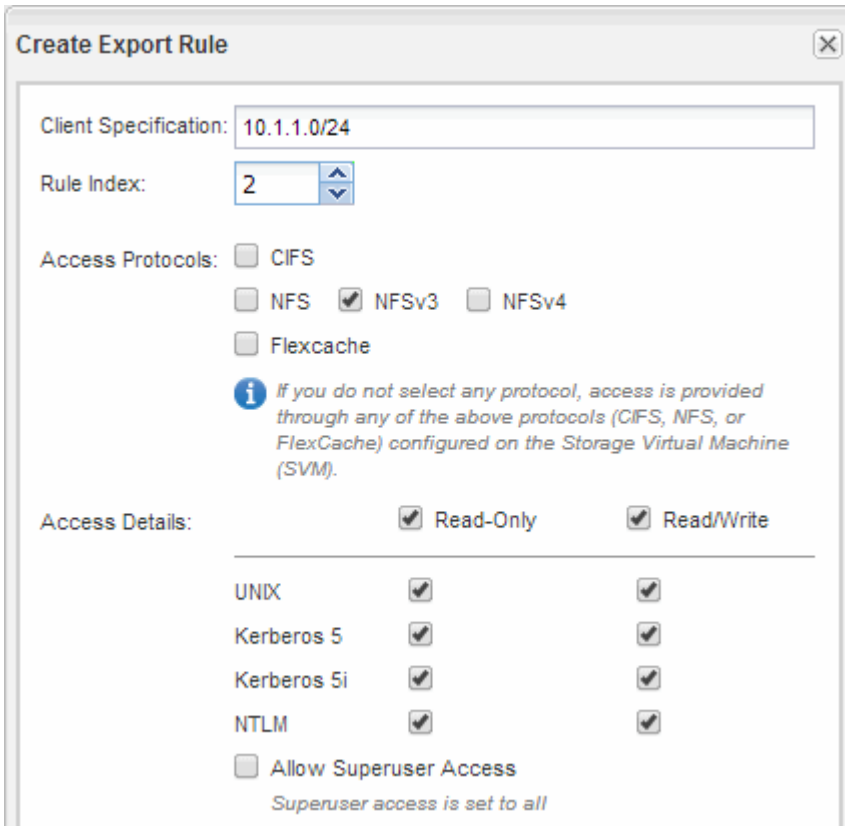
Configure and verify NFS client access (Add an NFS volume to an NFS-enabled SVM)

When you are ready, you can give select clients access to the share by setting UNIX file permissions on a UNIX administration host and adding an export rule in System Manager. Then you should test that the affected users or groups can access the volume.

Steps

1. Decide which clients and users or groups will be given access to the share.
2. On a UNIX administration host, use the root user to set UNIX ownership and permissions on the volume.
3. In System Manager, add rules to the export policy to permit NFS clients to access the share.
   a. Select the storage virtual machine (SVM), and click **SVM Settings**.
   b. In the **Policies** pane, click **Export Policies**.
   c. Select the export policy with the same name as the volume.
   d. In the **Export Rules** tab, click **Add**, and specify a set of clients.
   e. Select **2** for the **Rule Index** so that this rule executes after the rule that allows access to the administration host.
   f. Select **NFSv3**.
   g. Specify the access details that you want, and click **OK.**

      You can give full read/write access to clients by typing the subnet `10.1.1.0/24` as the **Client Specification**, and selecting all the access check boxes except **Allow Superuser Access**.



4. On a UNIX client, log in as one of the users who now has access to the volume, and verify that you can mount the volume and create a file.

NFS configuration for ESXi using VSC

NFS configuration for ESXi using VSC overview

Using the ONTAP System Manager classic interface (ONTAP 9.7 and earlier), you can quickly set up NFS access for ESXi hosts to datastores using ONTAP volumes.

Use this procedure if:

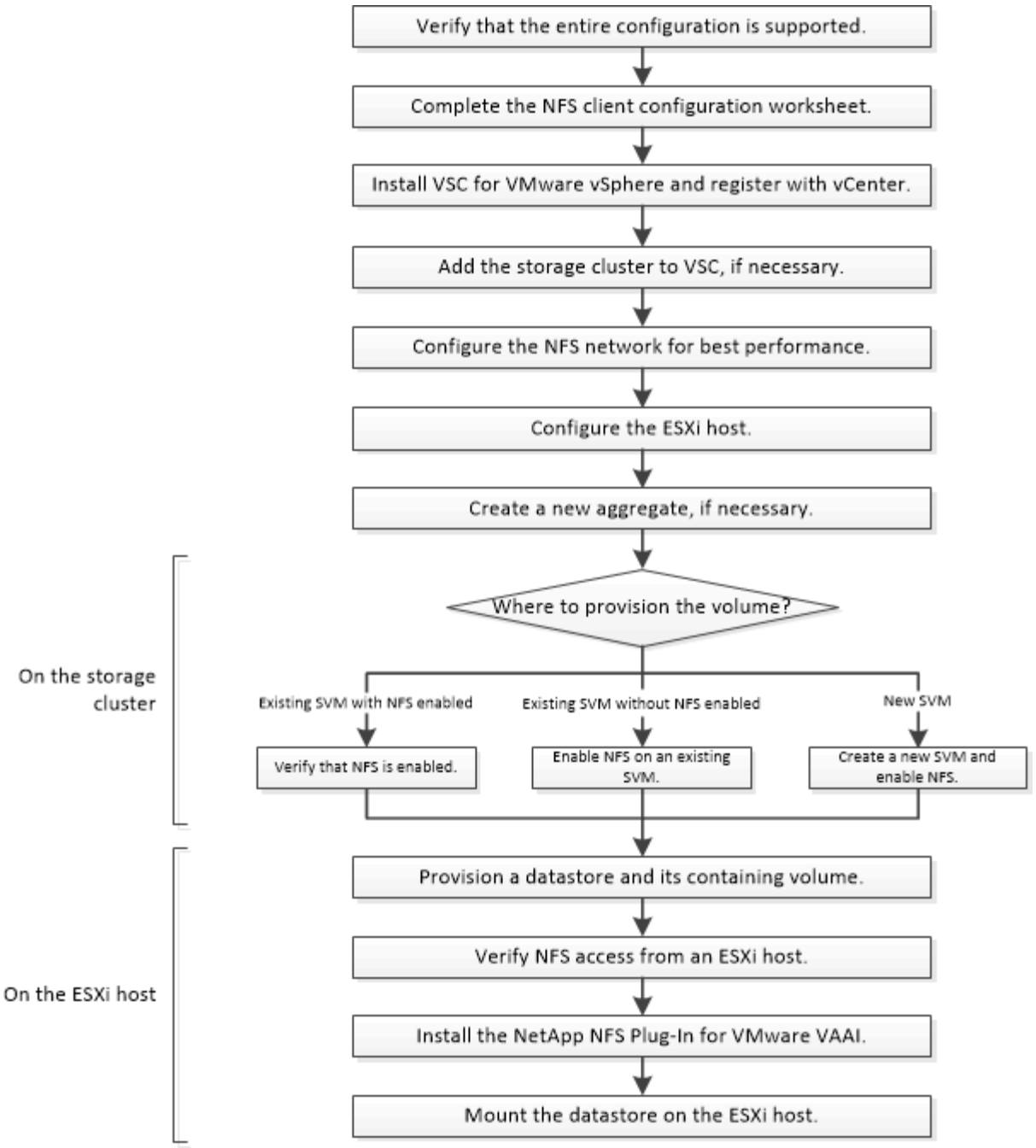
- You are using a supported version of Virtual Storage Console for VMware vSphere (VSC) to provision a datastore and create a volume.
  - Beginning with VSC 7.0, VSC is part of the ONTAP Tools for VMware vSphere virtual appliance, which includes VSC, vStorage APIs for Storage Awareness (VASA) Provider, and Storage Replication Adapter (SRA) for VMware vSphere capabilities.
  - Be sure to check the NetApp Interoperability Matrix Tool to confirm compatibility between your current ONTAP and VSC releases.
- Your data network uses the default IPspace, the default broadcast domain, and the default failover group.

  If your data network is flat, these default objects prescribe that LIFs will fail over correctly in the event of a link failure. If you are not using the default objects, you should refer to Network Management for information about how to configure LIF path failover.
- You want to use the Plug-In for VMware VAAI.
  - VMware vStorage APIs for Array Integration (VAAI) enable you to perform copy offload and space reservations. The Plug-In for VMware VAAI uses this to improve host performance because operations do not need to go through the ESXi host, thereby taking advantage of space- and time-efficient cloning in ONTAP.
  - Using VMware VAAI for datastore provisioning is a best practice.
  - The NFS Plug-In for VMware VAAI is available from the NetApp Support site.
- NFS access will be through NFSv3 and NFSv4 for use with VMware VAAI.

For more information, see TR-4597: VMware vSphere for ONTAP and the documentation for your VSC release.

NFS Client Configuration for ESXi workflow

When you make storage available to an ESXi host using NFS, you provision a volume on the using for and then connect to the NFS export from the ESXi host.



Verify that the configuration is supported

For reliable operation, you must verify that the entire configuration is supported. The lists the supported configurations for NFS and for Virtual Storage Console.

Steps

1. Go to the to verify that you have a supported combination of the following components:

   NetApp Interoperability Matrix Tool

   - ONTAP software
   - NFS storage protocol
   - ESXi operating system version

- Guest operating system type and version
- for (VSC) software
- NFS Plug-In for VAAI

2. Click the configuration name for the selected configuration.

   Details for that configuration are displayed in the Configuration Details window.

3. Review the information in the following tabs:
   - Notes

     Lists important alerts and information that are specific to your configuration.

   - Policies and Guidelines

     Provides general guidelines for all NAS configurations.

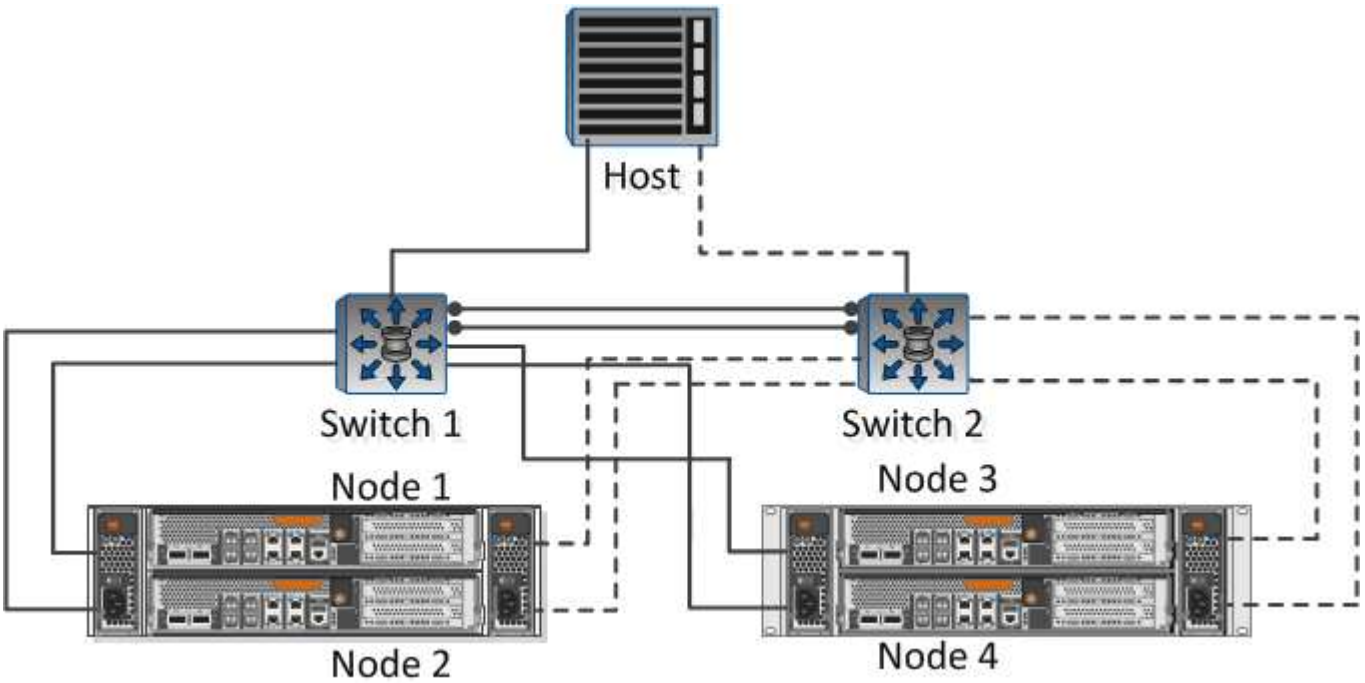
Complete the NFS client configuration worksheet

You require network addresses and storage configuration information to perform NFS client configuration tasks.

Target network addresses

You require a subnet with two IP addresses for NFS data LIFs for each node in the cluster. There should be two separate networks for high availability. The specific IP addresses are assigned by ONTAP when you create the LIFs as part of creating the SVM.

If possible, separate network traffic on separate physical networks or on VLANs.



Subnet for LIFs:

Node or LIF with port to switch	IP address	Network mask	Gateway	VLAN ID	Home port
Node 1 / LIF to switch 1					
Node 2 / LIF to switch 1					
Node 3 / LIF to switch 1					
Node 4 / LIF to switch 1					
Node 1 / LIF to switch 2					
Node 2 / LIF to switch 2					
Node 3 / LIF to switch 2					
Node 4 / LIF to switch 2					

Storage configuration

If the aggregate and are already created, record their names here; otherwise, you can create them as required:

Node to own NFS export
Aggregate name
name

NFS export information

Export size
Export name (optional)
Export description (optional)

SVM information

If you are not using an existing , you require the following information to create a new one:

SVM name	
Aggregate for SVM root volume	
SVM user name (optional)	
SVM password (optional)	
SVM management LIF (optional)	
	Subnet:
	IP address:
	Network mask:
	Gateway:
	Home node:

Install

Virtual Storage Console for automates many of the configuration and provisioning tasks required to use storage with an ESXi host. is a plug-in to vCenter Server.

Before you begin

You must have administrator credentials on the vCenter Server used to manage the ESXi host.

About this task

- Virtual Storage Console is installed as a virtual appliance that includes Virtual Storage Console, vStorage APIs for Storage Awareness (VASA) Provider, and Storage Replication Adapter (SRA) for VMware vSphere capabilities.

Steps

1. Download the version of that is supported for your configuration, as shown in the Interoperability Matrix tool.

   NetApp Support

2. Deploy the virtual appliance and configure it following the steps in *Deployment and Setup Guide*.

Add the storage cluster to VSC

Before you can provision the first datastore to an ESXi host in your Datacenter, you must add the cluster or a specific storage virtual machine (SVM) to Virtual Storage Console for

VMware vSphere. Adding the cluster enables you to provision storage on any SVM in the cluster.

Before you begin

You must have administrator credentials for the storage cluster or the that is being added.

About this task

Depending on your configuration, the cluster might have been discovered automatically, or might have already been added.

Steps

1. Log in to the vSphere Web Client.
2. Select **Virtual Storage Console**.
3. Select **Storage Systems** and then click the **Add** icon.
4. In the **Add Storage System** dialog box, enter the host name and administrator credentials for the storage cluster or and then click **OK**.

Configure your network for best performance

Ethernet networks vary greatly in performance. You can maximize the performance of the network by selecting specific configuration values.

Steps

1. Connect the host and storage ports to the same network.

   It is best to connect to the same switches.

2. Select the highest speed ports available.

   10 GbE or faster ports are best. 1 GbE ports are the minimum.

3. Enable jumbo frames if desired and supported by your network.

   Jumbo frames should have an MTU of 9000 for ESXi hosts and storage systems, and 9216 for most switches. All network devices in the data path — including ESXi NICs, storage NICs, and switches — must support jumbo frames and should be configured for their maximum MTU values.

   For more information, see Check the network settings on the data switches and the switch vendor documentation.

Configure the ESXi host

Configuring the ESXi host involves configuring ports and vSwitches, and using ESXi host best practice settings. After verifying that these settings are correct, you can then create an aggregate and decide where to provision the new volume.

Configure host ports and vSwitches

The ESXi host requires network ports for the NFS connections to the storage cluster.

About this task

It is recommended that you use IP Hash as the NIC teaming policy, which requires a single VMkernel port on a single vSwitch.

The host ports and storage cluster ports used for NFS must have IP addresses in the same subnet.

This task lists the high-level steps for configuring the ESXi host. If you require more detailed instructions, see the VMware publication *Storage* for your version of ESXi.

VMware

Steps

1. Log in to the vSphere Client, and then select the ESXi host from the inventory pane.
2. On the **Manage** tab, click **Networking**.
3. Click **Add Networking**, and then select **VMkernel** and **Create a vSphere standard switch** to create the VMkernel port and vSwitch.
4. Configure jumbo frames for the vSwitch (MTU size of 9000, if used).

Configure the ESXi host best practice settings

You must ensure that the ESXi host best practice settings are correct so that the ESXi host can correctly manage the loss of an NFS connection or a storage.

Steps

1. From the VMware vSphere Web Client **Home** page, click **vCenter** > **Hosts**.
2. Right-click the host, and then select **Actions** > **NetApp VSC** > **Set Recommended Values**.
3. In the **NetApp Recommended Settings** dialog box, ensure that all of the options are selected, and then click **OK**.

   MPIO Settings do not apply to NFS. However, if you use other protocols, you should ensure that all options are selected.

   The vCenter Web Client displays the task progress.

Create an aggregate

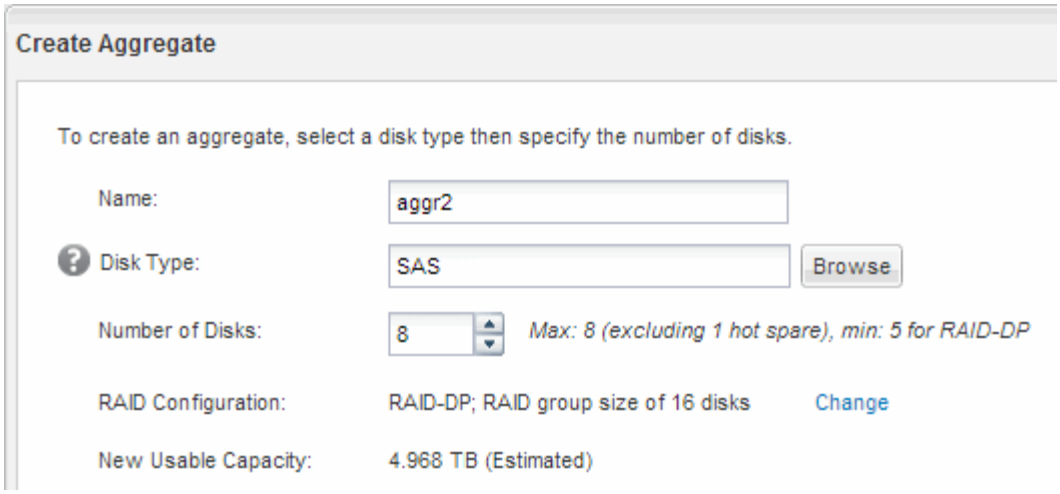
If you do not want to use an existing aggregate, you can create a new aggregate to provide physical storage to the volume which you are provisioning.

About this task

If you have an existing aggregate that you want to use for the new volume, you can skip this procedure.

Steps

1. Enter the URL `https://IP-address-of-cluster-management-LIF` in a web browser and log in to using your cluster administrator credential.
2. Navigate to the **Aggregates** window.
3. Click **Create.**
4. Follow the instructions on the screen to create the aggregate using the default RAID-DP configuration, and then click **Create**.



Results

The aggregate is created with the specified configuration and added to the list of aggregates in the Aggregates window.

Decide where to provision the new volume

Before you create an NFS volume, you must decide whether to place it in an existing and, if so, how much configuration the requires. This decision determines your workflow.

Procedure

- If you want a new , follow the steps that you do for creating an NFS-enabled on an existing SVM.

  Creating a new NFS-enabled SVM

  You must choose this option if NFS is not enabled on an existing SVM.

- If you want to provision a volume on an existing that has NFS enabled but not configured, follow the steps that you do for configuring NFS access to an existing SVM.

  Configuring NFS access to an existing SVM

  This is the case if you followed this procedure to create the SVM.

- If you want to provision a volume on an existing that is fully configured for NFS access, follow the steps that you do for verifying settings on an existing SVM.

  Verifying settings on an existing SVM

Create a new NFS-enabled SVM

Setting up a new SVM involves creating the new and enabling NFS. You can then configure NFS access on the ESXi host and verify that NFS is enabled for ESXi by using Virtual Storage Console.

Before you begin

- Your network must be configured and the relevant physical ports must be connected to the network.

- You must know which of the following networking components the will use:
  - The node and the specific port on that node where the data logical interface (LIF) will be created
  - The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
- Any external firewalls must be appropriately configured to allow access to network services.

About this task

You can use a wizard that guides you through the process of creating the SVM, configuring DNS, creating a data LIF, and enabling NFS.

Steps

1. Navigate to the **SVMs** window.
2. Click **Create**.
3. In the **Storage Virtual Machine (SVM) Setup** window, create the SVM:

   a. Specify a unique name for the SVM.

      The name must either be a fully qualified domain name (FQDN) or follow another convention that ensures unique names across a cluster.

   b. Select **NFS** for the data protocol.

      If you plan to use additional protocols on the same SVM, you should select them even if you do not want to configure them immediately.

   c. Keep the default language setting, C.UTF-8.

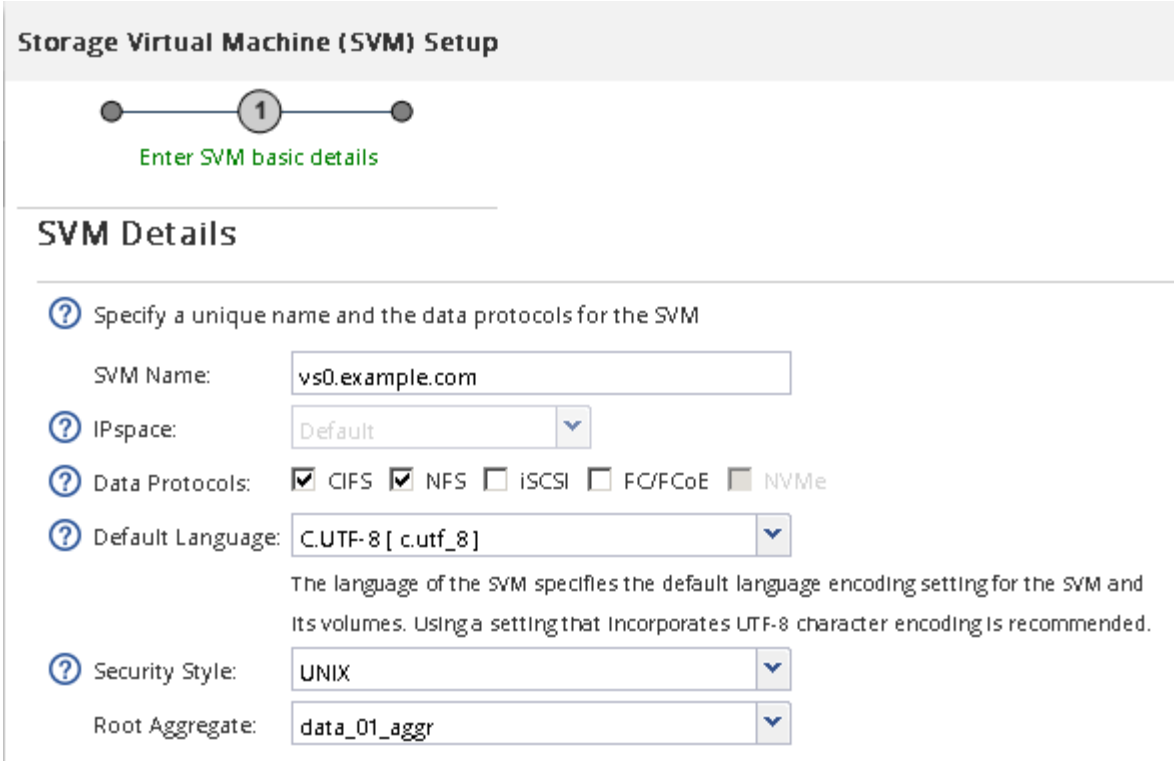
      This language is inherited by the volume that you create later, and a volume's language cannot be changed.

   d. **Optional**: If you enabled the CIFS protocol, change the security style to **UNIX**.

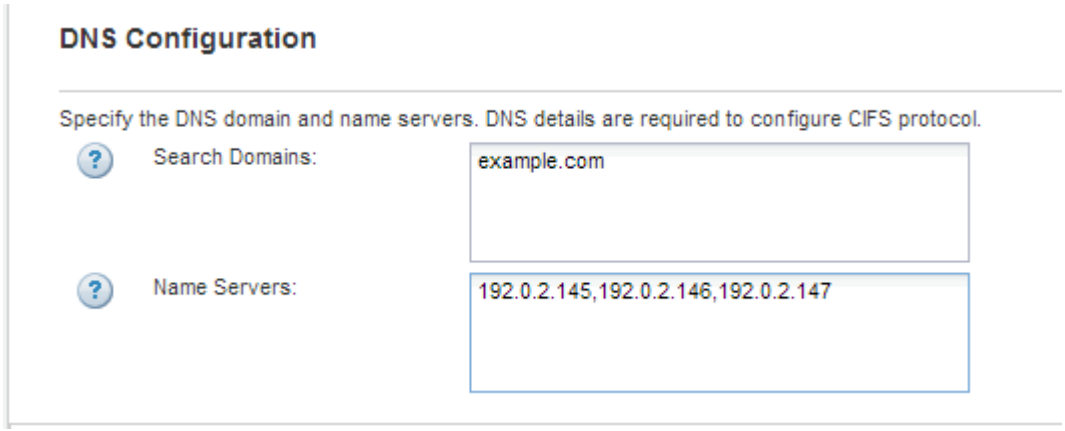
      Selecting the CIFS protocol sets the security style to NTFS by default.

   e. **Optional**: Select the root aggregate to contain the root volume.

      The aggregate that you select for the root volume does not determine the location of the data volume.



f. **Optional**: In the **DNS Configuration** area, ensure that the default DNS search domain and name servers are the ones that you want to use for this SVM.



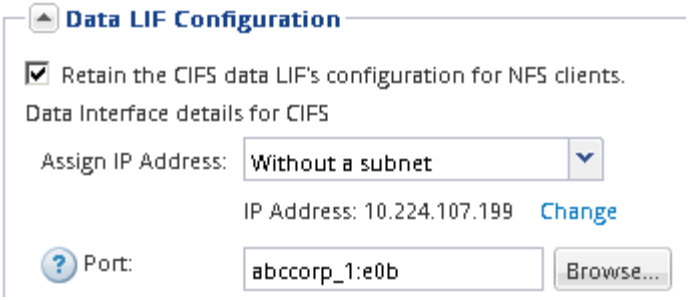
g. Click **Submit & Continue**.

The is created, but protocols are not yet configured.

4. In the **Data LIF Configuration** section of the **Configure CIFS/NFS protocol** page, specify the details of the first data LIF of the first datastore.

   a. Assign an IP address to the LIF automatically from a subnet you specify or manually enter the address.

   b. Click **Browse** and select a node and port that will be associated with the LIF.



Do not enter any information to provision a volume. You can provision datastores later using

5. Click **Submit & Continue**.

   The following objects are created:

   - A data LIF named after the with the suffix "_nfs_lif1"
   - An NFS server

6. For all other protocol configuration pages that are displayed, click **Skip**, and then configure the protocol later.
7. When the **SVM Administration** page is displayed, configure or defer configuring a separate administrator for this SVM:
   - Click **Skip**, and then configure an administrator later if required.
   - Enter the requested information, and then click **Submit & Continue**.
8. Review the **Summary** page, record any information that you might require later, and then click **OK**.

   NFS clients need to know the IP address of the data LIF.

Results

A new SVM is created with NFS enabled.

Add NFS access to an existing SVM

To add NFS access to an existing SVM, you must first create a data logical interface (LIF). You can then configure NFS access on the ESXi host and verify that NFS is enabled for ESXi using Virtual Storage Console.

Before you begin

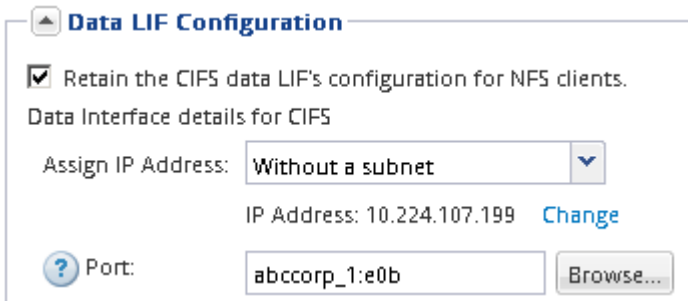
- You must know which of the following networking components the will use:
  - The node and the specific port on that node where the data LIF will be created
  - The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
- Any external firewalls must be appropriately configured to allow access to network services.
- The NFS protocol must be allowed on the SVM.

  This is the case if you did not follow this procedure to create the SVM while configuring a different protocol.

Steps

1. Navigate to the **Details** pane where you can configure the protocols of the SVM:
   a. Select the SVM that you want to configure.
   b. In the **Details** pane, next to **Protocols**, click **NFS**.

2. In the **Configure NFS protocol** dialog box, create a data LIF:
   a. Assign an IP address to the LIF automatically from a subnet you specify or manually enter the address.
   b. Click **Browse** and select a node and port that will be associated with the LIF.



   Do not enter any information to provision a volume. You can provision datastores later using the Virtual Storage Console.

3. Click **Submit & Close**, and then click **OK**.

Verify that NFS is enabled on an existing SVM

If you choose to use an existing SVM, you must first verify that NFS is enabled on the SVM. You can then configure NFS access and verify that NFS is enabled for ESXi by using ESXi by using Virtual Storage Console.

Steps

1. Navigate to the **SVMs** window.
2. Click the **SVM Settings** tab.
3. In the **Protocols** pane, click **NFS**.
4. Verify that NFS is displayed as enabled.

   If NFS is not enabled, you must enable it or create a new SVM.

Provision a datastore and create its containing volume

A datastore contains virtual machines and their VMDKs on the ESXi host. The datastore on the ESXi host is provisioned on a volume on the storage cluster.

Before you begin

Virtual Storage Console for VMware vSphere for (VSC) must be installed and registered with the vCenter Server that manages the ESXi host.

VSC must have sufficient cluster or credentials to create the volume on the specified SVM.

About this task

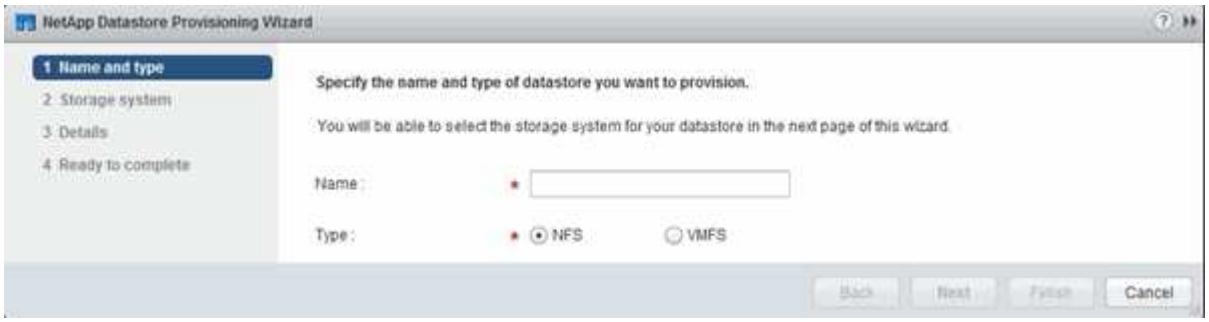
VSC automates the datastore provisioning, including creating a volume on the specified SVM.

Steps

1. From the vSphere Web Client **Home** page, click **Hosts and Clusters**.
2. In the navigation pane, expand the datacenter where you want to provision the datastore.
3. Right-click the ESXi host, and then select **NetApp VSC** > **Provision Datastore**.

   Alternatively, you can right-click the cluster when provisioning to make the datastore available to all hosts in the cluster.

4. Provide the required information in the wizard:



Verify NFS access from an ESXi host

After you have provisioned a datastore, you can verify that the ESXi host has NFS access by creating a virtual machine on the datastore and powering it on.

Steps

1. From the vSphere Web Client **Home** page, click **Hosts and Clusters**.
2. In the navigation pane, expand the datacenter to locate the datastore you previously created.
3. Click **Create a new virtual machine** and provide the required information in the wizard.

   To verify NFS access, you should select the datacenter, ESXi host, and datastore that you previously created.

   The virtual machine appears in the vSphere Web Client inventory.

4. Power on the virtual machine.

Deploy the NFS Plug-in for VMware VAAI

The plug-in is a software library that integrates the VMware Virtual Disk Libraries that are installed on the ESXi host. Downloading and installing the NFS Plug-In for VMware VAAI enables you to improve the performance of cloning operations by using the copy offload and space reservation options.

About this task

To provide consistent access to the virtual machines residing on the ESXi host on which you are installing the NFS plug-in, you can migrate virtual machines or install the NFS plug-in during planned maintenance.

Steps

1. Download the NFS Plug-In for VMware VAAI.

   NetApp Support

   You should download the online bundle (`NetAppNasPlugIn.vib`) of the most recent plug-in

2. Verify that VAAI is enabled on each ESXi host.

   In VMware vSphere 5.0 and later, VAAI is enabled by default.

3. In Virtual Storage Console, go to **Tools** > **NFS VAAI Tools**.
4. Click **Select File** to upload the `NetAppNasPlugIn.vib` file.
5. Click **Upload**.

   You see an `uploaded successfully` message.

6. Click **Install on host**.
7. Select the ESXi hosts on which you want to install the plug-in, click **Install**, and then click **OK**.
8. Reboot the ESXi host to enable the plug-in.

   After installing the plug-in, you must reboot the ESXi host before installation is complete.

   You do not need to reboot the storage system.

Mount datastores on hosts

Mounting a datastore gives a host access to storage. When datastores are provisioned by , they are automatically mounted to the host or cluster. You might need to mount a datastore on a host after you add the host to your VMware environment.

Steps

1. From the vSphere Web Client **Home** page, click **Hosts and Clusters**:
2. In the navigation pane, expand the datacenter that contains the host:
3. Right-click the host, and then select **NetApp VSC** > **Mount Datastores**.
4. Select the datastores that you want to mount, and then click **OK**.

Related information

Virtual Storage Console, VASA Provider, and Storage Replication Adapter for VMware vSphere Administration for 9.6 release

SMB/CIFS and NFS multiprotocol configuration

SMB and NFS multiprotocol configuration overview

Using the ONTAP System Manager classic interface (ONTAP 9.7 and earlier), you can quickly set up both SMB and NFS access to a new volume on either a new or existing

storage virtual machine (SVM).

Use this procedure if you want to configure access to a volume in the following way:

- NFS access will be through NFSv3, not NFSv4 or NFSv4.1.
- You want to use best practices, not explore every available option.
- Your data network uses the default IPspace, the default broadcast domain, and the default failover group.

  If your data network is flat, using these default objects ensures that LIFs will fail over correctly in the event of a link failure. If you are not using the default objects, you should refer to Network Management for information on how to configure LIF path failover.

- LDAP, if used, is provided by Active Directory.

If you want details about the range of ONTAP NFS and SMB protocol capabilities, see the following documentation:

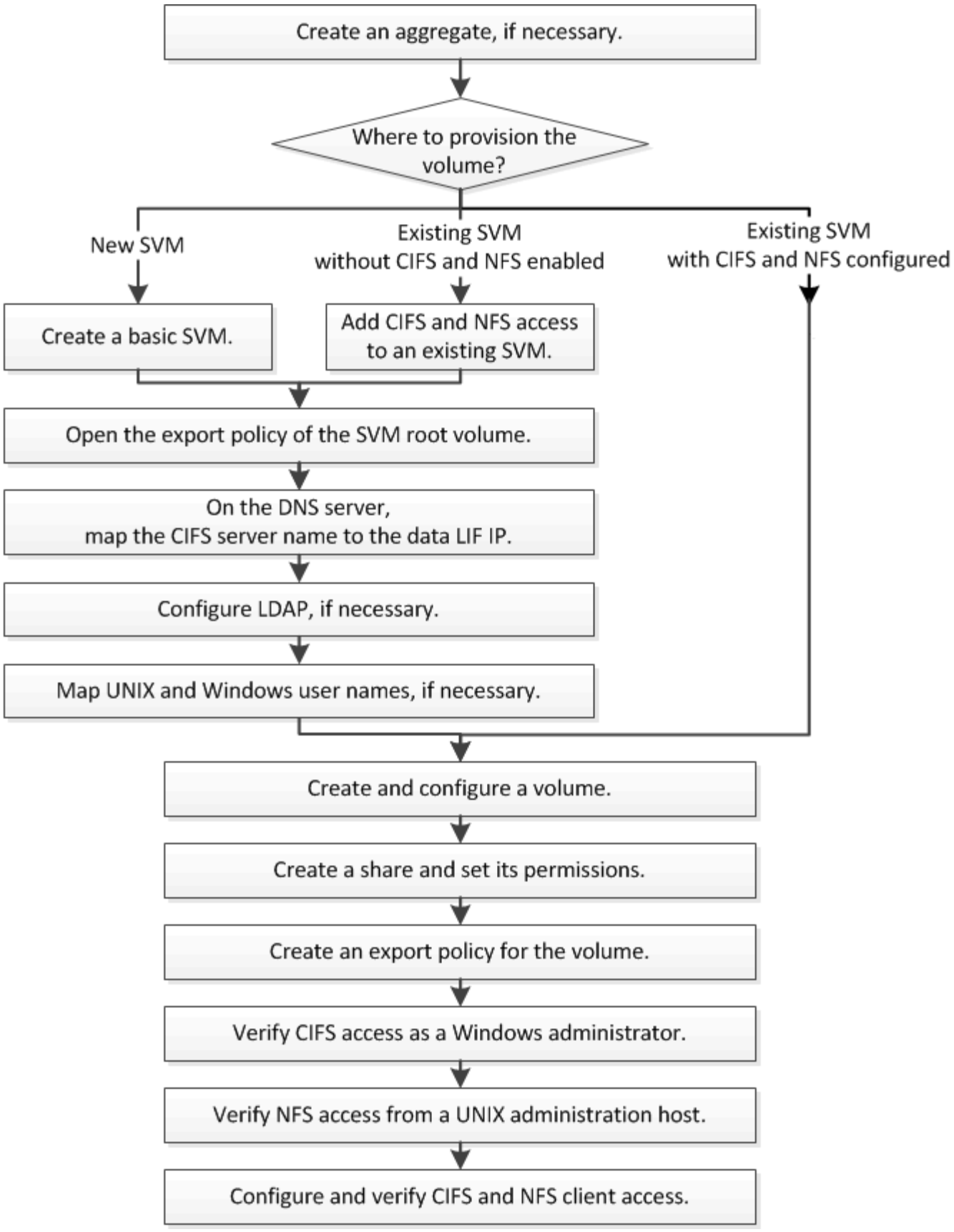
- NFS management
- SMB management

Other ways to do this in ONTAP

To perform these tasks with…	Refer to…
The redesigned System Manager (available with ONTAP 9.7 and later)	Provision NAS storage for both Windows and Linux using both NFS and SMB
The ONTAP command line interface	SMB configuration overview with the CLI NFS configuration overview with the CLI What the security styles and their effects are Case-sensitivity of file and directory names in a multiprotocol environment

Multiprotocol configuration workflow

Configuring both SMB/CIFS and NFS involves optionally creating an aggregate; optionally creating a new SVM or configuring an existing one; creating a volume, share, and export; and verifying access from UNIX and Windows administration hosts. You can then open access to SMB/CIFS and NFS clients.



Create an aggregate

If you do not want to use an existing aggregate, you can create a new aggregate to

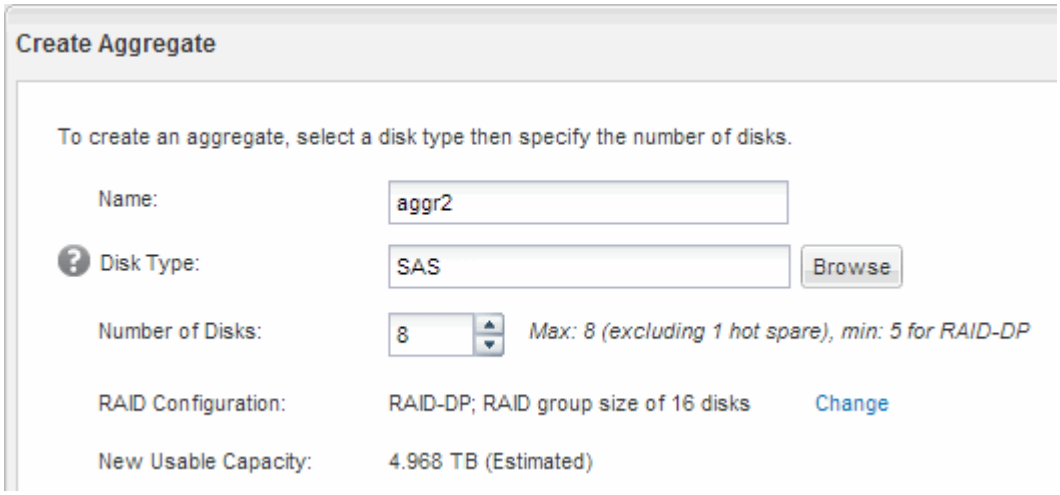
provide physical storage to the volume which you are provisioning.

About this task

If you have an existing aggregate that you want to use for the new volume, you can skip this procedure.

Steps

1. Enter the URL `https://IP-address-of-cluster-management-LIF` in a web browser and log in to System Manager using your cluster administrator credential.
2. Navigate to the **Aggregates** window.
3. Click **Create.**
4. Follow the instructions on the screen to create the aggregate using the default RAID-DP configuration, and then click **Create**.



Results

The aggregate is created with the specified configuration and added to the list of aggregates in the Aggregates window.

Decide where to provision the new volume

Before you create a new multiprotocol volume, you must decide whether to place the volume in an existing storage virtual machine (SVM), and, if so, how much configuration the SVM requires. This decision determines your workflow.

Procedure

- If you want to provision a volume on a new SVM, create a basic SVM.

  Creating a basic SVM

  You must choose this option if CIFS and NFS are not already enabled on an existing SVM.

- If you want to provision a volume on an existing SVM that has both CIFS and NFS enabled but not configured, add CIFS and NFS access on the existing SVM.

  Adding CIFS and NFS access on an existing SVM

- If you want to provision a volume on an existing SVM that is fully configured for CIFS and NFS multiprotocol access, you can directly create and configure the volume.

  Creating and configuring a volume

Create a basic SVM

You can use a wizard that guides you through the process of creating a new storage virtual machine (SVM), configuring Domain Name System (DNS), creating a data logical interface (LIF), configuring a CIFS server, enabling NFS, and optionally configuring NIS.

Before you begin

- Your network must be configured and the relevant physical ports must be connected to the network.
- You must know which of the following networking components the SVM will use:
  - The node and the specific port on that node where the data logical interface (LIF) will be created
  - The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
  - Active Directory (AD) domain that this SVM will join, along with the credentials required to add the SVM to it
  - NIS information, if your site uses NIS for name services or name mapping
- The subnet must be routable to all external servers required for services such as Network Information Service (NIS), Lightweight Directory Access Protocol (LDAP), Active Directory (AD), and DNS.
- Any external firewalls must be appropriately configured to allow access to network services.
- The time on the AD domain controllers, clients, and SVM must be synchronized to within five minutes of each other.

About this task

When you are creating an SVM for multiprotocol access, you should not use the provisioning sections of the Storage Virtual Machine (SVM) Setup window, which creates two volumes—not a single volume with multiprotocol access. You can provision the volume later in the workflow.

Steps

1. Navigate to the **SVMs** window.
2. Click **Create.**
3. In the **Storage Virtual Machine (SVM) Setup** dialog box, create the SVM:

   a. Specify a unique name for the SVM.

      The name must either be a fully qualified domain name (FQDN) or follow another convention that ensures unique names across a cluster.

   b. Select all the protocols that you have licenses for and that you will eventually use on the SVM, even if you do not want to configure all the protocols immediately.

   c. Keep the default language setting, C.UTF-8.

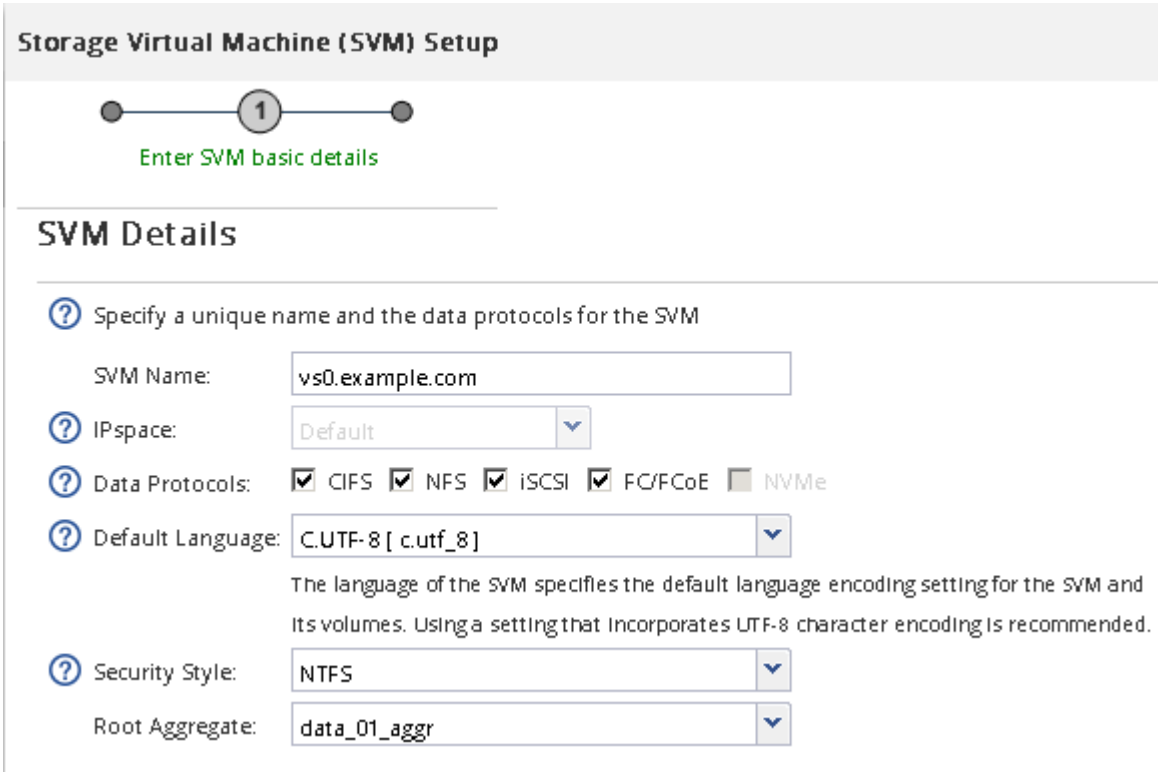
If you support international character display in both NFS and SMB/CIFS clients, consider using the **UTF8MB4** language code, which is available beginning with ONTAP 9.5.

d. **Optional**: Make sure that the security style is set to your preference.

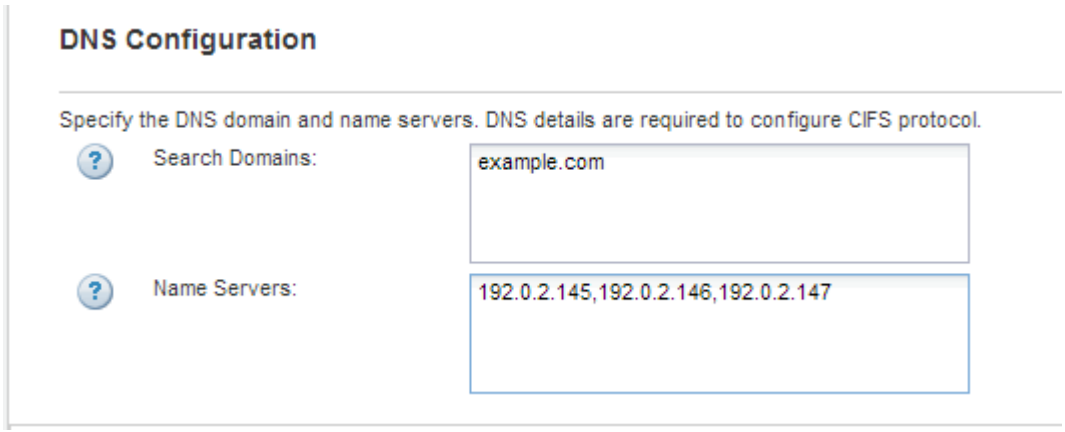
   Selecting the CIFS protocol sets the security style to NTFS by default.

e. **Optional**: Select the root aggregate to contain the SVM root volume.

   The aggregate that you select for the root volume does not determine the location of the data volume. The aggregate for the data volume is selected separately in a later step.



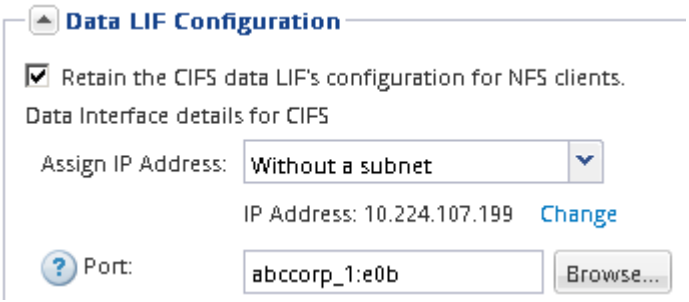
f. **Optional**: In the **DNS Configuration** area, ensure that the default DNS search domain and name servers are the ones that you want to use for this SVM.



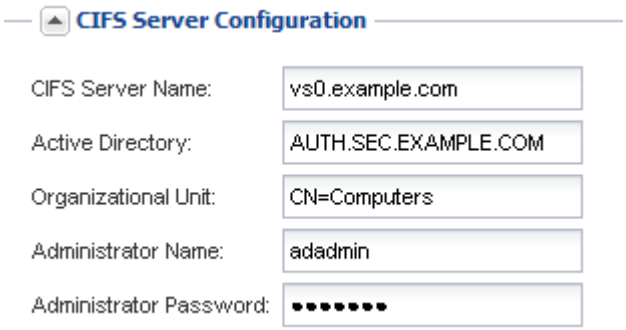
g. Click **Submit & Continue**.

The SVM is created, but protocols are not yet configured.

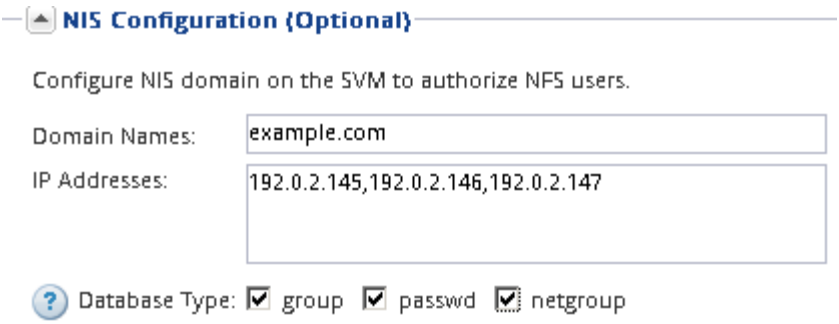
4. In the **Data LIF Configuration** section of the **Configure CIFS/NFS protocol** page, specify the details of the LIF that clients will use to access data:
   a. Assign an IP address to the LIF automatically from a subnet you specify or manually enter the address.
   b. Click **Browse** and select a node and port that will be associated with the LIF.



5. In the **CIFS Server Configuration** section, define the CIFS server and configure it to access the AD domain:
   a. Specify a name for the CIFS server that is unique in the AD domain.
   b. Specify the FQDN of the AD domain that the CIFS server can join.
   c. If you want to associate an organizational unit (OU) within the AD domain other than CN=Computers, enter the OU.
   d. Specify the name and password of an administrative account that has sufficient privileges to add the CIFS server to the OU.
   e. If you want to avoid unauthorized access to all the shares on this SVM, select the option to encrypt data using SMB 3.0.



6. Skip the **Provision a volume for CIFS Storage** area because it provisions a volume for only CIFS access—not for multiprotocol access.
7. If the **NIS Configuration** area is collapsed, expand it.
8. If your site uses NIS for name services or name mapping, specify the domain and IP addresses of the NIS servers.



9. Skip the **Provision a volume for NFS Storage** area because it provisions a volume for NFS access only—not for multiprotocol access.
10. Click **Submit & Continue**.

    The following objects are created:

    - A data LIF named after the SVM with the suffix "_cifs_nfs_lif1"
    - A CIFS server that is part of the AD domain
    - An NFS server
11. For all other protocol configuration pages that are displayed, click **Skip** and configure the protocol later.
12. When the **SVM Administration** page is displayed, configure or defer configuring a separate administrator for this SVM:
    - Click **Skip** and configure an administrator later if required.
    - Enter the requested information and then click **Submit & Continue**.
13. Review the **Summary** page, record any information you might require later and then click **OK**.

    The DNS administrator needs to know the CIFS server name and the IP address of the data LIF. Windows clients need to know the name of the CIFS server. NFS clients need to know the IP address of the data LIF.

Results

A new SVM is created that has a CIFS server and an NFS server accessible through the same data LIF.

What to do next

You must now open the export policy of the SVM root volume.

Related information

Opening the export policy of the SVM root volume (Creating a new NFS-enabled SVM)

Add CIFS and NFS access to an existing SVM

Adding both CIFS/SMB and NFS access to an existing SVM involves creating a data LIF, configuring a CIFS server, enabling NFS, and optionally configuring NIS.

Before you begin

- You must know which of the following networking components the SVM will use:
  - The node and the specific port on that node where the data logical interface (LIF) will be created

- The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
- The Active Directory (AD) domain that this SVM will join, along with the credentials required to add the SVM to it
- NIS information if your site uses NIS for name services or name mapping

- Any external firewalls must be appropriately configured to allow access to network services.
- The time on the AD domain controllers, clients, and SVM must be synchronized within five minutes of each other.
- The CIFS and NFS protocols must be allowed on the SVM.

  This is the case if you did not follow this procedure to create the SVM while configuring a different protocol.

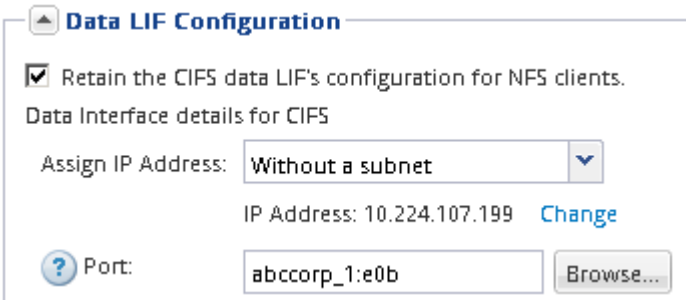
About this task

The order in which you configure CIFS and NFS affects the dialog boxes that are displayed. In this procedure, you must configure CIFS first and NFS second.

Steps

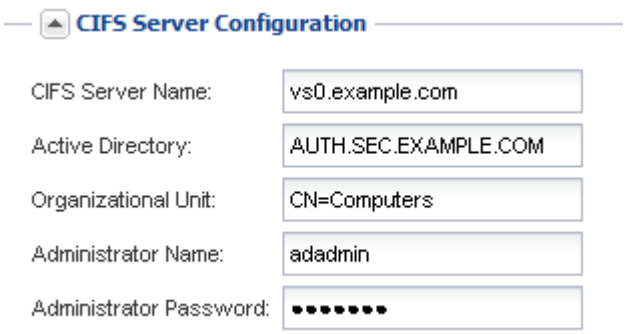
1. Navigate to the area where you can configure the protocols of the SVM:
   a. Select the SVM that you want to configure.
   b. In the **Details** pane, next to **Protocols**, click **CIFS**.

2. In the **Data LIF Configuration** section of the **Configure CIFS protocol** dialog box, create a data LIF for the SVM:
   a. Assign an IP address to the LIF automatically from a subnet you specify or manually enter the address.
   b. Click **Browse** and select a node and port that will be associated with the LIF.



3. In the **CIFS Server Configuration** section, define the CIFS server and configure it to access the AD domain:
   a. Specify a name for the CIFS server that is unique in the AD domain.
   b. Specify the FQDN of the AD domain that the CIFS server can join.
   c. If you want to associate an organizational unit (OU) within the AD domain other than CN=Computers, enter the OU.
   d. Specify the name and password of an administrative account that has sufficient privileges to add the CIFS server to the OU.
   e. If you want to avoid unauthorized access to all the shares on this SVM, select the option to encrypt

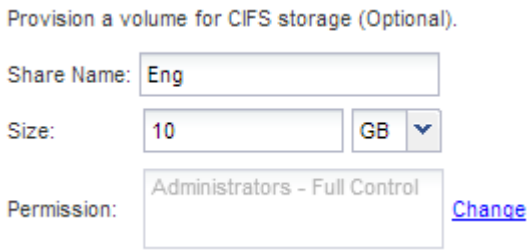
data using SMB 3.0.



4. Create a volume for CIFS/SMB access and provision a share on it:
   a. Name the share that CIFS/SMB clients will use to access the volume.

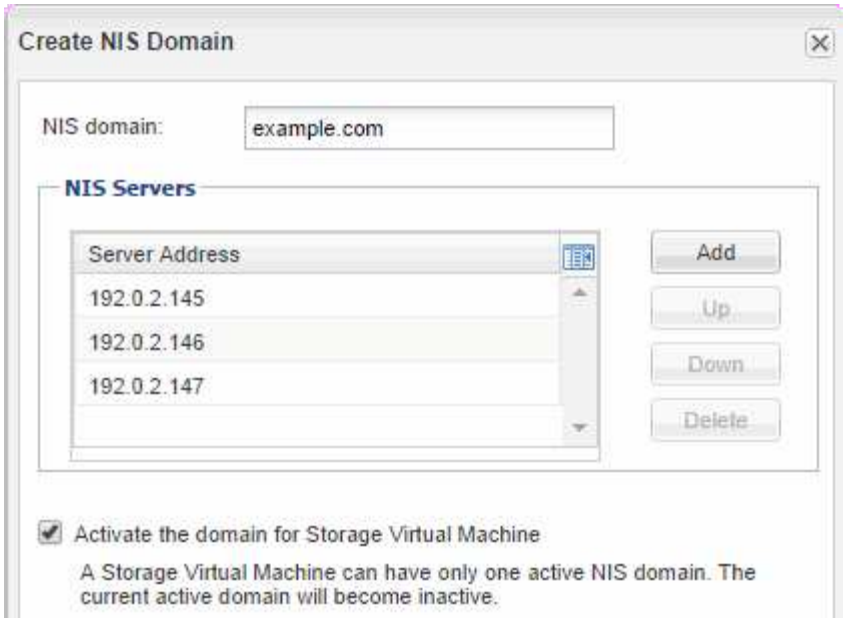
      The name you enter for the share will also be used as the volume name.

   b. Specify a size for the volume.



   You do not have to specify the aggregate for the volume because it is automatically located on the aggregate with the most available space.

5. Skip the **Provision a volume for CIFS Storage** area, because it provisions a volume for only CIFS access—not for multiprotocol access.
6. Click **Submit & Close**, and then click **OK**.
7. Enable NFS:
   a. From the SVMs tab, select the SVM for which you want to enable NFS and click **Manage**.
   b. In the **Protocols** pane, click **NFS** and then click **Enable**.
8. If your site uses NIS for name services or name mapping, configure NIS:
   a. In the **Services** window, click **NIS**.
   b. In the **NIS** window, click **Create**.
   c. Specify the domain of the NIS servers.
   d. Add the IP addresses of the NIS servers.
   e. Select **Activate the domain for Storage Virtual Machine**, and then click **Create**.



What to do next

Open the export policy of the SVM root volume.

Open the export policy of the SVM root volume (Create a new NFS-enabled SVM)

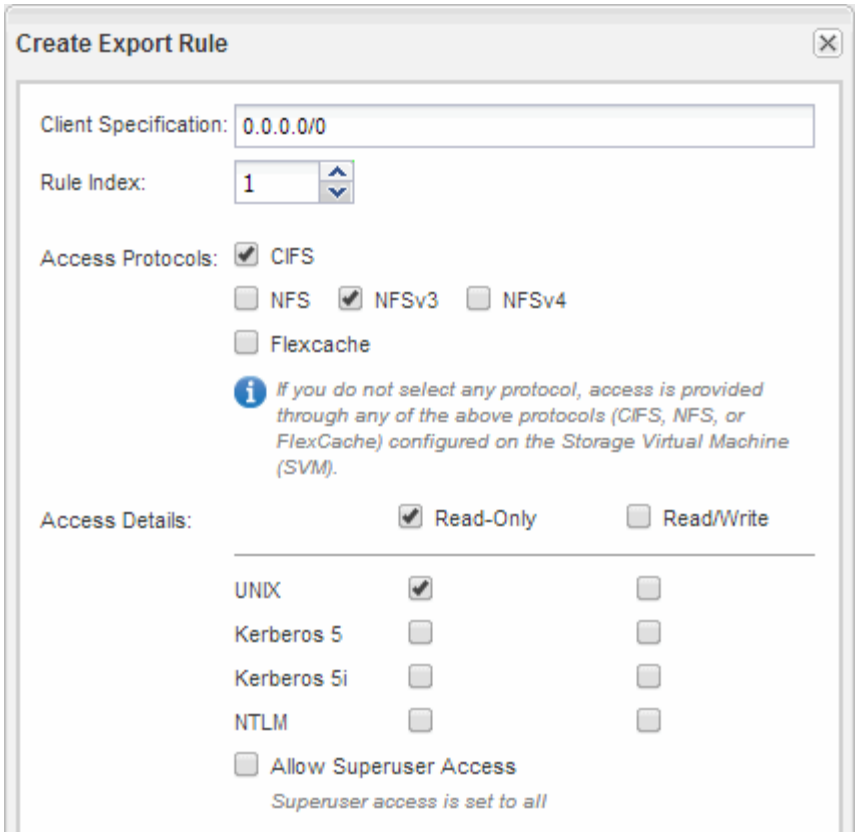
You must add a rule to the default export policy to allow all clients access through NFSv3. Without such a rule, all NFS clients are denied access to the storage virtual machine (SVM) and its volumes.

About this task

You should specify all NFS access as the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes.

Steps

1. Navigate to the **SVMs** window.
2. Click the **SVM Settings** tab.
3. In the **Policies** pane, click **Export Policies**.
4. Select the export policy named **default**, which is applied to the SVM root volume.
5. In the lower pane, click **Add**.
6. In the **Create Export Rule** dialog box, create a rule that opens access to all clients for NFS clients:
   a. In the **Client Specification** field, enter `0.0.0.0/0` so that the rule applies to all clients.
   b. Retain the default value as **1** for the rule index.
   c. Select **NFSv3**.
   d. Clear all the check boxes except the **UNIX** check box under **Read-Only**.
   e. Click **OK**.



Results

NFSv3 clients can now access any volumes created on the SVM.

Map the SMB server on the DNS server

Your site's DNS server must have an entry pointing the SMB server name, and any NetBIOS aliases, to the IP address of the data LIF so that Windows users can map a drive to the SMB server name.

Before you begin

You must have administrative access to your site's DNS server. If you do not have administrative access, you must ask the DNS administrator to perform this task.

About this task

If you use NetBIOS aliases for the SMB server name, it is a best practice to create DNS server entry points for each alias.

Steps

1. Log in to the DNS server.
2. 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 LIF.
3. 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 LIF.

Results

After the mapping is propagated across the network, Windows users can map a drive to the SMB server name

or its NetBIOS aliases.

Configure LDAP (Create a new NFS-enabled SVM)

If you want the storage virtual machine (SVM) to get user information from Active Directory-based Lightweight Directory Access Protocol (LDAP), you must create an LDAP client, enable it for the SVM, and give LDAP priority over other sources of user information.

Before you begin

- The LDAP configuration must be using Active Directory (AD).

  If you use another type of LDAP, you must use the command-line interface (CLI) and other documentation to configure LDAP.

  NetApp Technical Report 4067: NFS in NetApp ONTAP

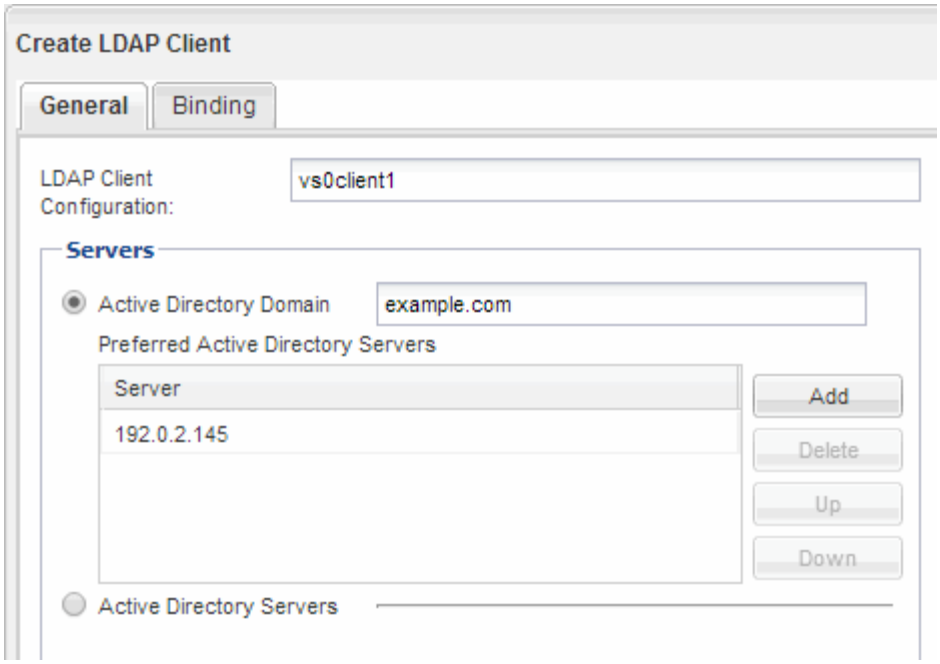
  NetApp Technical Report 4616: NFS Kerberos in ONTAP with Microsoft Active Directory

  NetApp Technical Report 4835: How to Configure LDAP in ONTAP

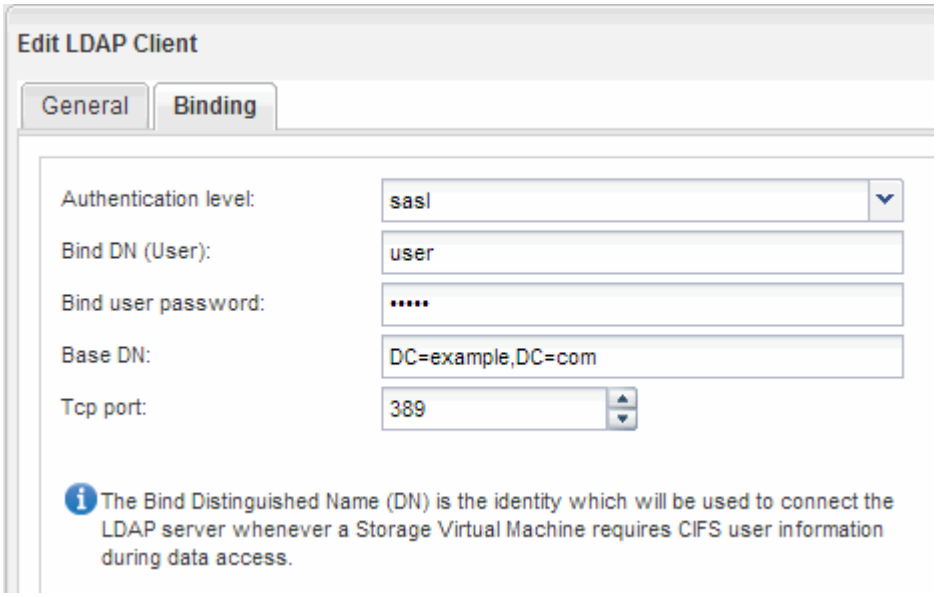
- You must know the AD domain and servers, as well as the following binding information: the authentication level, the Bind user and password, the base DN, and the LDAP port.

Steps

1. Navigate to the **SVMs** window.
2. Select the required SVM
3. Click the **SVM Settings** tab.
4. Set up an LDAP client for the SVM to use:
   a. In the **Services** pane, click **LDAP Client**.
   b. In the **LDAP Client Configuration** window, click **Add**.
   c. In the **General** tab of the **Create LDAP Client** window, type the name of the LDAP client configuration, such as `vs0client1`.
   d. Add either the AD domain or the AD servers.



e. Click **Binding**, and specify the authentication level, the Bind user and password, the base DN, and the port.



f. Click **Save and Close**.

A new client is created and available for the SVM to use.

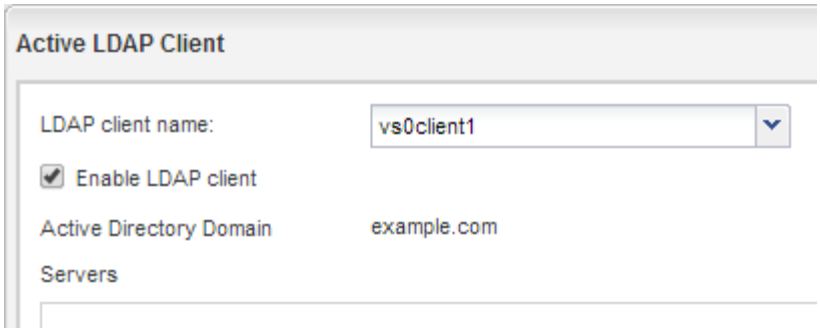
5. Enable the new LDAP client for the SVM:

   a. In the navigation pane, click **LDAP Configuration**.

   b. Click **Edit**.

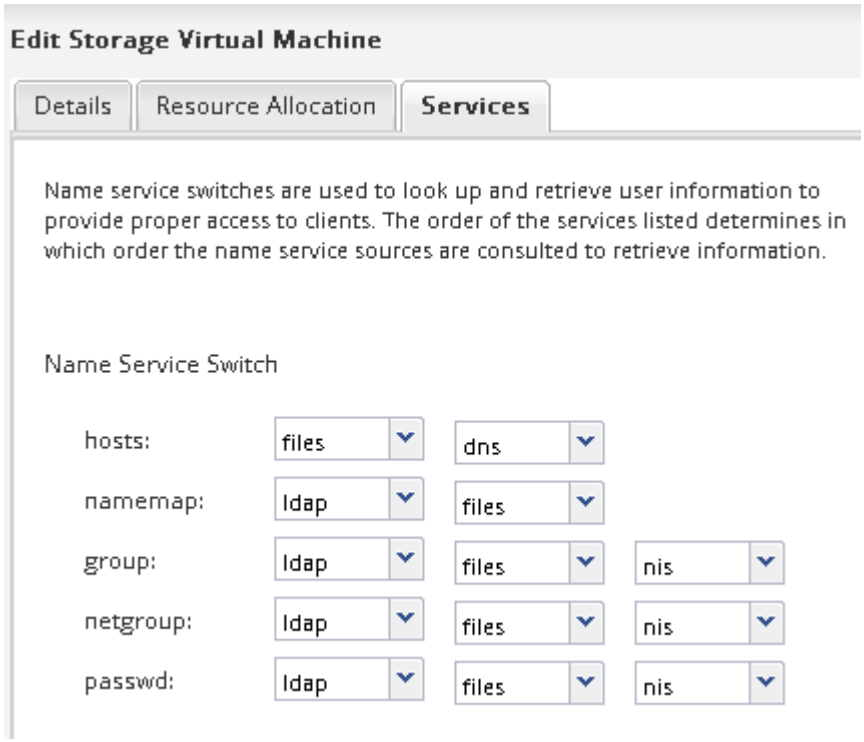
   c. Ensure that the client you just created is selected in **LDAP client name**.

   d. Select **Enable LDAP client**, and click **OK**.



The SVM uses the new LDAP client.

6. Give LDAP priority over other sources of user information, such as Network Information Service (NIS) and local users and groups:
   a. Navigate to the **SVMs** window.
   b. Select the SVM and click **Edit**.
   c. Click the **Services** tab.
   d. Under **Name Service Switch**, specify **LDAP** as the preferred name service switch source for the database types.
   e. Click **Save and Close**.



LDAP is the primary source of user information for name services and name mapping on this SVM.

Map UNIX and Windows user names

If your site has both Windows and UNIX user accounts, you should use name mapping to ensure that Windows users can access files with UNIX file permissions and to ensure that UNIX users can access files with NTFS file permissions. Name mapping can involve any

combination of implicit mapping, conversion rules, and default users.

About this task

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 can be done using NIS, LDAP, or local users. If you have two sets of users that do not match, you should configure name mapping.

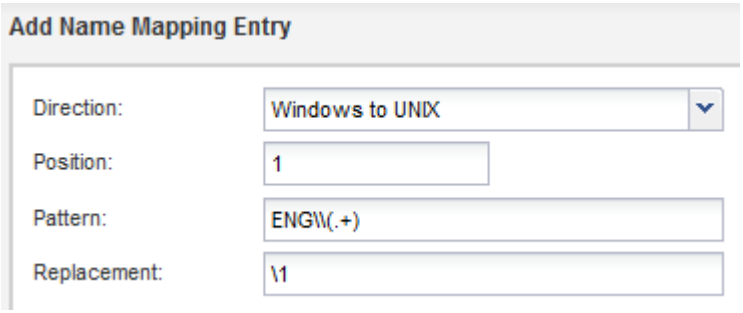
Steps

1. Decide on a method of name mapping—name mapping conversion rules, default user mappings, or both—by considering the following factors:
   - Conversion rules use regular expressions to convert one user name to another, which is useful if you want to control or track access at an individual level.

     For example, you can map UNIX users to Windows users in a domain, and vice versa.
   - Default users enable you to assign a user name to all users who are not mapped by implicit mappings or name mapping conversion rules.

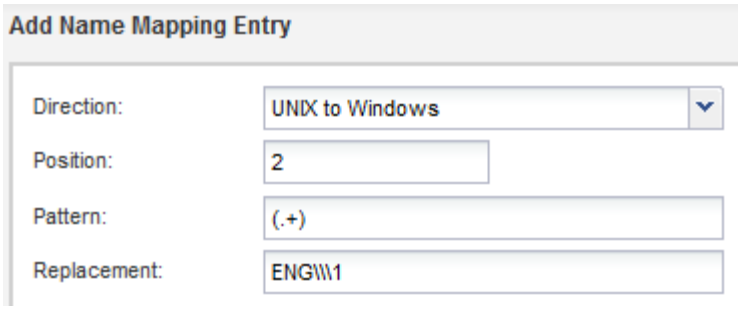
     Each SVM has a default UNIX user named “pcuser” but does not have a default Windows user.
2. Navigate to the **SVMs** window.
3. Select the SVM that you want to configure.
4. Click the **SVM Settings** tab.
5. **Optional**: Create a name mapping that converts UNIX user accounts to Windows user accounts, and vice versa:
   a. In the **Host Users and Groups** pane, click **Name Mapping**.
   b. Click **Add**, retain the default **Windows to UNIX** direction, and then create a regular expression that produces a UNIX credential when a Windows user tries to access a file that uses UNIX file permissions.

      Use the following entry to convert any Windows user in the ENG domain into a UNIX user of the same name. The pattern `ENG\\(.+)` finds any Windows user name with the prefix `ENG\\`, and the replacement `\1` creates the UNIX version by removing everything except the user name.

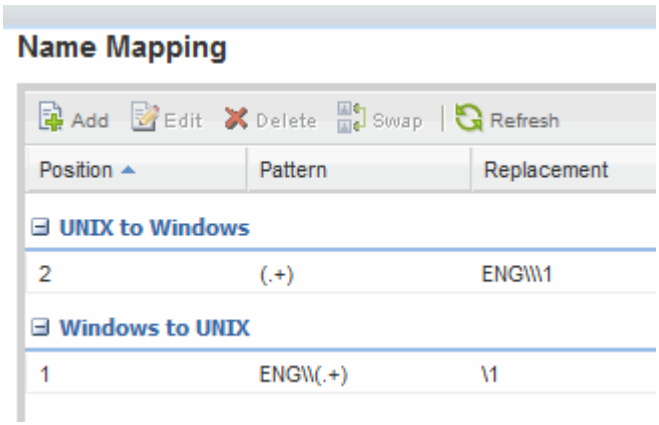
      

   c. Click**Add**, select the **UNIX to Windows** direction, and then create the corresponding mapping that produces a Windows credential when a UNIX user tries to access a file that has NTFS file permissions.

      Use the following entry to convert every UNIX user into a Windows user of the same name in the ENG domain. The pattern `(.+)` finds any UNIX name, and the replacement `ENG\\\1` creates the Windows version by inserting `ENG\\` before the user name.



d. Because the position of each rule determines the order in which the rules are applied, you should review the result and confirm that the order matches your expectations.



e. Repeat steps 5b to 5d to map all of the domains and names on the SVM.

6. **Optional**: Create a default Windows user:

   a. Create a Windows user account in LDAP, NIS, or the local users of the SVM.

      If you use local users, you can create an account under **Windows** in the Host Users and Groups pane.

   b. Set the default Windows user by selecting **NFS** > **Edit** in the **Protocols** pane, and entering the user name.

   You can create a local Windows user named “unixusers” and set it as the default Windows user.

7. **Optional**: Configure the default UNIX user if you want a user different from the default value, which is the “pcuser” user.

   a. Create a UNIX user account in LDAP, NIS, or the local users of the SVM.

      If you use local users, you can create an account under **UNIX** in the Host Users and Groups pane.

   b. Set the default UNIX user by selecting **CIFS** > **Options** in the **Protocols** pane, and entering the user name.

   You can create a local UNIX user named “winusers” and set it as the default UNIX user.

What to do next

If you configured default users, when you configure file permissions later in the workflow, you should set permissions for the default Windows user and the default UNIX user.

Create and configure a volume

You must create a FlexVol volume to contain your data. You can optionally change the volume's default security style, which is inherited from the security style of the root volume. You can also optionally change the volume's default location in the namespace, which is at the root volume of the storage virtual machine (SVM).

Steps

1. Navigate to the **Volumes** window.
2. Click **Create** > **Create FlexVol**.

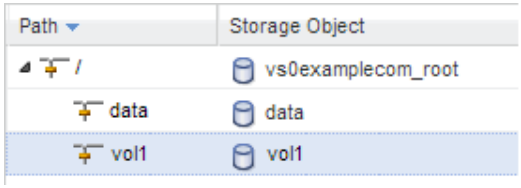
   The Create Volume dialog box is displayed.

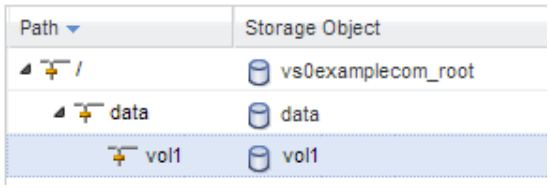
3. If you want to change the default name, which ends in a date and time stamp, specify a new name, such as `vol1`.
4. Select an aggregate for the volume.
5. Specify the size of the volume.
6. Click **Create**.

   Any new volume created in System Manager is mounted by default at the root volume using the volume name as the junction name. You use the junction path and the junction name when configuring CIFS shares, and NFS clients use the junction path and the junction name when mounting the volume.

7. **Optional**: If you do not want the volume to be located at the root of the SVM, modify the place of the new volume in the existing namespace:
   a. Navigate to the **Namespace** window.
   b. Select the **SVM** from the drop-down menu.
   c. Click **Mount**.
   d. In the **Mount Volume** dialog box, specify the volume, the name of its junction path, and the junction path on which you want the volume mounted.
   e. Verify the new junction path in the **Namespace** window.

      If you want to organize certain volumes under a main volume named "data", you can move the new volume "vol1" from the root volume to the "data" volume.

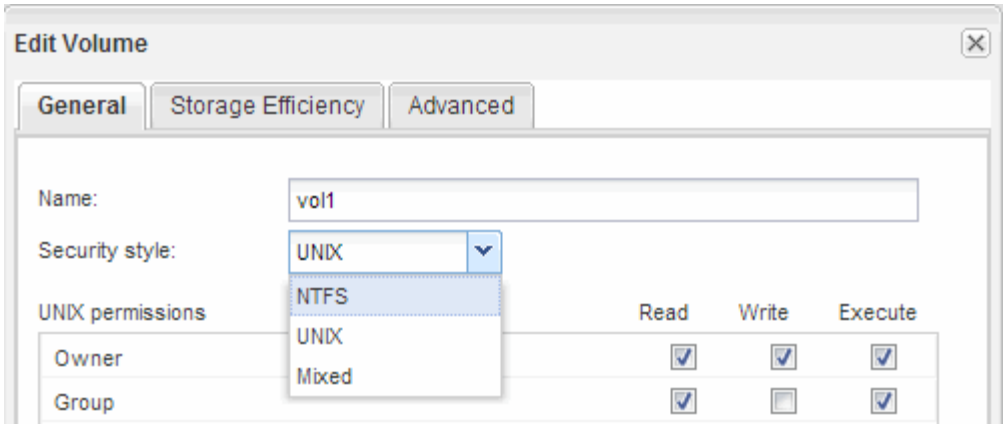




8. Review the volume's security style and change it, if necessary:
   a. In the **Volume** window, select the volume you just created, and click **Edit**.

      The Edit Volume dialog box is displayed, showing the volume's current security style, which is inherited from the security style of the SVM root volume.

   b. Select the security style you prefer, and click **Save and Close**.



Create a share and set its permissions

Before Windows users can access a volume, you must create a CIFS share on the volume and restrict access to the share by modifying the access control list (ACL) for the share.

About this task

For testing purposes, you should permit access only to administrators. Later, after you have verified that the volume is accessible, you can permit access to more clients.

Steps

1. Navigate to the **Shares** window.
2. Create a share so that SMB clients can access the volume:
   a. Click **Create Share**.
   b. In the **Create Share** dialog box, click **Browse**, expand the namespace hierarchy, and then select the volume that you created earlier.
   c. If you want the share name to be different from the volume name, change the share name.
   d. Click **Create**.

   The share is created with a default ACL set to Full Control for the Everyone group.
3. Restrict access to the share by modifying the share ACL:
   a. Select the share, and then click **Edit**.
   b. In the **Permissions** tab, select the **Everyone** group, and then click **Remove**.
   c. Click **Add**, and then enter the name of an administrator group defined in the Windows Active Directory domain that includes the SVM.
   d. With the new administrator group selected, select all permissions for it.
   e. Click **Save and Close**.

   The updated share access permissions are listed in the Share Access Control pane.

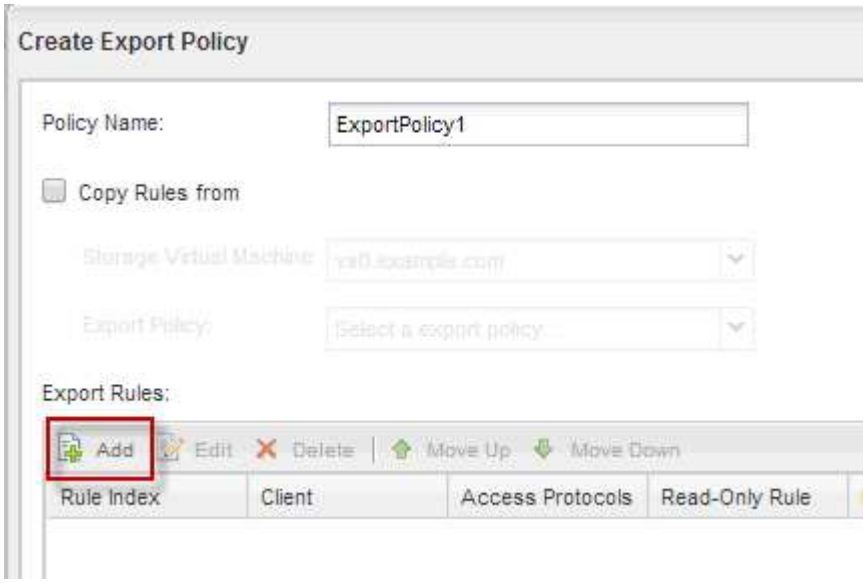
Create an export policy for the volume

Before any NFS clients can access a volume, you must create an export policy for the

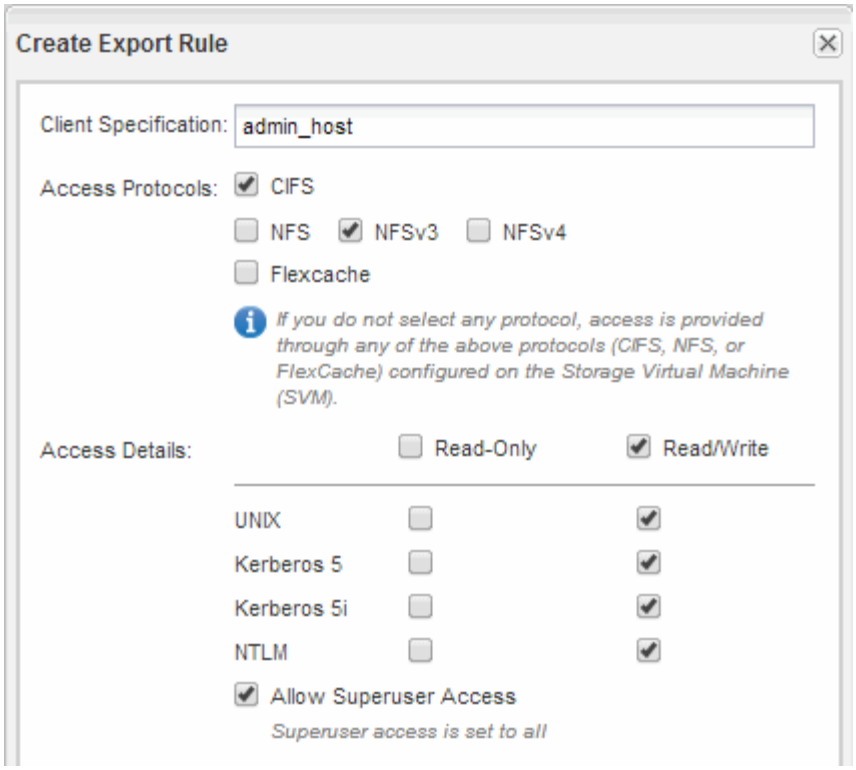
volume, add a rule that permits access by an administration host, and apply the new export policy to the volume.

Steps

1. Navigate to the **SVMs** window.
2. Click the **SVM Settings** tab.
3. Create a new export policy:
   a. In the **Policies** pane, click **Export Policies** and then click **Create**.
   b. In the **Create Export Policy** window, specify a policy name.
   c. Under **Export Rules**, click **Add** to add a rule to the new policy.



4. In the **Create Export Rule** dialog box, create a rule that allows an administrator full access to the export through all protocols:
   a. Specify the IP address or client name, such as admin_host, from which the exported volume will be administered.
   b. Select **CIFS** and **NFSv3**.
   c. Ensure that all **Read/Write** access details are selected, as well as **Allow Superuser Access**.



d. Click **OK** and then click **Create**.

The new export policy is created, along with its new rule.

5. Apply the new export policy to the new volume so that the administrator host can access the volume:
   a. Navigate to the **Namespace** window.
   b. Select the volume and click **Change Export Policy**.
   c. Select the new policy and click **Change**.

Verify SMB client access

You should verify that you have configured SMB correctly by accessing and writing data to the share. You should test access using the SMB server name and any NetBIOS aliases.

Steps

1. Log in to a Windows client.
2. Test access using the SMB server name:

   a. In Windows Explorer, map a drive to the share in the following format: `\\SMB_Server_Name\Share_Name`

      If the mapping is not successful, it is possible that the DNS mapping has not yet propagated throughout the network. You must test access using the SMB server name later.

      If the SMB server is named vs1.example.com and the share is named SHARE1, you should enter the following: `\\vs0.example.com\SHARE1`

   b. On the newly created drive, create a test file, and then delete the file.

You have verified write access to the share using the SMB server name.

3. Repeat Step 2 for any NetBIOS aliases.

Verify NFS access from a UNIX administration host

After you configure NFS access to storage virtual machine (SVM), you should verify the configuration by logging in to an NFS administration host and reading data from and writing data to the SVM.

Before you begin

- The client system must have an IP address that is allowed by the export rule you specified earlier.
- You must have the login information for the root user.

Steps

1. Log in as the root user to the client system.
2. Enter `cd /mnt/` to change the directory to the mount folder.
3. Create and mount a new folder using the IP address of the SVM:
   a. Enter `mkdir /mnt/folder` to create a new folder.
   b. Enter `mount -t nfs -o nfsvers=3,hard IPAddress:/volume_name /mnt/folder` to mount the volume at this new directory.
   c. Enter `cd folder` to change the directory to the new folder.

   The following commands create a folder named test1, mount the vol1 volume at the 192.0.2.130 IP address on the test1 mount folder, and change to the new test1 directory:

   ```
   host# mkdir /mnt/test1
   host# mount -t nfs -o nfsvers=3,hard 192.0.2.130:/vol1 /mnt/test1
   host# cd /mnt/test1
   ```

4. Create a new file, verify that it exists, and write text to it:
   a. Enter `touch filename` to create a test file.
   b. Enter `ls -l filename` to verify that the file exists.
   c. Enter `cat >filename`, type some text, and then press Ctrl+D to write text to the test file.
   d. Enter `cat filename` to display the content of the test file.
   e. Enter `rm filename` to remove the test file.
   f. Enter `cd ..` to return to the parent directory.

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

Results

You have confirmed that you have enabled NFS access to the SVM.

Configure and verify CIFS and NFS client access

When you are ready, you can configure client access by setting either UNIX or NTFS file permissions, modifying the share ACL, and adding an export rule. Then you should test that the affected users or groups can access the volume.

Steps

1. Decide which clients and users or groups will be given access to the share.
2. Set file permissions using a method that corresponds to the volume's security style:

If the volume's security style is this…	Do this…
NTFS	a. Log in to a Windows client as an administrator who has sufficient administrative rights to manage NTFS permissions. b. In Windows Explorer, right-click the drive, and then select **Properties**. c. Select the Security tab, and adjust the security settings for the groups and users as required.
UNIX	On a UNIX administration host, use the root user to set UNIX ownership and permissions on the volume.

3. In System Manager, modify the share ACL to give Windows users or groups access to the share.
   a. Navigate to the **Shares** window.
   b. Select the share, and click **Edit**.
   c. Select the **Permissions** tab, and give the users or groups access to the share.
4. In System Manager, add rules to the export policy to permit NFS clients to access the share.
   a. Select the storage virtual machine (SVM), and click **SVM Settings**.
   b. In the **Policies** pane, click **Export Policies**.

c. Select the export policy that is applied to the volume.

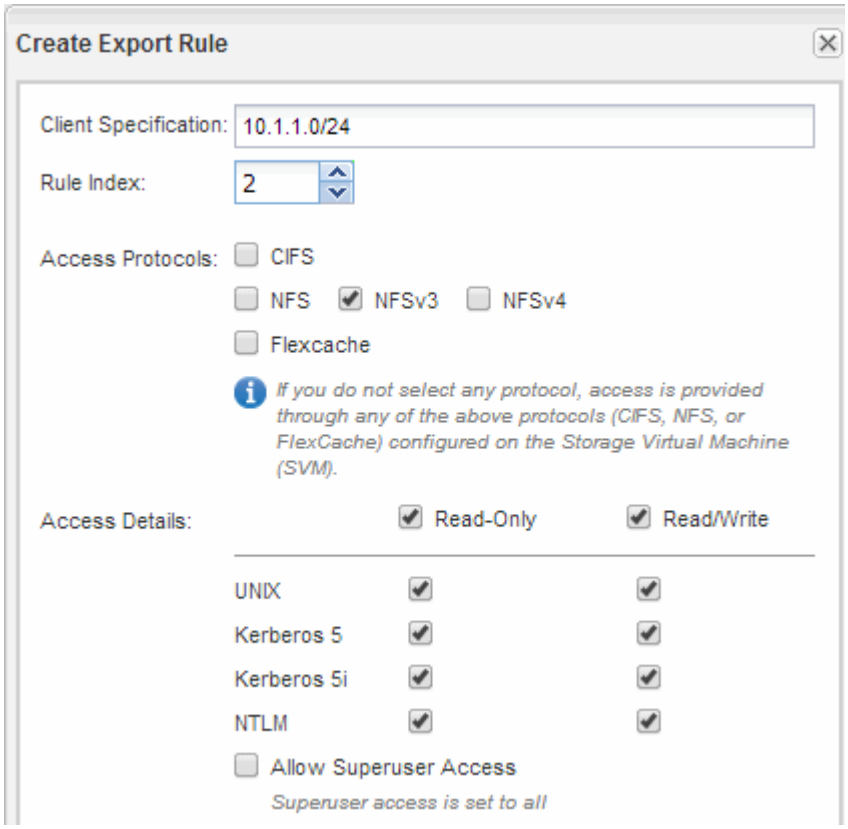
d. In the **Export Rules** tab, click **Add**, and specify a set of clients.

e. Select **2** for the **Rule Index** so that this rule executes after the rule that allows access to the administration host.

f. Select **CIFS** and **NFSv3**.

g. Specify the access details that you want, and click **OK.**

You can give full read/write access to clients by typing the subnet `10.1.1.0/24` as the **Client Specification**, and selecting all the access check boxes except **Allow Superuser Access**.



5. On a Windows client, log in as one of the users who now has access to the share and files, and verify that you can access the share and create a file.
6. On a UNIX client, log in as one of the users who now has access to the volume, and verify that you can mount the volume and create a file.

SMB/CIFS configuration

SMB/CIFS configuration overview

Using the ONTAP System Manager classic interface (ONTAP 9.7 and earlier), you can quickly set up SMB/CIFS access to a new volume on either a new or existing storage virtual machine (SVM).

Use this procedure if you want to configure access to a volume in the following way:

- You want to use best practices, not explore every available option.

- Your data network uses the default IPspace, the default broadcast domain, and the default failover group.

  If your data network is flat, using these default objects ensures that LIFs will fail over correctly in the event of a link failure. If you are not using the default objects, you should refer to the Network management documentation for information on how to configure LIF path failover.

- NTFS file permissions will be used to secure the new volume.

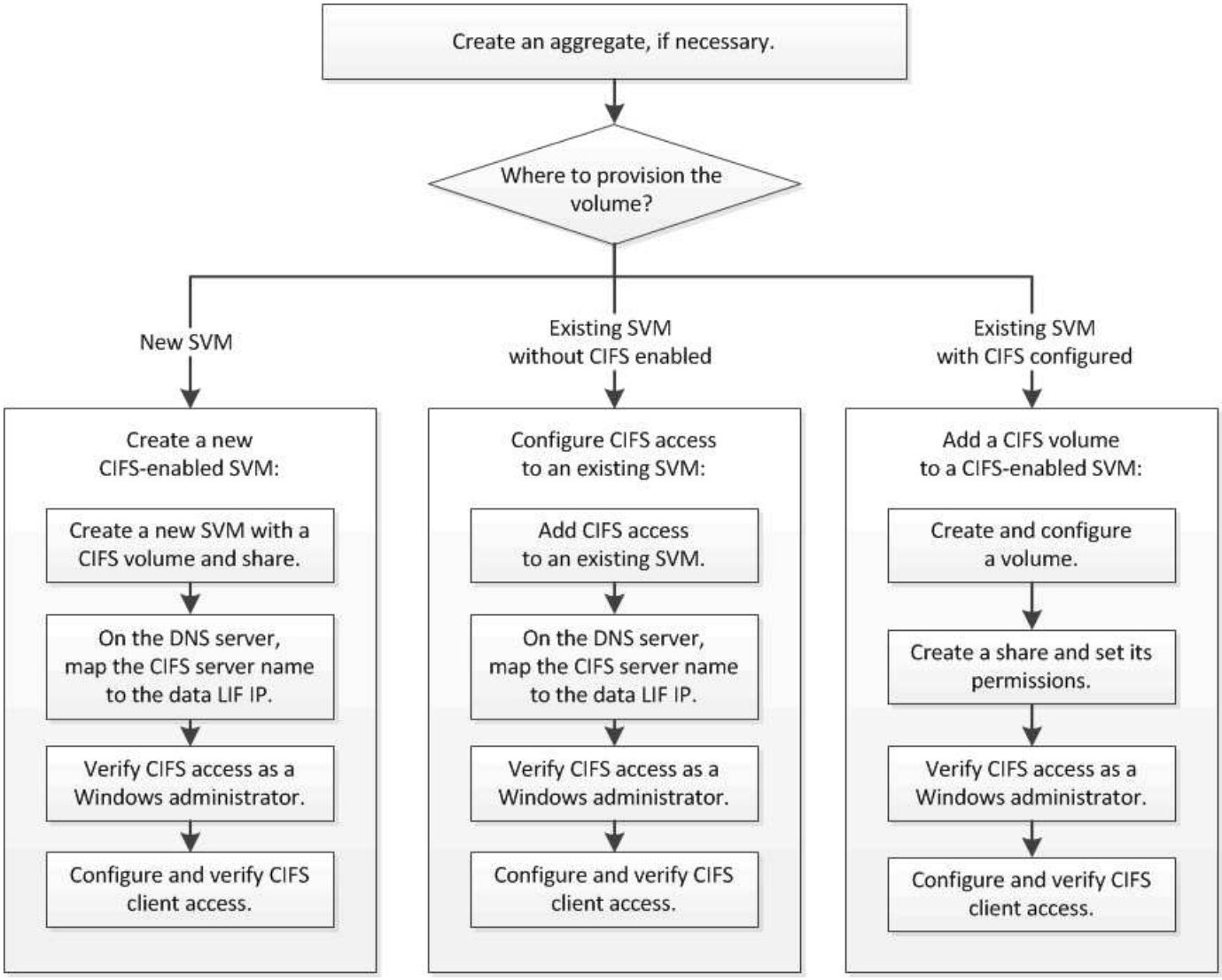
If you want details about the range of ONTAP SMB protocol capabilities, consult the SMB reference overview.

Other ways to do this in ONTAP

To perform these tasks with…	Refer to…
The redesigned System Manager (available with ONTAP 9.7 and later)	Provision NAS storage for Windows servers using SMB
The ONTAP command line interface	SMB configuration overview with the CLI

SMB/CIFS configuration workflow

Configuring SMB/CIFS involves optionally creating an aggregate and then choosing a workflow that is specific to your goal—creating a new CIFS-enabled SVM, configuring CIFS access to an existing SVM, or simply adding a CIFS volume to an existing SVM that is already fully configured for CIFS access.



Create an aggregate

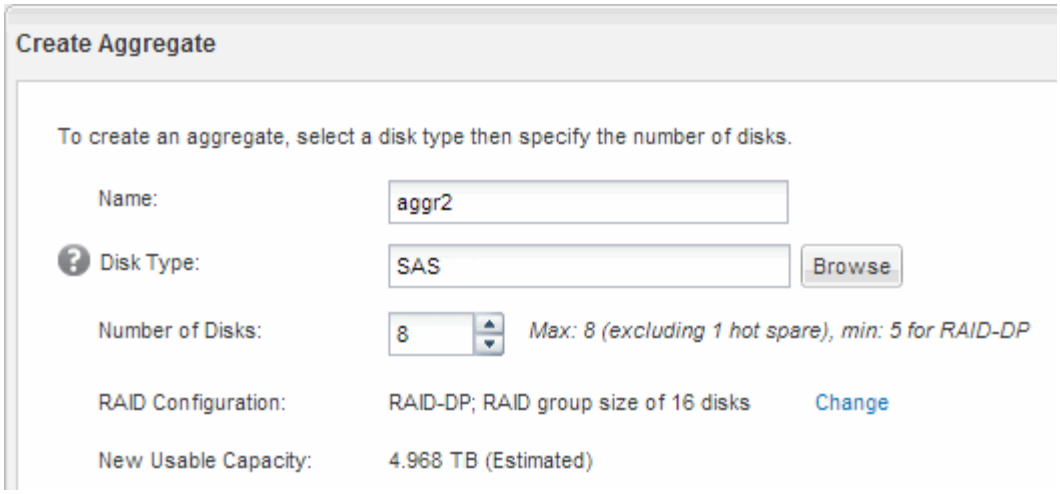
If you do not want to use an existing aggregate, you can create a new aggregate to provide physical storage to the volume which you are provisioning.

About this task

If you have an existing aggregate that you want to use for the new volume, you can skip this procedure.

Steps

1. Enter the URL `https://IP-address-of-cluster-management-LIF` in a web browser and log in to System Manager using your cluster administrator credential.
2. Navigate to the **Aggregates** window.
3. Click **Create.**
4. Follow the instructions on the screen to create the aggregate using the default RAID-DP configuration, and then click **Create**.



Results

The aggregate is created with the specified configuration and added to the list of aggregates in the Aggregates window.

Decide where to provision the new volume

Before you create a new CIFS volume, you must decide whether to place it in an existing storage virtual machine (SVM), and, if so, how much configuration the SVM requires. This decision determines your workflow.

Procedure

- If you want to provision a volume on a new SVM, create a new CIFS-enabled SVM.

  Creating a new CIFS-enabled SVM

  You must choose this option if CIFS is not enabled on an existing SVM.

- If you want to provision a volume on an existing SVM on which CIFS is enabled but not configured, configure CIFS/SMB access on the existing SVM.

  Configuring CIFS/SMB access on an existing SVM

  You should choose this option if you used the procedure to create the SVM for SAN access.

- If you want to provision a volume on an existing SVM that is fully configured for CIFS access, add a CIFS volume to the CIFS-enabled SVM.

  Adding a CIFS volume to a CIFS-enabled SVM

Create a new CIFS-enabled SVM

Setting up a new CIFS-enabled SVM involves creating the new SVM with a CIFS volume and share, adding a mapping on the DNS server, and verifying CIFS access from a Windows administration host. You can then configure CIFS client access.

Create a new SVM with a CIFS volume and share

You can use a wizard that guides you through the process of creating a new storage virtual machine (SVM), configuring Domain Name System (DNS), creating a data logical interface (LIF), configuring a CIFS server, and creating and sharing a volume.

Before you begin

- Your network must be configured and the relevant physical ports must be connected to the network.
- You must know which of the following networking components the SVM will use:
  - The node and the specific port on that node where the data logical interface (LIF) will be created
  - The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
  - Active Directory (AD) domain that this SVM will join, along with the credentials required to add the SVM to it
- The subnet must be routable to all external servers required for services such as Network Information Service (NIS), Lightweight Directory Access Protocol (LDAP), Active Directory (AD), and DNS.
- Any external firewalls must be appropriately configured to allow access to network services.
- The time on the AD domain controllers, clients, and SVM must be synchronized to within five minutes of each other.

Steps

1. Navigate to the **SVMs** window.
2. Click **Create.**
3. In the **Storage Virtual Machine (SVM) Setup** dialog box, create the SVM:

   a. Specify a unique name for the SVM.

      The name must either be a fully qualified domain name (FQDN) or follow another convention that ensures unique names across a cluster.

   b. Select all the protocols that you have licenses for and that you will eventually use on the SVM, even if you do not want to configure all the protocols immediately.

      If NFS access is required eventually, you must select **NFS** now so that CIFS and NFS clients can share the same data LIF.

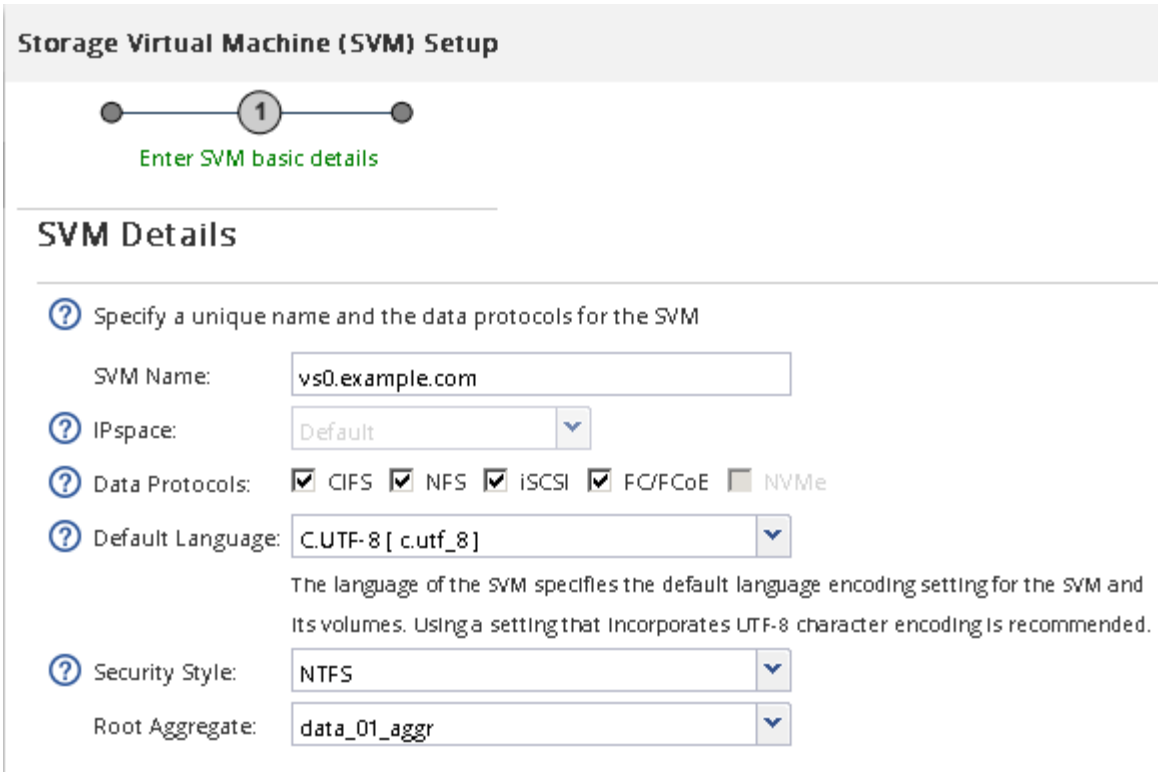
   c. Keep the default language setting, C.UTF-8.

      If you support international character display in both NFS and SMB/CIFS clients, consider using the **UTF8MB4** language code, which is available beginning with ONTAP 9.5.

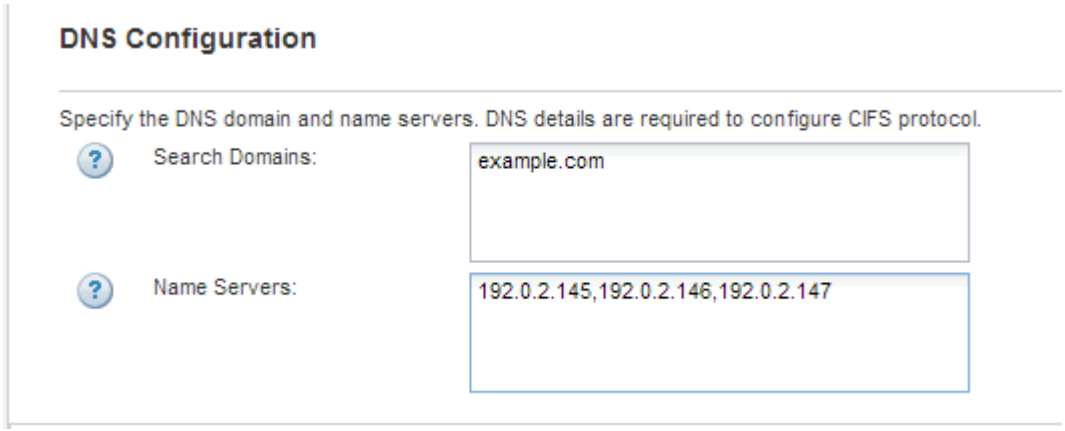
      This language is inherited by the volume that you create later, and a volume's language cannot be changed.

   d. **Optional**: Select the root aggregate to contain the SVM root volume.

      The aggregate that you select for the root volume does not determine the location of the data volume. The aggregate for the data volume is selected automatically when you provision storage in a later step.



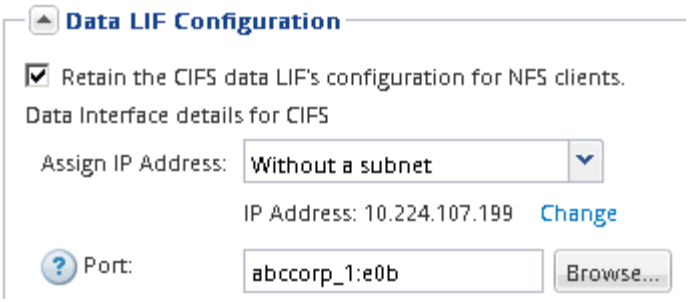
e. **Optional**: In the **DNS Configuration** area, ensure that the default DNS search domain and name servers are the ones that you want to use for this SVM.



f. Click **Submit & Continue**.

The SVM is created, but protocols are not yet configured.

4. In the **Data LIF Configuration** section of the **Configure CIFS/NFS protocol** page, specify the details of the LIF that clients will use to access data:
   a. Assign an IP address to the LIF automatically from a subnet you specify or manually enter the address.
   b. Click **Browse** and select a node and port that will be associated with the LIF.



5. In the **CIFS Server Configuration** section, define the CIFS server and configure it to access the AD domain:

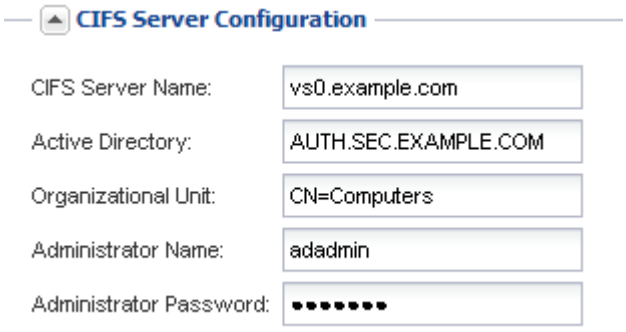
   a. Specify a name for the CIFS server that is unique in the AD domain.

   b. Specify the FQDN of the AD domain that the CIFS server can join.

   c. If you want to associate an organizational unit (OU) within the AD domain other than CN=Computers, enter the OU.

   d. Specify the name and password of an administrative account that has sufficient privileges to add the CIFS server to the OU.

   e. If you want to avoid unauthorized access to all the shares on this SVM, select the option to encrypt data using SMB 3.0.

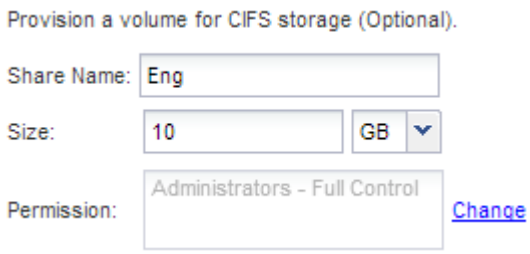


6. Create a volume for CIFS/SMB access and provision a share on it:

   a. Name the share that CIFS/SMB clients will use to access the volume.

      The name you enter for the share will also be used as the volume name.

   b. Specify a size for the volume.



   You do not have to specify the aggregate for the volume because it is automatically located on the aggregate with the most available space.

7. **Optional**: Restrict access to the share by modifying the share ACL:

a. In the **Permission** field, click **Change**.

b. Select the Everyone group, and click **Remove**.

c. **Optional**: Click **Add**, and enter the name of an administrator group defined in the Windows Active Directory domain that includes the SVM.

d. Select the new administrator group, and then select **Full Control**.

e. Click **Save and Close**.

8. Click **Submit & Continue**.

   The following objects are created:

   - A data LIF named after the SVM with the suffix "_cifs_lif1"
   - A CIFS server that is part of the AD domain
   - A volume that is located on the aggregate with the most available space and has a name that matches the name of the share and ends in the suffix "_CIFS_volume"
   - A share on the volume

9. For all other protocol configuration pages that are displayed, click **Skip** and configure the protocol later.
10. When the **SVM Administration** page is displayed, configure or defer configuring a separate administrator for this SVM:
    - Click **Skip** and configure an administrator later if required.
    - Enter the requested information and then click **Submit & Continue**.
11. Review the **Summary** page, record any information you might require later and then click **OK**.

    The DNS administrator needs to know the CIFS server name and the IP address of the data LIF. Windows clients need to know the names of the CIFS server and the share.

Results

A new SVM is created with a CIFS server containing a new volume that is shared.

Map the SMB server on the DNS server

Your site's DNS server must have an entry pointing the SMB server name, and any NetBIOS aliases, to the IP address of the data LIF so that Windows users can map a drive to the SMB server name.

Before you begin

You must have administrative access to your site's DNS server. If you do not have administrative access, you must ask the DNS administrator to perform this task.

About this task

If you use NetBIOS aliases for the SMB server name, it is a best practice to create DNS server entry points for each alias.

Steps

1. Log in to the DNS server.
2. 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 LIF.

3. 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 LIF.

Results

After the mapping is propagated across the network, Windows users can map a drive to the SMB server name or its NetBIOS aliases.

Verify SMB client access

You should verify that you have configured SMB correctly by accessing and writing data to the share. You should test access using the SMB server name and any NetBIOS aliases.

Steps

1. Log in to a Windows client.
2. Test access using the SMB server name:

   a. In Windows Explorer, map a drive to the share in the following format: `\\SMB_Server_Name\Share_Name`

      If the mapping is not successful, it is possible that the DNS mapping has not yet propagated throughout the network. You must test access using the SMB server name later.

      If the SMB server is named vs1.example.com and the share is named SHARE1, you should enter the following: `\\vs0.example.com\SHARE1`

   b. On the newly created drive, create a test file, and then delete the file.

   You have verified write access to the share using the SMB server name.

3. Repeat Step 2 for any NetBIOS aliases.

Configure and verify CIFS client access

When you are ready, you can give select clients access to the share by setting NTFS file permissions in Windows Explorer and modifying the share ACL in System Manager. Then you should test that the affected users or groups can access the volume.

Steps

1. Decide which clients and users or groups will be given access to the share.
2. On a Windows client, use an administrator role to give the users or groups permissions to the files and folders.
   a. Log in to a Windows client as an administrator who has sufficient administrative rights to manage NTFS permissions.
   b. In Windows Explorer, right-click the drive, and then select **Properties**.
   c. Select the **Security** tab, and adjust the security settings for the groups and users as required.
3. In System Manager, modify the share ACL to give Windows users or groups access to the share.
   a. Navigate to the **Shares** window.
   b. Select the share, and click **Edit**.

c. Select the **Permissions** tab, and give the users or groups access to the share.

4. On a Windows client, log in as one of the users who now has access to the share and files, and verify that you can access the share and create a file.

Configure SMB/CIFS access to an existing SVM

Adding access for SMB/CIFS clients to an existing SVM involves adding CIFS configurations to the SVM, adding a mapping on the DNS server, and verifying CIFS access from a Windows administration host. You can then configure CIFS client access.

Add CIFS access to an existing SVM

Adding CIFS/SMB access to an existing SVM involves creating a data LIF, configuring a CIFS server, provisioning a volume, sharing the volume, and configuring the share permissions.

Before you begin

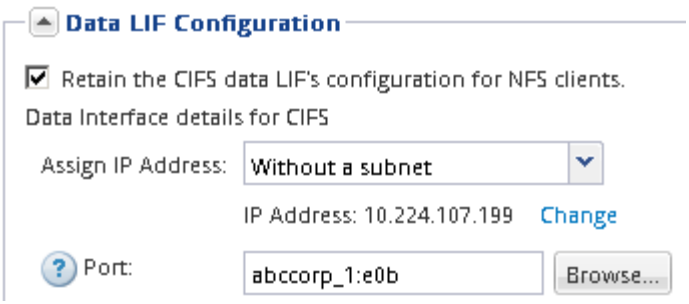
- You must know which of the following networking components the SVM will use:
  - The node and the specific port on that node where the data logical interface (LIF) will be created
  - The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
  - The Active Directory (AD) domain that this SVM will join, along with the credentials required to add the SVM to it
- Any external firewalls must be appropriately configured to allow access to network services.
- The CIFS protocol must be allowed on the SVM.

  This is the case if you did not created the SVM following the procedure to configure a SAN protocol.

Steps

1. Navigate to the area where you can configure the protocols of the SVM:
   a. Select the SVM that you want to configure.
   b. In the **Details** pane, next to **Protocols**, click **CIFS**.

2. In the **Data LIF Configuration** section of the **Configure CIFS protocol** dialog box, create a data LIF for the SVM:
   a. Assign an IP address to the LIF automatically from a subnet you specify or manually enter the address.
   b. Click **Browse** and select a node and port that will be associated with the LIF.



3. In the **CIFS Server Configuration** section, define the CIFS server and configure it to access the AD domain:

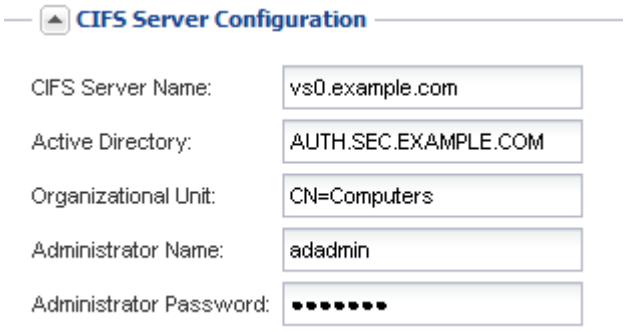
   a. Specify a name for the CIFS server that is unique in the AD domain.

   b. Specify the FQDN of the AD domain that the CIFS server can join.

   c. If you want to associate an organizational unit (OU) within the AD domain other than CN=Computers, enter the OU.

   d. Specify the name and password of an administrative account that has sufficient privileges to add the CIFS server to the OU.

   e. If you want to avoid unauthorized access to all the shares on this SVM, select the option to encrypt data using SMB 3.0.

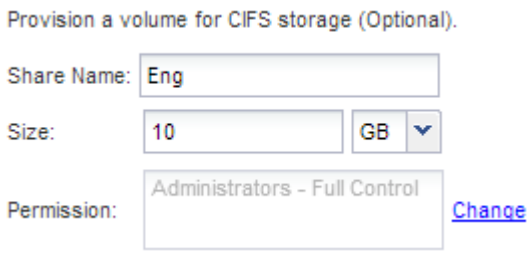


4. Create a volume for CIFS/SMB access and provision a share on it:

   a. Name the share that CIFS/SMB clients will use to access the volume.

      The name you enter for the share will also be used as the volume name.

   b. Specify a size for the volume.



   You do not have to specify the aggregate for the volume because it is automatically located on the aggregate with the most available space.

5. **Optional**: Restrict access to the share by modifying the share ACL:

a. In the **Permission** field, click **Change**.

b. Select the Everyone group, and click **Remove**.

c. **Optional**: Click **Add**, and enter the name of an administrator group defined in the Windows Active Directory domain that includes the SVM.

d. Select the new administrator group, and then select **Full Control**.

e. Click **Save and Close**.

6. Click **Submit & Close**, and then click **OK**.

Map the SMB server on the DNS server

Your site's DNS server must have an entry pointing the SMB server name, and any NetBIOS aliases, to the IP address of the data LIF so that Windows users can map a drive to the SMB server name.

Before you begin

You must have administrative access to your site's DNS server. If you do not have administrative access, you must ask the DNS administrator to perform this task.

About this task

If you use NetBIOS aliases for the SMB server name, it is a best practice to create DNS server entry points for each alias.

Steps

1. Log in to the DNS server.
2. 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 LIF.
3. 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 LIF.

Results

After the mapping is propagated across the network, Windows users can map a drive to the SMB server name or its NetBIOS aliases.

Verify SMB client access

You should verify that you have configured SMB correctly by accessing and writing data to the share. You should test access using the SMB server name and any NetBIOS aliases.

Steps

1. Log in to a Windows client.
2. Test access using the SMB server name:

   a. In Windows Explorer, map a drive to the share in the following format: `\\SMB_Server_Name\Share_Name`

      If the mapping is not successful, it is possible that the DNS mapping has not yet propagated throughout the network. You must test access using the SMB server name later.

If the SMB server is named vs1.example.com and the share is named SHARE1, you should enter the following: `\\vs0.example.com\SHARE1`

b. On the newly created drive, create a test file, and then delete the file.

You have verified write access to the share using the SMB server name.

3. Repeat Step 2 for any NetBIOS aliases.

Configure and verify CIFS client access

When you are ready, you can give select clients access to the share by setting NTFS file permissions in Windows Explorer and modifying the share ACL in System Manager. Then you should test that the affected users or groups can access the volume.

Steps

1. Decide which clients and users or groups will be given access to the share.
2. On a Windows client, use an administrator role to give the users or groups permissions to the files and folders.
   a. Log in to a Windows client as an administrator who has sufficient administrative rights to manage NTFS permissions.
   b. In Windows Explorer, right-click the drive, and then select **Properties**.
   c. Select the **Security** tab, and adjust the security settings for the groups and users as required.
3. In System Manager, modify the share ACL to give Windows users or groups access to the share.
   a. Navigate to the **Shares** window.
   b. Select the share, and click **Edit**.
   c. Select the **Permissions** tab, and give the users or groups access to the share.
4. On a Windows client, log in as one of the users who now has access to the share and files, and verify that you can access the share and create a file.

Add a CIFS volume to a CIFS-enabled SVM

Adding a CIFS volume to a CIFS-enabled SVM involves creating and configuring a volume, creating a share and setting its permissions, and verifying access from a Windows administration host. You can then configure CIFS client access.

Before you begin

CIFS must be completely set up on the SVM.

Create and configure a volume

You must create a FlexVol volume to contain your data. You can optionally change the volume's default security style, which is inherited from the security style of the root volume. You can also optionally change the volume's default location in the namespace, which is at the root volume of the storage virtual machine (SVM).

Steps

1. Navigate to the **Volumes** window.
2. Click **Create** > **Create FlexVol**.

   The Create Volume dialog box is displayed.

3. If you want to change the default name, which ends in a date and time stamp, specify a new name, such as `vol1`.
4. Select an aggregate for the volume.
5. Specify the size of the volume.
6. Click **Create**.

   Any new volume created in System Manager is mounted by default at the root volume using the volume name as the junction name. You use the junction path and the junction name when configuring CIFS shares.

7. **Optional**: If you do not want the volume to be located at the root of the SVM, modify the place of the new volume in the existing namespace:

   a. Navigate to the **Namespace** window.

   b. Select the **SVM** from the drop-down menu.

   c. Click **Mount**.

   d. In the **Mount Volume** dialog box, specify the volume, the name of its junction path, and the junction path on which you want the volume mounted.

   e. Verify the new junction path in the **Namespace** window.

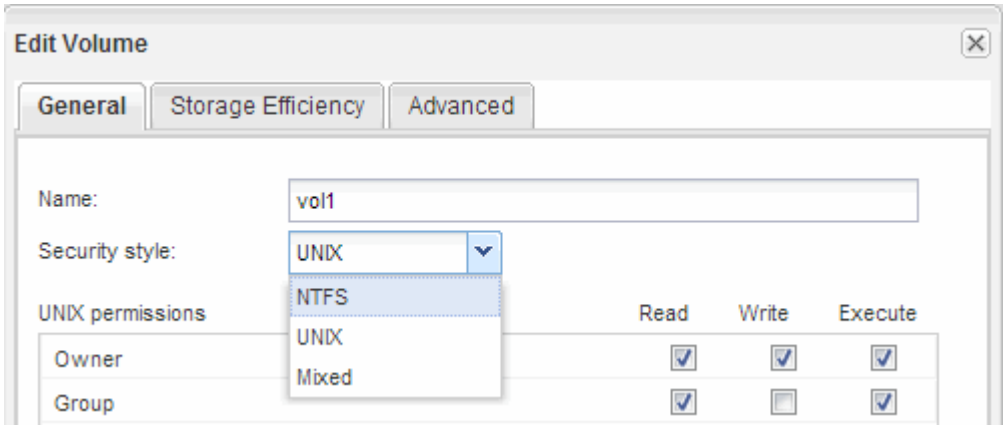
   If you want to organize certain volumes under a main volume named “data”, you can move the new volume “vol1” from the root volume to the “data” volume.

8. Review the volume’s security style and change it, if necessary:

   a. In the **Volume** window, select the volume you just created, and click **Edit**.

      The Edit Volume dialog box is displayed, showing the volume’s current security style, which is inherited from the security style of the SVM root volume.

   b. Make sure the security style is NTFS.



Create a share and set its permissions

Before Windows users can access a volume, you must create a CIFS share on the volume and restrict access to the share by modifying the access control list (ACL) for the share.

About this task

For testing purposes, you should permit access only to administrators. Later, after you have verified that the volume is accessible, you can permit access to more clients.

Steps

1. Navigate to the **Shares** window.
2. Create a share so that SMB clients can access the volume:
   a. Click **Create Share**.
   b. In the **Create Share** dialog box, click **Browse**, expand the namespace hierarchy, and then select the volume that you created earlier.
   c. **Optional**: If you want the share name to be different from the volume name, change the share name.
   d. Click **Create**.

   The share is created with a default ACL set to Full Control for the Everyone group.
3. **Optional**: Restrict access to the share by modifying the share ACL:
   a. Select the share, and then click **Edit**.
   b. In the **Permissions** tab, select the **Everyone** group, and then click **Remove**.
   c. Click **Add**, and then enter the name of an administrator group defined in the Windows Active Directory domain that includes the SVM.
   d. With the new administrator group selected, select all permissions for it.
   e. Click **Save and Close**.

   The updated share access permissions are listed in the Share Access Control pane.

What to do next

You should verify access as a Windows administrator.

Verify SMB client access

You should verify that you have configured SMB correctly by accessing and writing data to the share. You should test access using the SMB server name and any NetBIOS aliases.

Steps

1. Log in to a Windows client.
2. Test access using the SMB server name:
   a. In Windows Explorer, map a drive to the share in the following format: `\\SMB_Server_Name\Share_Name`

If the mapping is not successful, it is possible that the DNS mapping has not yet propagated throughout the network. You must test access using the SMB server name later.

If the SMB server is named vs1.example.com and the share is named SHARE1, you should enter the following: `\\vs0.example.com\SHARE1`

b. On the newly created drive, create a test file, and then delete the file.

You have verified write access to the share using the SMB server name.

3. Repeat Step 2 for any NetBIOS aliases.

Configure and verify CIFS client access

When you are ready, you can give select clients access to the share by setting NTFS file permissions in Windows Explorer and modifying the share ACL in System Manager. Then you should test that the affected users or groups can access the volume.

Steps

1. Decide which clients and users or groups will be given access to the share.
2. On a Windows client, use an administrator role to give the users or groups permissions to the files and folders.
   a. Log in to a Windows client as an administrator who has sufficient administrative rights to manage NTFS permissions.
   b. In Windows Explorer, right-click the drive, and then select **Properties**.
   c. Select the **Security** tab, and adjust the security settings for the groups and users as required.
3. In System Manager, modify the share ACL to give Windows users or groups access to the share.
   a. Navigate to the **Shares** window.
   b. Select the share, and click **Edit**.
   c. Select the **Permissions** tab, and give the users or groups access to the share.
4. On a Windows client, log in as one of the users who now has access to the share and files, and verify that you can access the share and create a file.

Provision SAN storage

FC configuration for ESXi using VSC

FC configuration for ESXi using VSC overview

Using the ONTAP System Manager classic interface (ONTAP 9.7 and earlier), you can quickly set up the FC service on a storage virtual machine (SVM), provision a LUN, and make the LUN available as a datastore using an FC HBA on an ESX host computer.

Use this procedure if:

- You are using a supported version of Virtual Storage Console for VMware vSphere (VSC) to configure storage settings for your ESX host and to provision the datastores.
  - Beginning with VSC 7.0, VSC is part of the ONTAP Tools for VMware vSphere virtual appliance, which includes VSC, vStorage APIs for Storage Awareness (VASA) Provider, and Storage Replication Adapter (SRA) for VMware vSphere capabilities.
  - Be sure to check the NetApp Interoperability Matrix Tool to confirm compatibility between your current ONTAP and VSC releases.
- Your network uses IPv4 addressing.
- You are using traditional FC HBAs on ESXi 5.x and traditional FC switches.

  This procedure does not cover FCoE.
- You have at least two FC target ports available on each node in the cluster.

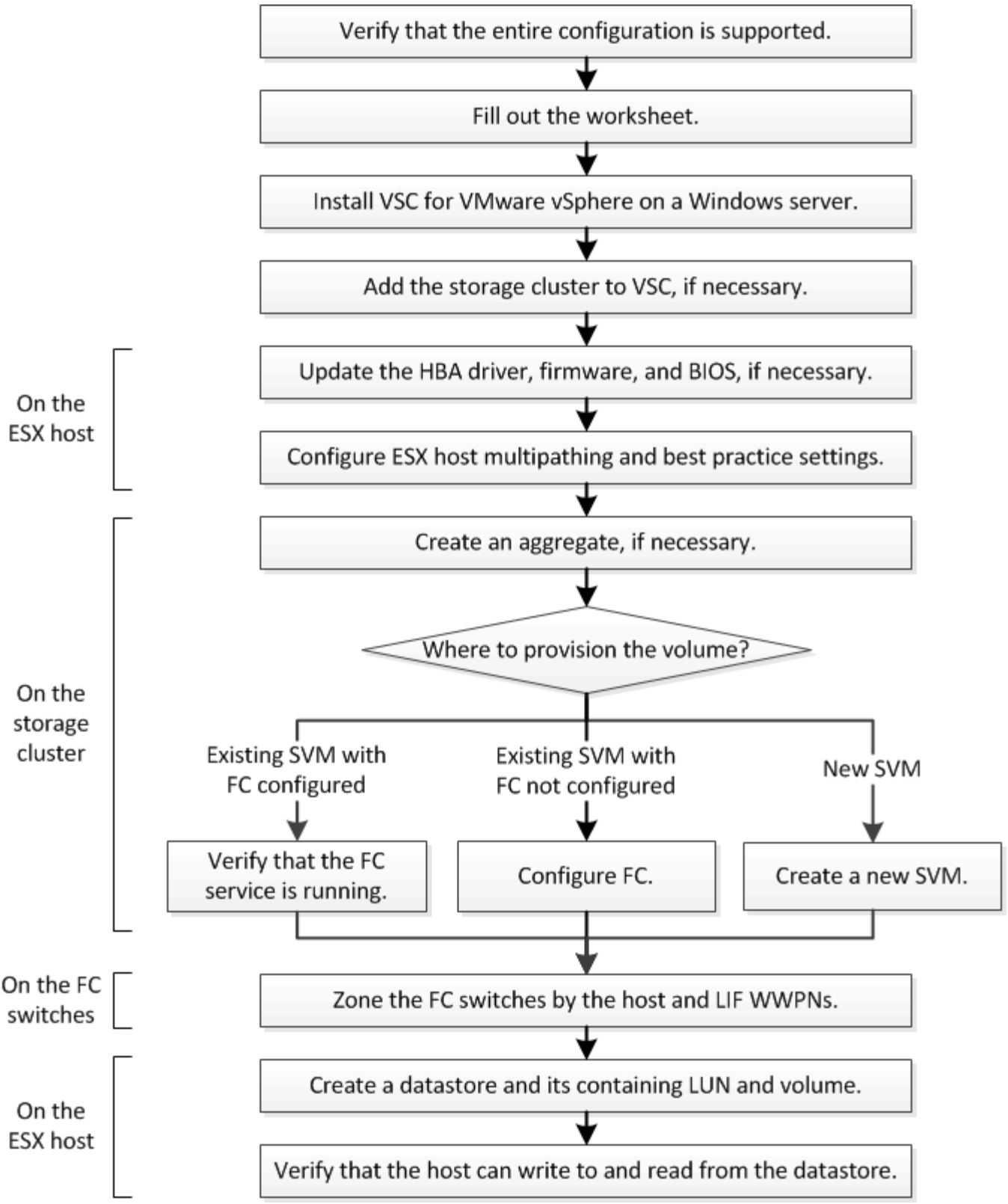
  Onboard FC and UTA2 (also called “CNA”) ports, as well as some adapters are configurable. Configuring those ports is done in the ONTAP CLI and is not covered in this procedure.
- You are not configuring FC SAN boot.
- You are creating datastores on the host.

  This procedure does not cover raw device mapping (RDM) disks or using N-port ID virtualization (NPIV) to provide FC directly to VMs.

For more information, see TR-4597: VMware vSphere for ONTAP and the documentation for your VSC release.

FC configuration workflow

When you make storage available to a host using FC, you provision a volume and LUN on the storage virtual machine (SVM), and then connect to the LUN from the host.



Verify that the FC configuration is supported

For reliable operation, you must verify that the entire FC configuration is supported.

Steps

1. Go to the Interoperability Matrix to verify that you have a supported combination of the following

components:

- ONTAP software
- Host computer CPU architecture (for standard rack servers)
- Specific processor blade model (for blade servers)
- FC host bus adapter (HBA) model and driver, firmware, and BIOS versions
- Storage protocol (FC)
- ESXi operating system version
- Guest operating system type and version
- Virtual Storage Console (VSC) for VMware vSphere software
- Windows Server version to run VSC

2. Click the configuration name for the selected configuration.

   Details for that configuration are displayed in the Configuration Details window.

3. Review the information in the following tabs:
   - Notes

     Lists important alerts and information that are specific to your configuration.

   - Policies and Guidelines

     Provides general guidelines for all SAN configurations.

Complete the FC configuration worksheet

You require FC initiator and target WWPNs and storage configuration information to perform FC configuration tasks.

FC host WWPNs

Port	WWPN
Initiator (host) port connected to FC switch 1	
Initiator (host) port connected to FC switch 2	

FC target WWPNs

You require two FC data LIFs for each node in the cluster. The WWPNs are assigned by ONTAP when you create the LIFs as part of creating the storage virtual machine (SVM).

LIF	WWPN
Node 1 LIF with port connected to FC switch 1	

LIF	WWPN
Node 2 LIF with port connected to FC switch 1	
Node 3 LIF with port connected to FC switch 1	
Node 4 LIF with port connected to FC switch 1	
Node 1 LIF with port connected to FC switch 2	
Node 2 LIF with port connected to FC switch 2	
Node 3 LIF with port connected to FC switch 2	
Node 4 LIF with port connected to FC switch 2	

Storage configuration

If the aggregate and SVM are already created, record their names here; otherwise, you can create them as required:

Node to own LUN
Aggregate name
SVM name

LUN information

LUN size
LUN name (optional)
LUN description (optional)

SVM information

If you are not using an existing SVM, you require the following information to create a new one:

SVM name
SVM IPspace
Aggregate for SVM root volume
SVM user name (optional)

SVM name	
SVM password (optional)	
SVM management LIF (optional)	
	Subnet:
	IP address:
	Network mask:
	Gateway:
	Home node:
	Home port:

Install Virtual Storage Console

Virtual Storage Console for VMware vSphere automates many of the configuration and provisioning tasks required to use NetApp FC storage with an ESXi host. Virtual Storage Console is a plug-in to vCenter Server.

Before you begin

You must have administrator credentials on the vCenter Server used to manage the ESXi host.

About this task

- Virtual Storage Console is installed as a virtual appliance that includes Virtual Storage Console, vStorage APIs for Storage Awareness (VASA) Provider, and Storage Replication Adapter (SRA) for VMware vSphere capabilities.

Steps

1. Download the version of Virtual Storage Console that is supported for your configuration, as shown in the Interoperability Matrix tool.

   NetApp Support

2. Deploy the virtual appliance and configure it following the steps in the *Deployment and Setup Guide*.

Add the storage cluster or SVM to VSC for VMware vSphere

Before you can provision the first datastore to an ESXi host in your Datacenter, you must add the cluster or a specific storage virtual machine (SVM) to Virtual Storage Console for VMware vSphere. Adding the cluster enables you to provision storage on any SVM in the cluster.

Before you begin

You must have administrator credentials for the storage cluster or the SVM that is being added.

About this task

Depending on your configuration, the cluster might have been discovered automatically, or might have already been added.

Steps

1. Log in to the vSphere Web Client.
2. Select **Virtual Storage Console**.
3. Select **Storage Systems** and then click the **Add** icon.
4. In the **Add Storage System** dialog box, enter the host name and administrator credentials for the storage cluster or SVM and then click **OK**.

Update the HBA driver, firmware, and BIOS

If the FC host bus adapters (HBAs) in the ESX host are not running supported driver, firmware, and BIOS versions, you must update them.

Before you begin

You must have identified the supported driver, firmware, and BIOS versions for your configuration from the NetApp Interoperability Matrix Tool.

About this task

Drivers, firmware, BIOS, and HBA utilities are provided by the HBA vendors.

Steps

1. List the installed HBA driver, firmware, and BIOS versions using the ESXi host console commands for your version of ESXi.
2. Download and install the new driver, firmware, and BIOS as needed from the HBA vendor's support site.

   Installation instructions and any required installation utilities are available with the download.

Related information

VMware KB article 1002413: Identifying the firmware of a Qlogic or Emulex FC HBA

Configure the ESXi host best practice settings

You must ensure that the host multipathing and best practice settings are correct so that the ESXi host can correctly manage the loss of an FC path or a storage failover event.

Steps

1. From the VMware vSphere Web Client **Home** page, click **vCenter** > **Hosts**.
2. Right-click the host, and then select **Actions** > **NetApp VSC** > **Set Recommended Values**.
3. In the **NetApp Recommended Settings** dialog box, ensure that all of the options are selected, and then click **OK**.

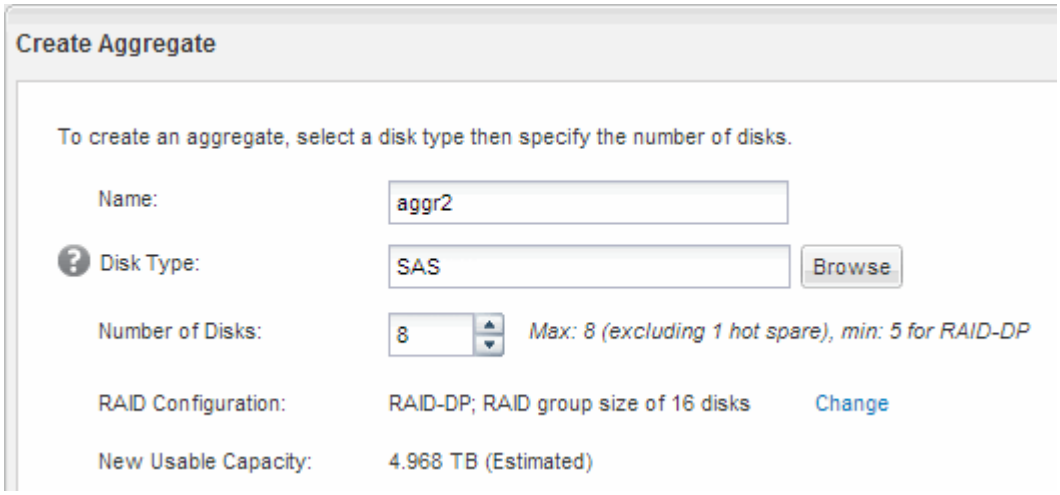
   The vCenter Web Client displays the task progress.

Create an aggregate

If you do not want to use an existing aggregate, you can create a new aggregate to provide physical storage to the volume which you are provisioning.

Steps

1. Enter the URL `https://IP-address-of-cluster-management-LIF` in a web browser and log in to System Manager using your cluster administrator credential.
2. Navigate to the **Aggregates** window.
3. Click **Create.**
4. Follow the instructions on the screen to create the aggregate using the default RAID-DP configuration, and then click **Create**.



Results

The aggregate is created with the specified configuration and added to the list of aggregates in the Aggregates window.

Decide where to provision the volume

Before you provision a volume to contain your LUNs, you need to decide whether to add the volume to an existing storage virtual machine (SVM) or to create a new SVM for the volume. You might also need to configure FC on an existing SVM.

About this task

If an existing SVM is already configured with the needed protocols and has LIFs that can be accessed from the host, it is easier to use the existing SVM.

You can create a new SVM to separate data or administration from other users of the storage cluster. There is no advantage to using separate SVMs just to separate different protocols.

Procedure

- If you want to provision volumes on an SVM that is already configured for FC, you must verify that the FC service is running.

  Verifying that the FC service is running on an existing SVM

- If you want to provision volumes on an existing SVM that has FC enabled but not configured, configure iSCSI on the existing SVM.

  Configuring FC on an existing SVM

  This is the case if you did not follow this procedure to create the SVM while configuring a different protocol.

- If you want to provision volumes on a new SVM, create the SVM.

  Creating a new SVM

Verify that the FC service is running on an existing SVM

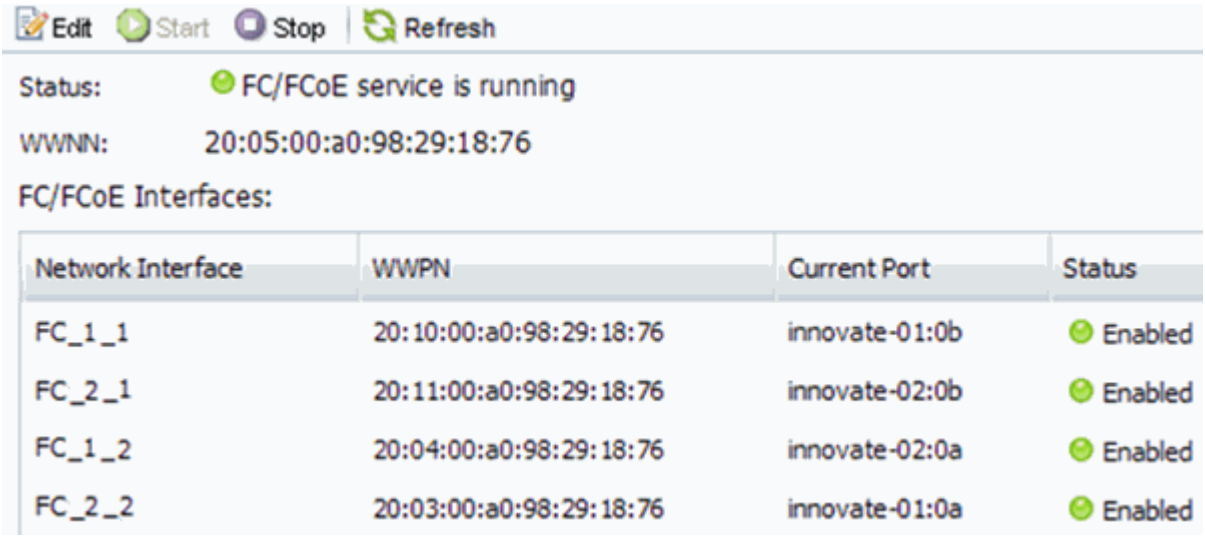
If you choose to use an existing storage virtual machine (SVM), you must verify that the FC service is running on the SVM by using ONTAP System Manager. You must also verify that FC logical interfaces (LIFs) are already created.

Before you begin

You must have selected an existing SVM on which you plan to create a new LUN.

Steps

1. Navigate to the **SVMs** window.
2. Select the required SVM.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **FC/FCoE**.
5. Verify that the FC service is running.



   If the FC service is not running, start the FC service or create a new SVM.

6. Verify that there are at least two FC LIFs listed for each node.

   If there are fewer than two FC LIFs per node, update the FC configuration on the SVM or create a new SVM for FC.

Configure FC on an existing SVM

You can configure FC on an existing storage virtual machine (SVM). The FC protocol must already be enabled but not configured on the SVM. This information is intended for SVMs for which you are configuring multiple protocols, but have not yet configured FC.

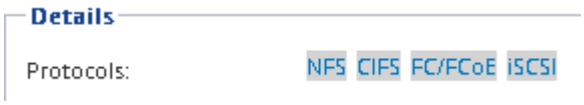
Before you begin

Your FC fabric must be configured and the desired physical ports must be connected to the fabric.

Steps

1. Navigate to the **SVMs** window.
2. Select the SVM that you want to configure.
3. In the SVM**Details** pane, verify that **FC/FCoE** is displayed with a gray background, which indicates that the protocol is enabled but not fully configured.

   If **FC/FCoE** is displayed with a green background, the SVM is already configured.

4. Click the **FC/FCoE** protocol link with the gray background.

   The Configure FC/FCoE Protocol window is displayed.

5. Configure the FC service and LIFs from the **Configure FC/FCoE protocol** page:
   a. Select the **Configure Data LIFs for FC** check box.
   b. Enter 2 in the **LIFs per node** field.

      Two LIFs are required for each node, to ensure availability and data mobility.

   c. Ignore the optional **Provision a LUN for FCP storage** area, because the LUN is provisioned by Virtual Storage Console for VMware vSphere in a later step.
   d. Click **Submit & Close**.
6. Review the **Summary** page, record the LIF information, and then click **OK**.

Create a new SVM

The storage virtual machine (SVM) provides the FC target through which a host accesses LUNs. When you create the SVM, you also create logical interfaces (LIFs) that provide paths to the LUN. You can create an SVM to separate the data and administration functions of a user from those of the other users in a cluster.

Before you begin

- Your FC fabric must be configured and the desired physical ports must be connected to the fabric.

Steps

1. Navigate to the **SVMs** window.
2. Click **Create**.

3. In the **Storage Virtual Machine (SVM) Setup** window, create the SVM:

   a. Specify a unique name for the SVM.

      The name must either be a fully qualified domain name (FQDN) or follow another convention that ensures unique names across a cluster.

   b. Select the IPspace that the SVM will belong to.

      If the cluster does not use multiple IPspaces, the “Default” IPspace is used.

   c. Keep the default volume type selection.

      Only FlexVol volumes are supported with SAN protocols.

   d. Select all of the protocols that you have licenses for and that you might use on the SVM, even if you do not want to configure all of the protocols immediately.

      Selecting both NFS and CIFS when you create the SVM enables these two protocols to share the same LIFs. Adding these protocols later does not allow them to share LIFs.

      If CIFS is one of the protocols you selected, then the security style is set to NTFS. Otherwise, the security style is set to UNIX.

   e. Keep the default language setting C.UTF-8.

   f. Select the desired root aggregate to contain the SVM root volume.

      The aggregate for the data volume is selected separately in a later step.

   g. Click **Submit & Continue**.

   The SVM is created, but protocols are not yet configured.

4. If the **Configure CIFS/NFS protocol** page appears because you enabled CIFS or NFS, click **Skip** and then configure CIFS or NFS later.
5. If the **Configure iSCSI protocol** page appears because you enabled iSCSI, click **Skip** and then configure iSCSI later.
6. Configure the FC service and LIFs from the **Configure FC/FCoE protocol** page:

   a. Select the **Configure Data LIFs for FC** check box.

   b. Enter `2` in the **LIFs per node** field.

      Two LIFs are required for each node to ensure availability and data mobility.

   c. Skip the optional **Provision a LUN for FCP storage** area because the LUN is provisioned by Virtual Storage Console for VMware vSphere in a later step.

   d. Click **Submit & Continue**.

7. When the **SVM Administration** appears, configure or defer configuring a separate administrator for this SVM:

   - Click **Skip** and configure an administrator later if desired.
   - Enter the requested information, and then click **Submit & Continue**.

8. Review the **Summary** page, record the LIF information, and then click **OK**.

Zone the FC switches by the host and LIF WWPNs

Zoning the FC switches enables the hosts to connect to the storage and limits the number of paths. You zone the switches using the management interface of the switches.

Before you begin

- You must have administrator credentials for the switches.
- You must know the WWPN of each host initiator port and of each FC LIF for the storage virtual machine (SVM) in which you created the LUN.

About this task

For details about zoning your switches, see the switch vendor's documentation.

You must zone by WWPN, not by physical port. Each initiator port must be in a separate zone with all of its corresponding target ports.

LUNs are mapped to a subset of the initiators in the igroup to limit the number of paths from the host to the LUN.

- By default, ONTAP uses Selective LUN Map to make the LUN accessible only through paths on the node owning the LUN and its HA partner.
- You still must zone all of the FC LIFs on every node for LUN mobility in case the LUN is moved to another node in the cluster.
- When moving a volume or a LUN, you must modify the Selective LUN Map reporting-nodes list before moving.

The following illustration shows a host connected to a four-node cluster. There are two zones, one zone indicated by the solid lines and one zone indicated by the dashed lines. Each zone contains one initiator from the host and a LIF from each storage node.

You must use the WWPNs of the target LIFs, not the WWPNs of the physical FC ports on the storage nodes. The LIF WWPNs are all in the range `2x:xx:00:a0:98:xx:xx:xx`, where `x` is any hexadecimal digit. The physical port WWPNs are all in the range `50:0a:09:8x:xx:xx:xx:xx`.

Steps

1. Log in to the FC switch administration program, and then select the zoning configuration option.
2. Create a new zone that includes the first initiator and all of the FC LIFs that connect to the same FC switch as the initiator.
3. Create additional zones for each FC initiator in the host.
4. Save the zones, and then activate the new zoning configuration.

Provision a datastore and create its containing LUN and volume

A datastore contains virtual machines and their VMDKs on the ESXi host. The datastore on the ESXi host is provisioned on a LUN on the storage cluster.

Before you begin

Virtual Storage Console for VMware vSphere (VSC) must be installed and registered with the vCenter Server that manages the ESXi host.

VSC must have sufficient cluster or storage virtual machine (SVM) credentials to create the LUN and volume.

About this task

VSC automates the datastore provisioning, including creating a LUN and volume on the specified SVM.

Steps

1. From the vSphere Web Client **Home** page, click **Hosts and Clusters**.
2. In the navigation pane, expand the datacenter where you want to provision the datastore.
3. Right-click the ESXi host, and then select **NetApp VSC** > **Provision Datastore**.

   Alternatively, you can right-click the cluster when provisioning to make the datastore available to all hosts in the cluster.

4. Provide the required information in the wizard:

   - Select **VMFS** as the datastore type.
   - Select **FC/FCoE** as the VMFS protocol.
   - Select **None** as the Storage Capability Profile.
   - Select the box for **Thin provision**.
   - Select the **Create new volume** check box.

Verify that the host can write to and read from the LUN

Before using the LUN, you should verify that the host can write data to the LUN and read it back.

About this task

If the cluster node on which the LUN is created can be failed over to its partner node, you should verify reading the data while the node is failed over. This test might not be possible if the cluster is in production use.

Steps

1. On the vSphere Web Client **Home** page, click **Hosts and Clusters**.

2. In the navigation pane, click the **Storage** tab.
3. Expand the datacenter, and then select the new datastore.
4. In the center pane, click **Manage** > **Files**.

   The contents of the datastore are displayed.

5. Create a new folder in the datastore and upload a file to the new folder.

   You might need to install the Client Integration Plug-in.

6. Verify that you can access the file you just wrote.
7. **Optional:** Fail over the cluster node containing the LUN and verify that you can still write and read a file.

   If any of the tests fail, verify that the FC service is running on the storage cluster and check the FC paths to the LUN and FC switch zoning.

8. **Optional:** If you failed over the cluster node, be sure to give back the node and return all LIFs to their home ports.
9. For an ESXi cluster, view the datastore from each ESXi host in the cluster and verify that the file you uploaded is displayed.

Related information

ONTAP 9 High-Availability Configuration

FC configuration for Red Hat Enterprise Linux

FC configuration for Red Hat Enterprise Linux overview

You can quickly set up the FC service on a storage virtual machine (SVM), provision a LUN, and make the LUN available using an FC host bus adapter (HBA) on a Red Hat Enterprise Linux server using the ONTAP System Manager classic interface (ONTAP 9.7 and earlier).

Use this procedure to set up FC service on an SVM if:

- The host is running a supported version of Red Hat Enterprise Linux 6.4 or later.
- You are using traditional FC HBAs and switches.

  Fibre Channel over Ethernet (FCoE) is not covered in this procedure.

- You have at least two FC target ports available on each node in the cluster.
  Onboard FC and UTA2 (also called “CNA”) ports, as well as some adapters, are configurable. Configuring those ports is done in the ONTAP command-line interface (CLI) and is not covered in this procedure.
- You are not configuring FC SAN boot.

If these assumptions are not correct for your situation, you should see the following resources:

- SAN administration

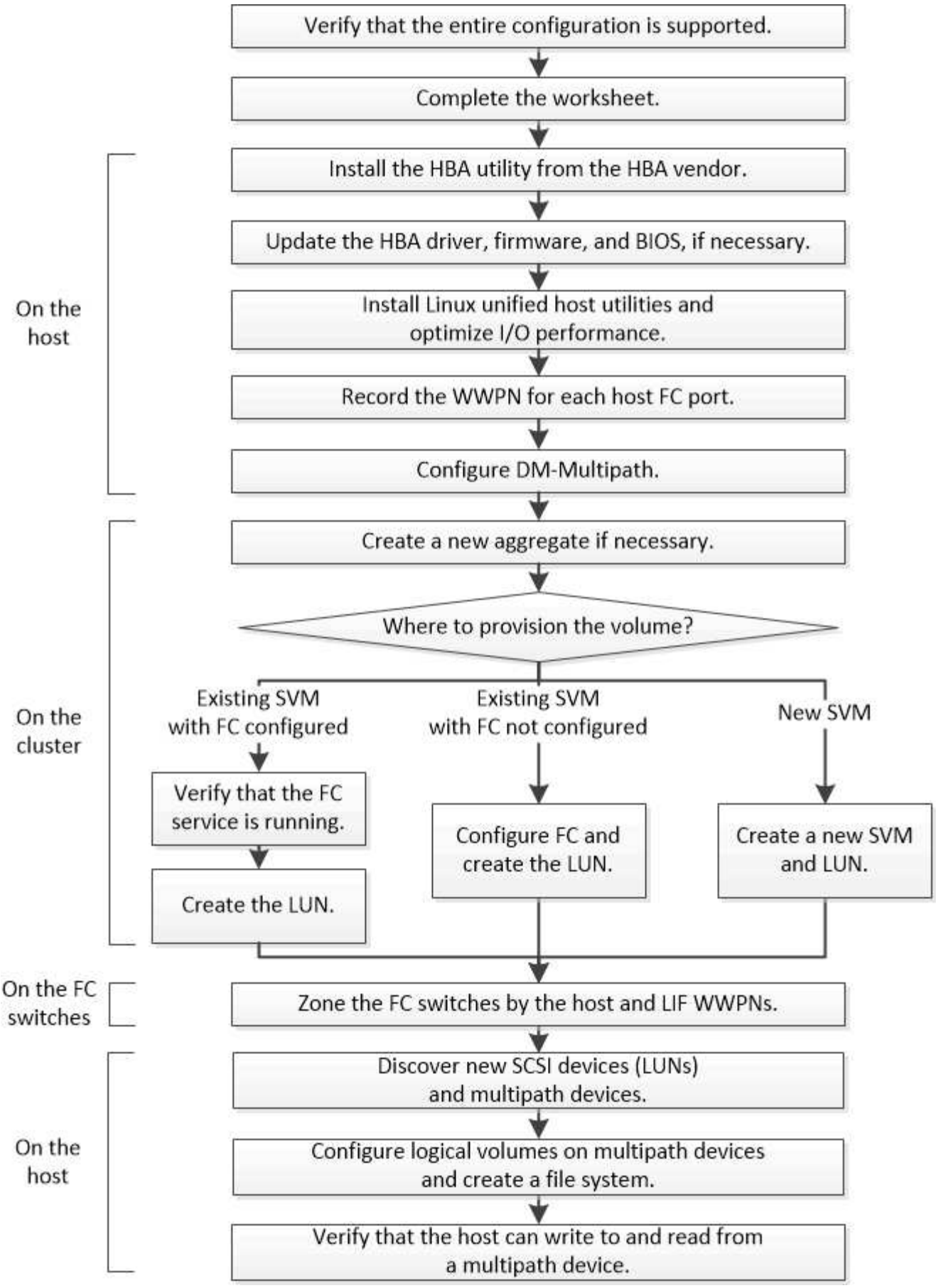
- SAN configuration
- Linux Unified Host Utilities 7.1 Installation

Other ways to do this in ONTAP

To perform these tasks with…	Refer to…
The redesigned System Manager (available with ONTAP 9.7 and later)	Provision SAN storage for Linux servers
The ONTAP command line interface (CLI)	LUN setup workflow with the CLI

FC configuration and provisioning workflow

When you make storage available to a host using FC, you provision a volume and LUN on the storage virtual machine (SVM), and then connect to the LUN from the host.


Verify that the entire configuration is supported.
Complete the worksheet.
Install the HBA utility from the HBA vendor.
Update the HBA driver, firmware, and BIOS, if necessary.
Install Linux unified host utilities and optimize I/O performance.
Record the WWPN for each host FC port.
Configure DM-Multipath.
On the host
Create a new aggregate if necessary.
Where to provision the volume?
Existing SVM with FC configured
Existing SVM with FC not configured
New SVM
Verify that the FC service is running.
Create the LUN.
Configure FC and create the LUN.
Create a new SVM and LUN.
On the cluster
Zone the FC switches by the host and LIF WWPNs.
On the FC switches
Discover new SCSI devices (LUNs) and multipath devices.
Configure logical volumes on multipath devices and create a file system.
Verify that the host can write to and read from a multipath device.
On the host

Verify that the FC configuration is supported

For reliable operation, you must verify that the entire FC configuration is supported.

Steps

1. Go to the Interoperability Matrix to verify that you have a supported combination of the following components:
   - ONTAP software
   - Host computer CPU architecture (for standard rack servers)
   - Specific processor blade model (for blade servers)
   - FC host bus adapter (HBA) model and driver, firmware, and BIOS versions
   - Storage protocol (FC)
   - Linux operating system version
   - DM-Multipath package
   - Linux Unified Host Utilities
2. Select the configuration name for the selected configuration.

   Details for that configuration are displayed in the Configuration Details window.
3. Review the information in the following tabs:
   - Notes

     Lists important alerts and information that are specific to your configuration.

     Review the alerts to identify the packages that are required for your operating system.
   - Policies and Guidelines

     Provides general guidelines for all SAN configurations.

Complete the FC configuration worksheet

You require FC initiator and target WWPNs and storage configuration information to perform FC configuration tasks.

FC host WWPNs

Port	WWPN
Initiator (host) port connected to FC switch 1	
Initiator (host) port connected to FC switch 2	

FC target WWPNs

You require two FC data LIFs for each node in the cluster. The WWPNs are assigned by ONTAP when you create the LIFs as part of creating the storage virtual machine (SVM).

LIF	WWPN
Node 1 LIF with port connected to FC switch 1	
Node 2 LIF with port connected to FC switch 1	
Node 3 LIF with port connected to FC switch 1	
Node 4 LIF with port connected to FC switch 1	
Node 1 LIF with port connected to FC switch 2	
Node 2 LIF with port connected to FC switch 2	
Node 3 LIF with port connected to FC switch 2	
Node 4 LIF with port connected to FC switch 2	

Storage configuration

If the aggregate and SVM are already created, record their names here; otherwise, you can create them as required:

Node to own LUN
Aggregate name
SVM name

LUN information

LUN size
LUN name (optional)
LUN description (optional)

SVM information

If you are not using an existing SVM, you require the following information to create a new one:

SVM name
SVM IPspace
Aggregate for SVM root volume

SVM name	
SVM user name (optional)	
SVM password (optional)	
SVM management LIF (optional)	
	Subnet:
	IP address:
	Network mask:
	Gateway:
	Home node:
	Home port:

Install the HBA utility from the HBA vendor

The HBA utility enables you to view the worldwide port name (WWPN) of each FC port. The utility is also useful for troubleshooting FC issues.

About this task

Each HBA vendor offers an HBA utility for their FC HBAs. You must download the correct version for your host operating system and CPU.

The following is a partial list of HBA utilities:

- Emulex HBA Manager, formerly known as OneCommand Manager, for Emulex HBAs
- QLogic QConvergeConsole for QLogic HBAs

Steps

1. Download the appropriate utility from your HBA vendor's web site.
2. Run the installation program and follow the prompts to complete the installation.

Related information

Broadcom (Emulex) Support Documents and Downloads

Emulex HBA Manager

QLogic: NetApp Downloads

Update the HBA driver, firmware, and BIOS

If the FC host bus adapters (HBAs) in the Linux host are not running supported driver, firmware, and BIOS versions, you must update them.

Before you begin

You must have identified the supported driver, firmware, and BIOS versions for your configuration from the Interoperability Matrix tool.

NetApp Interoperability Matrix Tool

About this task

Drivers, firmware, BIOS, and HBA utilities are provided by the HBA vendors.

Steps

1. List the installed HBA driver, firmware, and BIOS versions by using the HBA utility from your HBA vendor.
2. Download and install the new driver, firmware, and BIOS as needed from the HBA vendor's support site.

   Installation instructions and any required installation utilities are available with the download.

Install Linux Unified Host Utilities and optimize I/O performance

Linux Unified Host Utilities software includes the `sanlun` utility, a NetApp LUN reporting tool that you can use to display information about storage cluster nodesand Host Bus Adapters (HBAs) that are on the Linux host. You must also enable the correct server profile on the Linux host to optimize NetApp storage performance.

Before you begin

You must have identified the supported Linux Unified Host Utilities version for your configuration by using the Interoperability Matrix. You must also have the `tuned` package, which is part of your Linux OS distribution and contains the `tuned-adm` command, which you use to set the server profile on the host.

Steps

1. Download the supported Linux Unified Host Utilities version from the NetApp Support Site.

   NetApp Downloads: Software

2. Install Linux Unified Host Utilities software by following the instructions in the installation documentation.
3. If the `tuned` package is not installed, enter the following command:`yum install tuned`
4. For a physical host, ensure that you have set the `enterprise-storage` profile: `tuned-adm profile enterprise-storage`
5. For a virtual host, ensure that you have set the `virtual-guest` profile: `tuned-adm profile virtual-guest`

   Linux Unified Host Utilities 7.1 Installation

Record the WWPN for each host FC port

The worldwide port name (WWPN) is required to zone the FC switches and to create the

igroups that allow the host to access its LUN.

Before you begin

You must have installed the vendor's HBA utility for the HBAs in your host and verified HBAs are running supported driver, firmware, and BIOS versions for your configuration.

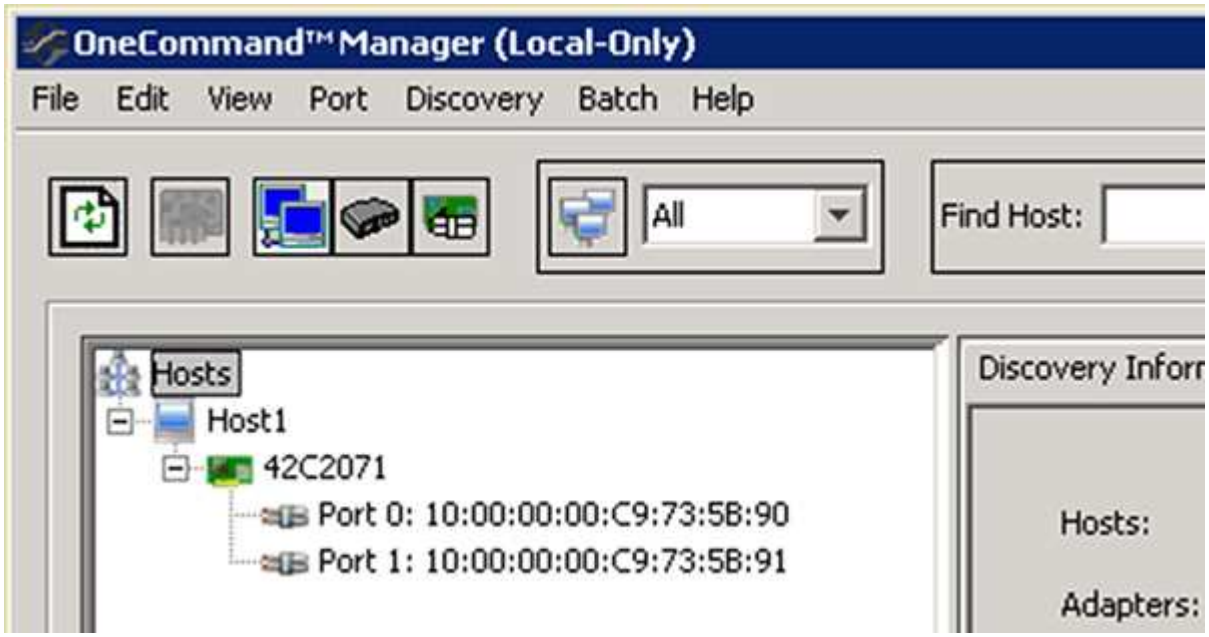
About this task

The WWPN is used for all configuration. You do not have to record the worldwide node name (WWNN).

Steps

1. Run the HBA utility for your FC HBA type.
2. Select the HBA.
3. Record the WWPN of each port.

   The following example shows Emulex HBA Manager, formerly known as OneCommand Manager.



   Other utilities, such as QLogic QConvergeConsole, provide the equivalent information.

4. Repeat the previous step for each FC HBA in the host.

   In Linux, you can also obtain the WWPN by running the `sanlun` utility.

   The following example shows output from the `sanlun` command.

```
# sanlun fcp show adapter -v

adapter name:      host0
**WWPN:              10000000c9813a14**
WWNN:              20000000c9813a14
driver name:       lpfc
model:             LPe12002-M8
model description: Emulex LPe12002-M8 8Gb 2-port PCIe Fibre Channel
Adapter
serial number:     VM84364896
hardware version:  31004549
driver version:    8.3.7.34.3p; HBAAPI(I) v2.3.b, 07-12-10
firmware version:  2.01A12 (U3D2.01A12)
Number of ports:   1
port type:         Fabric
port state:        Operational
supported speed:   2 GBit/sec, 4 GBit/sec, 8 GBit/sec
negotiated speed:  8 GBit/sec
OS device name:    /sys/class/scsi_host/host0

adapter name:      host5
**WWPN:              10000000c9813a15**
WWNN:              20000000c9813a15
driver name:       lpfc
model:             LPe12002-M8
model description: Emulex LPe12002-M8 8Gb 2-port PCIe Fibre Channel
Adapter
serial number:     VM84364896
hardware version:  31004549
driver version:    8.3.7.34.3p; HBAAPI(I) v2.3.b, 07-12-10
firmware version:  2.01A12 (U3D2.01A12)
Number of ports:   1
port type:         Fabric
port state:        Operational
supported speed:   2 GBit/sec, 4 GBit/sec, 8 GBit/sec
negotiated speed:  8 GBit/sec
OS device name:    /sys/class/scsi_host/host5
```

Configure DM-Multipath

DM-Multipath manages multiple paths between the Linux host and the storage cluster. Configuring DM-Multipath on a LUN, which appears to the Linux host as a SCSI device, enables your Linux host to access its LUN on the storage cluster if a path or component fails.

Before you begin

You must have identified the required version of DM-Multipath from the Interoperability Matrix tool.

NetApp Interoperability Matrix Tool

> The recommended approach is that you configure two paths per node into each fabric or Ethernet network. This allows a path to fail without the node switching over to its partner. Using link aggregation (LAG) for the physical ports is not recommended with a Windows-based operating system.

Steps

1. Edit the `/etc/multipath.conf` file as follows:
   a. Determine whether there are non-NetApp SCSI devices to exclude (blacklist).

      These are devices that are not displayed when you enter the `sanlun lun show` command.

      - If there are non-NetApp SCSI devices to exclude, enter the worldwide identifier (WWID) for the devices in the blacklist section of the `multipath.conf` file.

        To display the WWID of a non-NetApp SCSI device, enter the following command on the device that you want to exclude, where `SCSI_device_name` is a device that you specify:

        ```
        /lib/udev/scsi_id -gud /dev/SCSI_device_name
        ```

        For example, if `/dev/sda` is the non-NetApp SCSI device that you want to exclude, you would enter the following:

        ```
        /lib/udev/scsi_id -gud /dev/sda
        ```

        This displays the WWID of the device, which you can copy and paste in the `multipath.conf` file.

        In the following example showing the blacklist section of the `multipath.conf` file, the non-NetApp SCSI device with WWID `3600508e000000000753250f933cc4606` is excluded:

        ```
        blacklist {
                    **wwid       3600508e000000000753250f933cc4606**
                    devnode    "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
                    devnode    "^hd[a-z]"
                    devnode     "^cciss.*"
        }
        ```

      - If there are no devices to exclude, remove the *wwid* line from the `multipath.conf` file.

   b. Enable NetApp recommended DM-Multipath settings by appending the following string to the end of the kernel line in the boot loader:

      ```
      rdloaddriver=scsi_dh_alua
      ```

2. Start the DM-Multipath daemon:

```
/etc/init.d/multipathd start
```

3. Add the multipath service to the boot sequence so that the multipath daemon always starts during system boot:

```
chkconfig multipathd on
```

4. Reboot the Linux host.
5. Verify that the `rdloaddriver` setting appears in the output when you run `cat /proc/cmdline`.

   The `rdloaddriver` setting appears as one of several boot options that are passed to the kernel:

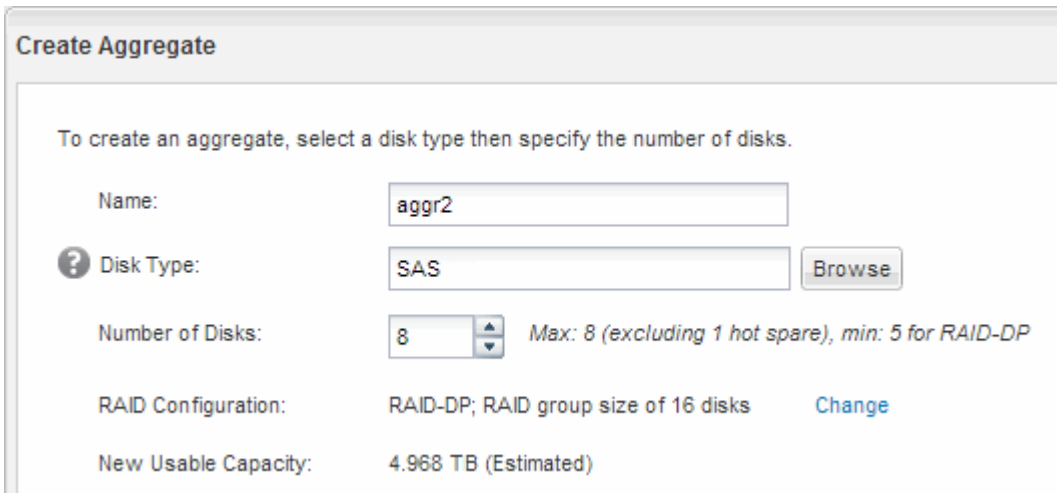
```
# cat /proc/cmdline
ro root=/dev/mapper/vg_ibmx3650210104-lv_root rd_NO_LUKS LANG=en_US.UTF-
8 rd_NO_MD rd_LVM_LV=vg_ibmx3650210104/lv_root SYSFONT=latarcyrheb-sun16
rd_LVM_LV=vg_ibmx3650210104/lv_swap crashkernel=129M@0M  KEYBOARDTYPE=pc
KEYTABLE=us rd_NO_DM rhgb quiet **rdloaddriver=scsi_dh_alua**
```

Create an aggregate

If you do not want to use an existing aggregate, you can create a new aggregate to provide physical storage to the volume which you are provisioning.

Steps

1. Enter the URL `https://IP-address-of-cluster-management-LIF` in a web browser and log in to System Manager using your cluster administrator credential.
2. Navigate to the **Aggregates** window.
3. Select **Create.**
4. Follow the instructions on the screen to create the aggregate using the default RAID-DP configuration, and then select **Create**.



Results

The aggregate is created with the specified configuration and added to the list of aggregates in the Aggregates

window.

Decide where to provision the volume

Before you provision a volume to contain your LUNs, you need to decide whether to add the volume to an existing storage virtual machine (SVM) or to create a new SVM for the volume. You might also need to configure FC on an existing SVM.

About this task

If an existing SVM is already configured with the needed protocols and has LIFs that can be accessed from the host, it is easier to use the existing SVM.

You can create a new SVM to separate data or administration from other users of the storage cluster. There is no advantage to using separate SVMs just to separate different protocols.

Procedure

- If you want to provision volumes on an SVM that is already configured for FC, you must verify that the FC service is running and then create a LUN on the SVM.

  Verifying that the FC service is running on an existing SVM

  Creating a LUN

- If you want to provision volumes on an existing SVM that has FC enabled but not configured, configure iSCSI on the existing SVM.

  Configuring FC on an existing SVM

  This is the case if you did not follow this procedure to create the SVM while configuring a different protocol.

- If you want to provision volumes on a new SVM, create the SVM.

  Creating a new SVM

Verify that the FC service is running on an existing SVM

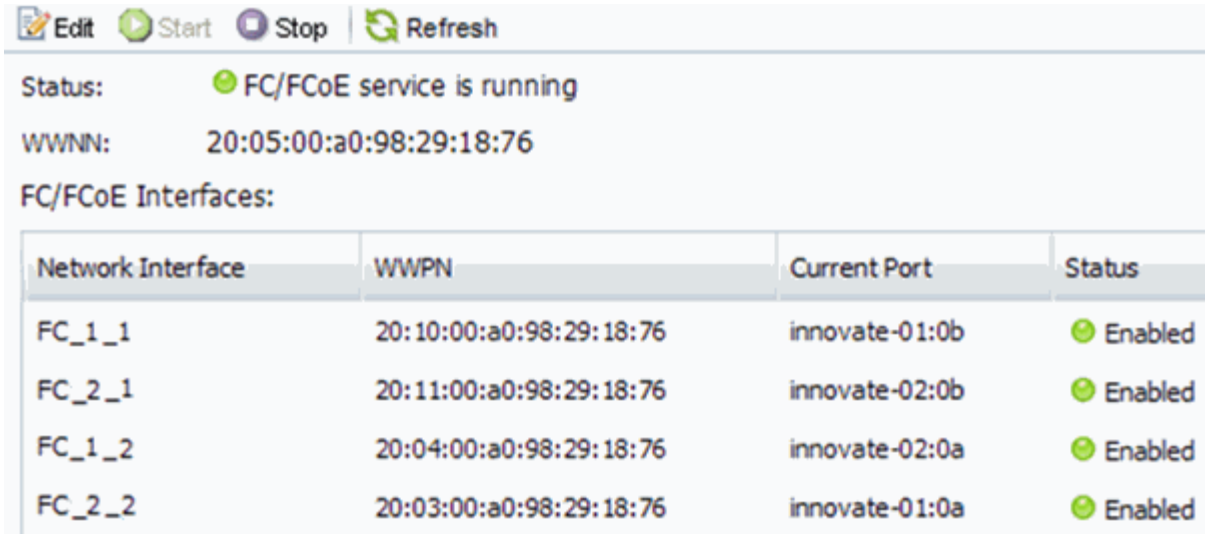
If you choose to use an existing storage virtual machine (SVM), you must verify that the FC service is running on the SVM by using ONTAP System Manager. You must also verify that FC logical interfaces (LIFs) are already created.

Before you begin

You must have selected an existing SVM on which you plan to create a new LUN.

Steps

1. Navigate to the **SVMs** window.
2. Select the required SVM.
3. Select the **SVM Settings** tab.
4. In the **Protocols** pane, select **FC/FCoE**.
5. Verify that the FC service is running.



If the FC service is not running, start the FC service or create a new SVM.

6. Verify that there are at least two FC LIFs listed for each node.

   If there are fewer than two FC LIFs per node, update the FC configuration on the SVM or create a new SVM for FC.

Create a LUN

You use the Create LUN wizard to create a LUN. The wizard also creates the igroup and maps the LUN to the igroup, which enables the specified host to access the LUN.

Before you begin

- There must be an aggregate with enough free space to contain the LUN.
- There must be a storage virtual machine (SVM) with the FC protocol enabled and the appropriate logical interfaces (LIFs) created.
- You must have recorded the worldwide port names (WWPNs) of the host FC ports.

About this task

If your organization has a naming convention, you should use names for the LUN, volume, and so on that fit your convention. Otherwise, you should accept the default names.

Steps

1. Navigate to the **LUNs** window.
2. Select **Create.**
3. Browse and select an SVM in which you want to create the LUNs.

   The Create LUN Wizard is displayed.

4. On the **General Properties** page, select the LUN type **Linux** for LUNs used directly by the Linux host.

   Leave the **Thin Provisioned** check box unselected.

5. On the **LUN Container** page, select an existing FlexVol volume.

   You must ensure that there is enough space in the volume. If sufficient space is not available in the existing volumes, you can create a new volume.

6. On the **Initiators Mapping** page, select **Add Initiator Group**, enter the required information on the **General** tab, and then on the **Initiators** tab, enter all the WWPNs of the host FC ports that you recorded.
7. Confirm the details, and then select **Finish** to complete the wizard.

Related information

System administration

Configure FC on an existing SVM

You can configure FC on an existing storage virtual machine (SVM)and create a LUN and its containing volume with a single wizard. The FC protocol must already be enabled but not configured on the SVM. This information is intended for SVMs for which you are configuring multiple protocols, but have not yet configured FC.

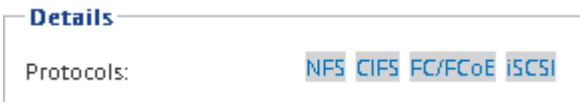
Before you begin

Your FC fabric must be configured and the desired physical ports must be connected to the fabric.

Steps

1. Navigate to the **SVMs** window.
2. Select the SVM that you want to configure.
3. In the SVM**Details** pane, verify that **FC/FCoE** is displayed with a gray background, which indicates that the protocol is enabled but not fully configured.

   If **FC/FCoE** is displayed with a green background, the SVM is already configured.



4. Select the **FC/FCoE** protocol link with the gray background.

   The Configure FC/FCoE Protocol window is displayed.

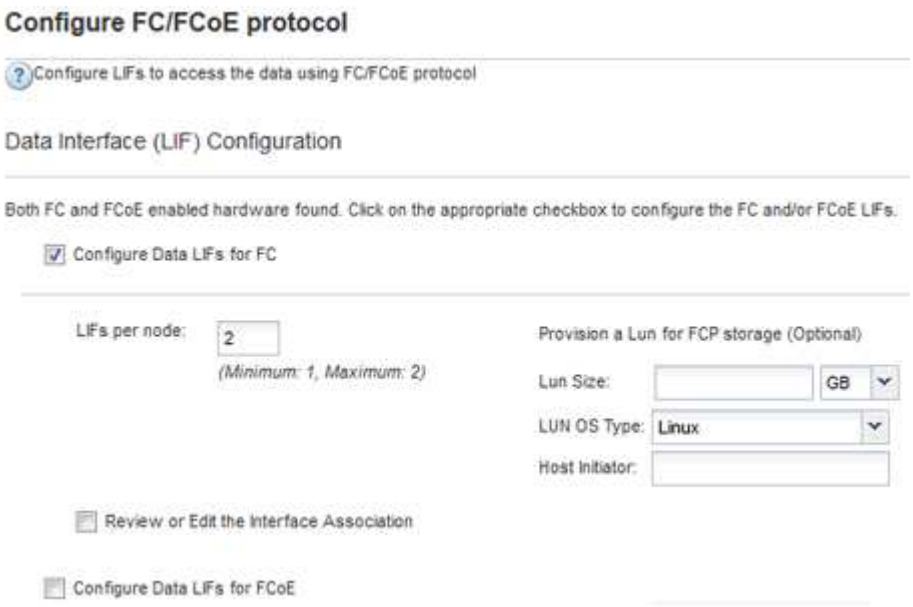
5. Configure the FC service and LIFs from the **Configure FC/FCoE protocol** page:

   a. Select the **Configure Data LIFs for FC** check box.

b. Enter 2 in the **LIFs per node** field.

   Two LIFs are required for each node, to ensure availability and data mobility.

c. Select **Submit & Close**.



6. Review the **Summary** page, record the LIF information, and then select **OK**.

Create a new SVM

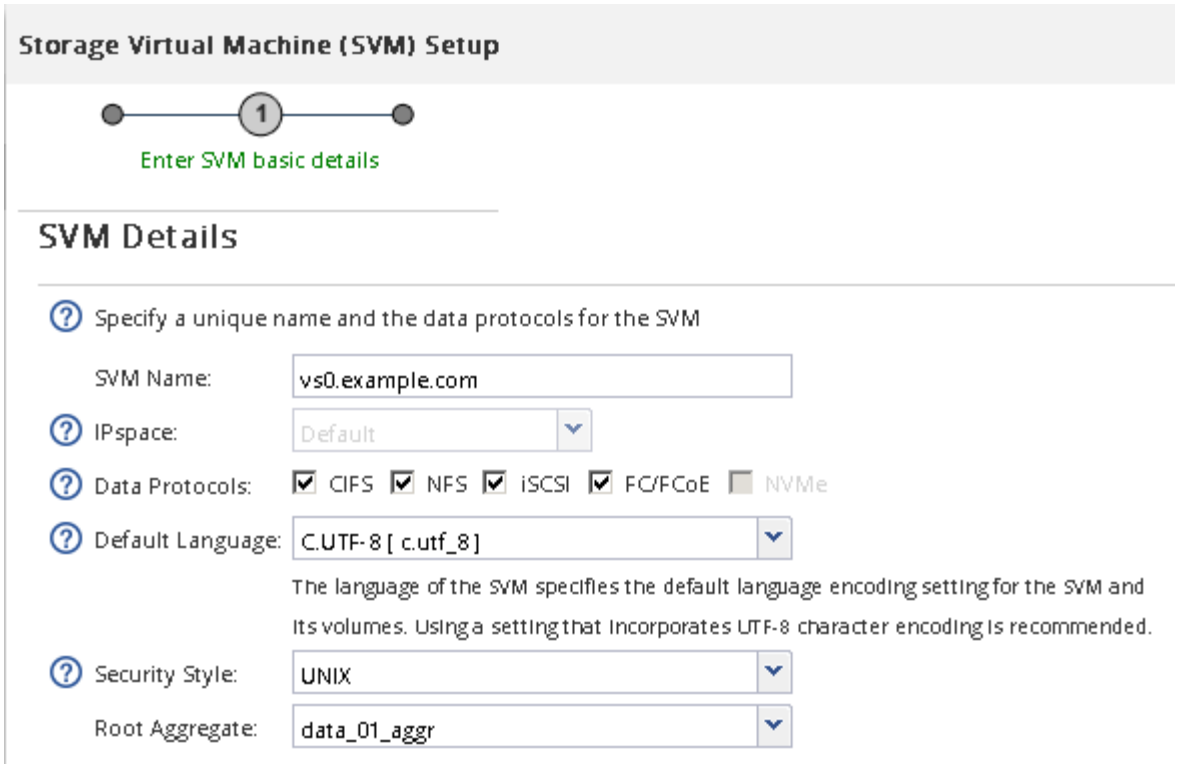
The storage virtual machine (SVM) provides the FC target through which a host accesses LUNs. When you create the SVM, you also create logical interfaces (LIFs) and the LUN and its containing volume. You can create an SVM to separate the data and administration functions of a user from those of the other users in a cluster.

Before you begin

- Your FC fabric must be configured and the desired physical ports must be connected to the fabric.

Steps

1. Navigate to the **SVMs** window.
2. Select **Create**.
3. In the **Storage Virtual Machine (SVM) Setup** window, create the SVM:



a. Specify a unique name for the SVM.

   The name must either be a fully qualified domain name (FQDN) or follow another convention that ensures unique names across a cluster.

b. Select the IPspace that the SVM will belong to.

   If the cluster does not use multiple IPspaces, the “Default” IPspace is used.

c. Keep the default volume type selection.

   Only FlexVol volumes are supported with SAN protocols.

d. Select all of the protocols that you have licenses for and that you might use on the SVM, even if you do not want to configure all of the protocols immediately.

   Selecting both NFS and CIFS when you create the SVM enables these two protocols to share the same LIFs. Adding these protocols later does not allow them to share LIFs.

   If CIFS is one of the protocols you selected, then the security style is set to NTFS. Otherwise, the security style is set to UNIX.

e. Keep the default language setting C.UTF-8.

f. Select the desired root aggregate to contain the SVM root volume.

   The aggregate for the data volume is selected separately in a later step.

g. Select **Submit & Continue**.

The SVM is created, but protocols are not yet configured.

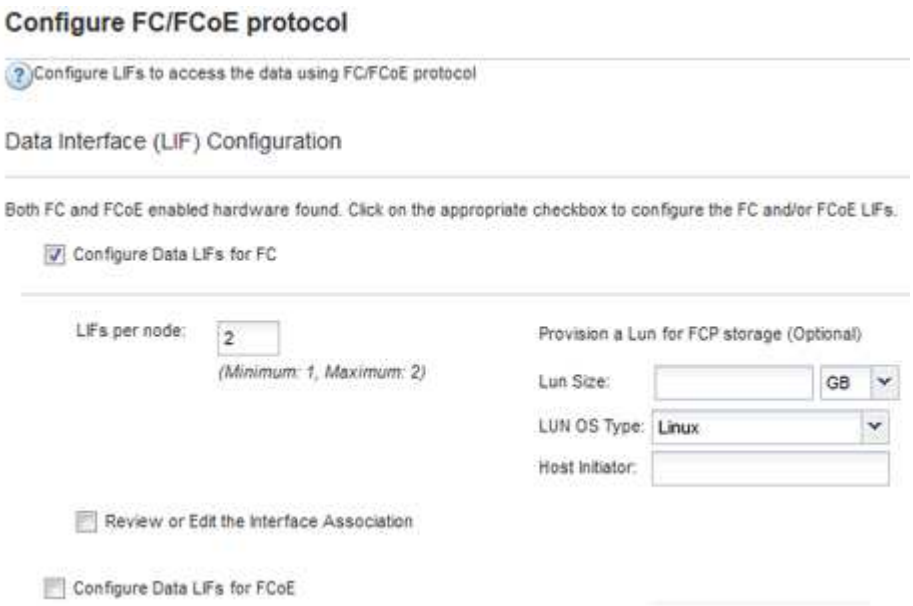
4. If the **Configure CIFS/NFS protocol** page appears because you enabled CIFS or NFS, select **Skip** and

then configure CIFS or NFS later.

5. If the **Configure iSCSI protocol** page appears because you enabled iSCSI, select **Skip** and then configure iSCSI later.
6. Configure the FC service and create LIFs, and the LUN and its containing volume from the **Configure FC/FCoE protocol** page:
   a. Select the **Configure Data LIFs for FC** check box.
   b. Enter **2** in the **LIFs per node** field.

      Two LIFs are required for each node to ensure availability and data mobility.

   c. In the **Provision a LUN for FCP storage** area, enter the desired LUN size, host type, and WWPNs of the host initiators.
   d. Select **Submit & Continue**.



7. When the **SVM Administration** appears, configure or defer configuring a separate administrator for this SVM:
   - Select **Skip** and configure an administrator later if desired.
   - Enter the requested information, and then select **Submit & Continue**.
8. Review the **Summary** page, record the LIF information, and then select **OK**.

Zone the FC switches by the host and LIF WWPNs

Zoning the FC switches enables the hosts to connect to the storage and limits the number of paths. You zone the switches using the management interface of the switches.

Before you begin

- You must have administrator credentials for the switches.
- You must know the WWPN of each host initiator port and of each FC LIF for the storage virtual machine (SVM) in which you created the LUN.

About this task

For details about zoning your switches, see the switch vendor's documentation.

You must zone by WWPN, not by physical port. Each initiator port must be in a separate zone with all of its corresponding target ports.

LUNs are mapped to a subset of the initiators in the igroup to limit the number of paths from the host to the LUN.

- By default, ONTAP uses Selective LUN Map to make the LUN accessible only through paths on the node owning the LUN and its HA partner.
- You still must zone all of the FC LIFs on every node for LUN mobility in case the LUN is moved to another node in the cluster.
- When moving a volume or a LUN, you must modify the Selective LUN Map reporting-nodes list before moving.

The following illustration shows a host connected to a four-node cluster. There are two zones, one zone indicated by the solid lines and one zone indicated by the dashed lines. Each zone contains one initiator from the host and a LIF from each storage node.

You must use the WWPNs of the target LIFs, not the WWPNs of the physical FC ports on the storage nodes. The LIF WWPNs are all in the range `2x:xx:00:a0:98:xx:xx:xx`, where `x` is any hexadecimal digit. The physical port WWPNs are all in the range `50:0a:09:8x:xx:xx:xx:xx`.

Steps

1. Log in to the FC switch administration program, and then select the zoning configuration option.
2. Create a new zone that includes the first initiator and all of the FC LIFs that connect to the same FC switch as the initiator.
3. Create additional zones for each FC initiator in the host.
4. Save the zones, and then activate the new zoning configuration.

Discover new SCSI devices (LUNs) and multipath devices

LUNs on the storage cluster appear to the Linux host as SCSI devices, which are I/O paths that DM-Multipath aggregates into a new device, called a multipath device. The host does not automatically discover new SCSI devices (LUNs) that you add to your system. You must manually rescan them to discover them.

Before you begin

You must have a copy of the `rescan` script, which is in the `sg3_utils` package that is part of your Linux OS distribution.

Steps

1. Discover new SCSI devices (LUNs) and create the corresponding multipath devices for the LUNs: `/usr/bin/rescan-scsi-bus.sh`
2. Verify DM-Multipath configuration:

   ```
   multipath -ll
   ```

   This displays the following type of output, listing the recommended settings for each NetApp LUN:

```
3600a0980324666546e2b443251655177 dm-2 NETAPP,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='round-robin 0' prio=50 status=active
| |- 0:0:1:0 sdb 8:16  active ready  running
| |- 0:0:0:0 sda 8:0   active ready  running
| |- 1:0:0:0 sde 8:64  active ready  running
| `- 1:0:1:0 sdf 8:80  active ready  running
`-+- policy='round-robin 0' prio=10 status=enabled
  |- 0:0:3:0 sdd 8:48  active ready  running
  |- 1:0:3:0 sdh 8:112 active ready  running
  |- 0:0:2:0 sdc 8:32  active ready  running
  `- 1:0:2:0 sdg 8:96  active ready  running
```

Configure logical volumes on multipath devices and creating a file system

When the Linux host first accesses a new SCSI device (LUN), there is no partition or file system. If you want to use a partitioned multipath device, you must first partition the underlying SCSI devices. You might also want to create logical volumes on multipath devices, and optionally create a file system.

Before you begin

SCSI devices and corresponding multipath devices must have been discovered by the Linux host.

About this task

At a minimum DM-Multipath should be configured on the SCSI devices. Any configuration beyond DM-Multipath is optional. The following steps are general guidelines if you wish to perform additional configuration, such as partitioning, configuring logical volumes on multipath devices, and creating a file system. For details on Linux commands, refer to Red Hat Enterprise Linux documentation and man pages.

Steps

1. To use a partitioned multipath device, first partition the underlying SCSI devices using the `fdisk` or `parted` utility.
2. Create corresponding multipath partitions using the `kpartx` utility.
3. Create logical volumes on corresponding multipath devices using Logical Volume Manager (LVM) commands.
4. Create a file system, such as Ext4 or XFS, on logical volumes or multipath devices using the `mkfs` utility.

Verify that the host can write to and read from a multipath device

Before using a multipath device, you should verify that the host can write data to the multipath device and read it back.

Before you begin

DM-Multipath must be configured on the Linux host for the storage cluster nodes you are accessing.

About this task

If the storage cluster node that the multipath device corresponds to can be failed over to its partner node, you should verify reading the data while the node is failed over. This verification might not be possible if the storage cluster is in production use.

Steps

1. Run some I/O on the specified multipath device:

   ```
   dd if=/dev/zero of=<multipath_device_name\>
   ```

2. Verify that I/O is running on the multipath device, specifying the number of seconds to refresh statistics (for example, every two seconds, as shown):

   ```
   iostat 2
   ```

   When I/O is running on the multipath device, you can see the various I/O counters output change dynamically, indicating that I/O is running successfully on the multipath device.

   ```
   avg-cpu:  %user   %nice %system %iowait  %steal   %idle
              0.00    0.00    0.01    0.00    0.00   99.98

   Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
   sda               0.18         1.34         2.29     832606    1428026
   dm-0              0.37         1.29         2.29     801530    1427984
   dm-1              0.00         0.00         0.00       2576          0
   dm-2              0.00         0.00         0.00       1770         24
   sdd               0.17         1.18        17.87     734688   11128584
   sde               0.17         1.18        18.01     734560   11219016
   sdf               0.00         0.00         0.00       1344          0
   sdg               0.00         0.00         0.00       1344          0
   dm-3              0.68         4.71        71.96    2932496   44816008
   sdh               0.17         1.18        18.22     734360   11343920
   sdi               0.17         1.18        17.86     734272   11124488
   sdj               0.00         0.00         0.00       1344          0
   sdk               0.00         0.00         0.00       1344          0
   ..............
   ```

3. If possible, run the `takeover` command on the storage cluster node:

   ```
   storage failover takeover -ofnode <node_name\>
   ```

4. Verify that I/O is still running on the multipath device by re-running the`iostat` command.
5. Run the `giveback` command on the storage cluster node:

   ```
   storage failover giveback -ofnode <node_name\>
   ```

6. Check `iostat` output to verify that I/O is still running.

What to do next

If any of the tests fail, verify that the FC service is running and re-check the DM-Multipath configuration and the FC paths to the multipath device.

FC configuration for Windows

FC configuration for Windows overview

You can quickly set up the FC service on a storage virtual machine (SVM), provision a LUN, and make the LUN available using an FC HBA on a Windows host computer with the ONTAP System Manager classic interface (ONTAP 9.7 and earlier).

Use this procedure to set up FC service on an SVM if:

- You are using traditional FC HBAs and switches.

This procedure does not covers situations where:

- You have at least two FC target ports available on each node in the cluster.
  Onboard FC and UTA2 (also called `CNA`) ports, as well as some adapters are configurable. Configuring those ports is done in the ONTAP CLI and is not covered in this procedure.
- You are not configuring FC SAN boot.
- You are not using virtual Fibre Channel (VFC) with Hyper-V or ESX guests.

Other ways to do this in ONTAP

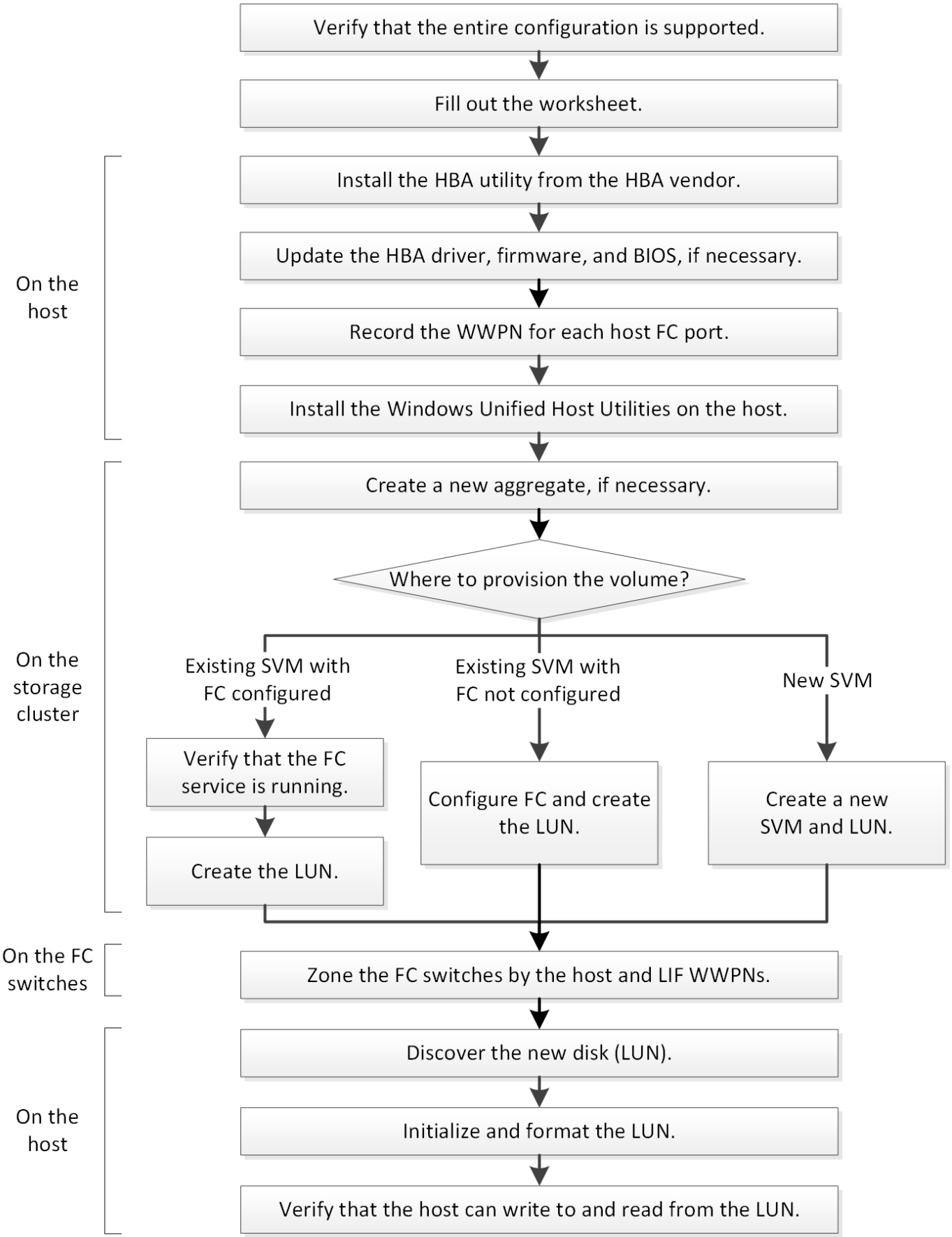
To perform these tasks with…	Refer to…
The redesigned System Manager (available with ONTAP 9.7 and later)	Provision SAN storage for Windows servers
The ONTAP command line interface (CLI)	LUN setup workflow with the CLI

Additional Resources

- NetApp Documentation: Host Utilities

FC configuration workflow

When you make storage available to a host using FC, you provision a volume and LUN on the storage virtual machine (SVM), and then connect to the LUN from the host.


Verify that the entire configuration is supported.
Fill out the worksheet.
Install the HBA utility from the HBA vendor.
Update the HBA driver, firmware, and BIOS, if necessary.
Record the WWPN for each host FC port.
Install the Windows Unified Host Utilities on the host.
Create a new aggregate, if necessary.
Where to provision the volume?
Existing SVM with FC configured
Existing SVM with FC not configured
New SVM
Verify that the FC service is running.
Create the LUN.
Configure FC and create the LUN.
Create a new SVM and LUN.
Zone the FC switches by the host and LIF WWPNs.
Discover the new disk (LUN).
Initialize and format the LUN.
Verify that the host can write to and read from the LUN.
On the host
On the storage cluster
On the FC switches
On the host

Verify that the FC configuration is supported

For reliable operation, you must verify that the entire FC configuration is supported.

Steps

1. Go to the Interoperability Matrix to verify that you have a supported combination of the following components:
   - ONTAP software
   - Host computer CPU architecture (for standard rack servers)
   - Specific processor blade model (for blade servers)
   - FC host bus adapter (HBA) model and driver, firmware, and BIOS versions
   - Storage protocol (FC)
   - Windows operating system version
   - Windows Unified Host Utilities
2. Click the configuration name for the selected configuration.

   Details for that configuration are displayed in the Configuration Details window.
3. Review the information in the following tabs:
   - Notes

     Lists important alerts and information that are specific to your configuration.

     Review the alerts to identify the hotfixes that are required for your operating system.
   - Policies and Guidelines

     Provides general guidelines for all SAN configurations.

Complete the FC configuration worksheet

You require FC initiator and target WWPNs and storage configuration information to perform FC configuration tasks.

FC host WWPNs

Port	WWPN
Initiator (host) port connected to FC switch 1	
Initiator (host) port connected to FC switch 2	

FC target WWPNs

You require two FC data LIFs for each node in the cluster. The WWPNs are assigned by ONTAP when you create the LIFs as part of creating the storage virtual machine (SVM).

LIF	WWPN
Node 1 LIF with port connected to FC switch 1	
Node 2 LIF with port connected to FC switch 1	
Node 3 LIF with port connected to FC switch 1	
Node 4 LIF with port connected to FC switch 1	
Node 1 LIF with port connected to FC switch 2	
Node 2 LIF with port connected to FC switch 2	
Node 3 LIF with port connected to FC switch 2	
Node 4 LIF with port connected to FC switch 2	

Storage configuration

If the aggregate and SVM are already created, record their names here; otherwise, you can create them as required:

Node to own LUN
Aggregate name
SVM name

LUN information

LUN size
Host operating system
LUN name (optional)
LUN description (optional)

SVM information

If you are not using an existing SVM, you require the following information to create a new one:

SVM name
SVM IPspace

SVM name	
Aggregate for SVM root volume	
SVM user name (optional)	
SVM password (optional)	
SVM management LIF (optional)	
	Subnet:
	IP address:
	Network mask:
	Gateway:
	Home node:
	Home port:

Install the HBA utility from the HBA vendor

The HBA utility enables you to view the worldwide port name (WWPN) of each FC port. The utility is also useful for troubleshooting FC issues.

About this task

Each HBA vendor offers an HBA utility for their FC HBAs. You must download the correct version for your host operating system and CPU.

The following is a partial list of HBA utilities:

- Emulex HBA Manager, formerly known as OneCommand Manager, for Emulex HBAs
- QLogic QConvergeConsole for QLogic HBAs

Steps

1. Download the appropriate utility from your HBA vendor's web site.
2. Run the installation program and follow the prompts to complete the installation.

Related information

Broadcom (Emulex) Support Documents and Downloads

Emulex HBA Manager

QLogic: NetApp Downloads

Update the HBA driver, firmware, and BIOS

If the FC host bus adapters (HBAs) in the Windows host are not running supported driver, firmware, and BIOS versions, you must update them.

Before you begin

You must have identified the supported driver, firmware, and BIOS versions for your configuration from the Interoperability Matrix tool.

NetApp Interoperability Matrix Tool

About this task

Drivers, firmware, BIOS, and HBA utilities are provided by the HBA vendors.

Steps

1. List the installed HBA driver, firmware, and BIOS versions by using the HBA utility from your HBA vendor.
2. Download and install the new driver, firmware, and BIOS as needed from the HBA vendor's support site.

   Installation instructions and any required installation utilities are available with the download.

Record the WWPN for each host FC port

The worldwide port name (WWPN) is required to zone the FC switches and to create the igroups that allow the host to access its LUN.

Before you begin

You must have installed the vendor's HBA utility for the HBAs in your host and verified HBAs are running supported driver, firmware, and BIOS versions for your configuration.

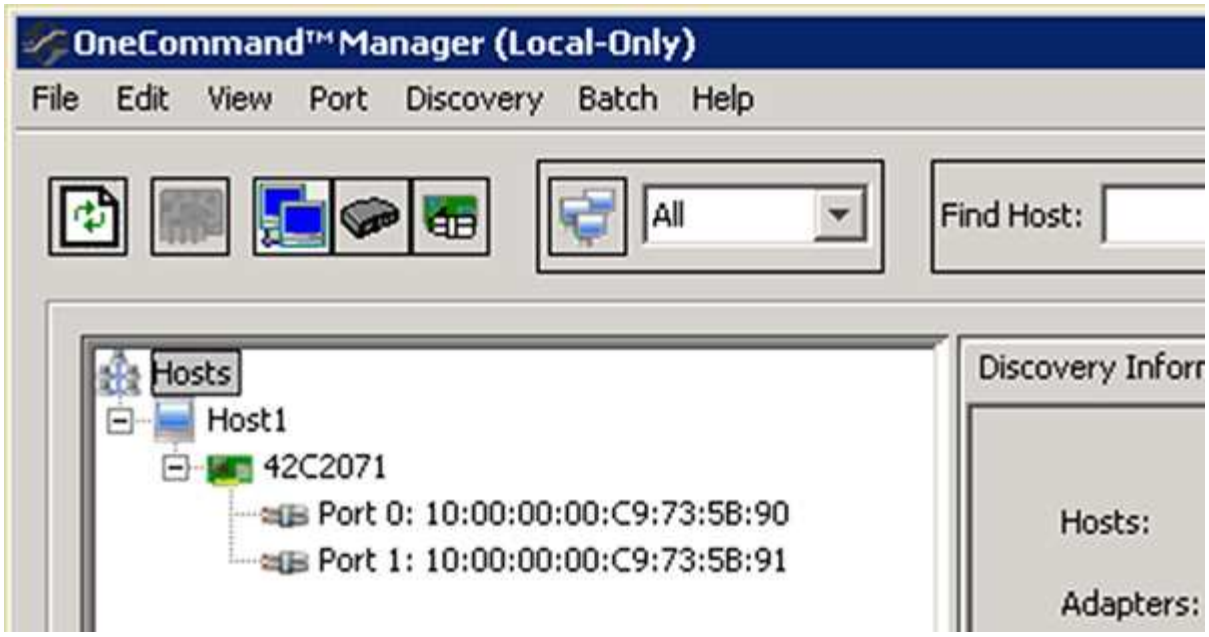
About this task

The WWPN is used for all configuration. You do not have to record the worldwide node name (WWNN).

Steps

1. Run the HBA utility for your FC HBA type.
2. Select the HBA.
3. Record the WWPN of each port.

   The following example shows Emulex HBA Manager, formerly known as OneCommand Manager.



Other utilities, such as QLogic QConvergeConsole, provide the equivalent information.

4. Repeat the previous step for each FC HBA in the host.

Install Windows Unified Host Utilities

Windows Unified Host Utilities includes an installation program that sets the required Windows registry and HBA parameters so that the Windows host correctly handles the storage system behaviors for NetApp ONTAP and E-Series platforms.

Before you begin

You must have completed the following tasks:

- Check the supported configuration in the Interoperability Matrix

  NetApp Interoperability Matrix Tool

- Identified any required Windows hotfixes from the Interoperability Matrix

  NetApp Interoperability Matrix Tool

- Add the FCP license and start the target service
- Verify your cabling

  See *SAN Configuration* for your version of ONTAP or *Hardware Cabling* for your E-Series storage system on the NetApp Support Site for detailed cabling and configuration information.

About this task

You must specify whether to include multipathing support when you install the Windows Unified Host Utilities software package. Choose MPIO if you have more than one path from the Windows host or virtual machine to the storage system. Choose no MPIO only if you are using a single path to the storage system.

The MPIO selection is not available for Windows XP and Windows Vista systems; multipath I/O is not supported on these guest operating systems.

For Hyper-V guests, raw (pass-through) disks do not appear in the guest OS if you choose multipathing support. You can either use raw disks, or you can use MPIO, but you cannot use both in the guest OS.

Detailed installation information is available in Windows Unified Host Installation.

NetApp Support

Steps

1. Download the appropriate version of the Windows Unified Host Utilities from the NetApp Support Site.

   NetApp Support

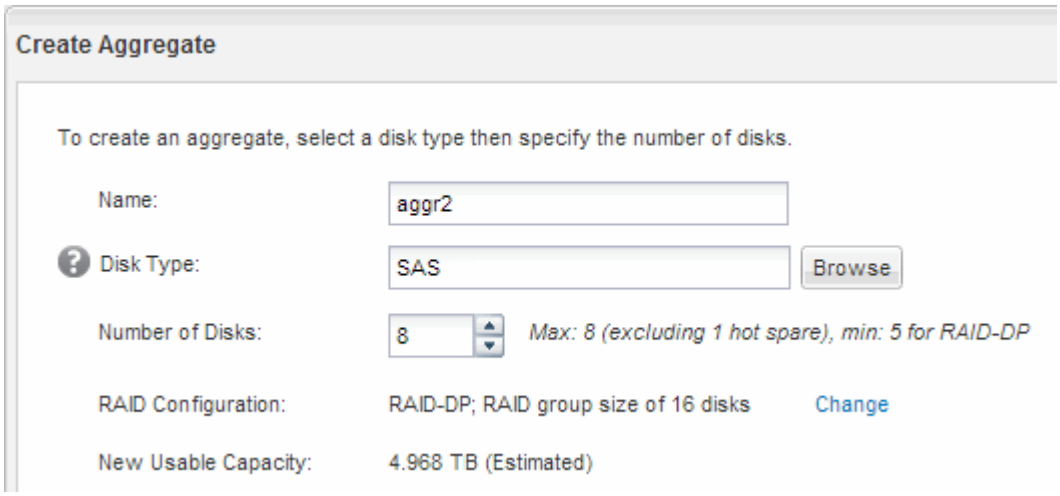
2. Run the executable file and follow the instructions on the screen.
3. Reboot the Windows host when prompted.

Create an aggregate

If you do not want to use an existing aggregate, you can create a new aggregate to provide physical storage to the volume which you are provisioning.

Steps

1. Enter the URL `https://IP-address-of-cluster-management-LIF` in a web browser and log in to System Manager using your cluster administrator credential.
2. Navigate to the **Aggregates** window.
3. Click **Create.**
4. Follow the instructions on the screen to create the aggregate using the default RAID-DP configuration, and then click **Create**.



Results

The aggregate is created with the specified configuration and added to the list of aggregates in the Aggregates window.

Decide where to provision the volume

Before you provision a volume to contain your LUNs, you need to decide whether to add the volume to an existing storage virtual machine (SVM) or to create a new SVM for the volume. You might also need to configure FC on an existing SVM.

About this task

If an existing SVM is already configured with the needed protocols and has LIFs that can be accessed from the host, it is easier to use the existing SVM.

You can create a new SVM to separate data or administration from other users of the storage cluster. There is no advantage to using separate SVMs just to separate different protocols.

Procedure

- If you want to provision volumes on an SVM that is already configured for FC, you must verify that the FC service is running and then create a LUN on the SVM.

  Verifying that the FC service is running on an existing SVM

  Creating a LUN

- If you want to provision volumes on an existing SVM that has FC enabled but not configured, configure iSCSI on the existing SVM.

  Configuring FC on an existing SVM

  This is the case when you did not follow the procedure to create the SVM while configuring a different protocol.

- If you want to provision volumes on a new SVM, create the SVM.

  Creating a new SVM

Verify that the FC service is running on an existing SVM

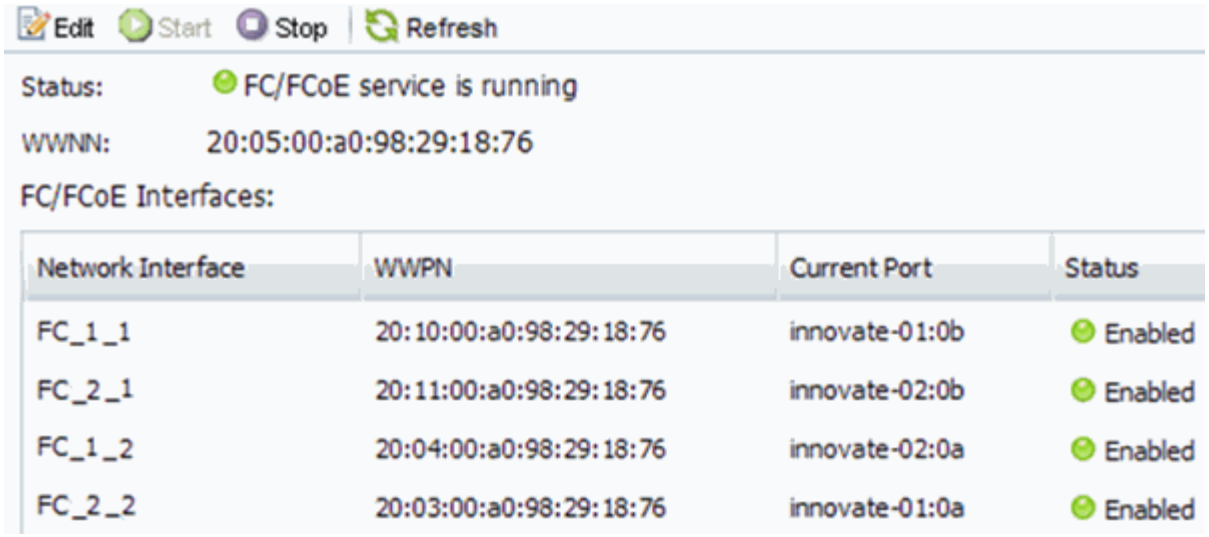
If you choose to use an existing storage virtual machine (SVM), you must verify that the FC service is running on the SVM by using ONTAP System Manager. You must also verify that FC logical interfaces (LIFs) are already created.

Before you begin

You must have selected an existing SVM on which you plan to create a new LUN.

Steps

1. Navigate to the **SVMs** window.
2. Select the required SVM.
3. Click the **SVM Settings** tab.
4. In the **Protocols** pane, click **FC/FCoE**.
5. Verify that the FC service is running.



If the FC service is not running, start the FC service or create a new SVM.

6. Verify that there are at least two FC LIFs listed for each node.

   If there are fewer than two FC LIFs per node, update the FC configuration on the SVM or create a new SVM for FC.

Create a LUN

You use the Create LUN wizard to create a LUN. The wizard also creates the igroup and maps the LUN to the igroup, which enables the specified host to access the LUN.

Before you begin

- There must be an aggregate with enough free space to contain the LUN.
- There must be a storage virtual machine (SVM) with the FC protocol enabled and the appropriate logical interfaces (LIFs) created.
- You must have recorded the worldwide port names (WWPNs) of the host FC ports.

About this task

If your organization has a naming convention, you should use names for the LUN, volume, and so on that fit your convention. Otherwise, you should accept the default names.

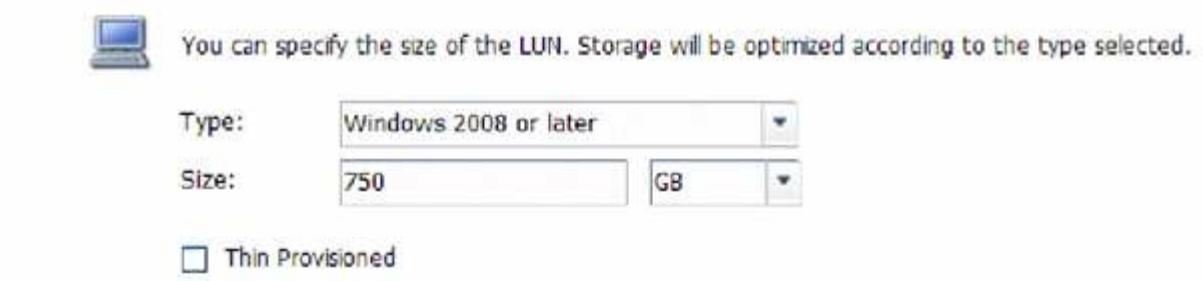
Steps

1. Navigate to the **LUNs** window.
2. Click **Create.**
3. Browse and select an SVM in which you want to create the LUNs.

   The Create LUN Wizard is displayed.

4. On the **General Properties** page, select the LUN type **Windows 2008 or later** for LUNs used directly by the Windows host, or select **Hyper-V** for LUNs containing virtual hard disks (VHDs) for Hyper-V virtual machines.

   Leave the **Thin Provisioned** check box unselected.



5. On the **LUN Container** page, select an existing FlexVol volume.

   You must ensure that there is enough space in the volume. If sufficient space is not available in the existing volumes, you can create a new volume.

6. On the **Initiators Mapping** page, click **Add Initiator Group**, enter the required information on the **General** tab, and then on the **Initiators** tab, enter all the WWPNs of the host FC ports that you recorded.
7. Confirm the details, and then click **Finish** to complete the wizard.

Related information

System administration

Configure FC on an existing SVM

You can configure FC on an existing storage virtual machine (SVM)and create a LUN and its containing volume with a single wizard. The FC protocol must already be enabled but not configured on the SVM. This information is intended for SVMs for which you are configuring multiple protocols, but have not yet configured FC.

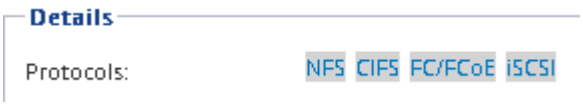
Before you begin

Your FC fabric must be configured and the desired physical ports must be connected to the fabric.

Steps

1. Navigate to the **SVMs** window.
2. Select the SVM that you want to configure.
3. In the SVM**Details** pane, verify that **FC/FCoE** is displayed with a gray background, which indicates that the protocol is enabled but not fully configured.

   If **FC/FCoE** is displayed with a green background, the SVM is already configured.



4. Click the **FC/FCoE** protocol link with the gray background.

   The Configure FC/FCoE Protocol window is displayed.

5. Configure the FC service and LIFs from the **Configure FC/FCoE protocol** page:

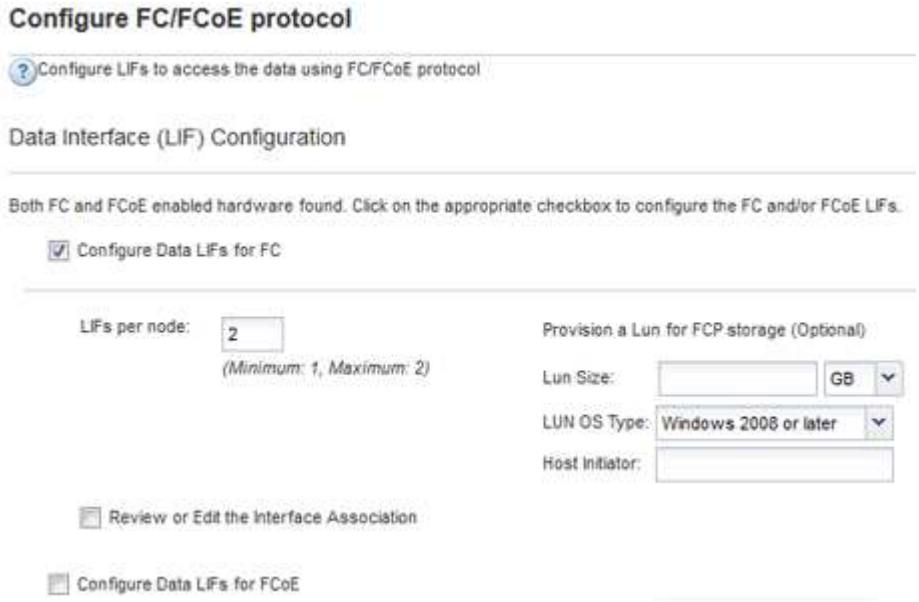
   a. Select the **Configure Data LIFs for FC** check box.

b. Enter 2 in the **LIFs per node** field.

   Two LIFs are required for each node, to ensure availability and data mobility.

c. In the **Provision a LUN for FCP storage** area, enter the desired LUN size, host type, and WWPNs of the host initiators.

d. Click **Submit & Close**.



6. Review the **Summary** page, record the LIF information, and then click **OK**.

Create a new SVM

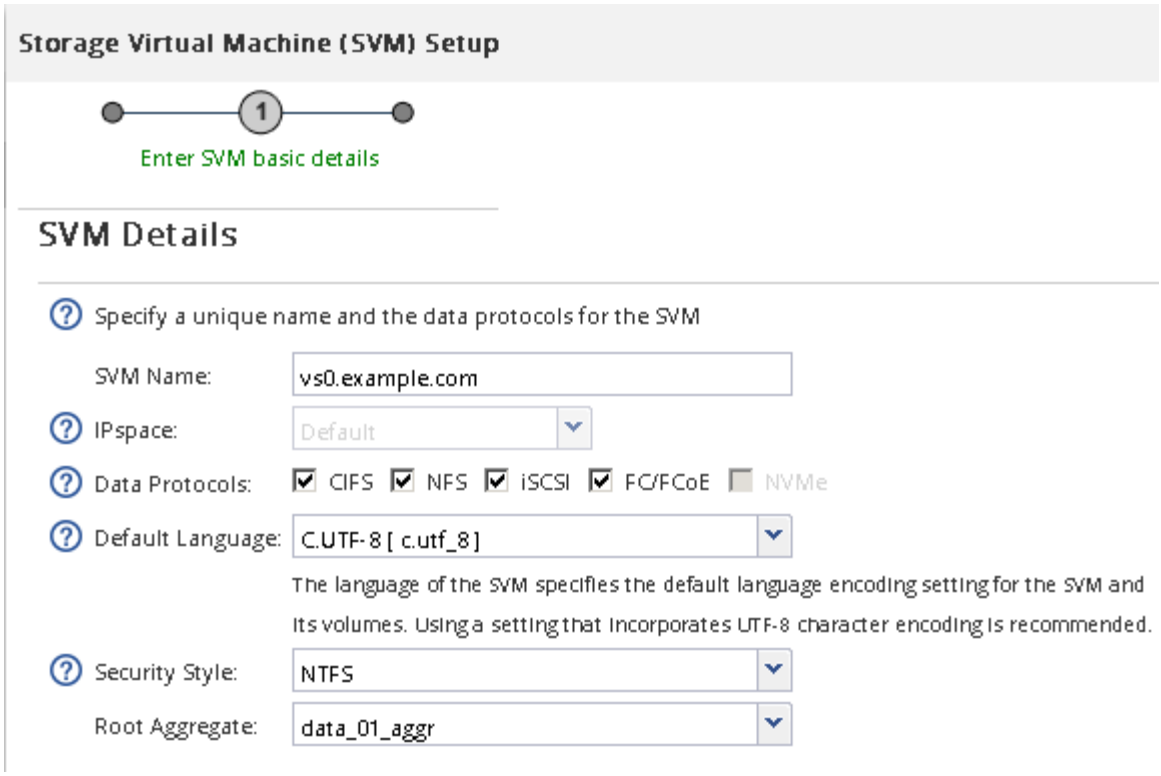
The storage virtual machine (SVM) provides the FC target through which a host accesses LUNs. When you create the SVM, you also create logical interfaces (LIFs) and the LUN and its containing volume. You can create an SVM to separate the data and administration functions of a user from those of the other users in a cluster.

Before you begin

- Your FC fabric must be configured and the desired physical ports must be connected to the fabric.

Steps

1. Navigate to the **SVMs** window.
2. Click **Create**.
3. In the **Storage Virtual Machine (SVM) Setup** window, create the SVM:



a. Specify a unique name for the SVM.

   The name must either be a fully qualified domain name (FQDN) or follow another convention that ensures unique names across a cluster.

b. Select the IPspace that the SVM will belong to.

   If the cluster does not use multiple IPspaces, the “Default” IPspace is used.

c. Keep the default volume type selection.

   Only FlexVol volumes are supported with SAN protocols.

d. Select all of the protocols that you have licenses for and that you might use on the SVM, even if you do not want to configure all of the protocols immediately.

   Selecting both NFS and CIFS when you create the SVM enables these two protocols to share the same LIFs. Adding these protocols later does not allow them to share LIFs.

   If CIFS is one of the protocols you selected, then the security style is set to NTFS. Otherwise, the security style is set to UNIX.

e. Keep the default language setting C.UTF-8.

f. Select the desired root aggregate to contain the SVM root volume.

   The aggregate for the data volume is selected separately in a later step.

g. Click **Submit & Continue**.

The SVM is created, but protocols are not yet configured.

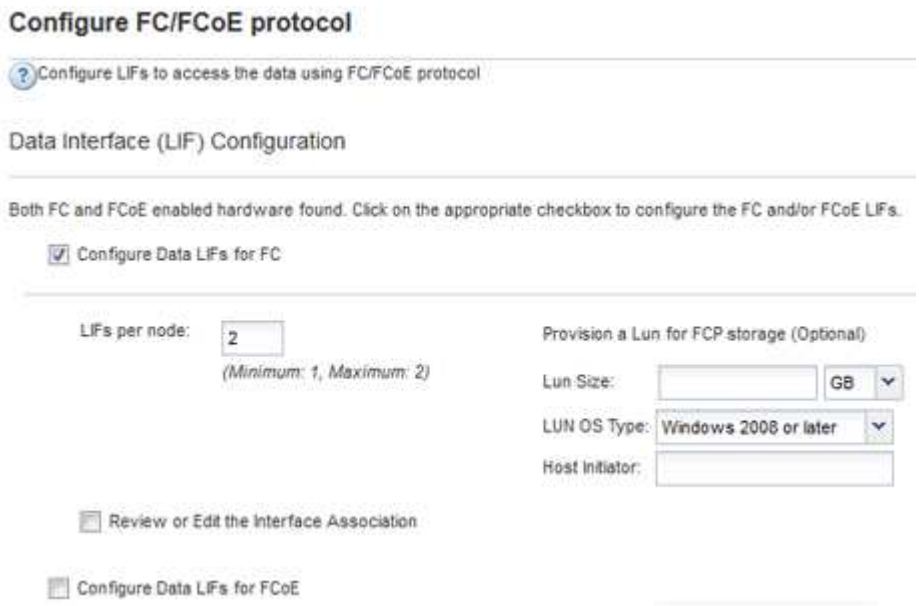
4. If the **Configure CIFS/NFS protocol** page appears because you enabled CIFS or NFS, click **Skip** and

then configure CIFS or NFS later.

5. If the **Configure iSCSI protocol** page appears because you enabled iSCSI, click **Skip** and then configure iSCSI later.
6. Configure the FC service and create LIFs, and the LUN and its containing volume from the **Configure FC/FCoE protocol** page:
   a. Select the **Configure Data LIFs for FC** check box.
   b. Enter **2** in the **LIFs per node** field.

      Two LIFs are required for each node to ensure availability and data mobility.

   c. In the **Provision a LUN for FCP storage** area, enter the desired LUN size, host type, and WWPNs of the host initiators.
   d. Click **Submit & Continue**.



7. When the **SVM Administration** appears, configure or defer configuring a separate administrator for this SVM:
   - Click **Skip** and configure an administrator later if desired.
   - Enter the requested information, and then click **Submit & Continue**.
8. Review the **Summary** page, record the LIF information, and then click **OK**.

Zone the FC switches by the host and LIF WWPNs

Zoning the FC switches enables the hosts to connect to the storage and limits the number of paths. You zone the switches using the management interface of the switches.

Before you begin

- You must have administrator credentials for the switches.
- You must know the WWPN of each host initiator port and of each FC LIF for the storage virtual machine (SVM) in which you created the LUN.

About this task

For details about zoning your switches, see the switch vendor's documentation.

You must zone by WWPN, not by physical port. Each initiator port must be in a separate zone with all of its corresponding target ports.

LUNs are mapped to a subset of the initiators in the igroup to limit the number of paths from the host to the LUN.

- By default, ONTAP uses Selective LUN Map to make the LUN accessible only through paths on the node owning the LUN and its HA partner.
- You still must zone all of the FC LIFs on every node for LUN mobility in case the LUN is moved to another node in the cluster.
- When moving a volume or a LUN, you must modify the Selective LUN Map reporting-nodes list before moving.

The following illustration shows a host connected to a four-node cluster. There are two zones, one zone indicated by the solid lines and one zone indicated by the dashed lines. Each zone contains one initiator from the host and a LIF from each storage node.

You must use the WWPNs of the target LIFs, not the WWPNs of the physical FC ports on the storage nodes. The LIF WWPNs are all in the range `2x:xx:00:a0:98:xx:xx:xx`, where `x` is any hexadecimal digit. The physical port WWPNs are all in the range `50:0a:09:8x:xx:xx:xx:xx`.

Steps

1. Log in to the FC switch administration program, and then select the zoning configuration option.
2. Create a new zone that includes the first initiator and all of the FC LIFs that connect to the same FC switch as the initiator.
3. Create additional zones for each FC initiator in the host.
4. Save the zones, and then activate the new zoning configuration.

Discover new disks

LUNs on your storage virtual machine (SVM) appear as disks to the Windows host. Any new disks for LUNs you add to your system are not automatically discovered by the host. You must manually rescan disks to discover them.

Steps

1. Open the Windows Computer Management utility:

If you are using…	Navigate to…
Windows Server 2012	**Tools** > **Computer Management**
Windows Server 2008	**Start** > **Administrative Tools** > **Computer Management**
Windows Server 2016	**Start > Administrative Tools > Computer Management**

2. Expand the **Storage** node in the navigation tree.
3. Click **Disk Management**.
4. Click **Action** > **Rescan Disks**.

Initialize and format the LUN

When a new LUN is first accessed by the Windows host, it has no partition or file system. You must initialize the LUN, and optionally format it with a file system.

Before you begin

The LUN must have been discovered by the Windows host.

About this task

LUNs appear in Windows Disk Management as disks.

You can initialize the disk as a basic disk with a GPT or MBR partition table.

You typically format the LUN with a file system such as NTFS, but some applications use raw disks instead.

Steps

1. Start Windows Disk Management.
2. Right-click the LUN, and then select the required disk or partition type.
3. Follow the instructions in the wizard.

   If you choose to format the LUN as NTFS, you must select the **Perform a quick format** check box.

Verify that the host can write to and read from the LUN

Before using the LUN, you should verify that the host can write data to the LUN and read it back.

Before you begin

The LUN must be initialized and formatted with a file system.

About this task

If the storage cluster node on which the LUN is created can be failed over to its partner node, you should verify reading the data while the node is failed over. This test might not be possible if the storage cluster is in production use.

If any of the tests fail, you should verify that the FC service is running and check the FC paths to the LUN.

Steps

1. On the host, copy one or more files to the LUN.
2. Copy the files back to a different folder on the original disk.
3. Compare the copied files to the original.

   You can use the `comp` command at the Windows command prompt to compare two files.

4. **Optional:** Fail over the storage cluster node containing the LUN and verify that you can still access the

files on the LUN.

5. Use the native DSM to view the paths to the LUN and verify that you have the expected number of paths.

   You should see two paths to the storage cluster node on which the LUN is created, and two paths to the partner node.

iSCSI configuration for ESXi using VSC

iSCSI configuration for ESXi using VSC overview

Using the ONTAP System Manager classic interface (ONTAP 9.7 and earlier), you can quickly set up the iSCSI service on a storage virtual machine (SVM), provision a LUN, and make the LUN available using an iSCSI initiator on an ESXi host computer.

Use this procedure if:

- You are using the native ESXi iSCSI software initiator on ESXi 5.x.
- You are not using CHAP authentication for iSCSI.
- You are using a supported version of Virtual Storage Console for VMware vSphere (VSC) to configure storage settings for your ESX host.
  - Beginning with VSC 7.0, VSC is part of the ONTAP Tools for VMware vSphere virtual appliance, which includes VSC, vStorage APIs for Storage Awareness (VASA) Provider, and Storage Replication Adapter (SRA) for VMware vSphere capabilities.
  - Be sure to check the NetApp Interoperability Matrix Tool to confirm compatibility between your current ONTAP and VSC releases.
- Your network uses IPv4 addressing.
- You want to assign addresses to logical interfaces using any of the following methods:
  - Automatically from a subnet you define
  - Manually, using an address selected from an existing subnet
  - Manually, using an address that will be added to an existing subnet
- You have at least two high-speed Ethernet ports (1 GbE minimum, 10 GbE recommended) available on each node in the cluster.

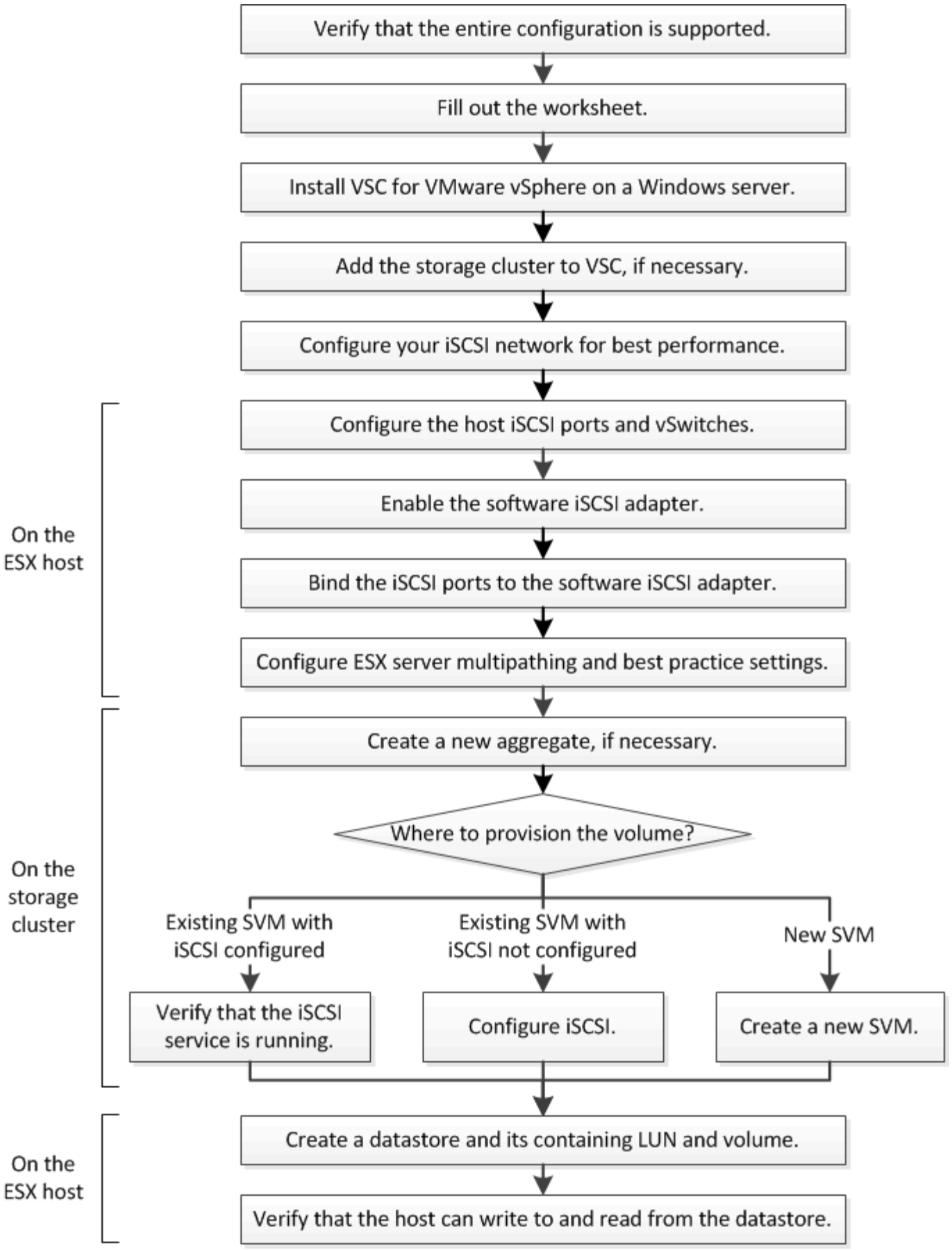
  Onboard UTA2 (also called `CNA`) ports are configurable. You configure those ports in the ONTAP CLI; that process is not covered in his procedure.

  See Network Management for using the CLI to configure Ethernet port flow control.
- You are not configuring iSCSI SAN boot.
- You are providing storage to VMs through the ESXi hypervisor and not running an iSCSI initiator within the VM.

For more information, see TR-4597: VMware vSphere for ONTAP and the documentation for your VSC release.

iSCSI configuration workflow

When you make storage available to an ESXi host using iSCSI, you provision a volume and LUN on the storage virtual machine (SVM) using Virtual Storage Console for VMware vSphere, and then connect to the LUN from the host.


Verify that the entire configuration is supported.
Fill out the worksheet.
Install VSC for VMware vSphere on a Windows server.
Add the storage cluster to VSC, if necessary.
Configure your iSCSI network for best performance.
Configure the host iSCSI ports and vSwitches.
Enable the software iSCSI adapter.
Bind the iSCSI ports to the software iSCSI adapter.
Configure ESX server multipathing and best practice settings.
On the ESX host
Create a new aggregate, if necessary.
Where to provision the volume?
Existing SVM with iSCSI configured
Existing SVM with iSCSI not configured
New SVM
Verify that the iSCSI service is running.
Configure iSCSI.
Create a new SVM.
On the storage cluster
Create a datastore and its containing LUN and volume.
Verify that the host can write to and read from the datastore.
On the ESX host

Verify that the iSCSI configuration is supported

For reliable operation, you must verify that the entire iSCSI configuration is supported.

Steps

1. Go to the Interoperability Matrix to verify that you have a supported combination of the following components:
   - ONTAP software
   - Host computer CPU architecture (for standard rack servers)
   - Specific processor blade model (for blade servers)
   - Storage protocol (iSCSI)
   - ESXi operating system version
   - Guest operating system type and version
   - Virtual Storage Console (VSC) for VMware vSphere software
   - Windows Server version to run VSC
2. Click the configuration name for the selected configuration.

   Details for that configuration are displayed in the Configuration Details window.
3. Review the information in the following tabs:
   - Notes

     Lists important alerts and information that are specific to your configuration.
   - Policies and Guidelines

     Provides general guidelines for all SAN configurations.

Completing the iSCSI configuration worksheet

You require network addresses and storage configuration information to perform iSCSI configuration tasks.

Target network addresses

The storage virtual machine (SVM) is the iSCSI target.

You require a subnet with two IP addresses for iSCSI data LIFs for each node in the cluster. There should be two separate networks for high availability. The specific IP addresses are assigned by ONTAP when you create the LIFs as part of creating the SVM.

If possible, separate iSCSI traffic on separate physical networks or on VLANs.

Subnet for LIFs:

Node or LIF with port to switch	IP address	Network mask	Gateway	VLAN ID	Home port
Node 1 / LIF to switch 1					
Node 2 / LIF to switch 1					
Node 3 / LIF to switch 1					
Node 4 / LIF to switch 1					
Node 1 / LIF to switch 2					
Node 2 / LIF to switch 2					
Node 3 / LIF to switch 2					
Node 4 / LIF to switch 2					

Storage configuration

If the aggregate and SVM are already created, record their names here; otherwise, you can create them as required:

Node to own LUN
Aggregate name
SVM name

LUN information

LUN size
LUN name (optional)
LUN description (optional)

SVM information

If you are not using an existing SVM, you require the following information to create a new one:

SVM name	
SVM IPspace	
Aggregate for SVM root volume	
SVM user name (optional)	
SVM password (optional)	
SVM management LIF (optional)	
	Subnet:
	IP address:
	Network mask:
	Gateway:
	Home node:
	Home port:

Install Virtual Storage Console

Virtual Storage Console for VMware vSphere automates many of the configuration and provisioning tasks required to use NetApp iSCSI storage with an ESXi host. Virtual Storage Console is a plug-in to vCenter Server.

Before you begin

You must have administrator credentials on the vCenter Server used to manage the ESXi host.

About this task

- Virtual Storage Console is installed as a virtual appliance that includes Virtual Storage Console, vStorage APIs for Storage Awareness (VASA) Provider, and Storage Replication Adapter (SRA) for VMware vSphere capabilities.

Steps

1. Download the version of Virtual Storage Console that is supported for your configuration, as shown in the Interoperability Matrix tool.

   NetApp Support

2. Deploy the virtual appliance and configure it following the steps in the *Deployment and Setup Guide*.

Add the storage cluster or SVM to VSC for VMware vSphere

Before you can provision the first datastore to an ESXi host in your Datacenter, you must add the cluster or a specific storage virtual machine (SVM) to Virtual Storage Console for VMware vSphere. Adding the cluster enables you to provision storage on any SVM in the cluster.

Before you begin

You must have administrator credentials for the storage cluster or the SVM that is being added.

About this task

Depending on your configuration, the cluster might have been discovered automatically, or might have already been added.

Steps

1. Log in to the vSphere Web Client.
2. Select **Virtual Storage Console**.
3. Select **Storage Systems** and then click the **Add** icon.
4. In the **Add Storage System** dialog box, enter the host name and administrator credentials for the storage cluster or SVM and then click **OK**.

Configure your network for best performance

Ethernet networks vary greatly in performance. You can maximize the performance of the network used for iSCSI by selecting specific configuration values.

Steps

1. Connect the host and storage ports to the same network.

   It is best to connect to the same switches. Routing should never be used.

2. Select the highest speed ports available, and dedicate them to iSCSI.

   10 GbE ports are best. 1 GbE ports are the minimum.

3. Disable Ethernet flow control for all ports.

   You should see ONTAP 9 Network Management for using the CLI to configure Ethernet port flow control.

4. Enable jumbo frames (typically MTU of 9000).

   All devices in the data path, including initiators, targets, and switches, must support jumbo frames. Otherwise, enabling jumbo frames actually reduces network performance substantially.

Configure host iSCSI ports and vSwitches

The ESXi host requires network ports for the iSCSI connections to the storage cluster.

About this task

It is recommended that you use IP Hash as the NIC teaming policy, which requires a single VMkernel port on a single vSwitch.

The host ports and storage cluster ports used for iSCSI must have IP addresses in the same subnet.

This task lists the high-level steps for configuring the ESXi host. If you require more detailed instructions, see the VMware publication *VMware vSphere Storage* for your version of ESXi.

VMware

Steps

1. Log in to the vSphere Client, and then select the ESXi host from the inventory pane.
2. On the **Manage** tab, click **Networking**.
3. Click **Add Networking**, and then select **VMkernel** and **Create a vSphere standard switch** to create the VMkernel port and vSwitch.
4. Configure jumbo frames for the vSwitch (MTU size of 9000, if used).
5. Repeat the previous step to create a second VMkernel port and vSwitch.

Enable the iSCSI software adapter

The iSCSI software adapter creates the iSCSI connection on the ESXi host. It is built into the operating system, but must be enabled before it can be used.

Before you begin

You must have a VMware vSphere Client installed on your workstation or you must have access to a vSphere Web Client.

Steps

1. Log in to the vSphere Client.
2. Select the ESX host from the inventory pane.
3. Click **Configuration** > **Storage Adapters**.
4. Select the iSCSI software adapter and click **Properties** > **Configure**.
5. Select **Enabled** and then click **OK**.

Bind iSCSI ports to the iSCSI software adapter

The ports you created for iSCSI must be associated with the iSCSI software adapter to support multipathing.

Before you begin

- The iSCSI VMkernel ports must be created.
- The iSCSI software adapter must be enabled on the ESXi host.

About this task

You can bind the iSCSI ports using the vSphere Client.

For detailed instructions, see *VMware vSphere Storage* for your version of ESXi 5 from VMware.

VMware

Steps

1. Bind the first iSCSI port to the iSCSI software adapter by using the **Network Port Binding** tab of the iSCSI software adapter **Adapter Details** dialog box in the vSphere Client.
2. Bind the second iSCSI port to the iSCSI software adapter.

Configure the ESXi host best practice settings

You must ensure that the host multipathing and best practice settings are correct so that the ESXi host can correctly manage the loss of an iSCSI connection or a storage failover event.

Steps

1. From the VMware vSphere Web Client **Home** page, click **vCenter** > **Hosts**.
2. Right-click the host, and then select **Actions** > **NetApp VSC** > **Set Recommended Values**.
3. In the **NetApp Recommended Settings** dialog box, ensure that all of the options are selected, and then click **OK**.

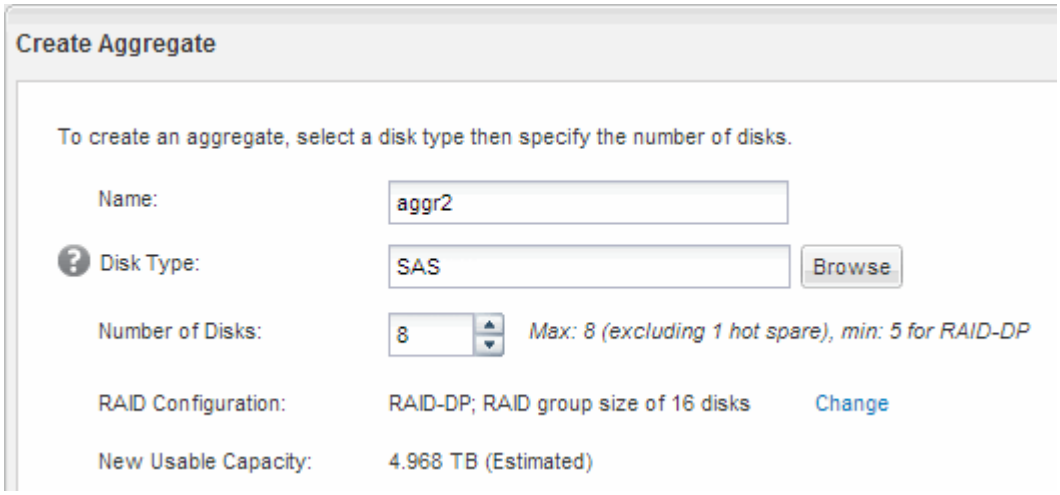
   The vCenter Web Client displays the task progress.

Create an aggregate

If you do not want to use an existing aggregate, you can create a new aggregate to provide physical storage to the volume which you are provisioning.

Steps

1. Enter the URL `https://IP-address-of-cluster-management-LIF` in a web browser and log in to System Manager using your cluster administrator credential.
2. Navigate to the **Aggregates** window.
3. Click **Create.**
4. Follow the instructions on the screen to create the aggregate using the default RAID-DP configuration, and then click **Create**.



Results

The aggregate is created with the specified configuration and added to the list of aggregates in the Aggregates

window.

Decide where to provision the volume

Before you provision a volume to contain your LUNs, you need to decide whether to add the volume to an existing storage virtual machine (SVM) or to create a new SVM for the volume. You might also need to configure iSCSI on an existing SVM.

About this task

If an existing SVM is already configured with the needed protocols and has LIFs that can be accessed from the host, it is easier to use the existing SVM.

You can create a new SVM to separate data or administration from other users of the storage cluster. There is no advantage to using separate SVMs just to separate different protocols.

Procedure

- If you want to provision volumes on an SVM that is already configured for iSCSI, you must verify that the iSCSI service is running.

  Verifying that the iSCSI service is running on an existing SVM

- If you want to provision volumes on an existing SVM that has iSCSI enabled but not configured, configure iSCSI on the existing SVM.

  Configuring iSCSI on an existing SVM

  This is the case when you did not follow this procedure to create the SVM while configuring a different protocol.

- If you want to provision volumes on a new SVM, create a new SVM.

Verify that the iSCSI service is running on an existing SVM

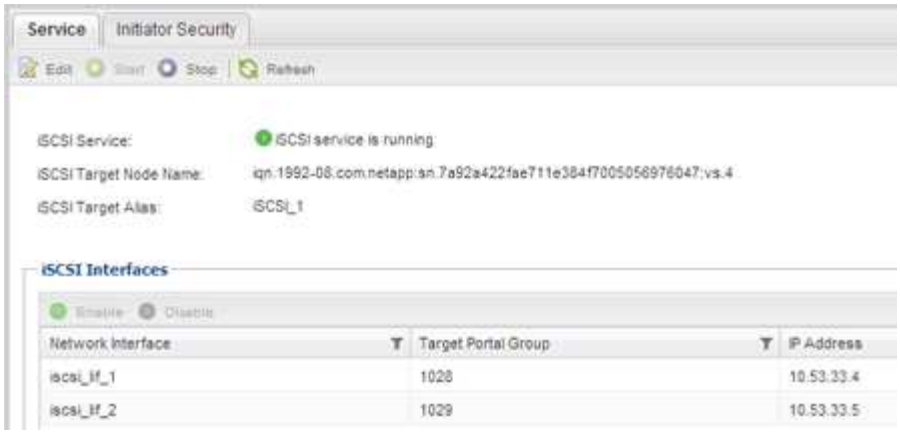
If you choose to use an existing storage virtual machine (SVM), you must verify that the iSCSI service is running on the SVM.

Before you begin

You must have selected an existing SVM on which you plan to create a new LUN.

Steps

1. Navigate to the **SVMs** window.
2. Click the **SVM Settings** tab.
3. In the **Protocols** pane, click **iSCSI**.
4. Verify that the iSCSI service is running.



5. Record the iSCSI interfaces listed for the SVM.

What to do next

If the iSCSI service is not running, start the iSCSI service or create a new SVM.

If there are fewer than two iSCSI interfaces per node, update the iSCSI configuration on the SVM or create a new SVM for iSCSI.

Configure iSCSI on an existing SVM

You can configure iSCSI on an existing storage virtual machine (SVM). The iSCSI protocol must already be enabled but not configured on the SVM. This information is intended for SVMs for which you are configuring multiple protocols, but have not yet configured iSCSI.

Before you begin

You must have enough network addresses available to create two LIFs for each node.

Steps

1. Navigate to the **SVMs** window.
2. Select the SVM that you want to configure.
3. In the SVM **Details** pane, verify that **iSCSI** is displayed with a gray background, which indicates that the protocol is enabled but not fully configured.

   If **iSCSI** is displayed with a green background, the SVM is already configured.

4. Click the **iSCSI** protocol link with the gray background.

   The Configure iSCSI Protocol window is displayed.

5. Configure the iSCSI service and LIFs from the **Configure iSCSI protocol** page:
   a. Enter a target alias name.
   b. Enter **2** in the **LIFs per node** field.

Two LIFs are required for each node to ensure availability and data mobility.

c. Assign IP addresses for the LIFs either with a subnet or without a subnet.

d. Ignore the optional **Provision a LUN for iSCSI storage** area, because the LUN is provisioned by Virtual Storage Console for VMware vSphere in a later step.

e. Click **Submit & Close**.

6. Review the **Summary** page, record the LIF information, and then click **OK**.

Create a new SVM

The storage virtual machine (SVM) provides the iSCSI target through which a host accesses LUNs. When you create the SVM, you also create logical interfaces (LIFs) that provide paths to the LUN. You can create an SVM to separate the data and administration functions of a user from those of the other users in a cluster.

Before you begin

- You must have enough network addresses available to create two LIFs for each node.

Steps

1. Navigate to the **SVMs** window.
2. Click **Create**.
3. In the **Storage Virtual Machine (SVM) Setup** window, create the SVM:

   a. Specify a unique name for the SVM.

      The name must either be a fully qualified domain name (FQDN) or follow another convention that ensures unique names across a cluster.

   b. Select the IPspace that the SVM will belong to.

      If the cluster does not use multiple IPspaces, the “Default” IPspace is used.

   c. Keep the default volume type selection.

      Only FlexVol volumes are supported with SAN protocols.

   d. Select all of the protocols that you have licenses for and that you might use on the SVM, even if you do not want to configure all of the protocols immediately.

      Selecting both NFS and CIFS when you create the SVM enables these two protocols to share the same LIFs. Adding these protocols later does not allow them to share LIFs.

      If CIFS is one of the protocols you selected, then the security style is set to NTFS. Otherwise, the security style is set to UNIX.

   e. Keep the default language setting C.UTF-8.

   f. Select the desired root aggregate to contain the SVM root volume.

      The aggregate for the data volume is selected separately in a later step.

   g. Click **Submit & Continue**.

The SVM is created, but protocols are not yet configured.

4. If the **Configure CIFS/NFS protocol** page appears because you enabled CIFS or NFS, click **Skip** and then configure CIFS or NFS later.
5. Configure the iSCSI service and create LIFs from the **Configure iSCSI protocol** page:
   a. Enter a target alias name.
   b. Assign IP address for the LIFs either by using a subnet or without a subnet.
   c. Enter `2` in the **LIFs per node** field.

      Two LIFs are required for each node to ensure availability and data mobility.

   d. Skip the optional **Provision a LUN for iSCSI storage** area because the LUN is provisioned by Virtual Storage Console for VMware vSphere in a later step.
   e. Click **Submit & Continue**.
6. If the **Configure FC/FCoE protocol** page appears because you enabled FC, click **Skip** and then configure FC later.
7. When the **SVM Administration** appears, configure or defer configuring a separate administrator for this SVM:
   - Click **Skip** and configure an administrator later if desired.
   - Enter the requested information, and then click **Submit & Continue**.
8. Review the **Summary** page, record the LIF information, and then click **OK**.

Test iSCSI paths from the host to the storage cluster

To ensure successful storage failover and data mobility, you need to ensure that you have two paths from the host to every node in the storage cluster. Because the number of paths advertised by the iSCSI target is limited, you need to ping the storage cluster ports from the host.

Before you begin

You must know the IP address or host name of all of the logical interfaces (LIFs) to be used for iSCSI paths.

About this task

LUNs are mapped to a subset of the initiators in the igroup to limit the number of paths from the host to the LUN.

- By default, only paths from the host to the node containing the storage virtual machine (SVM) where the LUN was created, and paths to the HA partner of that node, are visible to the host.
- You still must create and test paths from the host to every node in the cluster, but the host can access only those paths on the owning node and its HA partner.
- You should use the default LUN mapping behavior.

  Only add nodes in other HA pairs to the LUN map in preparation for moving the LUN to a different node.

Steps

1. From the ESXi host, use the `ping` command to verify the path to the first LIF.

The `ping` command is available from the ESXi service console.

2. Repeat the `ping` command to verify connectivity to each iSCSI LIF on each node in the cluster.

Related information

VMware KB article 1003486: Testing network connectivity with the ping command

Provision a datastore and creating its containing LUN and volume

A datastore contains virtual machines and their VMDKs on the ESXi host. The datastore on the ESXi host is provisioned on a LUN on the storage cluster.

Before you begin

Virtual Storage Console for VMware vSphere (VSC) must be installed and registered with the vCenter Server that manages the ESXi host.

VSC must have sufficient cluster or storage virtual machine (SVM) credentials to create the LUN and volume.

About this task

VSC automates the datastore provisioning, including creating a LUN and volume on the specified SVM.

Steps

1. From the vSphere Web Client **Home** page, click **Hosts and Clusters**.
2. In the navigation pane, expand the datacenter where you want to provision the datastore.
3. Right-click the ESXi host, and then select **NetApp VSC** > **Provision Datastore**.

   Alternatively, you can right-click the cluster when provisioning to make the datastore available to all hosts in the cluster.

4. Provide the required information in the wizard:

   - Select **VMFS** as the datastore type.
   - Select **iSCSI** as the VMFS protocol.

- Select **None** as the Storage Capability Profile.
- Select the box for **Thin provision**.
- Select the **Create new volume** check box.

Verify that the host can write to and read from the LUN

Before using the LUN, you should verify that the host can write data to the LUN and read it back.

About this task

If the cluster node on which the LUN is created can be failed over to its partner node, you should verify reading the data while the node is failed over. This test might not be possible if the cluster is in production use.

Steps

1. On the vSphere Web Client **Home** page, click **Hosts and Clusters**.
2. In the navigation pane, click the **Storage** tab.
3. Expand the datacenter, and then select the new datastore.
4. In the center pane, click **Manage** > **Files**.

   The contents of the datastore are displayed.

5. Create a new folder in the datastore and upload a file to the new folder.

   You might need to install the Client Integration Plug-in.

6. Verify that you can access the file you just wrote.
7. **Optional:** Fail over the cluster node containing the LUN and verify that you can still write and read a file.

   If any of the tests fail, verify that the iSCSI service is running on the storage cluster and check the iSCSI paths to the LUN.

8. **Optional:** If you failed over the cluster node, be sure to give back the node and return all LIFs to their home ports.
9. For an ESXi cluster, view the datastore from each ESXi host in the cluster and verify that the file you uploaded is displayed.

Related information

High availability management

iSCSI configuration for Red Hat Enterprise Linux

iSCSI configuration for Red Hat Enterprise Linux overview

Using the ONTAP System Manager classic interface (ONTAP 9.7 and earlier), you can quickly set up the iSCSI service on a storage virtual machine (SVM), provision a LUN, and make the LUN available on a Red Hat Enterprise Linux server.

These procedures are based on the following assumptions:

- You are using the iSCSI software initiator on a Red Hat Enterprise Linux host running a supported version of RHEL Series 6.4 or higher.
- Your network uses IPv4 addressing.
- You want to assign addresses to logical interfaces using any of the following methods:
  - Automatically, from a subnet you define
  - Manually, using an address selected from an existing subnet
  - Manually, using an address that will be added to an existing subnet
- You are not configuring iSCSI SAN boot.

For more information on how to configure your specific host with ONTAP, see ONTAP SAN Host Configuration.

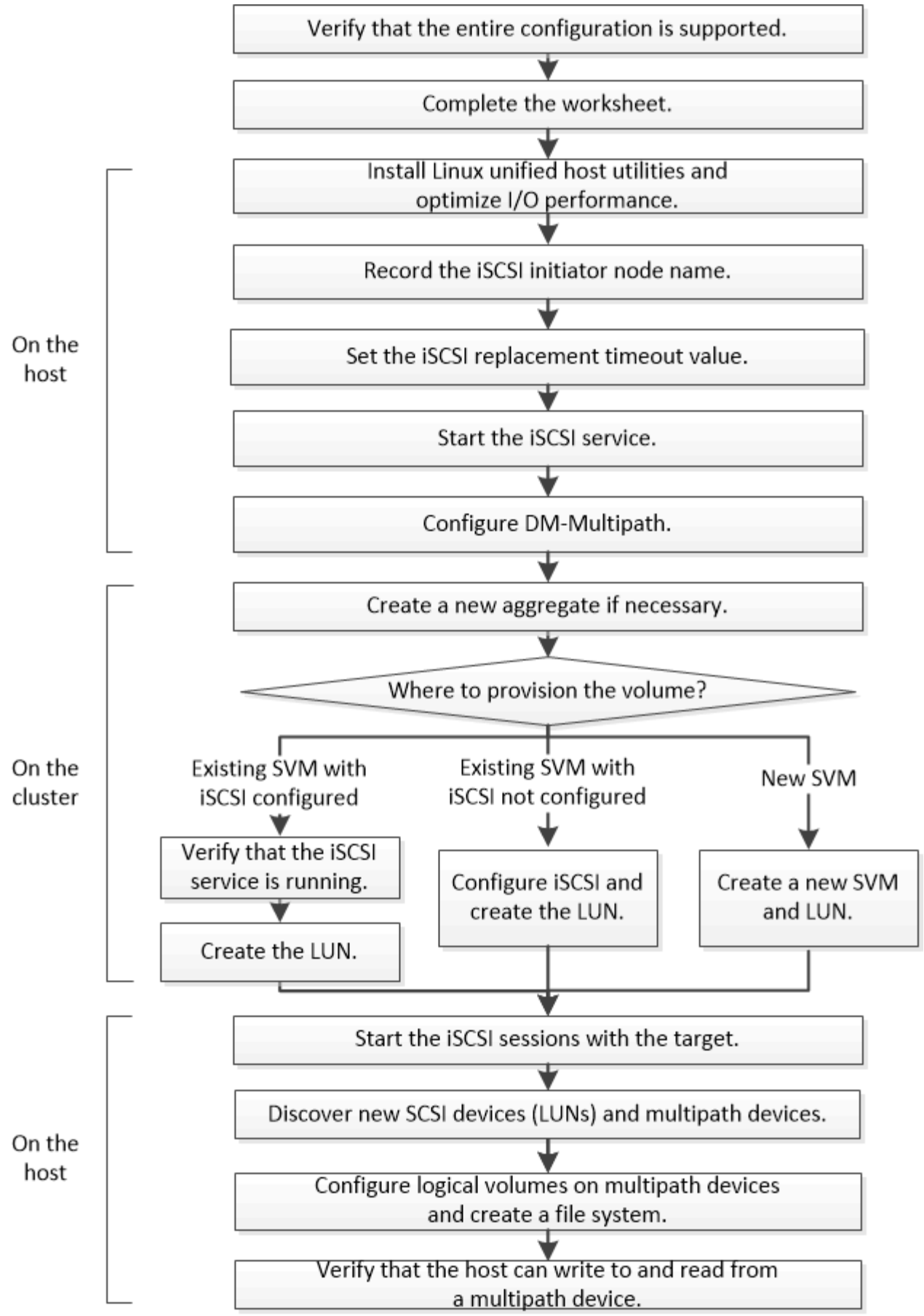
For additional details about SAN Administration, consult the ONTAP 9 SAN administration overview

Other ways to do this in ONTAP

To complete this task using…	Refer to…
The redesigned System Manager (available with 9.7 and later)	Provision SAN storage
The ONTAP command line interface (CLI)	LUN setup workflow with the CLI

iSCSI configuration and provisioning workflow

When you make storage available to a host using iSCSI, you provision a volume and LUN on the storage virtual machine (SVM), and then connect to the LUN from the host.


Verify that the entire configuration is supported.
Complete the worksheet.
Install Linux unified host utilities and optimize I/O performance.
Record the iSCSI initiator node name.
Set the iSCSI replacement timeout value.
Start the iSCSI service.
Configure DM-Multipath.
On the host
Create a new aggregate if necessary.
Where to provision the volume?
Existing SVM with iSCSI configured
Existing SVM with iSCSI not configured
New SVM
Verify that the iSCSI service is running.
Create the LUN.
Configure iSCSI and create the LUN.
Create a new SVM and LUN.
On the cluster
Start the iSCSI sessions with the target.
Discover new SCSI devices (LUNs) and multipath devices.
Configure logical volumes on multipath devices and create a file system.
Verify that the host can write to and read from a multipath device.
On the host

Verify that the iSCSI configuration is supported

For reliable operation, you must verify that the entire iSCSI configuration is supported.

Steps

1. Go to the NetApp Interoperability Matrix Tool to verify that you have a supported combination of the following components:
   - ONTAP software
   - Host computer CPU architecture (for standard rack servers)
   - Specific processor blade model (for blade servers)
   - Storage protocol (iSCSI)
   - Linux operating system version
   - DM-Multipath package
   - Linux Unified Host Utilities
2. Click the configuration name for the selected configuration.

   Details for that configuration are displayed in the Configuration Details window.
3. Review the information in the following tabs:
   - Notes

     Lists important alerts and information that are specific to your configuration.

     Review the alerts to identify the packages that are required for your operating system.
   - Policies and Guidelines

     Provides general guidelines for all SAN configurations.

Complete the iSCSI configuration worksheet

You require iSCSI identifiers, network addresses, and storage configuration information to perform iSCSI configuration tasks.

iSCSI identifiers

Initiator (host) iSCSI node name (IQN)
Target alias (optional)

Target network addresses

The storage virtual machine (SVM) is the iSCSI target.

You require a subnet with two IP addresses for iSCSI data LIFs for each node in the cluster. There should be two separate networks for high availability. The specific IP addresses are assigned by ONTAP when you create the LIFs as part of creating the SVM.

If possible, separate iSCSI traffic on separate physical networks or on VLANs.

Subnet for LIFs:

Node or LIF with port to switch	IP address	Network mask	Gateway	VLAN ID	Home port
Node 1 / LIF to switch 1					
Node 2 / LIF to switch 1					
Node 3 / LIF to switch 1					
Node 4 / LIF to switch 1					
Node 1 / LIF to switch 2					
Node 2 / LIF to switch 2					
Node 3 / LIF to switch 2					
Node 4 / LIF to switch 2					

Storage configuration

If the aggregate and SVM are already created, record their names here; otherwise, you can create them as required:

Node to own LUN
Aggregate name
SVM name

LUN information

LUN size
LUN name (optional)
LUN description (optional)

SVM information

If you are not using an existing SVM, you require the following information to create a new one:

SVM name	
SVM IPspace	
Aggregate for SVM root volume	
SVM user name (optional)	
SVM password (optional)	
SVM management LIF (optional)	
	Subnet:
	IP address:
	Network mask:
	Gateway:
	Home node:
	Home port:

Install Linux Unified Host Utilities and optimizing I/O performance

Linux Unified Host Utilities software includes the `sanlun` utility, a NetApp LUN reporting tool that you can use to display information about storage cluster nodes. You must also enable the correct server profile on the Linux host to optimize NetApp storage performance.

Before you begin

You must have identified the supported Linux Unified Host Utilities version for your configuration by using the Interoperability Matrix. You must also have the `tuned` package, which is part of your Linux OS distribution and contains the `tuned-adm` command, which you use to set the server profile on the host.

Steps

1. Download the supported Linux Unified Host Utilities version from the NetApp Support Site.

   NetApp Downloads: Software

2. Install Linux Unified Host Utilities software by following the instructions in the installation documentation.
3. If the `tuned` package is not installed, enter the following command:

```
yum install tuned
```

4. For a physical host, ensure that you have set the `enterprise-storage` profile:

```
tuned-adm profile enterprise-storage
```

5. For a virtual host, ensure that you have set the `virtual-guest` profile:

```
tuned-adm profile virtual-guest
```

Related Information
Linux Unified Host Utilities 7.1 Installation

Record the iSCSI node name

You must record the iSCSI initiator node name on the Linux host so that you have it when you configure the storage system.

Steps

1. Use a text editor to open the `/etc/iscsi/initiatorname.iscsi` file containing the node names.
2. Write down the node name or copy it to a text file.

   The iSCSI initiator node name looks something like this:

```
iqn.1994-05.com.redhat:127
```

Set the iSCSI replacement timeout value

To support multipathing, you must modify the replacement timeout value in the iSCSI configuration file.

Step

1. Change the replacement timeout value in the `/etc/iscsi/iscsid.conf` file from the default of 120 to 5.

   The replacement timeout value looks like the following in `iscsid.conf`:

```
node.session.timeo.replacement_timeout = 5
```

Start the iSCSI service

After you edit the iSCSI configuration file, you must start the iSCSI service so that the host can discover the targets and access LUNs. If the iSCSI service is running, you must restart it.

Step

1. Start the iSCSI service at the Linux host command prompt:

If you are using…	Enter…
Red Hat Enterprise Linux 7 series and SUSE Linux Enterprise 12 series	`systemctl start iscsid`
Red Hat Enterprise Linux 6 series You must execute this command the first time you start the iSCSI service on a host running Red Hat Enterprise Linux 6 series and Oracle Linux 6 series. If you execute `/etc/init.d/iscsi start` without previously executing `service iscsid force-start`, you get an error message.	`service iscsid force-start`
Red Hat Enterprise Linux 5 or 4 series and Oracle Linux 5 series, Red Hat Enterprise Virtualization, Oracle Linux, and Oracle VM	`/etc/init.d/iscsi start`
SUSE Linux Enterprise Server 10 or 11 series	`/etc/init.d/open-iscsi start`

Citrix discourages the use of the iscsiadm tool. The native XAPI stack accomplishes the tasks of starting and stopping the iscsi service, automatic login on boot, and other iSCSI operations.

Configure DM-Multipath

DM-Multipath manages multiple paths between the Linux host and the storage cluster. Configuring DM-Multipath on a LUN, which appears to the Linux host as a SCSI device, enables your Linux host to access its LUN on the storage cluster if a path or component fails.

Before you begin

You must have identified the required version of DM-Multipath from the Interoperability Matrix tool.

NetApp Interoperability Matrix Tool

The recommended approach is that you configure two paths per node into each fabric or Ethernet network. This allows a path to fail without the node switching over to its partner. Using link aggregation (LAG) for the physical ports is not recommended with a Windows-based operating system.

Steps

1. Edit the `/etc/multipath.conf` file as follows:
   a. Determine whether there are non-NetApp SCSI devices to exclude (blacklist).

These are devices that are not displayed when you enter the `sanlun lun show` command.

- If there are non-NetApp SCSI devices to exclude, enter the worldwide identifier (WWID) for the devices in the blacklist section of the `multipath.conf` file.

  To display the WWID of a non-NetApp SCSI device, enter the following command on the device that you want to exclude, where `SCSI_device_name` is a device that you specify: `/lib/udev/scsi_id -gud /dev/SCSI_device_name`

  For example, if `/dev/sda` is the non-NetApp SCSI device that you want to exclude, you would enter the following:

  ```
  /lib/udev/scsi_id -gud /dev/sda
  ```

  This displays the WWID of the device, which you can copy and paste in the `multipath.conf` file.

  In the following example showing the blacklist section of the `multipath.conf` file, the non-NetApp SCSI device with WWID `3600508e000000000753250f933cc4606` is excluded:

  ```
  blacklist {
              **wwid       3600508e000000000753250f933cc4606**
              devnode    "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
              devnode    "^hd[a-z]"
              devnode     "^cciss.*"
  }
  ```

- If there are no devices to exclude, remove the *wwid* line from the `multipath.conf` file.

b. Enable NetApp recommended DM-Multipath settings by appending the following string to the end of the kernel line in the boot loader: `rdloaddriver=scsi_dh_alua`

2. Start the DM-Multipath daemon:

   ```
   /etc/init.d/multipathd start
   ```

3. Add the multipath service to the boot sequence so that the multipath daemon always starts during system boot:

   ```
   chkconfig multipathd on
   ```

4. Reboot the Linux host.
5. Verify that the `rdloaddriver` setting appears in the output when you run `cat /proc/cmdline`.

   The `rdloaddriver` setting appears as one of several boot options that are passed to the kernel:

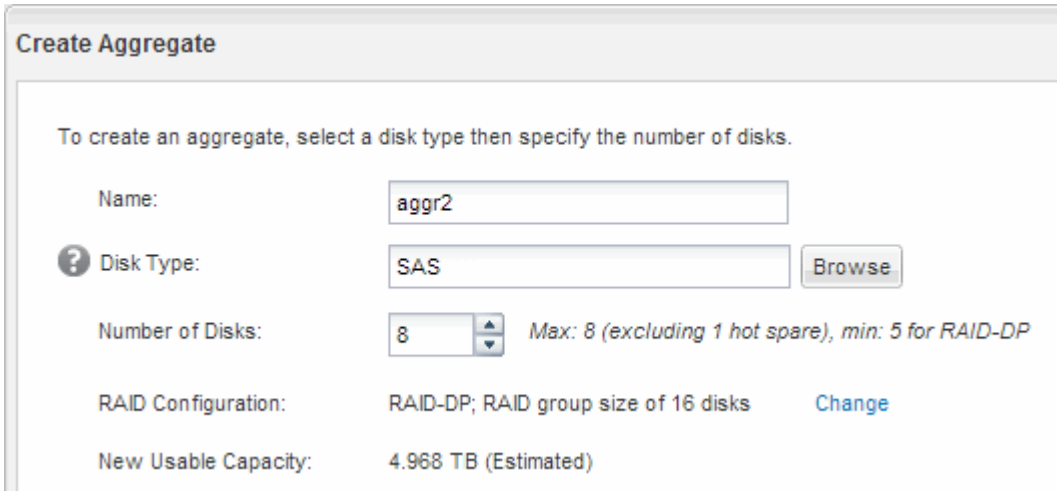
```
# cat /proc/cmdline
ro root=/dev/mapper/vg_ibmx3650210104-lv_root rd_NO_LUKS LANG=en_US.UTF-
8 rd_NO_MD rd_LVM_LV=vg_ibmx3650210104/lv_root SYSFONT=latarcyrheb-sun16
rd_LVM_LV=vg_ibmx3650210104/lv_swap crashkernel=129M@0M  KEYBOARDTYPE=pc
KEYTABLE=us rd_NO_DM rhgb quiet **rdloaddriver=scsi_dh_alua**
```

Create an aggregate

If you do not want to use an existing aggregate, you can create a new aggregate to provide physical storage to the volume which you are provisioning.

Steps

1. Enter the URL `https://IP-address-of-cluster-management-LIF` in a web browser and log in to System Manager using your cluster administrator credential.
2. Navigate to the **Aggregates** window.
3. Click **Create.**
4. Follow the instructions on the screen to create the aggregate using the default RAID-DP configuration, and then click **Create**.



Results

The aggregate is created with the specified configuration and added to the list of aggregates in the Aggregates window.

Decide where to provision the volume

Before you provision a volume to contain your LUNs, you need to decide whether to add the volume to an existing storage virtual machine (SVM) or to create a new SVM for the volume. You might also need to configure iSCSI on an existing SVM.

About this task

If an existing SVM is already configured with the needed protocols and has LIFs that can be accessed from the host, it is easier to use the existing SVM.

You can create a new SVM to separate data or administration from other users of the storage cluster. There is no advantage to using separate SVMs just to separate different protocols.

Procedure

- If you want to provision volumes on an SVM that is already configured for iSCSI, you must verify that the iSCSI service is running and then create a LUN on the SVM.

  Verifying that the iSCSI service is running on an existing SVM

  Creating a LUN

- If you want to provision volumes on an existing SVM that has iSCSI enabled but not configured, configure iSCSI on the existing SVM.

  Configuring iSCSI on an existing SVM

  This is the case when you did not follow this procedure to create the SVM while configuring a different protocol.

- If you want to provision volumes on a new SVM, create the SVM.

  Creating a new SVM

Verify that the iSCSI service is running on an existing SVM

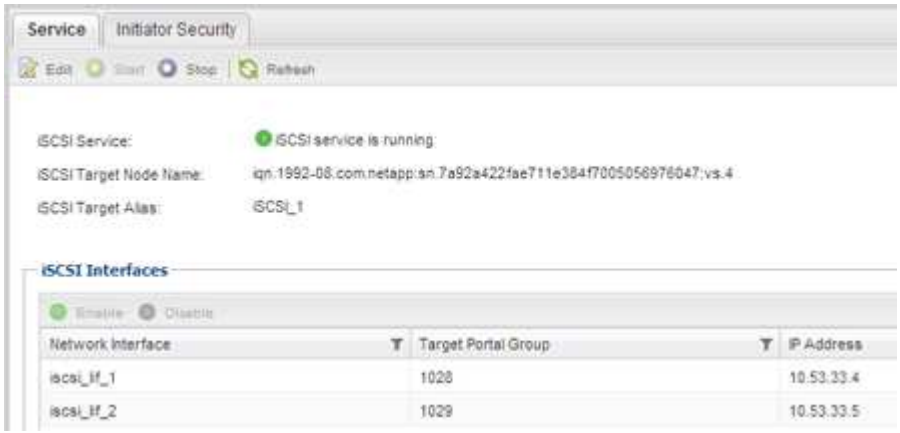
If you choose to use an existing storage virtual machine (SVM), you must verify that the iSCSI service is running on the SVM.

Before you begin

You must have selected an existing SVM on which you plan to create a new LUN.

Steps

1. Navigate to the **SVMs** window.
2. Click the **SVM Settings** tab.
3. In the **Protocols** pane, click **iSCSI**.
4. Verify that the iSCSI service is running.



5. Record the iSCSI interfaces listed for the SVM.

What to do next

If the iSCSI service is not running, start the iSCSI service or create a new SVM.

If there are fewer than two iSCSI interfaces per node, update the iSCSI configuration on the SVM or create a new SVM for iSCSI.

Create a LUN

You use the Create LUN wizard to create a LUN. The wizard also creates the igroup and maps the LUN to the igroup, which enables the specified host to access the LUN.

Before you begin

- There must be an aggregate with enough free space to contain the LUN.
- There must be a storage virtual machine (SVM) with the iSCSI protocol enabled and the appropriate logical interfaces (LIFs) created.
- You must have recorded the iSCSI initiator node name of the host.

LUNs are mapped to a subset of the initiators in the igroup to limit the number of paths from the host to the LUN.

- By default, ONTAP uses Selective LUN Map (SLM) to make the LUN accessible only through paths on the node owning the LUN and its high-availability (HA) partner.
- You still must configure all of the iSCSI LIFs on every node for LUN mobility in case the LUN is moved to another node in the cluster.
- When moving a volume or a LUN, you must modify the SLM reporting-nodes list before moving.

About this task

If your organization has a naming convention, you should use names for the LUN, volume, and so on that fit your convention. Otherwise, you should accept the default names.

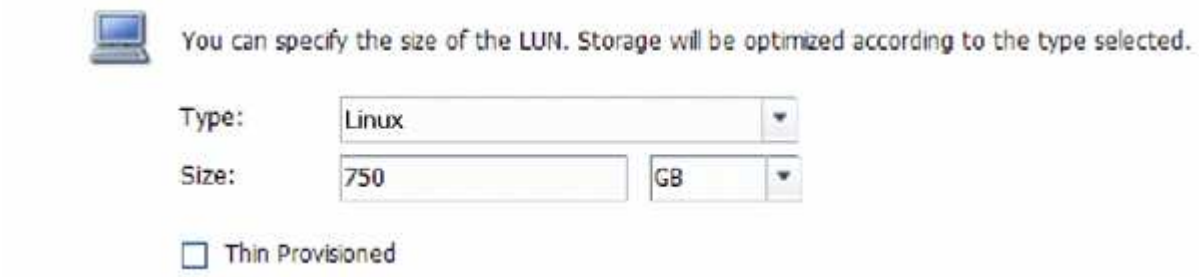
Steps

1. Navigate to the **LUNs** window.
2. Click **Create.**
3. Browse and select an SVM in which you want to create the LUNs.

   The Create LUN Wizard is displayed.

4. On the **General Properties** page, select the LUN type **Linux** for LUNs used directly by the Linux host.

   Leave the **Thin Provisioned** check box unselected.



5. On the **LUN Container** page, select an existing FlexVol volume.

   You must ensure that there is enough space in the volume. If sufficient space is not available in the existing volumes, you can create a new volume.

6. On the **Initiators Mapping** page, click **Add Initiator Group**, enter the required information on the **General** tab, and then on the **Initiators** tab, enter the iSCSI initiator node name of the host that you recorded.
7. Confirm the details, and then click **Finish** to complete the wizard.

Related information

System administration

Configure iSCSI on an existing SVM

You can configure iSCSI on an existing storage virtual machine (SVM)and create a LUN and its containing volume with a single wizard. The iSCSI protocol must already be enabled but not configured on the SVM. This information is intended for SVMs for which you are configuring multiple protocols, but have not yet configured iSCSI.

Before you begin

You must have enough network addresses available to create two LIFs for each node.

About this task

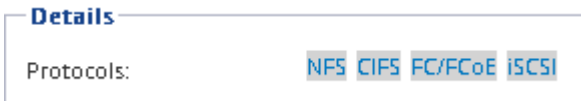
LUNs are mapped to a subset of the initiators in the igroup to limit the number of paths from the host to the LUN.

- ONTAP uses Selective LUN Map (SLM) to make the LUN accessible only through paths on the node owning the LUN and its HA partner.
- You still must configure all of the iSCSI LIFs on every node for LUN mobility in case the LUN is moved to another node in the cluster.
- You must modify the SLM reporting-nodes list before moving a volume or a LUN.

Steps

1. Navigate to the **SVMs** window.
2. Select the SVM that you want to configure.
3. In the SVM**Details** pane, verify that **iSCSI** is displayed with a gray background, which indicates that the protocol is enabled but not fully configured.

   If **iSCSI** is displayed with a green background, the SVM is already configured.

4. Click the **iSCSI** protocol link with the gray background.

   The Configure iSCSI Protocol window is displayed.

5. Configure the iSCSI service and LIFs from the **Configure iSCSI protocol** page:

a. **Optional:** Enter a target alias name.

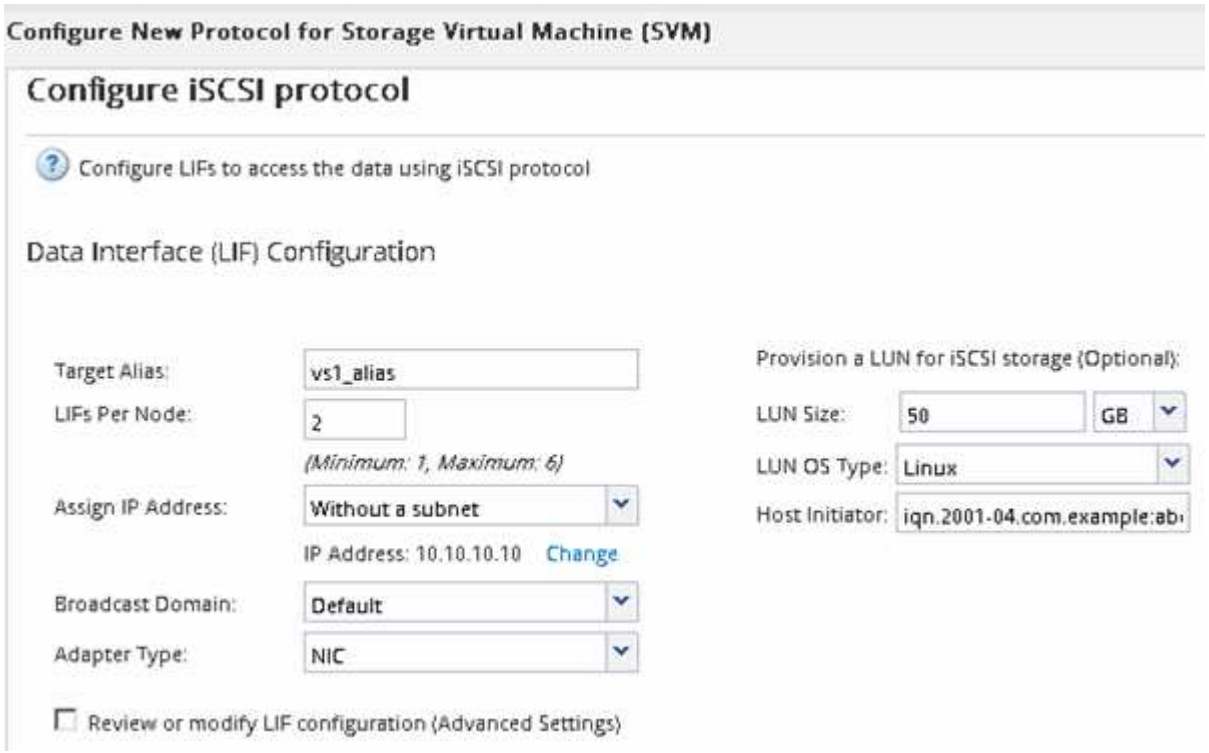
b. Enter **2** in the **LIFs per node** field.

   Two LIFs are required for each node to ensure availability and data mobility.

c. Assign IP addresses for the LIFs either with a subnet or without a subnet.

d. In the **Provision a LUN for iSCSI storage** area, enter the desired LUN size, host type, and iSCSI initiator name of the host.

e. Click **Submit & Close**.



6. Review the **Summary** page, record the LIF information, and then click **OK**.

Create a new SVM

The storage virtual machine (SVM) provides the iSCSI target through which a host accesses LUNs. When you create the SVM, you also create logical interfaces (LIFs) and the LUN and its containing volume. You can create an SVM to separate the data and administration functions of a user from those of the other users in a cluster.

Before you begin

- You must have enough network addresses available to create two LIFs for each node.

About this task

LUNs are mapped to a subset of the initiators in the igroup to limit the number of paths from the host to the LUN.

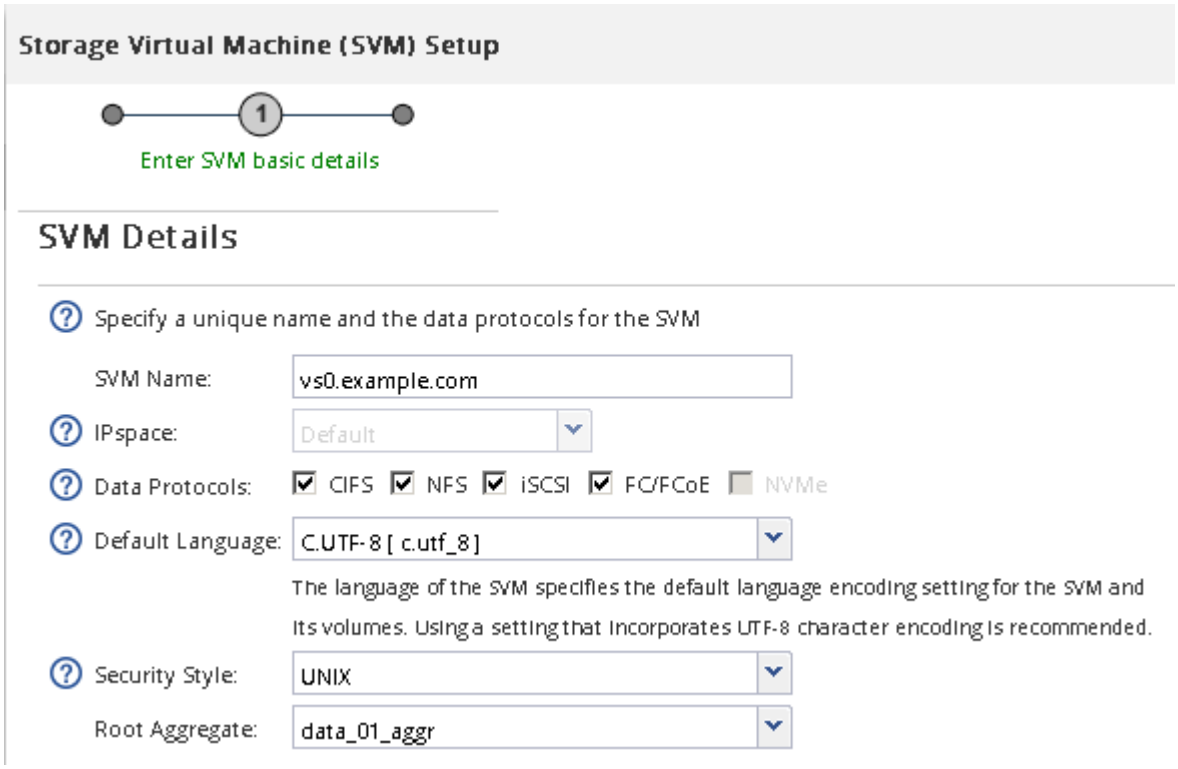
- By default, ONTAP uses Selective LUN Map (SLM) to make the LUN accessible only through paths on the node owning the LUN and its HA partner.
- You still must configure all of the iSCSI LIFs on every node for LUN mobility in case the LUN is moved to

another node in the cluster.

- When moving a volume or a LUN, you must modify the SLM-reporting-nodes list before moving.

Steps

1. Navigate to the **SVMs** window.
2. Click **Create**.
3. In the **Storage Virtual Machine (SVM) Setup** window, create the SVM:



a. Specify a unique name for the SVM.

   The name must either be a fully qualified domain name (FQDN) or follow another convention that ensures unique names across a cluster.

b. Select the IPspace that the SVM will belong to.

   If the cluster does not use multiple IPspaces, the “Default” IPspace is used.

c. Keep the default volume type selection.

   Only FlexVol volumes are supported with SAN protocols.

d. Select all of the protocols that you have licenses for and that you might use on the SVM, even if you do not want to configure all of the protocols immediately.

   Selecting both NFS and CIFS when you create the SVM enables these two protocols to share the same LIFs. Adding these protocols later does not allow them to share LIFs.

   If CIFS is one of the protocols you selected, then the security style is set to NTFS. Otherwise, the security style is set to UNIX.

e. Keep the default language setting C.UTF-8.

f. Select the desired root aggregate to contain the SVM root volume.

   The aggregate for the data volume is selected separately in a later step.

g. Click **Submit & Continue**.

The SVM is created, but protocols are not yet configured.

4. If the **Configure CIFS/NFS protocol** page appears because you enabled CIFS or NFS, click **Skip** and then configure CIFS or NFS later.
5. Configure the iSCSI service and create LIFs, and the LUN and its containing volume from the **Configure iSCSI protocol** page:

   a. **Optional:** Enter a target alias name.

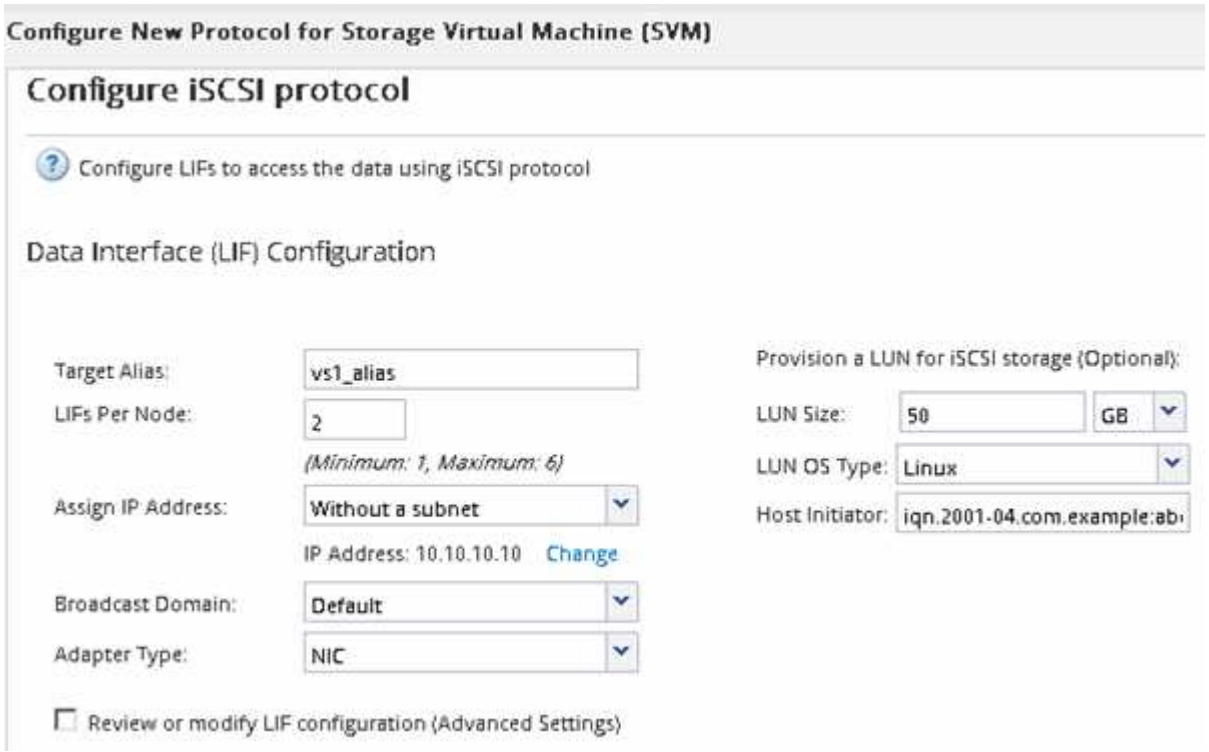
   b. Assign IP address for the LIFs either by using a subnet or without a subnet.

   c. Enter **2** in the **LIFs per node** field.

      Two LIFs are required for each node to ensure availability and data mobility.

   d. In the **Provision a LUN for iSCSI storage** area, enter the desired LUN size, host type, and iSCSI initiator name of the host.

   e. Click **Submit & Continue**.



6. If the **Configure FC/FCoE protocol** page appears because you enabled FC, click **Skip** and then configure FC later.
7. When the **SVM Administration** appears, configure or defer configuring a separate administrator for this SVM:

   ◦ Click **Skip** and configure an administrator later if desired.

- Enter the requested information, and then click **Submit & Continue**.

8. Review the **Summary** page, record the LIF information, and then click **OK**.

Start the iSCSI sessions with the target

The Linux host must have an iSCSI connection with each node (target) in the storage cluster. You establish the sessions from the host.

About this task

In ONTAP, the iSCSI host must have paths to each node in the cluster. DM-Multipath selects the best paths to use. If paths fail, DM-Multipath selects alternate paths.

Steps

1. Start the iSCSI service from the Linux host command prompt:

   ```
   service iscsid force-start
   ```

2. Discover the iSCSI target:

   ```
   iscsiadm --mode discovery --op update --type sendtargets --portal targetIP
   ```

   The IP address of each discovered target displays on a separate line.

3. Establish iSCSI sessions by logging in to each target:

   ```
   iscsiadm --mode node -l all
   ```

4. You can view a list of the active iSCSI sessions:

   ```
   iscsiadm --mode session
   ```

Discover new SCSI devices (LUNs) and multipath devices

LUNs on the storage cluster appear to the Linux host as SCSI devices, which are I/O paths that DM-Multipath aggregates into a new device, called a multipath device. The host does not automatically discover new SCSI devices (LUNs) that you add to your system. You must manually rescan them to discover them.

Before you begin

You must have a copy of the `rescan` script, which is in the `sg3_utils` package that is part of your Linux OS distribution.

Steps

1. Discover new SCSI devices (LUNs) and create the corresponding multipath devices for the LUNs:

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

2. Verify DM-Multipath configuration:

   ```
   multipath -ll
   ```

This displays the following type of output, listing the recommended settings for each NetApp LUN:

```
3600a0980324666546e2b443251655177 dm-2 NETAPP,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50
retain_attached_hw_handle' hwhandler='1 alua' wp=rw
|-+- policy='round-robin 0' prio=50 status=active
| |- 0:0:1:0 sdb 8:16  active ready  running
| |- 0:0:0:0 sda 8:0   active ready  running
| |- 1:0:0:0 sde 8:64  active ready  running
| `- 1:0:1:0 sdf 8:80  active ready  running
`-+- policy='round-robin 0' prio=10 status=enabled
  |- 0:0:3:0 sdd 8:48  active ready  running
  |- 1:0:3:0 sdh 8:112 active ready  running
  |- 0:0:2:0 sdc 8:32  active ready  running
  `- 1:0:2:0 sdg 8:96  active ready  running
```

Configure logical volumes on multipath devices and creating a file system

When the Linux host first accesses a new SCSI device (LUN), there is no partition or file system. If you want to use a partitioned multipath device, you must first partition the underlying SCSI devices. You might also want to create logical volumes on multipath devices, and optionally create a file system.

Before you begin

SCSI devices and corresponding multipath devices must have been discovered by the Linux host.

About this task

At a minimum DM-Multipath should be configured on the SCSI devices. Any configuration beyond DM-Multipath is optional. The following steps are general guidelines if you wish to perform additional configuration, such as partitioning, configuring logical volumes on multipath devices, and creating a file system. For details on Linux commands, refer to Red Hat Enterprise Linux documentation and man pages.

Steps

1. To use a partitioned multipath device, first partition the underlying SCSI devices using the `fdisk` or `parted` utility.
2. Create corresponding multipath partitions using the `kpartx` utility.
3. Create logical volumes on corresponding multipath devices using Logical Volume Manager (LVM) commands.
4. Create a file system, such as Ext4 or XFS, on logical volumes or multipath devices using the `mkfs` utility.

Verify that the host can write to and read from a multipath device

Before using a multipath device, you should verify that the host can write data to the multipath device and read it back.

Before you begin

DM-Multipath must be configured on the Linux host for the storage cluster nodes you are accessing.

About this task

If the storage cluster node that the multipath device corresponds to can be failed over to its partner node, you should verify reading the data while the node is failed over. This verification might not be possible if the storage cluster is in production use.

Steps

1. Run some I/O on the specified multipath device:

   ```
   dd if=/dev/zero of=<multipath_device_name\>
   ```

2. Verify that I/O is running on the multipath device, specifying the number of seconds to refresh statistics (for example, every two seconds, as shown):

   ```
   iostat 2
   ```

   When I/O is running on the multipath device, you can see the various I/O counters output change dynamically, indicating that I/O is running successfully on the multipath device.

   ```
   avg-cpu:  %user   %nice %system %iowait  %steal   %idle
              0.00    0.00    0.01    0.00    0.00   99.98

   Device:            tps   Blk_read/s   Blk_wrtn/s   Blk_read   Blk_wrtn
   sda               0.18         1.34         2.29     832606    1428026
   dm-0              0.37         1.29         2.29     801530    1427984
   dm-1              0.00         0.00         0.00       2576          0
   dm-2              0.00         0.00         0.00       1770         24
   sdd               0.17         1.18        17.87     734688   11128584
   sde               0.17         1.18        18.01     734560   11219016
   sdf               0.00         0.00         0.00       1344          0
   sdg               0.00         0.00         0.00       1344          0
   dm-3              0.68         4.71        71.96    2932496   44816008
   sdh               0.17         1.18        18.22     734360   11343920
   sdi               0.17         1.18        17.86     734272   11124488
   sdj               0.00         0.00         0.00       1344          0
   sdk               0.00         0.00         0.00       1344          0
   ..............
   ```

3. If possible, run the `takeover` command on the storage cluster node:

   ```
   storage failover takeover -ofnode <node_name\>
   ```

4. Verify that I/O is still running on the multipath device by re-running the `iostat` command.
5. Run the `giveback` command on the storage cluster node:

   ```
   storage failover giveback -ofnode <node_name\>
   ```

6. Check `iostat` output to verify that I/O is still running.

What to do next

If any of the tests fail, verify that the iSCSI service is running and re-check the DM-Multipath configuration and the iSCSI paths to the multipath device.

iSCSI configuration for Windows

iSCSI configuration for Windows overview

Using the ONTAP System Manager classic interface (ONTAP 9.7 and earlier), you can quickly set up the iSCSI service on a storage virtual machine (SVM), provision a LUN, and make the LUN available using an iSCSI initiator on a Windows host computer.

These procedures are based on the following assumptions:

- You are using the Microsoft iSCSI software initiator on Windows Server 2008 or Windows Server 2012.
- Your network uses IPv4 addressing.
- You want to assign addresses to logical interfaces using any of the following methods:
  - Automatically, from a subnet you define
  - Manually, using an address selected from an existing subnet
  - Manually, using an address that will be added to an existing subnet
- You are not configuring iSCSI SAN boot.

For more information on how to configure your specific host with ONTAP, see ONTAP SAN Host Configuration.

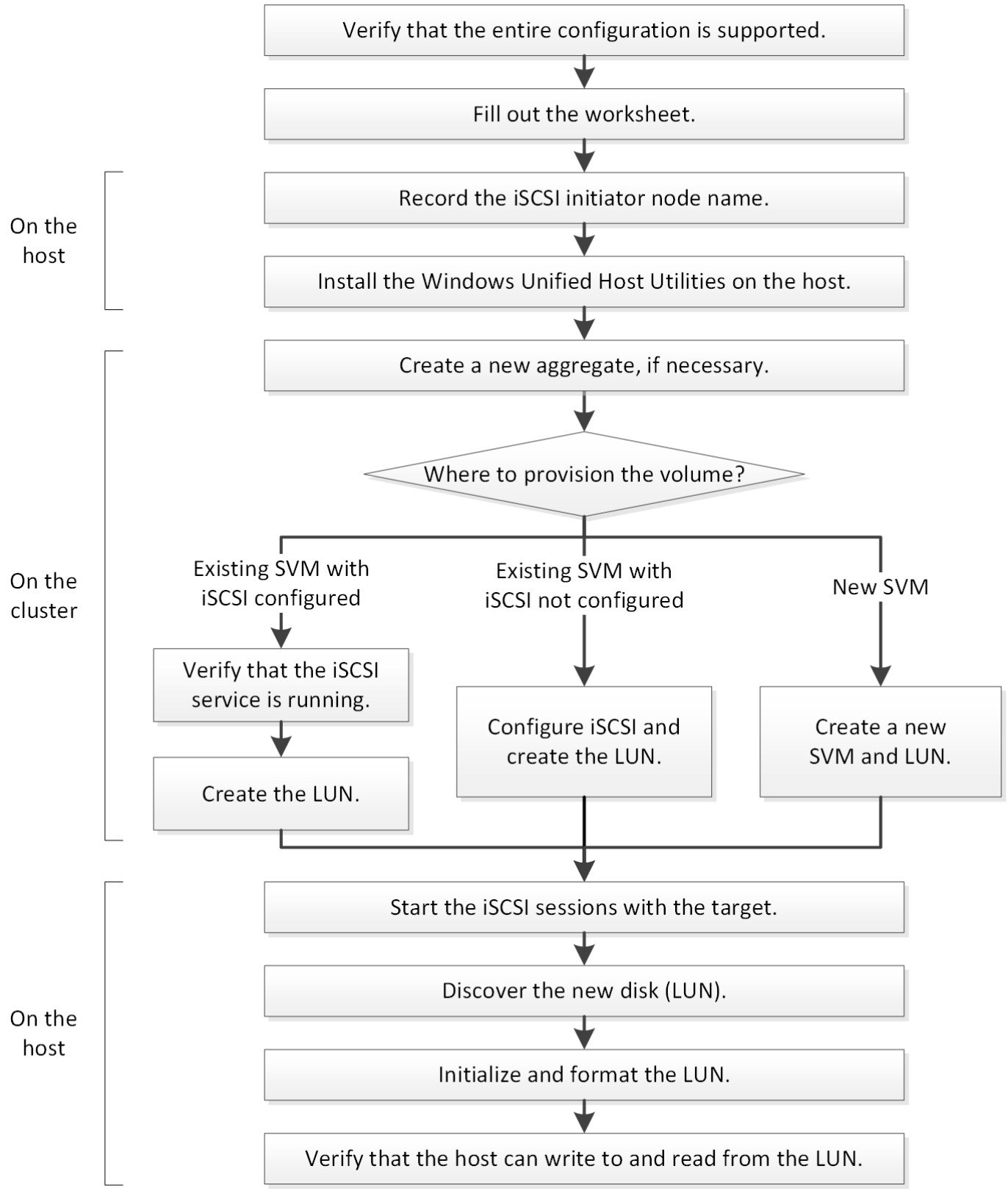
For additional details about SAN administration, consult the ONTAP 9 SAN administration overview

Other ways to do this in ONTAP

To complete this task using…	Refer to…
The redesigned System Manager (available with 9.7 and later)	Provision SAN storage for Windows servers
The ONTAP command line interface (CLI)	LUN setup workflow with the CLI

iSCSI configuration and provisioning workflow

When you make storage available to a host using iSCSI, you provision a volume and LUN on the storage virtual machine (SVM), and then connect to the LUN from the host.



Verify that the iSCSI configuration is supported

For reliable operation, you must verify that the entire iSCSI configuration is supported.

Steps

1. Go to the Interoperability Matrix to verify that you have a supported combination of the following

components:

- ONTAP software
- Host computer CPU architecture (for standard rack servers)
- Specific processor blade model (for blade servers)
- Storage protocol (iSCSI)
- Windows operating system version
- Windows Unified Host Utilities

2. Click the configuration name for the selected configuration.

   Details for that configuration are displayed in the Configuration Details window.

3. Review the information in the following tabs:
   - Notes

     Lists important alerts and information that are specific to your configuration.

     Review the alerts to identify the hotfixes that are required for your operating system.

   - Policies and Guidelines

     Provides general guidelines for all SAN configurations.

Complete the iSCSI configuration worksheet

You require iSCSI identifiers, network addresses, and storage configuration information to perform iSCSI configuration tasks.

iSCSI identifiers

Initiator (host) iSCSI node name (IQN)
Target alias (optional)

Target network addresses

The storage virtual machine (SVM) is the iSCSI target.

You require a subnet with two IP addresses for iSCSI data LIFs for each node in the cluster. There should be two separate networks for high availability. The specific IP addresses are assigned by ONTAP when you create the LIFs as part of creating the SVM.

If possible, separate iSCSI traffic on separate physical networks or on VLANs.

Subnet for LIFs:

Node or LIF with port to switch	IP address	Network mask	Gateway	VLAN ID	Home port
Node 1 / LIF to switch 1					
Node 2 / LIF to switch 1					
Node 3 / LIF to switch 1					
Node 4 / LIF to switch 1					
Node 1 / LIF to switch 2					
Node 2 / LIF to switch 2					
Node 3 / LIF to switch 2					
Node 4 / LIF to switch 2					

Storage configuration

If the aggregate and SVM are already created, record their names here; otherwise, you can create them as required:

Node to own LUN
Aggregate name
SVM name

LUN information

LUN size
Host operating system
LUN name (optional)
LUN description (optional)

SVM information

If you are not using an existing SVM, you require the following information to create a new one:

SVM name	
SVM IPspace	
Aggregate for SVM root volume	
SVM user name (optional)	
SVM password (optional)	
SVM management LIF (optional)	
	Subnet:
	IP address:
	Network mask:
	Gateway:
	Home node:
	Home port:

Record the iSCSI initiator node name

You must record the iSCSI initiator node name from the iSCSI initiator program on the Windows host.

Steps

1. Open the **iSCSI Initiator Properties** dialog box:

If you are using…	Navigate to…
Windows Server 2012 or Windows Server 2012 R2 or Windows Server 2016	**Server Manager** > **Dashboard** > **Tools** > **iSCSI Initiator** > **Configuration**
Windows Server 2008, Windows Server 2008 R2	**Start** > **Administrative Tools** > **iSCSI Initiator**

2. Copy the **Initiator Name** or **Initiator Node Name** value to a text file or write it down.

   The exact label in the dialog box differs depending on the Windows version. The iSCSI initiator node name should look like the following example:

```
iqn.1991-05.com.microsoft:server3
```

Install Windows Unified Host Utilities

Windows Unified Host Utilities includes an installation program that sets the required Windows registry and HBA parameters so that the Windows host correctly handles the storage system behaviors for NetApp ONTAP and E-Series platforms.

Before you begin

You must have completed the following tasks:

- Check the supported configuration in the Interoperability Matrix

  NetApp Interoperability Matrix Tool

- Identified any required Windows hotfixes from the Interoperability Matrix

  NetApp Interoperability Matrix Tool

- Add the FCP license and start the target service
- Verify your cabling

  See *SAN Configuration* for your version of ONTAP or *Hardware Cabling* for your E-Series storage system on the NetApp Support Site for detailed cabling and configuration information.

About this task

You must specify whether to include multipathing support when you install the Windows Unified Host Utilities software package. Choose MPIO if you have more than one path from the Windows host or virtual machine to the storage system. Choose no MPIO only if you are using a single path to the storage system.

> The MPIO selection is not available for Windows XP and Windows Vista systems; multipath I/O is not supported on these guest operating systems.

For Hyper-V guests, raw (pass-through) disks do not appear in the guest OS if you choose multipathing support. You can either use raw disks, or you can use MPIO, but you cannot use both in the guest OS.

See Windows Unified Host Installation for detailed information.

Steps

1. Download the appropriate version of the Windows Unified Host Utilities from the NetApp Support Site.

   NetApp Support

2. Run the executable file and follow the instructions on the screen.
3. Reboot the Windows host when prompted.

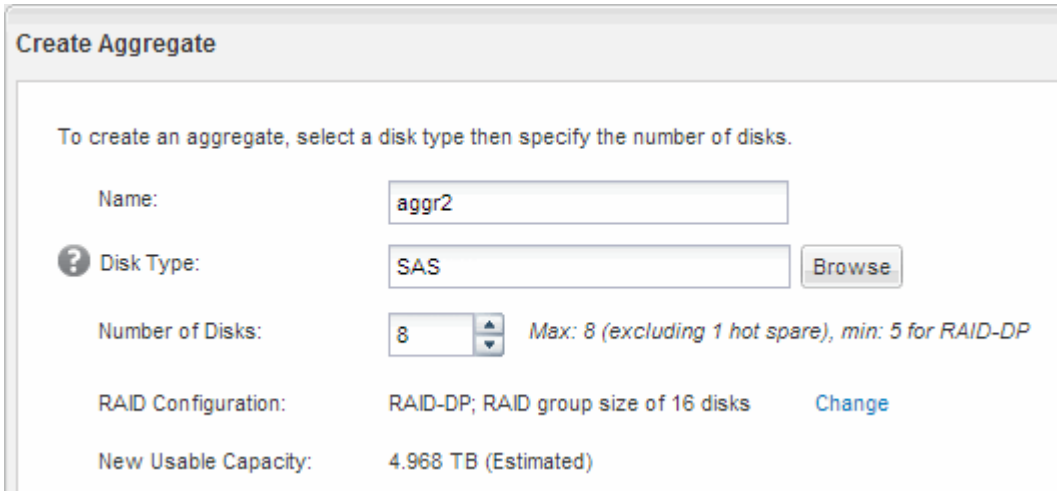
Create an aggregate

If you do not want to use an existing aggregate, you can create a new aggregate to

provide physical storage to the volume which you are provisioning.

Steps

1. Enter the URL `https://IP-address-of-cluster-management-LIF` in a web browser and log in to System Manager using your cluster administrator credential.
2. Navigate to the **Aggregates** window.
3. Click **Create.**
4. Follow the instructions on the screen to create the aggregate using the default RAID-DP configuration, and then click **Create**.



Results

The aggregate is created with the specified configuration and added to the list of aggregates in the Aggregates window.

Decide where to provision the volume

Before you provision a volume to contain your LUNs, you need to decide whether to add the volume to an existing storage virtual machine (SVM) or to create a new SVM for the volume. You might also need to configure iSCSI on an existing SVM.

About this task

If an existing SVM is already configured with the needed protocols and has LIFs that can be accessed from the host, it is easier to use the existing SVM.

You can create a new SVM to separate data or administration from other users of the storage cluster. There is no advantage to using separate SVMs just to separate different protocols.

Procedure

- If you want to provision volumes on an SVM that is already configured for iSCSI, you must verify that the iSCSI service is running and then create a LUN on the SVM.

  Verifying that the iSCSI service is running on an existing SVM

  Creating a LUN

- If you want to provision volumes on an existing SVM that has iSCSI enabled but not configured, configure iSCSI on the existing SVM.

  Configuring iSCSI on an existing SVM

  This is the case when you did not follow this procedure to create the SVM while configuring a different protocol.

- If you want to provision volumes on a new SVM, create the SVM.

  Creating a new SVM

Verify that the iSCSI service is running on an existing SVM

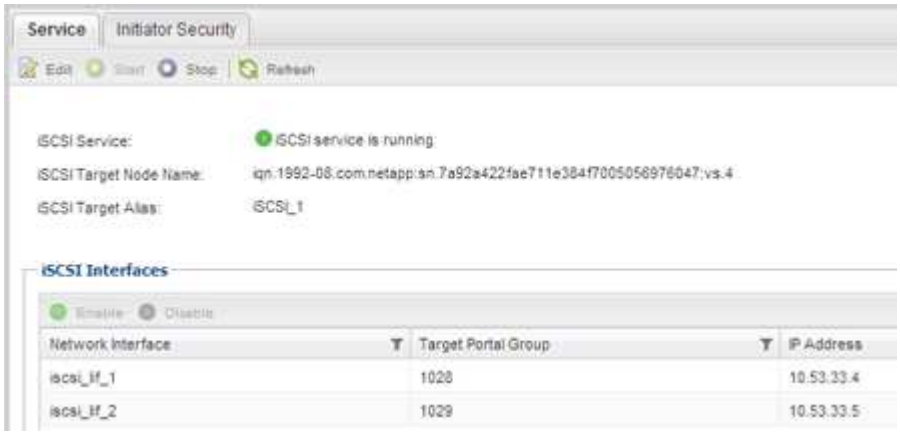
If you choose to use an existing storage virtual machine (SVM), you must verify that the iSCSI service is running on the SVM.

Before you begin

You must have selected an existing SVM on which you plan to create a new LUN.

Steps

1. Navigate to the **SVMs** window.
2. Click the **SVM Settings** tab.
3. In the **Protocols** pane, click **iSCSI**.
4. Verify that the iSCSI service is running.



5. Record the iSCSI interfaces listed for the SVM.

What to do next

If the iSCSI service is not running, start the iSCSI service or create a new SVM.

If there are fewer than two iSCSI interfaces per node, update the iSCSI configuration on the SVM or create a new SVM for iSCSI.

Create a LUN

You use the Create LUN wizard to create a LUN. The wizard also creates the igroup and maps the LUN to the igroup, which enables the specified host to access the LUN.

Before you begin

- There must be an aggregate with enough free space to contain the LUN.
- There must be a storage virtual machine (SVM) with the iSCSI protocol enabled and the appropriate logical interfaces (LIFs) created.
- You must have recorded the iSCSI initiator node name of the host.

LUNs are mapped to a subset of the initiators in the igroup to limit the number of paths from the host to the LUN.

- By default, ONTAP uses Selective LUN Map (SLM) to make the LUN accessible only through paths on the node owning the LUN and its high-availability (HA) partner.
- You still must configure all of the iSCSI LIFs on every node for LUN mobility in case the LUN is moved to another node in the cluster.
- When moving a volume or a LUN, you must modify the SLM reporting-nodes list before moving.

About this task

If your organization has a naming convention, you should use names for the LUN, volume, and so on that fit your convention. Otherwise, you should accept the default names.

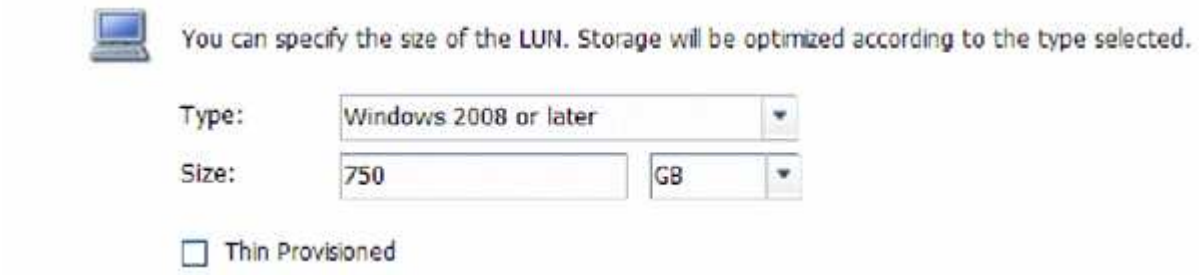
Steps

1. Navigate to the **LUNs** window.
2. Click **Create.**
3. Browse and select an SVM in which you want to create the LUNs.

   The Create LUN Wizard is displayed.

4. On the **General Properties** page, select the LUN type **Windows 2008 or later** for LUNs used directly by the Windows host, or select **Hyper-V** for LUNs containing virtual hard disks (VHDs) for Hyper-V virtual machines.

   Leave the **Thin Provisioned** check box unselected.



5. On the **LUN Container** page, select an existing FlexVol volume.

   You must ensure that there is enough space in the volume. If sufficient space is not available in the existing volumes, you can create a new volume.

6. On the **Initiators Mapping** page, click **Add Initiator Group**, enter the required information on the **General** tab, and then on the **Initiators** tab, enter the iSCSI initiator node name of the host that you recorded.
7. Confirm the details, and then click **Finish** to complete the wizard.

Related information

Configure iSCSI on an existing SVM

You can configure iSCSI on an existing storage virtual machine (SVM)and create a LUN and its containing volume with a single wizard. The iSCSI protocol must already be enabled but not configured on the SVM. This information is intended for SVMs for which you are configuring multiple protocols, but have not yet configured iSCSI.

Before you begin

You must have enough network addresses available to create two LIFs for each node.

About this task

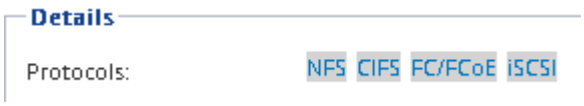
LUNs are mapped to a subset of the initiators in the igroup to limit the number of paths from the host to the LUN.

- ONTAP uses Selective LUN Map (SLM) to make the LUN accessible only through paths on the node owning the LUN and its HA partner.
- You still must configure all of the iSCSI LIFs on every node for LUN mobility in case the LUN is moved to another node in the cluster.
- You must modify the SLM reporting-nodes list before moving a volume or a LUN.

Steps

1. Navigate to the **SVMs** window.
2. Select the SVM that you want to configure.
3. In the SVM**Details** pane, verify that **iSCSI** is displayed with a gray background, which indicates that the protocol is enabled but not fully configured.

   If **iSCSI** is displayed with a green background, the SVM is already configured.

4. Click the **iSCSI** protocol link with the gray background.

   The Configure iSCSI Protocol window is displayed.

5. Configure the iSCSI service and LIFs from the **Configure iSCSI protocol** page:

   a. Enter a target alias name.

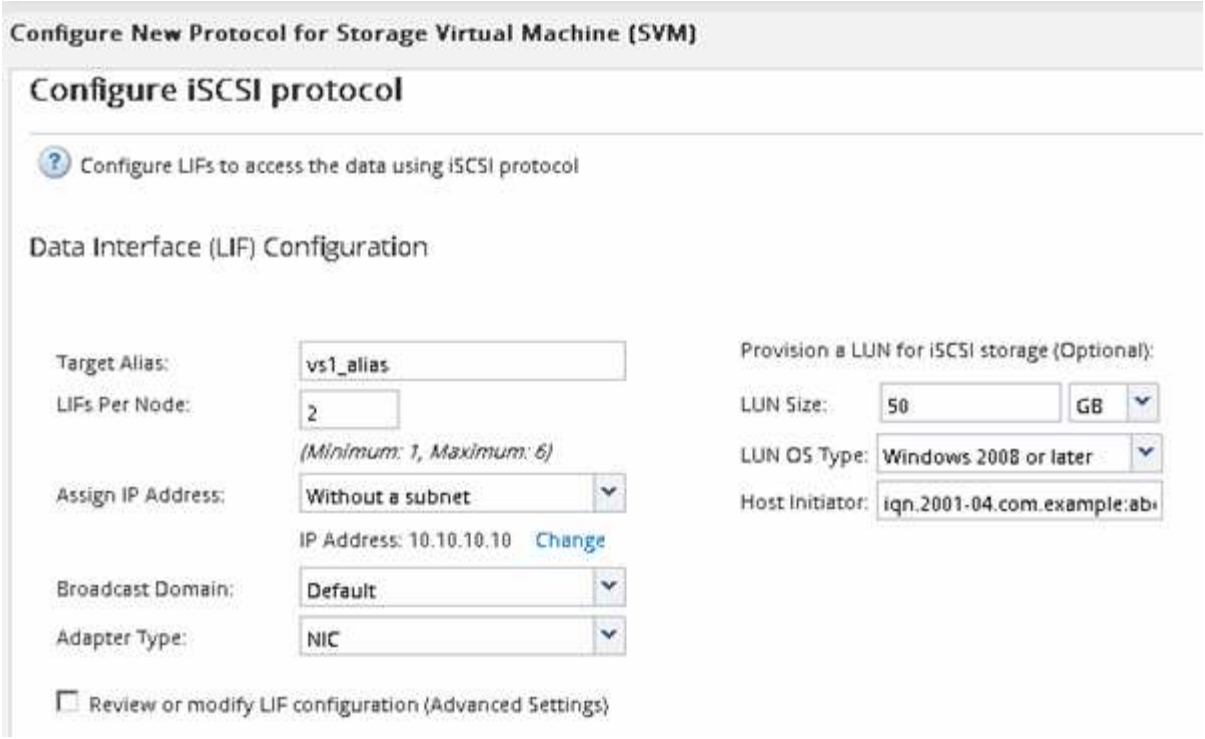
   b. Enter **2** in the **LIFs per node** field.

      Two LIFs are required for each node to ensure availability and data mobility.

   c. Assign IP addresses for the LIFs either with a subnet or without a subnet.

   d. In the **Provision a LUN for iSCSI storage** area, enter the desired LUN size, host type, and iSCSI initiator name of the host.

   e. Click **Submit & Close**.



6. Review the **Summary** page, record the LIF information, and then click **OK**.

Create a new SVM

The storage virtual machine (SVM) provides the iSCSI target through which a host accesses LUNs. When you create the SVM, you also create logical interfaces (LIFs) and the LUN and its containing volume. You can create an SVM to separate the data and administration functions of a user from those of the other users in a cluster.

Before you begin

- You must have enough network addresses available to create two LIFs for each node.

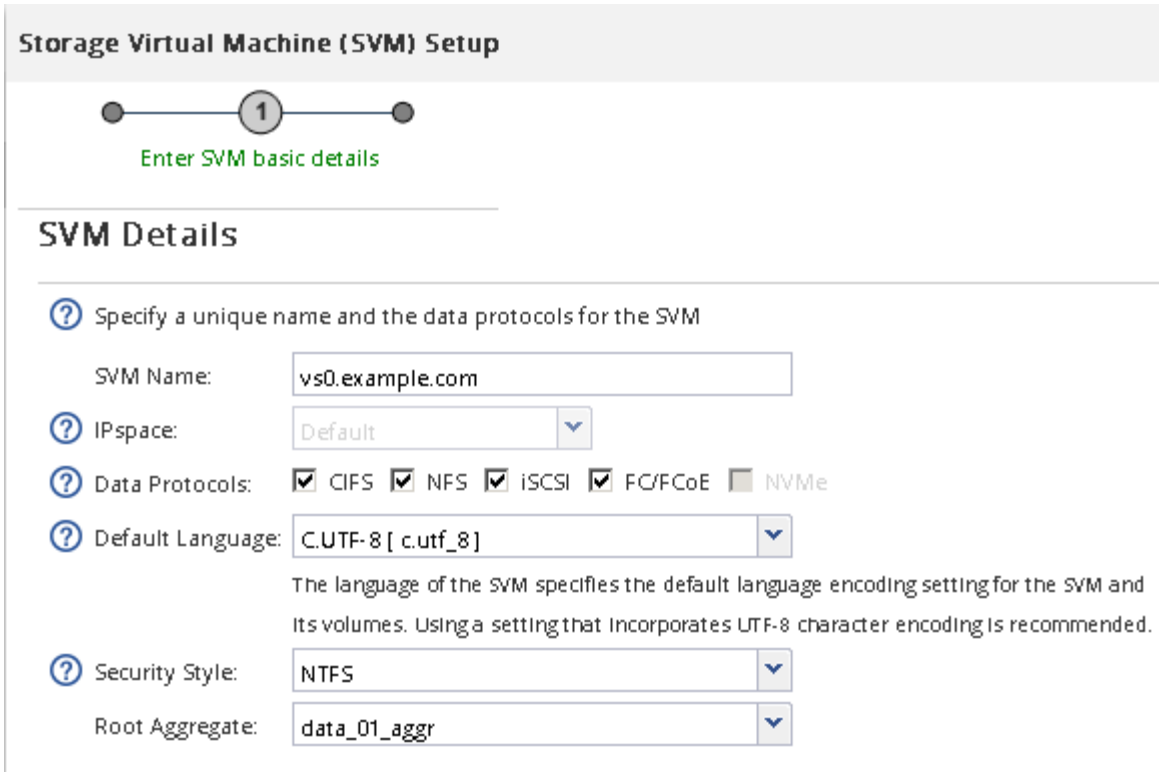
About this task

LUNs are mapped to a subset of the initiators in the igroup to limit the number of paths from the host to the LUN.

- By default, ONTAP uses Selective LUN Map (SLM) to make the LUN accessible only through paths on the node owning the LUN and its HA partner.
- You still must configure all of the iSCSI LIFs on every node for LUN mobility in case the LUN is moved to another node in the cluster.
- When moving a volume or a LUN, you must modify the SLM-reporting-nodes list before moving.

Steps

1. Navigate to the **SVMs** window.
2. Click **Create**.
3. In the **Storage Virtual Machine (SVM) Setup** window, create the SVM:



a. Specify a unique name for the SVM.

   The name must either be a fully qualified domain name (FQDN) or follow another convention that ensures unique names across a cluster.

b. Select the IPspace that the SVM will belong to.

   If the cluster does not use multiple IPspaces, the “Default” IPspace is used.

c. Keep the default volume type selection.

   Only FlexVol volumes are supported with SAN protocols.

d. Select all of the protocols that you have licenses for and that you might use on the SVM, even if you do not want to configure all of the protocols immediately.

   Selecting both NFS and CIFS when you create the SVM enables these two protocols to share the same LIFs. Adding these protocols later does not allow them to share LIFs.

   If CIFS is one of the protocols you selected, then the security style is set to NTFS. Otherwise, the security style is set to UNIX.

e. Keep the default language setting C.UTF-8.

f. Select the desired root aggregate to contain the SVM root volume.

   The aggregate for the data volume is selected separately in a later step.

g. Click **Submit & Continue**.

The SVM is created, but protocols are not yet configured.

4. If the **Configure CIFS/NFS protocol** page appears because you enabled CIFS or NFS, click **Skip** and

then configure CIFS or NFS later.

5. Configure the iSCSI service and create LIFs, and the LUN and its containing volume from the **Configure iSCSI protocol** page:

   a. **Optional:** Enter a target alias name.

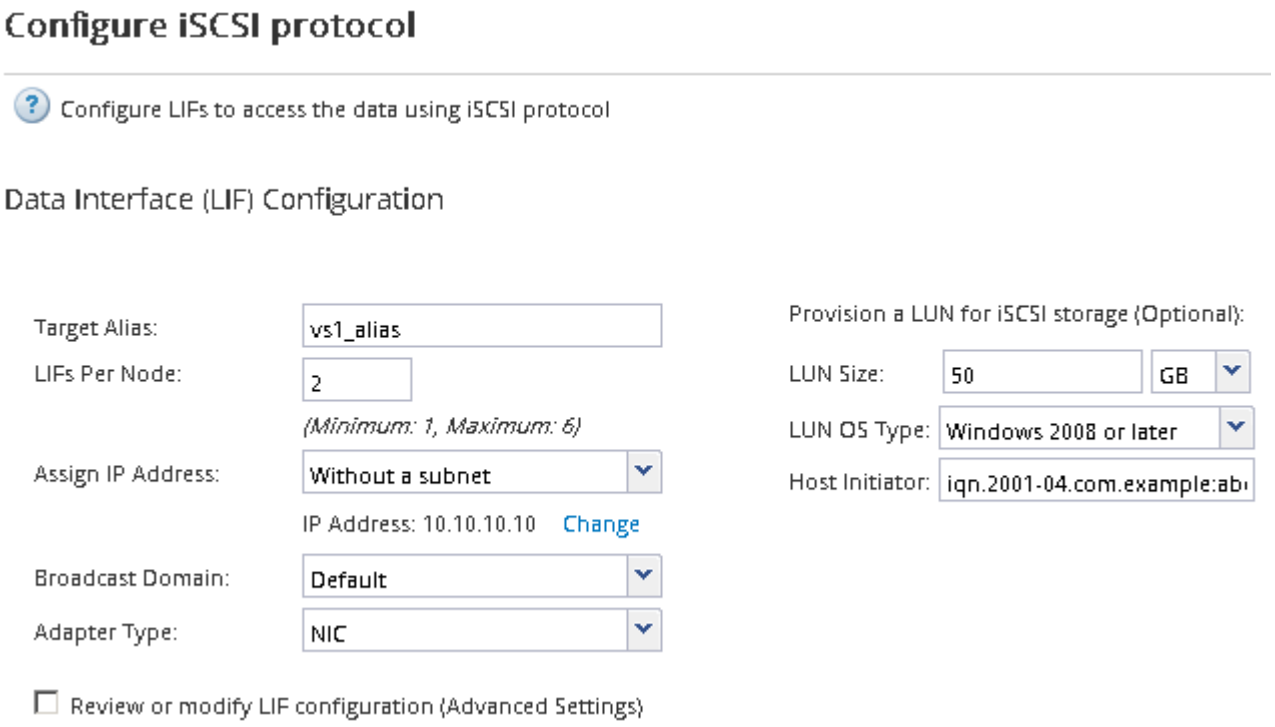
   b. Assign IP address for the LIFs either by using a subnet or without a subnet.

   c. Enter **2** in the **LIFs per node** field.

      Two LIFs are required for each node to ensure availability and data mobility.

   d. In the **Provision a LUN for iSCSI storage** area, enter the desired LUN size, host type, and iSCSI initiator name of the host.

   e. Click **Submit & Continue**.



6. If the **Configure FC/FCoE protocol** page appears because you enabled FC, click **Skip** and then configure FC later.

7. When the **SVM Administration** appears, configure or defer configuring a separate administrator for this SVM:

   - Click **Skip** and configure an administrator later if desired.
   - Enter the requested information, and then click **Submit & Continue**.

8. Review the **Summary** page, record the LIF information, and then click **OK**.

Start iSCSI sessions with the target

The Windows host must have an iSCSI connection to each node in the cluster. You establish the sessions from the host by using the iSCSI Initiator Properties dialog box on the host.

Before you begin

You must know the IP address of an iSCSI data LIF on the storage virtual machine (SVM) that contains the LUN you are accessing.

About this task

In ONTAP, the iSCSI host must have paths to each node in the cluster. The native DSM selects the best paths to use. If paths fail, the native DSM selects alternate paths.

The buttons and labels in the iSCSI Initiator Properties dialog box vary between versions of Windows. Some of the steps in the task include more than one button or label name; you should pick the name that matches the version of Windows you are using.

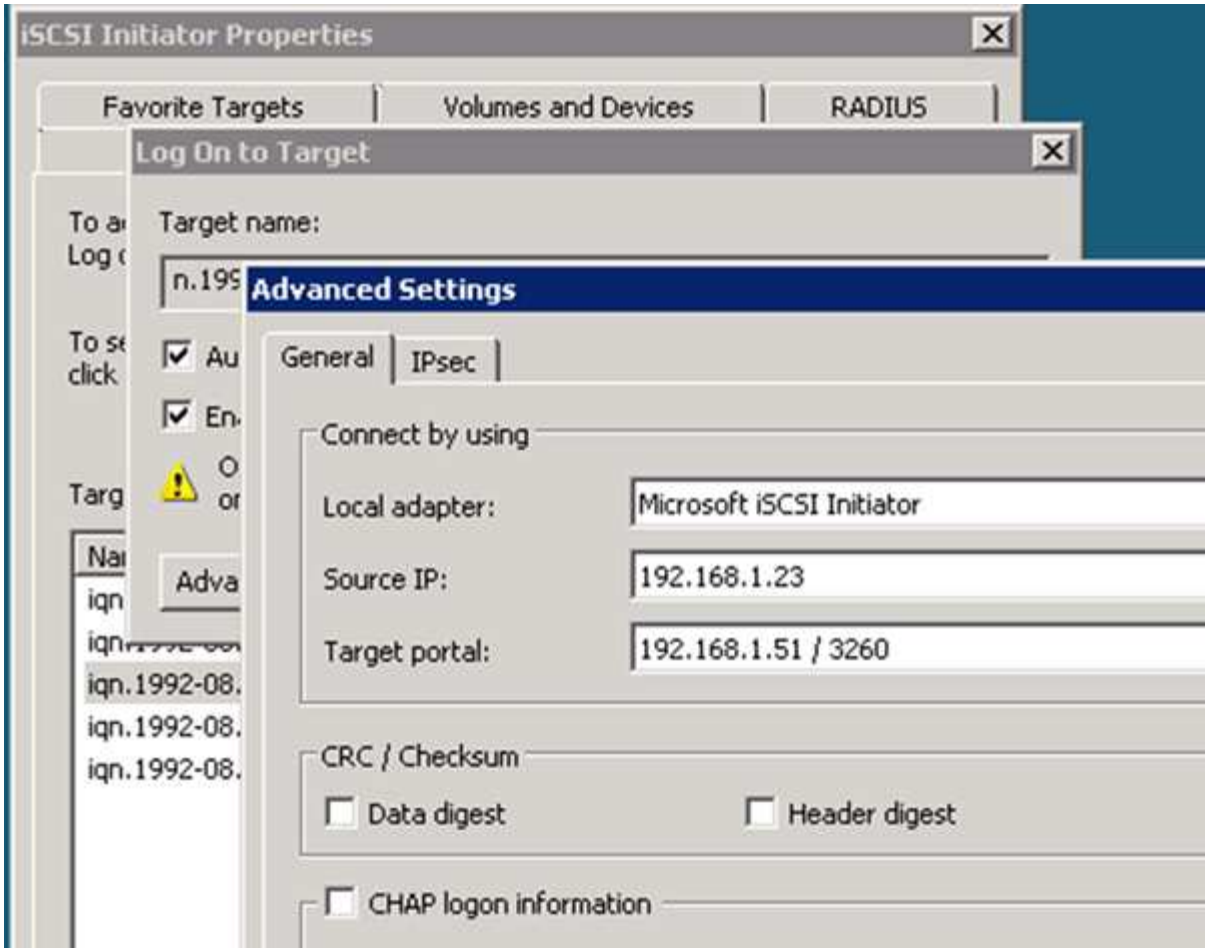
Steps

1. Open the **iSCSI Initiator Properties** dialog box:

For…	Click…
Windows Server 2012	**Server Manager** > **Dashboard** > **Tools** > **iSCSI Initiator**
Windows Server 2008	**Start** > **Administrative Tools** > **iSCSI Initiator**

2. On the **Discovery** tab, click **Discover Portal** or **Add Portal**, and then enter the IP address of the iSCSI target port.
3. On the **Targets** tab, select the target you discovered, and then click **Log on** or **Connect**.
4. Select **Enable multi-path**, select **Automatically restore this connection when the computer starts** or **Add this connection to the list of Favorite Targets**, and then click **Advanced**.
5. For **Local adapter**, select **Microsoft iSCSI Initiator**.

   The following example is from Windows Server 2008:



6. For **Source IP** or **Initiator IP**, select the IP address of a port on the same subnet or VLAN as one of the iSCSI target LIFs.
7. Retain the default values for the remaining check boxes, and then click **OK**.
8. On the **Targets** tab, select the same target again, and then click **Log on** or **Connect**.
9. Select **Enable multi-path**, select **Automatically restore this connection when the computer starts** or **Add this connection to the list of Favorite Targets**, and then click **Advanced**.
10. For **Source IP** or **Initiator IP**, select the IP address of a different port on the subnet or VLAN of a different iSCSI target LIF.
11. For **Target portal**, select the IP address of the iSCSI target LIF that corresponds to the port you just selected for **Source IP**.
12. Retain the default values for the remaining check boxes, and then click **OK**.
13. Repeat steps 8 through 12 to connect to each target LIF that is available.

Discover new disks

LUNs on your storage virtual machine (SVM) appear as disks to the Windows host. Any new disks for LUNs you add to your system are not automatically discovered by the host. You must manually rescan disks to discover them.

Steps

1. Open the Windows Computer Management utility:

If you are using…	Navigate to…
Windows Server 2012	**Tools** > **Computer Management**
Windows Server 2008	**Start** > **Administrative Tools** > **Computer Management**
Windows Server 2016	**Start > Administrative Tools > Computer Management**

2. Expand the **Storage** node in the navigation tree.
3. Click **Disk Management**.
4. Click **Action** > **Rescan Disks**.

Initialize and format the LUN

When a new LUN is first accessed by the Windows host, it has no partition or file system. You must initialize the LUN, and optionally format it with a file system.

Before you begin

The LUN must have been discovered by the Windows host.

About this task

LUNs appear in Windows Disk Management as disks.

You can initialize the disk as a basic disk with a GPT or MBR partition table.

You typically format the LUN with a file system such as NTFS, but some applications use raw disks instead.

Steps

1. Start Windows Disk Management.
2. Right-click the LUN, and then select the required disk or partition type.
3. Follow the instructions in the wizard.

   If you choose to format the LUN as NTFS, you must select the **Perform a quick format** check box.

Verify that the host can write to and read from the LUN

Before using the LUN, you should verify that the host can write data to the LUN and read it back.

Before you begin

The LUN must be initialized and formatted with a file system.

About this task

If the storage cluster node on which the LUN is created can be failed over to its partner node, you should verify reading the data while the node is failed over. This test might not be possible if the storage cluster is in production use.

If any of the tests fail, you should verify that the iSCSI service is running and check the iSCSI paths to the LUN.

Steps

1. On the host, copy one or more files to the LUN.
2. Copy the files back to a different folder on the original disk.
3. Compare the copied files to the original.

   You can use the `comp` command at the Windows command prompt to compare two files.

4. **Optional:** Fail over the storage cluster node containing the LUN and verify that you can still access the files on the LUN.
5. Use the native DSM to view the paths to the LUN and verify that you have the expected number of paths.

   You should see two paths to the storage cluster node on which the LUN is created, and two paths to the partner node.

Data protection and disaster recovery

Cluster and SVM peering configuration

Cluster and SVM peering overview

Cluster administrators can create authenticated peer relationships between clusters and SVMs to enable the clusters to communicate with each other so that data is replicated between volumes in different clusters. You can perform the procedures using the ONTAP System Manager *classic* interface, which is available with ONTAP 9.7 and earlier ONTAP 9 releases.

Use the ONTAP System Manager *classic* interface to create cluster peer relationships and SVM peer relationships if the following apply:

- You are working with clusters running ONTAP 9.7 or earlier ONTAP 9 releases.
- You want cluster peering relationships that are authenticated.
- You want to use best practices, not explore every available option.
- You want to use System Manager, not the ONTAP command-line interface (CLI) or an automated scripting tool.

Other ways to do this in ONTAP

ONTAP System Manager in ONTAP 9.3 simplifies the way that you configure peer relationships between clusters and between SVMs. The cluster peering procedure and SVM peering procedure can be used for all ONTAP 9 versions. You should use the appropriate procedure for your version of ONTAP.

To perform these tasks with…	Refer to…
The redesigned System Manager (available with ONTAP 9.7 and later)	• Cluster management with System Manager
The ONTAP command-line interface (CLI)	• Cluster and SVM peering overview with the CLI Use the command-line interface to set up cluster peering relationships and SVM peering relationships. • Network management Use the command-line interface to configure subnets, intercluster LIFs, routes, firewall policies, and other networking components

Prerequisites for cluster peering

Before you set up cluster peering using the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier, you should confirm that the connectivity, port, IP address,

subnet, firewall, and cluster-naming requirements are met.

Connectivity requirements

Every intercluster LIF on the local cluster must be able to communicate with every intercluster LIF on the remote cluster.

Although it is not required, it is typically simpler to configure the IP addresses used for intercluster LIFs in the same subnet. The IP addresses can reside in the same subnet as data LIFs, or in a different subnet. The subnet used in each cluster must meet the following requirements:

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

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

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

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

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

Port requirements

You can use dedicated ports for intercluster communication, or share ports used by the data network. Ports must meet the following requirements:

- All ports that are used to communicate with a given remote cluster must be in the same IPspace.

  You can use multiple IPspaces to peer with multiple clusters. Pair-wise full-mesh connectivity is required only within an IPspace.

- The broadcast domain that is used for intercluster communication must include at least two ports per node so that intercluster communication can fail over from one port to another port.

  Ports added to a broadcast domain can be physical network ports, VLANs, or interface groups (ifgrps).

- All ports must be cabled.
- All ports must be in a healthy state.
- The MTU settings of the ports must be consistent.

Firewall requirements

Firewalls and the intercluster firewall policy must allow the following protocols:

- ICMP service
- TCP to the IP addresses of all the intercluster LIFs over the ports 10000, 11104, and 11105
- Bidirectional HTTPS between the intercluster LIFs

Although HTTPS is not required when you set up cluster peering using the CLI, HTTPS is required later if you use ONTAP System Manager to configure data protection.

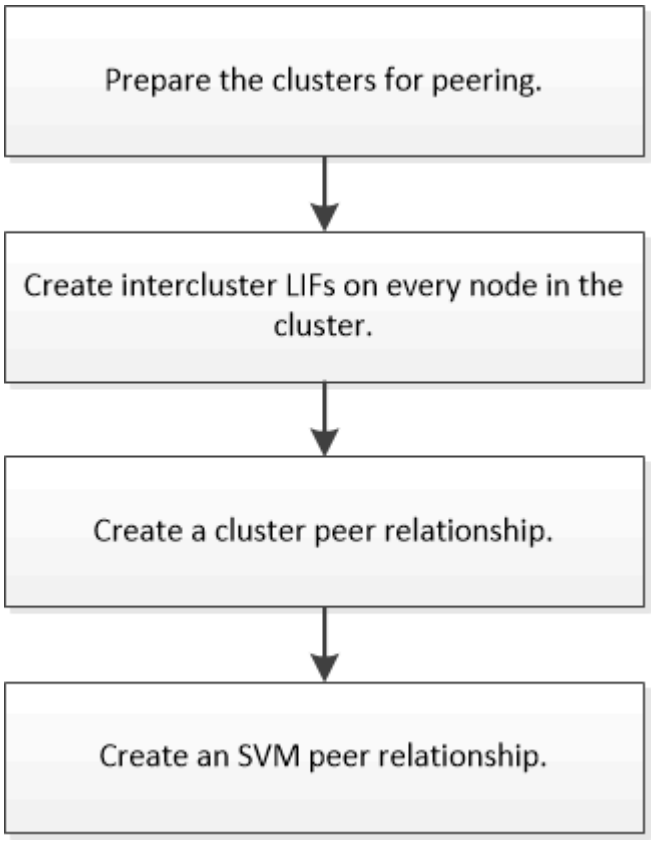
The default `intercluster` firewall policy allows access through the HTTPS protocol and from all IP addresses (0.0.0.0/0). You can modify or replace the policy if necessary.

Related information

Data protection

Cluster and SVM peering workflow

You can set up a peering relationship by using the ONTAP System Manager with ONTAP 9.7 or earlier.
Setting up a peering relationship involves preparing each cluster for peering, creating intercluster logical interfaces (LIFs) on each node of each cluster, setting up a cluster peer relationship, and then setting up an SVM peering relationship.



If you are running ONTAP 9.2 or earlier, you create an SVM peering relationship while creating a data protection relationship between the source volume and the destination volume.

Prepare for cluster peering

Before creating a cluster peering relationship using the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier, you must verify that the time on each cluster is synchronized with an external Network Time Protocol (NTP) server, and determine the subnets, ports, and passphrases that you want to use.

Steps

1. If you are running ONTAP 9.2 or earlier, determine the passphrase that you want to use for each cluster peer relationship.

   The passphrase must include at least eight characters.

For the relationship between…	The passphrase is…
Cluster A and Cluster B	

   Beginning with ONTAP 9.3, you can generate the passphrase from the remote cluster while creating the cluster peer relationship.

   Creating a cluster peer relationship (Beginning with ONTAP 9.3)

2. Identify the subnets, IP addresses, and ports that you will use for intercluster LIFs.

   By default, the IP address is automatically selected from the subnet. If you want to specify the IP address manually, you must ensure that the IP address either is already available in the subnet or can be added to the subnet later. Information about subnets is available in the Network tab.

   Create a table similar to the following table to record information about the clusters. The following table assumes that each cluster has four nodes. If a cluster has more than four nodes, add rows for the additional information.

	Cluster A	Cluster B
Subnet (ONTAP 9.2 or earlier)		
IP address (Beginning with ONTAP 9.3, optional for ONTAP 9.2 or earlier)		
Node 1 port		
Node 2 port		
Node 3 port		
Node 4 port		

Configure peer relationships (Beginning with ONTAP 9.3)

A peer relationship defines the network connections that enable clusters and SVMs to exchange data securely. Beginning with ONTAP 9.3, until ONTAP 9.7, you can use the ONTAP System Manager *classic* interface to perform a simplified method to configure peer relationships between clusters and between SVMs.

Create intercluster LIFs (Beginning with ONTAP 9.3)

Beginning with ONTAP 9.3, until ONTAP 9.7, you can use the ONTAP System Manager *classic* interface to create intercluster logical interfaces (LIFs), which enable the cluster network to communicate with a node. You must create an intercluster LIF within each IPspace that will be used for peering, on each node in each cluster for which you want to create a peer relationship.

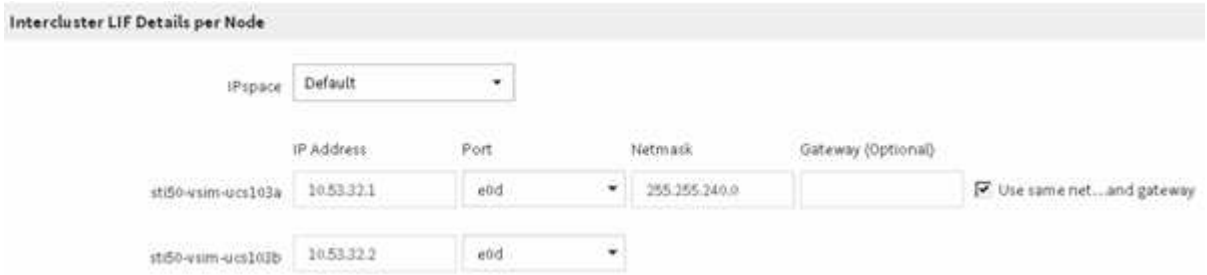
About this task

For example, if you have a four-node cluster that you want to peer with cluster X over IPspace A, and peer with cluster Y over IPspace Y, then you need a total of eight intercluster LIFs; Four on IPspace A (one per node), and four on IPspace Y (one per node).

You must perform this procedure on both clusters for which you want to create a peer relationship.

Steps

1. Click **Configuration** > **Advanced Cluster Setup**.
2. In the **Setup Advanced Cluster Features** window, click **Proceed** next to the **Cluster Peering** option.
3. Select an IPspace from the **IPspace** list.
4. Enter the IP address, port, network mask, and gateway details of each node.



5. Click **Submit and Continue**.

What to do next

You should enter the cluster details in the Cluster Peering window to continue with cluster peering.

Create a cluster peer relationship (Beginning with ONTAP 9.3)

Beginning with ONTAP 9.3, until ONTAP 9.7, you can use the ONTAP System Manager *classic* interface create a cluster peer relationship between two clusters by providing a system-generated passphrase and the IP addresses of the intercluster LIFs of the remote cluster.

About this task

Beginning with ONTAP 9.6, cluster peering encryption is enabled by default on all newly created cluster peering relationships. Cluster peering encryption must be enabled manually for peering relationship created prior to upgrading to ONTAP 9.6. Cluster peering encryption is not available for clusters running ONTAP 9.5 or earlier. Therefore, both clusters in the peering relationship must be running ONTAP 9.6 in order to enable cluster peering encryption.

Cluster peering encryption uses the Transport Security Layer (TLS) to secure cross-cluster peering

communications for ONTAP features such as SnapMirror and FlexCache.

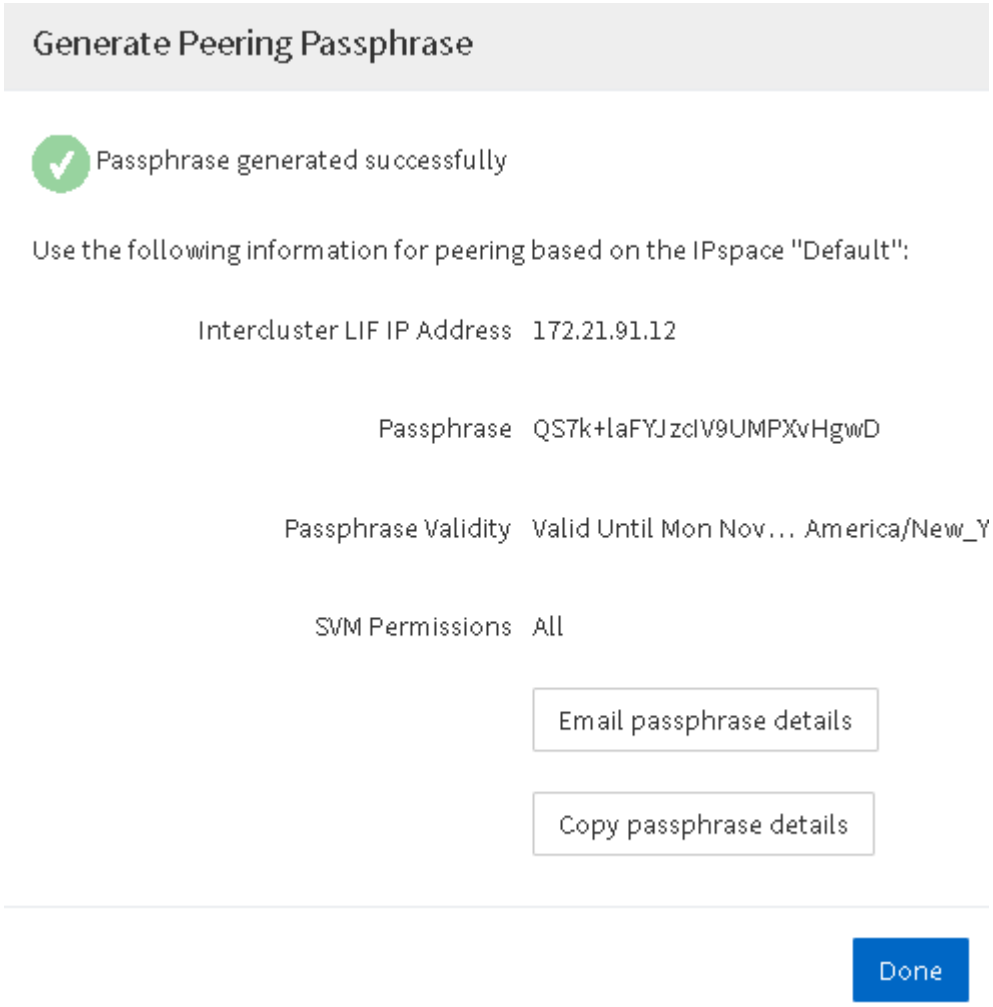
Steps

1. In the **Target Cluster Intercluster LIF IP addresses** field, enter the IP addresses of the intercluster LIFs of the remote cluster.
2. Generate a passphrase from the remote cluster.
   a. Specify the management address of the remote cluster.
   b. Click **Management URL** to launch ONTAP System Manager on the remote cluster.
   c. Log in to the remote cluster.
   d. In the **Cluster Peers** window, click **Generate Peering Passphrase**.
   e. Select the IPspace, validity of the passphrase, and SVM permissions.

      You can allow all of the SVMs or selected SVMs for peering. When a SVM peer request is generated, the permitted SVMs are automatically peered with the source SVMs without requiring you to accept the peer relationship from the remote SVMs.

   f. Click **Generate**.

      The passphrase information is displayed.



   g. Click **Copy passphrase details** or **Email passphrase details**.

h. Click **Done**.

3. In the source cluster, enter the generated passphrase that you obtained in Step 2.
4. Click **Initiate Cluster Peering**.

   The cluster peer relationship is successfully created.

5. Click **Continue**.

What to do next

You should specify the SVM details in the SVM Peering window to continue with the peering process.

Create SVM peer relationships

Beginning with ONTAP 9.3, until ONTAP 9.7, you can use the ONTAP System Manager *classic* interface to create SVM peer relationships. The storage virtual machine (SVM) peering enables you to establish a peer relationship between two SVMs for data protection.

Steps

1. Select the initiator SVM.
2. Select the target SVM from the list of permitted SVMs.
3. Click **Initiate SVM Peering**.
4. Click **Continue**.

What to do next

You can view the intercluster LIFs, cluster peer relationship, and SVM peer relationship in the Summary window.

Configure peer relationships (ONTAP 9.2 and earlier)

Using the ONTAP System Manager *classic* interface with ONTAP 9.2 or an earlier ONTAP 9 release, you can create SVM peer relationships.

A peer relationship defines network connections that enable clusters and SVMs to exchange data securely. You must create a cluster peer relationship before you can create an SVM peer relationship.

Create intercluster interfaces on all nodes (ONTAP 9.2 or earlier)

Using the ONTAP System Manager *classic* interface with ONTAP 9.2 or an earlier ONTAP 9 release, you can create intercluster LIFs that will be used for peering.

Clusters communicate with each other through logical interfaces (LIFs) that are dedicated to intercluster communication. You must create an intercluster LIF within each IPspace that will be used for peering. The LIFs must be created on each node in each cluster for which you want to create a peer relationship.

Before you begin

You must have identified the subnet and ports, and optionally the IP addresses, that you plan to use for the intercluster LIFs.

About this task

You must perform this procedure on both clusters for which you want to create a peer relationship. For example, if you have a four-node cluster that you want to peer with cluster X over IPspace A, and peer with cluster Y over IPspace Y, then you need a total of eight intercluster LIFs; Four on IPspace A (one per node), and four on IPspace Y (one per node).

Steps

1. Create an intercluster LIF on one node of the source cluster:
   a. Navigate to the **Network Interfaces** window.
   b. Click **Create**.

      The Create Network Interface dialog box is displayed.

   c. Enter a name for the intercluster LIF.

      You can use “icl01” for the intercluster LIF on the first node, and “icl02” for the intercluster LIF on the second node.

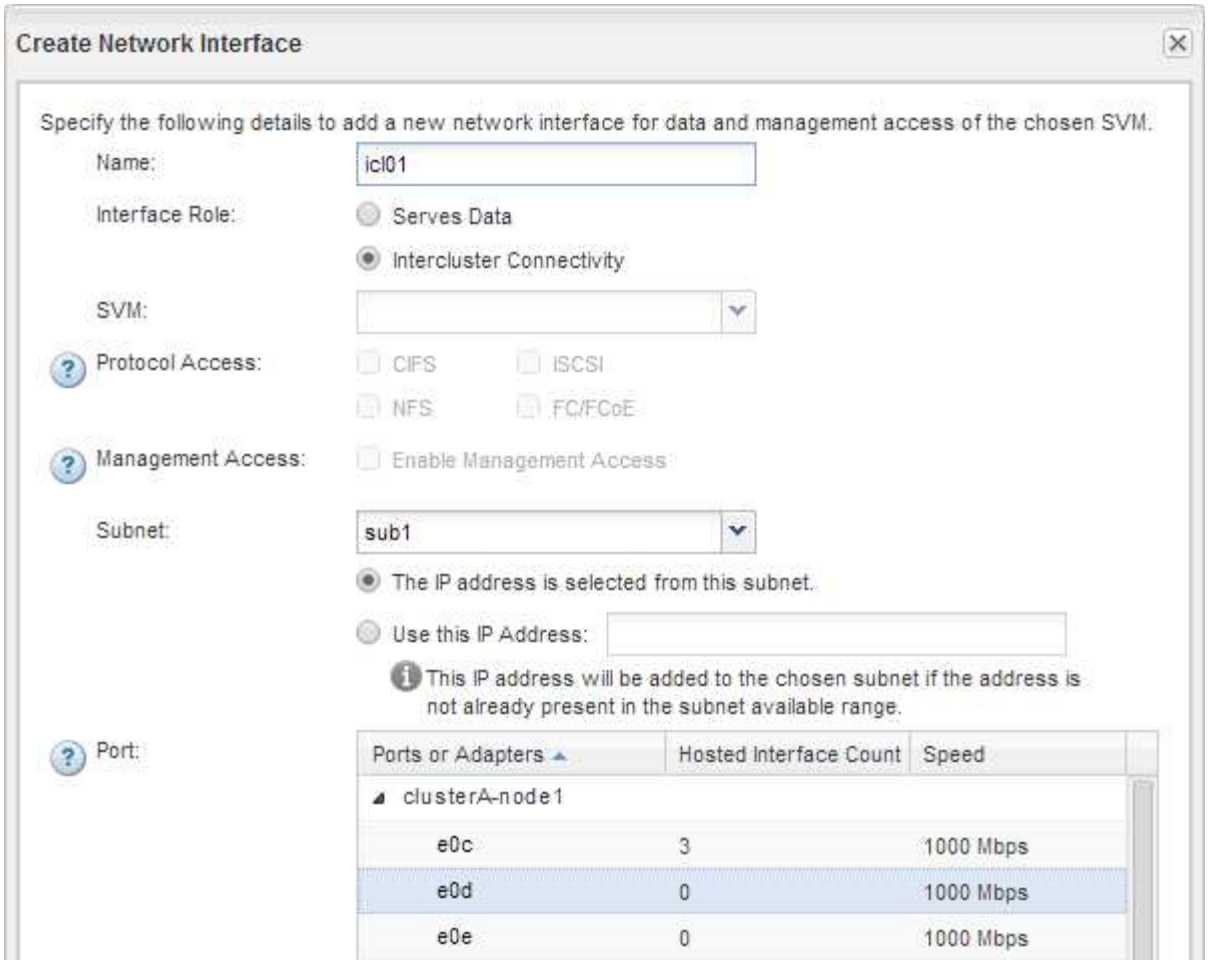
   d. Select **Intercluster Connectivity** as the interface role.
   e. Select the IPspace.
   f. In the **Add Details** dialog box, select **Using a subnet** from the **Assign IP Address** drop-down list, and then select the subnet that you want to use for intercluster communication.

      By default, the IP address is automatically selected from the subnet after you click **Create**. If you do not want to use the IP address that is automatically selected, you must manually specify the IP address that the node uses for intercluster communication.

   g. If you want to manually specify the IP address that the node uses for intercluster communication, select **Use this IP Address**, and type the IP address.

      You must ensure that the IP address that you want to use either is already available in the subnet or can be added to the subnet later.

   h. In the **Ports** area, click the node that you are configuring, and select the port that you want to use for this node.
   i. If you decided not to share ports for intercluster communication with data communication, confirm that the selected port displays “0” in the **Hosted Interface Count** column.



j. Click **Create**.

2. Repeat Step 1 for each node in the cluster.

   Each node in the cluster has an intercluster LIF.

3. Make a note of the IP addresses of the intercluster LIFs so that you can use them later when you create peer relationships with other clusters:

   a. In the **Network Interfaces** window, in the **Role** column, click , clear the **All** check box, and then select **Intercluster**.

      The Network Interfaces window displays only intercluster LIFs.

   b. Note down the IP addresses that are listed in the **IP Addresses/WWPN** column, or leave the **Network Interfaces** window open so that you can retrieve the IP addresses later.

      You can click the column display icon ( ) to hide the columns that you do not want to view.

Results

All of the nodes in each cluster have intercluster LIFs that can all communicate with each other.

Create a cluster peer relationship (ONTAP 9.2 or earlier)

Using the ONTAP System Manager *classic* interface with ONTAP 9.2 or an earlier ONTAP 9 release, you can create a cluster peer relationship between two clusters by

entering a predetermined passphrase and the IP addresses of the intercluster LIFs of the remote cluster, and then verifying that the relationship was created successfully.

Before you begin

- You must know the IP addresses of all of the intercluster LIFs of the clusters that you want to peer.
- You must know the passphrase that you will use for each peer relationship.

About this task

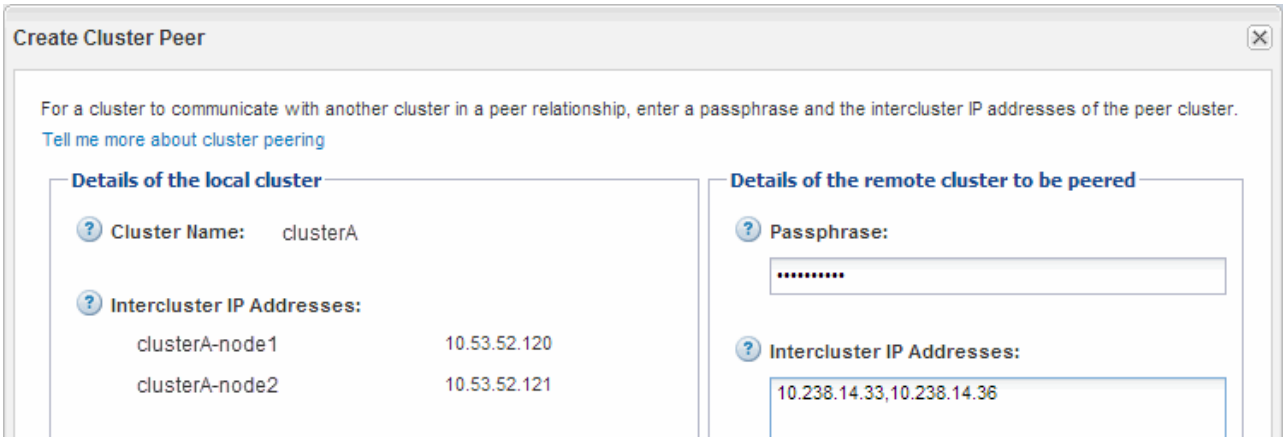
You must perform this procedure on each cluster.

Steps

1. From the source cluster, create a cluster peer relationship with the destination cluster.
   a. Click the **Configurations** tab.
   b. In the **Cluster Settings** pane, click **Cluster Peers**.
   c. Click **Create**.

      The **Create Cluster Peer** dialog box is displayed.

   d. In the **Details of the remote cluster to be peered** area, specify the passphrase that both peers will use to ensure an authenticated cluster peer relationship.
   e. Enter the IP addresses of all of the intercluster LIFs of the destination cluster (one per node) separated by commas.



   f. Click **Create**.

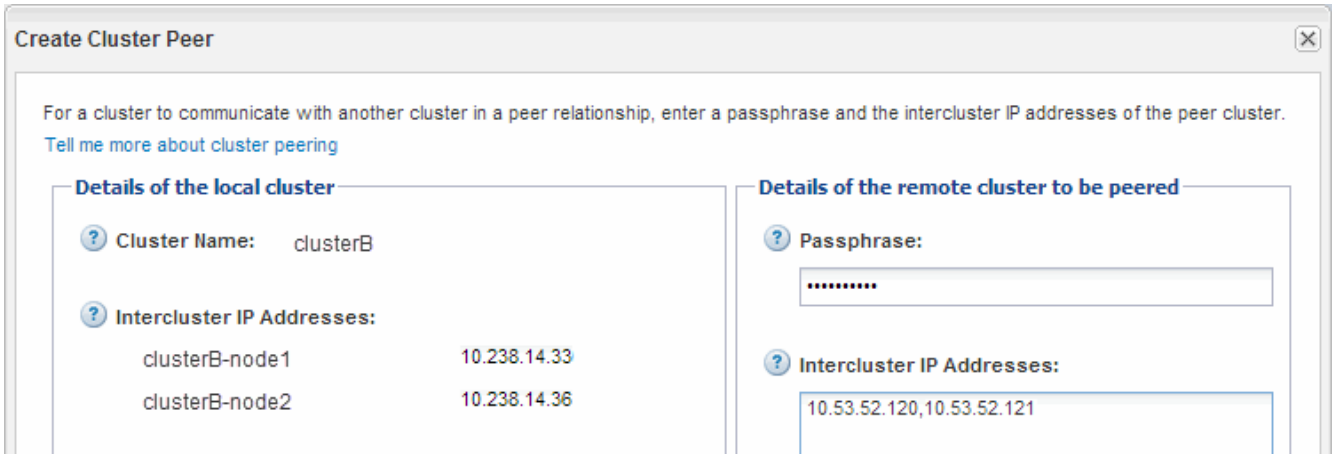
      The authentication status is “pending” because only one cluster has been configured.

2. Switch to the destination cluster, and then create a cluster peer relationship with the source cluster:
   a. Click the **Configurations** tab.
   b. In the **Cluster Settings** pane, click **Cluster Peers**.
   c. Click **Create**.

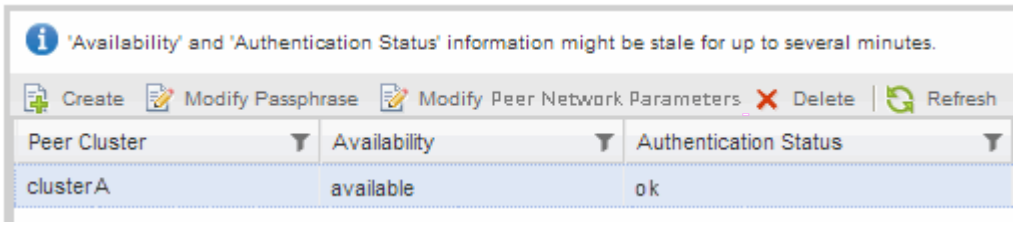
      The Create Cluster Peer dialog box is displayed.

   d. In the **Details of the remote cluster to be peered** area, specify the same passphrase that you specified in Step 1d and the IP addresses of the intercluster LIFs of the source cluster, and then click

Create.



3. From the **Cluster Peers** window of the destination cluster, confirm that the source cluster is “available” and that the authentication status is “OK”.



   You might have to click **Refresh** to view the updated information.

   The two clusters are in a peer relationship.

4. Switch to the source cluster, and confirm that the destination cluster is “available” and that the authentication status is “OK”.

   You might have to click **Refresh** to view the updated information.

What to do next

Create an SVM peer relationship between the source and destination SVMs while creating a data protection relationship between the source volume and the destination volume.

Volume backup using SnapVault

Volume disaster recovery preparation

Volume disaster recovery

Volume disaster recovery overview

You can quickly activate a destination volume after a disaster and then reactivate the source volume in ONTAP using the ONTAP System Manager classic interface (ONTAP 9.7 and earlier).

Use this procedure if you want to perform volume-level disaster recovery in the following way:

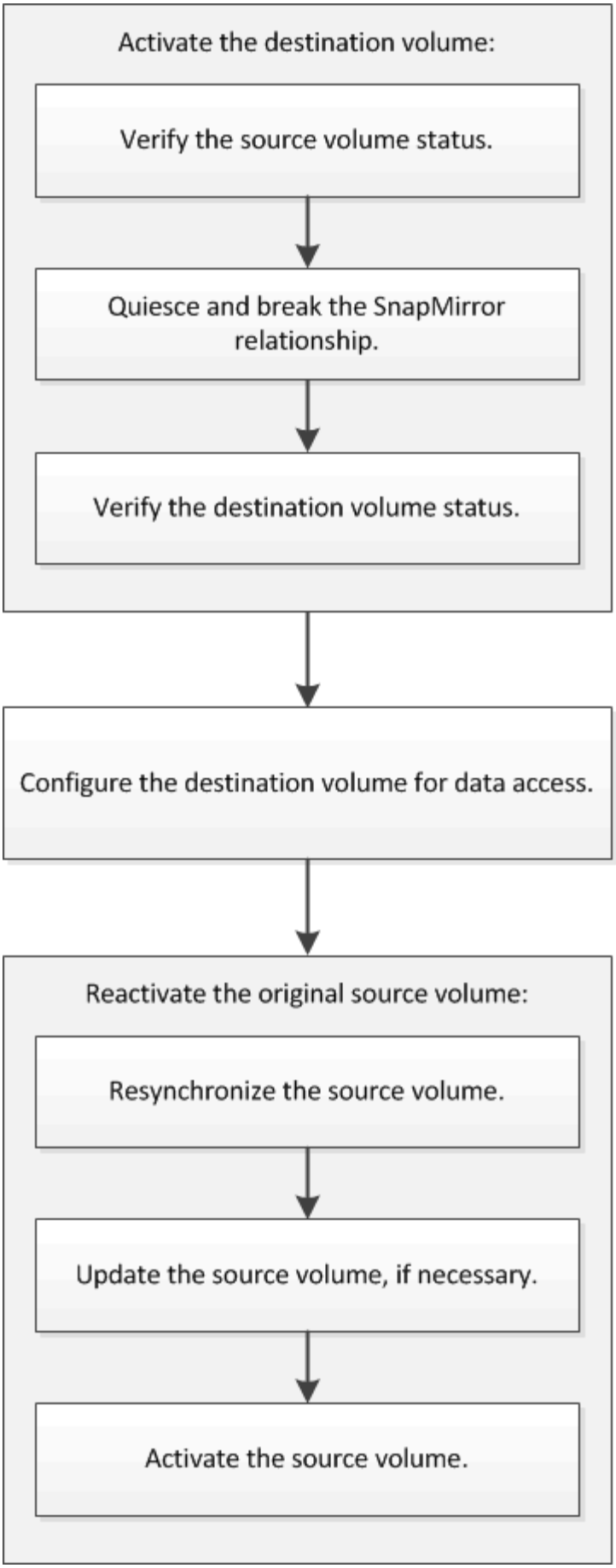
- You are working with clusters running ONTAP 9.
- You are a cluster administrator.
- You have configured the SnapMirror relationship following Volume disaster recovery preparation
- The cluster administrator of the source cluster has declared that the data in the source volume is unavailable due to events such as virus infection leading to data corruption or accidental deletion of data.
- You want to use System Manager, not the ONTAP command-line interface or an automated scripting tool.
- You want to use the System Manager classic interface for ONTAP 9.7 and earlier releases, not the ONTAP System Manager UI for ONTAP 9.7 and later.
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
The redesigned System Manager (available with ONTAP 9.7 and later)	Serve data from a SnapMirror destination
The ONTAP command line interface	Activate the destination volume

Volume disaster recovery workflow

The volume disaster recovery workflow includes activating the destination volume, configuring the destination volume for data access, and reactivating the original source volume.


Activate the destination volume:
Verify the source volume status.
Quiesce and break the SnapMirror relationship.
Verify the destination volume status.
Configure the destination volume for data access.
Reactivate the original source volume:
Resynchronize the source volume.
Update the source volume, if necessary.
Activate the source volume.

Additional information is available to help you to manage the volume-level disaster recovery relationships and provides other methods of disaster recovery to protect the availability of your data resources.

- Volume backup using SnapVault

  Describes how to quickly configure backup vault relationships between volumes that are located in different ONTAP clusters.

- Volume restore management using SnapVault

  Describes how to quickly restore a volume from a backup vault in ONTAP.

Activate the destination volume

When the source volume is unable to serve data due to events such as data corruption, accidental deletion or an offline state, you must activate the destination volume to provide data access until you recover the data on the source volume. Activation involves stopping future SnapMirror data transfers and breaking the SnapMirror relationship.

Verify the status of the source volume

When the source volume is unavailable, you must verify that the source volume is offline and then identify the destination volume that must be activated for providing data access.

About this task

You must perform this task from the **source** cluster.

Steps

1. Navigate to the **Volumes** window.
2. Select the source volume, and then verify that the source volume is offline.
3. Identify the destination volume in the SnapMirror relationship.
   - Beginning with ONTAP 9.3: Double-click the source volume to view the details, and then click **PROTECTION** to identify the destination volume in the SnapMirror relationship and the name of the SVM that contains the volume.

   - ONTAP 9.2 or earlier: Click the **Data Protection** tab at the bottom of the Volumes page to identify the destination volume in the SnapMirror relationship and the name of the SVM that contains the volume.

Break the SnapMirror relationship

You must quiesce and break the SnapMirror relationship to activate the destination volume. After quiescing, future SnapMirror data transfers are disabled.

Before you begin

The destination volume must be mounted on the destination SVM namespace.

About this task

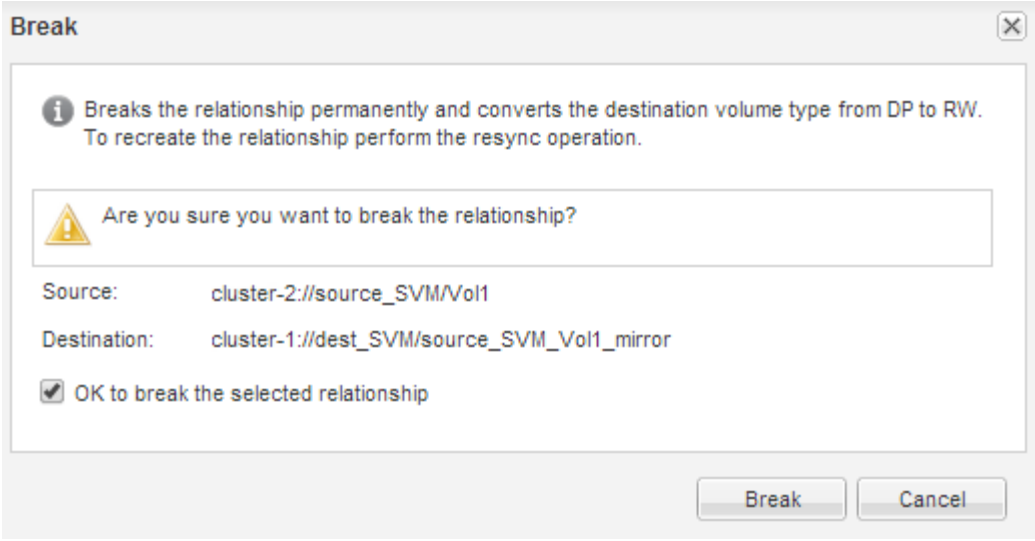
You must perform this task from the **destination** cluster.

Steps

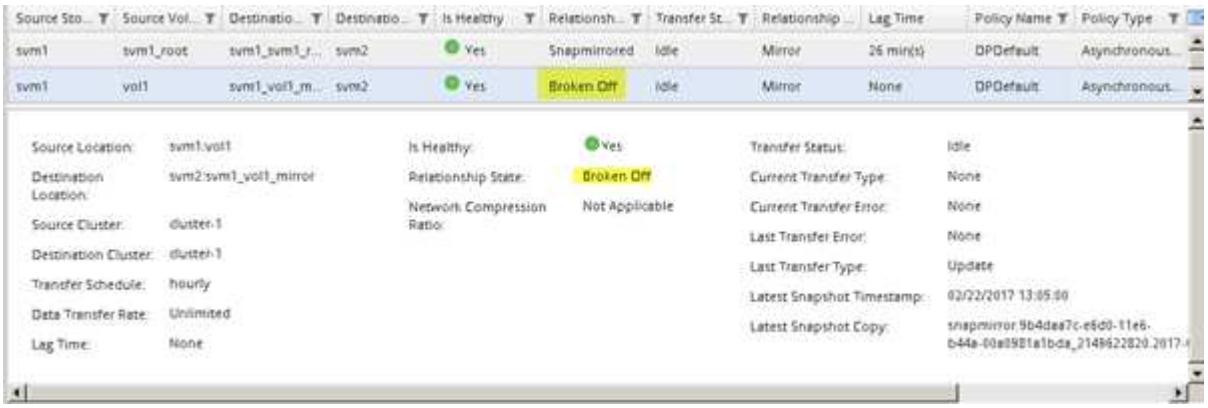
1. Depending on the System Manager version that you are running, perform one of the following steps:
   - ONTAP 9.4 or earlier: Click **Protection** > **Relationships**.
   - Beginning with ONTAP 9.5: Click **Protection** > **Volume Relationships**.
2. Select the SnapMirror relationship between the source and the destination volumes.
3. Click **Operations** > **Quiesce** to disable future data transfers.
4. Select the confirmation check box, and then click **Quiesce**.

   The quiesce operation might take some time; you must not perform any other operation on the SnapMirror relationship until the transfer status is displayed as `Quiesced`.

5. Click **Operations** > **Break**.
6. Select the confirmation check box, and then click **Break**.



The SnapMirror relationship is in `Broken Off` state.



Verify the destination volume status

After breaking the SnapMirror relationship, you must verify that the destination volume has read/write access and that the destination volume settings match the settings of the source volume.

About this task

You must perform this task from the **destination** cluster.

Steps

1. Navigate to the **Volumes** window.
2. Select the destination volume from the **Volumes** list, and then verify that the destination volume type is `rw`, which indicates read/write access.
3. Verify that the volume settings such as thin provisioning, deduplication, compression, and autogrow on the destination volume match the settings of the source volume.

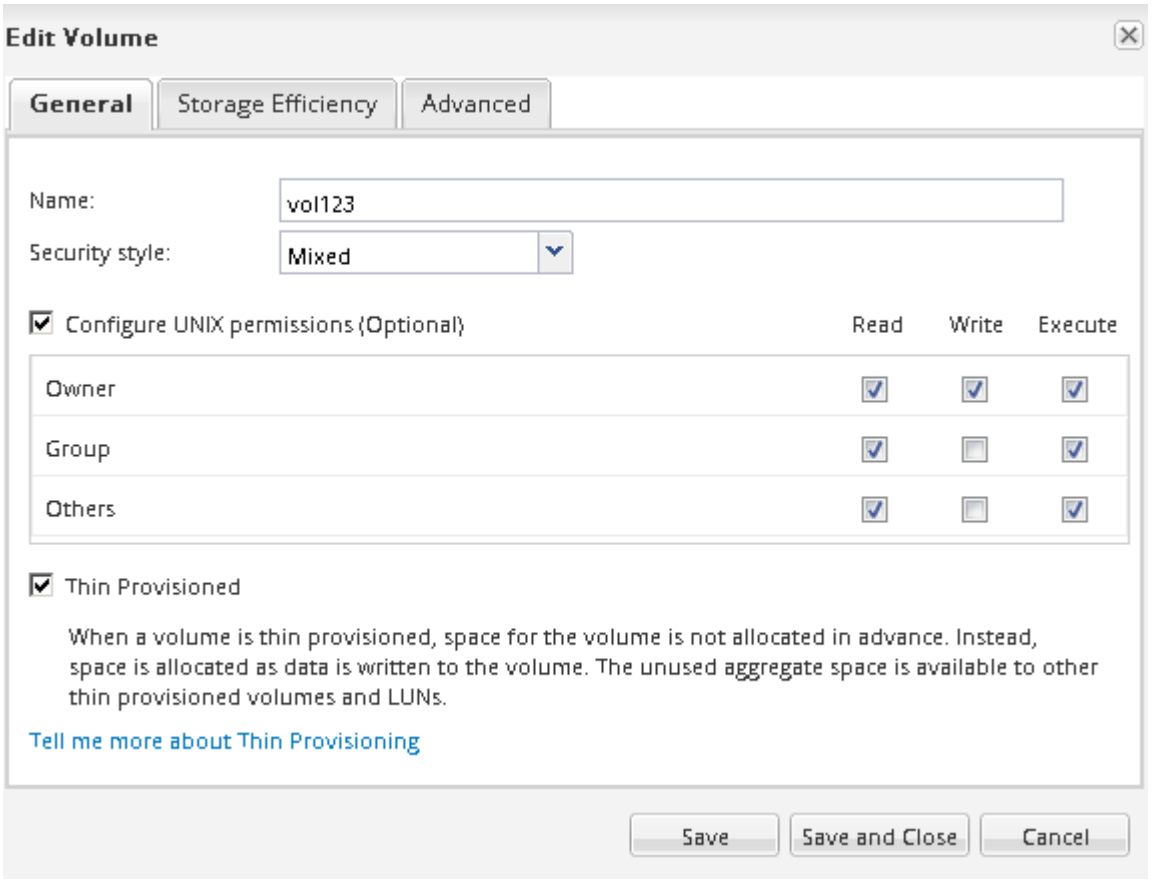
   You can use the volume settings information that you noted after creating the SnapMirror relationship to verify the destination volume settings.

4. If the volume settings do not match, modify the settings on the destination volume as required:

a. Click **Edit**.

b. Modify the general settings, storage efficiency settings, and advanced settings for your environment, as required.

c. Click **Save and Close**.



d. Verify that the columns in the **Volumes** list are updated with the appropriate values.

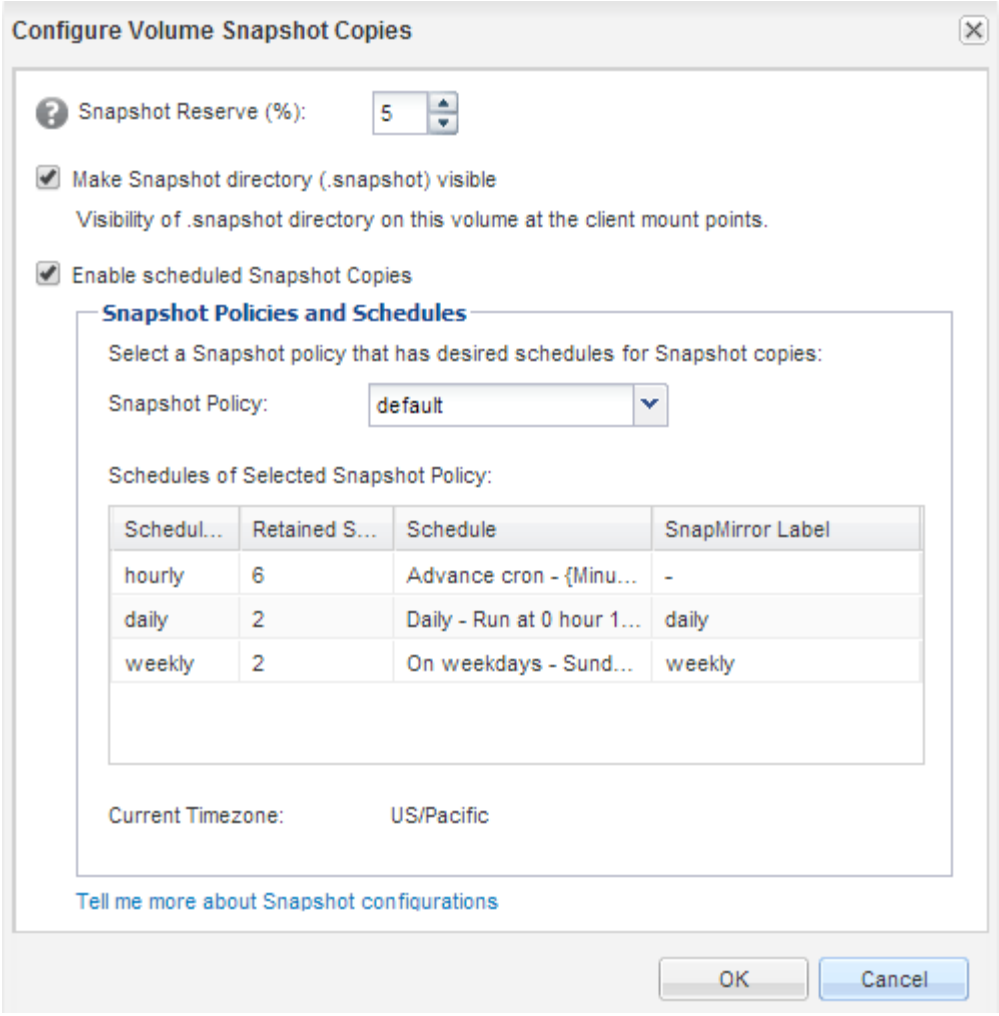
5. Enable Snapshot copy creation for the destination volume.

a. Depending on your ONTAP version, navigate to the **Configure Volume Snapshot Copies** page in one of the following ways:

Beginning with ONTAP 9.3: Select the destination volume, and then click **Actions** > **Manage Snapshots** > **Configure**.

ONTAP 9.2 or earlier: Select the destination volume, and then click **Snapshot Copies** > **Configure**.

b. Select the **Enable scheduled Snapshot Copies** check box, and then click **OK**.



Configure the destination volume for data access

After activating the destination volume, you must configure the volume for data access. NAS clients and SAN hosts can access the data from the destination volume until the source volume is reactivated.

About this task

You must perform this task from the **destination** cluster.

Procedure

- NAS environment:
  a. Mount the NAS volumes to the namespace using the same junction path that the source volume was mounted to in the source SVM.
  b. Apply the appropriate ACLs to the CIFS shares at the destination volume.
  c. Assign the NFS export policies to the destination volume.
  d. Apply the quota rules to the destination volume.
  e. Redirect clients to the destination volume by performing the necessary steps such as changing the DNS name resolution.
  f. Remount the NFS and CIFS shares on the clients.

- SAN environment:
  a. Map the LUNs to the appropriate initiator group to make the LUNs in the volume available to the SAN clients.
  b. For iSCSI, create iSCSI sessions from the SAN host initiators to the SAN LIFs.
  c. On the SAN client, perform a storage re-scan to detect the connected LUNs.

What to do next

You should resolve the problem that caused the source volume to become unavailable. You must bring the source volume back online when possible, and then resynchronize and reactivate the source volume.

Related information

ONTAP 9 Documentation Center

Reactivate the source volume

When the source volume becomes available, you must resynchronize the data from the destination volume to the source volume, update any modifications after the resynchronization operation, and activate the source volume.

Resynchronize the source volume

When the source volume is online, you must resynchronize the data between the destination volume and the source volume to replicate the latest data from the destination volume.

Before you begin

The source volume must be online.

About this task

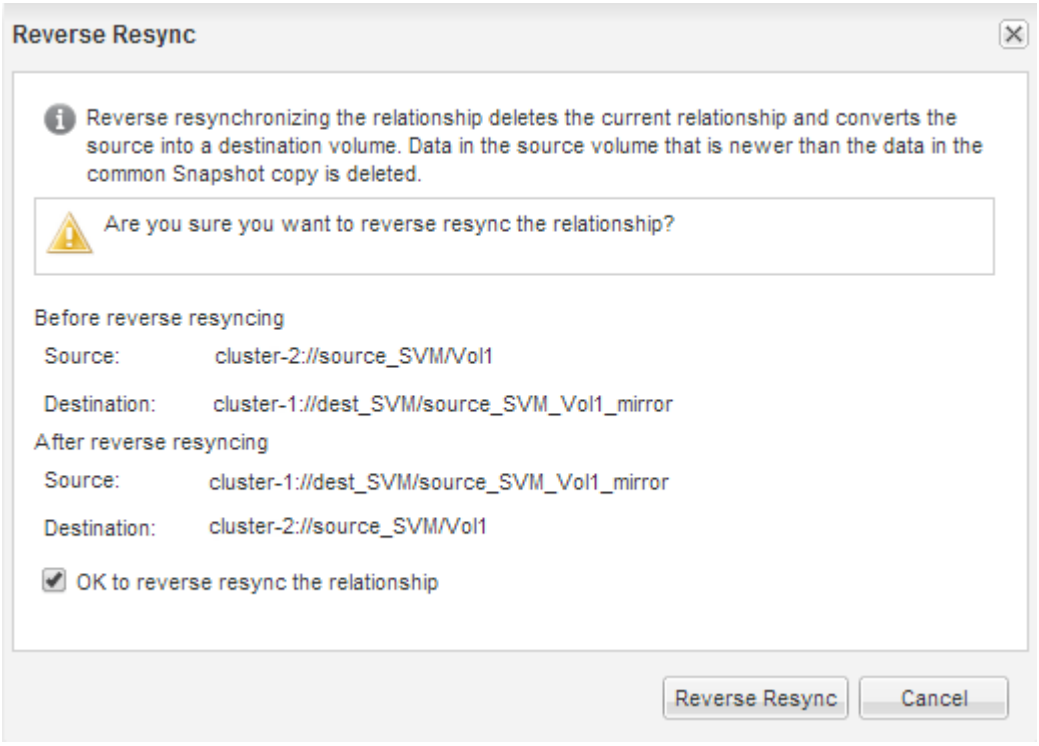
You must perform the task from the **destination** cluster.

The following image shows that the data is replicated from the active destination volume to the read-only source volume:

Steps

1. Depending on the System Manager version that you are running, perform one of the following steps:
   - ONTAP 9.4 or earlier: Click **Protection** > **Relationships**.
   - Beginning with ONTAP 9.5: Click **Protection** > **Volume Relationships**.
2. Select the SnapMirror relationship between the source and destination volumes.
3. Make a note of the transfer schedule and the policy configured for the SnapMirror relationship.

4. Click **Operations** > **Reverse Resync**.
5. Select the confirmation check box, and then click **Reverse Resync**.



Beginning with ONTAP 9.3, the SnapMirror policy of the relationship is set to `MirrorAllSnapshots` and the mirror schedule is set to `None`.

If you are running ONTAP 9.2 or earlier, the SnapMirror policy of the relationship is set to `DPDefault` and the mirror schedule is set to `None`.

6. On the source cluster, specify a SnapMirror policy and schedule that match the protection configuration of the original SnapMirror relationship:
   a. Depending on the System Manager version that you are running, perform one of the following steps:
      - ONTAP 9.4 or earlier: Click **Protection** > **Relationships**.
      - Beginning with ONTAP 9.5: Click **Protection** > **Volume Relationships**.
   b. Select the SnapMirror relationship between the resynchronized source volume and the destination volume, and then click **Edit**.
   c. Select the SnapMirror policy and schedule, and then click **OK**.

Update the source volume

After resynchronizing the source volume, you might want to ensure that all the latest changes are updated on the source volume before activating the source volume.

About this task

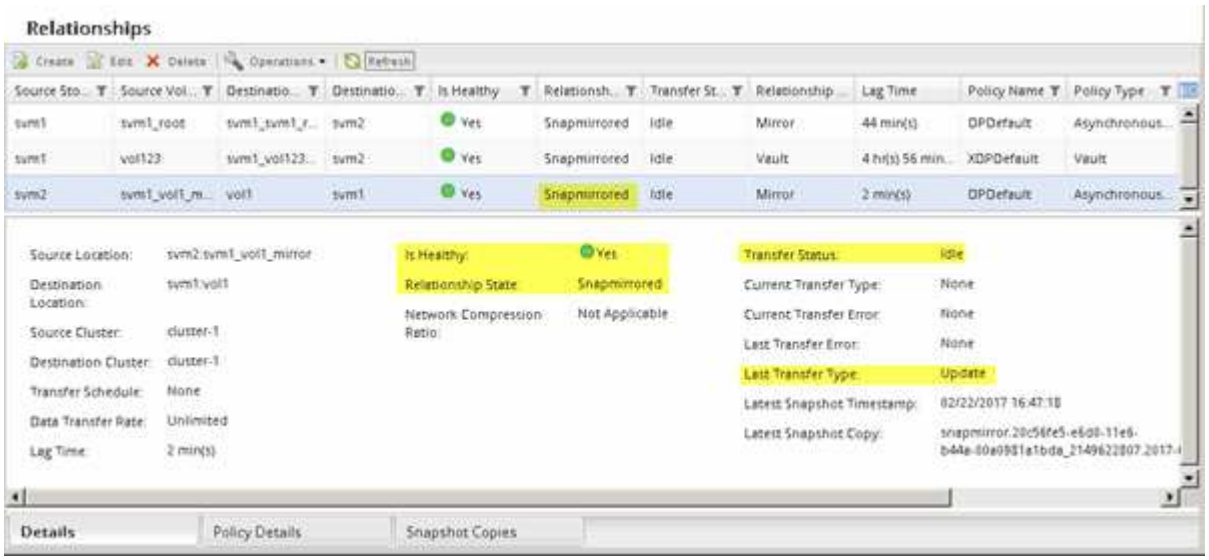
You must perform this task from the **source** cluster.

Steps

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

- ONTAP 9.4 or earlier: Click **Protection** > **Relationships**.
- Beginning with ONTAP 9.5: Click **Protection** > **Volume Relationships**.

2. Select the SnapMirror relationship between the source and the destination volumes, and then click **Operations** > **Update**.
3. Perform an incremental transfer from the recent common Snapshot copy between the source and destination volumes.
   - Beginning with ONTAP 9.3: Select the **As per policy** option.
   - ONTAP 9.2 or earlier: Select the **On demand** option.
4. **Optional:** Select **Limit transfer bandwidth to** in order to limit the network bandwidth used for transfers, and then specify the maximum transfer speed.
5. Click **Update**.
6. Verify that the transfer status is `Idle` and last transfer type is `Update` in the **Details** tab.



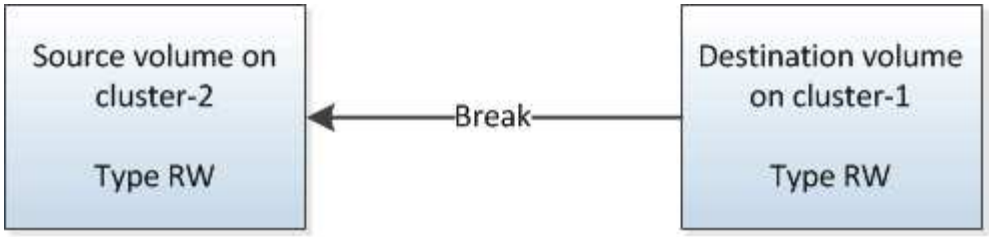
Reactivate the source volume

After resynchronizing the data from the destination volume to the source volume, you must activate the source volume by breaking the SnapMirror relationship. You should then resynchronize the destination volume to protect the reactivated source volume.

About this task

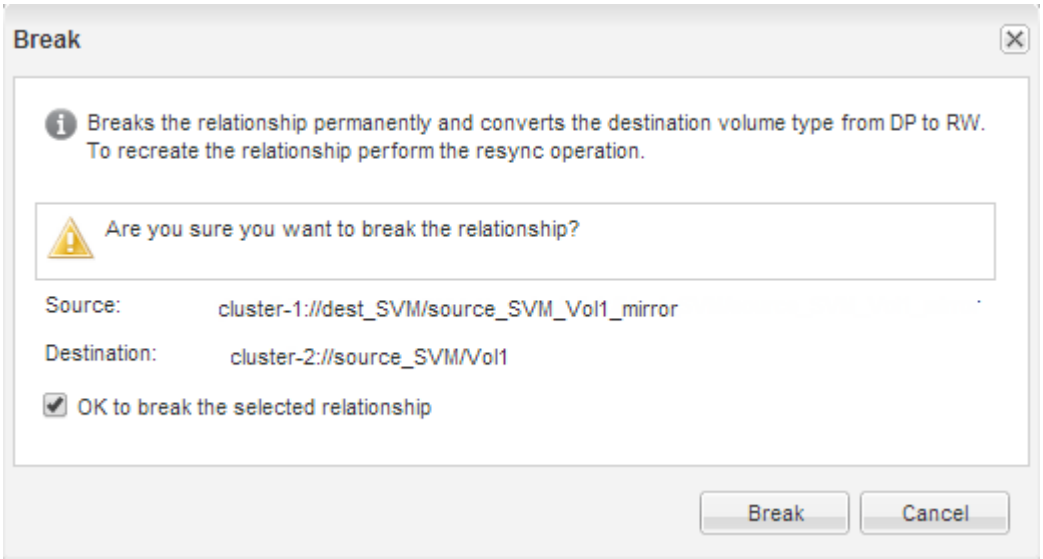
Both the break and reverse resync operations are performed from the **source** cluster.

The following image shows that the source and destination volumes are read/write when you break the SnapMirror relationship. After the reverse resync operation, the data is replicated from the active source volume to the read-only destination volume.

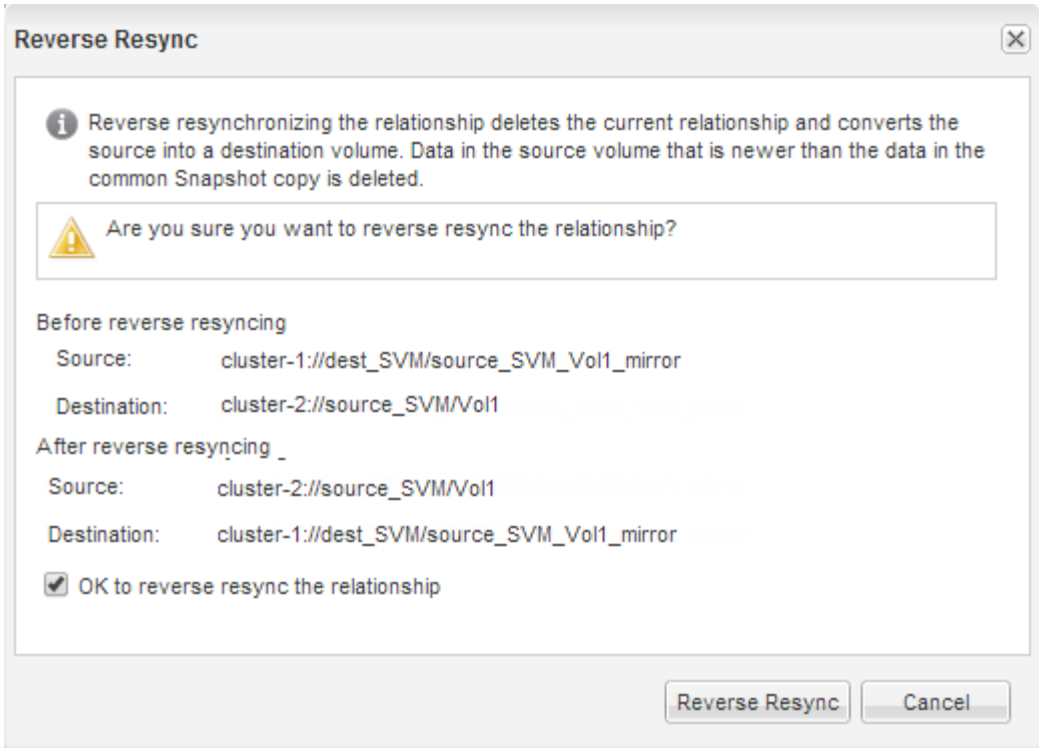


Steps

1. Depending on the System Manager version that you are running, perform one of the following steps:
   - ONTAP 9.4 or earlier: Click **Protection** > **Relationships**.
   - Beginning with ONTAP 9.5: Click **Protection** > **Volume Relationships**.
2. Select the SnapMirror relationship between the source and the destination volumes.
3. Click **Operations** > **Quiesce**.
4. Select the confirmation check box, and then click **Quiesce**.
5. Click **Operations** > **Break**.
6. Select the confirmation check box, and then click **Break**.



7. Click **Operations** > **Reverse Resync**.
8. Select the confirmation check box, and then click **Reverse Resync**.



Beginning with ONTAP 9.3, the SnapMirror policy of the relationship is set to `MirrorAllSnapshots` and the SnapMirror schedule is set to `None`.

If you are running ONTAP 9.2 or earlier, the SnapMirror policy of the relationship is set to `DPDefault` and the SnapMirror schedule is set to `None`.

9. Navigate to the source volume in the volumes page, and verify that the SnapMirror relationship you created is listed and the relationship state is `Snapmirrored`.
10. On the destination cluster, specify a SnapMirror policy and schedule that match the protection configuration of the original SnapMirror relationship for the new SnapMirror relationship:
    a. Depending on the System Manager version that you are running, perform one of the following steps:
        - ONTAP 9.4 or earlier: Click **Protection** > **Relationships**.
        - Beginning with ONTAP 9.5: Click **Protection** > **Volume Relationships**.
    b. Select the SnapMirror relationship between the reactivated source and the destination volumes, and then click **Edit**.
    c. Select the SnapMirror policy and schedule, and then click **OK**.

Results

The source volume has read/write access and is protected by the destination volume.

Volume disaster recovery preparation

Volume disaster recovery preparation overview

You can quickly protect a source volume on a peered ONTAP cluster in preparation for disaster recovery. You should use this procedure if you want to configure and monitor SnapMirror relationships between peered clusters for volume disaster recovery and do

not need a lot of conceptual background for the tasks.

SnapMirror provides scheduled asynchronous, block-level data protection. SnapMirror replicates Snapshot copies and can replicate NAS or SAN volumes on which deduplication, data compression, or both are run, including volumes containing qtrees and LUNs. SnapMirror configuration information is stored in a database that ONTAP replicates to all the nodes in the cluster.

Use this procedure if you want to create SnapMirror relationships for volume-level disaster recovery in the following way:

- You are working with clusters running ONTAP 9.
- You are a cluster administrator.
- You have configured the cluster peer relationship and the SVM peer relationship.

  Cluster and SVM peering configuration

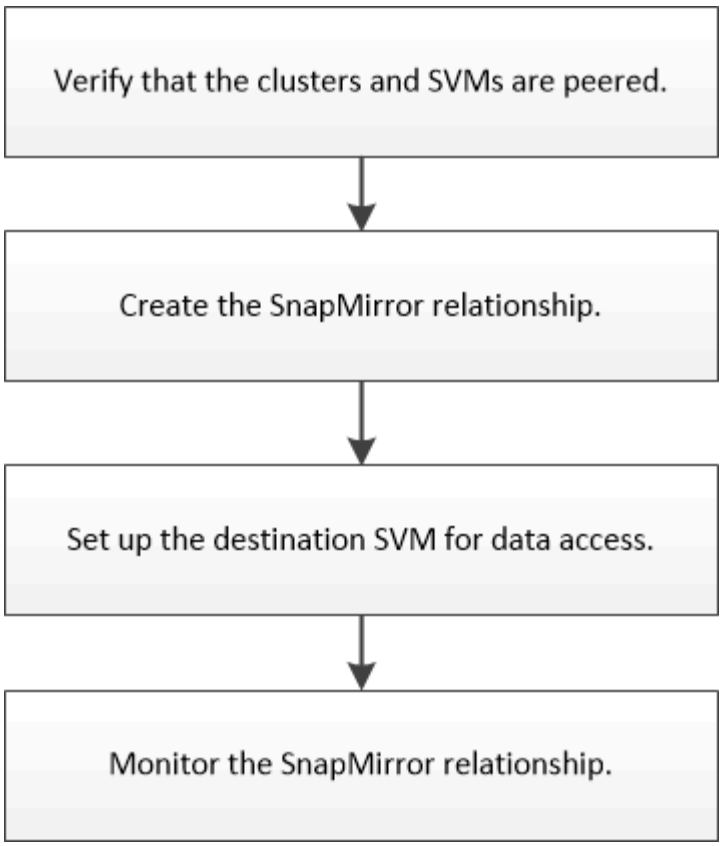
- You have enabled the SnapMirror license on both the source and the destination clusters.
- You want to use default policies and schedules, and not create custom policies.
- You want to use best practices, not explore every available option (ONTAP 9.7 and earlier).

Other ways to do this in ONTAP

To perform these tasks with…	Refer to…
The redesigned System Manager (available with ONTAP 9.7 and later)	Prepare for mirroring and vaulting
The ONTAP command line interface	Create a cluster peer relationship (ONTAP 9.3 and later)

Volume disaster recovery preparation workflow

Preparing volumes for disaster recovery involves verifying the cluster peer relationship, creating the SnapMirror relationship between volumes residing on peered clusters, setting up the destination SVM for data access, and monitoring the SnapMirror relationship periodically.



Additional documentation is available to help you activate the destination volume to test the disaster recovery setup or when a disaster occurs. You can also learn more about how to reactivate the source volume after the disaster.

Volume disaster recovery

+
Describes how to quickly activate a destination volume after a disaster and then reactivate the source volume in ONTAP.

Verify the cluster peer relationship and SVM peer relationship

Before you set up a volume for disaster recovery, you must verify that the source and destination clusters are peered and are communicating with each other through the peer relationship.

Procedure

- If you are running ONTAP 9.3 or later, perform the following steps to verify the cluster peer relationship and SVM peer relationship:
  a. Click **Configuration** > **Cluster Peers**.
  b. Verify that the peered cluster is authenticated and is available.

c. Click **Configuration** > **SVM Peers**.

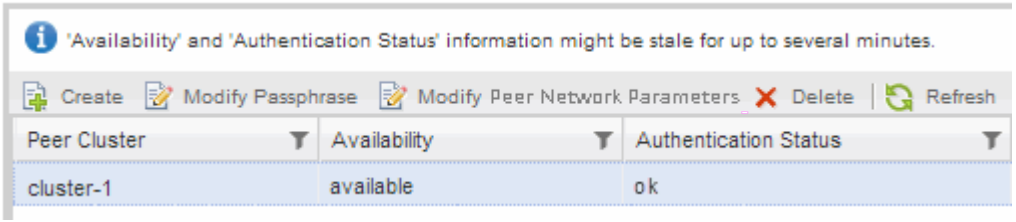
d. Verify that the destination SVM is peered with the source SVM.

- If you are running ONTAP 9.2 or earlier, perform the following steps to verify the cluster peer relationship and SVM peer relationship:

a. Click the **Configurations** tab.

b. In the **Cluster Details** pane, click **Cluster Peers**.

c. Verify that the peered cluster is authenticated and available.



d. Click the **SVMs** tab and select the source SVM.

e. In the **Peer Storage Virtual Machines** area, verify the destination SVM is peered with the source SVM.

If you do not see any peered SVM in this area, you can create the SVM peer relationship when creating the SnapMirror relationship.

Creating the SnapMirror relationship (ONTAP 9.2 or earlier)

Create the SnapMirror relationship (Beginning with ONTAP 9.3)

You must create a SnapMirror relationship between the source volume on one cluster and the destination volume on the peered cluster for replicating data for disaster recovery.

Before you begin

- The destination aggregate must have available space.
- Both the clusters must be configured and set up appropriately to meet the requirements of your environment for user access, authentication, and client access.

About this task

You must perform this task from the **source** cluster.

Steps

1. Click **Storage** > **Volumes**.
2. Select the volume for which you want to create a mirror relationship, and then click **Actions** > **Protect**.
3. In the **Relationship Type** section, select **Mirror** from the **Relationship Type** drop-down list.
4. In the **Volumes: Protect Volumes** page, provide the following information:
   a. Select **Mirror** as the relationship type.
   b. Select the destination cluster, destination SVM, and the suffix for the name of the destination volume.

      Only peered SVMs and allowed SVMs are listed under destination SVMs.

c. Click .

d. In the **Advanced Options** dialog box, verify that `MirrorAllSnapshots` is set as the protection policy.

   `DPDefault` and `MirrorLatest` are the other default protection policies that are available for SnapMirror relationships.

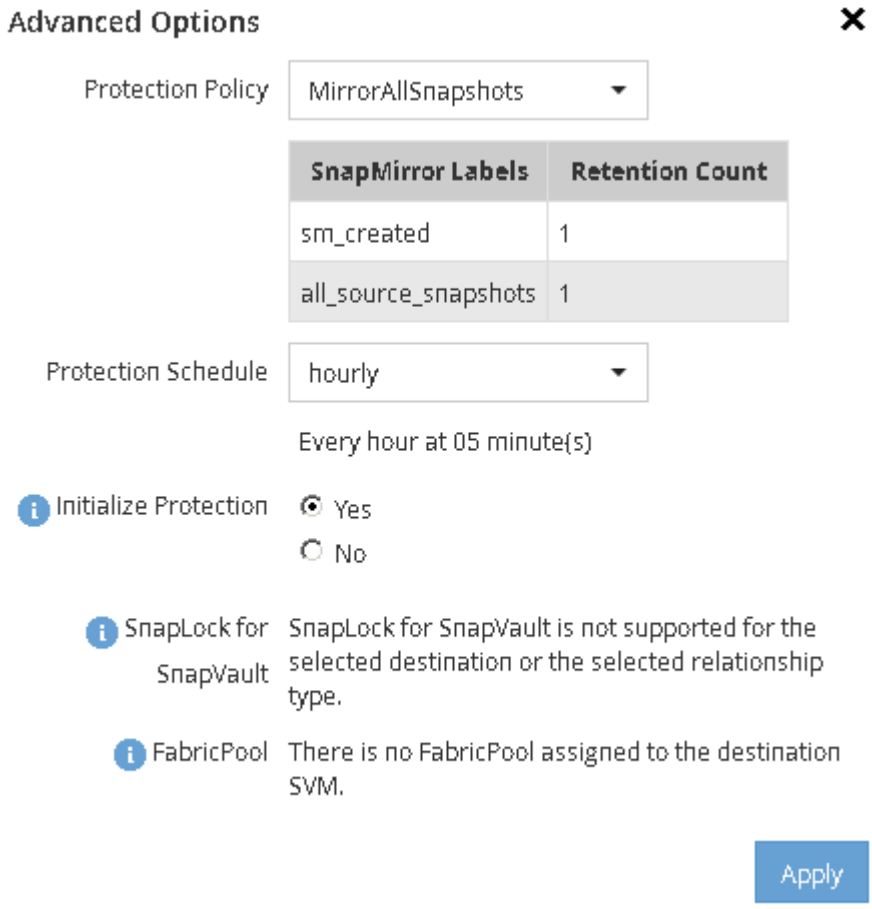
e. Select a protection schedule.

   By default, the `hourly` schedule is selected.

f. Verify that **Yes** is selected for initializing the SnapVault relationship.

   All of the data protection relationships are initialized by default. Initializing the SnapMirror relationship ensures that the destination volume has a baseline to start protecting the source volume.

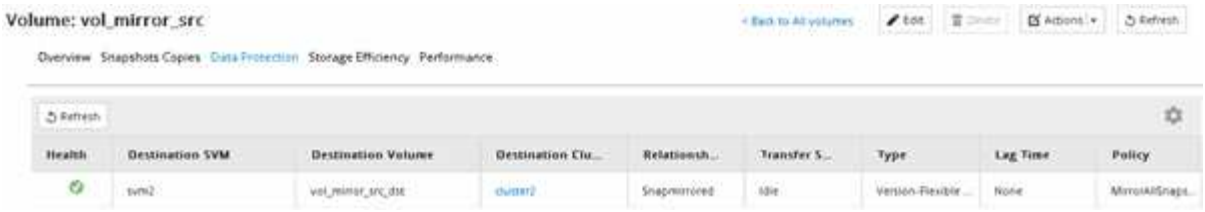
g. Click **Apply** to save the changes.



5. Click **Save** to create the SnapMirror relationship.
6. Verify that the relationship status of the SnapMirror relationship is in the `Snapmirrored` state.

   a. Navigate to the **Volumes** window, and then select the volume that the volume for which you created the SnapMirror relationship.

   b. Double-click the volume to view the volume details, and then click **PROTECTION** to view the data protection status of the volume.



What to do next

You must make a note of the settings for the source volume such as thin provisioning, deduplication, compression, and autogrow. You can use this information to verify the destination volume settings when you break the SnapMirror relationship.

Create the SnapMirror relationship (ONTAP 9.2 or earlier)

You must create a SnapMirror relationship between the source volume on one cluster and the destination volume on the peered cluster for replicating data for disaster recovery.

Before you begin

- You must have the cluster administrator user name and password for the destination cluster.
- The destination aggregate must have available space.
- Both the clusters must be configured and set up appropriately to meet the requirements of your environment for user access, authentication, and client access.

About this task

You must perform this task from the **source** cluster.

Steps

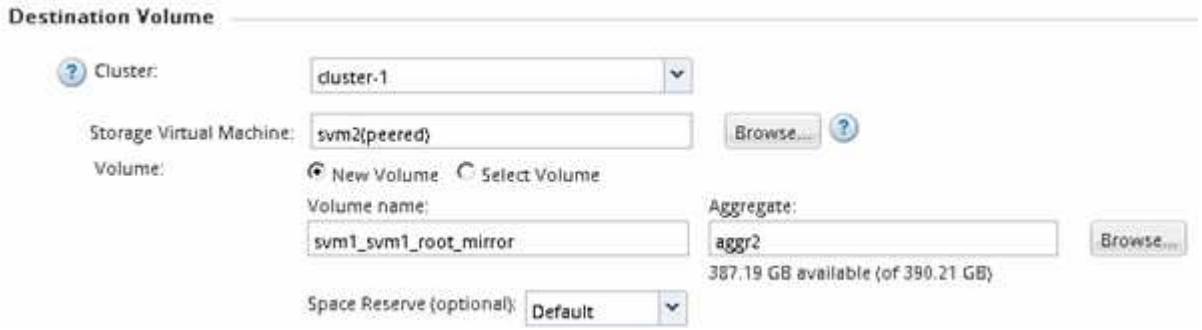
1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. Click the **Volumes** tab.
4. Select the volume for which you want to create a mirror relationship, and then click **Protect**.

   The Create Protection Relationship window is displayed.

5. In the **Relationship Type** section, select **Mirror** from the **Relationship Type** drop-down list.
6. In the **Destination Volume** section, select the peered cluster.
7. Specify the SVM for the destination volume:

If the SVM is…	Then…
Peered	Select the peered SVM from the list.
Not peered	a. Select the SVM. b. Click **Authenticate**. c. Enter the cluster administrator's credentials of the peered cluster, and then click **Create**.

8. Create a new destination volume:
   a. Select the **New Volume** option.
   b. Use the default volume name or specify a new volume name.
   c. Select the destination aggregate.

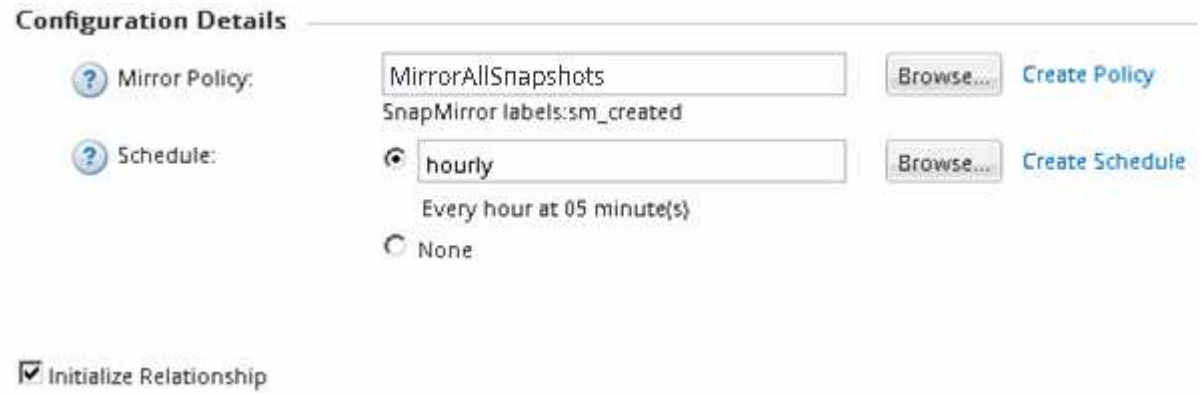


9. In the **Configuration Details** section, select **MirrorAllSnapshots** as the mirror policy.

   `DPDefault` and `MirrorLatest` are the other default mirror policies that are available for SnapMirror relationships.

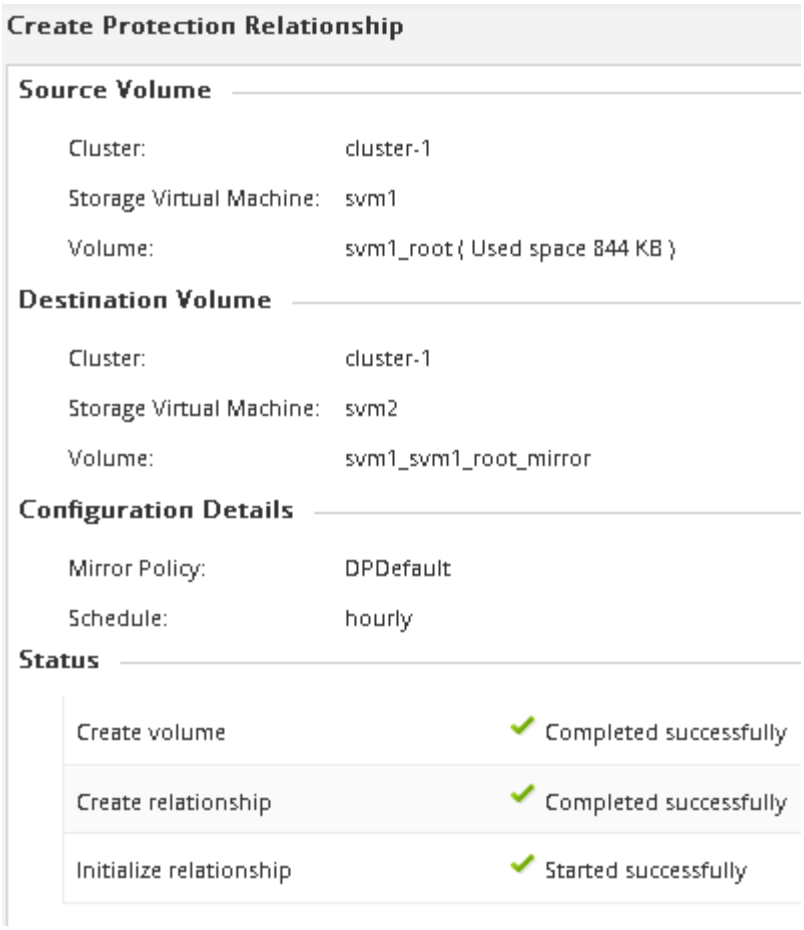
10. Select a protection schedule from the list of schedules.
11. Ensure that the **Initialize Relationship** check box is selected, and then click **Create**.

    Initializing the SnapMirror relationship ensures that the destination volume has a baseline to start protecting the source volume.



    The relationship is initialized by starting a baseline transfer of data from the source volume to the destination volume.

    The initialization operation might take some time. The Status section shows the status of each job.



12. Verify the relationship status of the SnapMirror relationship:
    a. Select the volume for which you created the SnapMirror relationship from the **Volumes** list, and then click **Data Protection**.
    b. In the **Data Protection** tab, verify that the SnapMirror relationship that you created is listed and that the relationship state is `Snapmirrored`.

What to do next

You must make a note of the settings for the source volume such as thin provisioning, deduplication, compression, and autogrow. You can use this information to verify the destination volume settings when you break the SnapMirror relationship.

Set up the destination SVM for data access

You can minimize data access disruption when activating the destination volume by setting up required configurations such as LIFs, CIFS shares, and export policies for the NAS environment, and LIFs and initiator groups for the SAN environment on the SVM containing the destination volume.

About this task

You must perform this task on the **destination** cluster for the SVM containing the destination volume.

Procedure

- NAS environment:
  a. Create NAS LIFs.
  b. Create CIFS shares with the same share names that were used on the source.
  c. Create appropriate NFS export policies.
  d. Create appropriate quota rules.
- SAN environment:
  a. Create SAN LIFs.
  b. **Optional:** Configure portsets.
  c. Configure initiator groups.
  d. For FC, zone the FC switches to enable the SAN clients to access the LIFs.

What to do next

If any changes were made on the SVM containing the source volume, you must replicate the changes manually on the SVM containing the destination volume.

Related information

ONTAP 9 Documentation Center

Monitor the status of SnapMirror data transfers

You should periodically monitor the status of the SnapMirror relationships to ensure that the SnapMirror data transfers are occurring as per the specified schedule.

About this task

You must perform this task from the **destination** cluster.

Steps

1. Depending on the System Manager version that you are running, perform one of the following steps:
   - ONTAP 9.4 or earlier: Click **Protection** > **Relationships**.
   - Beginning with ONTAP 9.5: Click **Protection** > **Volume Relationships**.
2. Select the SnapMirror relationship between the source and the destination volumes, and then verify the status in the **Details** bottom tab.

   The Details tab displays the health status of the SnapMirror relationship and shows the transfer errors and lag time.

   - The Is Healthy field must display `Yes`.

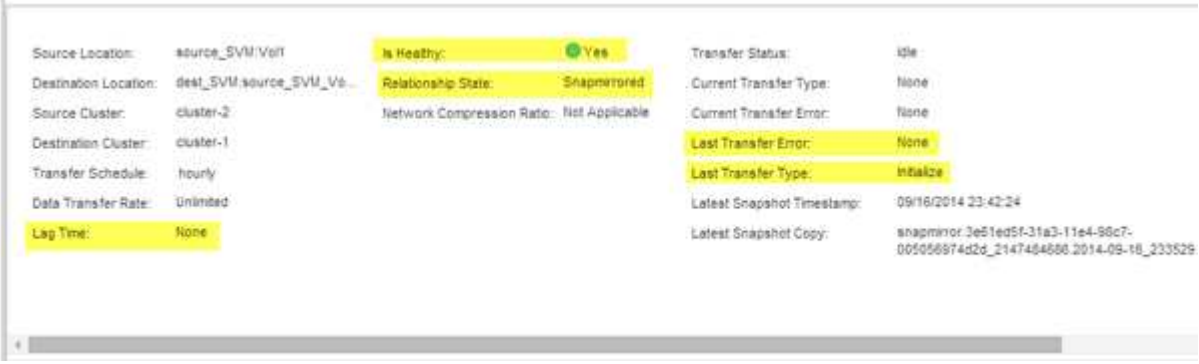
     For most SnapMirror data transfer failures, the field displays `No`. In some failure cases, however, the field continues to display `Yes`. You must check the transfer errors in the Details section to ensure that no data transfer failure occurred.

   - The Relationship State field must display `Snapmirrored`.
   - The Lag Time must be no more than the transfer schedule interval.

For example, if the transfer schedule is hourly, then the lag time must not be more than an hour.

You should troubleshoot any issues in the SnapMirror relationships.

NetApp Technical Report 4015: SnapMirror Configuration and Best Practices for ONTAP 9.1, 9.2



Volume backup using SnapVault

Volume backup using SnapVault overview

You can quickly configure SnapVault backup relationships between volumes that are located in different clusters. The SnapVault backup contains a set of read-only backup copies, which are located on a destination volume that you can use for restoring data when data is corrupted or lost.

Use this procedure if you want to create SnapVault backup relationships for volumes in the following way:

- You are working with clusters running ONTAP 9.
- You are a cluster administrator.
- You have configured the cluster peer relationship and the SVM peer relationship.

  Cluster and SVM peering configuration

- You must have enabled either the SnapMirror or SnapVault license, after all of the nodes in the cluster have been upgraded to the same version of ONTAP 9.
- You want to use default protection policies and schedules, and not create custom policies.
- You do not want to back up data for a single file or LUN restore.
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.
- You want to use System Manager, not the ONTAP command-line interface or an automated scripting tool.
- You want to use the System Manager classic interface for ONTAP 9.7 and earlier releases, not the ONTAP System Manager UI for ONTAP 9.7 and later.

If these assumptions are not correct for your situation, or if you want more conceptual background information, you should see the following resource:

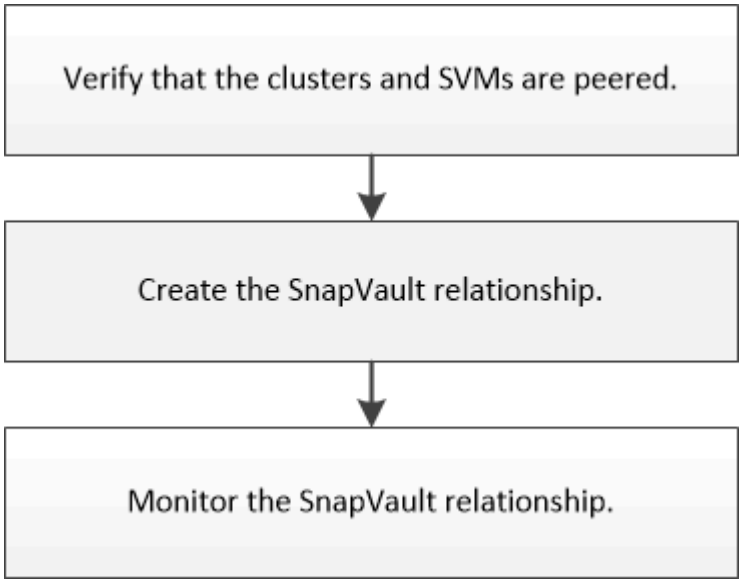
NetApp Technical Report 4183: SnapVault Best Practices

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
The redesigned System Manager (available with ONTAP 9.7 and later)	Configure mirrors and vaults
The ONTAP command line interface	Create a replication relationship

SnapVault backup configuration workflow

Configuring a SnapVault backup relationship includes verifying the cluster peer relationship, creating the SnapVault relationship between the source and the destination volumes, and monitoring the SnapVault relationship.



Additional documentation is available to help you restore data from a destination volume to test the backed-up data or when the source volume is lost.

- Volume restore management using SnapVault

  Describes how to quickly restore a volume from a SnapVault backup in ONTAP

Verify cluster peer relationship and SVM peer relationship

Before you set up a volume for data protection by using SnapVault technology, you must verify that the source cluster and destination cluster are peered and are communicating with each other through the peer relationship. You must also verify that the source SVM and destination SVM are peered and are communicating with each other through the peer relationship.

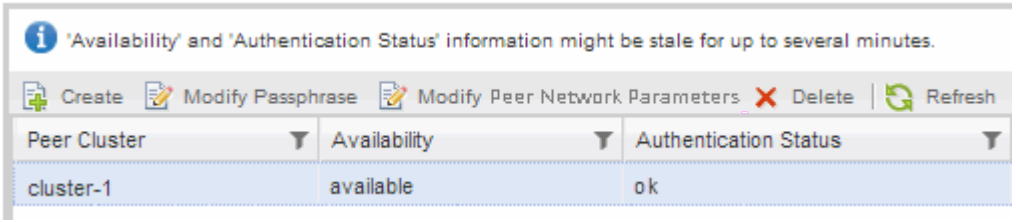
About this task

You must perform this task from the **source** cluster.

Procedure

- If you are running ONTAP 9.3 or later, perform the following steps to verify the cluster peer relationship and SVM peer relationship:
  a. Click **Configuration** > **Cluster Peers**.
  b. Verify that the peered cluster is authenticated and is available.

  c. Click **Configuration** > **SVM Peers**.
  d. Verify that the destination SVM is peered with the source SVM.
- If you are running ONTAP 9.2 or earlier, perform the following steps to verify the cluster peer relationship and SVM peer relationship:
  a. Click the **Configurations** tab.
  b. In the **Cluster Details** pane, click **Cluster Peers**.
  c. Verify that the peered cluster is authenticated and available.



  d. Click the **SVMs** tab and select the source SVM.
  e. In the **Peer Storage Virtual Machines** area, verify the destination SVM is peered with the source SVM.

     If you do not see any peered SVM in this area, you can create the SVM peer relationship when creating the SnapVault relationship.

Creating the SnapVault relationship (ONTAP 9.2 or earlier)

Create a SnapVault relationship (Beginning with ONTAP 9.3)

You must create a SnapVault relationship between the source volume on one cluster and the destination volume on the peered cluster to create a SnapVault backup.

Before you begin

- You must have the cluster administrator user name and password for the destination cluster.
- The destination aggregate must have available space.

About this task

You must perform this task from the **source** cluster.

Steps

1. Click **Storage** > **Volumes**.
2. Select the volume that you want to back up, and then click **Actions** > **Protect**.

   You can also select multiple source volumes, and then create SnapVault relationships with a single destination volume.

3. In the **Volumes: Protect Volumes** page, provide the following information:
   a. Select **Vault** from the **Relationship Type** drop-down list.
   b. Select the destination cluster, destination SVM, and the suffix for the destination volume.

      Only peered SVMs and permitted SVMs are listed under destination SVMs.

      The destination volume is automatically created. The name of the destination volume is the source volume name appended with the suffix.

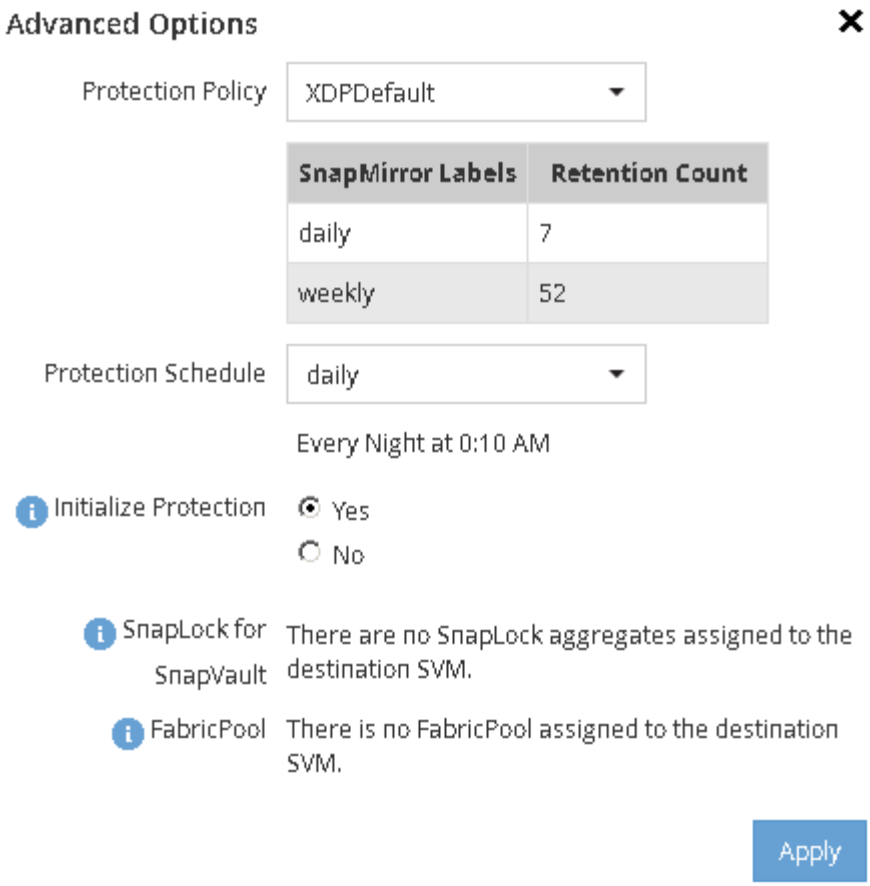
   c. Click .
   d. In the **Advanced Options** dialog box, verify that the **Protection Policy** is set as `XDPDefault`.
   e. Select the **Protection Schedule**.

      By default, the `daily` schedule is selected.

   f. Verify that **Yes** is selected for initializing the SnapVault relationship.

      All data protection relationships are initialized by default.

   g. Click **Apply** to save the changes.



4. In the **Volumes: Protect Volumes** page, click **Validate** to verify whether the volumes have matching SnapMirror labels.
5. Click **Save** to create the SnapVault relationship.
6. Verify that the status of the SnapVault relationship is in the `Snapmirrored` state.
   a. Navigate to the **Volumes** window, and then select the volume that is backed up.
   b. Expand the volume and click **PROTECTION** to view the data protection status of the volume.

Create the SnapVault relationship (ONTAP 9.2 or earlier)

You must create a SnapVault relationship between the source volume on one cluster and the destination volume on the peered cluster to create a SnapVault backup.

Before you begin

- You must have the cluster administrator user name and password for the destination cluster.
- The destination aggregate must have available space.

About this task

You must perform this task from the **source** cluster.

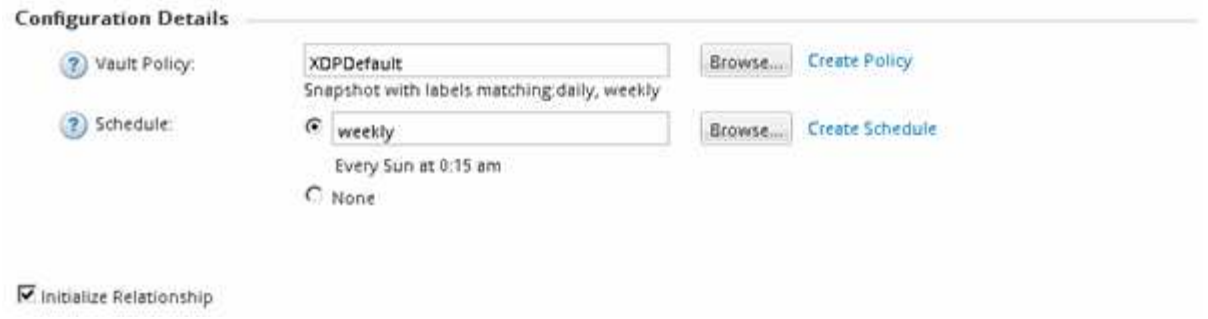
Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. Click the **Volumes** tab.
4. Select the volume that you want to back up, and then click **Protect**.
5. In the **Create Protection Relationship** dialog box, select **Vault** from the **Relationship Type** drop-down list.
6. In the **Destination Volume** section, select the peered cluster.
7. Specify the SVM for the destination volume:

If the SVM is…	Then…
Peered	Select the peered SVM from the list.
Not peered	a. Select the SVM. b. Click **Authenticate**. c. Enter the cluster administrator's credentials of the peered cluster, and then click **Create**.

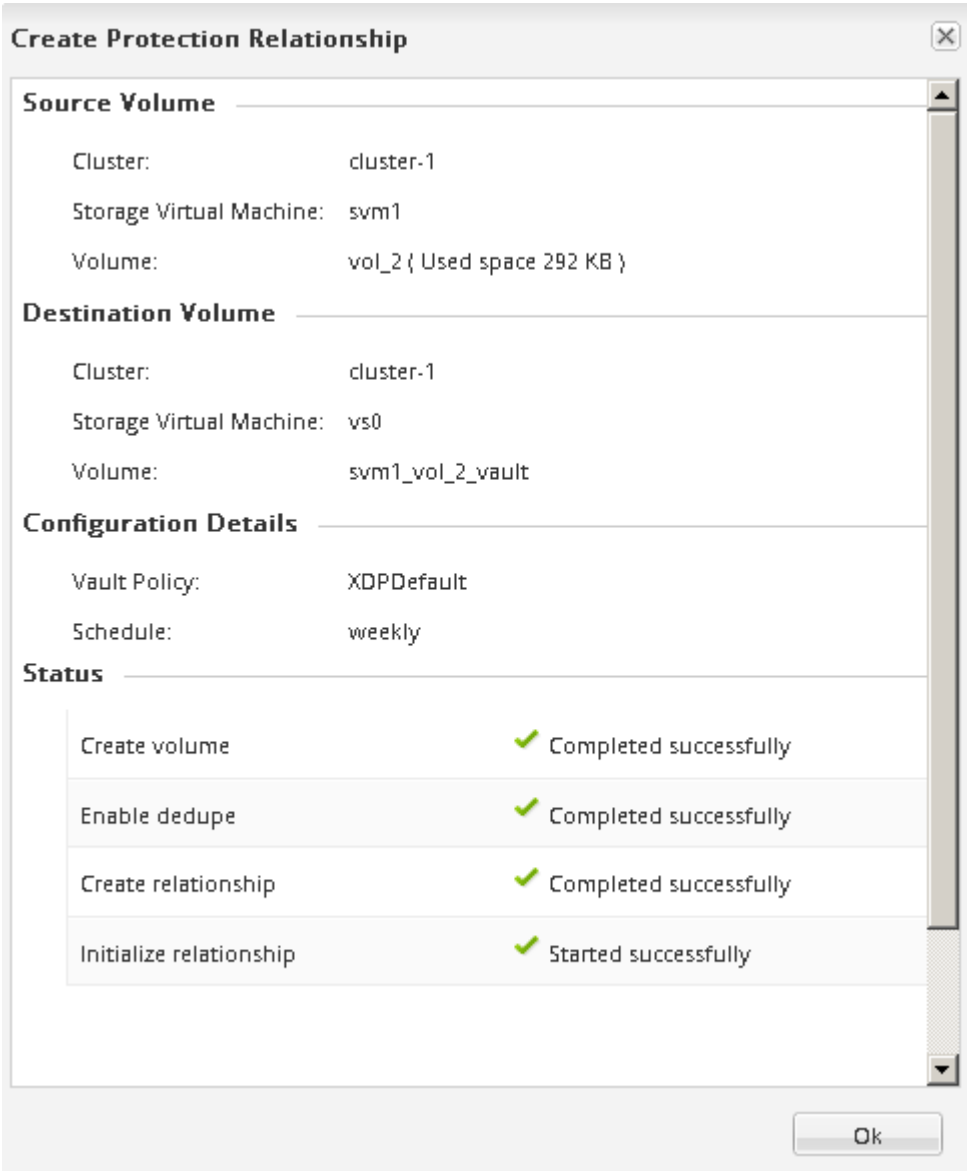
8. Create a new destination volume:
   a. Select the **New Volume** option.
   b. Use the default volume name or enter a new volume name.
   c. Select the destination aggregate.
   d. Ensure that the **Enable dedupe** check box is selected.

9. In the **Configuration Details** section, select `XDPDefault` as the protection policy.
10. Select a protection schedule from the list of schedules.
11. Ensure that the **Initialize Relationship** check box is selected to transfer the base Snapshot copy, and then click **Create**



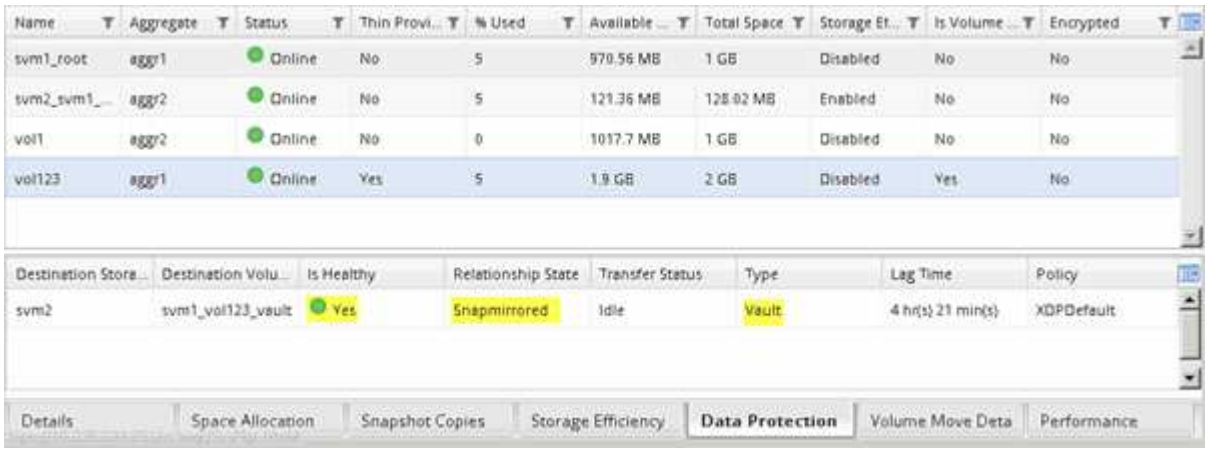
The wizard creates the relationship with the specified vault policy and schedule. The relationship is initialized by starting a baseline transfer of data from the source volume to the destination volume.

The Status section shows the status of each job.



12. Verify that the relationship status of the SnapVault relationship is in the `Snapmirrored` state.
    a. Select the volume from the Volumes list, and then click **Data Protection**.
    b. In the **Data Protection** bottom tab, verify that the SnapMirror relationship you created is listed and the

relationship state is `Snapmirrored` and type is `Vault`.



Monitor the SnapVault relationship

You should periodically monitor the status of the SnapVault relationships to ensure that the data is backed up on the destination volume per the specified schedule.

About this task

You must perform this task from the **destination** cluster.

Steps

1. Depending on the System Manager version that you are running, perform one of the following steps:
   - ONTAP 9.4 or earlier: Click **Protection** > **Relationships**.
   - Beginning with ONTAP 9.5: Click **Protection** > **Volume Relationships**.
2. Select the SnapVault relationship between the source and the destination volumes, and then verify the status in the **Details** bottom tab.

   The health status of the SnapVault relationship, any transfer errors, and the lag time are displayed:

   - The Is Healthy field must display `Yes`.

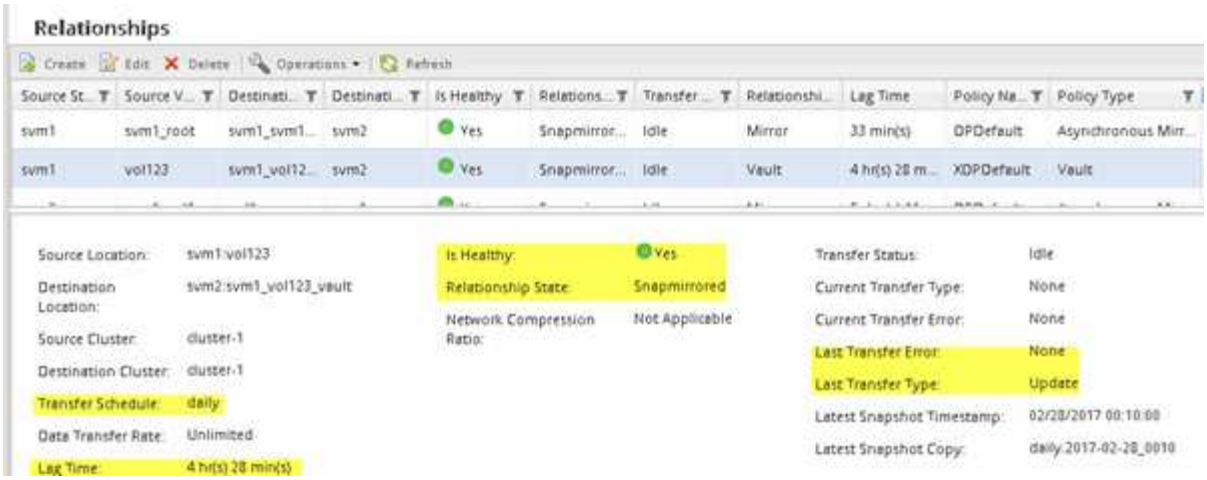
     For most data transfer failures, the field displays `No`. In some failure cases, however, the field continues to display `Yes`. You must check the transfer errors in the Details section to ensure that no data transfer failure occurred.

   - The Relationship State field must display `Snapmirrored`.
   - The Lag Time must be not more than the transfer schedule interval.

     For example, if the transfer schedule is daily, then the lag time must not be more than a day.

     You should troubleshoot any issues in the SnapVault relationships. The troubleshooting procedures for SnapMirror relationships are also applicable to SnapVault relationships.

     NetApp Technical Report 4015: SnapMirror Configuration and Best Practices for ONTAP 9.1, 9.2



Volume restore management using SnapVault

Volume restore using SnapVault overview

You can quickly restore a volume from a SnapVault backup in ONTAP when there is a data loss.

Use this procedure if you want to restore from the vault backup in the following way:

- You are working with clusters running ONTAP 9.
- You are a cluster administrator.
- You have configured the vault relationship following the procedure described in Volume backup using SnapVault
- You do not want to perform a single file or LUN restore.
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.
- You want to use the System Manager classic interface for ONTAP 9.7 and earlier releases, not the ONTAP System Manager UI for ONTAP 9.7 and later.

If these assumptions are not correct for your situation, or if you want more conceptual background information, you should see the following resource:

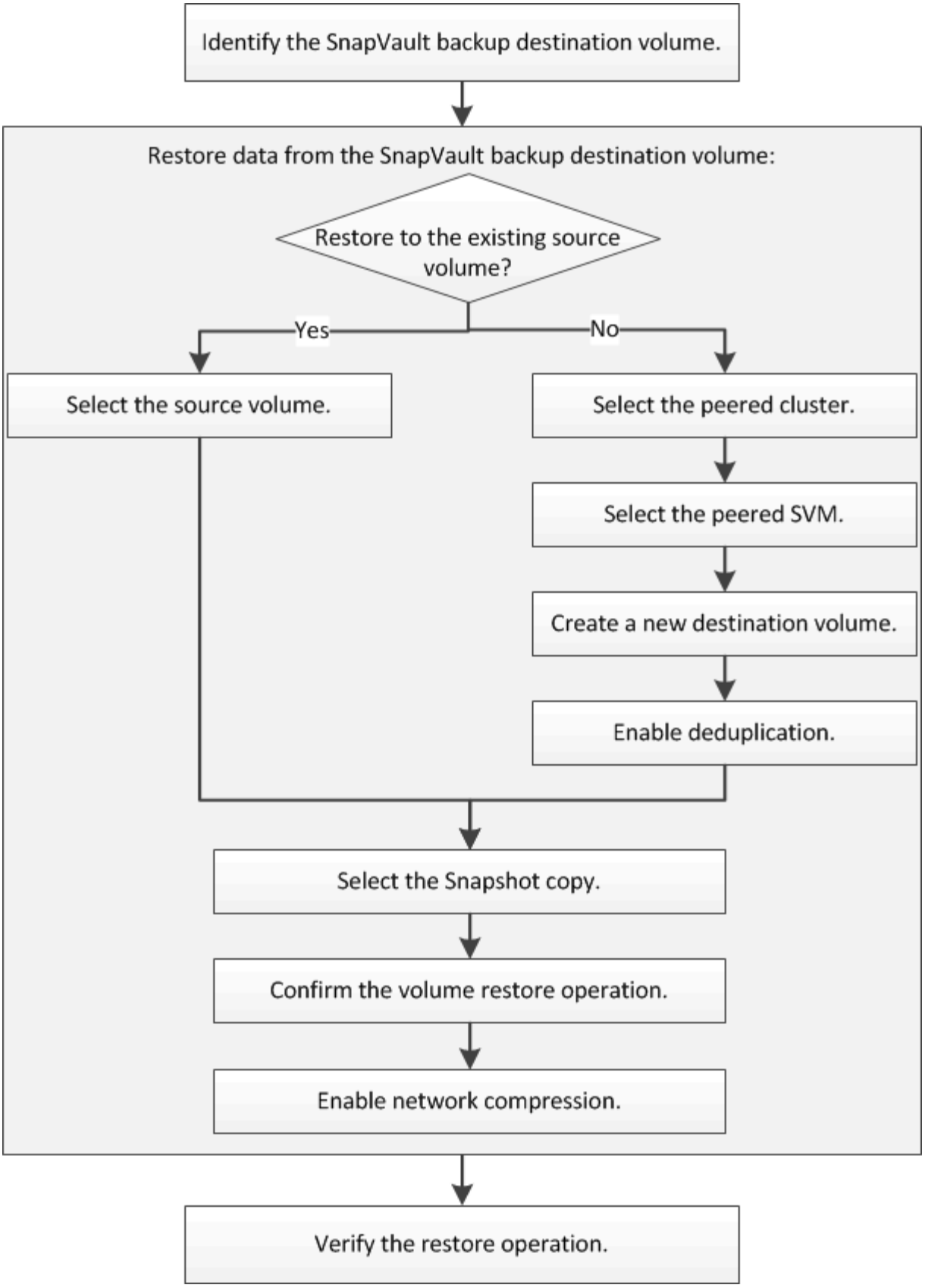
NetApp Technical Report 4183: SnapVault Best Practices

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
The redesigned System Manager (available with ONTAP 9.7 and later)	Restore a volume from an earlier Snapshot copy
The ONTAP command line interface	Restore the contents of a volume from a SnapMirror destination

Volume restore workflow

When your source volume is unavailable or data is corrupted, you can perform a restore from a SnapVault backup. Restoring a volume from a SnapVault backup involves selecting the SnapVault destination volume, restoring either to a new volume or existing volume, and verifying the restore operation.



Additional information is available to help you to manage the SnapVault backup relationships and to use other methods of data protection to protect the availability of your data resources.

- Volume disaster recovery preparation

Describes how to quickly configure a destination volume on a different ONTAP cluster in preparation for disaster recovery.

- Volume disaster recovery

  Describes how to quickly activate a destination volume from a different ONTAP cluster after a disaster, as well as how to restore the SnapMirror relationship to its original state by reactivating the source volume after its recovery.

Identify the SnapVault backup destination volume

You must identify the SnapVault backup destination volume from which you want to restore data when the data in the source volume is corrupted or lost.

About this task

You must perform this task from the **source** cluster.

Steps

1. Enter the URL `https://IP-address-of-cluster-management-LIF` in a web browser and log in to System Manager using your cluster administrator credential.
2. Navigate to the **Volumes** window.
3. Identify the destination volume in the SnapVault relationship and the name of the SVM that contains the volume:
   - ONTAP 9.3 or later: Double-click the volume to view the details, and then click **PROTECTION**.
   - ONTAP 9.2 or earlier: Click the **Data Protection** tab at the bottom of the Volumes window.

Restore data from a SnapVault backup

After selecting the SnapVault backup destination volume, you must perform the restore operation either to a new volume to test the backed-up data or to an existing volume to restore the lost or corrupted data.

About this task

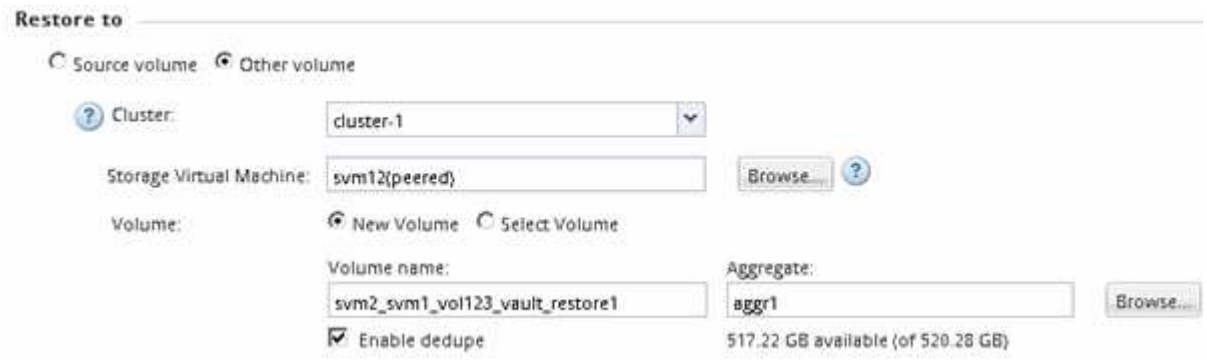
You must perform this task from the **destination** cluster.

Steps

1. Depending on the System Manager version that you are running, perform one of the following steps:
   - ONTAP 9.4 or earlier: Click **Protection** > **Relationships**.
   - Beginning with ONTAP 9.5: Click **Protection** > **Volume Relationships**.
2. Select the SVM that contains the SnapVault backup destination volume, and then click **Operations** > **Restore**.
3. In the **Restore** dialog box, restore the data to the original source volume or a new volume:

If you want to restore to…	Then…
The original source volume	Select **Source volume**.

If you want to restore to…	Then…
A new volume	a. Select **Other volume**. b. Select the peered cluster and the peered SVM for the volume. c. Select a peered SVM from the list. d. If the SVM is not peered, create the SVM peer relationship: i. Select the SVM. ii. Click **Authenticate**. iii. Enter the cluster administrator's credentials of the peered cluster, and then click **Create**. e. Select **New Volume**. f. If you want to change the default name, displayed in the format `destination_SVM_name_destination_volume_name_restore`, specify a new name and select the containing aggregate for the volume. g. Select the **Enable dedupe** check box.



4. Select either the latest Snapshot copy or select a specific Snapshot copy that you want to restore.
5. Select the **OK to restore the volume from the Snapshot copy** check box.
6. Select the **Enable Network Compression** check box to compress the data that is being transferred during the restore operation.
7. Click **Restore**.

   During the restore process, the volume being restored is changed to read-only. After the restore operation finishes, the temporary relationship is removed and the restored volume is changed to read/write.

8. Click **OK** in the message box.

Verify the restore operation

After performing the restore operation from the SnapVault backup destination volume, you must verify the status of the restore operation on the source cluster.

About this task

You must perform this task from the **source** cluster.

Steps

1. Navigate to the **Volumes** window.
2. Select the source volume in the volumes list and perform one of the following actions, depending on your ONTAP version:
   - Beginning with ONTAP 9.3: Double-click the source volume to view the details, and then click **PROTECTION** to identify the destination volume in the SnapMirror relationship and the name of the SVM that contains the volume.
   - ONTAP 9.2 or earlier: Click the **Data Protection** bottom tab to identify the destination volume in the SnapMirror relationship and the name of the SVM that contains the volume.
     The Type field displays `Restore` temporarily. After the restore operation is completed, the field displays `Vault`.

     You should troubleshoot any issues in the SnapVault relationships. The troubleshooting procedures for SnapMirror relationships are also applicable to SnapVault relationships.

     NetApp Technical Report 4015: SnapMirror Configuration and Best Practices for ONTAP 9.1, 9.2

Cluster administration

Cluster administration

Cluster expansion administration

Cluster expansion overview

You can quickly and nondisruptively expand an existing cluster by adding an HA pair. A larger cluster increases performance and storage capacity available in the cluster.

You should use this procedure only if the following is true:

- The existing cluster meets the following requirements:
  - It is running ONTAP 9.
  - It contains at least two nodes.

    Although examples in this procedure use a two-node cluster, it also applies to clusters with more than two nodes.

    If you want to add a node to a single-node cluster, you must follow a different procedure.

    Adding a second controller to create an HA pair

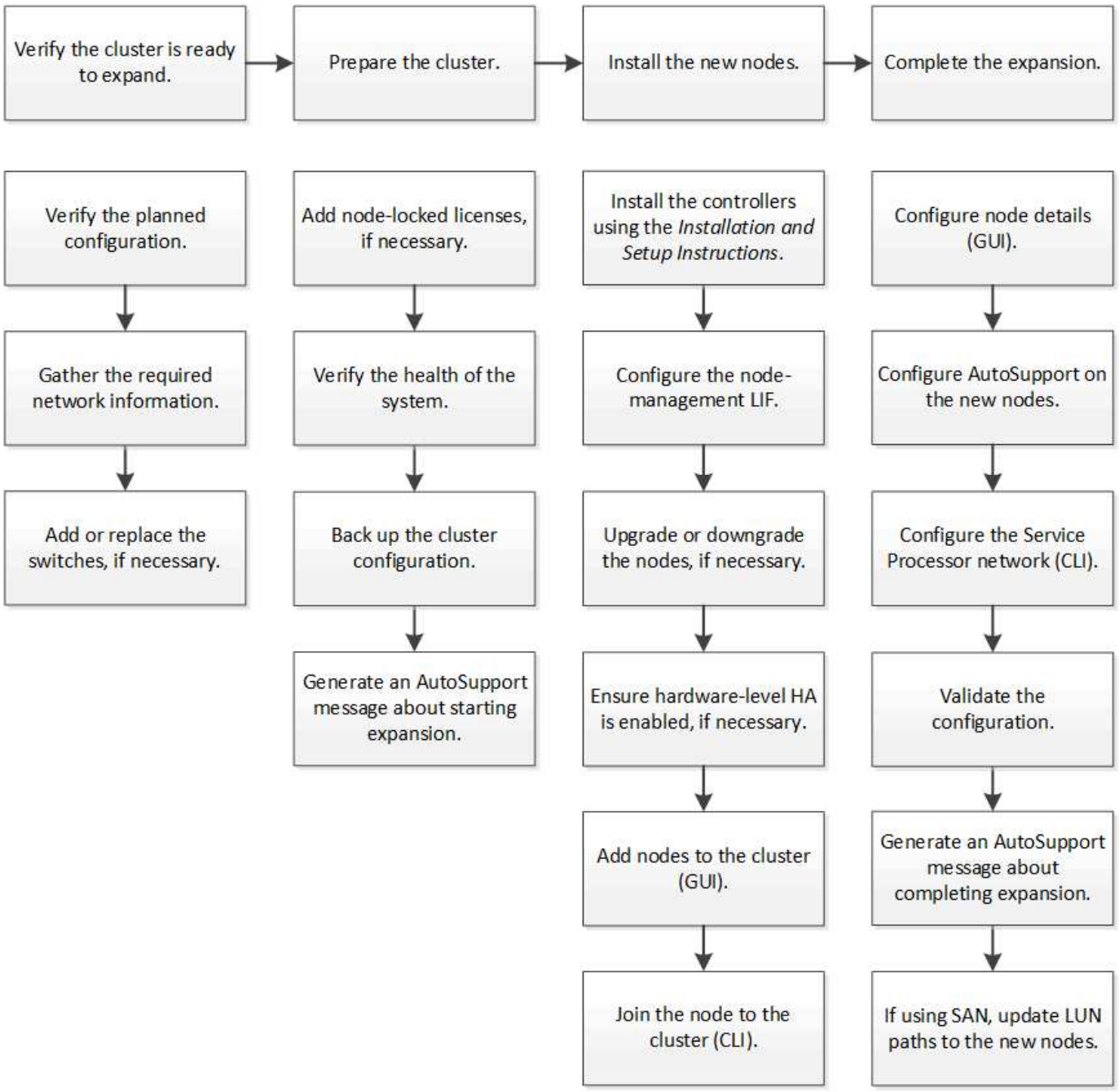
  - It does not use IPv6 addressing or Storage Encryption.
  - It is not a MetroCluster configuration.
- The controller modules that you plan to add meet the following requirements:
  - If they are not new, they have been wiped clean, are no longer part of a cluster, and are ready to be added to the new cluster.
  - They support ONTAP 9.
  - They are running a version of the ONTAP 9 release family.
- When completing ONTAP configuration tasks with System Manager, you want to use the *Classic* System Manager UI for ONTAP 9.7 and earlier releases, not the ONTAP System Manager UI for ONTAP 9.7 and later.

  ONTAP System Manager documentation

- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.

Cluster expansion workflow

Adding two nodes to an existing cluster involves verifying that the cluster is ready for expansion, preparing the cluster, installing the new nodes, and completing the expansion.



Verify the cluster is ready for expansion

Before you start expanding a cluster, you must verify the planned configuration, gather the required network information, and add or replace switches, if necessary.

Verify the planned configuration

Before you expand a cluster, you must ensure the following: the planned configuration is supported, the required licenses exist, the site is ready, the cluster switches support the expansion, and the existing nodes are using the same version of ONTAP 9.

Before you begin

You must have two sets of credentials—the user name and password required to log in to the cluster as an

administrator, and the user name and password required to log in to the NetApp Support Site.

Steps

1. Verify the planned configuration:

   a. Verify that the platform of the new controllers can be mixed with the cluster's existing controllers.

   b. Verify that the expanded cluster does not exceed the system limits for the platforms.

      NetApp Hardware Universe

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

      SAN configuration

   If these requirements are not met, you cannot proceed with the expansion.

2. Ensure that licenses cover the new nodes:

   a. On the existing cluster, view the licenses by using the `system license show` command.

```
cluster1::> system license show

Serial Number: 9-99-999999
Owner: cluster1
Package           Type    Description           Expiration
----------------- ------- --------------------- --------------------
Base              site    Cluster Base License  -
NFS               license NFS License           -
CIFS              license CIFS License          -
...
```

   b. Review the output to identify the node-locked licenses (identified by the type `license`) that will be required for the additional nodes.

   c. Ensure that the licenses that are included with the additional nodes are consistent with the cluster's existing node-locked licenses.

      NetApp Software License Search

   If you do not have the required licenses for the additional nodes, you must purchase additional licenses before you proceed.

3. Verify that the site is ready for all the new equipment.

   NetApp Hardware Universe

   If the site is not ready, you must prepare the site before continuing with the expansion.

4. Verify that the existing switches support the additional controllers.

   NetApp Hardware Universe

If the cluster is switchless or if the existing switches do not support the additional nodes, you must obtain cluster switches, which you can install later in the expansion process.

5. Verify that all nodes in the existing cluster are running the same version of ONTAP 9—including the same minor release and patch, if applicable—by using the `cluster image show` command.

```
cluster1::> cluster image show
                Current                 Installation
Node            Version                 Date
--------------- ----------------------- ------------
cluster1-1      8.3RC1                  12/15/2014 17:37:26
cluster1-2      8.3RC1                  12/15/2014 17:37:42
2 entries were displayed.
```

You should make note of the version of ONTAP software for reference later in this workflow.

Gather the required network information

Before you expand a cluster, you must obtain networking information required to later configure the node-management LIFs and the Service Processor IP addresses for both of the nodes.

Steps

1. Obtain the following details to configure two node-management LIFs—one for each of the nodes that you plan to add to the cluster:
   - IP address
   - Network mask
   - Gateway
   - Port
2. If your site typically has DNS entries for node-management LIFs, ensure that DNS entries are created for the new nodes.
3. Determine whether the cluster uses automatic or manual network configuration for the SP by using the `system service-processor network auto-configuration show` command.

   If a subnet name is displayed in either the `SP IPv4 Subnet Name` or `SP IPv6 Subnet Name` column, the cluster is using automatic SP networking. If both columns are blank, the cluster is using manual SP networking.

   In the following output, the sub1 subnet indicates that cluster1 SP uses automatic network configuration:

```
cluster1::> system service-processor network auto-configuration show
Cluster Name         SP IPv4 Subnet Name          SP IPv6 Subnet Name
-------------------- ---------------------------- -------------------
cluster1             sub1                            -
```

In the following output, the blank subnet fields indicate that cluster1 SP uses manual network configuration:

```
cluster1::> system service-processor network auto-configuration show
Cluster Name         SP IPv4 Subnet Name          SP IPv6 Subnet Name
-------------------- ---------------------------- -------------------
cluster1             -                            -
```

4. Depending on the SP network configuration, perform one of the following actions:
   - If the SP uses manual network configuration, obtain two IP addresses that you will use later when configuring SP on the new nodes.
   - If the SP uses automatic network configuration, verify that the subnet used by the SP has available IP addresses for the two new nodes by using the `network subnet show` command.
     In the following output, the sub1 subnet has 2 addresses available:

```
cluster1::>  network subnet show
IPspace: Default
Subnet                     Broadcast                    Avail/
Name      Subnet           Domain    Gateway           Total   Ranges
--------- ---------------- --------- --------------- ---------
---------------
sub1      10.53.33.1/18    Default   10.53.0.1          2/4
10.53.33.3-10.53.33.6
...
```

Add or replace switches

Before you expand the cluster, you must ensure that the cluster switches support the expanded configuration. If the cluster is switchless, you must add switches. If the existing switches do not have enough ports available to support the new configuration, you must replace the switches.

Procedure

- If the cluster is currently a two-node switchless cluster, migrate the cluster to a two-node switched cluster using the type of switch you prefer.

  Migrating to a two-node switched cluster with Cisco cluster switches

  Migrating to a two-node switched cluster with NetApp CN1610 cluster switches

- If the existing switches do not have enough ports available to support the future configuration, replace the switches by using the appropriate replacement procedure.

  NetApp Documentation: Cluster, Management and Storage Switches

Prepare the cluster for expansion

To prepare a cluster for expansion, you must add node-locked licenses, verify the system health, back up the cluster's configuration, and generate an AutoSupport message.

Add node-locked licenses

If the cluster has features that use node-locked licenses (which entitle only specific nodes to the licensed functionality), you must ensure that node-locked licenses are installed for the new nodes. You should add the licenses before the nodes are joined to the cluster.

Complete this task if you are using the *Classic* System Manager UI with ONTAP 9.7 and earlier releases. If you are using the System Manager UI with ONTAP 9.7 and later, see Enable new features by adding license keys.

For more information about managing licenses, see Manage licenses overview.

Steps

1. Add each license key by using the `system license add` command.

```
cluster1::> system license add -license-code AAAAAAAAAAAAAA
```

2. View the existing licenses by using the `system license show` command.

```
cluster1::> system license show

Serial Number: 9-99-999999
Owner: cluster1
Package           Type    Description           Expiration
----------------- ------- --------------------- --------------------
Base              site    Cluster Base License  -
NFS               license NFS License           -
CIFS              license CIFS License          -
...
```

3. Review the output to ensure that a node-locked license is displayed for all serial numbers, including serial numbers for existing and new nodes.

Verify the health of the system

Before you expand a cluster, you must verify that all components of the cluster are healthy by running the Config Advisor tool and running several ONTAP CLI commands.

Steps

1. Verify that you have the latest version of Config Advisor:
   - If you do not have Config Advisor on your laptop, download it.

     NetApp Downloads: Config Advisor

◦ If you have Config Advisor, start it, click **Help** > **Check for Updates**, and follow the prompts to upgrade it if necessary.

> Do not uninstall the previous version of the tool or delete the data folder during the upgrade. The tool uninstalls the previous version and replaces it with the latest version. It renames the data folder as the latest folder and retains all of the contents in the folder.

2. Verify the cabling and configuration by running Config Advisor:
   a. Connect your laptop to the management network for the cluster.
   b. Click **Collect Data**.

      Config Advisor displays any problems found.

   c. If problems are found, correct them and run the tool again.
3. Check the health of the system with the following commands:
   a. Verify that the cluster is in a healthy state by using the `system health status show` command and verifying that the Status is `ok`.

```
cluster1::> system health status show
Status
---------------
ok
```

   b. Verify that all nodes in the cluster are in a healthy state by using the `cluster show` command and verifying that the Health of each node is `true`.

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-1            true    true
cluster1-2            true    true
2 entries were displayed.
```

Back up the cluster configuration

Before you expand a cluster, you should use advanced privilege to create a backup file to save the cluster configuration information and optionally save the node configurations.

Steps

1. Set the privilege level to advanced by using the `set -privilege advanced` command.
2. Create a backup file of the cluster configuration by using the `system configuration backup create` command with the `-backup-type cluster` parameter.

```
cluster1::*> system configuration backup create -node cluster1-1 -backup
-name clusterbeforeexpansion.7z -backup-type cluster
[Job 5573] Job is queued: Cluster Backup OnDemand Job.
```

3. Create a backup file of each node's configuration by using the `system configuration backup create` command with the `-backup-type node` parameter for each node.
4. Return the privilege level to admin by using the `set -privilege admin` command.

Generate an AutoSupport message about starting expansion

Immediately before you expand a cluster, you should send an AutoSupport message to indicate that you are about to start the expansion process. The message informs internal and external support staff about expansion and acts as a timestamp for any troubleshooting that might be required later.

Before you begin

AutoSupport must be set up.

Steps

1. For each node in the cluster, send an AutoSupport message by using the `system node autosupport invoke` command.

```
cluster1::> system node autosupport invoke -node * -message "cluster
expansion started" -type all
The AutoSupport was successfully invoked on node "cluster1-1". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
The AutoSupport was successfully invoked on node "cluster1-2". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
2 entries were acted on.
```

Install the new nodes

After the cluster is prepared, you must install the controllers and configure the node-management LIFs. If the controllers are not running the same ONTAP version as the existing cluster, or are repurposed and lack hardware-level HA, you must address those issues in Maintenance mode. Finally, you can join the nodes to the cluster.

Install the controllers

When you install controllers that will be added to an existing cluster, you must follow the first three steps of the appropriate *Installation and Setup Instructions*.

About this task

As of ONTAP 9.0, HA mode is enabled by default on new hardware.

Steps

1. Obtain the *Installation and Setup Instructions* for the FAS model number of the controller module that you plan to add to the cluster.
   - For a new controller module, the document is available in the box.
   - For a repurposed controller module, you can download the document.
     NetApp Documentation
2. Follow the *Prepare for installation* section with the following exceptions:
   - You can skip any instructions about downloading software or a worksheet.
   - You must provide a serial console connection even if it is not mentioned in the *Installation and Setup Instructions*.

     You require a serial console because you must use the nodeshell CLI to configure node-management LIFs.

     If the ONTAP section does not mention the serial console, you can see the 7-mode section.
3. Follow the *Install hardware* section.
4. Follow the *Cable storage* section.
5. Skip most of the *Complete System Setup* section with the following exceptions:
   - If instructed to, you must power on all disk shelves and check IDs.
   - You must cable the serial console so that you can access the node.

     If the ONTAP section does not mention the serial console, you can see the 7-mode section.
6. Skip the *Complete configuration* section.

Configure node-management LIFs

After the controller modules are physically installed, you can power on each one and configure its node-management LIF.

About this task

You must perform this procedure on both the nodes.

Steps

1. Access the controller module through the serial console.
2. Power on the controller module, and wait while the node boots and the Cluster Setup wizard automatically starts on the console.

```
Welcome to the cluster setup wizard.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the cluster setup wizard.
   Any changes you made before quitting will be saved.

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

3. Follow the prompts in the web-based Cluster Setup wizard to configure a node management LIF using the networking information you gathered earlier.
4. Type `exit` after node management LIF configuration is complete to exit the setup wizard and complete the administration tasks.

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

Otherwise, press Enter to complete cluster setup using the command line
interface:
exit
```

5. Log in to the node as the `admin` user, which does not require a password.

```
Tue Mar 4 23:13:33 UTC 2015
login: admin
****************************************************
* This is a serial console session. Output from this *
* session is mirrored on the SP console session.     *
```

6. Repeat the entire procedure for the second newly installed controller module.

Upgrade or downgrade the nodes

Before joining the newly installed nodes to the cluster, you must ensure that they are running the same version of ONTAP that the cluster is running. If the nodes are running a different version, you must upgrade or downgrade the nodes to match the cluster.

Steps

1. Determine the version of ONTAP installed on the cluster: `cluster image show`
2. View the current version of ONTAP on the nodes:
   a. On the first node, view the software version: `system node image show`

```
::*> system node image show
                  Is      Is                                    Install
Node     Image    Default Current Version                       Date
-------- -------  ------- ------- --------------------------
------------------
localhost
         image1   false   false   9.3                       MM/DD/YYYY
TIMESTAMP
         image1   true    true    9.3                       MM/DD/YYYY
TIMESTAMP
2 entries were displayed.
```

b. Repeat the previous step for the second node.

3. Compare the versions of ONTAP on the cluster and the nodes, and perform either of the following actions:
   - If the versions of ONTAP on the cluster and the nodes are the same, no upgrade or downgrade is needed.
   - If the versions of ONTAP on the cluster and the nodes are different, you can Upgrade ONTAP on nodes with earlier versions or you can Revert ONTAP for nodes with later versions.

Ensure hardware-level HA is enabled

If the newly installed controller modules are reused—not new—you must enter Maintenance mode and ensure that their HA state is set to HA.

About this task

If you are using new controller modules, you can skip this procedure because HA is enabled by default. Otherwise, you must perform this procedure on both the nodes.

Steps

1. On the first node, enter Maintenance mode:
   a. Exit the nodeshell by entering `halt`.

      The LOADER prompt is displayed.

   b. Enter Maintenance mode by entering `boot_ontap maint`.

      After some information is displayed, the Maintenance mode prompt is displayed.

2. In Maintenance mode, ensure that the controller module and chassis are in HA state:
   a. Display the HA state of the controller module and chassis by entering `ha-config show`.
   b. If the displayed state of the controller is not `HA`, enter `ha-config modify controller ha`.
   c. If the displayed state of the chassis is not `HA`, enter `ha-config modify chassis ha`.
   d. Verify that HA is enabled on both the controller module and chassis by entering `ha-config show`.
3. Return to ONTAP:

a. Enter `halt` to exit Maintenance mode.

b. Boot ONTAP by entering `boot_ontap`

c. Wait while the node boots and the Cluster Setup wizard automatically starts on the console.

d. Press Enter four times to accept the existing settings for the node-management LIF.

e. Log in to the node as the `admin` user, which does not require a password.

4. Repeat this procedure on the other node that you are adding to the cluster.

Add nodes to a cluster using System Manager

You can use System Manager to increase the size and capabilities of your storage system by adding nodes to an existing cluster. This feature is automatically enabled in System Manager when the effective cluster version is ONTAP 9.2.

Before you begin

- New compatible nodes must be cabled to the cluster.

  Only the ports that are in the default broadcast domain will be listed in the Network window.

- All of the nodes in the cluster must be up and running.
- All of the nodes must be of the same version.

Step

1. Add the new compatible nodes to the cluster:

If you are…	Do this…
Not logged in to System Manager	a. Log in to System Manager. The new compatible nodes are automatically detected by System Manager at login. System Manager prompts you to add the new compatible nodes to the cluster. b. Click **Add Nodes to Cluster**. c. Modify the name of the nodes. d. Specify the node licenses. e. Click **Submit and Proceed**.

Logged in to System Manager	a. Depending on the System Manager version that you are running, perform one of the following steps: ◦ ONTAP 9.4 or earlier: Click **Configuration** > **Cluster Expansion**. ◦ Beginning with ONTAP 9.5: Click **Configuration** > **Cluster** > **Expansion** System Manager searches for newly added nodes. If any warnings are displayed, you must fix them before proceeding. If new compatible nodes are discovered, proceed to the next step. b. Modify the name of the nodes. c. Specify the node licenses. d. Click **Submit and Proceed**.

Join nodes to the cluster using the CLI

When the newly installed controller modules are ready, you can add each one to the cluster by using the `cluster setup` command.

About this task

- You must perform this procedure on both nodes.
- You must join each node one at a time, not concurrently.

Steps

1. Start the Cluster Setup wizard by using the `cluster setup` command at the CLI prompt.

```
::> cluster setup

Welcome to the cluster setup wizard....

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

Otherwise, press Enter to complete cluster setup using the
command line interface:
```

> For instructions using the GUI-based cluster setup wizard, see Adding nodes to the cluster using System Manager.

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

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

3. When prompted with the existing cluster interface configuration, press `Enter` to accept it.

```
Existing cluster interface configuration found:

Port    MTU     IP              Netmask
e1a     9000    169.254.87.75   255.255.0.0

Do you want to use this configuration? {yes, no} [yes]:
```

4. Follow the prompts to join the existing cluster.

```
Step 1 of 3: Join an Existing Cluster
You can type "back", "exit", or "help" at any question.

Enter the name of the cluster you would like to join [cluster1]:
cluster1

Joining cluster cluster1

Starting cluster support services ..

This node has joined the cluster cluster1.

Step 2 of 3: Configure Storage Failover (SFO)
You can type "back", "exit", or "help" at any question.

SFO will be enabled when the partner joins the cluster.

Step 3 of 3: Set Up the Node

Cluster setup is now complete.
```

The node is automatically renamed to match the name of the cluster.

5. On the cluster, verify that the node is part of the cluster by using the `cluster show` command.

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-1            true    true
cluster1-2            true    true
cluster1-3            true    true
3 entries were displayed.
```

6. Repeat step 1 through step 5 for the second newly installed controller module.

   The Cluster Setup wizard differs on the second node in the following ways:

   - It defaults to joining the existing cluster because its partner is already part of a cluster.
   - It automatically enables storage failover on both nodes.

7. Verify that storage failover is enabled and possible by using the `storage failover show` command.

   The following output shows that storage failover is enabled and possible on all nodes of the cluster, including the newly added nodes:

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State
-------------- -------------- --------
-------------------------------------
cluster1-1     cluster1-2     true     Connected to cluster1-2
cluster1-2     cluster1-1     true     Connected to cluster1-1
cluster1-3     cluster1-4     true     Connected to cluster1-3
cluster1-4     cluster1-3     true     Connected to cluster1-4
4 entries were displayed.
```

Complete the expansion

After both nodes are joined to the cluster, you must finish configuring the newly added nodes by configuring AutoSupport and completing the SP network. You then validate the expanded cluster and generate an AutoSupport message to complete the expansion. If the cluster uses SAN, you should update LUN paths.

Configure the node details in System Manager

You can use System Manager to configure the node management LIF and Service Processor settings for the newly added nodes.

Before you begin

- Sufficient number of ports must be present in the default IPspace for LIF creation.
- All the ports must be up and running.

Steps

1. Configure node management:
   a. Enter the IP address in the **IP Address** field.
   b. Select the port for node management in the **Port** field.
   c. Enter the netmask and gateway details.
2. Configure Service Processor settings:
   a. Select the **Override defaults** check box to override the default values.

b. Enter the IP address, netmask, and gateway details.

3. Click **Submit and Proceed** to complete the network configuration of the nodes.
4. Verify the details of the nodes in the **Summary** page.

What to do next

- If your cluster is protected, you should create the required number of intercluster LIFs in the newly added nodes to avoid partial peering and unhealthy protection.
- If SAN data protocols are enabled in your cluster, you should create the required number of SAN Data LIFs for serving data.

Configure AutoSupport on the new nodes

After you add nodes to a cluster, you must configure AutoSupport on the nodes.

Before you begin

AutoSupport must be set up on the cluster's existing nodes.

About this task

You must perform this procedure on both the nodes.

Steps

1. View the AutoSupport configuration using the `system node autosupport show` command with the `-node` parameter set to one of the nodes in the original cluster.

```
cluster1::> system node autosupport show -node cluster1-1
                            Node: cluster1-1
                           State: enable
                 SMTP Mail Hosts: smtp.example.com

...
```

2. On one of the newly added nodes, configure AutoSupport in the same way that it is configured on the existing nodes by using the `system node autosupport modify` command.

```
cluster1::> system node autosupport modify -node cluster1-3 -state
enable -mail-hosts smtp.example.com -from alerts@node3.example.com -to
support@example.com -support enable -transport https -noteto
pda@example.com -retry-interval 23m
```

3. Repeat the previous step for the other newly added node.

Configure the Service Processor network

After you expand a cluster, you must configure the Service Processor (SP) network on the new nodes. If the SP uses manual network configuration, you must configure the IP

addresses for the SP on the new nodes. If the SP uses automatic network configuration, you must identify the IP addresses that were selected.

Steps

1. If the cluster SP uses manual network configuration, configure IP addresses on both nodes for the SP network by using the `system service-processor network modify` command.

   The following commands configure the SP network in cluster1-3 and cluster1-4 nodes:

   ```
   cluster1::> system service-processor network modify -node cluster1-3
   -address-family IPv4 -enable true -ip-address 192.168.123.98-netmask
   255.255.255.0 -gateway 192.168.123.1
   cluster1::> system service-processor network modify -node cluster1-4
   -address-family IPv4 -enable true -ip-address 192.168.123.99 -netmask
   255.255.255.0 -gateway 192.168.123.1
   ```

2. Verify that the SP network is configured correctly on both the new nodes by using the `system service-processor network show` command for each node.

   The status should be `succeeded`. Verification is required in all situations. Even if the SP network was automatically configured, you should verify that it was configured successfully, and you must determine which IP addresses were assigned.

   The following output indicates that both the cluster1-3 and the cluster1-4 nodes have successful SP network setup:

```
cluster1::> system service-processor network show -node cluster1-3
                            Address
Node          Status        Family    Link State  IP Address
------------- ------------- --------- -----------
------------------------
cluster1-3    online        IPv4      up          192.168.123.98

                                DHCP: none
                         MAC Address: 00:a0:98:43:a1:1e
                     Network Gateway: 10.60.172.1
              Network Mask (IPv4 only): 255.255.255.0
            Prefix Length (IPv6 only): -
                     IPv6 RA Enabled: -
                         Subnet Name: -
               SP Network Setup Status: succeeded
                                    ...

cluster1::> system service-processor network show -node cluster1-4
                            Address
Node          Status        Family    Link State  IP Address
------------- ------------- --------- -----------
------------------------
cluster1-4    online        IPv4      up          192.168.123.99

                                DHCP: none
                         MAC Address: 00:a0:98:43:a1:1e
                     Network Gateway: 10.60.172.1
              Network Mask (IPv4 only): 255.255.255.0
            Prefix Length (IPv6 only): -
                     IPv6 RA Enabled: -
                         Subnet Name: -
               SP Network Setup Status: succeeded
                                    ...
```

3. If your site typically has DNS entries for the SP network, verify that the DNS entries are created for the new nodes.

Validate the configuration of the expanded cluster

After you expand the cluster, you must validate the configuration by running Config Advisor and using some commands that verify cluster health and cluster replication rings.

Steps

1. Check the health of the configuration by running Config Advisor:
   a. Start Config Advisor, and then click **Collect Data**.

Config Advisor displays any problems found.

b. If problems are found, correct them and run the tool again.

2. Ensure that all nodes in the cluster are in a healthy state by using the `cluster show` command.

```
cluster-1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-1            true    true
cluster1-2            true    true
cluster1-3            true    true
cluster1-4            true    true
4 entries were displayed.
```

3. Ensure that the cluster replication rings have the same epoch, database epoch, and database transaction numbers on all nodes in the cluster:

   The easiest way to compare transaction numbers is to view them for one unit name at a time.

   a. Set the privilege level to advanced by using the `set -privilege advanced` command.

   b. View cluster ring information about the first unit name by using the `cluster ring show` command with the `-unitname mgmt` parameter, and verify that all nodes have the same number in the Epoch, DB Epoch, and DB Trnxs columns.

```
cluster-1::*> cluster ring show -unitname mgmt
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
cluster1-1
          mgmt     2        2        959      cluster1-1
                                                       master
cluster1-2
          mgmt     2        2        959      cluster1-2
                                                       secondary
cluster1-3
          mgmt     2        2        959      cluster1-3
                                                       master
cluster1-4
          mgmt     2        2        959      cluster1-3
                                                       secondary
4 entries were displayed.
```

   c. Repeat the command with the `-unitname vldb` parameter.

   d. Repeat the command with the `-unitname vifmgr` parameter.

   e. Repeat the command with the `-unitname bcomd` parameter.

f. Repeat the command with the `-unitname crs` parameter.

g. Return the privilege level to admin by using the `set -privilege admin` command.

Generate an AutoSupport message about completing expansion

After you expand a cluster, you should send an AutoSupport message to indicate that the expansion process is complete. This message communicates to internal and external support staff that the expansion is complete and acts as a timestamp for any troubleshooting that might be required later.

Before you begin

AutoSupport must be set up.

Steps

1. For each node in the cluster, send an AutoSupport message by using the `system node autosupport invoke` command.

   You must issue the message once for each node in the cluster, including the newly added nodes.

   If you added two nodes to a two-node cluster, you must send the message four times.

```
cluster1::> system node autosupport invoke -node * -message "cluster
expansion complete" -type all
The AutoSupport was successfully invoked on node "cluster1-1". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
The AutoSupport was successfully invoked on node "cluster1-2". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
The AutoSupport was successfully invoked on node "cluster1-3". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
The AutoSupport was successfully invoked on node "cluster1-4". To view
the status
of the AutoSupport, use the "system node autosupport history show"
command.
Note: It may take several minutes for the AutoSupport to appear in the
history list.
4 entries were acted on.
```

Update LUN paths for the new nodes

If your cluster is configured for SAN, you must create SAN LIFs on the newly added nodes and then update paths.

About this task

This procedure is required only if the cluster contains LUNs. If the cluster contains only files, you can skip this procedure.

Steps

1. For each storage virtual machine (SVM) in the cluster, create new LIFs on the newly added nodes:
   a. Identify the SVMs that use FC or iSCSI protocols by using the `vserver show` command with the `-fields allowed-protocols` parameter and reviewing the output.

```
cluster1::> vserver show -fields allowed-protocols
vserver allowed-protocols
------- -----------------
vs1     cifs,ndmp
vs2     fcp
vs3     iscsi
...
```

b. For each SVM that uses FC or iSCSI, create at least two data LIFs on each of the newly added nodes by using the `network interface create` command with the `-role data` parameter.

```
cluster1::> network interface create -vserver vs1 -lif lif5 -role
data
-data-protocol iscsi -home-node cluster1-3 -home-port e0b
-address 192.168.2.72 -netmask 255.255.255.0
```

c. For each SVM, verify that it has LIFs on all nodes in the cluster by using the `network interface show` command with the `-vserver` parameter.

2. Update portsets:
   a. Determine whether portsets exist by using the `lun portset show` command.
   b. If you want to make the new LIFs visible to existing hosts, add each new LIF to the portsets by using the `lun portset add` command—once for each LIF.
3. If you use FC or FCoE, update zoning:
   a. Verify that zoning is set up correctly to enable the existing initiator ports on the host to connect to the new target ports on the new nodes.
   b. Update switch zoning to connect the new nodes to existing initiators.

      Zoning setup varies depending on the switch that you use.

   c. If you plan to move LUNs to the new nodes, expose the new paths to the hosts by using the `lun mapping add-reporting-nodes` command.
4. On all host operating systems, rescan to discover the newly added paths.
5. Depending on the host operating systems, remove any stale paths.
6. Add or remove paths to your MPIO configuration.

Related information

SAN configuration

SAN administration

Volume move management

Volume move overview

Using ONTAP System Manager classic interface with ONTAP 9.7 or earlier, you can nondisruptively move a data volume from one node to another node within the same storage virtual machine (SVM) in an ONTAP 9 cluster.

Requirements for using these procedures

Before you use perform these procedures, ensure that the following conditions are met:

- The cluster is running ONTAP 9.
- You have cluster administrator privileges.
- You want to use best practices, not explore every available option.
- You want to use the *Classic* System Manager UI for ONTAP 9.7 and earlier releases, not the ONTAP System Manager UI for ONTAP 9.7 and later.

  For some tasks, you must use the ONTAP command-line interface (CLI).

- You know which volume you want to move.

  For help in deciding which volumes to move, you can use Active IQ Unified Manager (formerly OnCommand Unified Manager).

- The volume that will be moved is a data volume.
- Any new or repurposed hardware is fully installed and already has aggregates.
- If the cluster has LUNs, all nodes have two paths per LUN.
- Flow control is not enabled on cluster network ports.
- For volumes containing namespaces, the cluster is running ONTAP 9.6 or later.

  Volume move is not supported for NVMe configurations running ONTAP 9.5.

Other ways to do this in ONTAP

To complete this task using…	Refer to…
The redesigned System Manager (available with ONTAP 9.7 and later)	Manage volumes
The ONTAP command-line interface	Logical storage management

Alternatives to volume move

Before moving volumes, you should evaluate whether the following approaches are better suited to your situation:

- If you want to nondisruptively upgrade a controller in place, you can consider using aggregate relocation

(ARL), which does not require physical data movement.

High Availability

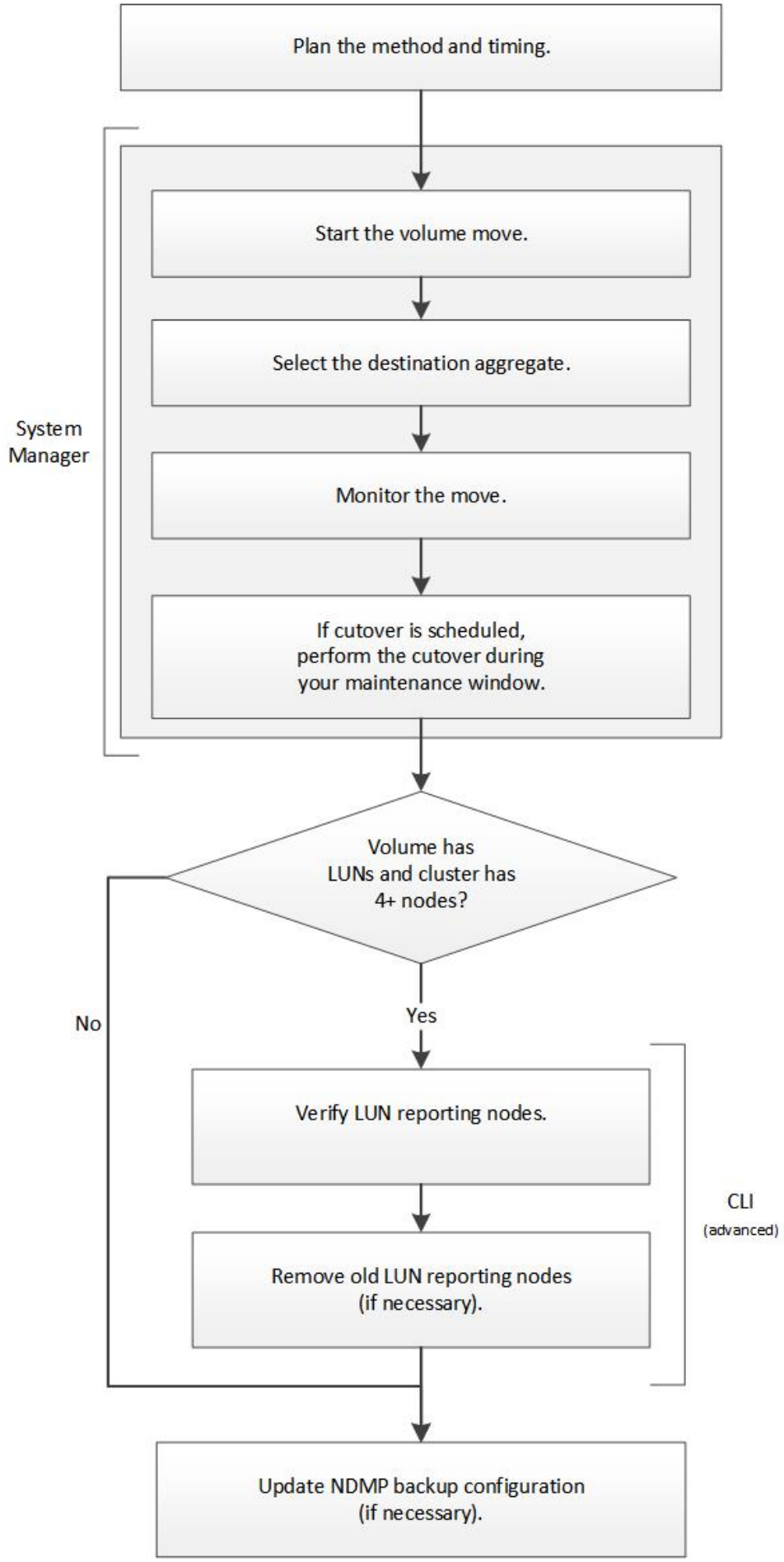
- If you want to move only a LUN without its containing volume, you can use the LUN move process.

  SAN administration

Volume move workflow

You can move a volume by using the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier.

Before moving a volume, you should select a method for the volume move operation and plan the timing of the operation. After the move, you might have to update the NDMP backup configuration.


Plan the method and timing.
System Manager
Start the volume move.
Select the destination aggregate.
Monitor the move.
If cutover is scheduled, perform the cutover during your maintenance window.
Volume has LUNs and cluster has 4+ nodes?
No
Yes
CLI (advanced)
Verify LUN reporting nodes.
Remove old LUN reporting nodes (if necessary).
Update NDMP backup configuration (if necessary).

Other ways to do this in ONTAP

To complete this workflow using…	Refer to…
The redesigned System Manager (available with ONTAP 9.7 and later)	Manage volumes
The ONTAP command-line interface	Logical storage management

Plan the method and timing of a volume move

You can use the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier to move a volume and to decide whether to have a manual cutover. If you need to update LUN reporting nodes, you must follow an advanced procedure in the command-line interface (CLI). Optionally, you can also plan the timing of a volume move.

About this task

The source volume of a SnapMirror or SnapVault relationship can be moved while the volume is being mirrored. SnapMirror services encounter a brief pause during the cutover phase of the volume move job.

The destination volume can also be moved. In the iterative phase, SnapMirror or SnapVault updates and volume move operations run concurrently. When evaluating whether a cutover is possible in the cutover phase, priority between the cutover and SnapMirror or SnapVault updates is determined on a first-come, first-served basis. Until the first operation finishes, other operations are blocked.

Steps

1. Decide whether you require a manual cutover.

   Cutover is the moment at which the move operation finishes and ONTAP starts serving data from the volume on the new aggregate. The cutover can occur automatically or you can trigger the cutover manually.

   If your company's standard practice requires you to control when changes occur in the storage system, you can manually perform the final cutover of the move operation during a maintenance window.

   A cutover does not require an outage, but you can use a maintenance window to control *when* it occurs.

   > The volume move operation is nondisruptive, regardless of whether you choose automatic or manual cutover.

2. If the volume contains LUNs and the cluster contains four or more nodes, use the CLI to update the LUN reporting nodes if the volume moves to a different HA pair.

   If the volume does not contain LUNs or if the cluster contains only two nodes, you can skip this step.

3. **Optional:** Plan a time using the following considerations:
   - A volume move operation might take more time than expected because moves are designed to occur nondisruptively in the background in a manner that preserves client access and overall system performance.

     For example, ONTAP throttles the resources that are available to the volume move operation.

- If you want the move to occur as quickly as possible, you must select a time with less cluster activity, especially the following activities:
  - I/O operations on the volume
  - Jobs using background resources, for example, when controller CPU usage is less than 50 percent
  - Jobs using the cluster interconnect
- A move cannot be started while the volume is affected by the following operations: volume offline, restrict, or destroy; SnapMirror resync, break, or restore; and Snapshot restore.

  You must wait for any of these specific operations to finish before you can start the move.
- While the volume move operation occurs, a MetroCluster switchback cannot occur, although a switchover can occur.
- MetroCluster switchbacks are blocked when volume move operations are in progress for volumes belonging to the switched over site. Switchbacks are not blocked when volume move operations are in progress for volumes local to the surviving site.
- Forced MetroCluster switchovers can occur when volume move operations are in progress.

Related information

Verifying LUN reporting nodes after moving a volume

Move a volume using System Manager

Using the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier, you can move a volume by selecting a volume and the destination aggregate, starting the volume move operation, and optionally monitoring the volume move job. When using System Manager, a volume move operation finishes automatically.

Before you begin

You should have reviewed the available space on the source aggregate and destination aggregate before the volume move operation and after the volume move operation.

About this task

A volume move operation is supported only within the same cluster. In addition, you should note that the aggregate you are moving the volume to and the aggregate you are moving the volume from must be in the same storage virtual machine (SVM). A volume move does not disrupt client access.

Steps

1. Navigate to the **Volumes** window.
2. Select the volume that you want to move, and then click **Actions** > **Move**.
3. Select the destination aggregate, and then start the volume move operation:
   a. Select a destination aggregate from the list of possible aggregates, which includes only the aggregates that have the required capacity.

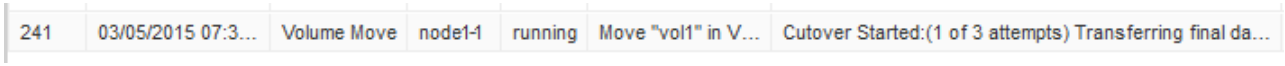
      You should review the available space, total space, RAID type, and storage type of the aggregates. For example, if the goal is to alter the performance characteristics of the volume, you can focus on aggregates with the desired storage type.

   b. Click **Move**, and then click **Move** again to confirm that you want to proceed with the volume move operation.

When the Move Volume dialog box is displayed, leave the dialog box open if you want to monitor the volume move job.

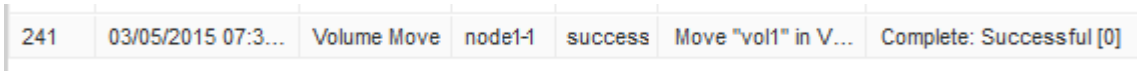
4. **Optional:** Monitor the volume move job:
   a. In the **Move Volume** dialog box, click the link to the **Job ID** of the volume move job.
   b. Locate the volume move job, and then review the information in the **Status** column.

      The job can be in any one of several phases, such as transferring the initial baseline of data or starting a cutover attempt.



241	03/05/2015 07:3...	Volume Move	node1-1	running	Move "vol1" in V...	Cutover Started:(1 of 3 attempts) Transferring final da...

   c. Click **Refresh** in the **Jobs** window to view the updated job status.



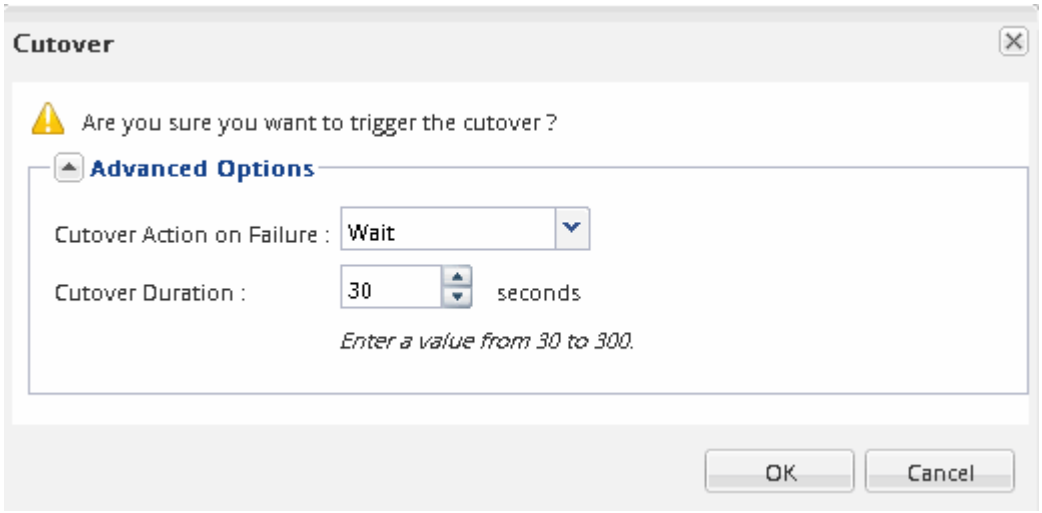
241	03/05/2015 07:3...	Volume Move	node1-1	success	Move "vol1" in V...	Complete: Successful [0]

      The job status changes to `Complete: Successful` when the volume move operation finishes.

5. If the volume move job enters the cutover deferred phase, perform a manual cutover.
   a. From the **Volumes** window, select the volume for which you initiated the volume move job.
   b. Initiate cutover for the volume:

If you are running…	Perform these steps…
ONTAP 9.3 or later	1. Expand the volume and click the **Show More Details** link to view more information about the volume. 2. In the **Overview** tab, click **Cutover**.
ONTAP 9.2 or earlier	In the **Volume Move Details** tab, click **Cutover**.

   c. In the **Cutover** dialog box, click **Advanced Options** .
   d. Specify the cutover action and the cutover duration.



e. Click **OK**.

6. Repeat Step 4.

Verify LUN reporting nodes after moving a volume

You can add LUN reporting nodes to help maintain optimized LUN paths.

If the volume that you move contains LUNs, and the destination aggregate is on another high-availability (HA) pair, ONTAP automatically adds an HA pair to the Selective LUN Map reporting-nodes list

Before you begin

Two LIFs must be configured: one LIF on the destination node and the other LIF on the HA partner of the destination node.

About this task

This procedure is required only if you move a volume from one HA pair to a different HA pair. If you move a volume to a different node of the same HA pair—for example, if you have a two-node cluster or a MetroCluster configuration—you can skip this procedure.

Steps

1. Verify that the destination node and its partner node are in the reporting-nodes list of the volume. If the nodes are not in the reporting-nodes list, add the destination node and its partner node to the reporting-nodes list of the volume:

   ```
   lun mapping add-reporting-nodes
   ```

2. Rescan from the host to discover the newly added paths.
3. Add the new paths to your MPIO configuration.
4. Remove the previous LUN owner and its partner node from the reporting-nodes list:

   ```
   lun mapping remove-reporting-nodes -remote-nodes -vserver vserver_name -path
   lun_path -igroup igroup_name
   ```

5. Rescan the host to verify removal of old paths.

   See your host documentation for specific steps to rescan your hosts.

Update LUN reporting nodes after moving a volume

If the volume that you moved contained LUNs and the volume is now on a different HA pair, you should remove all remote nodes from the Selective LUN Map (SLM) reporting-nodes list. The LUN map then contains only the owner node and its HA partner, which ensures that only optimized LUN paths are used.

About this task

This procedure is necessary only if you moved the volume from its HA pair to a different HA pair. If the volume is on a different node of the same HA pair, you can skip this procedure.

Steps

1. Remove all of the remote nodes from the reporting-nodes list by using the `lun mapping remove-`

`reporting-nodes` command with the `-remote-nodes` parameter.

```
cluster1::> lun mapping remove-reporting-nodes -vserver SVM1 -volume
vol1 -igroup ig1 -remote-nodes true
```

2. Verify that the LUN map contains only the owner node and its partner by using the `lun mapping show` command with the `-fields reporting-nodes` parameter.

```
cluster1::> lun mapping show -vserver SVM1 -volume vol1 -fields
reporting-nodes
vserver  path        igroup   reporting-nodes
-------- ----------- --------
-----------------------------------------------
SVM1     /vol/vol1   ig1      cluster1-3,cluster1-4
```

3. Remove stale device entries for the host operating system.
4. Rescan from the host to refresh the host's available paths.

   See your host documentation for specific steps to rescan your hosts.

Update NDMP backup after moving a volume

If the volume that you moved was previously backed up to tape using NDMP in a specific configuration, after moving the volume, you can perform one of the following actions to ensure the volume continues to be backed up successfully: create a baseline or migrate the backup LIF to the node containing the moved volume.

About this task

- This procedure is necessary only if the backup application does not support the cluster-aware backup (CAB) extension and the backup process uses node-scoped NDMP.

  If the backup application supports CAB and it is configured to use the SVM-scoped NDMP mode, you can skip this procedure.

- You must perform only one of these actions, not both.

Procedure

- From the backup application, create a new baseline.
- Identify the LIF that is configured for the backup process, and then migrate the LIF to the node where the volume now resides.

SNMP configuration

SNMP configuration overview

Using the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier, you can configure SNMP at the cluster management level; add communities, security users, and traphosts; and test the SNMP communication.

You should use these procedures if you want to configure SNMP access to a cluster in the following way:

- You are working with clusters running ONTAP 9.
- You want to use best practices, not explore every available option.

> There are a few steps in these procedures for which you must use the command-line interface.

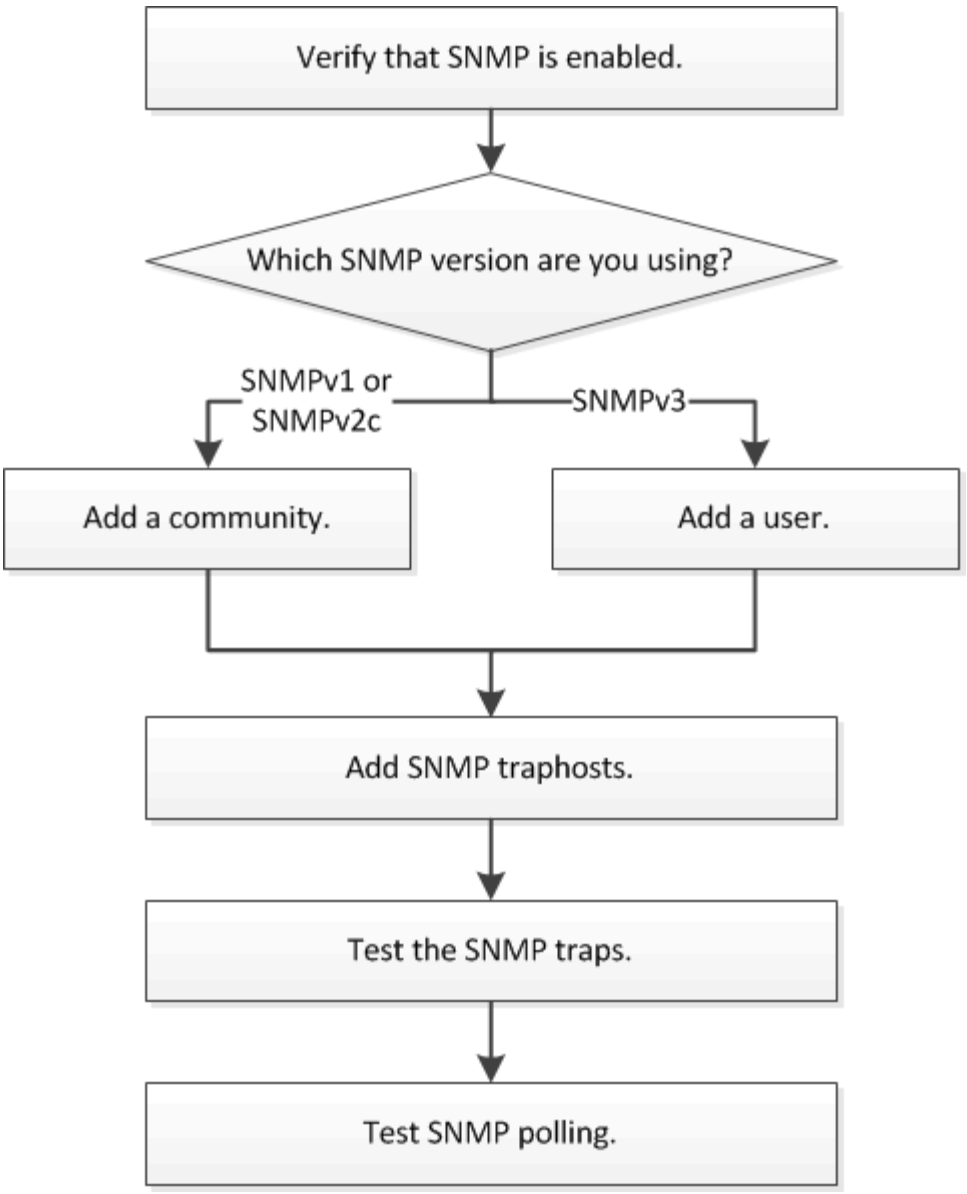
Other ways to do this in ONTAP

You can configure SNMP access to a cluster using for all ONTAP 9 versions. You should use the appropriate procedure for your version of ONTAP.

To perform these tasks with…	Refer to…
The redesigned System Manager (available with ONTAP 9.7 and later)	Manage SNMP on the cluster (cluster administrators only) > Overview
The ONTAP command-line interface (CLI)	Commands for managing SNMP

SNMP configuration workflow

Configuring SNMP involves enabling SNMP, optionally configuring an SNMPv1 or SNMPv2c community, optionally adding an SNMPv3 user, adding SNMP traphosts, and testing SNMP polling and traps.



Verify that SNMP is enabled

You can use the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier to verify whether SNMP is enabled on the cluster.

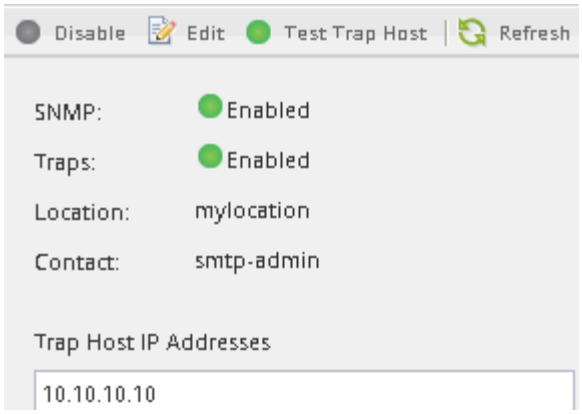
About this task

In all versions of ONTAP, SNMPv3 is enabled by default at the cluster level and SNMPv1 and SNMPv2c are disabled by default. SNMPv1 and SNMPv2c are enabled when you create an SNMP community.

SNMP is disabled by default on data LIFs. For information about enabling SNMP on data LIFs, see Network management.

Steps

1. Click the groove icon.
2. In the **Setup** pane, navigate to the **SNMP** window.



You can view the current SNMP status for the cluster.

If SNMP is not enabled, click **Enable**.

Add an SNMP community

You can use the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier to add a community to the administrative storage virtual machine (SVM) for a cluster that is running SNMPv1 or SNMPv2c. System Manager uses SNMP protocols SNMPv1 and SNMPv2c, and an SNMP community to discover storage systems.

About this task

This procedure is for adding an SNMP community to the administrative SVM for the cluster. The procedure for adding an SNMP community to a data SVM is described in Network management.

In new installations of ONTAP, SNMPv1 and SNMPv2c are disabled by default. SNMPv1 and SNMPv2c are enabled when you create an SNMP community.

Steps

1. In the SNMP window, click **Edit** to open the **Edit SNMP Settings** dialog box.
2. In the **General** tab, specify the contact personnel and location for the ONTAP system.
3. Click **Add**, enter a community name, and then click **OK** in the **Community Names** pane.

   You can add multiple community names. A community name can be a maximum of 32 characters and must not contain the following special characters: `, / : " ' |`

4. When you finish adding community names, click **OK** in the **Edit SNMP Settings** dialog box.

Add an SNMPv3 security user

You can use the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier to add an SNMPv3 user at the cluster level.

The SNMPv3 user can run SNMP utilities from the traphost (SNMP manager) using the authentication and privacy settings that you specify. SNMPv3 offers advanced security by using passphrases and encryption.

About this task

When you add an SNMPv3 user at the cluster level, that user can access the cluster through all the LIFs that

have the “mgmt” firewall policy applied.

Steps

1. In the SNMP window, click **Edit** to open the **Edit SNMP Settings** dialog box.
2. In the **SNMPv3** tab, click **Add** to open the **Add SNMPv3 User** dialog box.
3. Enter the following values:

   a. Enter an SNMPv3 user name.

      A security user name must not exceed 31 characters and must not contain the following special characters:

      `, / : " ' |`

   b. For Engine ID, select the default value `Local Engine ID`.

      The Engine ID is used to generate authentication and encryption keys for SNMPv3 messages.

   c. Select an authentication protocol and enter an authentication password.

      A password must contain a minimum of eight characters.

   d. Optional: Select a privacy protocol and enter a password for it.

4. Click **OK** in the **Add SNMPv3 User** dialog box.

   You can add multiple security user names, clicking **OK** after each addition. For example, if you use SNMP to monitor different applications that require different privileges, you might need to add an SNMPv3 user for each monitoring or management function.

5. When you finish adding user names, click **OK** in the **Edit SNMP Settings** dialog box.

Add an SNMP traphost

You can use the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier to add a traphost (SNMP manager) to receive SNMP notifications (SNMP trap protocol data units) when traps are generated in the cluster.

Before you begin

IPv6 must be enabled on the cluster if you configure SNMP traphosts that have IPv6 addresses.

About this task

SNMP and SNMP traps are enabled by default. The NetApp Technical Report TR-4220 on SNMP support contains lists of all default events that are supported by SNMP traps.

NetApp Technical Report 4220: SNMP Support in Data ONTAP

Steps

1. In the SNMP window, click **EDIT** to open the **Edit SNMP Settings** dialog box.
2. In the **Trap Hosts** tab, verify that the **Enable traps** check box is selected and click **Add**.
3. Enter the traphost IP address, and then click **OK** in the **Trap Hosts** pane.

The IP address of an SNMP traphost can be IPv4 or IPv6.

4. To add another traphost, repeat Step 2 and Step 3.
5. When you finish adding traphosts, click **OK** in the **Edit SNMP Settings** dialog box.

Test SNMP traps

You can use the ONTAP System Manager *classic* interface with ONTAP 9.7 or earlier to test SNMP traps. Because communication with a traphost is not automatically validated when you add it, you should verify that the SNMP traphost can correctly receive traps.

Steps

1. Navigate to the **SNMP** screen.
2. Click **Test Trap Host** to generate a trap from the cluster in which you added a traphost.
3. From the traphost location, verify that the trap was received.

   Use whatever software you ordinarily use to manage the SNMP traphost.

Test SNMP polling

After you configure SNMP, you should verify that you can poll the cluster.

About this task

To poll a cluster, you need to use a third-party command such as `snmpwalk`.

Steps

1. Send an SNMP command to poll the cluster from a different cluster.

   For systems running SNMPv1, use the CLI command `snmpwalk -v version -c community_stringip_address_or_host_name system` to discover the contents of the MIB (Management Information Base).

   In this example, the IP address of the cluster management LIF that you are polling is 10.11.12.123. The command displays the requested information from the MIB:

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

For systems running SNMPv2c, use the CLI command `snmpwalk -v version -c community_stringip_address_or_host_name system` to discover the contents of the MIB (Management Information Base).

In this example, the IP address of the cluster management LIF that you are polling is 10.11.12.123. The command displays the requested information from the MIB:

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

For systems running SNMPv3, use the CLI command `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` to discover the contents of the MIB (Management Information Base).

In this example, the IP address of the cluster management LIF that you are polling is 10.11.12.123. The command displays the requested information from the MIB:

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

Cluster management using System Manager 9.6 and 9.7

Cluster management using System Manager 9.6 and 9.7

Cluster Management Using OnCommand® System Manager

System Manager is an HTML5-based graphical management interface that enables you to manage storage systems and storage objects (such as disks, volumes, and aggregates) and perform common management tasks related to storage systems from a web browser. System Manager is included with ONTAP software as a web service, enabled by default, and accessible by using a browser. As a cluster administrator, you can use System Manager to administer the entire cluster and its resources.

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

System Manager enables you to perform many common tasks such as the following:

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

Dashboard window icons

You might see the following icons when viewing the dashboard for the storage system:

Icon	Name	Description
	Warning	There are minor issues, but none that require immediate attention.

Icon	Name	Description
	Error	Problems that might eventually result in downtime and therefore require attention.
	Critical	The storage system is not serving data or cannot be contacted. Immediate attention is required.
	Link arrow	If this is displayed next to a line item in a dashboard pane, clicking it links to another page from which you can get more information about the line item or make changes to the line item.

Set up the cluster by using ONTAP System Manager

Set up a cluster by using the template file in System Manager - ONTAP 9.7 and earlier

You can use the template file that is provided in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to set up a cluster by creating a cluster, setting up the node management and cluster management networks, and then setting up event notifications. (Beginning with ONTAP System Manager 9.6, AutoSupport is not supported.) You can download the template file in `.xlsx` format or `.csv` format.

About this task

- If the cluster supports ONTAP 9.1 or later, you can add only storage systems that are running ONTAP 9.1 or later.
- All fields are not automatically populated when you upload the file.

  You must manually enter the value of some fields such as password and cluster management port.

Steps

1. Open the web browser, and then enter the node management IP address that you have configured: `https://node-management-IP`
   - If you have set up the credentials for the cluster, the Login page is displayed.

     You must enter the credentials to log in.

   - If you have not set up the credentials for the cluster, the Guided Setup window is displayed.
2. Download the `.xlsx` template file or the `.csv` template file.
3. Provide all the required values in the template file, and save the file.

   - Do not edit any other column in the template other than Value.
   - Do not change the version of the template file.

4. Click **Browse**, and select the updated template file.
   - You can upload the template file only in the `.csv` format. If you have downloaded the template file in `.xlsx` format, you must save the file as a `.csv` file, and then upload the file.
   - You must ensure that the encoding used for this file is `UTF8`. If not, the values will not be read.
5. Click **Upload**.

   The details that you have provided in the template file are used to complete the cluster setup process.
6. Click the **Guided Setup** icon to view the details for the cluster.
7. Verify the details in the **Cluster** window, and then click **Submit and Continue**.

   You can edit the cluster details, if required.

   If you log in to the Cluster window for the second time, the **Feature Licenses** field is enabled by default. You can add new feature license keys or retain the pre-populated license keys.
8. Verify the details in the **Network** window, and then click **Submit and Continue**.

   You can edit the network details, if required.
9. Verify the details in the **Support** window, and then click **Submit and Continue**.

   You can edit the support details, if required.
10. Verify the details in the **Storage** window, and then create aggregates or exit the cluster setup:

If you want to…	Then…
Exit cluster setup without provisioning storage and creating an SVM	Click **Skip this step**.
Provision storage using aggregates and create an SVM	Click **Submit and Continue**.

    You can edit the support details, if required.
11. Verify the details in the **Create Storage Virtual Machine (SVM)** window, and then click **Submit and Continue**.

    You can edit the SVM name, select a different data protocol, and modify the Network Interface and Adapter Details, if required.
12. If you have clicked **Skip this step** on the **Storage** window, view the details on the **Summary** window, and then click **Manage your Cluster** to launch System Manager.
13. If you have clicked **Submit and Continue** on the **Storage** window, verify the details in the SVM window, and then click **Submit and Continue**.

    You can edit the SVM details, if required.
14. Verify all the details in the **Summary** window, and then click **Provision an Application** to provision storage for applications, or click **Manage your Cluster** to complete the cluster setup process and launch System

Manager, or click **Export Configuration** to download the configuration file.

Related information

System Manager Cluster Guided Setup Templates

Create a cluster with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create and set up a cluster in your data center.

About this task

If the cluster supports ONTAP 9.1 or later, you can add only those storage systems that are running ONTAP 9.1 or later.

Steps

1. Open the web browser, and then enter the node management IP address that you have configured: `https://node-management-IP`
   - If you have set up the credentials for the cluster, the Login page is displayed.

     You must enter the credentials to log in.
   - If you have not set up the credentials for the cluster, the Guided Setup window is displayed.

     Click the **Guided Setup** icon to set up a cluster.
2. In the **Cluster** page, enter a name for the cluster.

   If all the nodes are not discovered, click **Refresh**.

   The nodes in that cluster network are displayed in the Nodes field.
3. **Optional:** If desired, update the node names in the **Nodes** field.
4. Enter the password for the cluster.
5. **Optional:** Enter the feature license keys.
6. Click **Submit**.

What to do next

Enter the network details in the Network page to continue with the cluster setup.

Related information

Licenses window

Configuration Updates window

Set up a network with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage your cluster, nodes, and Service Processors by setting up a network. You can

also set up DNS and NTP details by using the network window.

Before you begin

You must have set up the cluster.

About this task

- Only those nodes that are up and running are listed for cluster creation.

  You can create LIFs for those nodes.

- You can disable IP address range and enter individual IP addresses for cluster management, node management, and Service Processor management networks.

Set up a network when an IP address range is enabled

You can set up a network by enabling an IP address range. The IP address range enables you to enter IP addresses that are in the same netmask range or in the different netmask range.

Steps

1. Enter a range of IP addresses in the **IP Address Range** field, and then click **Apply**.

Option	Description
You have a range of IP addresses in the same netmask	Enter the IP address range, and then click **Apply**. IP addresses are applied to cluster management, node management, and Service Processor management networks sequentially.
You have a range of IP addresses in different netmasks	Enter each IP address range on a separate line, and then click **Apply**. The first IP address applied to cluster management and other IP addresses are applied to node management and Service Processor management networks sequentially.

> After entering the IP address range for cluster management, node management, and Service Processor management, you must not manually modify the IP address values in these fields. You must ensure that all the IP addresses are IPv4 addresses.

2. Enter the netmask and gateway details.
3. Select the port for cluster management in the **Port** field.
4. If the **Port** field in the node management is not populated with **e0M**, enter the port details.

> By default, the Port field displays e0M.

5. For Service Processor management, if you are overriding the default values, ensure that you have entered the mandatory gateway details.
6. If you have enabled the **DNS Details** field, enter the DNS server details.

7. If you have enabled the **NTP Details** field, enter the NTP server details.

   Providing alternative NTP server details is optional.

8. Click **Submit**.

What to do next

Enter event notifications in the Support page to continue with the cluster setup.

Set up a network when an IP address range is disabled

You can set up a network by disabling an IP address range and entering individual IP addresses for cluster management, node management, and service provider networks.

About this task

In the Networks page, if the **IP Address Range** is disabled, enter individual IP addresses for cluster management, node management, and service processor networks.

Steps

1. Enter the cluster management IP address in the **Cluster Management IP Address** field.
2. Enter the netmask details for cluster management.
3. **Optional:** Enter the gateway details for cluster management.
4. Select the port for cluster management in the **Port** field.
5. If you want to provide netmask and gateway details to manage your nodes, clear the **Retain Netmask and Gateway configuration of the Cluster Management** check box, and then enter the netmask and gateway details.
6. Enter the node management IP addresses in the **Node Management** field.
7. If the **Port** field in the node management is not populated with **e0M**, enter the port details.

   By default, the Port field displays e0M.

8. Enter the Service Processor management netmask and gateway details.
9. Enter the Service Processor IP management addresses in the **Service Processor Management** field.
10. If you have enabled the **DNS Details** field, enter the DNS server details.
11. If you have enabled the **NTP Details** field, enter the NTP server details.

    Providing alternative NTP server details is optional.

12. Click **Submit**.

What to do next

Enter event notifications in the Support page to continue with the cluster setup.

Related information

What is a Service Processor and how do I use it?

How to configure and troubleshoot NTP on clustered Data ONTAP 8.2 and later using CLI

ONTAP 9 Documentation Center

Network window

Configuration Updates window

Date and Time window

Service Processors window

Set up a support page with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to set up a support page. Setting up the support page completes the cluster setup, and involves setting up event notifications, and for single-node clusters, configuring system backup.

Before you begin

You must have set up the cluster and network.

Steps

1. Set up the event notifications by using the mailhost, or SNMP trap host, or Syslog server.

   You must set up at least one event notification system.

2. If you have a single-node cluster, configure a system backup on an FTP server or on an HTTP server.

   System backup is applicable only for single-node clusters.

3. Click **Submit and continue**.

What to do next

View the storage recommendations and create SVMs to continue with the cluster setup.

Review storage recommendations with System Manager - ONTAP 9.7 and earlier

You can review the storage recommendations that are provided for creating aggregates by using the storage window in ONTAP System Manager classic (available in ONTAP 9.7 and earlier).

Before you begin

You must have set up the cluster, network, and the support details.

About this task

You can create data aggregates per the storage recommendations or you can skip this step and create data aggregates at a later time using System Manager.

Procedure

- To create data aggregates as per the storage recommendations, click **Submit and Continue**.
- To create data aggregates at a later time using System Manager, click **Skip this step**.

What to do next

If you opted to create aggregates per the storage recommendations, you must create a storage virtual machine (SVM) to continue with the cluster setup.

Create an SVM with System Manager - ONTAP 9.7 and earlier

In ONTAP System Manager classic (available in ONTAP 9.7 and earlier), you can use the Storage Virtual Machine (SVM) window to create fully configured SVMs. The SVMs serve data after storage objects are created on these SVMs.

Before you begin

- You must have created an aggregate and the aggregate must be online.
- You must have ensured that the aggregate has sufficient space for the SVM root volume.

Steps

1. Enter a name for the SVM.
2. Select data protocols for the SVM:

If you want to…	Then…
Enable CIFS protocol by configuring the CIFS server using an Active Directory	a. Select the **Active Directory** box. b. Enter the Active Directory administrator name. c. Enter the Active Directory administrator password. d. Enter a name for the CIFS server. e. Enter a name for the Active Directory domain. f. Depending on your requirements, select the **One data LIF on this SVM** or **One data LIF per node on this SVM** box. g. Provide data LIF details such as IP address, netmask, gateway, and port. h. Provide DNS details.

If you want to…	Then…
Enable CIFS protocol by configuring the CIFS server using a workgroup	a. Select the **Workgroup** box. b. Enter a name for the workgroup. c. Enter a name for the CIFS server. d. Depending on your requirements, select the **One data LIF on this SVM** or **One data LIF per node on this SVM** check box. e. Provide data LIF details such as IP address, netmask, gateway, and port.
Enable NFS protocol	a. Select the **NFS** box. b. Depending on your requirements, select the **One data LIF on this SVM** or **One data LIF per node on this SVM** check box. c. Provide data LIF details such as IP address, netmask, gateway, and port.
Enable iSCSI protocol	a. Select the **iSCSI** box. b. Provide data LIF details such as IP address, netmask, gateway, and port.
Enable FC/FCoE protocol	a. Select the **FC/FCoE** box. b. Select the FC/FCoE ports for FC or FCoE protocols. Each node must have at least one correctly configured port for each protocol (FC and FCoE).
Enable NVMe protocol	a. Select the **NVMe** box. b. Select the NVMe ports for NVMe protocols. At least one NVMe capable adapter must be available in one of the nodes to configure NVMe. Also, Beginning with ONTAP 9.5, at least one NVMe LIF must be configured for each node of a HA pair associated with the SVM. You can create a maximum of two NVMe LIFs for each node in the pair.

3. **Optional:** Click the **Advanced Options** icon and provide details to configure advanced options such as the default language, security style, CIFS server details, and NFS details.

4. Click **Submit and Continue** to create the SVM.

What to do next

If you have clicked **Submit and Continue**, you must verify the details that you have provided in the Summary window, and then click **Manage your Cluster** to launch System Manager, or click **Provision an Application** to provision storage applications, or click **Export Configuration** to download the configuration file.

Access a cluster with a browser-based graphic interface in System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) if you prefer to use a graphic interface instead of the command-line interface for accessing and managing a cluster. ONTAP System Manager is included with ONTAP as a web service, is enabled by default, and is accessible by using a browser.

Before you begin

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

About this task

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

Steps

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

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

     Only HTTPS is supported for browser access of ONTAP System Manager.

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

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

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

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

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

Configure System Manager options - ONTAP 9.7 and earlier

You can enable logging and specify the inactivity timeout value for ONTAP System

Manager classic (available in ONTAP 9.7 or earlier).

About this task

You can configure the options from the System Manager login window. However, you must log in to the application to specify the inactivity timeout value.

Steps

1. Click ⚙.
2. In the **Setup** pane, click **General**.
3. Specify a log level.
4. Specify the inactivity timeout value in minutes.

   ⓘ This option is not available if you have enabled Security Assertion Markup Language (SAML) authentication.

5. Click **OK**.

View System Manager log files - ONTAP 9.7 and earlier

If you encounter any issues when using ONTAP System Manager classic (available in ONTAP 9.7 and earlier), you can send the log files to help troubleshoot the issues if directed by NetApp Support. The System Manager log files are located in the `mlog` directory along with the ONTAP log files.

Steps

1. Identify the node that hosts the cluster management LIF.
2. Enter the following URL in a web browser: `https://cluster-mgmt-LIF/spi`

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

3. Type your cluster administrator credentials, and then click **OK**.
4. In the **Data ONTAP - Root Volume File Access** window, click the **logs** link for the node that hosts the cluster management LIF.
5. Navigate to the `mlog` directory to access the System Manager log files.

   You might require the following log files, depending on the type of issue that you encountered:

   - `sysmgr.log`

     This file contains the latest logs for System Manager.

   - `mgwd.log`
   - `php.log`
   - `apache_access.log`
   - `messages.log`

How system logging works

System logging is an essential tool for application troubleshooting. You should enable system logging so that if there is a problem with an application, the problem can be located. You can enable System Manager logging at runtime without modifying the application binary.

Log output can be voluminous and therefore can become difficult to manage. System Manager enables you to refine the logging output by selecting which type of log statements are output. By default, system logging is set to INFO. You can choose one of the following log levels:

- OFF
- ERROR
- WARN
- INFO
- DEBUG

These levels function hierarchically. A log level set to OFF indicates no logging of messages.

Set up the cluster

Set up the cluster with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manger classic (available in ONTAP 9.7 and earlier) to set up the cluster.

Setting up the cluster involves gathering the configuration information, creating cluster-management and node-management interfaces, adding licenses, setting up the cluster time, and monitoring HA pairs.

Update the cluster name

You can use System Manager to modify the name of a cluster when required.

Steps

1. Click **Configuration** > **Cluster** > **Configuration Updates**.
2. In the **Cluster Details** pane, click **Update Cluster Name**.
3. In the **Update Cluster Name** dialog box, specify a new name for the cluster, and then click **Submit**.

Change the cluster password

You can use System Manager to reset the password of a cluster.

Steps

1. Click **Configuration** > **Cluster** > **Configuration Updates**.
2. In the **Cluster Details** pane, click **Change Password**.
3. In the **Change Password** dialog box, specify a new password, confirm the new password, and then click **Change**.

Edit DNS configurations

You can use System Manager to add host information to centrally manage DNS configurations. You can modify

the DNS details when you want to change the domain names or IP addresses.

Steps

1. Click **Configuration** > **Cluster** > **Configuration Updates**.
2. In the **Cluster Details** pane, click **Edit DNS Configuration**.
3. In the **DNS Domains** area, add or modify the DNS domain names.
4. In the **Name Servers** area, add or modify the IP addresses.
5. Click **OK**.

Create a cluster management logical interface

You can use System Manager to create a cluster management logical interface (LIF) to provide a single management interface for a cluster. You can use this LIF to manage all of the activities of the cluster.

Steps

1. Click **Configuration** > **Cluster** > **Configuration Updates**.
2. In the **Cluster Details** pane, click **Create Cluster-management LIF**.
3. In the **Create Cluster-Management LIF** dialog box, specify a name for the cluster management LIF.
4. Assign an IP address to the cluster management LIF:

If you want to…	Then…
Specify the IP address by using a subnet	a. Select **Using a subnet**. b. In the Add Details dialog box, select the subnet from which the IP address should be assigned. For an intercluster LIF, only the subnets that are associated with the selected IPspace are displayed. c. If you want to assign a specific IP address to the LIF, select **Use a specific IP address**, and then type the IP address. The IP address that you specify is added to the subnet if the IP address is not already present in the subnet range. d. Click **OK**.

If you want to…	Then…
Specify the IP address manually without using a subnet	a. Select **Without a subnet**. b. In the Add Details dialog box, perform the following steps: i. Specify the IP address and the network mask or prefix. ii. Optional: Specify the gateway. iii. If you do not want to use the default value for the Destination field, specify a new destination value. If you do not specify a value, the Destination field is populated with the default value based on the family of the IP address. If a route does not exist, a new route is automatically created based on the gateway and destination. c. Click **OK**.

5. Select the required ports from the **Port details** area.
6. Click **Create**.

Edit the node name

You can use System Manager to modify the name of a node when required.

Steps

1. Click **Configuration** > **Cluster** > **Configuration Updates**.
2. In the **Nodes** tab, select the node that you want to rename, and then click **Edit Node Name**.
3. In the **Edit Node Name** dialog box, type the new name for the node, and then click **Submit**.

Create a node management logical interface

You can use System Manager to create a dedicated node management logical interface (LIF) for managing a particular node in a cluster. You can use this LIF to manage the system maintenance activities of the node.

Steps

1. Click **Configuration** > **Cluster** > **Configuration Updates**.
2. In the **Nodes** tab, select the node for which you want to create a node management LIF, and then click **Create Node-Management LIF**.
3. In the **Create Node-Management LIF** dialog box, specify a name for the node management LIF.
4. Assign the IP address to the node management LIF:

If you want to…	Then…
Specify the IP address by using a subnet	a. Select **Using a subnet**. b. In the Add Details dialog box, select the subnet from which the IP address should be assigned. For an intercluster LIF, only the subnets that are associated with the selected IPspace are displayed. c. If you want to assign a specific IP address to the LIF, select **Use a specific IP address**, and then type the IP address. The IP address that you specify is added to the subnet if the IP address is not already present in the subnet range. d. Click **OK**.
Specify the IP address manually without using a subnet	a. Select **Without a subnet**. b. In the Add Details dialog box, perform the following steps: i. Specify the IP address and the network mask or prefix. ii. Optional: Specify the gateway. iii. If you do not want to use the default value for the Destination field, specify a new destination value. If you do not specify a value, the Destination field is populated with the default value based on the family of the IP address. If a route does not exist, a new route is automatically created based on the gateway and destination. c. Click **OK**.

5. Select the required ports from the **Ports details** area.
6. Click **Create**.

What to do next

If you want to delete an existing node management LIF, you must use the command-line interface (CLI).

Edit AutoSupport settings

You can use System Manager to modify your AutoSupport settings to specify an email address from which

email notifications are sent and to add multiple email host names.

Steps

1. Click ⚙ > **AutoSupport**.
2. Select the node for which you want to modify AutoSupport settings, and then click **Edit**.
3. In the **Email Recipient** tab, type the email address from which email notifications are sent, specify the email recipients and the message content for each email recipient, and then add the mail hosts.

   You can add up to five email addresses for each host.
4. In the **Others** tab, select a transport protocol for delivering the email messages, and then specify the HTTP or HTTPS proxy server details.
5. Click **OK**.

Add licenses with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to add the software license if the software was not installed at the factory or if you want to add additional software licenses.

If your storage system software was installed at the factory, System Manager automatically adds the software to its list of licenses.

Before you begin

The software license code for the specific ONTAP service must be available.

About this task

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

  For more information, see Enable new features by adding license keys

  For information about managing licenses, see Manage licenses overview (cluster administrators only)
- When you add a new license in a MetroCluster configuration, it is a best practice to add the license on the surviving site cluster as well.
- You cannot use System Manager to add the Cloud Volumes ONTAP license.

  The Cloud Volumes ONTAP license is not listed in the license page. System Manager does not raise any alert about the entitlement risk status of the Cloud Volumes ONTAP license.
- You can upload only capacity-based licenses.

  The capacity-based licenses are of “json” type.

Steps

1. Click **Configuration** > **Cluster** > **Licenses**.
2. Click **Add**.

3. In the **Add License** dialog box, perform the appropriate steps:

If you want to…	Do this…
Add a license for a specific ONTAP service	a. Enter the software license key. You can add multiple licenses by entering the software license keys separated by commas. b. Click **Add**.
Add a capacity based license	a. Click Browse, and then select the capacity based license file. b. Click **Add**.
Add a license for a specific ONTAP service and add a capacity-based license	a. Enter the software license key. You can add multiple licenses by entering the software license keys separated by commas. b. Click Browse, and then select the capacity based license file. c. Click **Add**.

   The new license is added.

   The Add License Status dialog box displays the list of licenses that were added successfully. The dialog box also displays the license keys of the licenses that were not added and the reason why the licenses were not added.

4. Click **Close**.

Results

The software license is added to your storage system and is displayed in the list of licenses in the Licenses window.

Related information

Licenses window

Set the time zone for a cluster with System Manager - ONTAP 9.7 and earlier

You can manually set or modify the time zone for a cluster by using the Edit Date and Time dialog box in ONTAP System Manager classic (available in ONTAP 9.7 and earlier). You can also add time servers to the cluster.

About this task

Network Time Protocol (NTP) is always enabled on a cluster. You can disable NTP, but it is not recommended.

You can add the IP addresses of the NTP server at your site. This server is used to synchronize the time across the cluster.

You can specify either an IPv4 address or an IPv6 address for the time server.

Steps

1. Click .
2. In the **Setup** panel, click **Date and Time**.
3. Click **Edit**.
4. In the **Edit Date and Time** dialog box, select the time zone.
5. Specify the IP address of the time servers, and then click **Add**.
6. Click **OK**.
7. Verify the changes that you made to the time settings in the **Date and Time** window.

Related information

Date and Time window

Creating a Kerberos realm configuration

Monitor HA pairs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to monitor the node status and interconnect status of all of the high-availability (HA) pairs in a cluster. You can also verify whether takeover or giveback is enabled or has occurred, and view the reasons why takeover or giveback is not currently possible.

Steps

1. Click **Configuration** > **Cluster** > **High Availability**.
2. In the **High Availability** window, click the HA pair image to view details such as the cluster HA status, node status, interconnect status, and hardware model of each node.

   If the cluster management LIF or the data LIFs of a node are not in their home node, a warning message is displayed indicating that the node has some LIFs that are not in the home node.

Related information

High Availability window

Set up the network with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to set up the network. Setting up the network consists of creating IPspaces, a broadcast domain, and subnets.

Create IPspaces

You can create an IPspace by using System Manager to configure a single ONTAP cluster for client access from more than one administratively separate network domain, even when the clients use the same IP address subnet range. This enables you to separate client traffic for privacy and security.

About this task

All of the IPspace names must be unique within a cluster and must not consist of names that are reserved by the system, such as “local” or “localhost.”

Steps

1. Click the **Network** tab.
2. In the **IPspaces** tab, click **Create**.
3. In the **Create IPspaces** dialog box, specify a name for the IPspace that you want to create.
4. Click **Create**.

Create broadcast domains

You can create a broadcast domain by using System Manager to provide a logical division of a computer network. In a broadcast domain, all associated nodes can be reached through broadcast at the datalink layer

Steps

1. Click the **Network** tab.
2. In the **Broadcast Domains** tab, click **Create**.
3. In the **Create Broadcast Domain** dialog box, specify the name, MTU size, IPspace, and ports for the broadcast domain that you want to create.
4. Click **Create**.

Create subnets

You can create a subnet by using System Manager to provide a logical subdivision of an IP network to pre-allocate the IP addresses. A subnet enables you to create interfaces more easily by specifying a subnet instead of an IP address and network mask values for each new interface.

Before you begin

You must have created the broadcast domain on which the subnet is used.

About this task

If you specify a gateway when creating a subnet, a default route to the gateway is added automatically to the SVM when a LIF is created using that subnet.

Steps

1. Click the **Network** tab.
2. In the **Subnets** tab, click **Create**.
3. In the **Create Subnet** dialog box, specify subnet details, such as the name, subnet IP address or subnet mask, range of IP addresses, gateway address, and broadcast domain.

   You can specify the IP addresses as a range, as comma-separated multiple addresses, or as a mix of both.
4. Click **Create**.

Related information

Network window

Set up physical storage

Assign disks to nodes with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to assign ownership of an unassigned disk to a specific node to increase the capacity of an aggregate or storage pool.

About this task

- You can assign disks if the following conditions are true:
  - The container type of the selected disks must be “unassigned”.
  - The disks must be connected to nodes in an HA pair.
  - The disks must be visible to the node.
- For MetroCluster configurations, you cannot use System Manager to assign disks.

  You must use the command-line interface instead.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Disks**.
2. In the **Disks** window, select the **Inventory** tab.
3. Select the disks that you want to assign, and then click **Assign**.
4. In the **Assign Disks** dialog box, select the node to which you want to assign the disks.
5. Click **Assign**.

Zero spare disks with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to erase all the data and to format the spare disks by writing zeros to the disk. These disks can then be used in new aggregates.

About this task

When you zero the spare disks, all the spares in the cluster, including array LUNs, are zeroed. You can zero the spare disks for a specific node or for the entire cluster.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Disks**.
2. In the **Disks** window, select the **Inventory** tab.
3. Click **Zero Spares**.
4. In the **Zero Spares** dialog box, select a node or “All nodes” from which you want to zero the disks.
5. Select the **Zero all non-zeroed spares** check box to confirm the zeroing operation.
6. Click **Zero Spares**.

Related information

Storage recommendations for creating aggregates

Provision storage through aggregates with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create an aggregate based on storage recommendations or manually depending on your requirement. You can create Flash Pool aggregates, SnapLock aggregates, and a FabricPool-enabled aggregates to provide storage for one or more volumes by using System Manager.

Before you begin

You must have enough spare disks to create an aggregate.

About this task

You cannot perform the following actions by using System Manager:

- Combine disks of different sizes even if there are enough spare disks of different sizes.

  You can initially create an aggregate with disks of the same size and then add disks of a different size later.

- Combine disks with different checksum types.

  You can initially create an aggregate with a single checksum type and add storage of a different checksum type later.

Create an aggregate based on storage recommendations

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create an aggregate based on storage recommendations. System Manager analyzes the configuration of your storage system and provides storage recommendations such as the number of aggregates that will be created, the available nodes, and the available spare disks.

About this task

- You cannot create an aggregate based on storage recommendations in Cloud Volumes ONTAP, ONTAP Select, and MetroCluster configurations.
- Errors, if any, are displayed on the screen.

  You can fix these errors and then create an aggregate based on the storage recommendations, or you can create an aggregate manually.

Steps

1. Create an aggregate by using one of the following methods:
   - Click **Applications & Tiers** > **Storage Tiers** > **Add Aggregate**.
   - Click **Storage** > **Aggregate & Disks** > **Aggregates** > **Create**.
2. Review the storage recommendations, and then click **Submit**.

   The Information dialog box displays the status of the aggregates.

3. Click **Run in Background** to navigate to the **Aggregates** window.
4. Click **Refresh** to view the aggregates that are created.

Manually create an aggregate

You can manually create an aggregate that consists of only HDDs or only SSDs by using ONTAP System Manager classic (available in ONTAP 9.7 and earlier).

Before you begin

All of the disks must be of the same size.

About this task

- If you are creating an aggregate on a four-node cluster in ONTAP Select, the mirrored aggregate option is selected by default.
- Beginning with ONTAP 9.0, you can create aggregates with disk size equal to or larger than 10 TB.
- If the disk type of the aggregate disks is FSAS or MSATA, and the disk size is equal to or larger than 10 TB, then RAID-TEC is the only available RAID type.

Steps

1. Create an aggregate by using one of the following methods:
   - Click **Applications & Tiers** > **Storage Tiers** > **Add Aggregate**.
   - Click **Storage** > **Aggregate & Disks** > **Aggregates** > **Create**.
2. Enable the **Manually Create Aggregate** option to create an aggregate.
3. To create an aggregate:
   a. Specify the name of the aggregate, the disk type, and the number of disks or partitions to include in the aggregate.

      The minimum hot spare rule is applied to the disk group that has the largest disk size.

   b. **Optional:** Modify the RAID configuration of the aggregate:
      i. Click **Change**.
      ii. In the **Change RAID Configuration** dialog box, specify the RAID type and the RAID group size.

         Shared disks support two RAID types: RAID DP and RAID-TEC.

      iii. Click **Save**.
   c. If you want to mirror the aggregate, select the **Mirror this aggregate** check box.

      For MetroCluster configurations, creating unmirrored aggregates is restricted. Therefore, the mirroring option is enabled by default for MetroCluster configurations.
4. Click **Create**.

Results

The aggregate is created with the specified configuration, and is added to the list of aggregates in the Aggregates window.

Create a Flash Pool aggregate manually

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create a Flash Pool aggregate manually, or to convert an existing HDD aggregate to a Flash Pool aggregate by adding SSDs. When you create a new HDD aggregate, you can provision an SSD cache to it and create a Flash Pool aggregate.

Before you begin

- You must be aware of the platform-specific best practices and workload-specific best practices for the Flash Pool aggregate SSD tier size and configuration.
- All of the HDDs must be in the zeroed state.
- If you want to add SSDs to the aggregate, all of the existing SSDs and dedicated SSDs must be of the same size.

About this task

- You cannot use partitioned SSDs while creating a Flash Pool aggregate.
- You cannot mirror the aggregates if the cache source is storage pools.
- Beginning with ONTAP 9.0, you can create aggregates with disk size equal to or larger than 10 TB.
- If the disk type of the aggregate disks is FSAS or MSATA, and the disk size is equal to or larger than 10 TB, then RAID-TEC is the only option available for RAID type.

Steps

1. Create an aggregate by using one of the following methods:
   - Click **Applications & Tiers** > **Storage Tiers** > **Add Aggregate**.
   - Click **Storage** > **Aggregate & Disks** > **Aggregates** > **Create**.
2. Enable the **Manually Create Aggregate** option to create an aggregate.
3. In the **Create Aggregate** window, specify the name of the aggregate, the disk type, and the number of disks or partitions to include for the HDDs in the aggregate.
4. If you want to mirror the aggregate, select the **Mirror this aggregate** check box.

   For MetroCluster configurations, creating unmirrored aggregates is restricted. Therefore, the mirroring option is enabled by default for MetroCluster configurations.

5. Click **Use Flash Pool Cache with this aggregate**.
6. Specify the cache source:

If you want to select the cache source as…	Then…
Storage pools	a. Select **Storage pools** as the Cache Source. b. Select the storage pool from which the cache can be obtained, and then specify the cache size. c. Modify the RAID type, if required.

If you want to select the cache source as…	Then…
Dedicated SSDs	a. Select **Dedicated SSDs** as the Cache Source. b. Select the SSD size and the number of SSDs to include in the aggregate. c. Modify the RAID configuration, if required: i. Click **Change**. ii. In the Change RAID Configuration dialog box, specify the RAID type and the RAID group size. iii. Click **Save**.

7. Click **Create**.

Results

The Flash Pool aggregate is created with the specified configuration, and is added to the list of aggregates in the Aggregates window.

Create a SnapLock aggregate manually

You can use System Manager classic (available in ONTAP 9.7 and earlier) to create a SnapLock Compliance aggregate or a SnapLock Enterprise aggregate manually. You can create SnapLock volumes on these aggregates, which provide “write once, read many” (WORM) capabilities.

Before you begin

The SnapLock license must have been added.

About this task

- In MetroCluster configurations, you can create only SnapLock Enterprise aggregates.
- For array LUNs, only SnapLock Enterprise aggregates are supported.
- Beginning with ONTAP 9.0, you can create aggregates with disk size equal to or larger than 10 TB.
- If the disk type of the aggregate disks is FSAS or MSATA, and the disk size is equal to or larger than 10 TB, then RAID-TEC is the only option available for RAID type.
- Beginning with ONTAP 9.1, you can create a SnapLock aggregate on an AFF platform.

Steps

1. Create a SnapLock aggregate by using one of the following methods:
   - Click **Applications & Tiers** > **Storage Tiers** > **Add Aggregate**.
   - Click **Storage** > **Aggregate & Disks** > **Aggregates** > **Create**.
2. Enable the **Manually Create Aggregate** option to create an aggregate.
3. To create a SnapLock aggregate:
   a. Specify the name of the aggregate, the disk type, and the number of disks or partitions to include in the aggregate.

      You cannot change the name of a SnapLock Compliance aggregate after you create the aggregate.

The minimum hot spare rule is applied to the disk group that has the largest disk size.

b. **Optional:** Modify the RAID configuration of the aggregate:
   i. Click **Change**.
   ii. In the Change RAID Configuration dialog box, specify the RAID type and the RAID group size.

   Shared disks support two RAID types: RAID-DP and RAID-TEC.

   iii. Click **Save**.
c. Specify the SnapLock type.
d. If you have not initialized the system ComplianceClock, select the **Initialize ComplianceClock** check box.

   This option is not displayed if the ComplianceClock is already initialized on the node.

   > You must ensure that the current system time is correct. The ComplianceClock is set based on the system clock. Once the ComplianceClock is set, you cannot modify or stop the ComplianceClock.

e. **Optional:** If you want to mirror the aggregate, select the **Mirror this aggregate** check box.

   For MetroCluster configurations, creating unmirrored aggregates is restricted. Therefore, the mirroring option is enabled by default for MetroCluster configurations.

   By default, the mirroring option is disabled for SnapLock Compliance aggregates.

4. Click **Create**.

Create a FabricPool-enabled aggregate manually

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create a FabricPool-enabled aggregate manually or to convert an existing SSD aggregate to a FabricPool-enabled aggregate by attaching a cloud tier to the SSD aggregate.

Before you begin

- You must have created a cloud tier and attached it to the cluster in which the SSD aggregate resides.
- An on-premises cloud tier must have been created.
- A dedicated network connection must exist between the cloud tier and the aggregate.

About this task

The following object stores can be used as cloud tiers:

- StorageGRID
- Alibaba Cloud (Beginning with System Manager 9.6)
- Amazon Web Services (AWS) Simple Storage Service (S3)
- Amazon Web Services (AWS) Commercial Cloud Service (C2S)
- Microsoft Azure Blob storage
- IBM Cloud
- Google Cloud

- Azure Stack, which is an on-premises Azure services, is not supported.
- If you want to use any object store as a cloud tier, other than StorageGRID, you must have the FabricPool capacity license.

Steps

1. Create a FabricPool-enabled aggregate by using one of the following methods:
   - Click **Applications & Tiers** > **Storage Tiers** > **Add Aggregate**.
   - Click **Storage** > **Aggregate & Disks** > **Aggregates** > **Create**.
2. Enable the **Manually Create Aggregate** option to create an aggregate.
3. Create a FabricPool-enabled aggregate:
   a. Specify the name of the aggregate, the disk type, and the number of disks or partitions to include in the aggregate.

      Only all flash (all SSD) aggregates support FabricPool-enabled aggregates.

      The minimum hot spare rule is applied to the disk group that has the largest disk size.

   b. **Optional:** Modify the RAID configuration of the aggregate:
      i. Click **Change**.
      ii. In the Change RAID Configuration dialog box, specify the RAID type and the RAID group size.

      Shared disks support two RAID types: RAID-DP and RAID-TEC.

      iii. Click **Save**.
4. Select the **FabricPool** checkbox, and then select a cloud tier from the list.
5. Click **Create**.

Related information

NetApp Technical Report 4070: Flash Pool Design and Implementation

Create SVMs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create fully configured storage virtual machines (SVMs) that can serve data immediately. A cluster can have one or more SVMs.

Before you begin

- The cluster must have at least one non-root aggregate in the online state.
- The aggregate must have sufficient space for the SVM root volume.
- You must have synchronized the time across the cluster by configuring and enabling NTP to prevent CIFS creation and authentication failures.
- The protocols that you want to configure on the SVM must be licensed.
- You must have configured the CIFS protocol for secure DDNS to work.

About this task

- While creating SVMs, you can perform the following tasks:
  - Create and fully configure SVMs.
  - Configure the volume type that is allowed on SVMs.
  - Create and configure SVMs with minimal network configuration.
  - Delegate the administration to SVM administrators.
- To name the SVM, you can use alphanumeric characters and the following special characters: “.” (period), “-” (hyphen), and “_” (underscore).

  The SVM name should start with an alphabet or “_” (underscore) and must not contain more than 47 characters.

  You should use unique fully qualified domain names (FQDNs) for the SVM name such as vs0.example.com.

- You can establish SnapMirror relationships only between volumes that have the same language settings.

  The language of the SVM determines the character set that is used to display file names and data for all NAS volumes in the SVM.

- You cannot use a SnapLock aggregate as the root aggregate of SVMs.

Steps

1. Click **Storage** > **SVMs**.
2. Click **Create**.
3. In the **Storage Virtual Machine (SVM) Setup** window, specify the following details:
   - SVM name
   - IPspace allocated to the SVM
   - Volume type allowed
   - Protocols allowed
   - SVM language
   - Security style of the root volume
   - Root aggregate

     The default language setting for any SVM is C.UTF-8.

     By default, the aggregate with the maximum free space is selected as the container for the root volume of the SVM. Based on the protocols selected, the default security style and the root aggregate are selected.

     The security style is set to NTFS if you select CIFS protocol or a combination of CIFS protocol with the other protocols. The security style is set to UNIX if you select NFS, iSCSI, NVMe, or FC/FCoE, or a combination of these protocols.

     NVMe does not allow the combination of protocols.

   In a MetroCluster configuration, only the aggregates that are contained in the cluster are displayed.

4. Specify the DNS domain names and the name server IP addresses to configure the DNS services.

   The default values are selected from the existing SVM configurations.

5. **Optional:** When configuring a data LIF to access data using a protocol, specify the target alias, subnets, and the number of LIFs per node.

   You can select the **Review or Modify LIFs configuration (Advanced Settings)** checkbox to modify the number of portsets in the LIF.

   You can edit the details of the portset in a particular node by selecting the node from the nodes list in the details area.

6. **Optional:** Enable host-side applications such as SnapDrive and SnapManager for the SVM administrator by providing the SVM credentials.
7. **Optional:** For protocols other than NVMe, create a new LIF for SVM management by clicking **Create a new LIF for SVM management**, and then specify the portsets and the IP address with or without a subnet for the new management LIF.

   For CIFS and NFS protocols, data LIFs have management access by default. You must create a new management LIF only if required. For iSCSI and FC, a SVM management LIF is required because data protocols and management protocols cannot share the same LIF.

8. **Optional:** For NVMe protocol, Beginning with ONTAP 9.5, configure a minimum of one LIF for each node on the second page of the SVM Setup wizard: **Configure NVMe Protocol.**

   You must configure at least one LIF for each node in the HA pair. You can also specify two LIFs per node. Click the settings icon to toggle between one or two LIFs configurations.

9. Click **Submit & Continue**.

   The SVM is created with the specified configuration.

Results

The SVM that you created is started automatically. The root volume name is automatically generated as `SVM name_root`. By default, the `vsadmin` user account is created and is in the locked state.

What to do next

You must configure at least one protocol on the SVM to allow data access.

Configure CIFS and NFS protocols on SVMs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to configure CIFS and NFS protocols on a storage virtual machine (SVM) to provide file-level data access for NAS clients. To enable the CIFS protocol, you must create data LIFs and the CIFS server. To enable the NFS protocol, you can specify the NIS details and the data LIFs.

Before you begin

- The protocols that you want to configure or enable on the SVM must be licensed.

If the protocol that you want to configure is not enabled on the SVM, you can use the Edit Storage Virtual Machine window to enable the protocol for the SVM.

- You must have the Active Directory, organizational unit, and administrative account credentials for configuring the CIFS protocol.

About this task

SnapLock aggregates are not considered for automatically creating volumes.

Steps

1. If you have not configured the protocols while creating the SVM, click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click the protocol that you want to configure.
4. In the **Data LIF Configuration** section, if you want to retain the same data LIF configuration for both CIFS and NFS, select the **Retain the CIFS data LIF's configuration for NFS client** check box.

   If you do not retain the same data LIF configuration for both CIFS and NFS, you must specify the IP address and ports separately for CIFS and NFS.

5. Specify the IP address by choosing one of the following options:

If you want to…	Then…
Specify the IP address by using a subnet	a. Select **Using a subnet**. b. In the Add Details dialog box, select the subnet from which the IP address must be assigned. For intercluster LIFs, only the subnets that are associated with the selected IPspace are displayed. c. If you want to assign a specific IP address to the interface, select **Use a specific IP address**, and then type the IP address. The IP address that you specify is added to the subnet if the IP address is not already present in the subnet range. d. Click **OK**.

If you want to…	Then…
Specify the IP address manually without using a subnet	a. Select **Without a subnet**. b. In the Add Details dialog box, perform the following steps: i. Specify the IP address and the network mask or prefix. ii. Optional: Specify the gateway. iii. If you do not want to use the default value for the Destination field, specify a new destination value. If you do not specify a destination value, the Destination field is populated with the default value based on the family of the IP address. If a route does not exist, a new route is automatically created based on the gateway and destination. c. Click **OK**.

6. Specify a port to create a data LIF:
   a. Click **Browse**.
   b. In the **Select Network Port or Adapter** dialog box, select a port.
   c. Click **OK**.
7. Configure the CIFS server by performing the following steps:
   a. Specify the following information to create a CIFS server:
      - CIFS server name
      - Active Directory to associate with the CIFS server
      - Organizational unit (OU) within the Active Directory domain to associate with the CIFS server

        By default, this parameter is set to CN=Computers.
      - Credentials of an administrative account that has sufficient privileges to add the CIFS server to the OU
   b. **Optional:** Select **Encrypt Data while accessing all shares of this SVM** to enable SMB 3.0 encryption for all of the shares of the SVM.
   c. Provision a volume for CIFS storage when configuring the protocol by specifying the share name, size of the share, and access permissions.
   d. Select **Encrypt Data while accessing this share** to enable SMB 3.0 encryption for a particular share.
8. **Optional:** Configure NIS services:
   a. Specify the IP addresses of the NIS servers and NIS domain name to configure NIS services on the SVM.

b. Select the appropriate database type for which you want to add the “nis” name service source.

c. Provision a volume for NFS storage by specifying the export name, size, and permission.

9. Click **Submit & Continue**.

Results

The CIFS server and NIS domain are configured with the specified configuration, and the data LIFs are created. By default, the data LIFs have management access. You can view the configuration details on the Summary page.

Configure iSCSI protocol on SVMs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to configure the iSCSI protocol on a storage virtual machine (SVM) to provide block-level data access. You can create iSCSI LIFs and portsets and then add the LIFs to the portsets. LIFs are created on the most suitable adapters and are assigned to portsets to ensure data path redundancy.

Before you begin

- The iSCSI license must be enabled on the cluster.

  If the iSCSI protocol is not enabled on the SVM, you can use the Edit Storage Virtual Machine window to enable the protocol for the SVM.

- All of the nodes in the cluster must be healthy.
- Each node must have at least two data ports, and the port state must be `up`.

About this task

- You can configure the iSCSI protocol while creating the SVM or you can do so at a later time.
- SnapLock aggregates are not considered for automatically creating volumes.

Steps

1. If you have not configured the iSCSI protocol while creating the SVM, click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. **Optional:** In the **Network Access** section, specify an alias for the iSCSI target.

   The maximum number of characters for an alias name is 128. If you do not specify a target alias, the SVM name is used as an alias.

5. Specify the number of iSCSI LIFs that can be assigned to a single node.

   The minimum number of LIFs per node is one. The maximum number is the minimum of all the ports in the `up` state across the nodes. If the maximum value is an odd number, the previous even number is considered as the maximum value. You can choose any even number in the minimum and maximum value range.

   A 4-node cluster has node1, node2, and node3 with six ports each in the `up` state, and node4 with seven ports in the `up` state. The effective maximum value for the cluster is 6.

If the number of LIFs that you want to assign to the node is more than two, you must assign at least one portset to each LIF.

6. Specify the network details, including the subnet details, to create iSCSI LIFs:

If you want to…	Then…
Specify the IP address by using a subnet	a. Select **Using a subnet**. b. In the Add Details dialog box, select the subnet from which the IP address must be assigned. For intercluster LIFs, only the subnets that are associated with the selected IPspace are displayed. c. If you want to assign a specific IP address to the interface, select **Use a specific IP address**, and then type the IP address. The IP address that you specify is added to the subnet if the IP address is not already present in the subnet range. d. Click **OK**.
Specify the IP address manually without using a subnet	a. Select **Without a subnet**. b. In the Add Details dialog box, perform the following steps: i. Specify the IP address and the network mask or prefix. ii. Optional: Specify the gateway. iii. If you do not want to use the default value for the Destination field, specify a new destination value. If you do not specify a destination value, the Destination field is populated with the default value based on the family of the IP address. If a route does not exist, a new route is automatically created based on the gateway and destination. c. Click **OK**.

7. Select the broadcast domain.
8. Select the adapter type.

   If you have NIC cards configured in your cluster, you should select **NIC**.

If you have CNS cards configured in your cluster, you should select **CNA**.

If you have ifgrps configured in your cluster, you should select **Interface Group**.

The ifgrp port must be added in the broadcast domain.

9. **Optional:** Provision a LUN for iSCSI storage when configuring the iSCSI protocol by specifying the LUN size, OS type for the LUN, and host initiator details.
10. If you want to verify or modify the configuration of the automatically generated iSCSI LIFs, select **Review or Modify LIFs configuration (Advanced Settings)**.

    You can modify only the LIF name and the home port. By default, the portsets are set to the minimum value. You must specify unique entries. If you specify duplicate LIF names, System Manager appends numeric values to the duplicate LIF name.

    Based on the selected portset, the LIFs are distributed across the portsets by using a round-robin method to ensure redundancy in case of node failure or port failure.

11. Click **Submit & Continue**.

Results

The iSCSI LIFs and portsets are created with the specified configuration. The LIFs are distributed among the portsets based on the selected portset. The iSCSI service is started if all of the LIFs are successfully created.

If LIF creation fails, you can create the LIFs by using the Network Interfaces window, attach the LIFs to the portsets by using the LUNs window, and then start the iSCSI service by using the iSCSI window.

Configure FC protocol and FCoE protocol on SVMs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to configure the FC protocol and the FCoE protocol on the storage virtual machine (SVM) for SAN hosts. LIFs are created on the most suitable adapters and are assigned to portsets to ensure data path redundancy. Based on your requirements, you can configure either the FC protocol or the FCoE protocols, or both the protocols by using System Manager.

Before you begin

- The FCP license must be enabled on the cluster.
- All of the nodes in the cluster must be healthy.
- Each node must have at least two correctly configured ports for each protocol (FC and FCoE).

About this task

- You can configure the FC protocol and the FCoE protocol while creating the SVM or you can configure the protocols at a later time.

  If the protocols are not allowed on the SVM, you can use the Edit Storage Virtual Machine window to enable the protocols for the SVM.

- SnapLock aggregates are not considered for automatically creating volumes.

Steps

1. If you have not configured the protocols while creating the SVM, click the **Storage** > **SVMs** tab.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **FC/FCoE**.
4. In the **Data Interface Configuration** section, select the corresponding option to configure data LIFs for the FC protocol and the FCoE protocol.
5. Specify the number of data LIFs per node for each protocol.

   The minimum number of LIFs per node is one. The maximum number is the minimum of all the ports in the `up` state across the nodes. If the maximum value is an odd number, the previous even number is considered as the maximum value. You can choose any even number in the minimum and maximum value range.

   A four-node cluster has node1, node2, and node3 with six ports each in the `up` state, and node4 with seven ports in the `up` state. The effective maximum value for the cluster is six.

   If the number of LIFs that you want to assign to the node is more than two, you must assign at least one portset to each LIF.

6. If you want to verify or modify the automatically generated LIFs configuration, select **Review or Edit the Interface Association**.

   You can modify only the LIF name and home port. You must ensure that you do not specify duplicate entries.

7. **Optional:** Provision a LUN for the FC storage or FCoE storage when configuring the protocol by providing the LUN size, OS type for the LUN, and host initiator details.
8. Click **Submit & Continue**.

Results

The data LIFs and portsets are created with the specified configuration. The LIFs are distributed accordingly among the portsets. The FCP service is started if all of the LIFs are successfully created for at least one protocol.

If LIF creation fails, you can create the LIFs and start the FCP service from the FC/FCoE window.

Related information

ONTAP 9 Documentation Center

Configure NVMe protocol on SVMs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to configure the NVMe protocol on a storage virtual machine (SVM). You can then create namespaces and assign them to an NVMe subsystem and host.

About this task

The SVM with NVMe should not have any other protocol. If you select NVMe, then the rest of the protocols will be disabled. You can also configure NVMe while creating the SVM.

Steps

1. If you did not configure the NVMe protocol when creating the SVM, click **Storage** > **SVMs**

2. Select the SVM, and then click **SVM settings**.
3. In the **Protocols** pane, click **NVMe**.
4. Click the link to configure the protocol, as required.

   If there are any other protocols enabled, you must deselect these to make NVMe available to select. NVMe cannot be combined with any other protocol.

5. In the **Edit Storage Virtual Machine** pane, click on **Resource Allocation**.
6. In the **Resource Allocation** tab, you can choose not to delegate volume creation or you can select an aggregate to provision the volumes automatically.
7. Click on the **Services** tab to configure the Name Service Switch details.
8. Click **Save and Close**

   The NVMe protocol is configured on the SVM. After the protocol has been configured, you can start or stop the service using **SVM Settings**

Related information

Setting up NVMe

Delegate administration to SVM administrators with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to optionally delegate the administration of the SVM to SVM administrators after setting up a functional storage virtual machine (SVM) or SVMs with basic network configuration.

About this task

SVM administrators cannot use System Manager to manage delegated SVMs. Administrators can manage them only by using the command-line interface (CLI).

Steps

1. In the **Administrator Details** section, set up a password for the `vsadmin` user account.
2. If you want a dedicated LIF for SVM management, select **Create a LIF for SVM management**, and then specify the network details.

   A dedicated SVM management LIF is required for SAN protocols, where data and management protocols cannot share the same LIF. SVM management LIFs can be created only on data ports.

3. Specify the network details, including subnet details, for creating iSCSI LIFs:

If you want to…	Then…
Specify the IP address by using a subnet	a. Select **Using a subnet**. b. In the Add Details dialog box, select the subnet from which the IP address must be assigned. For intercluster LIFs, only the subnets that are associated with the selected IPspace are displayed. c. If you want to assign a specific IP address to the interface, select **Use a specific IP address**, and then type the IP address. The IP address that you specify is added to the subnet if the IP address is not already present in the subnet range. d. Click **OK**.
Specify the IP address manually without using a subnet	a. Select **Without a subnet**. b. In the Add Details dialog box, perform the following steps: i. Specify the IP address and the network mask or prefix. ii. Optional: Specify the gateway. iii. If you do not want to use the default value for the Destination field, specify a new destination value. If you do not specify a custom value, the Destination field is populated with the default value based on the family of the IP address. If a route does not exist, a new route is automatically created based on the gateway and destination. c. Click **OK**.

4. Specify a port for creating a data LIF:
   a. Click **Browse**.
   b. Select a port from the Select Network Port or Adapter dialog box.
   c. Click **OK**.

Results

The `vsadmin` account is unlocked and configured with the password.

The default access methods for the `vsadmin` account are ONTAP API `(ontapi)` and SSH `(ssh)`. The SVM administrator can log in to the storage system by using the management IP address.

What to do next

You must assign aggregates to the SVM by using the Edit Storage Virtual Machine dialog box.

If the SVM does not have any assigned aggregates, the SVM administrator cannot create volumes.

Create FlexVol volumes with System Manager - ONTAP 9.7 and earlier

You can create a FlexVol volume for your data by using the Create Volume dialog box in ONTAP System Manager classic (available in ONTAP 9.7 and earlier). You must always create a separate volume for your data rather than storing data in the root volume.

Before you begin

- The cluster must contain a non-root aggregate and a storage virtual machine (SVM).
- If you want to create read/write volumes, you must have configured the protocols for the SVM, and you must have installed either the SnapMirror license or the SnapVault license.

  If you have not configured the protocols but have installed any one of these licenses, you can create only data protection (DP) volumes.

- For creating an encrypted volume, you must have installed the volume encryption license by using System Manager, and you must have enabled “key-manager setup” by using the command-line interface (CLI).

  You must refresh your web browser after enabling “key-manager setup”.

About this task

- You can enable storage Quality of Service (QoS) only for a read/write (rw) volume.
- When you create a DP volume on the sync-source SVM in a MetroCluster configuration, the volume is not replicated on the sync-destination SVM.
- When you create a DP volume in a MetroCluster configuration, the source volume is not replicated (mirrored or vaulted) in the destination SVM.
- In a MetroCluster configuration, System Manager displays only the following aggregates for creating volumes:
  - In normal mode, when you create volumes on sync-source SVMs or data-serving SVMs in the primary site, only those aggregates that belong to the cluster in the primary site are displayed.
  - In switched-over mode, when you create volumes on sync-destination SVMs or data-serving SVMs in the surviving site, only switched-over aggregates are displayed.
- You cannot encrypt a volume in Cloud Volumes ONTAP.
- If encryption is enabled on the source volume and if the destination cluster is running a version of ONTAP software earlier than ONTAP 9.3, then encryption is disabled on the destination volume by default.

Steps

1. Click **Storage** > **Volumes**.
2. Click **Create** > **Create FlexVol**.

3. Browse and select the SVM in which you want to create the volume.

   The Create Volume dialog box is displayed. The dialogue box includes the following tabs:

   - General
   - Storage Efficiency
   - SnapLock
   - Quality of Service
   - Protection

4. On the **General** tab, perform the following steps:
   a. Specify a name for the FlexVol volume.
   b. Click the **FabricPool** button to specify that the volume is a FabricPool volume.
   c. Click **Choose** to select an aggregate.

      You can select only FabricPool-enabled aggregates if the volume is a FabricPool FlexVol volume, and you can select only non-FabricPool-enabled aggregates if the volume is a non-FabricPool FlexVol volume. If you choose an encrypted aggregate (NAE), the volume you are creating will inherit the encryption of the aggregate.

   d. Select a storage type.
   e. Specify the volume size and measurement units.
   f. Indicate how much space should be reserved for Snapshot copies.
   g. Select a space reserve option from the **Space Reserve** drop-down menu.
   h. Select the **Volume Encryption** checkbox to enable encryption for the volume. This option is available only if you have enabled the Volume Encryption license and if the corresponding platform is capable of supporting encryption.
5. On the **Storage Efficiency** tab, perform the following steps:
   a. Select the type of storage for which you are creating this volume.

      You must select **Data Protection** if you are creating a SnapMirror destination volume. You are provided read-only access to this volume.

   b. Specify the tiering policy for the volume.
   c. Specify the size of the volume and the percentage of the total volume size that you want to reserve for Snapshot copies.

      The default space reserved for Snapshot copies is zero percent for SAN volumes and VMware volumes. For NAS volumes, the default is 5 percent.

   d. Select **Default**, **Thin provisioned**, or **Thick provisioned** for the volume.

      When thin provisioning is enabled, space is allocated to the volume from the aggregate only when data is written to the volume.

      - For AFF storage systems, the value of thin provisioning is “Default”, and for other storage systems, the value of thick provisioning is “Default”.
      - For FabricPool-enabled aggregates, the value of thin provisioning is “Default”.

e. Specify whether you want to enable deduplication on the volume.

   System Manager uses the default deduplication schedule. If the specified volume size exceeds the limit that is required for running deduplication, the volume is created and deduplication is not enabled.

   For systems with All Flash Optimized personality, inline compression and the `auto` deduplication schedule are enabled by default.

6. On the **Quality of Service** tab, perform the following steps:
   a. Select the **Manage Storage Quality of Service** checkbox if you want to enable storage QoS for the FlexVol volume to manage workload performance.
   b. Create a new storage QoS policy group or select an existing policy group to control the input/output (I/O) performance of the FlexVol volume:

If you want to…	Do this…
Create a new policy group	a. Select **New Policy Group**. b. Specify the policy group name. c. Specify the minimum throughput limit. ◦ In System Manager 9.5, you can set the minimum throughput limit only on a performance-based All Flash Optimized personality. In System Manager 9.6, you can set the minimum throughput limit for the policy group. ◦ You cannot set the minimum throughput limit for volumes on a FabricPool-enabled aggregate. ◦ If you do not specify the minimum throughput value or if the minimum throughput value is set to 0, the system automatically displays “None” as the value. This value is case-sensitive. d. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group does not exceed the specified throughput limit. ◦ The minimum throughput limit and the maximum throughput limit must be of the same unit type. ◦ If you do not specify the minimum throughput limit, then you can set the maximum throughput limit in IOPS, B/s, KB/s, MB/s, and so on. ◦ If you do not specify the maximum throughput value, the system automatically displays “Unlimited” as the value. This value is case-sensitive. The unit that you specify does not affect the maximum throughput.

If you want to…	Do this…
Select an existing policy group	a. Select **Existing Policy Group**, and then click **Choose** to select an existing policy group from the Select Policy Group dialog box. b. Specify the minimum throughput limit. ◦ In System Manager 9.5, you can set the minimum throughput limit only on a performance-based All Flash Optimized personality. In System Manager 9.6, you can set the minimum throughput limit for the policy group. ◦ You cannot set the minimum throughput limit for volumes on a FabricPool-enabled aggregate. ◦ If you do not specify the minimum throughput value or if the minimum throughput value is set to 0, the system automatically displays “None” as the value. This value is case-sensitive. c. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group does not exceed the specified throughput limit. ◦ The minimum throughput limit and the maximum throughput limit must be of the same unit type. ◦ If you do not specify the minimum throughput limit, then you can set the maximum throughput limit in IOPS, B/s, KB/s, MB/s, and so on. ◦ If you do not specify the maximum throughput value, the system automatically displays “Unlimited” as the value. This value is case-sensitive. The unit that you specify does not affect the maximum throughput. If the policy group is assigned to more than one object, the maximum throughput that you specify is shared among the objects.

7. On the **Protection** tab, perform the following steps:

a. Specify whether you want to enable **Volume Protection**.

   A non-FabricPool FlexGroup volume can be protected with a FabricPool FlexGroup volume.

   A FabricPool FlexGroup volume can be protected with a non-FabricPool FlexGroup volume.

b. Select the **Replication** type:

If you selected the replication type as…	Do this…
Asynchronous	a. **Optional:** If you do not know the replication type and relationship type, click **Help me Choose**, specify the values, and then click **Apply**. b. Select the relationship type. The relationship type can be mirror, vault, or mirror and vault. c. Select a cluster and an SVM for the destination volume. If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed. d. Modify the volume name suffix, if required.
Synchronous	a. **Optional:** If you do not know the replication type and relationship type, click **Help me Choose**, specify the values, and then click **Apply**. b. Select the synchronization policy. The synchronization policy can be StrictSync or Sync. c. Select a cluster and an SVM for the destination volume. If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed. d. Modify the volume name suffix, if required.

8. Click **Create**.
9. Verify that the volume that you created is included in the list of volumes in the **Volume** window.

The volume is created with UNIX-style security and UNIX 700 “read write execute” permissions for the owner.

Related information

Volumes window

Create SnapLock volumes with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create a SnapLock Compliance volume or a SnapLock Enterprise volume. When you create a volume, you can also set retention times, and choose whether to automate setting the WORM state on data in the volume.

Before you begin

- The SnapLock license must have been installed.
- The SnapLock aggregate must be online.
- For creating an encrypted volume, you must have installed the volume encryption license by using System Manager, and you must have enabled “key-manager setup” by using the command-line interface (CLI).

  You must refresh your web browser after enabling “key-manager setup”.

About this task

- You can delete a complete SnapLock Enterprise volume or a file in a SnapLock Enterprise volume; however, you cannot delete only the data within a file in a SnapLock Enterprise volume.
- You cannot delete a SnapLock Compliance volume if data is committed to the volume.
- You cannot encrypt a volume in Cloud Volumes ONTAP.
- If encryption is enabled on the source volume and if the destination cluster is running a version of ONTAP software earlier than ONTAP 9.3, then encryption is disabled on the destination volume by default.

Steps

1. Click **Storage** > **Volumes**.
2. Click **Create** > **Create FlexVol**.
3. Browse and select the storage virtual machine (SVM) in which you want to create the volume.
4. In the **Create Volume** dialog box, specify a new name if you want to change the default name of the volume.

   You cannot change the name of a SnapLock Compliance volume after you create the volume.

5. Select the container aggregate for the volume.

   You must select a SnapLock Compliance aggregate or SnapLock Enterprise aggregate to create a SnapLock volume. The volume inherits the SnapLock type from the aggregate, and the SnapLock type cannot be changed after the volume is created; therefore, you must select the correct aggregate.

6. Select the **Volume Encryption** checkbox to enable encryption for the volume.

   This option is available only if you have enabled the Volume Encryption license and if the corresponding platform is capable of supporting encryption.

7. Select the type of storage for which you are creating this volume.

   If you are creating a SnapMirror destination volume, you must select **Data Protection**. You are provided read-only access to this volume.

8. Specify the size of the volume and the percentage of the total volume size that you want to reserve for Snapshot copies.

   The default space that is reserved for Snapshot copies is zero percent for SAN volumes and VMware volumes. For NAS volumes, the default is 5 percent.

9. **Optional:** Select **Thin Provisioned** to enable thin provisioning for the volume.

   When thin provisioning is enabled, space is allocated to the volume from the aggregate only when data is written to the volume.

10. **Optional:** Make the required changes in the **Storage Efficiency** tab to enable deduplication on the volume.

    System Manager uses the default deduplication schedule. If the specified volume size exceeds the limit that is required for running deduplication, the volume is created, and deduplication is not enabled.

11. Select the **SnapLock** tab, and then perform the following steps:
    a. **Optional:** Specify the autocommit period.

       The file in the volume remains unchanged for the period that you specify before the file is committed to the WORM state. To set files to the WORM state manually, you must select **Not specified** as the autocommit setting.

       The values must be in the range of 5 minutes to 10 years.

    b. Specify the minimum retention period and maximum retention period.

       The values must be in the range of 1 day through 70 years or Infinite.

    c. Select the default retention period.

       The default retention period must be within the specified minimum retention period and maximum retention period.

12. **Optional:** Select the **Manage Storage Quality of Service** checkbox in the **Quality of Service** tab to enable storage QoS for the FlexVol volume in order to manage workload performance.
13. Create a storage QoS policy group or select an existing policy group to control the input/output (I/O) performance of the FlexVol volume.

If you want to…	Do this…
Create a storage QoS policy group	a. Select **New Policy Group**. b. Specify the policy group name. c. Specify the minimum throughput limit. ◦ In System Manager 9.5, you can set the minimum throughput limit only on a performance-based All Flash Optimized personality. In System Manager 9.6, you can also set the minimum throughput limit for ONTAP Select Premium systems. ◦ You cannot set the minimum throughput limit for volumes on a FabricPool-enabled aggregate. ◦ If you do not specify the minimum throughput value or if the minimum throughput value is set to 0, the system automatically displays “None” as the value. This value is case-sensitive. d. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group does not exceed the specified throughput limit. ◦ The minimum throughput limit and the maximum throughput limit must be of the same unit type. ◦ If you do not specify the minimum throughput limit, then you can set the maximum throughput limit in IOPS, B/s, KB/s, MB/s, and so on. ◦ If you do not specify the maximum throughput value, the system automatically displays “Unlimited” as the value. This value is case-sensitive. The unit that you specify does not affect the maximum throughput.

If you want to…	Do this…
Select an existing policy group	a. Select **Existing Policy Group**, and then click **Choose** to select an existing policy group from the Select Policy Group dialog box. b. Specify the minimum throughput limit. ◦ In System Manager 9.5, you can set the minimum throughput limit only on a performance-based All Flash Optimized personality. In System Manager 9.6, you can also set the minimum throughput limit for ONTAP Select Premium systems. ◦ You cannot set the minimum throughput limit for volumes on a FabricPool-enabled aggregate. ◦ If you do not specify the minimum throughput value or if the minimum throughput value is set to 0, the system automatically displays “None” as the value. This value is case-sensitive. c. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group does not exceed the specified throughput limit. ◦ The minimum throughput limit and the maximum throughput limit must be of the same unit type. ◦ If you do not specify the minimum throughput limit, then you can set the maximum throughput limit in IOPS, B/s, KB/s, MB/s, and so on. ◦ If you do not specify the maximum throughput value, the system automatically displays “Unlimited” as the value. This value is case-sensitive. The unit that you specify does not affect the maximum throughput. If the policy group is assigned to more than one object, the maximum throughput that you specify is shared among the objects.

14. Enable **Volume Protection** in the **Protection** tab to protect the volume:
15. In the **Protection** tab, select the **Replication** type:

If you selected the replication type as…	Do this…
Asynchronous	a. **Optional:** If you do not know the replication type and relationship type, click **Help me Choose**, specify the values, and then click **Apply**. b. Select the relationship type. The relationship type can be mirror, vault, or mirror and vault. c. Select a cluster and an SVM for the destination volume. If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed. d. Modify the volume name suffix, if required.
Synchronous	a. **Optional:** If you do not know the replication type and relationship type, click **Help me Choose**, specify the values, and then click **Apply**. b. Select the synchronization policy. The synchronization policy can be StrictSync or Sync. c. Select a cluster and an SVM for the destination volume. If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed. d. Modify the volume name suffix, if required.

16. Click **Create**.
17. Verify that the volume that you created is included in the list of volumes in the **Volume** window.

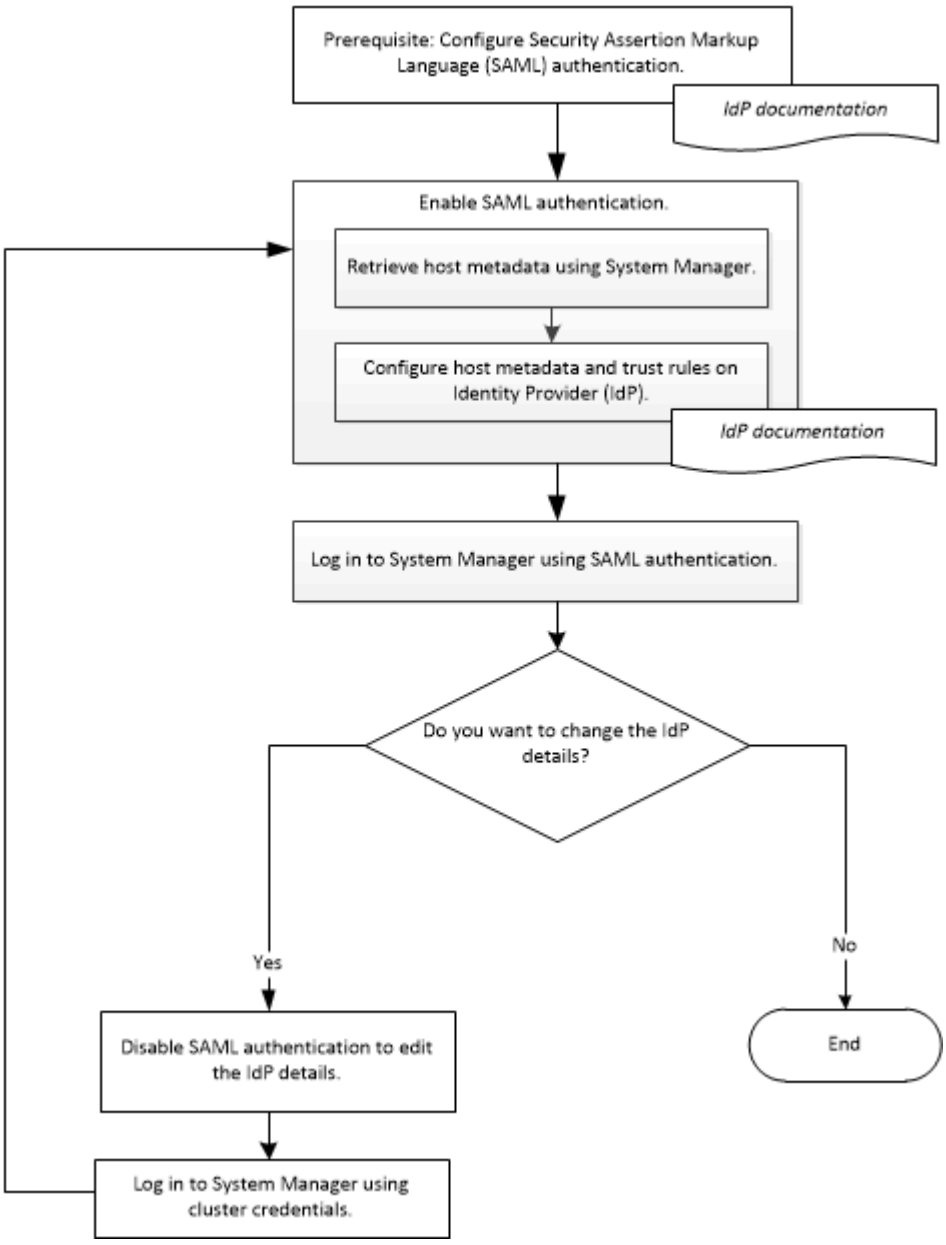
Results

The volume is created with UNIX-style security and UNIX 700 “read write execute” permissions for the owner.

Set up SAML authentication with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to set

up Security Assertion Markup Language (SAML) authentication. Remote users are authenticated through a secure identity provider (IdP) before they log in to System Manager.



Enable SAML authentication

You can use System Manager to configure Security Assertion Markup Language (SAML) authentication so that remote users can log in by using a secure identity provider (IdP).

Before you begin

- The IdP that you plan to use for remote authentication must be configured.

  See the documentation that is provided by the IdP that you have configured.

- You must have the URI of the IdP.

About this task

The following IdPs have been validated with System Manager:

- Active Directory Federation Services
- Cisco DUO (validated with the following ONTAP versions:)
  - 9.7P21 and later 9.7 releases
  - 9.8P17 and later 9.8 releases
  - 9.9.1P13 and later 9.9 releases
  - 9.10.1P9 and later 9.10 releases
  - 9.11.1P4 and later 9.11 releases
  - 9.12.1 and later releases
- Shibboleth

> After SAML authentication is enabled, only remote users can access the System Manager GUI. Local users cannot access the System Manager GUI after SAML authentication is enabled.

Steps

1. Click **Configuration** > **Cluster** > **Authentication**.
2. Select the **Enable SAML authentication** check box.
3. Configure System Manager to use SAML authentication:
   a. Enter the URI of the IdP.
   b. Enter the IP address of the host system.
   c. **Optional:** If required, change the host system certificate.
4. Click **Retrieve Host Metadata** to retrieve the host URI and host metadata information.
5. Copy the host URI or host metadata details, access your IdP, and then specify the host URI or host metadata details and the trust rules in the IdP window.

   > See the documentation that is provided by the IdP that you have configured.

6. Click **Save**.

   The IdP login window is displayed.

7. Log in to System Manager by using the IdP login window.

   After the IdP is configured, if the user tries to log in by using the fully qualified domain name (FQDN), IPv6, or a cluster management LIF, then the system automatically changes the IP address to the IP address of the host system that was specified during the IdP configuration.

Disable SAML authentication

You can disable Security Assertion Markup Language (SAML) authentication if you want to disable remote access to System Manager, or to edit the SAML configuration.

About this task

Disabling SAML authentication does not delete SAML configuration.

Steps

1. Click **Configuration** > **Cluster** > **Authentication**.
2. Clear the **Enable SAML authentication** check box.
3. Click **Save**.

   System Manager restarts.

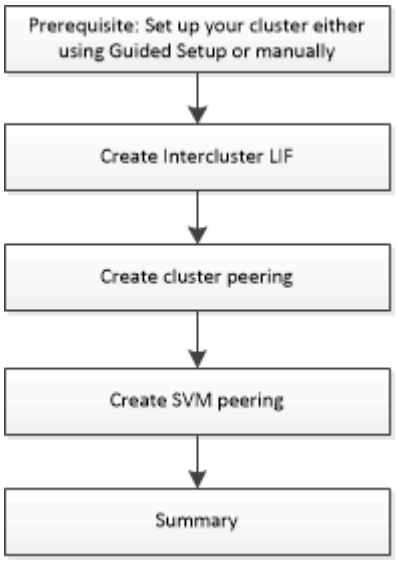
4. Log in to System Manager by using the cluster credentials.

Related information

Accessing a cluster by using the ONTAP System Manager browser-based graphic interface

Set up peering with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to set up peering. Setting up peering involves creating intercluster logical interfaces (LIFs) on each node, creating cluster peering, and creating SVM peering.



Prerequisites for cluster peering

Before you set up cluster peering, you should confirm that the connectivity, port, IP address, subnet, firewall, and cluster-naming requirements are met.

Connectivity requirements

Every intercluster LIF on the local cluster must be able to communicate with every intercluster LIF on the remote cluster.

Although it is not required, it is typically simpler to configure the IP addresses used for intercluster LIFs in the same subnet. The IP addresses can reside in the same subnet as data LIFs, or in a different subnet. The subnet used in each cluster must meet the following requirements:

- The subnet must belong to the broadcast domain that contains the ports that are used for intercluster communication.

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

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

Port requirements

You can use dedicated ports for intercluster communication, or share ports used by the data network. Ports must meet the following requirements:

- All ports that are used to communicate with a given remote cluster must be in the same IPspace.

  You can use multiple IPspaces to peer with multiple clusters. Pair-wise full-mesh connectivity is required only within an IPspace.

- The broadcast domain that is used for intercluster communication must include at least two ports per node so that intercluster communication can fail over from one port to another port.

  Ports added to a broadcast domain can be physical network ports, VLANs, or interface groups (ifgrps).

- All ports must be cabled.
- All ports must be in a healthy state.
- The MTU settings of the ports must be consistent.

Firewall requirements

Firewalls and the intercluster firewall policy must allow the following protocols:

- ICMP service
- TCP to the IP addresses of all the intercluster LIFs over the ports 10000, 11104, and 11105
- Bidirectional HTTPS between the intercluster LIFs

The default `intercluster` firewall policy allows access through the HTTPS protocol and from all IP addresses (0.0.0.0/0). You can modify or replace the policy if necessary.

Create intercluster LIFs

Creating intercluster logical interfaces (LIFs) enables the cluster network to communicate with a node. You must create an intercluster LIF within each IPspace that will be used for peering, on each node in each cluster for which you want to create a peer relationship.

Steps

1. Click **Configuration** > **Advanced Cluster Setup**.
2. In the **Setup Advanced Cluster Features** window, click **Proceed** next to the **Cluster Peering** option.
3. Select an IPspace from the **IPspace** list.
4. Enter the IP address, port, network mask, and gateway details of each node.
5. Click **Submit and Continue**.

What to do next

You should enter the cluster details in the Cluster Peering window to continue with cluster peering.

Create cluster peer relationships

You can create an authenticated cluster peer relationship to connect clusters so that the clusters in the peer relationship can communicate securely with each other.

Before you begin

- You must have reviewed and completed the requirements for performing this task.

  Prerequisites for cluster peering

- You must have created intercluster logical interfaces (LIFs).
- You should be aware of which version of ONTAP each cluster is running.

About this task

- If you want to create a peer relationship with a cluster running Data ONTAP 8.2.2 or earlier, you must use the CLI.
- You can create a peer relationship between a cluster running ONTAP 9.5 and a cluster running ONTAP 9.6. However, encryption is not supported in ONTAP 9.5, so the peer relationship cannot be encrypted.
- In a MetroCluster configuration, when you create a peer relationship between the primary cluster and an external cluster, it is a best practice to create a peer relationship between the surviving site cluster and the external cluster as well.
- You can create a custom passphrase or you can use the system-generated passphrase to authenticate the cluster peer relationship. However, the passphrases of both clusters must match.

Steps

1. Click **Configuration** > **Advanced Cluster Setup**.
2. In the **Target Cluster Intercluster LIF IP addresses** field, enter the IP addresses of the remote cluster's intercluster LIFs.
3. **Optional:** If you are creating a peer relationship between a cluster running ONTAP 9.5 and a cluster running ONTAP 9.6, select the checkbox.

   The peer relationship will not be encrypted. If you do not select the checkbox, the peer relationship will not be established.

4. In the **Passphrase** field, specify a passphrase for the cluster peer relationship.

   If you create a custom passphrase, the passphrase will be validated against the passphrase of the peered cluster to ensure an authenticated cluster peer relationship.

   If the names of the local cluster and remote cluster are identical, and if you are using a custom passphrase, an alias is created for the remote cluster.

5. **Optional:** To generate a passphrase from the remote cluster, enter the management IP address of the remote cluster.
6. Initiate cluster peering.

If you want to…	Do this…
Initiate cluster peering from the initiator cluster	Click **Initiate Cluster Peering**.
Initiate cluster peering from the remote cluster (Applicable if you have created a custom passphrase)	a. Enter the management IP address of the remote cluster. b. Click the **Management URL** link to access the remote cluster. c. Click **Create Cluster Peering**. d. Specify the intercluster LIF IP addresses and passphrase of the initiator cluster. e. Click **Initiate Peering**. f. Access the initiator cluster, and then click **Validate Peering**.

What to do next

You should specify the SVM details in the SVM Peering window to continue with the peering process.

Create SVM Peers

SVM peering enables you to establish a peer relationship between two storage virtual machines (SVMs) for data protection.

Before you begin

You must have created a peer relationship between the clusters in which the SVMs that you plan to peer reside.

About this task

- The clusters that you can select as target clusters are listed when you create SVM peers by using the **Configuration** > **SVM Peers** window.
- If the target SVM resides on a cluster in a system running ONTAP 9.2 or earlier, SVM peering cannot be accepted by using System Manager.

  In such a scenario, you can use the command-line interface (CLI) to accept SVM peering.

Steps

1. Select the initiator SVM.
2. Select the target SVM from the list of permitted SVMs.
3. Specify the name of the target SVM in the **Enter an SVM** field.

   If you have navigated from the **Configuration** > **SVM Peers** window, you should select the target SVM from the list of peered clusters.

4. Initiate SVM peering.

If you want to…	Do this…
Initiate SVM peering from the initiator cluster	Click Initiate SVM Peering.
Accept SVM peering from the remote cluster	Applicable for non-permitted SVMs a. Specify the management address of the remote cluster. b. Click the **Management URL** link to access the SVM Peer window of the remote cluster. c. On the remote cluster, accept the **Pending SVM Peer** request. d. Access the initiator cluster, and then click **Validate Peering**.

5. Click **Continue**.

What to do next

You can view the intercluster LIFs, cluster peer relationship, and SVM peer relationship in the Summary window.

When you use System Manager to create the peer relationship, the encryption status is “Enabled” by default.

What passphrases are

You can use a passphrase to authorize peering requests. You can use a custom passphrase or a system-generated passphrase for cluster peering.

- You can generate a passphrase on the remote cluster.
- The minimum required length for a passphrase is eight characters.
- The passphrase is generated based on the IPspace.
- If you are using a system-generated passphrase for cluster peering, after you enter the passphrase in the initiator cluster, peering is authorized automatically.
- If you are using a custom passphrase for cluster peering, you have to navigate to the remote cluster to complete the peering process.

Manage clusters

Dashboard window for System Manager - ONTAP 9.7 and earlier

The Dashboard window in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) contains multiple panels that provide cumulative at-a-glance information about your system and its performance.

You can use the Dashboard window to view information about important alerts and notifications, the efficiency and capacity of aggregates and volumes, the nodes that are available in a cluster, the status of the nodes in a high-availability (HA) pair, the most active applications and objects, and the performance metrics of a cluster or a node.

- **Alerts and Notifications**

  Displays all alerts in red, such as emergency EMS events, offline node details, broken disk details, license entitlements that are at high risk, and offline network port details. Displays all notifications in yellow, such as health monitor notifications that occurred in the past 24 hours at the cluster level, license entitlements that are at medium risk, unassigned disk details, the number of migrated LIFs, volume move operations that failed, and volume move operations that required administrative intervention in the past 24 hours.

  The Alerts and Notifications panel displays up to three alerts and notifications beyond which a View-All link is displayed. You can click the View-All link to view more information about the alerts and notifications.

  The refresh interval for the Alerts and Notifications panel is one minute.

- **Cluster Overview**

  Displays the aggregates and volumes that are nearing capacity, the storage efficiency of a cluster or node, and the protection details of top volumes.

  The Capacity tab displays the top online aggregates that are nearing capacity, in descending order of used space.

  The Capacity tab provides a link to the number of volumes with the highest capacity utilized when you enter a valid value in the Volumes exceeding used capacity of field. It also displays the amount of inactive (cold) data available in the cluster.

  The Efficiency tab displays the storage efficiency savings for a cluster or node. You can view the total logical space used, total physical space used, and the overall savings. You can select a cluster or a specific node to view the storage efficiency savings. For System Manager 9.5, the space used for Snapshot copies is *not* included in the values for total logical space used, total physical space used, and overall savings. However, Beginning with System Manager 9.6, the space used for Snapshot copies is included in the values for total logical space used, total physical space used, and overall savings.

  The refresh interval for the Cluster Overview panel is 15 minutes.

  The Protection tab displays information about cluster-wide volumes that do not have defined protection relationships. Only the FlexVol volumes and FlexGroup volumes that meet the following criteria are displayed:

  - The volumes are RW volumes and are online.
  - The aggregate containing the volumes is online.
  - The volumes have protection relationships and are not yet initialized.
    You can navigate to the Volumes window to view the volumes that do not have a defined protection relationship.

  The Protection tab also displays the top five SVMs that have the highest number of volumes that do not have defined protection relationships.

- **Nodes**

  Displays a pictorial representation of the number and names of the nodes that are available in the cluster, and the status of the nodes that are in an HA pair. You should position the cursor over the pictorial representation of the nodes to view the status of the nodes in an HA pair.

  You can view more information about all of the nodes by using the Nodes link. You can also click the pictorial representation to view the model of the nodes and the number of aggregates, storage pools,

shelves, and disks that are available in the nodes. You can manage the nodes by using the Manage Nodes link. You can manage the nodes in an HA pair by using the Manage HA link.

The refresh interval for the Nodes panel is 15 minutes.

- **Applications and Objects**

  You can use the Applications and Objects panel to display information about applications, clients, and files in a cluster.

  The Applications tab displays information about the top five applications of the cluster. You can view the top five applications based on either IOPS and latency (from low to high or from high to low) or capacity (from low to high or from high to low).

  You should click the specific bar chart to view more information about the application. The total space, used space, and available space are displayed for capacity, the IOPS details are displayed for IOPS, and the latency details are displayed for latency.

  You can click **View details** to open the Applications window of the specific application.

  The Objects tab displays information about the top five active clients and files in the cluster. You can view the top five active clients and files based on IOPS or throughput.

  This information is displayed only for CIFS and NFS protocols.

  The refresh interval for the Applications and Objects panel is one minute.

- **Performance**

  Displays the average performance metrics, read performance metrics, and write performance metrics of the cluster based on latency, IOPS, and throughput. The average performance metrics is displayed by default. You can click Read or Write to view the read performance metrics or write performance metrics, respectively. You can view the performance metrics of the cluster or a node.

  If the information about cluster performance cannot be retrieved from ONTAP, you cannot view the respective graph. In such cases, System Manager displays the specific error message.

  The refresh interval for the charts in the Performance panel is 15 seconds.

Monitoring a cluster using the dashboard

The dashboard in System Manager enables you to monitor the health and performance of a cluster. You can also identify hardware problems and storage configuration issues by using the dashboard.

Steps

1. Click the **Dashboard** tab to view the health and performance dashboard panels.

MetroCluster switchover and switchback

About MetroCluster switchover and switchback

Beginning with ONTAP System Manager 9.6, you can use MetroCluster switchover and switchback operations after a disaster that renders all the nodes in the source cluster unreachable and powered off. You can also use the switchover workflow for a negotiated

(planned) switchover in cases such as disaster recovery testing or a site going offline for maintenance.

About MetroCluster switchover and switchback

Beginning with System Manager 9.6, you can use MetroCluster switchover and switchback operations to allow one cluster site to take over the tasks of another cluster site. This capability allows you to facilitate maintenance or recovery from disasters.

A switchover operation allows one cluster (Site A) to take over the tasks that another cluster (Site B) usually performs. After the switchover, the cluster that has been taken over (Site B) can be brought down for maintenance and repairs. After the maintenance is completed, Site B can come up and healing tasks are completed, then you can initiate a switchback operation that allows the repaired cluster (Site B) to resume the tasks it usually performs.

System Manager supports two kinds of switchover operations, based on the status of the remote cluster site:

- A negotiated (planned) switchover: You initiate this operation when you need to do planned maintenance on a cluster or test your disaster recovery procedures.
- An unplanned switchover: You initiate this operation when a disaster has occurred on a cluster (Site B) and you want another site or cluster (Site A) to take over the tasks of the cluster affected by the disaster (Site B) while you perform repairs and maintenance.

You perform the same steps in System Manager for both switchover operations. When you initiate a switchover, System Manager determines whether the operation is feasible and aligns the workload accordingly.

MetroCluster switchover and switchback workflow

The overall process for switchover and switchback workflow includes the following three phases:

1. **Switchover**: The switchover process allows you to transfer control of the storage and client access from a source cluster site (Site B) to another cluster site (Site A). This operation helps you provide nondisruptive operations during testing and maintenance. In addition, this process also enables you to recover from a site failure. For disaster recovery testing or planned site maintenance, you can perform a MetroCluster switchover to transfer control to a disaster recovery (DR) site (Site A). Before you start the process, at least one of the surviving site nodes must be up and running before you perform the switchover. If a switchover operation previously failed on certain nodes on the DR site, the operation can be retried on all of those nodes.
2. **Site B Operations**: After switchover is completed, System Manager completes the healing process for the MetroCluster IP configuration. Healing is a planned event, which gives you full control of each step to minimize downtime. Healing is a two-phase process that occurs on the storage and controller components to prepare the nodes at the repaired site for the switchback process. During the first phase, the process heals the aggregates by resynchronizing the mirrored plexes and then heals the root aggregates by switching them back to the disaster site.

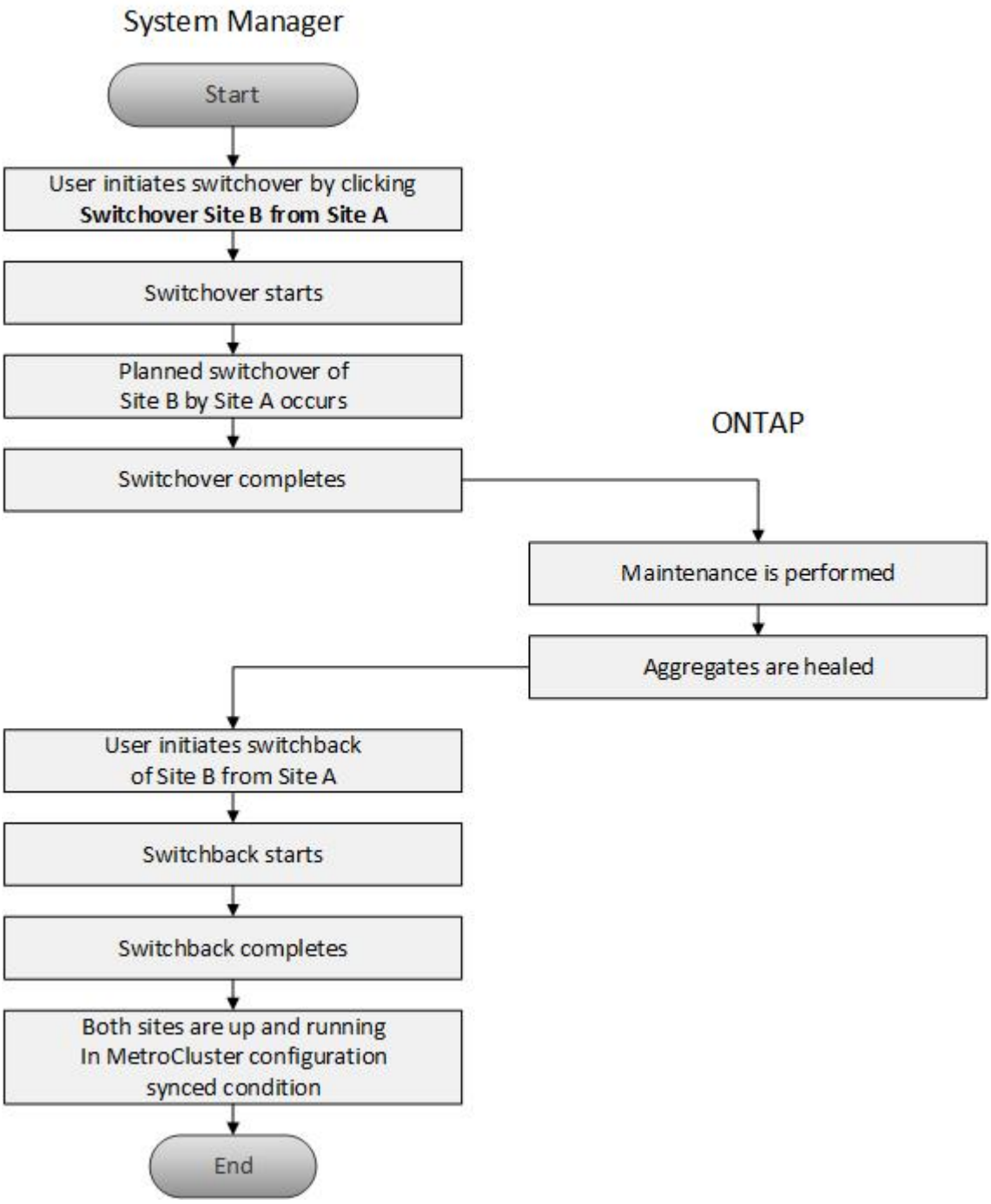
   In the second phase, the site is made ready for the switchback process.

3. **Switchback**: After maintenance and repairs are performed on Site B, you initiate the switchback operation to return control of the storage and client access from Site A to Site B. For a successful switchback, the following conditions must exist:
   - The home nodes and storage shelves must be powered on and reachable by nodes in Site A.
   - System Manager must have successfully completed the healing phase before you can initiate the switchback operation.

- All the aggregates in Site A should be in mirrored status and cannot be in degraded or resyncing status.
- All previous configuration changes must be complete before performing a switchback operation. This prevents those changes from competing with the negotiated switchover or switchback operation.

MetroCluster switchover and switchback workflow flowchart

The following flowchart illustrates the phases and processes that occur when you initiate switchover and switchback operations.



Prepare for switchover and switchback operations

Before you perform switchover operations using ONTAP System Manager classic 9.6, you should verify that the necessary steps have been performed on the affected site.

Steps

1. If you are recovering from a disaster on Site B, you must perform the following steps:
   a. Repair or replace any damaged disks or hardware.
   b. Restore power.
   c. Rectify error issues that occur.
   d. Bring up the disaster site.
2. Ensure the following conditions exist in your cluster:
   - Both sites are in Active state if you are performing a planned switchover.
   - The MetroCluster system uses configuration type “IP_Fabric”.
   - Both sites are operating with a two-node configuration (two nodes in each cluster). Sites with a single-node or four-node configuration are not supported for switchover and switchback operations using System Manager.
3. If you are launching the remote site (Site B) from the local site (Site A), ensure that Site B is running System Manager 9.6 or a later version.

Rename the MetroCluster local site (Site A) with System Manger - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to rename the MetroCluster local site (Site A) in a cluster.

Steps

1. Click **Configuration** > **Configuration Updates**.
2. Click **Update cluster name**.
3. Update the name in the text box, then click **Submit**.

   You can view the updated name when the MetroCluster Site A status is displayed.

4. To display the updated name of MetroCluster Site A when viewing it from the remote site (Site B), execute the following command within the CLI on the remote site (Site B): `cluster peer modify-local-name`

Performing a negotiated switchover

Beginning with System Manager 9.6, you can initiate a negotiated (planned) switchover of a MetroCluster site. This operation is useful when you want to perform disaster recovery testing or planned maintenance on the site.

Steps

1. In System Manager, use the cluster administrator credentials to log on to the local MetroCluster site (Site A).
2. Click **Configuration** > **MetroCluster**

   TheMetroCluster Switchover/Switchback Operations window displays.

3. Click **Next**.

   The MetroCluster Switchover and Switchback Operations window displays the status of the operations, and System Manager verifies whether a negotiated switchover is possible.

4. Perform one of the following substeps when the validation process has completed:
   - If validation is successful, proceed to Step 5.
   - If validation fails, but Site B is up, then an error has occurred, such as a problem with a subsystem or NVram mirroring is not synchronized. You can perform either of the following processes:
     - Fix the issue that is causing the error, click **Close**, and then start again at Step 1.
     - Halt the Site B nodes, click **Close**, and then perform the steps in Performing an unplanned switchover.
   - 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.

   A warning message displays, warning you that the switchover operation stops all data SVMs on Site B and restarts them on Site A.

6. If you want to proceed, click **Yes**.

   The switchover process begins. The states of Site A and Site B are displayed above the graphic representations of their configurations. If the switchover operation fails, an error message displays. Click **Close**. Correct any errors and start again at Step 1

7. Wait until System Manager shows that healing has been completed.

   When healing is completed, Site B is operational, and systems prepare for the switchback process.

   When the preparations for the switchback process are complete, the **Switchback from Site A to Site B** button is active at the bottom of the window.

8. To proceed with the switchback operation, perform the steps in Performing a switchback.

Performing a unplanned switchover

Beginning with System Manager 9.6, you can initiate an unplanned switchover of a MetroCluster site. This operation is useful after an outage event or disaster event.

Before you begin

Your MetroCluster is running in normal operating condition; however, the nodes in the local cluster (Site A) are up, but the nodes in the remote cluster (Site B) are down.

Steps

1. Verify that Site B is actually down.

   A connection error might make Site B appear to be down.

   ⓘ Starting the switchover process with Site B up could cause disastrous results.

2. In System Manager, log on to the local MetroCluster site (Site A) using the cluster administrator

credentials.

3. Click **Configuration** > **MetroCluster**

   TheMetroCluster Switchover/Switchback Operations window displays.

4. Click **Next**.

   The MetroCluster Switchover/Switchback Operations window displays the status of the operations, and System Manager verifies whether a negotiated switchover is feasible.

5. When the validation process is complete, click **Switchover Site B to Site A** to initiate the switchover process.

   A warning message displays, warning you that the switchover operation switches control from Site B to Site A. The status of Site B should be “UNREACHABLE”, and all Site B nodes are shown in red text.

   > As noted in Step 1, Site B must actually be down and not just unconnected. Also, you should be aware that the switchover operation might cause data loss.

6. If you want to proceed, ensure the check box is checked, and then click **Yes**.

   The switchover process begins. The states of Site A and Site B are displayed above the graphic representations of their configurations. If the switchover operation fails, an error message displays. Click **Close**. Correct any errors and start again at Step 1

7. Perform all required maintenance activities for Site B.
8. Ensure Site B is up.

   The healing process begins. When System Manager shows the healing is completed, Site B is operational and the systems prepare for the switchback process. The **Switchback from Site A to Site B** button appears at the bottom of the window.

9. Proceed to Performing a switchback to initiate the switchback operation.

Performing a switchback

Beginning with System Manager 9.6, you can perform a switchback operation that restores control to the original MetroCluster site (Site B) after the system has completed a successful switchover operation.

Before you begin

Before you perform a switchback operation, you must complete the following tasks:

- You must prepare the MetroCluster sites by Performing a negotiated (planned) switchover or Performing an unplanned switchover.
- If errors occurred during the healing operation, you must follow the displayed instructions to fix them.
- If the state of the remote site is displayed as “Getting ready for switchback”, then the aggregates are still resynchronizing. You should wait until the status of the remote site indicates that it is ready for switchback.

About this task

If a switchover operation is successful, the MetroCluster Switchover and Switchback Operations window displays. The window shows the status of both sites and provides a message that tells you the operation was

successful.

Steps

1. Click **Switchback from Site A to Site B** to initiate the switchback operation.

   A warning message tells you that the switchback operation is returning MetroCluster control to Site B and that the process might take some time.

2. If you want to proceed, click **Yes**.
3. Perform one of the following substeps when the switchback process has completed:
   - If the switchback operation is successful, click **Done** to acknowledge the completion of MetroCluster operations.

     Until you acknowledge the completion of the switchback operation, System Manager continues to display a message that the operation has completed. You cannot initiate another operation or monitor subsequent switchover or switchback operations until you acknowledge the completion of the switchback operation.

   - If the switchback operation is not successful, error messages display at the top of the status area. Make corrections if needed, and click **Switchback from Site A to Site B** to retry the process.

MetroCluster Switchover and Switchback Operations window

Beginning with System Manager 9.6, you can use the MetroCluster Switchover and Switchback Operations window to initiate a negotiated (planned) switchover or an unplanned switchover from one site or cluster (Site B) to another site or cluster (Site A). After you perform maintenance or repairs on Site B, you can initiate a switchback from Site A to Site B and view the status of the operation in this window.

Command Buttons

- **Switchover Site B to Site A**

  Initiates the process that switches Site B over to Site A.

- **Switchback Site A to Site B**

  Initiates the process that switches Site A back to Site B.

Other actions

- **Navigate to Site B cluster**

  Enter the cluster management IP address of Site B.

- **Checkbox for unplanned switchover**

  If you want to initiate an unplanned switchover, check the box labeled **Continue with unplanned switchover**.

Status areas

As the system progresses through the process of switching over or switching back, System Manager displays status with the following methods:

- **Progress line graphic**

  Displays phases of the operations and indicates the phases that have been completed. The phases are Switchover, Site B Operations, and Switchback.

- **Show Details**

  Displays a list of time-stamped system events as the MetroCluster operations progress.

- **Local: Site A**

  Displays a graphic of the configuration of the cluster at Site A, including the status of that site as it progresses through the phases of the operation.

- **Remote: Site B**

  Displays a graphic of the configuration of the cluster at Site B, including the status of that site as it progresses through the phases of the operation.

If you log in to Site B and view the MetroCluster Switchover and Switchback Operations window, then the status of Site A is shown as “INACTIVE” and the status of Site B is shown as “SWITCHOVER MODE”.

Configure applications with System Manager - ONTAP 9.7 and earlier

You can use predefined application templates in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create new configurations that are based on existing application templates. You can then provision instances of the application in ONTAP.

You configure applications by clicking **Applications &Tiers** > **Applications**.

If someone adds new applications using the CLI or REST API while you are viewing the list of applications, then you will not be able to view those new applications when you scroll the list.

The following applications can be configured in System Manager:

General Applications

- NAS Container (volume is exported to NFS or CIFS clients)
- General SAN Application (set of LUNs exported to the application server)

Databases

- MongoDB (over SAN)
- Oracle (over NFS or SAN)
- Oracle (Real Application Cluster over NFS or SAN)

- Microsoft SQL Server (over SAN or SMB)

Virtual Infrastructure

- Virtual Servers (with VMware, Hyper-V, or XEN)

Related information

ONTAP concepts

Provision a basic template with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to quickly provision basic templates for SAP HANA.

About this task

As the cluster administrator, you can provision applications by configuring a basic template. The example describes how to configure the **SAP HANA Server**.

Steps

1. Click **Applications & Tiers** > **Applications**
2. In the **Basic** tab, select the **SAP HANA Server** template.
3. In the **Database Details**section, specify the following:
    - Database name
    - Database size
    - Log size
    - Tempdb size
    - Number of server cores
    - Span HA Controller Notes
4. Click **Provision Storage**

Results

The SAP HANA Server application is provisioned.

Related information

Refer to Application Provisioning Settings for field descriptions

Storage service definitions for System Manager - ONTAP 9.7 and earlier

ONTAP System Manager classic (available in ONTAP 9.7 and earlier) includes predefined storage services that are mapped to corresponding minimum performance factors.

The actual set of storage services available in a cluster or SVM is determined by the type of storage that makes up an aggregate in the SVM.

The following table shows how the minimum performance factors are mapped to the predefined storage services:

Storage service	Expected IOPS (SLA)	Peak IOPS (SLO)	Minimum volume IOPS	Estimated latency	Are expected IOPS enforced?
value	128 per TB	512 per TB	75	17 ms	On AFF: Yes Otherwise: No
performance	2048 per TB	4096 per TB	500	2 ms	Yes
extreme	6144 per TB	12288 per TB	1000	1 ms	Yes

The following table defines the available storage service level for each type of media or node:

Media or node	Available storage service level
Disk	value
Virtual machine disk	value
FlexArray LUN	value
Hybrid	value
Capacity-optimized Flash	value
Solid-state drive (SSD) - non-AFF	value
Performance-optimized Flash - SSD (AFF)	extreme, performance, value

Add Microsoft SQL Server over SAN to System Manager - ONTAP 9.7 and earlier

You can use the Enhanced tab to add an instance of Microsoft SQL Server over SAN to ONTAP System Manager classic (available in ONTAP 9.7 and earlier).

About this task

The following procedure describes how to add a **Microsoft SQL Server** instance over SAN to System Manager. You can choose SMB as the export protocol only if the cluster is licensed for CIFS, which must be configured on the storage virtual machine (SVM).

Steps

1. Click **Applications & Tiers** > **Applications**
2. In the **Enhanced** tab, click **Add**
3. Select **Microsoft SQL Server instance** from the menu.

   The dropdown list includes a list of all available application types and template types.

   The Add Microsoft SQL Server Instance window is displayed.

4. Specify the following details:
    - Database name
    - Database size and the required ONTAP service level
    - Number of server cores
    - Log size and the required ONTAP service level
    - Provision for Tempdb

      Specify if the server should be provisioned for Tempdb.

    - Export Protocol (SMB or SAN)

      Specify SAN

    - Host operating system
    - LUN format
    - Host mapping
5. Click **Add Application**

Results

The Microsoft SQL Server instance over SAN is added to System Manager.

Application provisioning settings in System Manager - ONTAP 9.7 and earlier

You must provide details when setting up a basic or enhanced template for a database, server, or virtual desktop in ONTAP System Manager classic (available in ONTAP 9.7 and earlier). After an application is provisioned, you can edit the details and specify a resizing (increased size only). This section describes the fields in each template. Only the fields that are required for provisioning or editing the settings of the specific application are displayed.

Details for Microsoft SQL Database Applications over SAN

You enter the following information to provision Microsoft SQL Database applications over SAN or edit the settings:

- **Database Name**

  Mandatory: The name of the database you are configuring; this string is used as a prefix when provisioning storage for each database.

- **Database Size**

  Mandatory: The size of the database, in units of MB, GB, TB, or PB.

- **ONTAP Service Level for Database**

  Mandatory: The service level for the database.

- **Log Size**

Mandatory: The size of the database log in units of MB, GB, TB, or PB.

- **ONTAP Service Level for Log**

  Mandatory: The service level for the log.

- **Tempdb**

  Mandatory: The size of the tempdb database in units of MB, GB, TB, or PB.

- **Export Protocol**

  Mandatory: The export protocol is SAN

- **Number of Server Cores (on the SQL server)**

  Indicates the number of CPU cores on the databases server in increments of 2.

- **Span HA Controller Nodes**

  Specifies if storage objects should be created across a high-availability pair of nodes.

Details for provisioning a SAP HANA database

- **Active SAP HANA Nodes**

  The number of active SAP HANA nodes. The maximum number of nodes is 16.

- **Memory Size per HANA Node**

  The memory size of a single SAP HANA node.

- **Data Disk Size per HANA Node**

  The data disk size for each node.

  If set to 0, the memory size field above is used to calculate the size of the data area.

Details for Microsoft SQL Database Applications over SMB

You enter the following information to provision Microsoft SQL Database applications over SMB or edit the settings:

- **Database Name**

  Mandatory: The name of the database you are configuring; this string is used as a prefix when provisioning storage for each database.

- **Database Size**

  Mandatory: The size of the database, in units of MB, GB, TB, or PB.

- **Database Service Level**

  Mandatory: The service level for the database.

- **Number of Server Cores (on the SQL server)**

  Indicates the number of CPU cores on the databases server in increments of 2.

- **Log Size**

  Mandatory: The size of the database log in units of MB, GB, TB, or PB.

- **Log Service Level**

  Mandatory: The service level for the log.

- **Provision for Tempdb**

  Mandatory: Indicates whether tempdb is provisioned.

- **Export Protocol**

  Mandatory: The export protocol is SMB or SAN.

  SMB can be chosen only when the cluster is licensed for CIFS, which has been configured for the SVM.

- **Grant Access to User**

  Mandatory: The access level for the application.

- **Permission**

  Mandatory: The permission level for the application.

Details for a SQL Server Account

You enter the following information to provide full control access to the SQL server accounts:

The installation account is granted `SeSecurityPrivilege`.

- **SQL Server Service Account**

  Mandatory: This is an existing domain account; specify as `domain\user`.

- **SQL Server Agent Service Account**

  Optional: This is this domain account if SQL server agent service is configured, specify in the format domain\user.

Details for Oracle Database Applications

You enter the following information to provision Oracle database applications or edit the settings:

- **Database Name**

  Mandatory: The name of the database you are configuring; this string is used as a prefix when provisioning storage for each database.

- **Datafile Size**

  Mandatory: The size of the datafile, in units of MB, GB, TB, or PB.

- **ONTAP Service Level for Datafile**

  Mandatory: The service level for the datafile.

- **Redo Log Group Size**

  Mandatory: The size of the redo log group, in units of MB, GB, TB, or PB.

- **ONTAP Service Level for Redo Log Group**

  Mandatory: The service level for the redo log group.

- **Archive Log Size**

  Mandatory: The size of the archive log, in units of MB, GB, TB, or PB.

- **ONTAP Service Level for the Archive Log**

  Mandatory: The service level for the archive group.

- **Export Protocol**

  The export protocol: SAN or NFS

- **Initiators**

  A comma-separated list of the initiators (WWPN or IQN) in the initiator group.

- **Grant Access to Host**

  The host name to give the application access to.

Details for MongoDB Applications

You enter the following information to provision MongoDB applications or edit the settings:

- **Database Name**

  Mandatory: The name of the database you are configuring; this string is used as a prefix when provisioning storage for each database.

- **Data Set Size**

  Mandatory: The size of the datafile, in units of MB, GB, TB, or PB.

- **ONTAP Service Level for Data Set**

  Mandatory: The service level for the datafile.

- **Replication Factor**

  Mandatory: The number of replications.

- **Mapping for Primary Host**

  Mandatory: The name of primary host.

- **Mapping for Replica Host 1**

  Mandatory: The name of first host replica.

- **Mapping for Replica Host 2**

  Mandatory: Name of second host replica.

Details for Virtual Desktop Applications

You enter the following information to provision virtual desktop infrastructures (VDI) or edit the settings:

- **Average Desktop Size (used for the SAN Virtual Desktop)**

  This is used to determine the thin-provisioned size of each volume in units of MB, GB, TB, or PB.

- **Desktop Size**

  This is used to determine the size of the volumes which should be provisioned in units of MB, GB, TB, or PB.

- **ONTAP Service Level for Desktops**

  Mandatory: The service level for the datafile.

- **Number of Desktops**

  This number is used to determine the number of volumes created.

  This is not used to provision the virtual machines.

- **Select Hypervisor**

  The hypervisor used for these volumes; the hypervisor determines the correct datastore protocol. The options are VMware, Hyper-V, or XenServer/KVM.

- **Desktop Persistence**

  Determines if the desktop is persistent or nonpersistent. Selecting the desktop persistence sets the default values for the volume such as Snapshot schedules and post-process deduplication policies. Inline efficiencies are enabled by default for all volumes.

  These policies can be modified manually after provisioning.

- **Datastore Prefix**

  The value entered is used to generate the names of the datastores and, if applicable, the export policy name or share name.

- **Export Protocol**

The export protocol: SAN or NFS

- **Initiators**

  A comma-separated list of the initiators (WWPN or IQN) in the initiator group.

- **Grant Access to Host**

  The host name to give the application access to.

Initiator Details

You enter the following information to set up the initiator:

- **Initiator Group**

  You can select an existing group or create a new group.

- **Initiator Group Name**

  The name of the new initiator group.

- **Initiators**

  A comma-separated list of the initiators (WWPN or IQN) in the initiator group.

The following fields apply only to *SAP HANA* provisioning:

- **Initiator OS Type**

  The operating system type of the new initiator group.

- **FCP Portset**

  The FCP portset that the initiator group is bound to.

Host Access Configuration

You enter the following information to configure the host access to the volumes:

- **Volume Export Configuration**

  Select the export policy to apply to the volumes during creation. The options are:

  - Allow All

    This option implies that an export rule is created which permits read-write access to any clients.

  - Create Custom Policy

    This option allows you to specify a list of host IP addresses to receive read-write access.

  You can modify the volume export policy later using System Manager workflows.

- **Host IP Addresses**

  This is a comma-separated list of IP addresses.

  For NFS-based systems, a new export policy is created using the datastore prefix and a rule is created in it to give access to the list of IP.

Application Details

When the application is added, you can view the configuration settings in the **Overview** tab of the Application Details window. Other details such as NFS or CIFS Access and Permissions are displayed depending on the type of application that was set up.

- **Type**

  This is the type of general application, database, or virtual infrastructure that was created.

- **SVM**

  The name of the server virtual machine that the application was created on.

- **Size**

  The total size of the volume.

- **Available**

  The amount of space currently available in the volume.

- **Protection**

  The type of data protection configured.

You can expand the **Components** and **Volumes** panes for performance details about space used, IOPs, and latency.

The used size displayed in the Components pane is different than the used size displayed in the CLI.

Edit an application with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to edit a provisioned application to increase to storage size or to manage the Snapshot copies of the application.

About this task

As the cluster administrator, after you provision an application, you can edit it to modify the storage size. You can also create, restore, or delete Snapshot copies of the application. The example procedure that follows describes how to edit a **NAS Container** application.

Steps

1. Click **Applications & Tiers** > **Applications**

2. Click on the name of the NAS container application.

   If someone adds new applications using the CLI or REST API while you are viewing the list of applications, then you will not be able to view those new applications when you scroll the list.

   The **Overview** tab of the Application Details: nas window displays the application settings.

3. Click **Edit**.

   The Edit NAS Container: nas displays the current storage size setting and the **NFS Access - Grant Access to Host** address.

4. Modify the **Storage Total Size** value.
5. In the size units field, select from the drop-down menu to specify the correct size units (Bytes, MB, GB, or TB).
6. In the **ONTAP Service Level** field, select from the drop-down menu to specify the value.
7. Click **Save**.
8. Navigate back to the **Application Details: nas** window, and select the **Snapshot Copies**tab.

   A list of Snapshot copies for this provisioned application is displayed. You can use the **Search** field to search for Snapshot copies by name.

9. Manage the Snapshot copies by performing the following tasks as necessary:

Task	Actions
Create	Click **Create** to create a new Snapshot copy.
Restore	Click the check boxes next to the Snapshot copies you want to restore, and then click **Restore**.
Delete	Click the check boxes next to the Snapshot copies you want to delete, and then click **Delete**.

Delete an application with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to delete a provisioned application when it is no longer required.

About this task

As the cluster administrator, after you provision an application, you can delete it when you no longer require it. The example procedure that follows describes how to delete a **NAS Container** application.

Steps

1. Click **Applications & Tiers** > **Applications**
2. Click the name of the NAS container application.

If someone adds new applications using the CLI or REST API while you are viewing the list of applications, then you will not be able to view those new applications when you scroll the list.

The **Overview** tab of the Application Details: nas window displays the application settings.

3. Click **Delete**.

   A dialog box displays a warning message that asks you if you are sure you want to delete this application.

4. Click **Delete**.

Any volume deleted using the Application delete operation is not placed in the recovery queue. The volume is deleted immediately.

Applications window in System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to display a list of the applications in a storage virtual machine (SVM). The list includes detailed information about each application.

Tabs

Depending on the configuration of the cluster, System Manager displays information about applications using one of the following methods:

- **No tabs**

  Detailed information about the application, including the name, the type, storage usage, performance, and related information.

- **Two tabs**

  The display provides two tabs of information about the application.

  - **Enhanced**

    Detailed information about the application, including the name, the type, storage usage, performance, and related information.

  - **Basic**

    Basic information about the application.

List of applications

Applications for the selected SVM are displayed on the **Enhanced** tab in a list in the following ways:

- For System Manager 9.5 and earlier, up to a maximum of 32 applications are displayed in the list.
- For System Manager 9.6, the first 25 applications are displayed in the list. As you scroll to the bottom of the list, another 25 applications are added to the list. When you continue to scroll, you can continue to add 25 applications at a time to expand the list up to a maximum of 1000 applications.

List columns

The information about each application is listed on the **Enhanced** tab in the following columns.

- **Expand/collapse arrow**

  Contains an arrow that you can click to expand the information to a show a detailed view or to collapse the information back to the summary view.

- **Name**

  The name of the application.

- **Type**

  The application type.

- **Component**

  The component of the application.

- **ONTAP Service Level**

  The level of ONTAP service for the application.

- **Usage**

  A graphical bar that shows the percentage of usage.

- **Used**

  The amount of storage space used by the application.

- **Available**

  The amount of storage space still available for the application.

- **Size**

  The size of the application.

- **IOPs**

  The number of input and output operations per second (IOPs) for the application.

- **Latency**

  The amount of latency for the application.

Entry fields

The following fields can be used to modify the display of information:

- **SVM**

  Enables you to display a drop-down list of SVMs from which you can select the SVM that contains the

applications you want to display.

- **Search field**

  Enables you to type all or part of an application name to initiate a search based on the criteria you type. Only the applications with names that match the criteria are then displayed in the list.

- **Sort by field**

  Enables you to sort the list of applications based on name, size, or type.

Action icons

The following icons on the **Enhanced** tab can be used to initiate actions:

- **Add icon**

  Enables you to add an application to the selected SVM.

- **Filter icon**

  Enables you to specify the type of application you want to display in your search results.

- **Display icon**

  Enables you to switch between a list view and a card view of the application information.

Configuration update with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to configure the administration details of storage virtual machines (SVMs).

Configure the adminstration details of an SVM

You can use System Manager to quickly configure the administration details of astorage virtual machine (SVM). You can optionally delegate the administration of the SVM to SVM administrators.

About this task

As an SVM administrator, you cannot use System Manager to manage delegated SVMs. You can manage theSVMsonly by using the command-line interface (CLI).

Steps

1. Click **Configuration** > **Cluster** > **Configuration Updates**.
2. In the **SVMs** tab, select the node, and then click **Configure Administration Details**.
3. In the **Administrator Details** section, set up a password for the `vsadmin` user account.
4. If you want a dedicated LIF for SVM management, select **Create a LIF for SVM management**, and then specify the network details.

   A dedicated SVM management LIF is required for SAN protocols, where data and management protocols cannot share the same LIF. SVM management LIFs can be created only on data ports.

5. Specify the network details:

If you want to…	Then…
Specify the IP address by using a subnet	a. Select **Using a subnet**. b. In the Add Details dialog box, select the subnet from which the IP address must be assigned. For intercluster LIFs, only the subnets that are associated with the selected IPspace are displayed. c. If you want to assign a specific IP address to the interface, select **Use a specific IP address**, and then type the IP address. The IP address that you specify is added to the subnet if that IP address is not already present in the subnet range. d. Click **OK**.
Specify the IP address manually without using a subnet	a. Select **Without a subnet**. b. In the Add Details dialog box, perform the following steps: i. Specify the IP address and network mask or prefix. ii. Optional: Specify the gateway. The destination field is populated with the default value based on the family of the IP address. iii. If you do not want the default value, specify a new destination value. If a route does not exist, a new route is automatically created based on the gateway and destination. c. Click **OK**.

6. Specify a port to create a data LIF:
   a. Click **Browse**.
   b. In the **Select Network Port or Adapter** dialog box, select a port, and then click **OK**.

Configuration updates window

You can use the Configuration Updates window to update the configuration details of the cluster, storage virtual machine (SVM), and nodes.

Tabs

- **Nodes**

  Enables you to configure details of the node.

- **SVMs**

  Enables you to configure details of the SVM.

Nodes tab

Command buttons

- **Edit Node Name**

  Opens the Edit Node Name dialog box, which enables you to modify the name of the node.

- **Create Node-management LIF**

  Opens the Create Node-management LIF dialog box, which enables you to create a node-management LIF for managing a specific node.

- **Edit AutoSupport**

  Opens the Edit AutoSupport Settings dialog box, which enables you to specify an email address from which email notifications are sent and to add multiple email addresses of the host names.

SVMs tab

Command button

- **Configure Administration Details**

  Opens the Configure Administration Details dialog box, which enables you configure the administration details of the SVM.

Related information

Creating a cluster

Setting up a network when an IP address range is disabled

Use a Service Processor with System Manager - ONTAP 9.7 and earlier

You can use a Services Processor with ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to monitor and manage your storage system parameters such as temperature, voltage, current, and fan speeds.

Isolate management network traffic

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

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

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

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

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

Assign IP addresses to Service Processors

You can use System Manager to assign IP addresses to all of your Service Processors at the same time and to use these Service Processors to monitor and manage various system parameters of your storage systems.

Steps

1. Click **Configuration** > **Cluster** > **Configuration Updates**.
2. In the **Service Processor** window, click **Global Settings**.
3. In the **Global Settings** dialog box, choose the source for assigning the IP addresses:

If you want to…	Then…
Assign IP addresses automatically from a DHCP server	Select **DHCP**.
Assign IP addresses from a subnet	Select **Subnet**.
Manually provide IP addresses	Select **Manual Assignment**.

4. Click **Save**.

Edit Service Processor settings

You can modify Service Processor attributes, such as the IP address, the network mask or the prefix length, and the gateway address, by using System Manager. You can also allocate IP addresses to Service Processors that do not have any IP addresses assigned.

About this task

- You can edit the settings of a Service Processor that was assigned an IP address manually.
- You cannot edit the settings of a Service Processor that was assigned an IP address through a DHCP server or through a subnet.

Steps

1. Click **Configuration** > **Cluster** > **Service Processor**.
2. In the **Service Processor** window, select the Service Processor that you want to modify, and then click **Edit**.
3. In the **Edit Service Processor** dialog box, make the required changes, and then click **Save and Close**.

Understand the Service Processor

A Service Processor is a system-independent resource in the storage system that helps you to monitor and manage storage system parameters such as temperature, voltage, current, and fan speeds.

When the Service Processor detects an abnormal condition in any of the storage system parameters, the Service Processor logs an event, notifies ONTAP about the issue, and generates AutoSupport messages through email or through SNMP traps.

The Service Processor monitors ONTAP through a watchdog mechanism and can facilitate a quick failover to the partner node. The Service Processor also tracks numerous system events and saves the events in a log file. The events include boot progress, field-replaceable unit (FRU) changes, ONTAP generated events, and user transaction history.

The Service Processor can remotely log in and administer the storage system and can diagnose, shut down, power cycle, or reboot the system, regardless of the state of the storage system. In addition, the Service Processor provides remote diagnostic features.

The combined monitoring and managing capabilities of the Service Processor enables you to evaluate the storage system in the event of an issue, and then immediately perform effective service actions.

Service Processors window

You can use the Service Processors window to view and modify Service Processors attributes, such as the IP address, network mask (IPv4) or prefix-length (IPv6), and gateway, and to configure the IP source for a Service Processor.

Command buttons

- **Edit**

  Opens the Edit Service Processor dialog box, which enables you to modify the IP address, network mask (IPv4) or prefix-length (IPv6), and gateway information of a Service Processor.

- **Global Settings**

  Opens the Global Settings dialog box, which allows you to configure the source of IP address for all your Service Processors as one of the following: DHCP, subnet, or manual.

- **Refresh**

  Updates the information in the window.

Service processors list

- **Node**

  Specifies the node on which the Service Processor is located.

- **IP Address**

  Specifies the IP addresses of the Service Processor.

- **Status**

  Specifies the status the Service Processor, which can be online, offline, daemon offline, node offline, degraded, rebooted, or unknown.

- **MAC Address**

  Specifies the MAC address of the Service Processor.

Details area

The area below the Service Processor list displays detailed information about the Service Processor, including network details, such as the IP address, network mask (IPv4) or prefix-length (IPv6), gateway, IP source, and MAC address, as well as general details, such as the firmware version and whether automatic update of the firmware is enabled.

Related information

Setting up a network when an IP address range is disabled

Cluster peers with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to peer two clusters so that the peered clusters can coordinate and share resources between them. Peered clusters are required for data replication using SnapMirror technology and SnapVault technology, and for data replication using FlexCache volumes and SyncMirror technology in MetroCluster configurations.

Generate a peering passphrase

Beginning with System Manager 9.6, you can generate a passphrase for the local cluster IPspace and use the same passphrase in the remote cluster when creating peering relationships.

Steps

1. Click **Configuration** > **Cluster Peers**.
2. Click **Generate Peering Passphrase**.

   The Generate Peering Passphrase dialog window displays.

3. Complete the following fields:
   - **IPspace**: Select the IPspace from the pull-down menu.
   - **Passphrase Validity**: Select from the drop-down menu the duration for which you want the passphrase to be valid.
   - **SVM Permissions**: Select one of the following:
     - **All SVMs** to indicate all SVMs are permitted to access the cluster.
     - **Selected SVMs** to indicate specific SVMs that are permitted to access the cluster. Highlight the

SVM names in the field that you want to specify.

4. **Optional:** Select the checkbox if the effective cluster version of the remote cluster is earlier than ONTAP 9.6. Otherwise, the cluster peering fails to generate.
5. Click **Generate** to generate the passphrase.

   For a successful generation, a message displays that identifies your passphrase.

6. If you want to email or copy the passphrase, perform one of the following actions:
   - Click **Email passphrase details**.
   - Click **Copy passphrase**.

Modify the cluster peer passphrase

You can modify the passphrase that is provided during cluster peer creation.

Steps

1. Click **Configuration** > **Cluster Peers**.
2. Select the peered cluster, and click **Edit**

   The drop-down menu displays.

3. Click **Local Cluster Passphrase**.

   The Edit Local Cluster Passphrase dialog window displays.

4. In the **Enter Passphrase** field, enter a new passphrase, and then click **Apply**.

   The minimum required length of the passphrase is eight characters.

   The passphrase is modified immediately. However, there might be a delay before the correct authentication status is displayed.

5. Log in to the remote cluster, and perform Steps 1 through 4 to modify the passphrase in the remote cluster.

   The authentication status for the local cluster is displayed as `ok_and_offer` until you modify the passphrase in the remote cluster.

Modify LIFs that are configured for the remote cluster

You can use System Manager to modify the IPspace and intercluster logical interfaces (LIFs) that are configured for the remote cluster. You can add new intercluster IP addresses or remove existing IP addresses.

Before you begin

You must have at least one intercluster IP address to create the cluster peer relationship.

Steps

1. Click **Configuration** > **Cluster** > **Configuration Updates**.
2. Select the peered cluster, and click **Edit**

   The drop-down menu displays.

3. Click **Peer Cluster Network Parameters**.

   The Edit Peer Network Parameters dialog window displays.

4. If required, modify the following fields:
   - **IPspace**: Select the IPspace from the pull-down menu.
   - **Intercluster LIFs**: Add or remove intercluster IP addresses. You can add multiple IP addresses by separating them with commas.
5. Click **Modify**.
6. Verify the changes that you made in the **Cluster Peers** window.

Change the peering encryption status

You can use System Manager to change the peering encryption status for the selected cluster.

About this task

The encryption status can be enabled or disabled. You can change the status from enabled to disabled or from disabled to enabled by selecting **Change Encryption**.

Steps

1. Click **Configuration** > **Cluster Peers**.
2. Select the peered cluster, and click **Edit**

   The drop-down menu displays.

3. Click **Change Encryption**.

   This action is not available if the encryption status is “N/A”.

   The Change Encryption dialog window displays. The toggle button indicates the current encryption status.

4. Slide the toggle button to change the peering encryption status and proceed.
   - If the current encryption status is “none”, you can enable encryption by sliding the toggle button to change the status to “tls_psk”.
   - If the current encryption status is “tls_psk”, you can disable the encryption by sliding the toggle button to change the status to “none”.
5. After you enable or disable peering encryption, you can either generate a new passphrase and provide it at the peered cluster or you can apply an existing passphrase that was already generated at the peered cluster.

   > If the passphrase used on the local site does not match the passphrase used on the remote site, the cluster peering relationship will not function properly.

   Select one of the following:

   - **Generate a passphrase**: Proceed to step 6.
   - **Already have a passphrase**: Proceed to step 9.
6. If you chose **Generate a passphrase**, complete the necessary fields:
   - **IPspace**: Select the IPspace from the drop-down menu.

- **Passphrase Validity**: Select from the drop-down menu the duration for which you want the passphrase to be valid.
- **SVM Permissions**: Select one of the following:
  - **All SVMs** to indicate that all SVMs are permitted to access the cluster.
  - **Selected SVMs** to indicate specific SVMs that are permitted to access the cluster. Highlight the SVM names in the field that you want to specify.

7. **Optional:** Select the checkbox if the effective cluster version of the remote cluster is earlier than ONTAP 9.6. Otherwise, the passphrase fails to generate.
8. Click **Apply**.

   The passphrase is generated for the relationship and displayed. You can either copy the passphrase or email it.

   The authentication status for the local cluster is displayed as `ok_and_offer` for the selected passphrase validity period until you provide the passphrase at the remote cluster.

9. If you already generated a new passphrase in the remote cluster, then perform the following substeps:
   a. Click **Already have a passphrase**.
   b. Enter in the **Passphrase** field the same passphrase that was generated in the remote cluster.
   c. Click **Apply**.

Delete cluster peer relationships

You can use System Manager to delete a cluster peer relationship if the relationship is no longer required. You must delete the cluster peering relationship from each of the clusters in the peer relationship.

Steps

1. Click **Configuration** > **Cluster Peers**.
2. Select the cluster peer for which you want to delete the relationship, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.
4. Log in to the remote cluster, and perform Steps 1 through 3 to delete the peer relationship between the local cluster and the remote cluster.

   The status of the peer relationship is displayed as “unhealthy” until the relationship is deleted from both the local cluster and the remote cluster.

Cluster Peers window

You can use the Cluster Peers window to manage peer cluster relationships, which enables you to move data from one cluster to another.

Command buttons

- **Create**

  Opens the Create Cluster Peering dialog box, which enables you to create a relationship with a remote cluster.

- **Edit**

Displays a drop-down menu with the following choices:

- **Local Cluster Passphrase**

  Opens the Edit Local Cluster Passphrase dialog box, which enables you to enter a new passphrase to validate the local cluster.

- **Peer Cluster Network Parameters**

  Opens the Edit Peer Cluster Network Parameters dialog box, which enables you to modify the IPspace and add or remove intercluster LIF IP addresses.

  You can add multiple IP addresses, separated by commas.

- **Change Encryption**

  Opens the Change Encryption dialog box for the selected peer cluster. While you are changing the encryption of the peered relationship, you can either generate a new passphrase or provide a passphrase that was already generated at the remote peered cluster.

  This action is not available if the encryption status is “N/A”.

- **Delete**

  Opens the Delete Cluster Peer Relationship dialog box, which enables you to delete the selected peer cluster relationship.

- **Refresh**

  Updates the information in the window.

- **Manage SVM Permissions**

  Enables SVMs to automatically accept SVM peering requests.

- **Generate Peering Passphrase**

  Enables you to generate a passphrase for the local cluster IPspace by specifying the IPspace, setting the passphrase validity duration, and specifying which SVMs are given permission.

  You use the same passphrase in the remote cluster for peering.

Peer cluster list

- **Peer Cluster**

  Specifies the name of the peer cluster in the relationship.

- **Availability**

  Specifies whether the peer cluster is available for communication.

- **Authentication Status**

  Specifies whether the peer cluster is authenticated or not.

- **Local Cluster IPspace**

  Displays IPspace associated with the local cluster peer relationship.

- **Peer Cluster Intercluster IP Addresses**

  Displays IP addresses associated with the intercluster peer relationship.

- **Last Updated Time**

  Displays the time at which peer cluster was last modified.

- **Encryption**

  Displays the status of the encryption of the peering relationship.

  Starting with System Manager 9.6, peering is encrypted by default when you establish a peering relationship between two clusters

  - **N/A**: Encryption is not applicable to the relationship.
  - **none**: The peering relationship is not encrypted.
  - **tls_psk**: The peering relationship is encrypted.

Create high availability pairs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create high availability (HA) pairs that provide hardware redundancy that is required for nondisruptive operations and fault tolerance.

High Availability window

The High Availability window provides a pictorial representation of the high-availability (HA) state, interconnect status, and takeover or giveback status of all of the HA pairs in ONTAP. You can also manually initiate a takeover operation or giveback operation by using the High Availability window.

You can view details such as the takeover or giveback status and the interconnect status by clicking the HA pair image.

The color indicates the HA pair status:

- Green: Indicates that the HA pair and the interconnect are optimally configured and available for takeover or giveback.

  Green also indicates the takeover in progress state, giveback in progress state, and waiting for giveback state.

- Red: Indicates a downgraded state such as a takeover failure.
- Yellow: Indicates that the interconnect status is down.

When multiple HA pairs in a cluster are simultaneously involved in storage failover operations, the cluster status that is displayed is based on the status and severity of the HA pair. The following order of severity is considered while displaying the cluster status: takeover in progress, giveback in progress, waiting for giveback.

Actions

You can perform tasks such as takeover or giveback based on the status of the nodes in the HA pair.

- Takeover `node_name`

  Enables you to perform a takeover operation when maintenance is required on the partner node.

- Giveback `node_name`

  Enables you to perform a giveback operation when the partner node that has been taken over is waiting for giveback or is in a partial giveback state.

- Enable or Disable automatic giveback

  Enables or disables the automatic giveback operation.

  Automatic giveback is enabled by default.

Command buttons

- **Refresh**

  Updates the information in the window.

  The information that is displayed in the High Availability window is automatically refreshed every 60 seconds.

Related information

Monitoring HA pairs

Manage licenses with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to view, manage, or delete any software licenses installed on a cluster or node.

Delete licenses

You can use the Licenses window in System Manager to delete any software license that is installed on a cluster or a node.

For information about managing licenses using ONTAP 9.8 and later, see the following information:

- Manage licenses overview (cluster administrators only)
- Enable new features by adding license keys

Before you begin

The software license that you want to delete must not be used by any service or feature.

Steps

1. Click **Configuration** > **Cluster** > **Licenses**.
2. In the **Licenses** window, perform the appropriate action:

If you want to…	Do this…
Delete a specific license package on a node or a master license	Click the **Details** tab.
Delete a specific license package across all of the nodes in the cluster	Click the **Packages** tab.

3. Select the software license package that you want to delete, and then click **Delete**.

   You can delete only one license package at a time.

4. Select the confirmation check box, and then click **Delete**.

Results

The software license is deleted from your storage system. The deleted license is also removed from the list of licenses in the Licenses window.

License types and entitlement risk

Understanding the various license types and the associated entitlement risk helps you manage the risk that is associated with the licenses in a cluster.

License types

A package can have one or more of the following types of licenses installed in the cluster:

- Node-locked license or standard license

  A node-locked license is issued for a node with a specific system serial number (also known as a *controller serial number*). This license is valid only for the node that has the matching serial number.

  Installing a node-locked license entitles a node to the licensed functionality. For the cluster to use the licensed functionality, at least one node must be licensed for the functionality. It might be out of compliance to use the licensed functionality on a node that does not have an entitlement for the functionality.

  ONTAP 8.2 and later releases treat a license that was installed prior to Data ONTAP 8.2 as a standard license. Therefore, in ONTAP 8.2 and later releases, all of the nodes in the cluster automatically have the standard license for the package that the previously licensed functionality is part of.

- Master or site license

  A master or site license is not tied to a specific system serial number. When you install a site license, all of the nodes in the cluster are entitled to the licensed functionality.

  If your cluster has a master license and you remove a node from the cluster, the node does not carry the site license with it, and the node is no longer entitled to the licensed functionality. If you add a node to a cluster that has a master license, the node is automatically entitled to the functionality that is granted by the site license.

- Demo or temporary license

  A demo or temporary license expires after a certain period of time. This license enables you to try certain software functionality without purchasing an entitlement. A temporary license is a cluster-wide license, and is not tied to a specific serial number of a node.

  If your cluster has a temporary license for a package and you remove a node from the cluster, the node does not carry the evaluation license with it.

- Capacity license (ONTAP Select and FabricPool only)

  An ONTAP Select instance is licensed according to the amount of data that the user wants to manage. For example, the user might buy a 10 TB capacity license to enable ONTAP Select to manage up to 10 TB of data. If more storage capacity is attached to the system than ONTAP Select is licensed to manage, ONTAP Select will not operate. By default, the maximum storage capacity that can be attached to an ONTAP Select instance is 2 TB until a capacity license (for example, a 5 TB capacity license, a 10 TB capacity license, and so on) is purchased and installed.

  Starting with ONTAP 9.2, FabricPool-enabled aggregates require a capacity license to be used with a third-party storage tier (for example, AWS). The FabricPool capacity license defines the amount of data that can be stored in the cloud tier storage.

Entitlement risk

An entitlement risk arises because of the non-uniform installation of a node-locked license. If the node-locked license is installed on all the nodes, there is no entitlement risk.

The entitlement risk level can be high risk, medium risk, no risk, or unknown risk depending on certain conditions:

- High risk
  - If there is usage on a particular node, but the node-locked license is not installed on that node
  - If the demo license that was installed on the cluster expires, and there is usage on any node

  If a site license is installed on a cluster, the entitlement risk is never high.

- Medium risk

  If a site license is not installed, and the node-locked license is non-uniformly installed on the nodes in a cluster

- No risk

  There is no entitlement risk if a node-locked license is installed on all of the nodes, or a site license is installed on the cluster, irrespective of usage.

- Unknown

  The risk is unknown if the API is sometimes unable to retrieve the data related to entitlement risk that is associated with a cluster or the nodes in the cluster.

Licenses window

Your storage system arrives from the factory with preinstalled software. If you want to add or remove a software license after you receive the storage system, you can use the Licenses window.

System Manager does not monitor evaluation licenses and does not provide any warning when an evaluation license is nearing expiry. An evaluation license is a temporary license that expires after a certain period of time.

Command buttons

- **Add**

  Opens the Add License window, which enables you to add new software licenses.

- **Delete**

  Deletes the software license that you select from the software license list.

- **Refresh**

  Updates the information in the window.

Packages tab

Displays information about the license packages that are installed on your storage system.

- **Package**

  Displays the name of the license package.

- **Entitlement Risk**

  Indicates the level of risk as a result of license entitlement issues for a cluster. The entitlement risk level can be high risk (), medium risk (), no risk (), unknown (), or unlicensed (-).

- **Description**

  Displays the level of risk as a result of license entitlement issues for a cluster.

License Package details area

The area below the license packages list displays additional information about the selected license package. This area includes information about the cluster or node on which the license is installed, the serial number of the license, usage in the previous week, whether the license is installed, the expiration date of the license, and whether the license is a legacy one.

Details tab

Displays additional information about the license packages that are installed on your storage system.

- **Package**

  Displays the name of the license package.

- **Cluster/Node**

  Displays the cluster or node on which the license package is installed.

- **Serial Number**

  Displays the serial number of the license package that is installed on the cluster or node.

- **Type**

  Displays the type of the license package, which can be the following:

  - Temporary: Specifies that the license is a temporary license, which is valid only during the demonstration period.
  - Master: Specifies that the license is a master license, which is installed on all the nodes in the cluster.
  - Node Locked: Specifies that the license is a node-locked license, which is installed on a single node in the cluster.
  - Capacity:
    - For ONTAP Select, specifies that the license is a capacity license, which defines the total amount of data capacity that the instance is licensed to manage.
    - For FabricPool, specifies that the license is a capacity license, which defines the amount of data that can be managed in the attached third-party storage (for example, AWS).

- **State**

  Displays the state of the license package, which can be the following:

  - Evaluation: Specifies that the installed license is an evaluation license.
  - Installed: Specifies that the installed license is a valid purchased license.
  - WARNING: Specifies that the installed license is a valid purchased license and is approaching maximum capacity.
  - Enforcement: Specifies that the installed license is a valid purchased license and has exceeded the expiry date.
  - Waiting for License: Specifies that the license has not yet been installed.

- **Legacy**

  Displays whether the license is a legacy license.

- **Maximum Capacity**
  - For ONTAP Select, displays the maximum amount of storage that can be attached to the ONTAP Select instance.
  - For FabricPool, displays the maximum amount of third-party object store storage that can be used as cloud tier storage.
- **Current Capacity**
  - For ONTAP Select, displays the total amount of storage that is currently attached to the ONTAP Select instance.
  - For FabricPool, displays the total amount of third-party object store storage that is currently used as cloud tier storage.

- **Expiration Date**

  Displays the expiration date of the software license package.

Related information

System administration

Creating a cluster

Cluster Expansion with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to increase the size and capabilities of your storage by adding compatible nodes to the cluster and configuring the node network details. You can also view the summary of the nodes.

When you log in to System Manager, System Manager automatically detects compatible nodes that have been cabled but have not been added to the cluster and prompts you to add the nodes. You can add compatible nodes as and when System Manager detects the nodes or you can manually add the nodes at a later time.

Add nodes to a cluster

You can use System Manager to increase the size and capabilities of your storage system by adding nodes to an existing cluster.

Before you begin

- New compatible nodes must be cabled to the cluster.

  Only the ports that are in the default broadcast domain will be listed in the Network window.

- All of the nodes in the cluster must be up and running.
- All of the nodes must be of the same version.

Steps

1. Add the new compatible nodes to the cluster:

If you are…	Do this…
Not logged in to System Manager	a. Log in to System Manager. The new compatible nodes are automatically detected by System Manager at login. System Manager prompts you to add the new compatible nodes to the cluster. b. Click **Add Nodes to Cluster**. c. Modify the name of the nodes. d. Specify the node licenses. e. Click **Submit and Proceed**.
Logged in to System Manager	a. Click **Configuration** > **Cluster** > **Expansion**. System Manager searches for newly added nodes. If any warnings are displayed, you must fix them before proceeding. If new compatible nodes are discovered, proceed to the next step. b. Modify the name of the nodes. c. Specify the node licenses. d. Click **Submit and Proceed**.

Configure the network details of the nodes

You can use System Manager to configure the node management LIF and Service Processor settings for the newly added nodes.

Before you begin

- Sufficient number of ports must be present in the default IPspace for LIF creation.
- All the ports must be up and running.

Steps

1. Configure node management:
   a. Enter the IP address in the **IP Address** field.
   b. Select the port for node management in the **Port** field.
   c. Enter the netmask and gateway details.
2. Configure Service Processor settings:
   a. Select the **Override defaults** check box to override the default values.
   b. Enter the IP address, netmask, and gateway details.
3. Click **Submit and Proceed** to complete the network configuration of the nodes.

4. Verify the details of the nodes in the **Summary** page.

What to do next

- If your cluster is protected, you should create the required number of intercluster LIFs in the newly added nodes to avoid partial peering and unhealthy protection.
- If SAN data protocols are enabled in your cluster, you should create the required number of SAN Data LIFs for serving data.

Related information

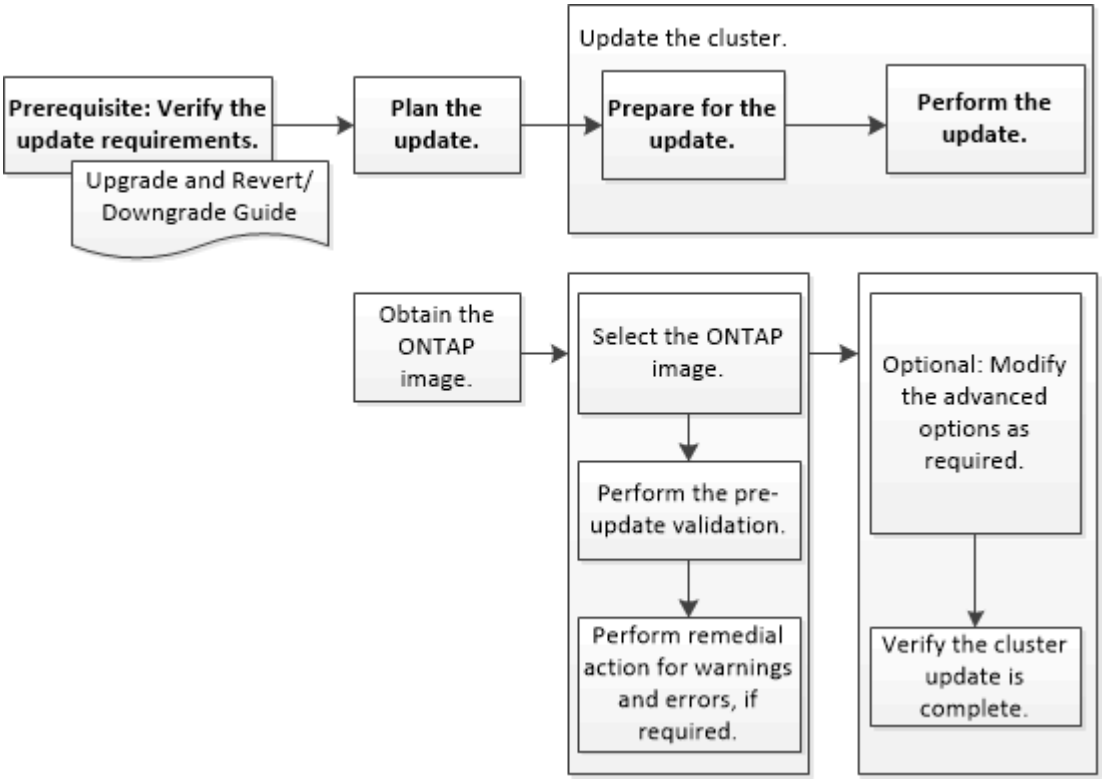
Creating network interfaces

Update clusters with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to update a cluster or the individual nodes in a high-availability (HA) pair. You can also update a cluster in a MetroCluster configuration.

Update clusters in a non MetroCluster configuration with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to update a cluster or the individual nodes in a high-availability (HA) pair. To perform an update, you should select an ONTAP image, validate that your cluster or the individual nodes in the HA pair are ready for the update, and then perform the update.

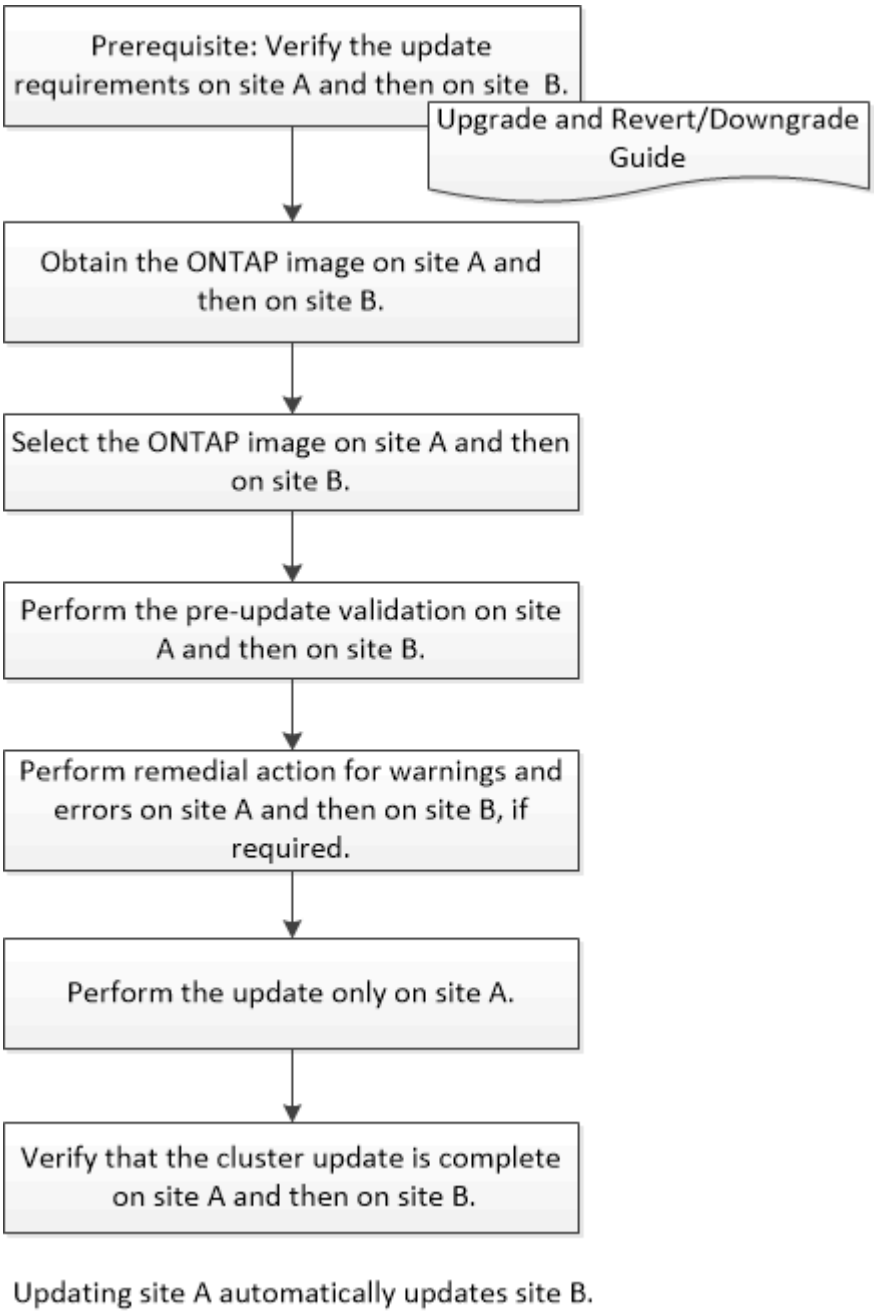


Related information

Upgrade ONTAP

Update clusters in a MetroCluster configuration with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to update a cluster in MetroCluster configurations. You must perform each operation on both the clusters except for updating the cluster.



Updating site A automatically updates site B.

Related information

Upgrade ONTAP

Obtain ONTAP software images with System Manager - ONTAP 9.7 and earlier

You can obtain ONTAP software images with ONTAP System Manager classic (available in ONTAP 9.7 and earlier). For ONTAP 9.4 and later, you can copy the ONTAP software

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

About this task

To upgrade the cluster to the target release of ONTAP, you require access to software images. Software images, firmware version information, and the latest firmware for your platform model are available on the NetApp Support Site. You should note the following important information:

- Software images are specific to platform models.

  You must obtain the correct image for your cluster.

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

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

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

Steps

1. Locate the target ONTAP software in the **Software Downloads** area of the NetApp Support Site.
2. Copy the software image.
   - For ONTAP 9.3 or earlier, copy the software image (for example, `93_q_image.tgz`) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served
   - For ONTAP 9.4 or later, copy the software image (for example, `97_q_image.tgz`) from the NetApp Support Site to the directory on the HTTP server or FTP server from which the image will be served or to a local folder.

Update single-node clusters with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to update single-node clusters.

Before you begin

- The clusters must be running ONTAP 9.4 or later.
- You must have copied the software image from the NetApp Support Site to an HTTP server on your network, to an FTP server on your network, or to your local system so that the nodes can access the image.

  Obtaining ONTAP software images

About this task

- Beginning with System Manager 9.5, you can update single-node clusters in two-pack MetroCluster configurations.

  You must perform this operation on both the sites.

- Updating single-node clusters in MetroCluster configurations is not disruptive.

  The System Manager user interface is not available while the cluster is rebooting.

- In System Manager 9.4 and later, you can update single-node clusters in non-MetroCluster configurations.

  Updating single-node clusters in non-MetroCluster configurations is disruptive. The client data is not available while the update is in progress.

- If you try to perform other tasks while updating the node that hosts the cluster management LIF, an error message might be displayed.

  You must wait for the update to finish before performing any operations.

- If the NVMe protocol is configured in System Manager 9.4 and you perform an update from System Manager 9.4 to System Manager 9.5, then the NVMe protocol is available for a grace period of 90 days without a license.

  This feature is not available in MetroCluster configurations.

- If the NVMe protocol is not configured in System Manager 9.5 and you perform an update from System Manager 9.5 to System Manager 9.6, then the grace period is not provided, and you must install the NVMe license to use the NVMe protocol.

  This feature is not available in MetroCluster configurations.

Steps

1. Click **Configuration** > **Cluster** > **Update**.
2. In the **Cluster Update** tab, add a new software image or select an available software image.

If you want to…	Then…
Add a new software image from the local client	a. Click **Add from Local Client**. b. Search for the software image, and then click **Open**.
Add a new software image from the NetApp Support Site	a. Click **Add from Server**. b. In the Add a New Software Image dialog box, enter the URL of the HTTP server or FTP server on which you have saved the image that was downloaded from the NetApp Support Site. For anonymous FTP, you must specify the URL in the `ftp://anonymous@ftpserver` format. c. Click **Add**.
Select an available image	Choose one of the listed images.

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

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

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

4. Click **Next**.
5. Click **Update**.

   Validation is performed again.

   - When the validation is complete, a table displays any errors and warnings, along with any required remedial actions to be taken before proceeding.
   - If the validation is completed with warnings, you can choose to select the **Continue update with warnings** checkbox, and then click **Continue**.
     When the validation is complete and the update is in progress, the update might be paused because of errors. You can click the error message to view the details, and then perform the remedial actions before resuming the update.

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

6. Log in to System Manager, and verify that the cluster is successfully updated to the selected version by clicking **Configuration** > **Cluster** > **Update** > **Update History**, and then viewing the details.

Update a cluster nondisruptively with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to update a cluster or individual nodes in high-availability (HA) pairs that are running ONTAP 8.3.1 or later to a specific version of ONTAP software without disrupting access to client data.

Before you begin

- All of the nodes must be in HA pairs.
- All of the nodes must be healthy.
- You must have copied the software image from the NetApp Support Site to an HTTP server or FTP server on your network so that the nodes can access the image.

  Obtaining ONTAP software images

About this task

- If you try to perform other tasks from System Manager while updating the node that hosts the cluster management LIF, an error message might be displayed.

  You must wait for the update to finish before performing any operations.

- A rolling update is performed for clusters with fewer than eight nodes, and a batch update is performed for clusters with more than eight nodes.

In a rolling update, the nodes in the cluster are updated one at a time. In a batch update, multiple nodes are updated in parallel.

- You can nondisruptively update ONTAP software from one long-term service (LTS) release to the next LTS release (LTS+1).

  For example, if ONTAP 9.1 and ONTAP 9.3 are LTS releases, you can nondisruptively update your cluster from ONTAP 9.1 to ONTAP 9.3.

- Beginning with System Manager 9.6, if the NVMe protocol is configured in System Manager 9.5 and you perform an upgrade from System Manager 9.5 to System Manager 9.6, you no longer have a grace period of 90 days to have the NVMe protocol available without a license. If the grace period is in effect when you upgrade from ONTAP 9.5 to 9.6, the grace period must be replaced with a valid NVMeoF license so you can continue to use the NVMe features.

  This feature is not available in MetroCluster configurations.

- If the NVMe protocol is not configured in System Manager 9.5 and you perform an update from System Manager 9.5 to System Manager 9.6, then the grace period is not provided, and you must install the NVMe license to use the NVMe protocol.

  This feature is not available in MetroCluster configurations.

- Beginning with ONTAP 9.5, at least one NVMe LIF must be configured for each node in an HA pair using the NVMe protocol. You can also create a maximum of two NVMe LIFs per node. When you upgrade to ONTAP 9.5, you must ensure that a minimum of one NVMe LIF is defined for each node in an HA pair using the NVMe protocol.

Steps

1. Click **Configuration** > **Cluster** > **Update**.
2. In the **Update** tab, add a new image or select an available image.

If you want to…	Then…
Add a new software image from the local client	a. Click **Add from Local Client**. b. Search for the software image, and then click **Open**.
Add a new software image from the NetApp Support Site	a. Click **Add from Server**. b. In the Add a New Software Image dialog box, enter the URL of the HTTP server or FTP server on which you have saved the image that was downloaded from the NetApp Support Site. For anonymous FTP, you must specify the URL in the `ftp://anonymous@ftpserver` format. c. Click **Add**.
Select an available image	Choose one of the listed images.

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

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

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

4. Click **Next**.
5. Click **Update**.

   Validation is performed again.

   - When the validation is complete, a table displays any errors and warnings, along with any required remedial actions to be taken before proceeding.
   - If the validation is completed with warnings, you can choose to select the **Continue update with warnings** checkbox, and then click **Continue**.
     When the validation is complete and the update is in progress, the update might be paused because of errors. You can click the error message to view the details, and then perform the remedial actions before resuming the update.

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

6. Log in to System Manager and verify that the cluster is successfully updated to the selected version by clicking **Configuration** > **Cluster** > **Update** > **Update History**, and then viewing the details.

Related information

How to update a cluster nondisruptively

Cluster Update window with System Manager - ONTAP 9.7 and earlier

You can use the Cluster Update window to perform an automated cluster update nondisruptively or you can update single-node clusters disruptively with ONTAP System Manager classic (available in ONTAP 9.7 and earlier).

Tabs

- **Cluster Update**

  Enables you to perform an automated cluster update nondisruptively or you can update single-node clusters disruptively.

- **Update History**

  Displays the details of previous cluster updates.

Cluster Update tab

The Cluster Update tab enables you perform an automated cluster update nondisruptively or you can update single-node clusters disruptively.

Command buttons

- **Refresh**

  Updates the information in the window.

- **Select**

  You can select the version of the software image for the update.

  - Cluster Version Details: Displays the current cluster version in use and the version details of the nodes or high-availability (HA) pairs.
  - Available Software Images: Enables you to select an existing software image for the update.

    Alternatively, you can download a software image from the NetApp Support Site and add the image for the update.

- **Validate**

  You can view and validate the cluster against the software image version for the update. A pre-update validation checks whether the cluster is in a state that is ready for an update. If the validation is completed with errors, a table displays the status of the various components and the required corrective action for the errors.

  You can perform the update only when the validation is completed successfully.

- **Update**

  You can update all of the nodes in the cluster or an HA pair in the cluster to the selected version of the software image. While the update is in progress, you can choose to pause the update, and you can then either cancel or resume the update.

  If an error occurs, the update is paused and an error message is displayed with the remedial steps. You can choose to either resume the update after performing the remedial steps or cancel the update. You can view the table with the node name, uptime, state, and ONTAP version when the update is successfully completed.

Update History tab

Displays details about the cluster update history.

Update History list

- **Image Version**

  Specifies the version of the ONTAP image to which the node will be updated.

- **Software Updates Installed on**

  Specifies the type of disk on which the updates are installed.

- **Status**

  Specifies the status of the software image update (whether the update is successful or cancelled).

- **Start Time**

  Specifies the time when the update was started.

- **Completion Time**

  Specifies the time when the update was completed.

  This field is hidden by default.

- **Time Taken for the Update**

  Specifies the time taken for the update to finish.

- **Previous Version**

  Specifies the ONTAP version of the node before the update.

- **Updated Version**

  Specifies the ONTAP version of the node after the update.

Manage the date and time settings of a cluster with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage the date and time settings of a cluster.

Date and Time window

The Date and Time window enables you to view the current date and time settings for your storage system and to modify the settings when required.

Command buttons

- **Edit**

  Opens the Edit Date and Time dialog box, which enables you to edit the time servers.

- **Refresh**

  Updates the information in the window.

Details area

The details area displays information about the date, time, time zone, NTP service, and time servers for your storage system.

Related information

Setting the time zone for a cluster

Setting up a network when an IP address range is disabled

Configure SNMP with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to configure SNMP to monitor SVMs in your cluster.

Enable or disable SNMP

You can enable or disable SNMP on your clusters by using System Manager. SNMP enables you to monitor the storage virtual machines (SVMs) in a cluster to avoid issues before they can occur and to prevent issues from occurring.

Steps

1. Click ⚙.
2. In the **Setup** pane, click **SNMP**.
3. In the **SNMP** window, click either **Enable** or **Disable**.

Edit SNMP information

You can use the Edit SNMP Settings dialog box in System Manager to update information about the storage system location and contact personnel, and to specify the SNMP communities of your system.

About this task

System Manager uses the SNMP protocols SNMPv1 and SNMPv2c and an SNMP community to discover storage systems.

Steps

1. Click ⚙.
2. In the **Setup** pane, click **SNMP**.
3. Click **Edit**.
4. In the **General** tab, specify the contact personnel information and location information for the storage system, and the SNMP communities.

   The community name can be of 32 characters and must not contain the following special characters: , / : " ' |.

5. In the **SNMPv3**tab, do the following:
   a. Click **Add** to add an SNMPv3 user.
   b. Specify the username and modify the engine ID, if required.
   c. Select the **Authentication Protocol** and enter your credentials.
   d. Select the **Privacy Protocol** and enter your credentials.
   e. Click **OK** to save the changes.
6. Click **OK**.
7. Verify the changes that you made to the SNMP settings in the **SNMP** window.

Enable or disable SNMP traps

SNMP traps enable you to monitor the health and state of the various components of your storage system. You can use the Edit SNMP Settings dialog box in System Manager to enable or disable SNMP traps on your storage system.

About this task

Although SNMP is enabled by default, SNMP traps are disabled by default.

Steps

1. Click .
2. In the **Setup** pane, click **SNMP**.
3. In the **SNMP** window, click **Edit**.
4. In the **Edit SNMP Settings** dialog box, select the **Trap hosts** tab, and then select or clear the **Enable traps** check box to enable or disable SNMP traps, respectively.
5. If you enable SNMP traps, add the host name or IP address of the hosts to which the traps are sent.
6. Click **OK**.

Test the trap host configuration

You can use System Manager to test whether you have configured the trap host settings correctly.

Steps

1. Click .
2. In the **Setup** pane, click **SNMP**.
3. In the **SNMP** window, click **Test Trap Host**.
4. Click **OK**.

SNMP window

The SNMP window enables you to view the current SNMP settings for your system. You can also change your system's SNMP settings, enable SNMP protocols, and add trap hosts.

Command buttons

- **Enable/Disable**

  Enables or disables SNMP.

- **Edit**

  Opens the Edit SNMP Settings dialog box, which enables you to specify the SNMP communities for your storage system and enable or disable traps.

- **Test Trap Host**

  Sends a test trap to all the configured hosts to check whether the test trap reaches all the hosts and whether the configurations for SNMP are set correctly.

- **Refresh**

Updates the information in the window.

Details

The details area displays the following information about the SNMP server and host traps for your storage system:

- **SNMP**

  Displays whether SNMP is enabled or not.

- **Traps**

  Displays if SNMP traps are enabled or not.

- **Location**

  Displays the address of the SNMP server.

- **Contact**

  Displays the contact details for the SNMP server.

- **Trap host IP Address**

  Displays the IP addresses of the trap host.

- **Community Names**

  Displays the community name of the SNMP server.

- **Security Names**

  Displays the security style for the SNMP server.

Related information

Network management

Configure an LDAP server with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to configure an LDAP server that centrally maintains user information.

View the LDAP client configuration

You can use System Manager to view the LDAP clients that are configured for a storage virtual machine (SVM) in a cluster.

Steps

1. Click .
2. In the **Setup** pane, click **LDAP**.

   The list of LDAP clients are displayed in the LDAP window.

Use LDAP services

An LDAP server enables you to centrally maintain user information. If you store your user database on an LDAP server in your environment, you can configure your storage virtual machine (SVM) to look up user information in your existing LDAP database.

About this task

ONTAP supports LDAP for user authentication, file access authorization, and user lookup and mapping services between NFS and CIFS.

LDAP window

You can use the LDAP window to view LDAP clients for user authentication, file access authorization, and user search, and to map services between NFS and CIFS at the cluster level.

Command buttons

- **Add**

  Opens the Create LDAP Client dialog box, which enables you to create and configure LDAP clients.

- **Edit**

  Opens the Edit LDAP Client dialog box, which enables you to edit LDAP client configurations. You can also edit active LDAP clients.

- **Delete**

  Opens the Delete LDAP Client(s) dialog box, which enables you to delete LDAP client configurations. You can also delete an active LDAP client.

- **Refresh**

  Updates the information in the window.

LDAP client list

Displays (in tabular format) details about LDAP clients.

- **LDAP Client Configuration**

  Displays the name of the LDAP client configuration that you specified.

- **Storage Virtual Machine**

  Displays the name of the storage virtual machine (SVM) for each LDAP client configuration.

- **Schema**

  Displays the schema for each LDAP client.

- **Minimum Bind Level**

  Displays the minimum bind level for each LDAP client.

- **Active Directory Domain**

  Displays the Active Directory domain for each LDAP client configuration.

- **LDAP Servers**

  Displays the LDAP server for each LDAP client configuration.

- **Preferred Active Directory Servers**

  Displays the preferred Active Directory server for each LDAP client configuration.

Related information

Adding an LDAP client configuration

Deleting an LDAP client configuration

Editing an LDAP client configuration

Manage user accounts with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to add, edit, and manage a cluster user account, and specify a login user method to access the storage system.

Add a cluster user account

You can use System Manager to add a cluster user account and to specify a user login method for accessing the storage system.

About this task

In clusters on which SAML authentication is enabled, for a particular application, you can add either SAML authentication or password-based authentication, or you can add both types of authentication.

Steps

1. Click ⚙.
2. In the **Management** pane, click **Users**.
3. Click **Add**.
4. Type a user name for the new user.
5. Type a password for the user to connect to the storage system, and then confirm the password.
6. Add one or more user login methods, and then click **Add**.

Edit a cluster user account

You can use System Manager to edit a cluster user account by modifying the user login methods for accessing the storage system.

Steps

1. Click ⚙.

2. In the **Management** pane, click **Users**.
3. In the **Users** window, select the user account that you want to modify, and then click **Edit**.
4. In the **Modify User** dialog box, modify the user login methods, and then click **Modify**.

Change passwords for cluster user accounts

You can use System Manager to reset the password for a cluster user account.

Steps

1. Click ⚙.
2. In the **Management** pane, click **Users**.
3. Select the user account for which you want to modify the password, and then click **Change Password**.
4. In the **Change Password** dialog box, type the new password, confirm the new password, and then click **Change**.

Lock or unlock cluster user accounts

You can use System Manager to lock or unlock cluster user accounts.

Steps

1. Click ⚙.
2. In the **Management** pane, click **Users**.
3. Select the user account for which you want to modify the status, and click either **Lock** or **Unlock**.

User accounts (cluster administrators only)

You can create, modify, lock, unlock, or delete a cluster user account, reset a user's password, or display information about all user accounts.

You can manage cluster user accounts in the following ways:

- Creating a login method for a user by specifying the user's account name, the access method, the authentication method, and, optionally, the access-control role that the user is assigned
- Displaying users' login information, such as the account name, allowed access method, authentication method, access-control role, and account status
- Modifying the access-control role that is associated with a user's login method

> ⓘ It is best to use a single role for all the access and authentication methods of a user account.

- Deleting a user's login method, such as the access method or the authentication method
- Changing the password for a user account
- Locking a user account to prevent the user from accessing the system
- Unlocking a previously locked user account to enable the user to access the system again

Users window

You can use the Users window to manage user accounts, to reset the password of a user, and to view

information about all of the user accounts.

Command buttons

- **Add**

  Opens the Add User dialog box, which enables you to add user accounts.

- **Edit**

  Opens the Modify User dialog box, which enables you to modify user login methods.

  It is a best practice to use a single role for all of the access and authentication methods of a user account.

- **Delete**

  Enables you to delete a selected user account.

- **Change Password**

  Opens the Change Password dialog box, which enables you to reset a selected user's password.

- **Lock**

  Locks the user account.

- **Refresh**

  Updates the information in the window.

Users list

The area below the users list displays detailed information about the selected user.

- **User**

  Displays the name of the user account.

- **Account Locked**

  Displays whether the user account is locked.

User Login Methods area

- **Application**

  Displays the access method that a user can use to access the storage system. The supported access methods include the following:

  - System console (console)
  - HTTP(S) (http)
  - ONTAP API (ontapi)

- Service Processor (service-processor)
- SSH (ssh)

- **Authentication**

  Displays the default supported authentication method, which is “password”.

- **Role**

  Displays the role of a selected user.

Manage roles with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create access-controlled user roles.

Add roles

You can use System Manager to add an access-control role and to specify the command or command directory that users of the role can access. You can also control the level of access that the role has to the command or command directory, and you can specify a query that applies to the command or command directory.

Steps

1. Click ⚙.
2. In the **Management** pane, click **Roles**.
3. In the **Roles** window, click **Add**.
4. In the **Add Role** dialog box, type the role name and add the role attributes.
5. Click **Add**.

Edit roles

You can use System Manager to modify an access-control role’s access to a command or command directory and to restrict a user’s access to only a specified set of commands. You can also remove a role’s access to the default command directory.

Steps

1. Click ⚙.
2. In the **Management** pane, click **Roles**.
3. In the **Roles** window, select the role that you want to modify, and then click **Edit**.
4. In the **Edit Role** dialog box, modify the role attributes, and then click **Modify**.
5. Verify the changes that you made in the **Roles** window.

Roles and permissions

The cluster administrator can restrict a user’s access to only a specified set of commands by creating a restricted access-control role and then assigning the role to a user.

You can manage access-control roles in the following ways:

- By creating an access-control role, and then specifying the command or command directory that the role's users can access.
- By controlling the level of access that the role has for the command or command directory, and then specifying a query that applies to the command or command directory.
- By modifying an access-control role's access to a command or command directory.
- By displaying information about access-control roles, such as the role name, the command or command directory that a role can access, the access level, and the query.
- By deleting an access-control role.
- By restricting a user's access to only a specified set of commands.
- By displaying ONTAP APIs and their corresponding command-line interface (CLI) commands.

Roles window

You can use the Roles window to manage the roles that are associated with user accounts.

Command buttons

- **Add**

  Opens the Add Role dialog box, which enables you to create an access-control role and specify the command or command directory that the role's users can access.

- **Edit**

  Opens the Edit Role dialog box, which enables you to add or modify role attributes.

- **Refresh**

  Updates the information in the window.

Roles list

The roles list provides a list of roles that are available to be assigned to users.

Role Attributes area

The details area displays the role attributes, such as the command or command directory that the selected role can access, the access level, and the query that applies to the command or command directory.

Related information

Administrator authentication and RBAC

Manage the network with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage the network of your storage system by creating and managing IPspaces, broadcast domains, subnets, network interfaces, Ethernet ports, and FC/FCoE adapters.

Network window

You can use the Network window to view the list of network components, such as subnets, network interfaces, Ethernet ports, broadcast domains, FC/FCoE and NVMe adapters, and IPspaces, and to create, edit, or delete these components in your storage system.

Tabs

- **Subnet**

  Enables you to view a list of subnets, and create, edit, or delete subnets from your storage system.

- **Network Interfaces**

  Enables you to view a list of network interfaces, create, edit, or delete interfaces from your storage system, migrate the LIFs, change the status of the interface, and send the interface back to the home port.

- **Ethernet Ports**

  Enables you to view and edit the ports of a cluster, and create, edit, or delete interface groups and VLAN ports.

- **Broadcast Domains**

  Enables you to view a list of broadcast domains, and create, edit, or delete domains from your storage system.

- **FC/FCoE and NVMe Adapters**

  Enables you to view the ports in a cluster, and edit the FC/FCoE and NVMe adapter settings.

- **IPspaces**

  Enables you to view a list of IPspaces and broadcast domains, and create, edit, or delete an IPspace from your storage system.

Subnet tab

Command buttons

- **Create**

  Opens the Create Subnet dialog box, which enables you to create new subnets that contain configuration information for creating a network interface.

- **Edit**

  Opens the Edit Subnet dialog box, which enables you to modify certain attributes of a subnet such as the name, subnet address, range of IP addresses, and gateway details.

- **Delete**

  Deletes the selected subnet.

- **Refresh**

  Updates the information in the window.

Subnet list

- **Name**

  Specifies the name of the subnet.

- **Subnet IP/Subnet mask**

  Specifies the subnet address details.

- **Gateway**

  Specifies the IP address of the gateway.

- **Available**

  Specifies the number of IP addresses available in the subnet.

- **Used**

  Specifies the number of IP addresses used in the subnet.

- **Total Count**

  Specifies the total number of IP addresses (available and used) in the subnet.

- **Broadcast domain**

  Specifies the broadcast domain to which the subnet belongs.

- **IPspace**

  Specifies the IPspace to which the subnet belongs.

Details area

The area below the subnet list displays detailed information about the selected subnet, including the subnet range and a graph showing the available, used, and total number of IP addresses.

Limitations of the Network Interfaces tab

- For cluster LIFs, node management LIFs, VIP LIFs, and BGP LIFs, you cannot use System Manager to perform the following actions:
  - Create, edit, delete, enable, or disable the LIFs
  - Migrate the LIFs or send the LIFs back to the home port
- For cluster management LIFs, you can use System Manager to migrate the LIFs, or send the LIFs back to the home port.

  However, you cannot create, edit, delete, enable, or disable the LIFs.

- For intercluster LIFs, you can use System Manager to create, edit, delete, enable, or disable the LIFs.

  However, you cannot migrate the LIFs, or send the LIFs back to the home port.

- You cannot create, edit, or delete network interfaces in the following configurations:
  - A MetroCluster configuration
  - SVMs configured for disaster recovery (DR).

Command buttons

- **Create**

  Opens the Create Network Interface dialog box, which enables you to create network interfaces and intercluster LIFs to serve data and manage SVMs.

- **Edit**

  Opens the Edit Network Interface dialog box, which you can use to enable management access for a data LIF.

- **Delete**

  Deletes the selected network interface.

  This button is enabled only if the data LIF is disabled.

- **Status**

  Open the drop-down menu, which provides the option to enable or disable the selected network interface.

- **Migrate**

  Enables you to migrate a data LIF or a cluster management LIF to a different port on the same node or a different node within the cluster.

- **Send to Home**

  Enables you to host the LIF back on its home port.

  This command button is enabled only when the selected interface is hosted on a non-home port and when the home port is available.

  This command button is disabled when any node in the cluster is down.

- **Refresh**

  Updates the information in the window.

Interface list

You can move the pointer over the color-coded icon to view the operational status of the interface:

- Green specifies that the interface is enabled.
- Red specifies that the interface is disabled.

- **Interface Name**

  Specifies the name of the network interface.

- **Storage Virtual Machine**

  Specifies the SVM to which the interface belongs.

- **IP Address/WWPN**

  Specifies the IP address or worldwide port name (WWPN) of the interface.

- **Current Port**

  Specifies the name of the node and port on which the interface is hosted.

- **Data Protocol Access**

  Specifies the protocol used to access data.

- **Management Access**

  Specifies whether management access is enabled on the interface.

- **Subnet**

  Specifies the subnet to which the interface belongs.

- **mx Role**

  Specifies the operational role of the interface, which can be data, intercluster, cluster, cluster management, or node management.

Details area

The area below the interface list displays detailed information about the selected interface: failover properties such as the home port, current port, speed of the ports, failover policy, failover group, and failover state, and general properties such as the administrative status, role, IPspace, broadcast domain, network mask, gateway, and DDNS status.

Ethernet Ports tab

Command buttons

- **Create Interface Group**

  Opens the Create Interface Group dialog box, which enables you create interface groups by choosing the ports, and determining the use of ports and network traffic distribution.

- **Create VLAN**

  Opens the Create VLAN dialog box, which enables you to create a VLAN by choosing an Ethernet port or an interface group, and adding VLAN tags.

- **Edit**

Opens one of the following dialog boxes:

- Edit Ethernet Port dialog box: Enables you to modify Ethernet port settings.
- Edit VLAN dialog box: Enables you to modify VLAN settings.
- Edit Interface Group dialog box: Enables you to modify interface groups.

You can only edit VLANs that are not associated with a broadcast domain.

- **Delete**

  Opens one of the following dialog boxes:

  - Delete VLAN dialog box: Enables you to delete a VLAN.
  - Delete Interface Group dialog box: Enables you to delete an interface group.
- **Refresh**

  Updates the information in the window.

Ports list

You can move the pointer over the color-coded icon to view the operational status of the port:

- Green specifies that the port is enabled.
- Red specifies that the port is disabled.
- **Port**

  Displays the port name of the physical port, VLAN port, or the interface group.
- **Node**

  Displays the node on which the physical interface is located.
- **Broadcast Domain**

  Displays the broadcast domain of the port.
- **IPspace**

  Displays the IPspace to which the port belongs.
- **Type**

  Displays the type of the interface such as interface group, physical interface, vip, or VLAN.

Details area

The area below the ports list displays detailed information about the port properties.

- **Details tab**

  Displays administrative details and operational details.

  As part of the operational details, the tab displays the health status of the ports. The ports can be healthy

or degraded. A degraded port is a port on which continuous network fluctuations occur, or a port that has no connectivity to any other ports in the same broadcast domain.

In addition, the tab also displays the interface name, SVM details, and IP address details of the network interfaces that are hosted on the selected port. It also indicates whether the interface is at the home port or not.

- **Performance tab**

  Displays performance metrics graphs of the ethernet ports, including error rate and throughput.

  Changing the client time zone or the cluster time zone impacts the performance metrics graphs. You should refresh your browser to view the updated graphs.

Broadcast Domain tab

Command buttons

- **Create**

  Opens the Create Broadcast Domain dialog box, which enables you to create new broadcast domains to contain ports.

- **Edit**

  Opens the Edit Broadcast Domain dialog box, which enables you to modify the attributes of a broadcast domain, such as the name, MTU size, and associated ports.

- **Delete**

  Deletes the selected broadcast domain.

- **Refresh**

  Updates the information in the window.

Broadcast domain list

- **Broadcast Domain**

  Specifies the name of the broadcast domain.

- **MTU**

  Specifies the MTU size.

- **IPspace**

  Specifies the IPspace.

- **Combined Port Update Status**

  Specifies the status of the port updates when you create or edit a broadcast domain. Any errors in the port updates are displayed in a separate window, which you can open by clicking the associated link.

Details area

The area below the broadcast domain list displays all the ports in a broadcast domain. In a non-default IPspace, if a broadcast domain has ports with update errors, such ports are not displayed in the details area. You can move the pointer over the color-coded icon to view the operational status of the ports:

- Green specifies that the port is enabled.
- Red specifies that the port is disabled.

FC/FCoE and NVMe Adapters tab

Command buttons

- **Edit**

  Opens the Edit FC/FCoE and NVMe Settings dialog box, which enables you to modify the speed of the adapter.

- **Status**

  Enables you to bring the adapter online or take it offline.

- **Refresh**

  Updates the information in the window.

FC/FCoE and NVMe adapters list

- **WWNN**

  Specifies the unique identifier of the FC/FCoE and NVMe adapter.

- **Node Name**

  Specifies the name of the node that is using the adapter.

- **Slot**

  Specifies the slot that is using the adapter.

- **WWPN**

  Specifies the FC worldwide port name (WWPN) of the adapter.

- **Status**

  Specifies whether the status of the adapter is online or offline.

- **Speed**

  Specifies whether the speed settings are automatic or manual.

Details area

The area below the FC/FCoE and NVMe adapters list displays detailed information about the selected adapters.

- **Details tab**

  Displays adapter details such as the media type, port address, data link rate, connection status, operation status, fabric status, and the speed of the adapter.

- **Performance tab**

  Displays performance metrics graphs of the FC/FCoE and NVMe adapter, including IOPS and response time.

  Changing the client time zone or the cluster time zone impacts the performance metrics graphs. You should refresh your browser to see the updated graphs.

IPspaces tab

Command buttons

- **Create**

  Opens the Create IPspace dialog box, which enables you to create a new IPspace.

- **Edit**

  Opens the Edit IPspace dialog box, which enables you to rename an existing IPspace.

- **Delete**

  Deletes the selected IPspace.

- **Refresh**

  Updates the information in the window.

IPspaces list

- **Name**

  Specifies the name of the IPspace.

- **Broadcast Domains**

  Specifies the broadcast domain.

Details area

The area below the IPspaces list displays the list of storage virtual machines (SVMs) in the selected IPspace.

Manage IPspaces with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create and manage IPspaces.

Edit IPspaces

You can use System Manager to rename an existing IPspace.

About this task

- All IPspace names must be unique within a cluster and must not consist of names that are reserved by the system, such as local or localhost.
- The system-defined “Default” IPspace and “Cluster” IPspace cannot be modified.

Steps

1. Click **Network** > **IPspaces**.
2. Select the IPspace that you want to modify, and then click **Edit**.
3. In the **Edit IPspace** dialog box, specify a new name for the IPspace.
4. Click **Rename**.

Delete IPspaces

You can use System Manager to delete an IPspace when you no longer require the IPspace.

Before you begin

The IPspace that you want to delete must not be associated with any broadcast domains, network interfaces, peer relationships, or storage virtual machines (SVMs).

About this task

The system-defined “Default” IPspace and “Cluster” IPspace cannot be deleted.

Steps

1. Click **Network** > **IPspaces**.
2. Select the IPspace that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Yes**.

Related information

Network management

Manage broadcast domains with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create and manage broadcast domains.

Edit broadcast domain settings

You can use System Manager to modify the attributes of a broadcast domain such as the name, the MTU size, and the ports that are associated with the broadcast domain.

About this task

- You must not modify the MTU size of the broadcast domain to which the management port e0M is assigned.
- You cannot use System Manager to edit broadcast domains in the cluster IPspace.

  You must use the command-line interface (CLI) instead.

Steps

1. Click **Network** > **Broadcast Domains**.
2. Select the broadcast domain that you want to modify, and then click **Edit**.
3. In the **Edit Broadcast Domain** dialog box, modify the broadcast domain attributes as required.
4. Click **Save and Close**.

Delete broadcast domains

You can delete a broadcast domain by using System Manager when you no longer require the broadcast domain.

Before you begin

No subnets must be associated with the broadcast domain that you want to delete.

About this task

- When you delete a broadcast domain, the ports that are associated with the broadcast domain are assigned to the default IPspace, and the MTU settings of the ports are not changed.
- You cannot use System Manager to delete broadcast domains that are in the cluster IPspace.

  You must use the command-line interface (CLI) instead.

Steps

1. Click **Network** > **Broadcast Domains**.
2. Select the broadcast domain that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

Related information

Network window

Network management

Manage subnets with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage subnets.

Edit subnet settings

You can use System Manager to modify subnet attributes such as the name, subnet address, range of IP addresses, and gateway address of the subnet.

About this task

- You cannot use System Manager to edit subnets in the cluster IPspace.

  You must use the command-line interface (CLI) instead.

- Modifying the gateway address does not update the route.

  You must use the CLI to update the route.

Steps

1. Click **Network** > **Subnets**.
2. Select the subnet that you want to modify, and then click **Edit**.

   You can modify the subnet even when the LIF in that subnet is still in use.

3. In the **Edit Subnet** dialog box, modify the subnet attributes as required.
4. Click **Save and Close**.

Delete subnets

You can use System Manager to delete a subnet when you no longer require the subnet and you want to reallocate the IP addresses that were assigned to the subnet.

Before you begin

The subnet that you want to delete must not have any LIFs that are using the IP addresses from the subnet.

About this task

You cannot use System Manager to delete subnets in the Cluster IPspace. You must use the command-line interface (CLI) instead.

Steps

1. Click **Network** > **Subnets**.
2. Select the subnet that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

Related information

Network window

Manage network interfaces with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create and manage network interfaces.

Create network interfaces

You can use System Manager to create a network interface or LIF to access data from storage virtual machines (SVMs), to manage SVMs and to provide an interface for intercluster connectivity.

Before you begin

The broadcast domain that is associated with the subnet must have allocated ports.

About this task

- Dynamic DNS (DDNS) is enabled by default when a LIF is created.

  However, DDNS is disabled if you configure the LIF for intercluster communication using iSCSI, NVMe, or FC/FCoE protocols, or for management access only.

- You can specify an IP address by using a subnet or by not using a subnet.
- You cannot use System Manager to create a network interface if the ports are degraded.

  You must use the command-line interface (CLI) to create a network interface in such cases.

- To create NVMeoF data LIF the SVM must already be set up, the NVMe service must already exist on the SVM and the NVMeoF capable adapters should be available.
- NVMe protocol is enabled only if the selected SVM has the NVMe service configured.

Steps

1. Click **Network** > **Network Interfaces**.
2. Click **Create**.
3. In the **Create Network Interface** dialog box, specify an interface name.
4. Specify an interface role:

If you want to…	Then…
Associate the network interface with a data LIF	a. Select **Serves Data**. b. Select the SVM for the network interface.
Associate the network interface with an intercluster LIF	a. Select **Intercluster Connectivity**. b. Select the IPspace for the network interface.

5. Select the appropriate protocols.

   The interface uses the selected protocols to access data from the SVM.

   If you select the NVMe protocol, the rest of the protocols are disabled. If NAS (CIFS and NFS) protocols are supported then they remain available. The NVMe transports field is displayed when you select the NVMe protocol and FC-NVMe is shown as the transport protocol.

6. If you want to enable management access on the data LIF, select the **Enable Management Access** check box.

   You cannot enable management access for intercluster LIFs or LIFs with FC/FCoE or NVMe protocols.

7. Assign the IP address:

If you want to…	Then…
Specify the IP address by using a subnet	a. Select **Using a subnet**. b. In the Add Details dialog box, select the subnet from which the IP address must be assigned. For intercluster LIF, only the subnets that are associated with the selected IPspace are displayed. c. If you want to assign a specific IP address to the interface, select **Use a specific IP address**, and then type the IP address. The IP address that you specify is added to the subnet if the IP address is not already present in the subnet range. d. Click **OK**.
Specify the IP address manually without using a subnet	a. Select **Without a subnet**. b. In the Add Details dialog box, perform the following steps: i. Specify the IP address and the network mask or prefix. ii. Optional: Specify the gateway. iii. If you do not want to use the default value for the Destination field, specify a new destination value. If you do not specify a destination value, the Destination field is populated with the default value based on the family of the IP address. If a route does not exist, a new route is automatically created based on the gateway and destination. c. Click **OK**.

8. Select the required ports from the **Port** details area.
   - For data LIFs, the Port details area displays all of the ports from the broadcast domain that is associated with the IPspace of the SVM.
   - For intercluster LIFs, the Port details area displays all of the ports from the broadcast domain that is associated with the required IPspace.
   - The Port details area will display only NVMe capable adapters if the NVMe protocol is selected.
9. **Optional:** Select the **Dynamic DNS (DDNS)** check box to enable DDNS.

10. Click **Create**.

Edit network interface settings

You can use System Manager to modify the network interface to enable management access for a data LIF.

About this task

- You cannot modify the network settings of cluster LIFs, cluster management LIFs, or node management LIFs through System Manager.
- You cannot enable management access for an intercluster LIF.

Steps

1. Click **Network** > **Network Interfaces**.
2. Select the interface that you want to modify, and then click **Edit**.
3. In the **Edit Network Interface** dialog box, modify the network interface settings as required.
4. Click **Save and Close**.

Delete network interfaces

You can use System Manager to delete a network interface to free the IP address of the interface and then use the IP address for a different purpose.

Before you begin

The status of the network interface must be disabled.

Steps

1. Click **Network** > **Network Interfaces**.
2. Select the interface that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

Migrate a LIF

You can use System Manager to migrate a data LIF or a cluster management LIF to a different port on the same node or on a different node within the cluster if the source port is faulty or requires maintenance.

Before you begin

The destination node and ports must be operational and must be able to access the same network as the source port.

About this task

- If you are removing the NIC from the node, you must migrate the LIFs that are hosted on the ports belonging to the NIC to other ports in the cluster.
- You cannot migrate iSCSI LIFs or FC LIFs.

Steps

1. Click **Network** > **Network Interfaces**.
2. Select the interface that you want to migrate, and then click **Migrate**.
3. In the **Migrate Interface** dialog box, select the destination port to which you want to migrate the LIF.

4. **Optional:** Select the **Migrate Permanently** check box if you want to set the destination port as the new home port for the LIF.
5. Click **Migrate**.

Related information

Network window

Configuring iSCSI protocol on SVMs

ONTAP concepts

Network management

Manage ethernet ports with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (avaiable in ONTAP 9.7 and earlier) to create and manage Ethernet ports.

Create interface groups

You can use System Manager to create an interface group—single-mode, static multimode, or dynamic multimode (LACP)--to present a single interface to clients by combining the capabilities of the aggregated network ports.

Before you begin

Free ports must be available that do not belong to any broadcast domain or interface group, or that host a VLAN.

Steps

1. Click **Network** > **Ethernet Ports**.
2. Click **Create Interface Group**.
3. In the **Create Interface Group** dialog box, specify the following settings:
   - Name of the interface group
   - Node
   - Ports that you want to include in the interface group
   - Usage mode of the ports: single-mode, static multiple, or dynamic multimode (LACP)
   - Network load distribution: IP-based, MAC address-based, sequential, or port
   - Broadcast domain for the interface group, if required
4. Click **Create**.

Create VLAN interfaces

You can create a VLAN to maintain separate broadcast domains within the same network domain by using System Manager.

Steps

1. Click **Network** > **Ethernet Ports**.

2. Click **Create VLAN**.
3. In the **Create VLAN** dialog box, select the node, the physical interface, and the broadcast domain (if required).

   The physical interface list includes only Ethernet ports and interface groups. The list does not display interfaces that are in another interface group or an existing VLAN.

4. Type a VLAN tag, and then click **Add**.

   You must add unique VLAN tags.

5. Click **Create**.

Edit Ethernet port settings

You can edit Ethernet port settings such as the duplex mode and speed settings by using System Manager.

Steps

1. Click **Network** > **Ethernet Ports**.
2. Select the physical port, and then click **Edit**.
3. In the **Edit Ethernet Port** dialog box, modify the duplex mode and speed settings to either `manual` or `automatic`.
4. Click **Edit**.

Edit interface group settings

You can use System Manager to add ports to an interface group, to remove ports from an interface group, and to modify the usage mode and load distribution pattern of the ports in an interface group.

About this task

You cannot modify the MTU settings of an interface group that is assigned to a broadcast domain.

Steps

1. Click **Network** > **Ethernet Ports**.
2. Select an interface group, and then click **Edit**.
3. Modify the interface group settings as required, and then click **Save and Close**.

Modify the MTU size of a VLAN

If you want to modify the MTU size of a VLAN interface that is not part of a broadcast domain, you can use System Manager to change the size.

About this task

You must not modify the MTU size of the management port e0M.

Steps

1. Click **Network** > **Ethernet Ports**.
2. Select the VLAN that you want to modify, and then click **Edit**.
3. In the **Edit VLAN** dialog box, modify the MTU size as required, and then click **Save**.

Delete VLANs

You can delete VLANs that are configured on network ports by using System Manager. You might have to delete a VLAN before removing a NIC from its slot. When you delete a VLAN, the VLAN is automatically removed from all of the failover rules and groups that use the VLAN.

Before you begin

No LIFs must be associated with the VLAN.

Steps

1. Click **Network** > **Ethernet Ports**.
2. Select the VLAN that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

Ports and adapters

Ports are grouped under nodes and the nodes are displayed based on the selected protocol category. For example, if the data is served using the FC protocol, then only the nodes with FCP adapters are displayed. The hosted interface count helps you in choosing a port which is less loaded.

Related information

Network management

ONTAP concepts

Network window

Manage FC/FCoE and NVMe adapters with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage FC/FCoE and NVMe adapters.

Edit the FC/FCoE and NVMe adapter speed settings

You can modify the FC/FCoE and NVMe adapter speed settings by using the Edit FC/FCoE and NVMe Adapter Settings dialog box in System Manager.

Steps

1. Click **Network** > **FC/FCoE and NVMe Adapters**.
2. Select the adapter that you want to edit, and then click **Edit**.
3. In the **Edit FC/FCoE and NVMe adapter settings** dialog box, set the adapter speed to **Manual** or **Automatic**, and then click **Save**.

Related information

Network window

Network management

Storage tiers

Edit aggregates with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to change the aggregate name, RAID type, and RAID group size of an existing aggregate when required.

Before you begin

For modifying the RAID type of an aggregate from RAID4 to RAID-DP, the aggregate must contain enough compatible spare disks, excluding the hot spares.

About this task

- You cannot change the RAID group of ONTAP systems that support array LUNs.

  RAID0 is the only available option.

- You cannot change the RAID type of partitioned disks.

  RAID-DP is the only option that is available for partitioned disks.

- You cannot rename a SnapLock Compliance aggregate.
- If the aggregate consists of SSDs with storage pool, you can modify only the name of the aggregate.
- If the triple parity disk size is 10 TB, and the other disks are smaller than 10 TB in size, then you can select RAID-DP or RAID-TEC as the RAID type.
- If the triple parity disk size is 10 TB, and if even one of the other disks is larger than 10 TB in size, then RAID-TEC is the only available option for RAID type.

Steps

1. Choose one of the following methods:
   - Click **Applications & Tiers** > **Storage Tiers**.
   - Click **Storage** > **Aggregates & Disks** > **Aggregates**.
2. Select the aggregate that you want to edit, and then click **Edit**.
3. In the **Edit Aggregate** dialog box, modify the aggregate name, the RAID type, and the RAID group size, as required.
4. Click **Save**.

Related information

Aggregates window

What compatible spare disks are

Storage Tiers window

Delete aggregates with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (avaiable in ONTAP 9.7 and earlier) to delete aggregates when you no longer require the data in the aggregates. However, you

cannot delete the root aggregate because it contains the root volume, which contains the system configuration information.

Before you begin

- All the FlexVol volumes and the associated storage virtual machines (SVMs) contained by the aggregate must be deleted.
- The aggregate must be offline.

Steps

1. Choose one of the following methods:
   - Click **Applications & Tiers** > **Storage Tiers**.
   - Click **Storage** > **Aggregates & Disks** > **Aggregates**.
2. Select one or more aggregates that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

Related information

Aggregates window

Storage Tiers window

Change the RAID configuration when creating an aggregate with System Manager - ONTAP 9.7 and earlier

While creating an aggregate, you can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to modify the default values of the RAID type and RAID group size options of the aggregate.

About this task

If the disk type of the aggregate disks is FSAS or MSATA, and the disk size is equal to or larger than 10 TB, then RAID-TEC is the only available RAID type.

Steps

1. Choose one of the following methods:
   - Click **Applications & Tiers** > **Storage Tiers**.
   - Click **Storage** > **Aggregates & Disks** > **Aggregates**.
2. In the **Storage Tiers** window, click **Add Aggregate**.
3. In the **Create Aggregate** dialog box, perform the following steps:
   a. Click **Change**.
   b. In the **Change RAID Configuration** dialog box, specify the RAID type and RAID group size.

      Shared disks support two RAID types: RAID DP and RAID-TEC.

      The recommended RAID group size is 12 disks through 20 disks for HDDs, and 20 disks through 28 disks for SSDs.

   c. Click **Save**.

Provision cache by adding SSDs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to add SSDs as either storage pools or dedicated SSDs to provision cache. By adding SSDs, you can convert a non-root aggregate or a root aggregate that does not contain partitioned disks to a Flash Pool aggregate, or increase the cache size of an existing Flash Pool aggregate.

About this task

- The added SSD cache does not add to the size of the aggregate, and you can add an SSD RAID group to an aggregate even when it is at the maximum size.
- You cannot use partitioned SSDs when you add cache by using System Manager.

Provisioning cache to aggregates by adding SSDs

You can use System Manager to add storage pools or dedicated SSDs to provision cache by converting an existing non-root HDD aggregate or a root aggregate that does not contain partitioned disks to a Flash Pool aggregate.

Before you begin

- The aggregate must be online.
- There must be sufficient spare SSDs or allocation units in the storage pool that can be assigned as cache disks.
- All of the nodes in the cluster must be running ONTAP 8.3 or later.

  If the cluster is in a mixed-version state, you can use the command-line interface to create a Flash Pool aggregate and then provision SSD cache.

- You must have identified a valid 64-bit non-root aggregate composed of HDDs that can be converted to a Flash Pool aggregate.
- The aggregate must not contain any array LUNs.

About this task

You must be aware of platform-specific and workload-specific best practices for Flash Pool aggregate SSD tier size and configuration.

Steps

1. Choose one of the following methods:
   - Click **Applications & Tiers** > **Storage Tiers**.
   - Click **Storage** > **Aggregates & Disks** > **Aggregates**.
2. In the **Storage Tiers** window, select the aggregate, and then click **More Actions** > **Add Cache**.

   Adding cache is not supported on FabricPool-enabled aggregates.

3. In the **Add Cache** dialog box, perform the appropriate action:

If you selected the cache source as…	Do this…
Storage pools	a. Select the storage pool from which cache can be obtained. b. Specify the cache size. c. Modify the RAID type, if required.
Dedicated SSDs	Select the SSD size and the number of SSDs to include, and optionally modify the RAID configuration: a. Click **Change**. b. In the Change RAID Configuration dialog box, specify the RAID type and RAID group size, and then click **Save**.

4. Click **Add**.

   For mirrored aggregates, an **Add Cache** dialog box is displayed with the information that twice the number of selected disks will be added.

5. In the **Add Cache** dialog box, click **Yes**.

Results

The cache disks are added to the selected aggregate.

Increasing the cache for Flash Pool aggregates by adding SSDs

You can add SSDs as either storage pools or dedicated SSDs to increase the size of a Flash Pool aggregate by using System Manager.

Before you begin

- The Flash Pool aggregate must be online.
- There must be sufficient spare SSDs or allocation units in the storage pool that can be assigned as cache disks.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Aggregates**.
2. In the **Aggregates** window, select the Flash Pool aggregate, and then click **Add Cache**.
3. In the **Add Cache** dialog box, perform the appropriate action:

If you selected the cache source as…	Do this…
Storage pools	Select the storage pool from which cache can be obtained, and specify the cache size.
Dedicated SSDs	Select the SSD size and the number of SSDs to include.

4. Click **Add**.

   For mirrored aggregates, an Add Cache dialog box is displayed with the information that twice the number of selected disks will be added.

5. In the **Add Cache** dialog box, click **Yes**.

Results

The cache disks are added to the selected Flash Pool aggregate.

Related information

NetApp Technical Report 4070: Flash Pool Design and Implementation

How storage pool works

Add capacity disks with System Manager - ONTAP 9.7 and earlier

You can increase the size of an existing non-root aggregate or a root aggregate containing disks by adding capacity disks. You can use System Manager classic (available in ONTAP 9.7 and earlier) to add HDDs or SSDs of the selected ONTAP disk type and to modify the RAID group options.

Before you begin

- The aggregate must be online.
- There must be sufficient compatible spare disks.

About this task

- It is a best practice to add disks that are of the same size as the other disks in the aggregate.

  If you add disks that are smaller in size than the other disks in the aggregate, the aggregate becomes suboptimal in configuration, which in turn might cause performance issues.

  If you add disks that are larger in size than the disks that are available in a pre-existing RAID group within the aggregate, then the disks are downsized, and their space is reduced to that of the other disks in that RAID group. If a new RAID group is created in the aggregate and similar sized disks remain in the new RAID group, the disks are not downsized.

  If you add disks that are not of the same size as the other disks in the aggregate, the selected disks might not be added; instead, other disks with a usable size between 90 percent and 105 percent of the specified size are automatically added. For example, for a 744 GB disk, all of the disks in the range of 669 GB through 781 GB are eligible for selection. For all of the spare disks in this range, ONTAP first selects only partitioned disks, then selects only unpartitioned disks, and finally selects both partitioned disks and unpartitioned disks.

- You cannot use System Manager to add HDDs to the following configurations:
  - Aggregates containing only SSDs
  - Root aggregates containing partitioned disks
    You must use the command-line interface to add HDDs to these configurations.
- Shared disks support two RAID types: RAID DP and RAID-TEC.
- You cannot use SSDs with storage pool.

- If the RAID group type is RAID DP, and if you are adding FSAS or MSATA type of disks that are equal to or larger than 10 TB in size, then you can add them only to `Specific RAID group`, and not to `New RAID group` or `All RAID groups`.

  The disks are added after downsizing the disk size to the size of the disks in the pre-existing RAID group of the existing aggregate.

- If the RAID group type is RAID-TEC, and if you are adding FSAS or MSATA type of disks that are equal to or larger than 10 TB in size, then you can add them to `All RAID groups`, `New RAID group`, and `Specific RAID group`.

  The disks are added after downsizing the disk size to the size of the disks in the pre-existing RAID group of the existing aggregate.

Steps

1. Choose one of the following methods:
   - Click **Applications & Tiers** > **Storage Tiers**.
   - Click **Storage** > **Aggregates & Disks** > **Aggregates**.
2. In the **Storage Tiers** window, select the aggregate to which you want to add capacity disks, and then click **More Actions › Add Capacity**.
3. Specify the following information in the **Add Capacity** dialog box:
   a. Specify the disk type for the capacity disks by using the **Disk Type to Add** option.
   b. Specify the number of capacity disks by using the **Number of Disks or Partitions** option.
4. Specify the RAID group to which the capacity disks are to be added by using the **Add Disks To** option.

   By default, System Manager adds the capacity disks to `All RAID groups`.

   a. Click **Change**.
   b. In the **RAID Group Selection** dialog box, specify the RAID group as `New RAID group` or `Specific RAID group` by using the **Add Disks To** option.

      Shared disks can be added only to the `New RAID group` option.

5. Click **Add**.

   For mirrored aggregates, an **Add Capacity** dialog box is displayed with the information that twice the number of selected disks will be added.

6. In the **Add Capacity** dialog box, click **Yes** to add the capacity disks.

Results

The capacity disks are added to the selected aggregate, and the aggregate size is increased.

Related information

What compatible spare disks are

Change the RAID group when adding capacity disks with System Manager - ONTAP 9.7 and earlier

While adding capacity disks (HDDs) to an aggregate, you can use ONTAP System Manager classic (avaiable in ONTAP 9.7 and earlier) to change the RAID group to which you want to add the disks.

About this task

- If the RAID type is RAID-DP, and if you are adding FSAS or MSATA type of disks that are equal to or larger than 10 TB in size, then you can add them only to `Specific RAID group`, and not to `New RAID group` or `All RAID groups`.

  The disks are added after downsizing the disk size to the size of the existing aggregates.

- If the RAID group is RAID-TEC, and if you are adding FSAS or MSATA type of disks that are equal to or larger than 10 TB in size, then you can add them to `All RAID groups`, `New RAID group`, and `Specific RAID group`.

  The disks are added after downsizing the disk size to the size of the existing aggregates.

Steps

1. Choose one of the following methods:
   - Click **Applications & Tiers** > **Storage Tiers**.
   - Click **Storage** > **Aggregates & Disks** > **Aggregates**.
2. In the **Storage Tiers** window, select the aggregate to which you want to add capacity disks, and then click **More Actions › Add Capacity**.
3. In the **Add Capacity** dialog box, perform the following steps:
   a. Click **Change**.
   b. In the **Change RAID Configuration** dialog box, specify the RAID group to which you want to add the capacity disks.

      You can change the default value `All RAID groups` to either `Specific RAID group` or `New RAID group`.

   c. Click **Save**.

Move FlexVol volumes with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (avaiable in ONTAP 9.7 and earlier) to nondisruptively move a FlexVol volume to a different aggregate or a different node for capacity utilization and improved performance.

Before you begin

If you are moving a data protection volume, data protection mirror relationships must be initialized before you move the volume.

About this task

- When you move a volume that is hosted on a Flash Pool aggregate, only the data that is stored in the HDD tier is moved to the destination aggregate.

The cached data that is associated with the volume is not moved to the destination aggregate. Therefore, some performance degradation might occur after the volume move.

- You cannot move volumes from a SnapLock aggregate.
- You cannot move volumes from an SVM that is configured for disaster recovery to a FabricPool-enabled aggregate.

Steps

1. Choose one of the following methods:
   - Click **Applications & Tiers** > **Storage Tiers**.
   - Click **Storage** > **Aggregates & Disks** > **Aggregates**.
2. Select the aggregate that contains the volume, and then click **More Actions › Volume Move**.
3. Type or select information as prompted by the wizard.
4. Confirm the details, and then click **Finish** to complete the wizard.

Mirror aggregates with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to protect data and to provide increased resiliency by mirroring data in real-time, within a single aggregate. Mirroring aggregates removes single points of failure in connecting to disks and array LUNs.

Before you begin

There must be sufficient free disks in the other pool to mirror the aggregate.

About this task

You cannot mirror a Flash Pool aggregate when the cache source is storage pool.

Steps

1. Choose one of the following methods:
   - Click **Applications & Tiers** > **Storage Tiers**.
   - Click **Storage** > **Aggregates & Disks** > **Aggregates**.
2. Select the aggregate that you want to mirror, and then click **More Actions › Mirror**.

   SyncMirror is not supported on FabricPool-enabled aggregates.

3. In the **Mirror this aggregate** dialog box, click **Mirror** to initiate the mirroring.

View aggregate information with System Manager - ONTAP 9.7 and earlier

You can use the Aggregates window in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to view the name, status, and space information about an aggregate.

Steps

1. Choose one of the following methods:

- Click **Applications & Tiers** > **Storage Tiers**.
- Click **Storage** > **Aggregates & Disks** > **Aggregates**.

2. Click on the aggregate name to view the details of the selected aggregate.

Install a CA certificate if you use StorageGRID with System Manager - ONTAP 9.7 and earlier

For ONTAP to authenticate with StorageGRID as the object store for a FabricPool-enabled aggregate, you can install a StorageGRID CA certificate on the cluster with System Manager classic (available in ONTAP 9.7 and earlier).

Steps

1. Follow the StorageGRID system documentation to copy the CA certificate of the StorageGRID system by using the Grid Management Interface.

   StorageGRID 11.3 Administrator Guide

   While adding StorageGRID as a cloud tier, a message is displayed if the CA certificate is not installed.

2. Add the StorageGRID CA certificate.

   The fully qualified domain name (FQDN) that you specify must match the custom common name on the StorageGRID CA certificate.

Related information

Adding a cloud tier

Use effective ONTAP disk type for mixing HDDs with System Manger - ONTAP 9.7 and earlier

Beginning with Data ONTAP 8.1, certain ONTAP disk types are considered equivalent for the purposes of creating and adding to aggregates, and managing spares. ONTAP assigns an effective disk type for each disk type. You can use ONTAP System Manager classic (available in 9.7 and earlier) to mix HDDs that have the same effective disk type.

When the `raid.disktype.enable` option is set to `off`, you can mix certain types of HDDs within the same aggregate. When the `raid.disktype.enable` option is set to `on`, the effective disk type is the same as the ONTAP disk type. Aggregates can be created using only one disk type. The default value for the `raid.disktype.enable` option is `off`.

Beginning with Data ONTAP 8.2, the option `raid.mix.hdd.disktype.capacity` must be set to `on` to mix disks of type BSAS, FSAS, and ATA. The option `raid.mix.hdd.disktype.performance` must be set to `on` to mix disks of type FCAL and SAS.

The following table shows how the disk types map to the effective disk type:

ONTAP disk type	Effective disk type
FCAL	SAS

ONTAP disk type	Effective disk type
SAS	SAS
ATA	FSAS
BSAS	FSAS
FCAL and SAS	SAS
MSATA	MSATA
FSAS	FSAS

Compatible spare disks in System Manager - ONTAP 9.7 and earlier

In ONTAP System Manager classic (available in ONTAP 9.7 and earlier), compatible spare disks are disks that match the properties of other disks in the aggregate. When you want to increase the size of an existing aggregate by adding HDDs (capacity disks) or change the RAID type of an aggregate from RAID4 to RAID-DP, the aggregate must contain sufficient compatible spare disks.

Disk properties that must match are the disk type, disk size (can be a higher size disk in case the same disk size is not available), disk RPM, checksum, node owner, pool, and shared disk properties. If you use higher sized disks, you must be aware that disk downsizing occurs and the size of all disks are reduced to the lowest disk size. Existing shared disks are matched with higher size non-shared disks, and the non-shared disks are converted to shared disks and added as spares.

If RAID mixing options, such as disk type mixing and disk RPM mixing, are enabled for the RAID group, the disk type and disk RPM of the existing disks of the aggregate are matched with the effective disk type and effective disk RPM of the spare disks to obtain compatible spares.

Related information

Adding capacity disks

Editing aggregates

How System Manager works with hot spares - ONTAP 9.7 and earlier

A hot spare is a disk that is assigned to a storage system but not used by any RAID group. Hot spares do not contain any data and are assigned to a RAID group when a disk failure occurs in the RAID group. ONTAP System Manager classic (available in ONTAP 9.7 and earlier) uses the largest disk as the hot spare.

When there are different disk types in the RAID group, the largest-sized disk of each disk type is left as the hot spare. For example, if there are 10 SATA disks and 10 SAS disks in the RAID group, the largest-sized SATA disk and the largest-sized SAS disk are serve as hot spares.

If the largest-sized disk is partitioned, then the hot spares are provided separately for partitioned and non-

partitioned RAID groups. If the largest-sized disk is unpartitioned, then a single spare disk is provided.

The largest-sized non-partitioned disk is left as a hot spare if there are root partitions in the disk group. When a non-partitioned disk of the same size is not available, then spare root partitions are left as hot spares for the root partitioned group.

A single spare disk can serve as a hot spare for multiple RAID groups. System Manager calculates the hot spares based on the value set in the option `raid.min_spare_count` at the node level. For example, if there are 10 SSDs in an SSD RAID group and the option `raid.min_spare_count` is set to `1` at the node level, System Manager leaves 1 SSD as the hot spare and uses the other 9 SSDs for SSD-related operations. Similarly, if there are 10 HDDs in an HDD RAID group and the option `raid.min_spare_count` is set to `2` at the node level, System Manager leaves 2 HDDs as hot spares and uses the other 8 HDDs for HDD-related operations.

System Manager enforces the hot spare rule for RAID groups when you create an aggregate, edit an aggregate, and when you add HDDs or SSDs to an aggregate. The hot spare rule is also used when you create a storage pool or add disks to an existing storage pool.

There are exceptions to the hot spare rule in System Manager:

- For MSATA or disks in a multi-disk carrier, the number of hot spares is twice the value set at the node level and the number must not be less than 2 at any time.
- Hot spares are not used if the disks are part of array LUNs or virtual storage appliances.

Rules for displaying disk types and disk RPM in System Manager - ONTAP 9.7 and earlier

When you are creating an aggregate and adding capacity disks to an aggregate, you should understand the rules that apply when disk types and disk RPM are displayed in ONTAP System Manager classic (available in ONTAP 9.7 and earlier).

When the disk type mixing and the disk RPM mixing options are not enabled, the actual disk type and actual disk RPM are displayed.

When these mixing options are enabled, the effective disk type and effective disk RPM are displayed instead of the actual disk type and actual disk RPM. For example, when the disk mixing option is enabled, System Manager displays BSAS disks as FSAS. Similarly, when the disk RPM mixing option is enabled, if the RPM of the disks is 10K and 15K, System Manager displays the effective RPM as 10K.

Storage recommendations for creating aggregates with System Manager - ONTAP 9.7 and earlier

Beginning with System Manager 9.4, you can create aggregates based on storage recommendations. However, you must determine whether creating aggregates based on storage recommendations is supported in your environment. If your environment does not support creating aggregates based on storage recommendations, you must decide the RAID policy and disk configuration, and then create the aggregates manually.

System Manager analyzes the available spare disks in the cluster and generates a recommendation about how the spare disks should be used to create aggregates according to best practices. System Manager displays the summary of recommended aggregates including their names and usable size.

In many cases, the storage recommendation will be optimal for your environment. However, if your cluster is running ONTAP 9.3 or earlier, or if your environment includes the following configurations, you must create aggregates manually:

- Aggregates using third-party array LUNs
- Virtual disks with Cloud Volumes ONTAP or ONTAP Select
- MetroCluster configurations
- SyncMirror functionality
- MSATA disks
- Flash Pool aggregates
- Multiple disk types or sizes are connected to the node

In addition, if any of the following disk conditions exist in your environment, you must rectify the disk conditions before you use the storage recommendation to create aggregates:

- Missing disks
- Fluctuation in spare disk numbers
- Unassigned disks
- Non-zeroed spares (for ONTAP versions earlier than 9.6)
- Disks that are undergoing maintenance testing

Related information

Disk and aggregate management

Zeroing spare disks

Storage Tiers window in System Manager - ONTAP 9.7 and earlier

You can use the Storage Tiers window in ONTAP System Manager classic (available in ONTAP 9.7 and earier) to view cluster-wide space details and to add and view aggregate details.

The Internal Tier panel, or the Performance Tier panel if the cluster has all flash (all SSD) aggregates, displays cluster-wide space details such as the sum of the total sizes of all of the aggregates, the space used by the aggregates in the cluster, and the available space in the cluster.

The Cloud Tier panel displays the total licensed cloud tiers in the cluster, the licensed space that is used in the cluster, and the licensed space that is available in the cluster. The Cloud Tier panel also displays the unlicensed cloud capacity that is used.

Aggregates are grouped by type, and the aggregate panel displays details about the total aggregate space, space used, and the available space. If inactive (cold) data is available on a solid-state drive (SSD) or All Flash FAS aggregate, the amount of space it uses is also displayed. You can select the aggregate and perform any of the aggregate-related actions.

Command buttons

- **Add Aggregate**

  Enables you to create an aggregate.

- **Actions**

Provides the following options:

- **Change status to**

  Changes the status of the selected aggregate to one of the following statuses:

  - **Online**

    Read and write access to the volumes that are contained in this aggregate is allowed.

  - **Offline**

    Read and write access is not allowed.

  - **Restrict**

    Some operations such as parity reconstruction are allowed, but data access is not allowed.

- **Add Capacity**

  Enables you to add capacity (HDDs or SSDs) to existing aggregates.

- **Add Cache**

  Enables you to add cache disks (SSDs) to existing HDD aggregates or Flash Pool aggregates.

  You cannot add cache disks to FabricPool-enabled aggregates.

  This option is not available for a cluster containing nodes with All Flash Optimized personality.

- **Mirror**

  Enables you to mirror the aggregates.

- **Volume Move**

  Enables you to move a FlexVol volume.

Details area

You can click the aggregate name to view detailed information about the aggregate.

- **Overview tab**

  Displays detailed information about the selected aggregate, and displays a pictorial representation of the space allocation of the aggregate, the space savings of the aggregate, and the performance of the aggregate.

- **Disk Information tab**

  Displays the disk layout information for the selected aggregate.

- **Volumes tab**

  Displays details about the total number of volumes on the aggregate, the total aggregate space, and the space committed to the aggregate.

- **Performance tab**

  Displays graphs that show the performance metrics of the aggregates, including throughput and IOPS. Performance metrics data for read, write, and total transfers is displayed for throughput and IOPS, and the data for SSDs and HDDs is recorded separately.

  Changing the client time zone or the cluster time zone impacts the performance metrics graphs. If you change the client time zone or the cluster time zone, you should refresh your browser to view the updated graphs.

Related information

Adding a cloud tier

Attaching an aggregate to a cloud tier

Deleting a cloud tier

Editing a cloud tier

Provisioning storage through aggregates

Deleting aggregates

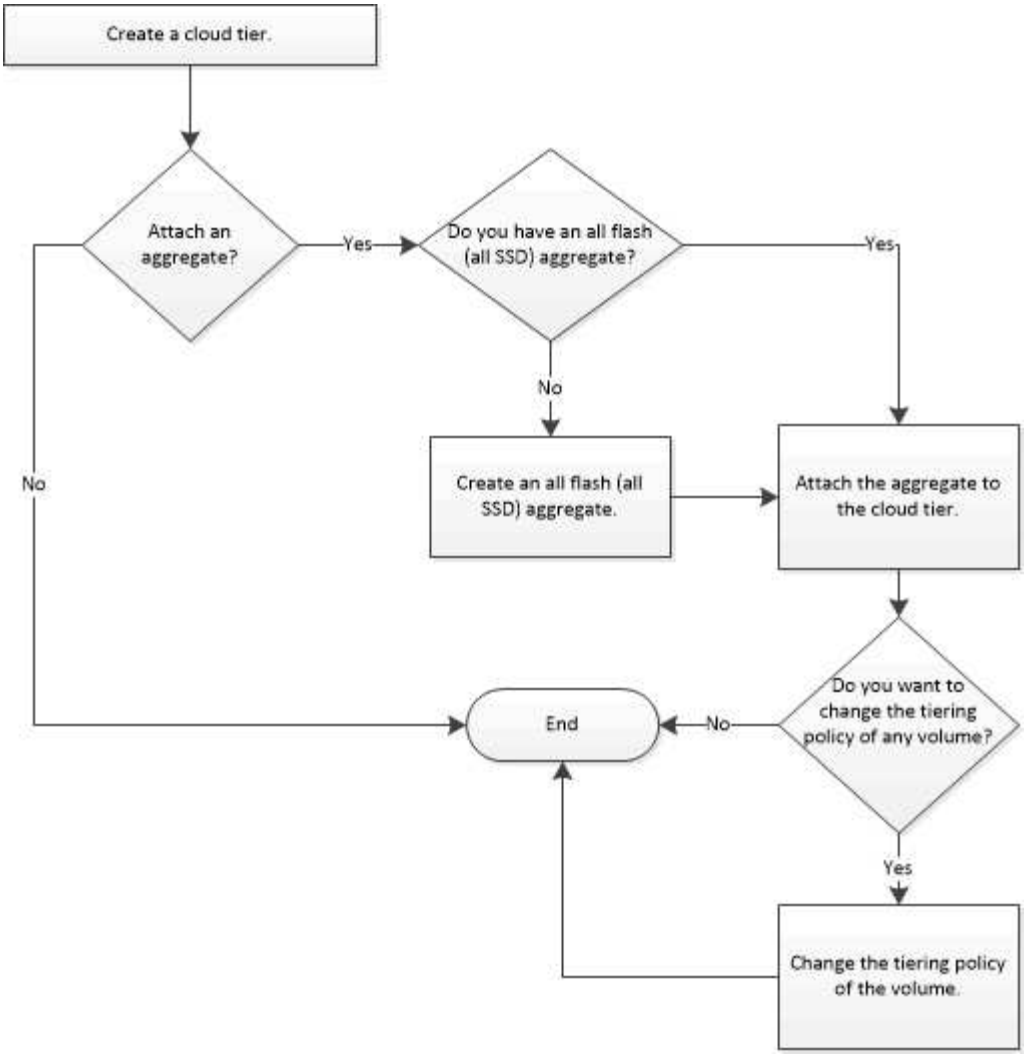
Editing aggregates

Configure and manage cloud tiers with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manger classic (available in ONTAP 9.7 and earlier) to configure and manage cloud tiers. Storing data in tiers can enhance the efficiency of your storage system. You manage storage tiers by using FabricPool-enabled aggregates. Cloud tiers store data in a tier based on whether the data is frequently accessed.

Before you begin

- You must be running ONTAP 9.2 or later.
- You must have all flash (all SSD) aggregates



Add a cloud tier

You can use System Manager to add a cloud tier to an SSD aggregate or a virtual machine disk (VMDK) aggregate. Cloud tiers provide storage for infrequently used data.

Before you begin

- You must have the access key ID and secret key to connect to the object store.
- You must have created a bucket inside the object store.
- Network connectivity must exist between the cluster and the cloud tier.
- If communication between the cloud tier and the cluster is encrypted using SSL or TLS, the required certificates must be installed.

About this task

The following object stores can be used as cloud tiers:

- StorageGRID
- Alibaba Cloud (Starting with System Manager 9.6)
- Amazon Web Services (AWS) Simple Storage Service (S3)
- Amazon Web Services (AWS) Commercial Cloud Service (C2S)

- Microsoft Azure Blob storage
- IBM Cloud
- Google Cloud

- Azure Stack, which is an on-premises Azure service, is not supported.
- If you want to use any object store as a cloud tier, other than StorageGRID, you must have the FabricPool capacity license. You can add the license by clicking **Add License**.
- If you want to use an IBM Cloud Object Storage environment (such as Cleversafe), with FabricPool, you should specify a certification authority (CA) certificate. You can specify the CA certificate by moving the **Object Store Certificate** toggle button and specifying the certificate credentials.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Cloud Tier**.
2. Click **Add**.

   A dialog box appears that lists all supported object store providers.

3. From the list, select the object store provider that you want to designate as the cloud tier.

   The Add Cloud Tier window is displayed.

4. Select a region from the drop-down list in the **Region** field.

   Based on your selection, the **Service Name (FQDN)** field is automatically populated with the server endpoint.

5. Specify the access key ID of the cloud tier, the secret key of the cloud tier, and the container name.

   If you have selected AWS Commercial Cloud Service (C2S) as the type, you must specify the CAP URL, server CA certificates, and client certificates.

6. If you want to modify any of the following settings, then click the Advanced Options icon to display the **Advanced Options** dialog window where you can make the changes:
   - The port number used to access the cloud tier
   - Enable or disable the **SSL** option that lets you transfer data securely to the cloud tier
7. **Optional:** If you want to add a cloud tier for StorageGRID or you want to use IBM Cloud Object Storage environment (such as Cleversafe) with FabricPool, you should specify a CA certificate. Specify the CA certificate by moving the **Object Store Certificate** toggle button and copying the contents of the certificate. Then paste the certificate contents in the signed certification.
8. From the **IPspace** list, select the IPspace that is used to connect to the cloud tier.
9. Click **Save** to save the cloud tier.
10. Click **Save and Attach Aggregates** to save the cloud tier and to attach aggregates to the cloud tier.

Attach an aggregate to a cloud tier

You can use System Manager to attach an All Flash aggregate to a cloud tier. You can store infrequently used data in cloud tiers.

Before you begin

You must have added a cloud tier to the cluster.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Cloud Tier**.
2. In the **Used in Aggregates** column, click **Attach Aggregates**.

   The Attach Aggregates window is displayed.
3. Select the aggregate that you want to attach to the cloud tier.
4. Click **Save**.

Provisioning storage by creating a FabricPool-enabled aggregate manually

You can use System Manager to create a FabricPool-enabled aggregate to attach a cloud tier to the SSD aggregate.

Before you begin

- You must have created a cloud tier and attached it to the cluster in which the SSD aggregate resides.
- An on-premises cloud tier must have been created.
- A dedicated network connection must exist between the cloud tier and the aggregate.

About this task

The following object stores can be used as cloud tiers:

- StorageGRID
- Alibaba Cloud (Starting with System Manager 9.6)
- Amazon Web Services (AWS) Simple Storage Service (S3)
- Amazon Web Services (AWS) Commercial Cloud Service (C2S)
- Microsoft Azure Blob storage
- IBM Cloud
- Google Cloud

- Azure Stack, which is an on-premises Azure services, is not supported.
- If you want to use any object store as a cloud tier, other than StorageGRID, you must have the FabricPool capacity license.

Steps

1. Create a FabricPool-enabled aggregate by using one of the following methods:
   - Click **Applications & Tiers** > **Storage Tiers** > **Add Aggregate**.
   - Click **Storage** > **Aggregate & Disks** > **Aggregates** > **Create**.
2. Enable the **Manually Create Aggregate** option to create an aggregate.
3. Create a FabricPool-enabled aggregate:
   a. Specify the name of the aggregate, the disk type, and the number of disks or partitions to include in the aggregate.

Only all flash (all SSD) aggregates support FabricPool-enabled aggregates.

The minimum hot spare rule is applied to the disk group that has the largest disk size.

b. **Optional:** Modify the RAID configuration of the aggregate:
   i. Click **Change**.
   ii. In the Change RAID Configuration dialog box, specify the RAID type and the RAID group size.

   Shared disks support two RAID types: RAID-DP and RAID-TEC.

   iii. Click **Save**.
4. Select the **FabricPool** checkbox, and then select a cloud tier from the list.
5. Click **Create**.

Change the tiering policy of a volume

You can use System Manager to change the default tiering policy of a volume to control whether the data of the volume is moved to the cloud tier when the data becomes inactive.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volume for which you want to change the tiering policy, and then click **More Actions** > **Change Tiering Policy**.
4. Select the required tiering policy from the **Tiering Policy** list, and then click **Save**.

Edit a cloud tier

You can use System Manager to modify the configuration information of cloud tier. The configuration details that you can edit include the name, fully qualified domain name (FQDN), port, access key ID, secret key, and object store certificate.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Cloud Tier**.
2. Select the cloud tier that you want to edit, and then click **Edit**.
3. In the **Edit Cloud Tier** window, modify the cloud tier name, FQDN, port, access key ID, secret key, and object store certificate, as required.

   If you have selected AWS Commercial Cloud Service (C2S) cloud tier, you can modify the server CA certificates, and client certificates.

4. Click **Save**.

Delete a cloud tier

You can use System Manager to delete a cloud tier that you no longer require.

Before you begin

You must have deleted the FabricPool-enabled aggregate that is associated with the cloud tier.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Cloud Tier**.
2. Select the cloud tier that you want to delete, and then click **Delete**.

What cloud tiers and tiering policies are

Cloud tiers provide storage for infrequently accessed data. You can attach an all-flash (all-SSD) aggregate to a cloud tier to store infrequently used data. You can use tiering policies to decide whether data should be moved to a cloud tier.

You can set one of the following tiering policies on a volume:

- **Snapshot-only**

  Moves the Snapshot copies of only those volumes that are currently not being referenced by the active file system. Snapshot-only policy is the default tiering policy.

- **Auto**

  Moves the inactive (cold) data and the Snapshot copies from the active file system to the cloud tier.

- **Backup (for System Manager 9.5)**

  Moves the newly transferred data of a data protection (DP) volume to the cloud tier.

- **All (starting with System Manager 9.6)**

  Moves all data to the cloud tier.

- **None**

  Prevents the data on the volume from being moved to a cloud tier.

What inactive (cold) data is

Infrequently accessed data in a performance tier is known as inactive (cold) data. By default, data that is not accessed for a period of 31 days becomes inactive.

Inactive data is displayed at the aggregate level, cluster level, and volume level. The inactive data for an aggregate or a cluster is displayed only if inactive scanning is complete on that aggregate or cluster. By default, inactive data is displayed for FabricPool-enabled aggregates and SSD aggregates. Inactive data is not displayed for FlexGroups.

Cloud Tier window

You can use System Manager to add, edit, and delete cloud tiers and to view cloud tier details.

The Cloud Tier window displays the total number of licensed cloud tiers in the cluster, the licensed space that is used in the cluster, and the licensed space that is available in the cluster. The Cloud Tier window also displays the unlicensed cloud capacity that is used.

Command buttons

- **Add**

Enables you to add a cloud tier.

- **Attach Aggregates**

  Enables you to attach aggregates to a cloud tier.

- **Delete**

  Enables you to delete a selected cloud tier.

- **Edit**

  Enables you to modify the properties of a selected cloud tier.

Details area

You can view detailed information about cloud tiers such as the list of cloud tiers, the details of the object stores, the aggregates used, and the used capacity.

If you create a cloud tier other than Alibaba Cloud, Amazon AWS S3, AWS Commercial Cloud Service (C2S), Google Cloud, IBM Cloud, Microsoft Azure Blob storage, or StorageGRID by using the command-line interface (CLI), this cloud tier is displayed as Others in System Manager. You can then attach aggregates to this cloud tier.

Related information

Installing a CA certificate if you use StorageGRID

Storage Tiers window

Manage aggregates with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create aggregates to support the differing security, backup, performance, and data sharing requirements of your users.

Aggregates window

You can use the Aggregates window to create, display, and manage information about aggregates.

Command buttons

- **Create**

  Opens the Create Aggregate dialog box, which enables you to create an aggregate.

- **Edit**

  Opens the Edit Aggregate dialog box, which enables you to change the name of an aggregate or the level of RAID protection that you want to provide for the aggregate.

- **Delete**

  Deletes the selected aggregate.

This button is disabled for the root aggregate.

- **More Actions**

  Provides the following options:

- **Change status to**

  Changes the status of the selected aggregate to one of the following statuses:

  - Online

    Read and write access to the volumes that are contained in this aggregate is allowed.

  - Offline

    Read and write access is not allowed.

  - Restrict

    Some operations—such as parity reconstruction—are allowed, but data access is not allowed.

- **Add Capacity**

  Enables you to add capacity (HDDs or SSDs) to existing aggregates.

- **Add Cache**

  Enables you to add cache disks (SSDs) to existing HDD aggregates or Flash Pool aggregates.

  This button is not available for a cluster containing nodes with All Flash Optimized personality.

- **Mirror**

  Enables you to mirror the aggregates.

- **Volume Move**

  Enables you to move a FlexVol volume.

- **Attach Cloud Tier**

  Enables you to attach a cloud tier to the aggregate.

- **Refresh**

  Updates the information in the window.

Aggregate list

Displays the name and the space usage information for each aggregate.

- **Status**

  Displays the status of the aggregate.

- **Name**

  Displays the name of the aggregate.

- **Node**

  Displays the name of the node to which the disks of the aggregate are assigned.

  This field is available only at the cluster level.

- **Type**

  Displays the type of the aggregate.

  This field is not displayed for a cluster containing nodes with All Flash Optimized personality.

- **Used (%)**

  Displays the percentage of space that is used in the aggregate.

- **Available Space**

  Displays the available space in the aggregate.

- **Used Space**

  Displays the amount of space that is used for data in the aggregate.

- **Total Space**

  Displays the total space of the aggregate.

- **FabricPool**

  Displays whether the selected aggregate is attached to a cloud tier.

- **Cloud Tier**

  If the selected aggregate is attached to a cloud tier, it displays the name of the cloud tier.

- **Volume Count**

  Displays the number of volumes that are associated with the aggregate.

- **Disk Count**

  Displays the number of disks that are used to create the aggregate.

- **Flash Pool**

  Displays the total cache size of the Flash Pool aggregate. A value of NA indicates that the aggregate is not a Flash Pool aggregate.

  This field is not displayed for a cluster containing nodes with All Flash Optimized personality.

- **Mirrored**

Displays whether the aggregate is mirrored.

- **SnapLock Type**

  Displays the SnapLock type of the aggregate.

Details area

Select an aggregate to view information about the selected aggregate. You can click Show More Details to view detailed information about the selected aggregate.

- **Overview tab**

  Displays detailed information about the selected aggregate, and displays a pictorial representation of the space allocation of the aggregate, the space savings of the aggregate, and the performance of the aggregate in IOPS and total data transfers.

- **Disk Information tab**

  Displays disk layout information such as the name of the disk, disk type, physical size, usable size, disk position, disk status, plex name, plex status, RAID group, RAID type, and storage pool (if any) for the selected aggregate. The disk port that is associated with the disk primary path and the disk name with the disk secondary path for a multipath configuration are also displayed.

- **Volumes tab**

  Displays details about the total number of volumes on the aggregate, total aggregate space, and the space committed to the aggregate.

- **Performance tab**

  Displays graphs that show the performance metrics of the aggregates, including throughput and IOPS. Performance metrics data for read, write, and total transfers is displayed for throughput and IOPS, and the data for SSDs and HDDs is recorded separately.

  Changing the client time zone or the cluster time zone impacts the performance metrics graphs. You should refresh your browser to view the updated graphs.

Related information

Provisioning storage through aggregates

Deleting aggregates

Editing aggregates

Manage storage pools with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create storage pools to enable SSDs to be shared by multiple Flash Pool aggregates.

Create a storage pool

A storage pool is a collection of SSDs (cache disks). You can use System Manager to combine SSDs to create a storage pool, which enables you to share the SSDs and SSD spares between an HA pair for allocation to two or more Flash Pool aggregates at the same time.

Before you begin

- Both nodes of the HA pair must be up and running in order to allocate SSDs and SSD spares through a storage pool.
- Storage pools must have a minimum of 3 SSDs.
- All SSDs in a storage pool must be owned by the same HA pair.

About this task

System Manager enforces the hot spare rule for SSD RAID groups when you use SSDs for adding disks to a storage pool. For example, if there are 10 SSDs in the SSD RAID group and the option `raid.min_spare_count` is set to `1` at the node level, System Manager leaves 1 SSD as the hot spare and uses the other 9 SSDs for SSD-related operations.

You cannot use partitioned SSDs when creating a storage pool by using System Manager.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Storage Pools**.
2. In the **Storage Pools** window, click **Create**.
3. In the **Create Storage Pool** dialog box, specify the name for the storage pool, disk size, and the number of disks.
4. Click **Create**.

Add disks to a storage pool

You can add SSDs to an existing storage pool and increase its cache size by using System Manager.

Before you begin

Both nodes of the HA pair must be up and running in order to allocate SSDs and SSD spares through a storage pool.

About this task

- The SSDs that you add to a storage pool are distributed proportionally among the aggregates using the storage pool cache and to the free space of the storage pool.
- System Manager enforces the hot spare rule for SSD RAID groups when you use SSDs for adding disks to a storage pool.

  For example, if there are 10 SSDs in the SSD RAID group and the option `raid.min_spare_count` is set to `1` at the node level, System Manager leaves 1 SSD as the hot spare and uses the other 9 SSDs for SSD-related operations.

- You cannot use partitioned SSDs when adding disks to a storage pool by using System Manager.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Storage Pools**.
2. In the **Storage Pools** window, select the storage pool, and then click **Add Disks**.

3. In the **Add Disks** dialog box, specify the number of disks that you want to add.
4. Click **Next**.
5. In the **Summary** dialog box, review how the cache is distributed among various aggregates and the free space of the storage pool.
6. Click **Add**.

Delete storage pools

You might want to delete a storage pool when the cache of the storage pool is not optimal or when it is no longer used by any aggregate or Flash Pool aggregate. You can delete a storage pool by using the Delete Storage Pool dialog box in System Manager.

Before you begin

The storage pool must not be used by any aggregate.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Storage Pools**.
2. In the **Storage Pools** window, select the storage pool that you want to delete, and then click **Delete**.
3. In the **Delete Storage Pool** dialog box, click **Delete**.

Use SSD storage pools

To enable SSDs to be shared by multiple Flash Pool aggregates, you can add the SSDs to a *storage pool*. After you add an SSD to a storage pool, you can no longer manage the SSD as a stand-alone entity. You must use the storage pool to assign or allocate the storage that is provided by the SSD.

You can create storage pools for a specific high-availability (HA) pair. Then, you can add allocation units from that storage pool to one or more Flash Pool aggregates that are owned by the same HA pair. Just as disks must be owned by the same node that owns an aggregate before the disks can be allocated to it, storage pools can provide storage only to the Flash Pool aggregates that are owned by one of the nodes that owns the storage pool.

If you have to increase the amount of Flash Pool cache on your system, you can add more SSDs to a storage pool, up to the maximum RAID group size for the RAID type of the Flash Pool caches that are using the storage pool. When you add an SSD to an existing storage pool, you increase the size of the storage pool's allocation units, including any allocation units that are already allocated to a Flash Pool aggregate.

You can use only one spare SSD for a storage pool, so that if an SSD in that storage pool becomes unavailable, ONTAP can use the spare SSD to reconstruct the partitions of the malfunctioning SSD. You do not have to reserve any allocation units as spare capacity; ONTAP can use only a full, unpartitioned SSD as a spare for the SSDs in a storage pool.

After you add an SSD to a storage pool, you cannot remove the SSD, just as you cannot remove disks from an aggregate. If you want to use the SSDs in a storage pool as discrete drives again, you must destroy all of the Flash Pool aggregates to which the storage pool's allocation units have been allocated, and then destroy the storage pool.

Requirements and best practices for using SSD storage pools

Some technologies cannot be combined with Flash Pool aggregates that use SSD storage pools.

You cannot use the following technologies with Flash Pool aggregates that use SSD storage pools for their

cache storage:

- MetroCluster
- SyncMirror functionality

  Mirrored aggregates can coexist with Flash Pool aggregates that use storage pools; however, Flash Pool aggregates cannot be mirrored.

- Physical SSDs

  Flash Pool aggregates can use SSD storage pools or physical SSDs, but not both.

SSD storage pools must conform to the following rules:

- SSD storage pools can contain only SSDs; HDDs cannot be added to an SSD storage pool.
- All of the SSDs in an SSD storage pool must be owned by the same high-availability (HA) pair.
- You cannot use SSDs that have been partitioned for root-data partitioning in a storage pool.

If you provide storage from a single storage pool to two caches with different RAID types, and you expand the size of the storage pool beyond the maximum RAID group size for RAID4, the extra partitions in the RAID4 allocation units go unused. Therefore, it is a best practice to keep your cache RAID types homogenous for a storage pool.

You cannot change the RAID type of cache RAID groups that are allocated from a storage pool. You set the RAID type for the cache before adding the first allocation units, and you cannot change the RAID type later.

When you create a storage pool or add SSDs to an existing storage pool, you must use the same size SSDs. If a failure occurs and no spare SSD of the correct size exists, ONTAP can use a larger SSD to replace the failed SSD. However, the larger SSD is right-sized to match the size of the other SSDs in the storage pool, resulting in lost SSD capacity.

You can use only one spare SSD for a storage pool. If the storage pool provides allocation units to the Flash Pool aggregates that are owned by both nodes in the HA pair, then the spare SSD can be owned by either node. However, if the storage pool provides allocation units only to the Flash Pool aggregates that are owned by one of the nodes in the HA pair, then the SSD spare must be owned by that same node.

Considerations for when to use SSD storage pools

SSD storage pools provide many benefits, but they also introduce some restrictions that you should be aware of when deciding whether to use SSD storage pools or dedicated SSDs.

SSD storage pools make sense only when they are providing cache to two or more Flash Pool aggregates. SSD storage pools provide the following benefits:

- Increased storage utilization for SSDs used in Flash Pool aggregates

  SSD storage pools reduce the overall percentage of SSDs needed for parity by enabling you to share parity SSDs between two or more Flash Pool aggregates.

- Ability to share spares between HA partners

  Because the storage pool is effectively owned by the HA pair, one spare, owned by one of the HA partners, can function as a spare for the entire SSD storage pool if needed.

- Better utilization of SSD performance

  The high performance provided by SSDs can support access by both controllers in an HA pair.

These advantages must be weighed against the costs of using SSD storage pools, which include the following items:

- Reduced fault isolation

  The loss of a single SSD affects all RAID groups that include one of its partitions. In this situation, every Flash Pool aggregate that has cache allocated from the SSD storage pool that contains the affected SSD has one or more RAID groups in reconstruction.

- Reduced performance isolation

  If the Flash Pool cache is not properly sized, there can be contention for the cache between the Flash Pool aggregates that are sharing it. This risk can be mitigated with proper cache sizing and QoS controls.

- Decreased management flexibility

  When you add storage to a storage pool, you increase the size of all Flash Pool caches that include one or more allocation units from that storage pool; you cannot determine how the extra capacity is distributed.

Considerations for adding SSDs to an existing storage pool versus creating a new one

You can increase the size of your SSD cache in two ways—by adding SSDs to an existing SSD storage pool or by creating a new SSD storage pool. The best method for you depends on your configuration and plans for the storage.

The choice between creating a new storage pool and adding storage capacity to an existing one is similar to deciding whether to create a new RAID group or add storage to an existing one:

- If you are adding a large number of SSDs, creating a new storage pool provides more flexibility because you can allocate the new storage pool differently from the existing one.
- If you are adding only a few SSDs, and increasing the RAID group size of your existing Flash Pool caches is not an issue, then adding SSDs to the existing storage pool keeps your spare and parity costs lower, and automatically allocates the new storage.

If your storage pool is providing allocation units to Flash Pool aggregates whose caches have different RAID types, and you expand the size of the storage pool beyond the maximum RAID4 RAID group size, the newly added partitions in the RAID4 allocation units are unused.

Why you add disks to storage pools

You can add SSDs to an existing storage pool and increase its cache size. When you add SSDs to a storage pool that has allocation units already allocated to Flash Pool aggregates, you increase the cache size of each of those aggregates and the total cache of the storage pool.

If the allocation units of the storage pool are not yet allocated, adding SSDs to that storage pool does not affect the SSD cache size.

When you add SSDs to an existing storage pool, the SSDs must be owned by one node or the other of the same HA pair that already owned the existing SSDs in the storage pool. You can add SSDs that are owned by either node of the HA pair.

How storage pool works

A *storage pool* is a collection of SSDs. You can combine SSDs to create a storage pool, which enables you to share the SSDs and SSD spares across multiple Flash Pool aggregates, at the same time.

Storage pools consist of allocation units, which you can use to provide SSDs and SSD spares to aggregates or to increase the existing SSD size.

After you add an SSD to a storage pool, you can no longer use the SSD as an individual disk. You must use the storage pool to assign or allocate the storage provided by the SSD.

Storage Pools window

You can use the Storage Pools window to create, display, and manage a dedicated cache of SSDs, also known as *storage pools*. These storage pools can be associated with a non-root aggregate to provide SSD cache and with a Flash Pool aggregate to increase its size.

This page is not available for a cluster containing nodes with All Flash Optimized personality.

Command buttons

- **Create**

  Opens the Create Storage Pool dialog box, which enables you to create a storage pool.

- **Add Disks**

  Opens the Add Disks dialog box, which enables you to add cache disks to a storage pool.

- **Delete**

  Deletes the selected storage pool.

- **Refresh**

  Updates the information in the window.

Storage pools list

- **Name**

  Displays the name of the storage pool.

- **Total Cache**

  Displays the total cache size of the storage pool.

- **Spare Cache**

  Displays the available spare cache size of the storage pool.

- **Used Cache (%)**

  Displays the percentage of used cache size of the storage pool.

- **Allocation Unit**

  Displays the minimum allocation unit of the total cache size that you can use to increase the size of your storage pool.

- **Owner**

  Displays the name of the HA pair or the node with which the storage pool is associated.

- **State**

  Displays the state of the storage pool, which can be Normal, Degraded, Creating, Deleting, Reassigning, or Growing.

- **Is Healthy**

  Displays whether storage pool is healthy or not.

Details tab

Displays detailed information about the selected storage pool, such as the name, health, storage type, disk count, total cache, spare cache, used cache size (in percent), and allocation unit. The tab also displays the names of the aggregates that are provisioned by the storage pool.

Disks tab

Displays detailed information about the disks in the selected storage pool, such as the names, disk types, useable size, and total size.

Related information

Provisioning storage by creating a Flash Pool aggregate manually

Provisioning cache by adding SSDs

Disk and aggregate management

Reassign disks to nodes with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to reassign the ownership of spare disks from one node to another node to increase the capacity of an aggregate or storage pool.

About this task

- You can reassign disks if the following conditions are true:
  - The container type of the selected disks must be “spare” or “shared”.
  - The disks must be connected to nodes in an HA configuration.
  - The disks must be visible to the node.
- You *cannot* reassign a disk if the following conditions are true:
  - The container type of the selected disk is “shared”, and the data partition is not spare.
  - The disk is associated with a storage pool.

- You cannot reassign the data partition of shared disks if storage failover is not enabled on the nodes that are associated with the shared disks.
- For partition disks, you can reassign only the data partition of the disks.
- For MetroCluster configurations, you cannot use System Manager to reassign disks.

  You must use the command-line interface to reassign disks for MetroCluster configurations.

In later ONTAP releases, you use the ONTAP CLI to remove disk ownership and then assign a new owner.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Disks**.
2. In the **Disks** window, select the **Inventory** tab.
3. Select the disks that you want to reassign, and then click **Assign**.
4. In the **Warning** dialog box, click **Continue**.
5. In the **Assign Disks** dialog box, select the node to which you want to reassign the disks.
6. Click **Assign**.

Related information

- Remove disk ownership using the ONTAP CLI (ONTAP 9.3 and later)
- Assign disks automatically using the ONTAP CLI (ONTAP 9.3 and later)
- Manually assign disks using the ONTAP CLI (ONTAP 9.3 and later)

Disks

View disk information with System Manager - ONTAP 9.7 and earlier

You can use the Disks window in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to view the name, size, and container details of disks along with graphical information about capacity disks and cache disks.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Disks**.
2. Select the disk that you want to view information about from the displayed list of disks.
3. Review the disk details.

Related information

Disks window

How ONTAP reports disk types in System Manager - ONTAP 9.7 and earlier

ONTAP System Manager classic (available in ONTAP 9.7 and earlier) associates a type with every disk. ONTAP reports some disk types differently than the industry standards; you should understand how ONTAP disk types map to industry standards to avoid confusion.

When ONTAP documentation refers to a disk type, it is the type used by ONTAP unless otherwise specified. *RAID disk types* denote the role that a specific disk plays for RAID. RAID disk types are not related to ONTAP disk types.

For a specific configuration, the disk types that are supported depend on the storage system model, the shelf type, and the I/O modules that are installed in the system.

The following tables show how ONTAP disk types map to industry standard disk types for the SAS and FC storage connection types, and for storage arrays.

SAS-connected storage

ONTAP disk type	Disk class	Industry standard disk type	Description
BSAS	Capacity	SATA	Bridged SAS-SATA disks with added hardware to enable them to be plugged into a SAS-connected storage shelf
FSAS	Capacity	NL-SAS	Near Line SAS
MSATA	Capacity	SATA	SATA disk in multi-disk carrier storage shelf
SAS	Performance	SAS	Serial-Attached SCSI
SSD	Ultra-performance	SSD	Solid-state drives

FC-connected storage

ONTAP disk type	Disk class	Industry standard disk type
ATA	Capacity	SATA
FCAL	Performance	FC

Storage arrays

ONTAP disk type	Disk class	Industry standard disk type	Description
LUN	N/A	LUN	Logical storage device that is backed by storage arrays and used by ONTAP as a disk These LUNs are referred to as *array LUNs* to distinguish them from the LUNs that ONTAP serves to clients.

Related information

NetApp Hardware Universe

NetApp Technical Report 3437: Storage Subsystem Resiliency

Determine when it is safe to remove a multi-disk carrier with System Manager - ONTAP 9.7 and earlier

Removing a multi-disk carrier before it is safe to do so can result in one or more RAID groups becoming degraded, or possibly even a storage disruption. ONTAP System Manager classic (available in ONTAP 9.7 and earlier) enables you to determine when it is safe to remove a multi-disk carrier.

When a multi-disk carrier has to be replaced, the following events must have occurred before you can remove the carrier safely:

- An AutoSupport message must have been logged indicating that the carrier is ready to be removed.
- An EMS message must have been logged indicating that the carrier is ready to be removed.
- The state of both disks in the carrier must be displayed as `broken` in the Disks window.

  You must remove the disks only after the carrier mate of a failed disk is evacuated. You can click Details to view the disk evacuation status in the Properties tab of the Disks window.
- The fault LED (amber) on the carrier must be lit continuously indicating that it is ready for removal.
- The activity LED (green) must be turned off indicating there is no disk activity.
- The shelf digital display only shows the shelf ID number.

> You cannot reuse the carrier mate of a failed disk. When you remove a multi-disk carrier that contains a failed disk, you must replace it with a new carrier.

Disks window in System Manager - ONTAP 9.7 and earlier

You can use the Disks window in ONTAP System Manager classic (avaiable in ONTAP 9.7 and earlier) to view all the disks in your storage system.

Command buttons

- **Assign**

  Assigns or reassigns the ownership of the disks to a node.

  This button is enabled only if the container type of the selected disks is unassigned, spare, or shared.

- **Zero Spares**

  Erases all the data, and formats the spare disks and array LUNs.

- **Refresh**

  Updates the information in the window.

Tabs

Summary

Displays detailed information about the disks in the cluster, including the size of the spare disks and assigned disks. The tab also graphically displays information about spare disks, aggregates, and root aggregates for HDDs and information about spare disks, disks in a storage pool, aggregates, Flash Pool aggregates, and root aggregates for cache disks (SSDs).

The HDD panel is not displayed for systems with All Flash Optimized personality.

The details panel provides additional information about partitioned and unpartitioned spare disks (disk type, node, disk size, RPM, checksum, number of available disks, and spare capacity), in tabular format.

Inventory

- **Name**

  Displays the name of the disk.

- **Container Type**

  Displays the purpose for which the disk is used. The possible values are Aggregate, Broken, Foreign, Label Maintenance, Maintenance, Shared, Spare, Unassigned, Volume, Unknown, and Unsupported.

- **Partition Type**

  Displays the partition type of the disk.

- **Node Name**

  Displays the name of the node that contains the aggregate.

  This field is available only at the cluster level.

- **Home owner**

  Displays the name of the home node to which this disk is assigned.

- **Current owner**

Displays the name of the node that currently owns this disk.

- **Root owner**

  Displays the name of the node that currently owns the root partition of this disk.

- **Data Owner**

  Displays the name of the node that currently owns the data partition of this disk.

- **Data1 Owner**

  Displays the name of the node that currently owns the data1 partition of the disk.

- **Data2 Owner**

  Displays the name of the node that currently owns the data2 partition of the disk.

- **Storage Pool**

  Displays the name of the storage pool with which the disk is associated.

- **Type**

  Displays the type of the disk.

- **Firmware Version**

  Displays the firmware version of the disk.

- **Model**

  Displays the model of the disk.

- **RPM**

  Displays the effective speed of the disk drive when the option `raid.mix.hdd.rpm.capacity` is enabled, and displays the actual speed of the disk drive when the option `raid.mix.hdd.rpm.capacity` is disabled.

  This field is not applicable to SSDs.

- **Effective Size**

  Displays the usable space available on the disk.

- **Physical Space**

  Displays the total physical space of the disk.

- **Shelf**

  Displays the shelf on which the physical disks are located.

  This field is hidden by default.

- **Bay**

  Displays the bay within the shelf for the physical disk.

  This field is hidden by default.

- **Pool**

  Displays the name of the pool to which the selected disk is assigned.

  This field is hidden by default.

- **Checksum**

  Displays the type of the checksum.

  This field is hidden by default.

- **Carrier ID**

  Specifies information about disks that are located within the specified multi-disk carrier. The ID is a 64-bit value.

  This field is hidden by default.

Inventory details area

The area below the inventory tab displays detailed information about the selected disk, including information about the aggregate or volume (if applicable), vendor ID, zeroing state (in percent), serial number of the disk, and error details in case of a broken disk. For shared disks, the Inventory details area displays the names of all the aggregates, including the root and the non-root aggregates.

Related information

Viewing disk information

Manage array LUNs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to assign array LUNs to an existing aggregate and manage array LUNs.

Assign array LUNs

You can use System Manager to assign unassigned array LUNs to an existing aggregate to increase the size of the aggregate.

About this task

- You can assign array LUNs if the following conditions are true:
  - The container type of the selected array LUNs must be “unassigned”.
  - The disks must be connected to nodes in an HA pair.
  - The disks must be visible to the node.
- For MetroCluster configurations, you cannot use System Manager to assign array LUNs as spares.

You must use the command-line interface instead.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Array LUNs**.
2. Select the array LUNs, and then click **Assign**.
3. In the **Assign Array LUNs** dialog box, select the node to which you want to assign the array LUNs.
4. Click **Assign**.

Reassign spare array LUNs to nodes

You can use System Manager to reassign the ownership of spare array LUNs from one node to another to increase the capacity of an aggregate.

About this task

- You can reassign array LUNs if the following conditions are true:
  - The container type of the selected array LUNs must be “spare”.
  - The disks must be connected to nodes in an HA pair.
  - The disks must be visible to the node.
- For MetroCluster configurations, you cannot use System Manager to reassign array LUNs as spares.

  You must use the command-line interface instead.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Array LUNs**.
2. Select the spare array LUNs that you want to reassign, and then click **Assign**.
3. In the **Warning** dialog box, click **Continue**.
4. In the **Assign Array LUNs** dialog box, select the node to which you want to reassign the spare array LUNs.
5. Click **Assign**.

Zeroing spare array LUNs

You can use System Manager to erase all the data and to format the spare array LUNs by writing zeros to the array LUNs. These array LUNs can then be used in new aggregates.

About this task

When you zero the spare array LUNs, all the spares in the cluster, including disks, are zeroed. You can zero the spare array LUNs for a specific node or for the entire cluster.

Steps

1. Click **Storage** > **Aggregates & Disks** > **Array LUNs**.
2. Click **Zero Spares**.
3. In the **Zero Spares** dialog box, select a node or “All nodes” from which you want to zero the array LUNs.
4. Select the **Zero all non-zeroed spares** check box to confirm the zeroing operation.
5. Click **Zero Spares**.

About disks and array LUNs

A disk is the basic unit of storage for storage systems that use ONTAP software to access native disk shelves. An array LUN is the basic unit of storage that third-party storage arrays provide to storage systems that run ONTAP software.

ONTAP software enables you to assign ownership to your disks and array LUNs, and to add them to an aggregate. ONTAP software also provides a number of ways to manage your disks, including removing them, replacing them, and sanitizing them. Because array LUNs are provided by the third-party storage array, you use the third-party storage array for all other management tasks for array LUNs.

You can create an aggregate using either disks or array LUNs. After you have created the aggregate, you manage it using ONTAP software in exactly the same way, whether it was created from disks or array LUNs.

Array LUNs window

The Array LUNs window enables you to assign ownership to your array LUNs and to add them to an aggregate.

The Array LUNs link in the left navigation pane is displayed only if there are any spare array LUNs, or if the V_StorageAttach license is installed.

Command buttons

- **Assign**

  Enables you to assign or reassign the ownership of array LUNs to a node.

- **Zero Spares**

  Erases all the data, and formats the spare array LUNs and disks.

- **Refresh**

  Updates the information in the window.

Array LUN list

Displays information such as the name, state, and vendor for each array LUN.

- **Name**

  Specifies the name of the array LUN.

- **State**

  Specifies the state of the array LUN.

- **Vendor**

  Specifies the name of the vendor.

- **Used Space**

  Specifies the space used by the array LUN.

- **Total Size**

  Specifies the size of the array LUN.

- **Container**

  Specifies the aggregate to which the array LUN belongs.

- **Node name**

  Specifies the name of the node to which the array LUN belongs.

- **Home owner**

  Displays the name of the home node to which the array LUN is assigned.

- **Current owner**

  Displays the name of the node that currently owns the array LUN.

- **Array name**

  Specifies the name of the array.

- **Pool**

  Displays the name of the pool to which the selected array LUN is assigned.

Details area

The area below the Array LUNs list displays detailed information about the selected array LUN.

Related information

FlexArray virtualization installation requirements and reference

Manage nodes with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to view the details of the nodes in the cluster.

Initialize the ComplianceClock time

You can use System Manager to initialize the ComplianceClock time to the current cluster time. You must initialize the ComplianceClock time in order to create SnapLock aggregates.

Before you begin

The SnapLock license must be installed.

About this task

You cannot modify or stop the ComplianceClock time after it is initialized.

Steps

1. Click **Storage** > **Nodes**.
2. Select the node, and then click **Initialize ComplianceClock**.
3. In the **Initialize ComplianceClock** dialog box, click **Yes** to initialize the ComplianceClock time to the current cluster time.

Nodes window

You can use the Nodes window to view the details of the nodes in a cluster.

Command buttons

- **Initialize ComplianceClock**

  Initializes the ComplianceClock of the selected node to the current value of the system clock.

- **Refresh**

  Updates the information in the window.

Nodes list

- **Name**

  Displays the name of the node.

- **State**

  Displays the state of the node (whether the node is up or down).

- **Up Time**

  Displays the duration for which the node is up.

- **ONTAP Version**

  Displays the ONTAP version that is installed on the node.

- **Model**

  Displays the platform model number of the node.

- **System ID**

  Displays the ID of the node.

- **Serial No**

  Displays the serial number of the node.

Details area

Displays detailed information about the selected node.

- **Details tab**

Displays information related to the selected node such as the name of the node, the state of the node, and the duration for which the node is up.

- **Performance tab**

  Displays the throughput, IOPS, and latency of the selected node.

  Changing the client time zone or the cluster time zone impacts the performance metrics graphs. You should refresh your browser to view the updated graphs.

Manage hardware cache with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage Hardware Cache modules.

Flash Cache is known as Hardware Cache in System Manager.

Enable or disable Flash Cache modules

You can enable or disable the external cache functionality for a storage system that has a Flash Cache module installed by using System Manager. You can enable Flash Cache modules based on the workload requirements of your storage system.

Steps

1. Click **Configuration** > **Hardware Cache**
2. If you want to modify a module or modules, move the slider button to enable or disable each module, as required.

How Flash Cache modules work

Using Flash Cache modules improves the performance of a storage system. The impact of using Flash Cache modules is displayed on the Hardware Cache window.

You can configure Flash Cache modules and disks based on the workload requirements of a storage system. By determining the read workload (number of read operations) served by Flash Cache modules and disks, you can analyze the performance of the storage system.

Flash Cache modules do not contain any data during the storage system boot or when control is returned to the storage system after a takeover event. Therefore, disks serve all the data read requests of the storage system.

The Flash Cache module is slowly populated with data when data read requests are served. Because the data read requests served by Flash Cache modules are faster than those served by the disks, the performance of the storage system improves.

Data read requests served by the Flash Cache module replace the data read requests served by the disks, and therefore, the performance improvement in the storage system is directly related to the disk reads that are replaced. To understand the impact of Flash Cache modules on storage system performance, you must view the read workload graph in the Hardware Cache window when the Flash Cache module contains data.

Hardware Cache window

You can use the Hardware Cache window to enable or disable Flash Cache modules for a storage system that has a Flash Cache module installed. You can also view the read-workload statistics.

Module Information

- **Storage system name**

  The name of the storage system that has a Flash Cache module installed displays under the graphic.

- **Enable/Disable toggle button**

  Move the toggle button to enable or disable the module.

- **Size**

  The size of the module in gigabytes. If there are multiple Flash Cache module cards, the total cache size from all of the cards is displayed.

  > The Flash Cache module size that is displayed differs from the actual size for the following reasons:
  > - System Manager reports only the usable capacity that is provided by ONTAP.
  > - A portion of the total capacity is reserved for storing metadata.

- **Model Names**

  The model names of the modules.

- **System Read Latency**

  Displays the average read latency in milliseconds.

Cache Read Workload

Indicates storage system performance by displaying a graph specifying the rate of the read workload that is served by the disks and the Flash Cache module.

Manage events with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to view the event log and event notifications.

Events window

You can use the Events window to view the event log and event notifications.

Command buttons

- **Refresh**

  Updates the information in the window.

Events list

- **Time**

  Displays the time when the event occurred.

- **Node**

  Displays the node and the cluster on which the event occurred.

- **Severity**

  Displays the severity of the event. The possible severity levels are:

  - Emergency

    Specifies that the event source unexpectedly stopped, and the system experienced unrecoverable data loss. You must take corrective action immediately to avoid extended downtime.

  - Alert

    Specifies that the event source has an alert, and action must be taken to avoid downtime.

  - Critical

    Specifies that the event source is critical, and might lead to service disruption if corrective action is not taken immediately.

  - Error

    Specifies that the event source is still performing, and a corrective action is required to avoid service disruption.

  - Warning

    Specifies that the event source experienced an occurrence that you must be aware of. Events of this severity might not cause service disruption; however, corrective action might be required.

  - Notice

    Specifies that the event source is normal, but the severity is a significant condition that you must be aware of.

  - Informational

    Specifies that the event source has an occurrence that you must be aware of. No corrective action might be required.

  - Debug

    Specifies that the event source includes a debugging message.

  By default, the alert severity type, emergency severity type, and the error severity type are displayed.

- **Source**

Displays the source of the event.

- **Event**

  Displays the description of the event.

Details area

Displays the event details, including the event description, message name, sequence number, message description, and corrective action for the selected event.

Manage system alerts with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to monitor different parts of a cluster.

Acknowledge system health alerts

You can use System Manager to acknowledge and respond to system health alerts for subsystems. You can use the information displayed to take the recommended action and correct the problem reported by the alert.

Steps

1. Click **Events & Jobs** > **System Alerts**.
2. In the **System Alerts** window, click the arrow icon next to the name of subsystem.
3. Select the alert that you want to acknowledge, and then click **Acknowledge**.
4. Type your name, and then click **Acknowledge**.

Suppress system health alerts

You can use System Manager to suppress system health alerts that do not require any intervention from you.

Steps

1. Click **Events & Jobs** > **System Alerts**.
2. In the **System Alerts** window, click the arrow icon next to the name of subsystem.
3. Select the alert that you want to suppress, and then click **Suppress**.
4. Type your name, and then click **Suppress**.

Delete system health alerts

You can use System Manager to delete system health alerts to which you have already responded.

Steps

1. Click **Events & Jobs** > **System Alerts**.
2. In the **System Alerts** window, click the arrow icon next to the name of subsystem.
3. Select the alert that you want to delete, and then click **Delete**.
4. Click **OK**.

Available cluster health monitors

There are several health monitors that monitor different parts of a cluster. Health monitors help you to recover from errors within ONTAP systems by detecting events, sending alerts to you, and deleting events as they clear.

Health monitor name (identifier)	Subsystem name (identifier)	Purpose
Cluster switch(cluster-switch)	Switch (Switch-Health)	Monitors cluster network switches and management network switches for temperature, utilization, interface configuration, redundancy (cluster network switches only), and fan and power supply operation. The cluster switch health monitor communicates with switches through SNMP. SNMPv2c is the default setting. Beginning with ONTAP 9.2, this monitor can detect and report when a cluster switch has rebooted since the last polling period.
MetroCluster Fabric	Switch	Monitors the MetroCluster configuration back-end fabric topology and detects misconfigurations such as incorrect cabling and zoning, and ISL failures.
MetroCluster Health	Interconnect, RAID, and storage	Monitors FC-VI adapters, FC initiator adapters, left-behind aggregates and disks, and inter-cluster ports
Node connectivity(node-connect)	CIFS nondisruptive operations (CIFS-NDO)	Monitors SMB connections for nondisruptive operations to Hyper-V applications.
	Storage (SAS-connect)	Monitors shelves, disks, and adapters at the node level for appropriate paths and connections.
System	not applicable	Aggregates information from other health monitors.

Health monitor name (identifier)	Subsystem name (identifier)	Purpose
System connectivity (system-connect)	Storage (SAS-connect)	Monitors shelves at the cluster level for appropriate paths to two HA clustered nodes.

Ways to respond to system health alerts

When a system health alert occurs, you can acknowledge it, learn more about it, repair the underlying condition, and prevent it from occurring again.

When a health monitor raises an alert, you can respond in any of the following ways:

- Get information about the alert, which includes the affected resource, alert severity, probable cause, possible effect, and corrective actions.
- Get detailed information about the alert, such as the time when the alert was raised and whether anyone else has acknowledged the alert already.
- Get health-related information about the state of the affected resource or subsystem, such as a specific shelf or disk.
- Acknowledge the alert to indicate that someone is working on the problem, and identify yourself as the “Acknowledger.”
- Resolve the problem by taking the corrective actions provided in the alert, such as fixing cabling to resolve a connectivity problem.
- Delete the alert, if the system did not automatically clear it.
- Suppress an alert to prevent it from affecting the health status of a subsystem.

  Suppressing is useful when you understand a problem. After you suppress an alert, it can still occur, but the subsystem health displays as “ok-with-suppressed.” when the suppressed alert occurs.

System Alerts window

You can use the System Alerts window to learn more about system health alerts. You can also acknowledge, delete, and suppress alerts from the window.

Command buttons

- **Acknowledge**

  Enables you to acknowledge the selected alert to indicate that the problem is being addressed and identifies the person who clicks the button as the “Acknowledger.”

- **Suppress**

  Enables you to suppress the selected alert to prevent the system from notifying you about the same alert again and identifies you as the “Suppressor.”

- **Delete**

  Deletes the selected alert.

- **Refresh**

Updates the information in the window.

Alerts list

- **SubSystem (No. of Alerts)**

  Displays the name of the subsystem, such as the SAS connection, switch health, CIFS NDO, or MetroCluster, for which the alert is generated.

- **Alert ID**

  Displays the alert ID.

- **Node**

  Displays the name of the node for which the alert is generated.

- **Severity**

  Displays the severity of the alert as Unknown, Other, Information, Degraded, Minor, Major, Critical, or Fatal.

- **Resource**

  Displays the resource that generated the alert, such as a specific shelf or disk.

- **Time**

  Displays the time when the alert was generated.

Details area

The details area displays detailed information about the alert, such as the time when the alert was generated and whether the alert has been acknowledged. The area also includes information about the probable cause and possible effect of the condition generated by the alert, and the recommended actions to correct the problem reported by the alert.

Related information

System administration

Manage AutoSupport notifications with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to configure AutoSupport notifications that help you to monitor your storage system health.

Set up AutoSupport notifications

You can use the Edit AutoSupport Settings dialog box in System Manager to set up AutoSupport notifications by specifying an email address from which email notifications are sent and adding multiple email host names.

Steps

1. Click ⚙ > **AutoSupport**.
2. Select the node, and then click **Edit**.

3. In the **Email Recipient** tab, type the email address from which email notifications are sent, specify the email recipients and the message content for each email recipient, and add the mail hosts.

   You can add up to five email addresses of the host names.

4. In the **Others** tab, select a transport protocol for delivering the email messages from the drop-down list and specify the HTTP or HTTPS proxy server details.
5. Click **OK**.
6. Verify that configuration you have set for AutoSupport notification is set up correctly in the **AutoSupport** window.

Enable or disable AutoSupport settings

You can enable or disable AutoSupport settings on your storage system by using System Manager. AutoSupport messages enable you to monitor your storage system health or send notifications to technical support and your internal support organization.

About this task

The AutoSupport option is enabled by default.

Steps

1. Click ⚙ > **AutoSupport**.
2. Select the node, and then click **Enable** or **Disable**.
3. Click **OK**.
4. Verify that the AutoSupport status correctly displays the change you made.

Add AutoSupport email recipients

You can use the **Email Recipient** tab of the Edit AutoSupport Settings dialog box in System Manager to add email addresses of the recipients of AutoSupport notifications.

Steps

1. Click ⚙ > **AutoSupport**.
2. Select the node, and then click **Edit**.
3. In the **Email Recipient** tab, type the address of the email recipient, specify whether the recipient receives a full message or a short message, and then click **Add**.
4. Click **OK**.
5. Verify that the details you specified are displayed in the **AutoSupport** window.

Test AutoSupport settings

You can use the AutoSupport Test dialog box in System Manager to test that you have configured the AutoSupport settings correctly.

Steps

1. Click ⚙ > **AutoSupport**.
2. Select the node, and then click **Test**.
3. In the **AutoSupport Test** dialog box, enter the AutoSupport subject text “Test AutoSupport” or any text that notifies the recipients that you are testing the AutoSupport settings.

4. Click **Test**.

   An email message with the subject “Test AutoSupport” or the text that you typed in the **AutoSupport subject** field is sent to the specified recipients.

Generate AutoSupport data

You can use System Manager to generate AutoSupport data for a single node or multiple nodes to monitor their health and to send notifications to technical support.

Steps

1. Click ⚙ > **AutoSupport**.
2. Select the node, and then click **AutoSupport Request** > **Generate AutoSupport**.

   By default, the AutoSupport data is generated for all nodes.

3. In the **Generate AutoSupport** dialog box, perform the following steps:
   a. If you want to generate AutoSupport data for a specific node, clear the **Generate Autosupport data for all nodes** check box, and then select the node.
   b. Type the case number.
4. Click **Generate**.
5. In the **Confirmation** dialog box, click **OK**.

View AutoSupport summary

System Manager enables you to view the status and details of all the previous AutoSupport data in order to review the data that has been sent to technical support. You can also view the information to understand the health and performance of your storage system.

Steps

1. Click ⚙ > **AutoSupport**.
2. Select the node, and then click **AutoSupport Request** > **View Previous Summary**.

   The AutoSupport data for all the nodes is displayed.

3. Click **OK**.

AutoSupport severity types

AutoSupport messages have severity types that help you understand the purpose of each message—for example, to draw immediate attention to an emergency problem, or only to provide information.

Messages have one of the following severities:

- **Alert**: Alert messages indicate that a next-higher level event might occur if you do not take some action.

  You must take an action against alert messages within 24 hours.

- **Emergency**: Emergency messages are displayed when a disruption has occurred.

  You must take an action against emergency messages immediately.

- **Error**: Error conditions indicate what might happen if you ignore.
- **Notice**: Normal but significant condition.
- **Info**: Informational message provides details about the issue, which you can ignore.
- **Debug**: Debug-level messages provide instructions you should perform.

If your internal support organization receives AutoSupport messages through email, the severity appears in the subject line of the email message.

AutoSupport window

The AutoSupport window enables you to view the current AutoSupport settings for your system. You can also change your system's AutoSupport settings.

Command buttons

- **Enable**

  Enables AutoSupport notification. **Enable** is the default.

- **Disable**

  Disables AutoSupport notification.

- **Edit**

  Opens the Edit AutoSupport Settings dialog box, which enables you to specify an email address from which email notifications are sent and to add multiple email addresses of the host names.

- **Test**

  Opens the AutoSupport Test dialog box, which enables you to generate an AutoSupport test message.

- **AutoSupport Request**

  Provides the following AutoSupport requests:

  - **Generate AutoSupport**

    Generates AutoSupport data for a selected node or all nodes.

  - **View Previous Summary**

    Displays the status and details of all the previous AutoSupport data.

- **Refresh**

  Updates the information in the window.

Details area

The details area displays AutoSupport setting information such as the node name, AutoSupport status, transport protocol used, and name of the proxy server.

Manage jobs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage job tasks such as displaying job information and monitoring the progress of a job.

Jobs

Jobs are asynchronous task and typically long-running volume operations, such as copying, moving, or mirroring data. Jobs are placed in a job queue and are run when resources are available. The cluster administrator can perform all the tasks related to job management.

A job can be one of the following categories:

- A *server-affiliated* job is placed in queue by the management framework to be run in a specific node.
- A *cluster-affiliated* job is placed in queue by the management framework to be run in any node in the cluster.
- A *private* job is specific to a node and does not use the replicated database (RDB) or any other cluster mechanism.

  You require the advanced privilege level or higher to run the commands to manage private jobs.

You can manage jobs in the following ways:

- Displaying job information, including the following:
  - Jobs on a per-node basis
  - Cluster-affiliated jobs
  - Completed jobs
  - Job history
- Monitoring a job's progress
- Displaying information about the initialization state for job managers.

You can determine the outcome of a completed job by checking the event log.

Job window

You can use the Job window to manage job tasks such as displaying job information and monitoring the progress of a job.

Command button

- **Refresh**

  Updates the information in the window.

Tabs

- **Current Jobs**

  This tab displays information about the job tasks that are in progress.

- **Job History**

  This tab displays information about all the jobs.

Job list

- **Job ID**

  Displays the ID of the job.

- **Start Time**

  Displays the start time of the job.

- **Job Name**

  Displays the name of the job.

- **Node**

  Displays the name of the node.

- **State**

  Displays the state of the job.

- **Job Description**

  Displays the description of the job.

- **Progress**

  Displays the state of the job.

- **Schedule Name**

  Displays the name of the schedule.

View Flash Pool statistics with System Manger - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to view the real-time SSD tier read and write workloads for a selected Flash Pool aggregate.

Flash Pool aggregate Statistics window

You can view the real-time SSD tier read and write workloads for a selected Flash Pool aggregate.

This page is not available for a cluster containing nodes with All Flash Optimized personality.

- **Displaying Statistics for Flash Pool aggregate**

  From the list of Flash Pool aggregates, you can select the Flash Pool aggregate whose statistics you want to view.

SSD Cache Read Workload

Displays a graphical view of the total read requests that are sent to the Flash Pool aggregate in comparison with the read operations that are performed by the SSD tier.

SSD Cache Write Workload

Displays a graphical view of the total write requests that are sent to the Flash Pool aggregate in comparison with the write operations that are performed by the SSD tier.

SVM Dashboard window in System Manager - ONTAP 9.7 and earlier

The dashboard window in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) provides a cumulative at-a-glance information about your storage virtual machine (SVM) and its performance. You can use the Dashboard window to view important information related to your SVM such as the protocols configured, the volumes that are nearing capacity, and the performance.

SVM Details

This window displays details about the SVM through various panels such as the Protocol Status panel, Volumes Nearing Capacity panel, Applications panel, and performance panel.

- **Protocol Status**

  Provides an overview of the protocols that are configured for the SVM. You can click the protocol name to view the configuration.

  If a protocol is not configured or if a protocol license is not available for the SVM, you can click the protocol name to configure the protocol or to add the protocol license.

- **Volumes Nearing Capacity**

  Displays information about the volumes that are nearing capacity utilization of 80 percent or more and that require immediate attention or corrective action.

- **Applications**

  Displays information about the top five applications of the SVM. You can view the top five applications based on either IOPS (from low to high or from high to low) or capacity (from low to high or from high to low). You must click the specific bar chart to view more information about the application. For capacity, the total space, used space, and available space are displayed, and for IOPS, the IOPS details are displayed. For L2/L3 applications, latency metrics are also displayed.

  The used size displayed in the Applications window does not equal the used size in the CLI.

  You can click **View details** to open the Applications window of the specific application. You can click **View all applications** to view all of the applications for the SVM.

  The refresh interval for the Applications panel is one minute.

- **SVM Performance**

  Displays the performance metrics of the protocols in the SVM, including latency and IOPS.

If the information about SVM performance cannot be retrieved from ONTAP, you cannot view the respective graph. In such cases, System Manager displays the specific error message.

The refresh interval for the SVM Performance panel is 15 seconds.

Monitor SVMs with System Manager - ONTAP 9.7 and earlier

The dashboard in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) enables you to monitor the health and performance of a storage virtual machine (SVM).

Steps

1. Click **Storage** > **SVMs**.
2. Select the name the SVM that you want to monitor.
3. View the details in the dashboard panels.

Edit SVM settings with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to edit the properties of storage virtual machines (SVMs), such as the name service switch, name mapping switch, and aggregate list.

About this task

- You can edit the values of the following SVM properties:
  - Name service switch
  - Protocols that are enabled to serve data

    The CIFS protocol that is configured on the SVM continues to serve data even when you disable the protocol on that SVM.

  - The list of aggregates that are available to create volumes

    For FlexVol volumes, you can assign aggregates only if you have delegated administration to an SVM administrator.

- System Manager does not display the values of the name service switch and the name mapping switch for an SVM that is created through the command-line interface or for the SVM services that are not configured and are not set to the default values by ONTAP.

  You can use the command-line interface to view the services because the Services tab is disabled.

  System Manager displays the name service switch and the name mapping switch of an SVM only when it is created by using System Manager or when the services of the SVM are set to the default values by ONTAP.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **Edit**.
3. In the **Details** tab, modify the required data protocols.

4. In the **Resource Allocation** tab, choose one of the following methods to delegate volume creation:

If you want to provision volume creation…	Then…
For all aggregates	Select the **Do not delegate volume creation** option.
For specific aggregates	a. Select the **Delegate volume creation** option. b. Select the required aggregates for delegating volume creation.

5. In the **Service** tab, specify the name service switch sources for the required database types and the order in which they should be consulted to retrieve name service information.

   The default values for each of the database types are as follows:

   - hosts: files, dns
   - namemap: files
   - group: files
   - netgroup: files
   - passwd: files

6. Click **Save and Close**.

Related information

How ONTAP name service switch configuration works

Delete SVMs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to delete storage virtual machines (SVMs) that you no longer require from the storage system configuration.

Before you begin

You must have completed the following tasks:

1. Disabled the Snapshot copies, data protection (DP) mirrors, and load-sharing (LS) mirrors for all the volumes

   You must use the command-line interface (CLI) to disable LS mirrors.

2. Deleted all the igroups that belong to the SVM manually if you are deleting SVMs
3. Deleted all the portsets
4. Deleted all the volumes in the SVM, including the root volume
5. Unmapped the LUNs, taken them offline, and deleted them
6. Deleted the CIFS server if you are deleting SVMs
7. Deleted any customized user accounts and roles that are associated with the SVM

8. Deleted any NVMe subsystems associated with the SVM using the CLI.
9. Stopped the SVM

About this task

When you delete SVMs, the following objects associated with the SVM are also deleted:

- LIFs, LIF failover groups, and LIF routing groups
- Export policies
- Efficiency policies

If you delete SVMs that are configured to use Kerberos, or modify SVMs to use a different Service Principal Name (SPN), the original service principal of the SVM is not automatically deleted or disabled from the Kerberos realm. You must manually delete or disable the principal. You must have the Kerberos realm administrator's user name and password to delete or disable the principal.

If you want to move data from an SVM to another SVM before you delete the first SVM, you can use the SnapMirror technology to do so.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

Start SVMs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to provide data access from a storage virtual machine (SVM) by starting the SVM.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM that you want to start, and then click **Start**.

Results

The SVM starts serving data to clients.

Stop SVMs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to stop a storage virtual machine (SVM) if you want to troubleshoot any issue with the SVM, delete the SVM, or stop data access from the SVM.

Before you begin

All the clients connected to the SVM must be disconnected.

If any clients are connected to the SVM when you stop it, data loss might occur.

About this task

- You cannot stop SVMs during storage failover (SFO).

- When you stop the SVM, an SVM administrator cannot log in to the SVM.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM that you want to stop, and then click **Stop**.

Results

The SVM stops serving data to clients.

Manage SVMs with System Manager - ONTAP 9.7 and earlier

In ONTAP System Manger classic (available in ONTAP 9.7 and earlier), a storage virtual machine (SVM) administrator can administer SVMs and their resources, such as volumes, protocols, and services, depending on the capabilities assigned by the cluster administrator. An SVM administrator cannot create, modify, or delete SVMs.

SVM administrators cannot log in to System Manager.

SVM administrators might have all or some of the following administration capabilities:

- Data access protocol configuration

  SVM administrators can configure data access protocols, such as NFS, CIFS, iSCSI, and Fibre Channel (FC) protocol (Fibre Channel over Ethernet or FCoE included).

- Services configuration

  SVM administrators can configure services such as LDAP, NIS, and DNS.

- Storage management

  SVM administrators can manage volumes, quotas, qtrees, and files.

- LUN management in a SAN environment
- Management of Snapshot copies of the volume
- Monitoring SVM

  SVM administrators can monitor jobs, network connection, network interface, and the SVM health.

Related information

ONTAP 9 Documentation Center

Trace file access to diagnose access errors on SVMs with System Manager

Beginning with System Manager 9.6, you can diagnose CIFS or NFS file access errors on a storage virtual machine (SVM).

About this task

File access issues, such as an “access denied” error, are likely to occur when there are problems with a share configuration, permissions, or user mapping. You can use System Manager to help you resolve file access

problems by viewing the access trace results for the file or share that a user wants to access. System Manager shows whether the file or share has effective read, write, or execute permissions and the reasons why access is or is not effective.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM that contains the files or shares for which file access errors were received.
3. Click **Trace File Access**.

   The Trace File Access window for the selected SVM shows the prerequisites and steps required to trace file access permissions.

4. Click **Continue** to begin the file tracing process.
5. Select the protocol that is used to access files or shares on the selected SVM.
6. In the **User Name** field, enter the name of the user who was trying to access the file or share.
7. **Optional:** Click to specify more details to narrow the scope of the trace.

   The Advanced Options dialog window allows you to specify the following details:

   - **Client IP Address**: Specify the IP address of the client.
   - **File**: Specify the file name or file path to trace.
   - **Show in Trace Results**: Specify whether you want to view only access denied entries or all entries. Click **Apply** to apply the details you specified and to return to the Trace File Access window.

8. Click **Start Tracing**.

   The trace is initiated and a results table is displayed. The table is empty until users receive errors when requesting file access. The results table is refreshed every 15 seconds and displays messages in reverse chronological order.

9. Notify the affected user or users that they should try accessing the files within the next 60 minutes.

   Details of the denied file access requests are shown in the results table when errors occur for the specified username for the duration of the trace. The Reasons column identifies the problems that are preventing the user from accessing files and reasons why they occurred.

10. **Optional:** In the **Reasons** column of the result table, click **View Permissions** to view permissions for the file that the user is trying to access.

    - When the trace result shows a message saying that access is not granted for "Synchronize", "Read Control", "Read Attributes", "Execute", "Read EA", "Write", or "Read"', the message is indicating that the desired access has not been granted for the set of permissions listed. In order to view the actual permissions status, you need to view the permissions using the provided link.
    - If you specified the CIFS protocol, the Effective File and Share Permissions dialog box displays, listing both file and share permissions associated with the share and file that the user is trying to access.
    - If you specified the NFS protocol, the Effective File Permissions dialog box displays, listing the file permissions associated with the file that the user is trying to access.
      A check mark indicates that permissions are granted, and an “X” indicates that permissions are not granted.

    Click **OK** to return to the Trace File Access window.

11. **Optional:** The results table displays read-only data. You can perform the following actions with the results of the trace:
    - Click **Copy to Clipboard** to copy the results to the clipboard.
    - Click **Export Trace Results** to export the results to a comma-separatedvalues (CSV) file.
12. When you want to end the tracing operation, click **Stop Tracing**.

About SVMs with System Manager - ONTAP 9.7 and earlier

You can use SVMS with ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to provide data access to clients regardless of the physical storage or controller, similar to any storage system. SVMs provide benefits such as nondisruptive operations, scalability, security, and unified storage.

SVMs provide the following benefits:

- Multi-tenancy

  SVM is the fundamental unit of secure multi-tenancy, which enables partitioning of the storage infrastructure so that it appears as multiple independent storage systems. These partitions isolate the data and management.

- Nondisruptive operations

  SVMs can operate continuously and nondisruptively for as long as they are needed. SVMs help clusters to operate continuously during software and hardware upgrades, addition and removal of nodes, and all administrative operations.

- Scalability

  SVMs meet on-demand data throughput and the other storage requirements.

- Security

  Each SVM appears as a single independent server, which enables multiple SVMs to coexist in a cluster while ensuring no data flows among them.

- Unified storage

  SVMs can serve data concurrently through multiple data access protocols. SVMs provide file-level data access through NAS protocols, such as CIFS and NFS, and block-level data access through SAN protocols, such as iSCSI, FC/FCoE, and NVMe. SVMs can serve data to SAN and NAS clients independently at the same time.

- Delegation of management

  SVM administrators have privileges assigned by the cluster administrator.

About ONTAP name service switch configuration in System Manager - ONTAP 9.7 and earlier

ONTAP System Manager classic (available in ONTAP 9.7 and earlier) stores name service configuration information in a table that is the equivalent of the `/etc/nsswitch.conf` file on UNIX systems. You must understand the function of the

table and how ONTAP uses it so that you can configure it appropriately for your environment.

The ONTAP name service switch table determines which name service sources ONTAP consults in which order to retrieve information for a certain type of name service information. ONTAP maintains a separate name service switch table for each SVM.

Database types

The table stores a separate name service list for each of the following database types:

Database type	Defines name service sources for…	Valid sources are…
hosts	Converting host names to IP addresses	files, dns
group	Looking up user group information	files, nis, ldap
passwd	Looking up user information	files, nis, ldap
netgroup	Looking up netgroup information	files, nis, ldap
namemap	Mapping user names	files, ldap

Source types

The sources specify which name service source to use for retrieving the appropriate information.

Specify source type…	To look up information in…	Managed by the command families…

files	Local source files	`vserver services name-service unix-user`
		
		`vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

nis	External NIS servers as specified in the NIS domain configuration of the SVM	`vserver services name-service nis-domain`

Specify source type…	To look up information in…	Managed by the command families…
ldap	External LDAP servers as specified in the LDAP client configuration of the SVM	`vserver services name-service ldap`
dns	External DNS servers as specified in the DNS configuration of the SVM	`vserver services name-service dns`

Even if you plan to use NIS or LDAP for both data access and SVM administration authentication, you should still include `files` and configure local users as a fallback in case NIS or LDAP authentication fails.

Related information

Editing SVM settings

Storage Virtual Machines window in System Manager - ONTAP 9.7 and earlier

You can use the Storage Virtual Machines window in ONTAP System Manger classic (available in ONTAP 9.7 and earlier) to manage your storage virtual machines (SVMs) and display information about them.

You cannot manage (create, delete, start, or stop) anSVM configured for disaster recovery (DR) by using System Manager. Also, you cannot view the storage objects associated with the SVM configured for disaster recovery in the application interface.

Command buttons

- **Create**

  Opens the Storage Virtual Machine (SVM) Setup wizard, which enables you to create a new SVM.

- **Edit**

  Opens the Edit Storage Virtual Machine dialog box, which enables you to modify the properties, such as the name service switch, name mapping switch, and aggregate list, of a selected SVM.

- **Delete**

  Deletes the selected SVMs.

- **Start**

  Starts the selected SVM.

- **Stop**

  Stops the selected SVM.

- **SVM Settings**

Manages the storage, policies, and configuration for the selected SVM.

- **Protection Operations**

  Provides the following options:

  - **Initialize**

    Enables you to initialize the SVM relationship to perform a baseline transfer from the source SVM to the destination SVM.

  - **Update**

    Enables you to update data from the source SVM to the destination SVM.

  - **Activate Destination SVM**

    Enables you to activate the destination SVM.

  - **Resync from Source SVM**

    Enables you to initiate resynchronization of the broken relationship.

  - **Resync from Destination SVM (Reverse Resync)**

    Enables you to resynchronize the relationship from the destination SVM to the source SVM.

  - **Reactivate Source SVM**

    Enables you to reactivate the source SVM.

- **Refresh**

  Updates the information in the window.

- **Trace File Access**

  Enables you to trace the accessibility of a file or share on the selected SVM for a specified username.

SVM list

The SVM list displays the name of each SVM and the allowed protocols on it.

You can view only data SVMs by using System Manager.

- **Name**

  Displays the name of the SVM.

- **State**

  Displays the SVM state, such as Running, Starting, Stopped, or Stopping.

- **Subtype**

  Displays the subtype of the SVM, which can be one of the following:

- default

  Specifies that the SVM is a data-serving SVM.

- dp-destination

  Specifies that the SVM is configured for disaster recovery.

- sync-source

  Specifies that the SVM is in the primary site of a MetroCluster configuration.

- sync-destination

  Specifies that the SVM is in the surviving site of a MetroCluster configuration.

- **Allowed Protocols**

  Displays the allowed protocols, such as CIFS and NFS, on each SVM.

- **IPspace**

  Displays the IPspace of the associated SVM.

- **Volume Type**

  Displays the allowed volume type, such as FlexVol volume, on each SVM.

- **Protected**

  Displays whether the SVM is protected or not.

- **Configuration State**

  Displays whether the configuration state of the SVM is locked or unlocked.

Details area

The area below the SVM list displays detailed information, such as the type of volumes allowed, language, and Snapshot policy, about the selected SVM.

You can also configure the protocols that are allowed on this SVM. If you have not configured the protocols while creating the SVM, you can click the protocol link to configure the protocol.

You cannot configure protocols for anSVM configured for disaster recovery by using System Manager.

If the FCP service is already started for the SVM, clicking the FC/FCoE link opens the Network Interfaces window.

The color indicates the status of the protocol configuration:

Status	Description
Green	LIFs exist and the protocol is configured. You can click the link to view the configuration details. Configuration might be partially completed. However, service is running. You can create the LIFs and complete the configuration from the Network Interfaces window.
Yellow	Indicates one of the following: • LIFs exist. Service is created but is not running. • LIFs exist. Service is not created. • Service is created. LIFs do not exist.
Grey	The protocol is not configured. You can click the protocol link to configure the protocol.
Grey border	The protocol license has expired or is missing. You can click the protocol link to add the licenses in the Licenses page.

You can also add the management interface and view details such as the protection relationships, protection policy, NIS domain, and so on.

The **Details** area also includes a link to view the Public SSL Certificate for an SVM. When you click this link, you can perform the following tasks:

- View certificate details, the serial number, the start date, and the expiration date.
- Copy the certificate to the clipboard.
- Email the certificate details.

Peer Storage Virtual Machines area

Displays a list of the SVMs that are peered with the selected SVM along with details of the applications that are using the peer relationship.

Trace File Access window in System Manager

Beginning with ONTAP System Manager 9.6, you can use the Trace File Access window to diagnose issues when you have problems accessing files and shares on an SVM using the CIFS or NFS protocol.

Command buttons

- **Continue**

  Starts the process of setting up and initiating a file access trace on the selected SVM.

- **Protocols**

  Allows you to select the protocol that is used to access files and shares on the selected SVM, either CIFS or NFS.

- **Advanced Options icon**

  Allows you to specify additional details to narrow the scope of the trace.

- **Show in Trace Results**

  Allows you to specify in the Advanced Options dialog box whether you want the trace results to display only file access requests that were denied or to display all file access requests—those that were successful and those that were denied.

- **Start Tracing**

  Allows you to start the trace. The results show access problems for file access requests submitted over the next 60 minutes.

- **Stop Tracing**

  Allows you to stop the trace.

- **View Permissions**

  Allows you to display permissions. When using the CIFS protocol, you can display effective file and share permissions. When using the NFS protocol, you can display effective file permissions.

- **Copy to Clipboard**

  Allows you copy the results table to the clipboard.

- **Export Trace Results**

  Allows you to export the trace results to a file in comma-separated-values (.csv) format.

Entry fields

- **User Name**

  You enter the name of the user who received file access request errors that you want to trace.

- **Search trace results**

  You enter specific information that you want to find in the search results, and then you click **Enter**.

- **Client IP Address**

  In theAdvanced Options dialog box, you can specify the IP address of the client as an additional detail to narrow the scope of the trace.

- **File**

  In theAdvanced Options dialog box, you can specify the file or file path that you want to access as an additional detail to narrow the scope of the trace.

Results list for CIFS protocol tracing

When you specify the CIFS protocol, the results list displays the following data for your trace based on the parameters you specified. The data is displayed in reverse chronological order. If you stop tracing, the results remain in the list until you start another trace.

- Share: The name of the share that the system attempted to access, whether successful or not.
- Path: The file path of the file that the system attempted to access, whether successful or not.
- Client IP Address: The IP address of the client from which access requests were initiated.
- Reasons: The reasons the attempt to access the file or share was successful or not.

> When the trace result shows a message saying that access is not granted for "Synchronize", "Read Control", "Read Attributes", "Execute", "Read EA", "Write", or "Read"', the message is indicating that the desired access has not been not granted for the set of permissions listed. In order to view the actual permissions status, you need to view the permissions using the provided link.

Results list for NFS protocol tracing

When you specify the NFS protocol, the results list displays the following data for your trace based on the parameters you specified. The data is displayed in reverse chronological order. If you stop tracing, the results remain in the list until you start another trace.

- Path: The file path of the file that the system attempted to access, whether successful or not.
- Client IP Address: The IP address of the client from which access requests were initiated.
- Reasons: The reasons the attempt to access the file or share was successful or not.

> When the trace result shows a message saying that access is not granted for "Synchronize", "Read Control", "Read Attributes", "Execute", "Read EA", "Write", or "Read"', the message is indicating that the desired access has not been not granted for the set of permissions listed. In order to view the actual permissions status, you need to view the permissions using the provided link.

Related information

SMB/CIFS management

SMB/CIFS and NFS multiprotocol configuration

Volumes

Edit volume properties with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to modify volume properties such as the volume name, security style, fractional reserve, and space guarantee. You can modify storage efficiency settings (deduplication schedule, deduplication policy, and compression) and space reclamation settings.

Before you begin

For enabling volume encryption, you must have installed the volume encryption license by using System

Manager, and you must have enabled “key-manager setup” by using the command-line interface (CLI). You must refresh your web browser after enabling “key-manager setup”.

About this task

- You can set the fractional reserve to either zero percent or 100 percent.
- Data compression is not supported on 32-bit volumes.
- For Data ONTAP 8.3.1 clusters, you can enable both inline compression and background compression for Cloud Volumes ONTAP for AWS (AWS).

  Compression is not supported for Data ONTAP Edge.

- You cannot rename a SnapLock Compliance volume.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select the storage virtual machine (SVM) in which the volume that you want to edit resides.
3. Select the volume that you want to modify, and then click **Edit**.

   The Edit Volume dialog box is displayed.

4. In the **General** tab, modify the following properties as required:
   - Change the volume name
   - Enable volume encryption

     This option is available only if you have enabled the Volume Encryption license and if the corresponding platform supports encryption. You can perform key-manager set up from the CLI.

   - Change the security style of the volume
   - Enable or disable thin provisioning
5. Click the **Storage Efficiency** tab, and enable storage efficiency by configuring the following properties:
   - Deduplication
   - Data compression
     You cannot enable background compression for a volume that is contained by an aggregate with All Flash Optimized personality. You can enable only inline compression for these volumes.

   You can enable inline deduplication only on a volume that is contained by an aggregate with All Flash Optimized personality or on a volume in a Flash Pool aggregate.

6. For SnapLock volumes, click the **SnapLock** tab, and perform the following steps:
   a. Specify the autocommit period.

      The autocommit period determines how long a file in the volume must remain unchanged before the file is committed to WORM state.

   b. Specify the minimum retention period and maximum retention period.

      The values must be in the range of 1 day through 70 years or Infinite.

   c. Select the default retention period.

The default retention period must be within the specified minimum retention period and maximum retention period.

7. Click the **Advanced** tab, and enable the following properties:
   - If you want the volume to automatically grow when the used space in the volume is above the grow threshold, select **Grow**.
   - If you want the volume to grow or shrink in size in response to the amount of used space, select **Grow or Shrink**.
     a. Specify the maximum size to which the volume can grow.
   - Enable automatic deletion of older Snapshot copies by choosing one of the following options:
     - Try

       Deletes the Snapshot copies that are not locked by any other subsystems.

     - Destroy

       Deletes the Snapshot copies that are locked by the data-backing functionality.

     - Disrupt

       Deletes the Snapshot copies that can disrupt the data transfer.
   - Select the caching policy that you want to assign to the volume.

     This option is available only for FlexVol volumes in a Flash Pool aggregate.
   - Select the retention priority for cached data in the volume.

     This option is available only for FlexVol volumes in a Flash Pool aggregate.
   - Specify the fractional reserve that you want to set for the volume.
   - Update the access time for reading the file.

     This option is disabled for SnapLock volumes.
8. Click **Save and Close**.

Related information

Volumes window

Setting up CIFS

Edit data protection volumes with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to modify the volume name for a data protection (DP) volume. If the source volume does not have storage efficiency enabled, you might want to enable storage efficiency only on the destination volume.

About this task

You cannot modify storage efficiency on a mirror DP volume.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select the storage virtual machine (SVM) in which the DP volume that you want to edit resides.
3. Select the volume that you want to modify, and then click **Edit**.
4. In the **Edit Data Protection Volume** dialog box, modify the volume name.
5. Ensure the **Enable Storage Efficiency** option is selected.

   If storage efficiency is already enabled on the volume, then the check box is selected by default.

6. **Optional:** Click the **Advanced** tab, and perform the following steps:

   a. Select the caching policy that you want to assign to the volume.

   b. Select the retention priority for the cached data in the volume.

   These options are available only for data protection FlexVol volumes in a Flash Pool aggregate.

7. Click **Save**.

Delete volumes with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to delete a FlexVol volume when you no longer require the data that a volume contains or if you have copied the data that a volume contains to another location. When you delete a volume, all the data in the volume is destroyed, and you cannot recover that data.

Before you begin

The following conditions must exist before you delete a FlexVol volume:

- The volume must be unmounted and must be in the offline state.
- FlexClone volumes must be either split from the parent volume or destroyed if the FlexVol volume is cloned.
- The SnapMirror relationships must be deleted if the volume is in one or more SnapMirror relationships.

About this task

You should be aware of the following limitations when deleting a FlexVol volume:

- You can delete a complete SnapLock Enterprise volume or a file in a SnapLock Enterprise volume; however, you cannot delete only the data within a file in a SnapLock Enterprise volume.
- You cannot delete a SnapLock Compliance volume if data is committed to the volume.
- If the FlexVol contains both qtrees and volumes, the qtrees appear as directories. You should be careful to not delete the qtrees accidentally when deleting volumes.
- If you have associated FlexCache volumes with an origin volume, then you must delete the FlexCache volumes before you can delete the origin volume.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select the storage virtual machine (SVM) in which the volume

that you want to delete resides.

3. Select the volumes that you want to delete.

> Verify that you have selected the correct volumes that you want to delete. When you delete a volume, all the data in the volume is destroyed, and you cannot recover that data.

4. Click **Delete**.
5. Select the confirmation check box, and then click **Delete**.

Related information

Volumes window

Create FlexClone volumes with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create a FlexClone volume when you require a writable, point-in-time copy of an existing FlexVol volume. You might want to create a copy of a volume for testing or to provide access to the volume for additional users without giving them access to the production data.

Before you begin

- The FlexClone license must be installed on the storage system.
- The volume that you want to clone must be online and must be a non-root volume.

About this task

The base Snapshot copy that is used to create a FlexClone volume of a SnapMirror destination is marked as busy and cannot be deleted. If a FlexClone volume is created from a Snapshot copy that is not the most recent Snapshot copy, and that Snapshot copy no longer exists on the source volume, all SnapMirror updates to the destination volume fail.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the FlexVol volume that you want to clone from the list of volumes.
4. Click **More Actions** > **Clone** > **Create** > **Volume**.
5. Type the name of the FlexClone volume that you want to create.
6. **Optional:** If you want to enable thin provisioning for the new FlexClone volume, select **Thin Provisioning**.

   By default, this setting is the same as that of the parent volume.

7. Create a Snapshot copy or select an existing Snapshot copy that you want to use as the base Snapshot copy for creating the FlexClone volume.
8. Click **Clone**.

Related information

Volumes window

Create FlexClone files with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create a FlexClone file, which is a writable copy of a parent file. You can use these copies to test applications.

Before you begin

- The file that is cloned must be part of the active file system.
- The FlexClone license must be installed on the storage system.

About this task

- FlexClone files are supported only for FlexVol volumes.

  You can create a FlexClone file of a parent file that is within a volume by accessing the parent file from the volume in which it resides, not from the parent volume.

- You cannot create a FlexClone file on a SnapLock volume.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volume in which you want to create a FlexClone file from the list of volumes.
4. Click **More Actions** > **Clone** > **Create** > **File**.
5. In the **Create FlexClone File** dialog box, select the file that you want to clone, and then specify a name for the FlexClone file.
6. Click **Clone**.

Results

The FlexClone file is created in the same volume as the parent file.

Related information

Volumes window

Split a FlexClone volume from its parent volume with System Manager - ONTAP 9.7 and earlier

You can use System Manager classic (available in ONTAP 9.7 and earlier) to split a FlexClone volume from its parent volume. After the split, the FlexClone volume becomes a normal FlexVol volume. It continues using the disk space of its parent volume and storage efficiency is preserved.

Before you begin

The FlexClone volume must be online.

About this task

For systems that are *not* AFF systems, the clone-splitting operation deletes all of the existing Snapshot copies of the clone. The Snapshot copies that are required for SnapMirror updates are also deleted. Therefore, any subsequent SnapMirror updates might fail.

You can pause the clone-splitting operation if you have to perform any other operation on the volume. You can resume the clone-splitting process after the other operation is complete.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the FlexClone volume that you want to split from its parent volume.
4. Click **More Actions** > **Clone** > **Split**.
5. Confirm the FlexClone volume details for the clone-splitting operation, and then click **Start Split** in the confirmation dialog box.

Related information

Volumes window

View the FlexClone volume hierarchy - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to view the hierarchy of FlexClone volumes and their parent volumes.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the required volume from the list of volumes.
4. Click **More Actions** > **Clone** > **View Hierarchy**.

Results

Volumes that have at least one child FlexClone volume are displayed. The FlexClone volumes are displayed as children of their respective parent volumes.

Related information

Volumes window

Change the status of a volume with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to change the status of a FlexVol volume when you want to take a volume offline, bring a volume back online, or restrict access to a volume.

Before you begin

- If you want a volume to be the target of a volume copy operation or a SnapMirror replication operation, the volume must be in the restricted state.
- If you want to take a NAS volume offline, the NAS volume must be unmounted.

About this task

You can take a volume offline to perform maintenance on the volume, to move the volume, or to destroy the volume. When a volume is offline, the volume is unavailable for read or write access by clients. You cannot take a root volume offline.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volume for which you want to modify the status.
4. From the **More Actions** > **Change status to** menu, select the required volume status.
5. Click **Ok** in the confirmation dialog box to change the volume status.

Related information

Volumes window

View the list of saved Snapshot copies with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to view the list of all of the saved Snapshot copies for a selected volume from the Snapshot Copies tab in the lower pane of the Volumes window. You can use the list of saved Snapshot copies to rename, restore, or delete a Snapshot copy.

Before you begin

The volume must be online.

About this task

You can view Snapshot copies for only one volume at a time.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Click the plus sign (+) next to the volume for which you want to view saved Snapshot copies.
4. Click the **Show More Details** link to view more information about the volume.
5. Click the **Snapshot Copies** tab.

   The list of available Snapshot copies for the selected volume is displayed.

Create Snapshot copies outside a defined schedule with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create a Snapshot copy of a volume outside a defined schedule to capture the state of the file system at a specific point in time.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volume from the list of volumes.
4. Click **More Actions** > **Manage Snapshots** > **Create**.
5. In the **Create Snapshot Copy** dialog box, if you want to change the default name, specify a new name for the Snapshot copy.

Valid characters are ASCII characters, numerals, hyphens (-), underscores (_), periods (.), and the plus (+) symbol.

The default name of a Snapshot copy consists of the volume name and the timestamp.

6. Click **Create**.
7. Verify that the Snapshot copy that you created is included in the list of Snapshot copies in the **Snapshot Copies** tab.

Related information

Volumes window

Set the Snapshot copy reserve with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (avaiable in ONTAP 9.7 and earlier) to reserve space (measured as a percentage) for the Snapshot copies in a volume. By setting the Snapshot copy reserve, you can allocate enough disk space for the Snapshot copies so that they do not consume the active file system space.

About this task

The default space that is reserved for Snapshot copies is 5 percent for SAN and VMware volumes.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volume for which you want to set the Snapshot copy reserve.
4. Click **More Actions** > **Manage Snapshots** > **Configuration Settings**.
5. Type or select the percentage of volume space that you want to reserve for the Snapshot copies, and then click **OK**.

Related information

Volumes window

Hide the Snapshot copy directory with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to hide the Snapshot copy directory (`.snapshot`) so that the Snapshot copy directory is not visible when you view your volume directories. By default, the `.snapshot` directory is visible.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volume for which you want hide the Snapshot copy directory.
4. Click **More Actions** > **Manage Snapshots** > **Configuration Settings**.
5. Ensure that the **Make snapshot directory (.snapshot) visible** option is not selected, and then click **OK**.

Related information

Volumes window

Schedule automatic creation of Snapshot copies with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to set up a schedule for the automatic creating automatic Snapshot copies of a volume. You can specify the time and frequency of creating the copies. You can also specify the number of Snapshot copies that are saved.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the required volume from the list of volumes.
4. Click **More Actions** > **Manage Snapshots** > **Configuration Settings**.
5. In the **Configure Volume Snapshot Copies** dialog box, select **Enable scheduled Snapshot Copies**.
6. Select a Snapshot policy.

   You can schedule the creation of only policy-based Snapshot copies.

7. Click **OK** to save your changes and start your Snapshot copy schedule.

Related information

Volumes window

Restore a volume from a Snapshot copy with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to restore a volume to a state that is recorded in a previously created Snapshot copy to retrieve lost information. When you restore a volume from a Snapshot copy, the restore operation overwrites the existing volume configuration. Any changes that were made to the data in the volume after the Snapshot copy was created are lost.

Before you begin

- The SnapRestore license must be installed on your system.
- If the FlexVol volume that you want to restore contains a LUN, the LUN must be unmounted or unmapped.
- There must be enough space available for the restored volume.
- Users accessing the volume must be notified that you are going to revert a volume, and that the data from the selected Snapshot copy replaces the current data in the volume.

About this task

- If the volume that you restore contains junction points to other volumes, the volumes that are mounted on these junction points will not be restored.
- You cannot restore Snapshot copies for SnapLock Compliance volumes.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volume that you want to restore from a Snapshot copy.
4. Click **More Actions** > **Manage Snapshots** > **Restore**.
5. Select the appropriate Snapshot copy, and then click **Restore**.
6. Select the confirmation check box, and then click **Restore**.

Related information

Volumes window

Extend the expiry date of Snapshot copies with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to extend the expiry date of the Snapshot copies in a volume.

Before you begin

The SnapLock license must be installed on your system.

About this task

You can extend the expiry date only for Snapshot copies in a data protection (DP) volume that is the destination in a SnapLock for SnapVault relationship.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select a volume.
4. Click **Show More Details** to view more information about the volume.
5. Click the **Snapshot Copies** tab.

   The list of available Snapshot copies for the selected volume is displayed.
6. Select the Snapshot copy that you want to modify, and then click **Extend Expiry Date**.
7. In the **Extend Expiry Date** dialog box, specify the expiry date.

   The values must be in the range of 1 day through 70 years or Infinite.
8. Click **OK**.

Rename Snapshot copies with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to rename a Snapshot copy to help you organize and manage your Snapshot copies.

About this task

You cannot rename the Snapshot copies (which are committed to the WORM state) of a SnapLock DP volume that is in a SnapVault relationship.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Click the required volume.
4. Click the **Show More Details** link to view more information about the volume.
5. Click the **Snapshot Copies** tab.

   The list of available Snapshot copies for the selected volume is displayed.

6. Select the Snapshot copy that you want to rename, and then click **More Actions** > **Rename**.
7. Specify a new name, and then click **Rename**.

   Valid characters are ASCII characters, numerals, hyphens (-), underscores (_), periods (.), and the plus (+) symbol.

8. Verify the Snapshot copy name in the **Snapshot Copies** tab of the **Volumes** window.

Related information

Volumes window

Delete Snapshot copies with System Manager - ONTAP 9.7 and earlier

You can delete a Snapshot copy to conserve disk space or to free disk space by using ONTAP System Manager classic (available in ONTAP 9.7 and earlier). You can also delete a Snapshot copy if the Snapshot copy is no longer required.

Before you begin

If you want to delete a Snapshot copy that is busy or locked, you must have released the Snapshot copy from the application that was using the Snapshot copy.

About this task

- You cannot delete the base Snapshot copy in a parent volume if a FlexClone volume is using that Snapshot copy.

  The base Snapshot copy is the Snapshot copy that is used to create a FlexClone volume. The base Snapshot copy always displays the status `busy` and Application Dependency as `busy,vclone` in the parent volume.

- You cannot delete a locked Snapshot copy that is used in a SnapMirror relationship.

  The Snapshot copy is locked and is required for the next update.

- You cannot delete a Snapshot copy from a SnapLock DP volume that is used in a SnapVault relationship before the expiry time of the Snapshot copy.
- You cannot delete the unexpired Snapshot copies (which are committed to WORM state) of a SnapLock DP volume that is in a SnapVault relationship.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.

3. Expand the required volume.
4. Click the **Show More Details** link to view more information about the volume.
5. Click the **Snapshot Copies** tab.

   The list of available Snapshot copies for the selected volume is displayed.
6. Select the Snapshot copy that you want to delete.
7. Click **Delete**.
8. Select the confirmation check box, and then click **Delete**.

Related information

Volumes window

ONTAP 9 Documentation Center

Resize volumes with System Manager - ONTAP 9.7 and earlier

When a volume reaches nearly full capacity, you can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to increase the size of the volume, delete some Snapshot copies, or adjust the Snapshot reserve. You can use the Volume Resize wizard in System Manager to provide more free space.

About this task

- For a volume that is configured to grow automatically, you can modify the limit to which the volume can grow automatically based on the increased size of the volume.
- You cannot resize a data protection volume if its mirror relationship is broken or if a reverse resynchronization operation has been performed on the volume.

  Instead, you must use the command-line interface (CLI).

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volume that you want to resize.
4. Click **More Actions** > **Resize**.
5. Type or select information as prompted by the wizard.
6. Confirm the details, and then click **Finish** to complete the wizard.
7. Verify the changes that you made to the available space and the total space of the volume in the **Volumes** window.

Related information

Volumes window

Enable storage efficiency on a volume with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to

enable storage efficiency and to configure both deduplication and data compression or only deduplication on a volume to save storage space. If you have not enabled storage efficiency when you created the volume, you can do so later by editing the volume.

Before you begin

- The volume must be online.
- If you want to use a policy-based deduplication schedule, you must have created an efficiency policy.

About this task

- You can enable background compression only if you have enabled background deduplication.
- You can enable inline compression and inline deduplication with or without enabling background compression and background deduplication, respectively.
- You can enable inline deduplication only on volumes that are contained by an aggregate with All Flash Optimized personality and on volumes that are contained by a Flash Pool aggregate.
- Beginning with System Manager 9.6, editing storage efficiency is supported for FlexGroup DP volumes.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volume for which you want to enable storage efficiency, and then click **Edit**.
4. In the **Edit Volume** dialog box, click **Storage Efficiency**.
5. Select the **Background Deduplication** check box.
6. Select one of the following methods to run deduplication:

If you want to run deduplication…	Then…
Based on a storage efficiency policy	a. Ensure that the **Policy based** option is selected. b. Click **Choose**, and then select a storage efficiency policy. c. Click **OK**.
When required	Select the **On-demand** option.

7. Select the **Background Compression** check box to enable background compression.

   You cannot enable background compression for a volume that is contained by an aggregate with All Flash Optimized personality.

8. Select the **Inline Compression** check box to compress data while it is being written to the volume.

   By default, inline compression is enabled on volumes that are contained by an aggregate with All Flash Optimized personality.

9. Select the **Inline Deduplication** check box to run deduplication before data is written to the disk.

   By default, inline deduplication is enabled on volumes that are contained by an aggregate with All Flash

Optimized personality.

10. Click **Save and Close**.

Related information

Volumes window

Change the deduplication schedule with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to change the deduplication schedule by choosing to run deduplication manually, automatically, or on a schedule that you specify.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the read/write volume for which you want to modify the deduplication schedule.
4. Click **Edit**, and then click the **Storage Efficiency** tab.
5. Change the deduplication schedule as required.
6. Click **Save and Close**.

Related information

Volumes window

Run deduplication operations with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to run deduplication immediately after creating a FlexVol volume or to schedule deduplication to run at a specified time.

Before you begin

- Deduplication must be enabled on the volume.
- The volume must be online and mounted.

About this task

Deduplication is a background process that consumes system resources during the operation; therefore, it might affect other operations that are in progress. You must cancel deduplication before you can perform any other operation.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volume for which you want to run deduplication.
4. Click **More Actions** > **Storage Efficiency**.
5. If you are running deduplication on the volume for the first time, run deduplication on the entire volume data by selecting **Scan Entire Volume** in the **Storage Efficiency** dialog box.

6. Click **Start**.
7. View the last-run details of the deduplication operation in the **Storage Efficiency** tab of the **Volumes** window.

Related information

Volumes window

Move FlexVol volumes between aggregates or nodes with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to nondisruptively move a FlexVol volume to a different aggregate or a different node for capacity utilization and improved performance.

Before you begin

If you are moving a data protection (DP) volume, the data protection mirror relationships must be initialized before you move the volume.

About this task

You cannot move SnapLock volumes between aggregates and nodes.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volume that you want to move.
4. Click **More Actions** > **Move**.
5. In the **Move Volume** dialog box, select the destination aggregate or node for the volume, and then change the tiering policy.

   - You cannot change the tiering policy of a root volume.
   - You cannot move the root volume to FabricPool.
   - For read/write volumes, you can set the tiering policy as “back up” during the volume move.

     The tiering policy changes to “snapshot-only” after the move.

   - Capacity tier values that are displayed in the “Used After Move” in both the source aggregate and destination aggregate are estimated values.

     For the exact values, you must navigate to the Aggregate window and view the details of a specific aggregate.

6. Click **Move**.

Manually triggering the cutover for volume move

For a volume move operation, you can use System Manager to manually trigger the cutover when the volume enters the cutover deferred phase. You can set the duration of the cutover and the cutover action to be performed by the system if the operation fails within that duration.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. Click the **Volumes** tab.
4. Expand the volume for which the volume move operation has been initiated.
5. Click the **Show More Details** link to view more information about the volume.
6. In the **Overview** tab, click **Cutover**.
7. In the **Cutover** dialog box, click **Advanced Options**.
8. **Optional:** Specify the cutover action and the cutover window period.
9. Click **OK**.

Assign volumes to Storage QoS with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to limit the throughput of FlexVol volumes and FlexGroup volumes by assigning them to storage Quality of Service (QoS) policy groups. You can assign storage QoS for new volumes, or you can modify the storage QoS details of the volumes that are already assigned to a policy group by using System Manager.

About this task

- You can assign storage QoS only to read/write (rw) volumes that are online.
- You cannot assign storage QoS to a volume if the following storage objects are assigned to a policy group:
  - Parent storage virtual machine (SVM) of the volume
  - Child LUNs of the volume
  - Child files of the volume
- You can assign storage QoS or modify the QoS details for a maximum of 10 volumes simultaneously.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select one or more volumes for which you want to assign storage QoS.
4. Click **More Actions** > **Storage QoS**.
5. In the **Quality of Service Details** dialog box, select the **Manage Storage Quality of Service** check box if you want to manage the workload performance of the FlexVol volume.

   If some of the volumes that you selected are already assigned to a policy group, the changes that you make might affect the performance of these volumes.

6. Create a new storage QoS policy group or select an existing policy group to control the input/output (I/O) performance of the FlexVol volume:

If you want to…	Do this…
Create a new policy group	a. Select **New Policy Group**. b. Specify the policy group name. c. Specify the minimum throughput limit. ◦ In System Manager 9.5, you can set the minimum throughput limit only on a performance-based All Flash Optimized personality. In System Manager 9.6, you can also set the minimum throughput limit for ONTAP Select Premium systems. ◦ You cannot set the minimum throughput limit for volumes on a FabricPool-enabled aggregate. ◦ If you do not specify the minimum throughput value or if the minimum throughput value is set to 0, the system automatically displays “None” as the value. This value is case-sensitive. d. Specify the maximum throughput limit to prevent the workload of the objects in the policy group from exceeding the specified throughput limit. ◦ The minimum throughput limit and the maximum throughput limit must be of the same unit type. ◦ If you do not specify the minimum throughput limit, then you can set the maximum throughput limit in IOPS, B/s, KB/s, MB/s, and so on. ◦ If you do not specify the maximum throughput value, the system automatically displays “Unlimited” as the value. This value is case-sensitive. The unit that you specify does not affect the maximum throughput.

If you want to…	Do this…
Select an existing policy group	a. Select **Existing Policy Group**, and then click **Choose** to select an existing policy group from the Select Policy Group dialog box. b. Specify the minimum throughput limit. ◦ In System Manager 9.5, you can set the minimum throughput limit only on a performance-based All Flash Optimized personality. In System Manager 9.6, you can also set the minimum throughput limit for ONTAP Select Premium systems. ◦ You cannot set the minimum throughput limit for volumes on a FabricPool-enabled aggregate. ◦ If you do not specify the minimum throughput value or if the minimum throughput value is set to 0, the system automatically displays “None” as the value. This value is case-sensitive. c. Specify the maximum throughput limit to prevent the workload of the objects in the policy group from exceeding the specified throughput limit. ◦ The minimum throughput limit and the maximum throughput limit must be of the same unit type. ◦ If you do not specify the minimum throughput limit, then you can set the maximum throughput limit in IOPS, B/s, KB/s, MB/s, and so on. ◦ If you do not specify the maximum throughput value, the system automatically displays “Unlimited” as the value. This value is case-sensitive. The unit that you specify does not affect the maximum throughput. If the policy group is assigned to more than one object, the maximum throughput that you specify is shared among the objects.

7. **Optional:** Click the link that specifies the number of volumes if you want to review the list of selected volumes, and then click **Discard** if you want to remove any volumes from the list.

   The link is displayed only when multiple volumes are selected.

8. Click **OK**.

Create a mirror relationship from a source SVM with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create a mirror relationship from the source storage virtual machine (SVM), and to assign a mirror policy and schedule to the mirror relationship. The mirror copy enables quick availability of data if the data on the source volume is corrupted or lost.

Before you begin

- The SnapMirror license must be enabled on the source cluster and destination cluster.

  - For some platforms, it is not mandatory for the source cluster to have the SnapMirror license enabled if the destination cluster has the SnapMirror license and Data Protection Optimization \(DPO\) license enabled.
  - After the DPO license is enabled on the destination cluster, you must refresh the browser of the source cluster to enable the `Protect` option.

- While mirroring a SnapLock volume, the SnapMirror license must be installed on both the source cluster and destination cluster, and the SnapLock license must be installed on the destination cluster.
- The source cluster and destination cluster and the source SVM and destination SVM must be in a healthy peer relationship.
- The destination aggregate must have space available.
- FlexVol volumes must be online and of type read/write.
- The SnapLock aggregate type must be the same on both clusters.
- A maximum of 25 volumes can be protected in one selection.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which Security Assertion Markup Language (SAML) authentication is enabled, password-based authentication must be enabled on the remote cluster.

About this task

- System Manager does not support a cascade relationship.

  For example, a destination volume in a relationship cannot be the source volume in another relationship.

- You can create a mirror relationship between SnapLock volumes of the same type only.

  For example, if the source volume is a SnapLock Enterprise volume, then the destination volume must also be a SnapLock Enterprise volume.

- If encryption is enabled on the source volume and the destination cluster is running a version of ONTAP software earlier than ONTAP 9.3, then encryption is disabled on the destination volume by default.
- SVMs that are peered only for FlexCache applications and do not have peering permissions for SnapMirror applications are not shown in the list of SVMs in this task. You can use the ONTAP System Manager 9.6 enhanced peering workflow to give permission to, or peer to, these SVMs. You then can select them in this task to create a protection relationship.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.

3. Select the volumes for which you want to create mirror relationships, and then click **More Actions** > **Protect**.

   The **Protect** option is available only for a read/write volume.

4. Select the **Replication** type:

If you selected the replication type as…	Do this…
Asynchronous	a. **Optional:** If you do not know the replication type and relationship type, click **Help me Choose**, specify the values, and then click **Apply**. b. Select the relationship type. The relationship type can be mirror, vault, or mirror and vault. c. Select a cluster and an SVM. If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed. d. Modify the volume name suffix, if required.
Synchronous	a. **Optional:** If you do not know the replication type and relationship type, click **Help me Choose**, specify the values, and then click **Apply**. b. Select the synchronization policy. The synchronization policy can be StrictSync or Sync. c. Select a cluster and an SVM. If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed. d. Modify the volume name suffix, if required.

5. Click ⚙, update the protection policy and protection schedule, select **FabricPool-enabled aggregate**, and then initialize the protection relationship.
6. Click **Save**.

Results

A new destination volume of type *dp* is created with the following default settings:

- Autogrow is enabled.
- Compression is disabled.
- The language attribute is set to match the language attribute of the source volume.

If the destination FlexVol volume is on a different SVM than the source FlexVol volume, then a peer relationship is created between the two SVMs if the relationship does not already exist.

A mirror relationship is created between the source volume and the destination volume. The base Snapshot copy is transferred to the destination volume if you have opted to initialize the relationship.

Related information

Protection window

Create a vault relationship from a source SVM with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create a vault relationship from the source storage virtual machine (SVM), and to assign a vault policy to the vault relationship to create a backup vault. In the event of data loss or corruption on a system, backed-up data can be restored from the backup vault destination.

Before you begin

- The SnapVault license or SnapMirror license must be enabled on both the source cluster and the destination cluster.

  - For some platforms, it is not mandatory for the source cluster to have the SnapVault license or the SnapMirror license enabled if the destination cluster has the SnapVault license or the SnapMirror license, and the Data Protection Optimization \(DPO\) license enabled.
  - After the DPO license is enabled on the destination cluster, you must refresh the browser of the source cluster to enable the `Protect` option.

- The source cluster and destination cluster and the source SVM and destination SVM must be in a healthy peer relationship.
- The destination aggregate must have space available.
- The source aggregate and the destination aggregate must be 64-bit aggregates.
- A vault (XDP) policy must exist.

  If a vault policy does not exist, you must create a vault policy or accept the default vault policy (named XDPDefault) that is automatically assigned.

- FlexVol volumes must be online and of type read/write.
- The SnapLock aggregate type must be the same.
- A maximum of 25 volumes can be protected in one selection.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which Security Assertion Markup Language (SAML) authentication is enabled, password-based authentication must be

enabled on the remote cluster.

About this task

- System Manager does not support a cascade relationship.

  For example, a destination volume in a relationship cannot be the source volume in another relationship.

- You can create a lock-vault relationship only between a non-SnapLock (primary) volume and a SnapLock destination (secondary) volume.
- If encryption is enabled on the source volume and the destination cluster is running a version of ONTAP software earlier than ONTAP 9.3, then encryption is disabled on the destination volume by default.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volumes for which you want to create vault relationships, and then click **More Actions** > **Protect**.

   The **Protect** option is available only for a read/write volume.

4. Select the **Replication** type:

If you selected the replication type as…	Do this…
Asynchronous	a. **Optional:** If you do not know the replication type and relationship type, click **Help me Choose**, specify the values, and then click **Apply**. b. Select the relationship type. The relationship type can be mirror, vault, or mirror and vault. c. Select a cluster and an SVM. If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed. d. Modify the volume name suffix, if required.

If you selected the replication type as…	Do this…
Synchronous	a. **Optional:** If you do not know the replication type and relationship type, click **Help me Choose**, specify the values, and then click **Apply**. b. Select the synchronization policy. The synchronization policy can be StrictSync or Sync. c. Select a cluster and an SVM. If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed. d. Modify the volume name suffix, if required.

5. Click ⚙, update the protection policy and protection schedule, enable SnapLock properties on the destination volume, select a FabricPool-enabled aggregate, and then initialize the protection relationship.
6. Click **Save**.

Related information

Protection window

Create a mirror and vault relationship from a source SVM with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create a mirror and vault relationship from the source storage virtual machine (SVM). Creating this relationship enables you to better protect your data by periodically transferring data from the source volume to the destination volume. This relationship also enables you to retain data for long periods by creating backups of the source volume.

Before you begin

- The source cluster must be running ONTAP 8.3.2 or later.
- The SnapMirror license must be enabled on the source cluster and destination cluster.

  - For some platforms, it is not mandatory for the source cluster to have the SnapMirror license enabled if the destination cluster has the SnapMirror license and Data Protection Optimization \(DPO\) license enabled.
  - After the DPO license is enabled on the destination cluster, you must refresh the browser of the source cluster to enable the `Protect` option.

- The source cluster and destination cluster must be in a healthy peer relationship.
- The source SVM and destination SVM must be in a healthy peer relationship, or the destination SVM must have permission to peer.

- The destination aggregate must have space available.
- The source aggregate and the destination aggregate must be 64-bit aggregates.
- FlexVol volumes must be online and of type read/write.
- The SnapLock aggregate type must be the same.
- A maximum of 25 volumes can be protected in one selection.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which Security Assertion Markup Language (SAML) authentication is enabled, password-based authentication must be enabled on the remote cluster.

About this task

- System Manager does not support a cascade relationship.

  For example, a destination volume in a relationship cannot be the source volume in another relationship.

- If encryption is enabled on the source volume and the destination cluster is running a version of ONTAP software earlier than ONTAP 9.3, then encryption is disabled on the destination volume by default.
- SVMs that are peered only for FlexCache applications and do not have peering permissionsforSnapMirror applications are not shown in the list of SVMs in this task. You can use the ONTAP System Manager 9.6 enhanced peering workflow to give permission to, or peer to, these SVMs. You then can select them in this task to create a protection relationship.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volumes for which you want to create mirror and vault relationships, and then click **More Actions** > **Protect**.

   The **Protect** option is available only for a read/write volume.

4. Select the **Replication** type:

If you selected the replication type as…	Do this…
Asynchronous	a. **Optional:** If you do not know the replication type and relationship type, click **Help me Choose**, specify the values, and then click **Apply**. b. Select the relationship type. The relationship type can be mirror, vault, or mirror and vault. c. Select a cluster and an SVM. If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed. d. Modify the volume name suffix, if required.
Synchronous	a. **Optional:** If you do not know the replication type and relationship type, click **Help me Choose**, specify the values, and then click **Apply**. b. Select the synchronization policy. The synchronization policy can be StrictSync or Sync. c. Select a cluster and an SVM. If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed. d. Modify the volume name suffix, if required.

5. **Optional:** Click ⚙, update the protection policy and protection schedule, select **FabricPool-enabled aggregate**, and then initialize the protection relationship.
6. Click **Save**.

Create an NFS datastore for VMware with System Manager - ONTAP 9.7 and earlier

You can use the Create NFS Datastore for VMware wizard in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create an NFS datastore for VMware. You can create a volume for the NFS datastore and specify the ESX servers that can access the NFS datastore.

Before you begin

The NFS service must be licensed.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volume, and then click **More Actions** > **Provision Storage for VMware**.
4. In the **Create NFS Datastore for VMware** wizard, type or select information as required.
5. Confirm the details, and then click **Finish** to complete the wizard.

Change the tiering policy of a volume with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to change the default tiering policy of a volume to control whether the data of the volume is moved to the cloud tier when the data becomes inactive.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the volume for which you want to change the tiering policy, and then click **More Actions** > **Change Tiering Policy**.
4. Select the required tiering policy from the **Tiering Policy** list, and then click **Save**.

Create FlexGroup volumes with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create a FlexGroup volume by selecting specific aggregates or by selecting system-recommended aggregates. A FlexGroup volume can contain many volumes that can be administered as a group instead of individually.

About this task

- You can create only read/write (rw) FlexGroup volumes.
- Beginning with System Manager 9.6, you can create FlexGroup volumes in a MetroCluster configuration.

Steps

1. Click **Storage** > **Volumes**.
2. Click **Create** > **Create FlexGroup**.
3. In the **Create FlexGroup** window, specify a name for the FlexGroup volume.

   By default, the aggregates are selected according to best practices.

4. Click the**Volume Encryption** button to enable encryption for the volume.

   This option is available only if you have enabled the Volume Encryption license and if the corresponding platform supports encryption.

   Turning on volume encryption might affect the cross-volume storage efficiency when the selected

aggregates are encrypted.

5. Specify a size for the FlexGroup volume.

   You must also specify the measurement units.

6. Enable the **FabricPool** toggle button to use FabricPool aggregates in the FlexGroup volume.
   - When you enable **FabricPool**, you can select the Tiering policy from the following choices in the drop-down menu:
     - **Snapshot-only**

       Moves the Snapshot copies of only those volumes that are currently not being referenced by the active file system. Snapshot-only policy is the default tiering policy.

     - **Auto**

       Moves the inactive (cold) data and the Snapshot copies from the active file system to the cloud tier.

     - **Backup (for System Manager 9.5)**

       Moves the newly transferred data of a data protection (DP) volume to the cloud tier.

     - **All (Beginning with System Manager 9.6)**

       Moves all data to the cloud tier.

     - **None**

       Prevents the data on the volume from being moved to a cloud tier.
   - If you leave **FabricPool** in the “not enabled” position, only non-FabricPool aggregates are included in the created FlexGroup volume, and the tiering policy is set to"`None`".
   - If no FabricPool aggregates exist in the SVM, then **FabricPool** displays in the "not enabled" position and cannot be changed.
   - If only FabricPool aggregates exist in the SVM, then the **FabricPool** button is displays in the "enabled" position and cannot be changed.
7. If you want to specify particular aggregates, click (advanced options).

   The aggregates associated with the FlexGroup volume you are creating are selected by default, according to best practices. They are displayed next to the **Aggregates** label.

8. In the **Protection** section, perform the following actions:
   a. Enable the **Volume Protection** option.
   b. Select the **Replication** type.

      The **Synchronous** replication type is not supported for FlexGroup volumes.

   c. Click **Help me Choose**, if you do not know the replication type and relationship type.
      - Specify the values and click **Apply**.

        The replication type and the relationship type is automatically selected based on the values

specified.

d. Select the relationship type.

   The relationship types can be mirror, vault, or mirror and vault.

e. Select a cluster and an SVM for the destination volume.

   If the selected cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the selected cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed.

f. Modify the volume name suffix as required.

9. Click **Create** to create the FlexGroup volume.

Related information

Volumes window

View FlexGroup volume information with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to view information about a FlexGroup volume. You can view a graphical representation of the space allocated, the protection status, and the performance of a FlexGroup volume.

About this task

You can also view the Snapshot copies that are available for the FlexGroup volume, the data protection relationships for the FlexGroup volume, and the average performance metrics, read performance metrics, and write performance metrics of the FlexGroup volume based on latency, IOPS, and throughput.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. From the displayed list of FlexGroup volumes, select the FlexGroup volume about which you want to view information.

   The information about the FlexGroup volume, the space allocated to the FlexGroup volume, the protection status of the FlexGroup volume, and the performance information about the FlexGroup volume are displayed.

4. Click the **Show More Details** link to view more information about the FlexGroup volume.
5. Click the **Snapshot Copies** tab to view the Snapshot copies of the FlexGroup volume.
6. Click the **Data Protection** tab to view the data protection relationships for the FlexGroup volume.
7. Click the **Storage Efficiency** tab to view the storage efficiency settings.
8. Click the **Performance** tab to view the average performance metrics, read performance metrics, and write performance metrics of the FlexGroup volume based on latency, IOPS, and throughput.

Related information

Volumes window

Editing FlexGroup volumes

Beginning with System Manager 9.6, you can edit the properties of an existing FlexGroup volume.

Before you begin

The FlexGroup volume must be online.

About this task

FabricPool FlexGroup volumes can be expanded under the following conditions:

- A FabricPool FlexGroup volume can be expanded only with FabricPool aggregates.
- A non-FabricPool FlexGroup volume can be expanded only with non-FabricPool aggregates.
- If the FlexGroup volume contains a mix of FabricPool and non-FabricPool volumes, then the FlexGroup volume can be expanded with both FabricPool and non-FabricPool aggregates.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the FlexGroup volume that you want to modify, and click **Edit**.
4. **Optional:** If you want to rename the FlexGroup volume, enter the new name in the **Name** field.

   Beginning with System Manager 9.6, you can also rename FlexGroup DP volumes.

5. **Optional:** Enable the **Encrypted** option to enable encryption for the volume.

   This option is available only if you have enabled the Volume Encryption license and if the corresponding platform supports encryption.

6. Specify the percentage of the Snapshot copy reserve.
7. **Optional:** Click ⚙ to modify the FlexGroup volume settings. Refer to Specifying advanced options for a FlexGroup volume.
8. Specify the size to which you want to resize the FlexGroup volume.

   By default, existing aggregates are used to resize the FlexGroup volume. The minimum size that is allowed for the volume is displayed next to the size fields.

   ⓘ If you want to expand the FlexGroup volume by adding new resources, click ⚙ (advanced options). Refer to Specifying advanced options for a FlexGroup volume.

9. Click **Save** to save the changes.

Related information

Volumes window

Specify advanced options for a FlexGroup volume with System Manager - ONTAP 9.7 and earlier

When you create a FlexGroup volume, you can use ONTAP System Manager classic (avaiable in ONTAP 9.7 and earlier) to specify options you want to associate with the

FlexGroup volume.

Steps

1. **Optional:** In the **Create FlexGroup** window, click ⚙ to specify the advanced options.

   The Advanced Options window displays. It contains sections (the headings in the left column), in which you can specify various options.

2. In the **General Details** section, select the space reserve and security style, and then set the UNIX permission for the volume.

   You should note the following limitations:

   - The Space Reserve option is not available for FabricPool aggregates.
   - When thin provisioning is enabled, space is allocated to the volume from the aggregate only when data is written to the volume.
   - For All-Flash Optimized storage systems, thin provisioning is enabled by default, and for other storage systems, thick provisioning is enabled by default.

3. In the **Aggregates** section, you can enable the **Select Aggregates** button to override the best practices defaults and select your choices from a list of FabricPool aggregates.
4. In the **Optimize Space** section, you can enable deduplication on the volume.

   System Manager uses the default deduplication schedule. If the specified volume size exceeds the limit that is required for running deduplication, the volume is created and deduplication is not enabled.

   For systems with All Flash Optimized personality, inline compression and the `auto` deduplication schedule is enabled by default.

5. In the **QoS** (Quality of Service) section, specify the policy group to control the input/output (I/O) performance of the FlexGroup volume.
6. Click **Apply** to update the changes.

Resize FlexGroup volumes with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to resize a FlexGroup volume by resizing existing resources or by adding new resources.

Before you begin

- To resize a FlexGroup volume, there must be enough free space on the existing aggregates.
- To expand a FlexGroup volume, there must be enough free space on the aggregate that you are using for expansion.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the FlexGroup volume that you want to resize, and then click **More Actions** > **Resize**.
4. In the **Resize FlexGroup Volume** window, specify the size to which you want to resize the FlexGroup volume.

   By default, existing aggregates are used to resize the FlexGroup volume. Beginning with System Manager

9.6, the minimum size that is allowed for the volume is displayed next to the size fields.

If you want to expand the FlexGroup volume by adding new resources, click (advanced options).

5. Specify the percentage of the Snapshot copy reserve.
6. Click **Resize** to resize the FlexGroup volume.

Related information

Volumes window

Change the status of a FlexGroup volume with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to change the status of a FlexGroup volume when you want to take a FlexGroup volume offline, bring a FlexGroup volume back online, or restrict access to a FlexGroup volume.

About this task

System Manager does not support constituent-level management for FlexGroup volumes.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the FlexGroup volume for which you want to modify the status.
4. Click **More Actions** > **Change status to**, and then update the FlexGroup volume status by selecting the required status.

Related information

Volumes window

Delete FlexGroup volumes with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to delete a FlexGroup volume when you no longer require the FlexGroup volume.

Before you begin

- The junction path of the FlexGroup volume must be unmounted.
- The FlexGroup volume must be offline.

About this task

System Manager does not support constituent level of management for FlexGroup volumes.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the FlexGroup volume that you want to delete, and then click **Delete**.

4. Select the confirmation check box, and then click **OK**.

Related information

Volumes window

Create FlexCache volumes

Beginning with System Manager 9.6, you can create a FlexCache volume.

About this task

You must have a FlexCache capacity license before you can create a FlexCache volume.

Steps

1. Click **Storage** > **Volumes**.
2. In the **Volumes** window, click **Create** > **FlexCache**.

   The Create FlexCache volume window displays.

3. **Optional:** The following fields in the **Origin Volume** area display values for the origin volume for which you want to create a FlexCache volume. You can modify them.
   - **Cluster**: Use the drop-down menu to select the cluster associated with the origin volume.
   - **SVM**: Use the drop-down menu to select the SVM that contains the origin volume.

     If you choose an SVM that is not peered, but is permitted to peer, System Manager allows you to peer it explicitly.

   - **Volume**: Use the drop-down menu to select the volume name, or enter the name into the field.
4. The following fields in the **FlexCache Volume** area display default values for the FlexCache volume you are creating. You can modify them.
   - **SVM**: Use the drop-down menu to select the SVM in which you want to create the FlexCache volume. If the FlexCache license capacity is full or almost full, you can select **Manage FlexCache license** to modify your license.
   - **New Volume Name**: Enter a name for the FlexCache volume.
   - **Size**: Specify the size for the FlexCache volume, including the measurement units.

     The size field is initially set by default. The size you specify cannot exceed the licensed capacity size.
5. Click **Save** to create the FlexCache volume.

   You can return to the **Volumes** window to view the FlexCache volume in the list of volumes.

Related information

Volumes window

Viewing FlexCache volume information

Beginning with System Manager 9.6, you can view information about a FlexCache volume. You can view a graphical representation of the space allocated and the

performance of a FlexCache volume.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. From the displayed list of volumes, select the FlexCache volume about which you want to view information.

   The **Style** column displays "FlexCache" for a FlexCache volume.

   When you make a selection, the Volume window for the selected FlexCache volume displays.

4. Initially, the **Volume** window displays the **Overview** tab. Click the tabs to view additional details about the FlexCache volume:

Click this tab…	To view these details…
Overview	General information about the FlexCache volume, the space allocated to the FlexCache volume, and performance information about the FlexCache volume.
Storage Efficiency	The storage efficiency settings of the FlexCache volume.
Performance	The average performance metrics, read performance metrics, and write performance metrics of the FlexCache volume based on latency, IOPS, and throughput. Also, the percentage of cache hits or cache misses is displayed.

5. **Optional:** Click **More actions** to view additional information and take actions from the selections in the drop-down menu:

Action	Description
Change status	Enables you to change the status of the FlexCache volume. Refer to Changing the status of a FlexCache volume.
Resize	Enables you to resize the FlexCache volume. Refer to Resizing FlexCache volumes.
Storage Efficiency	Enables you to adjust parameters to improve the storage efficiency of the FlexCache volume.
Storage QoS	Enables you to adjust the minimum and maximum storage limits for the FlexCache volume.

Action	Description
Encryption rekey	Enables you to reset the encryption key (only if you have enabled encryption on the peer cluster that includes the FlexCache volume)

Editing FlexCache volumes

Beginning with System Manager 9.6, you can edit the properties of an existing FlexCache volume.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the FlexCache volume that you want to modify, and click **Edit**.
4. **Optional:** Enter a new name for the FlexCache volume in the **Volume** field under **FlexCache Volume**.
5. **Optional:** Enter a new size for the FlexCache volume in the **Size** field under **FlexCache Volume**, and select the measurement unit from the drop-down menu.
6. **Optional:** Enable or disable encryption.
7. **Optional:** Click ⚙ to modify the FlexCache volume advanced settings. Refer to Specifying advanced options for a FlexCache volume.
8. Click **Save** to save the changes.

Related information

Volumes window

Specifying advanced options for a FlexCache volume

Beginning with System Manager 9.6, when you edit a FlexCache volume, you can specify the advanced options that you want to associate with the FlexCache volume.

Steps

1. **Optional:** In the **Edit FlexCache volume** window, click ⚙ to specify the advanced options.

   The Advanced Options window displays. It contains sections (the headings in the left column), in which you can specify various options.

2. **Optional:** In the **General Details** section, you can edit the permissions for the volume.
3. In the **Aggregates** section, you can enable the **Select Aggregates** toggle button to override the best practices defaults and select your choices from a list of aggregates.
4. In the **Storage Efficiency** section, you can enable compression and deduplication on the volume.

   Deduplication is not enabled by default for FlexCache volumes. System Manager uses the default deduplication schedule if the specified volume size exceeds the limit that is required for running deduplication.

5. Click **Apply** to update the changes.

Resizing FlexCache volumes

Beginning with System Manager 9.6, you can resize a FlexCache volume by resizing existing resources or by adding new resources.

Before you begin

- To resize a FlexCache volume, there must be enough free space on the existing aggregates.
- To expand a FlexCache volume, there must be enough free space on the aggregate that you are using for expansion.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the FlexCache volume that you want to resize, and then click **More Actions** > **Resize**.
4. In the **Resize FlexCache Volume** window, specify the size to which you want to resize the FlexCache volume.

   By default, existing aggregates are used to resize the FlexCache volume. Beginning with System Manager 9.6, the maximum size that is allowed for the volume is displayed next to the size field.

   If you want to expand the FlexCache volume by adding new resources, click ⚙ (advanced options). Refer to Specifying advanced options for FlexCache volumes.

5. Click **Save** to resize the FlexCache volume.

Related information

Volumes window

Changing the status of a FlexCache volume

Beginning with System Manager 9.6, you can change the status of a FlexCache volume when you want to take it offline, bring a FlexCache volume back online, or restrict access to a FlexCache volume.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the FlexCache volume for which you want to modify the status.
4. Click **More Actions** > **Change status to**, and then update the FlexCache volume status by selecting the required status.

   To take a FlexCache volume offline and to change the status to "restricted", you must first unmount the volume.

Deleting FlexCache volumes

Beginning with System Manager 9.6, you can delete a FlexCache volume when you no

longer require it.

Before you begin

- The junction path of the FlexCache volume must be unmounted.
- The FlexCache volume must be offline.

Steps

1. Click **Storage** > **Volumes**.
2. From the drop-down menu in the **SVM** field, select **All SVMs**.
3. Select the FlexCache volume that you want to delete, and then click **Delete**.
4. Select the confirmation check box, and then click **OK**.

Related information

Volumes window

About volume guarantees for FlexVol volumes with System Manager - ONTAP 9.7 and earlier

You can set volume guarantees for FlexVol volumes with System Manager classic (available in ONTAP 9.7 and earlier). Volume guarantees (sometimes called *space guarantees*) determine how space for a volume is allocated from its containing aggregate—whether or not the space is preallocated for the volume.

The guarantee is an attribute of the volume.

You set the guarantee when you create a new volume; you can also change the guarantee for an existing volume, provided that sufficient free space exists to honor the new guarantee.

Volume guarantee types can be `volume` (the default type) or `none`.

- A guarantee type of `volume` allocates space in the aggregate for the entire volume when you create the volume, regardless of whether that space is used for data yet.

  The allocated space cannot be provided to or allocated for any other volume in that aggregate.

- A guarantee of `none` allocates space from the aggregate only as it is needed by the volume.

  The amount of space consumed by volumes with this guarantee type grows as data is added instead of being determined by the initial volume size, which might leave space unused if the volume data does not grow to that size. The maximum size of a volume with a guarantee of `none` is not limited by the amount of free space in its aggregate. It is possible for the total size of all volumes associated with an aggregate to exceed the amount of free space for the aggregate, although the amount of space that can actually be used is limited by the size of aggregate.

  Writes to LUNs or files (including space-reserved LUNs and files) contained by that volume could fail if the containing aggregate does not have enough available space to accommodate the write.

When space in the aggregate is allocated for a `volume` guarantee for an existing volume, that space is no longer considered free in the aggregate, even if the volume is not yet using the space. Operations that consume free space in the aggregate, such as creation of aggregate Snapshot copies or creation of new volumes in the containing aggregate, can occur only if there is enough available free space in that aggregate;

these operations are prevented from using space already allocated to another volume.

When the free space in an aggregate is exhausted, only writes to volumes or files in that aggregate with preallocated space are guaranteed to succeed.

Guarantees are honored only for online volumes. If you take a volume offline, any allocated but unused space for that volume becomes available for other volumes in that aggregate. When you try to bring that volume back online, if there is insufficient available space in the aggregate to fulfill its guarantee, it will remain offline. You must force the volume online, at which point the volume's guarantee will be disabled.

Related information

NetApp Technical Report 3965: NetApp Thin Provisioning Deployment and Implementation Data ONTAP 8.1 (7-Mode)

Use space reservations with FlexVol volumes with System Manager - ONTAP 9.7 and earlier

In ONTAP System Manager classic (available in ONTAP 9.7 and earlier), you can use space reservation to provision FlexVol volumes. Thin provisioning appears to provide more storage than is actually available from a given aggregate, as long as not all of that storage is currently being used.

Thick provisioning sets aside enough storage from the aggregate to ensure that any block in the volume can be written to at any time.

Aggregates can provide storage to volumes contained by more than one storage virtual machine (SVM). If you are using thin provisioning, and you need to maintain strict separation between your SVMs (for example, if you are providing storage in a multi-tenancy environment), you should either use fully allocated volumes (thick provisioning) or ensure that your aggregates are not shared between tenants.

When the space reserve is set to "Default", the ONTAP space reservation settings apply to the volumes.

Related information

NetApp Technical Report 3563: NetApp Thin Provisioning Increases Storage Utilization With On Demand Allocation

NetApp Technical Report 3483: Thin Provisioning in a NetApp SAN or IP SAN Enterprise Environment

Options for resizing volumes with System Manager - ONTAP 9.7 and earlier

You can use the Volume Resize wizard in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to change your volume size, adjust the Snapshot reserve, delete Snapshot copies, and dynamically view the results of your changes.

The Volume Resize wizard displays a bar graph that displays the current space allocations within the volume, including the amount of used and free space. When you make changes to the size or Snapshot reserve of the volume, this graph is updated dynamically to reflect the changes.

You can also use the **Calculate space** button to determine the amount of space that is freed by deleting selected Snapshot copies.

You can use the Volume Resize wizard to make the following changes to your volume:

- **Change the volume size**

  You can change the total volume size to increase or decrease storage space.

- **Adjust Snapshot reserve**

  You can adjust the amount of space reserved for Snapshot copies to increase or decrease storage space.

- **Delete Snapshot copies**

  You can delete Snapshot copies to reclaim volume space.

  Snapshot copies that are in use cannot be deleted.

- **Autogrow**

  You can specify the limit to which the volume can be grown automatically, if required.

Volumes window in System Manager - ONTAP 9.7 and earlier

You can use the Volumes window in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage your FlexVol volumes and FlexGroup volumes. Beginning with System Manager 9.6, you can also manage FlexCache volumes.

You cannot view or manage volumes that are in storage virtual machines (SVMs) that are configured for disaster recovery by using System Manager. You must use the CLI instead.

The command buttons and list of columns will differ based on the type of volume that is selected. You can view only those command buttons and columns that are applicable for the selected volume.

Selection field

- **SVM selection pull-down menu**

  Enables you to select all SVMs or a specific SVM to display in the list.

Command buttons

- **Create**

  Provides the following options:

  - **FlexVol**

    Opens the Create Volume dialog box, which enables you to add FlexVol volumes.

  - **FlexGroup**

    Opens the Create FlexGroup window, which enables you to create FlexGroup volumes.

  - **FlexCache**

Opens the Create FlexCache Volume window, which enables you to create FlexCache volumes.

- **Edit**

  Enables you to edit the properties of the selected volume.

- **Delete**

  Deletes the selected volume or volumes.

- **More Actions**

  Provides the following options:

  - **Change status to**

    Changes the status of the selected volume to one of the following statuses:

    - Online
    - Offline
    - Restrict

  - **Resize**

    Enables you to change the size of the volume.

    For FlexGroup volumes, you can use existing resources to resize the volumes or you can add new resources to expand the volumes.

    For FlexCache volumes, you can also add or remove an aggregate.

  - **Protect**

    Opens the Create Protection Relationship window for the volumes that are selected as source.

  - **Manage Snapshots**

    Provides a list of Snapshot options, including the following:

    - **Create**

      Displays the Create Snapshot dialog box, which you can use to create a Snapshot copy of the selected volume.

    - **Configuration Settings**

      Configures the Snapshot settings.

    - **Restore**

      Restores a Snapshot copy of the selected volume.

  - **Clone**

    Provides a list of clone options, including the following:

- **Create**

  Creates a clone of the selected volume or a clone of a file from the selected volume.

- **Split**

  Splits the clone from the parent volume.

- **View Hierarchy**

  Displays information about the clone hierarchy.

◦ **Storage Efficiency**

Opens the Storage Efficiency dialog box, which you can use to manually start deduplication or to abort a running deduplication operation. This button is displayed only if deduplication is enabled on the storage system.

◦ **Move**

Opens the Move Volume dialog box, which you can use to move volumes from one aggregate or node to another aggregate or node within the same SVM.

◦ **Storage QoS**

Opens the Quality of Service details dialog box, which you can use to assign one or more volumes to a new or existing policy group.

◦ **Change Tiering Policy**

Enables you to change the tiering policy of the selected volume.

◦ **Volume Encryption Rekey**

Changes the data encryption key of the volume.

The data in the volume is re-encrypted using the new key that is automatically generated. The old key is automatically deleted after the rekey operation finishes.

Beginning with System Manager 9.6, volume encryption rekey is supported for FlexGroup DP volumes and FlexCache volumes. Rekey is disabled for volumes that have inherited encryption from an NAE aggregate.

If you initiate a volume move operation when the rekey operation of the same volume is in progress, the rekey operation is aborted. In System Manager 9.5 and earlier version, if you try to move a volume when a conversion or rekey operation of a volume is in progress, then the operation is aborted without warning. Beginning with System Manager 9.6, if you attempt a volume move during a conversion or rekey operation, a message is displayed warning that the conversion or rekey operation will be aborted if you continue.

◦ **Provision Storage for VMware**

Enables you to create a volume for the NFS datastore and to specify the ESX servers that can access the NFS datastore.

- **View Missing Protection Relationship**

  Displays the read/write volumes that are online and are not protected, and displays the volumes that have protection relationships but are not initialized.

- **Reset Filters**

  Enables you to reset the filters that were set to view missing protection relationships.

- **Refresh**

  Updates the information in the window.

-

  Enables you to select which details you want to display in the list on the Volumes window.

Volume list

- **Status**

  Displays the status of the volume.

- **Name**

  Displays the name of the volume.

- **Style**

  In System Manager 9.5, this column displays the type of volume, such as FlexVol or FlexGroup. FlexCache volumes created by using the CLI are displayed as FlexGroup volumes.

  In System Manager 9.6, this column displays the type of volume: FlexVol, FlexGroup, or FlexCache.

- **SVM**

  Displays the SVM that contains the volume.

- **Aggregates**

  Displays the name of the aggregates belonging to the volume.

- **Thin Provisioned**

  Displays whether a space guarantee is set for the selected volume. Valid values for online volumes are `Yes` and `No`.

- **Root volume**

  Displays whether the volume is a root volume.

- **Available Space**

  Displays the available space in the volume.

- **Total Space**

  Displays the total space in the volume, which includes the space that is reserved for Snapshot copies.

- **% Used**

  Displays the amount of space (in percentage) that is used in the volume.

- **Logical Used %**

  Displays the amount of logical space (in percentage), including space reserves, that is used in the volume.

  This field is displayed only if you have enabled logical space reporting by using the CLI.

- **Logical Space Reporting**

  Displays whether logical space reporting is enabled on the volume.

  This field is displayed only if you have enabled logical space reporting by using the CLI.

- **Logical Space Enforcement**

  Displays whether to perform logical space accounting on the volume.

- **Type**

  Displays the type of volume: `rw` for read/write, `ls` for load sharing, or `dp` for data protection.

- **Protection Relationship**

  Display whether the volume has a protection relationship initiated.

  If the relationship is between an ONTAP system and a non-ONTAP system, the value is displayed as `No` by default.

- **Storage Efficiency**

  Displays whether deduplication is enabled or disabled for the selected volume.

- **Encrypted**

  Displays whether the volume is encrypted or not.

- **QoS Policy Group**

  Displays the name of the Storage QoS policy group to which the volume is assigned. By default, this column is hidden.

- **SnapLock Type**

  Displays the SnapLock type of the volume.

- **Clone**

  Displays whether the volume is a FlexClone volume.

- **Is Volume Moving**

  Displays whether a volume is being moved from one aggregate to another aggregate or from one node to another node.

- **Tiering Policy**

  Displays the tiering policy of a FabricPool-enabled aggregate. The default tiering policy is “snapshot-only”.

- **Application**

  Displays the name of the application that is assigned to the volume.

Overview area

You can click the plus sign (+) to the left in the row in which a volume is listed to view an overview of the details about that volume.

- **Protection**

  Displays the **Data Protection** tab of the Volume window for the selected volume.

- **Performance**

  Displays the **Performance** tab of the Volume window for the selected volume.

- **Show More Details**

  Displays the Volume window for the selected volume.

Volume window for the selected volume

You can display this window by either of these methods:

- Clicking the volume name in the list of volumes on the Volumes window.
- Clicking **Show More Details** on the **Overview** area displayed for the selected volume.

The Volume window displays the following tabs:

- **Overview tab**

  Displays general information about the selected volume, and displays a pictorial representation of the space allocation of the volume, the protection status of the volume, and the performance of the volume. The Overview tab displays details about the encryption of the volume, such as the encryption status and the encryption type, the conversion status or rekey status, information about a volume that is being moved, such as the state and phase of the volume move, the destination node and aggregate to which the volume is being moved, the percentage of volume move that is complete, the estimated time to complete the volume move operation, and details of the volume move operation. This tab also displays information about whether the volume is blocked for input/output (I/O) operations and the application blocking the operation.

  For FlexCache volumes, details about the origin of the FlexCache volume are displayed.

  The refresh interval for performance data is 15 seconds.

This tab contains the following command button:

- **Cutover**

  Opens the Cutover dialog box, which enables you to manually trigger the cutover.

  The **Cutover** command button is displayed only if the volume move operation is in the “replication” or “hard deferred” state.

- **Snapshot Copies tab**

  Displays the Snapshot copies of the selected volume. This tab contains the following command buttons:

  - **Create**

    Opens the Create Snapshot Copy dialog box, which enables you to create a Snapshot copy of the selected volume.

  - **Configuration Settings**

    Configures the Snapshot settings.

  - **More Actions › Rename**

    Opens the Rename Snapshot Copy dialog box, which enables you to rename a selected Snapshot copy.

  - **More Actions › Restore**

    Restores a Snapshot copy.

  - **More Actions › Extend Expiry Period**

    Extends the expiry period of a Snapshot copy.

  - **Delete**

    Deletes the selected Snapshot copy.

  - **Refresh**

    Updates the information in the window.

- **Data Protection tab**

  Displays data protection information about the selected volume.

  If the source volume (read/write volume) is selected, the tab displays all of the mirror relationships, vault relationships, and mirror and vault relationships that are related to the destination volume (DP volume). If the destination volume is selected, the tab displays the relationship with the source volume.

  If some or all of the cluster peer relationships of the local cluster are in an unhealthy state, the Data Protection tab might take some time to display the protection relationships relating to a healthy cluster peer relationship. Relationships relating to unhealthy cluster peer relationships are not displayed.

- **Storage Efficiency tab**

Displays information in the following panes:

- Bar graph

  Displays (in graphical format) the volume space that is used by data and Snapshot copies. You can view details about the space used before and after applying settings for storage efficiency savings.

- Details

  Displays information about deduplication properties, including whether deduplication is enabled on the volume, the deduplication mode, the deduplication status, type, and whether inline or background compression is enabled on the volume.

- Last run details

  Provides details about the last-run deduplication operation on the volume. Space savings resulting from compression and deduplication operations that are applied on the data on the volume are also displayed.

- **Performance tab**

  Displays information about the average performance metrics, read performance metrics, and write performance metrics of the selected volume, including throughput, IOPS, and latency.

  Changing the client time zone or the cluster time zone impacts the performance metrics graphs. You must refresh your browser to view the updated graphs.

- **FlexCache tab**

  Displays details about FlexCache volumes only if the volume you selected is an origin volume that has FlexCache volumes associated with it. Otherwise, this tab does not appear.

Related information

Creating FlexVol volumes

Creating FlexClone volumes

Creating FlexClone files

Deleting volumes

Setting the Snapshot copy reserve

Deleting Snapshot copies

Creating Snapshot copies outside a defined schedule

Editing volume properties

Changing the status of a volume

Enabling storage efficiency on a volume

Changing the deduplication schedule

Running deduplication operations

Splitting a FlexClone volume from its parent volume

Resizing volumes

Restoring a volume from a Snapshot copy

Scheduling automatic creation of Snapshot copies

Renaming Snapshot copies

Hiding the Snapshot copy directory

Viewing the FlexClone volume hierarchy

Creating FlexGroup volumes

Editing FlexGroup volumes

Resizing FlexGroup volumes

Changing the status of a FlexGroup volume

Deleting FlexGroup volumes

Viewing FlexGroup volume information

Creating FlexCache volumes

Editing FlexCache volumes

Resizing FlexCache volumes

Deleting FlexCache volumes

Junction Path window in System Manager - ONTAP 9.7 and earlier

You can use the Junction Path window in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to mount or unmount FlexVol volumes to a junction in the SVM namespace.

Mount volumes

You can use System Manager to mount volumes to a junction in the storage virtual machine (SVM) namespace.

About this task

- If you mount a volume to a junction path with a language setting that is different from that of the immediate parent volume in the path, NFSv3 clients cannot access some of the files because some characters might not be decoded correctly.

  This issue does not occur if the immediate parent directory is the root volume.

- You can mount a SnapLock volume only under the root of the SVM.
- You cannot mount a regular volume under a SnapLock volume.

Steps

1. Click **Storage** > **Junction Path**.
2. From the drop-down menu in the **SVM** field, select the SVM on which you want to mount a volume.
3. Click **Mount**, and then select the volume that is to be mounted.
4. **Optional:** If you want to change the default junction name, specify a new name.
5. Click **Browse**, and then select the junction path to which you want to mount the volume.
6. Click **OK**, and then click **Mount**.
7. Verify the new junction path in the **Details** tab.

Unmount FlexVol volumes

You can use the Junction Path option of Storage pane in System Manager to unmount FlexVol volumes from a junction in the storage virtual machine (SVM) namespace.

Steps

1. Click **Storage** > **Junction Path**.
2. From the drop-down menu in the **SVM** field, select the SVM from which you want to unmount a volume.
3. Select the volumes that have to be unmounted, and then click **Unmount**.
4. Select the confirmation check box, and then click **Unmount**.

Change export policies

When a volume is created, the volume automatically inherits the default export policy of the root volume of the storage virtual machine (SVM). You can use System Manager to change the default export policy that is associated with the volume to redefine the client access to data.

Steps

1. Click **Storage** > **Junction Path**.
2. From the drop-down menu in the **SVM** field, select the SVM in which the volume that you want to modify resides.
3. Select the volume, and then click **Change Export Policy**.
4. Select the export policy, and then click **Change**.
5. Verify that the **Export Policy** column in the **Junction Path** window displays the export policy that you applied to the volume.

Results

The default export policy is replaced with the export policy that you selected.

Junction Path window

You can use the Junction Path menu to manage the NAS namespace of storage virtual machines (SVMs).

Command buttons

- **Mount**

  Opens the Mount Volume dialog box, which enables you to mount a volume to the junction in an SVM namespace.

- **Unmount**

  Opens the Unmount Volume dialog box, which enables you to unmount a volume from its parent volume.

- **Change Export Policy**

  Opens the Change Export Policy dialog box, which enables you to change the existing export policy associated with the volume.

- **Refresh**

  Updates the information in the window.

Junction Path list

- **Path**

  Specifies the junction path of the mounted volume. You can click the junction path to view the related volumes and qtrees.

- **Storage Object**

  Specifies the name of the volume mounted on the junction path. You can also view the qtrees that the volume contains.

- **Export Policy**

  Specifies the export policy of the mounted volume.

- **Security Style**

  Specifies the security style for the volume. Possible values include UNIX (for UNIX mode bits), NTFS (for CIFS ACLs), and Mixed (for mixed NFS and CIFS permissions).

Details tab

Displays general information about the selected volume or qtree, such as the name, type of storage object, junction path of the mounted object, and export policy. If the selected object is a qtree, details about the space hard limit, space soft limit, and space usage are displayed.

Manage shares with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create, edit, and manage shares.

Create a CIFS share

You can use System Manager to create a CIFS share that enables you to specify the folder, qtree, or volume that CIFS users can access.

Before you begin

You must have installed the CIFS license before you set up and start CIFS.

Steps

1. Click **Storage** > **Shares**.
2. From the drop-down menu in the **SVM** field, select the SVM on which you want to create a CIFS share.
3. Click **Create Share**.
4. In the **Create Share** window, click **Browse**, and then select the folder, qtree, or volume that should be shared.
5. Specify a name for the new CIFS share.
6. **Optional:** Select the **Enable continuous availability for Hyper-V and SQL** check box to permit clients that support SMB 3.0 and later to open files persistently during nondisruptive operations.

   Files that are opened by using this option are protected from disruptive events such as failover, giveback, and LIF migration.

   Starting with System Manager 9.6, continuous availability is supported for FlexGroup volumes.
7. Select the **Encrypt data while accessing this share** check box to enable SMB 3.0 encryption.
8. Provide a description or comment for the share, and then click **Create**.

Results

The CIFS share is created with the access permissions set to “Full Control for Everyone” in the group.

Stop share access

You can use System Manager to stop a share when you want to remove the shared network access to a folder, qtree, or volume.

Before you begin

You must have installed the CIFS license.

Steps

1. Click **Storage** > **Shares**.
2. From the drop-down menu in the **SVM** field, select the SVM on which the CIFS share that you want to stop resides.
3. From the list of shares, select the share that you want to stop sharing, and then click **Stop Sharing**.
4. Select the confirmation check box, and then click **Stop**.
5. Verify that the share is no longer listed in the **Shares** window.

Create home directory shares

You can use System Manager to create a home directory share and to manage home directory search paths.

Before you begin

CIFS must be set up and started.

Steps

1. Click **Storage** > **Shares**.
2. Click **Create Home Directory**, and then provide the pattern information that determines how a user is mapped to a directory.
3. Click **Create**.
4. Verify that the home directory that you created is listed in the **Shares** window.

Edit share settings

You can use System Manager to modify the settings of a share such as the symbolic link settings, share access permissions of users or groups, and the type of access to the share. You can also enable or disable continuous availability of a share over Hyper-V, and enable or disable access-based enumeration (ABE). Starting with System Manager 9.6, continuous availability is supported for FlexGroup volumes.

Steps

1. Click **Storage** > **Shares**.
2. Select the share that you want to modify from the list of shares, and then click **Edit**.
3. In the **Edit Share Settings** dialog box, modify the share settings as required:
   a. In the **General** tab, enable continuous availability of a share over Hyper-V.

      Enabling continuous availability permits SMB 3.0 and clients that support SMB 3.0 to open files persistently during nondisruptive operations. Files that are opened persistently are protected from disruptive events such as failover, giveback, and LIF migration.

   b. In the **Permissions** tab, add users or groups, and then assign permissions to specify the type of access.
   c. In the **Options** tab, select the required options.
4. Click **Save and Close**.
5. Verify the changes that you made to the selected share in the **Shares** window.

How ONTAP enables dynamic home directories

ONTAP home directories enable you to configure an SMB share that maps to different directories based on the user that connects to it and a set of variables. Instead of creating separate shares for each user, you can configure one share with a few home directory parameters to define a user’s relationship between an entry point (the share) and the home directory (a directory on the SVM).

A user who is logged in as a guest user does not have a home directory and cannot access other users' home directories. There are four variables that determine how a user is mapped to a directory:

- **Share name**

  This is the name of the share that you create to which the user connects. You must set the home directory property for this share.

  The share name can use the following dynamic names:

- `%w` (the user's Windows user name)
- `%d` (the user's Windows domain name)
- `%u` (the user's mapped UNIX user name)

To make the share name unique across all home directories, the share name must contain either the `%w` or the `%u` variable. The share name can contain both the `%d` and the `%w` variable (for example, `%d/%w`), or the share name can contain a static portion and a variable portion (for example, home_`%w`).

- **Share path**

  This is the relative path, which is defined by the share and is therefore associated with one of the share names, that is appended to each search path to generate the user's entire home directory path from the root of the SVM. It can be static (for example, `home`), dynamic (for example, `%w`), or a combination of the two (for example, `eng/%w`).

- **Search paths**

  This is the set of absolute paths from the root of the SVM that you specify that directs the ONTAP search for home directories. You can specify one or more search paths by using the `vserver cifs home-directory search-path add` command. If you specify multiple search paths, ONTAP tries them in the order specified until it finds a valid path.

- **Directory**

  This is the user's home directory that you create for the user. The directory name is usually the user's name. You must create the home directory in one of the directories that are defined by the search paths.

As an example, consider the following setup:

- User: John Smith
- User domain: acme
- User name: jsmith
- SVM name: vs1
- Home directory share name #1: home_`%w` - share path: `%w`
- Home directory share name #2: `%w` - share path: `%d/%w`
- Search path #1: `/vol0home/home`
- Search path #2: `/vol1home/home`
- Search path #3: `/vol2home/home`
- Home directory: `/vol1home/home/jsmith`

Scenario 1: The user connects to `\\vs1\home_jsmith`. This matches the first home directory share name and generates the relative path `jsmith`. ONTAP now searches for a directory named `jsmith` by checking each search path in order:

- `/vol0home/home/jsmith` does not exist; moving on to search path #2.
- `/vol1home/home/jsmith` does exist; therefore, search path #3 is not checked; the user is now connected to his home directory.

Scenario 2: The user connects to `\\vs1\jsmith`. This matches the second home directory share name and generates the relative path `acme/jsmith`. ONTAP now searches for a directory named `acme/jsmith` by checking each search path in order:

- `/vol0home/home/acme/jsmith` does not exist; moving on to search path #2.
- `/vol1home/home/acme/jsmith` does not exist; moving on to search path #3.
- `/vol2home/home/acme/jsmith` does not exist; the home directory does not exist; therefore, the connection fails.

Shares window

You can use the Shares window to manage your shares and to view information about the shares.

Command buttons

- **Create Share**

  Opens the Create Share dialog box, which enables you to create a share.

- **Create Home Directory**

  Opens the Create Home Directory Share dialog box, which enables you to create a new home directory share.

- **Edit**

  Opens the Edit Settings dialog box, which enables you to modify the properties of a selected share.

- **Stop Sharing**

  Stops the selected object from being shared.

- **Refresh**

  Updates the information in the window.

Shares list

The shares list displays the name and path of each share.

- **Share Name**

  Displays the name of the share.

- **Path**

  Displays the complete path name of an existing folder, qtree, or volume that is shared. Path separators can be backward slashes or forward slashes, although ONTAP displays all path separators as forward slashes.

- **Home Directory**

  Displays the name of the home directory share.

- **Comment**

Displays additional descriptions of the share, if any.

- **Continuously Available Share**

  Displays whether the share is enabled for continuous availability. Starting with System Manager 9.6, continuous availability is supported for FlexGroup volumes.

Details area

The area below the shares list displays the share properties and the access rights for each share.

- **Properties**
  - Name

    Displays the name of the share.

  - Oplocks status

    Specifies whether the share uses opportunistic locks (oplocks).

  - Browsable

    Specifies whether the share can be browsed by Windows clients.

  - Show Snapshot

    Specifies whether Snapshot copies can be viewed by clients.

  - Continuously Available Share

    Specifies whether the share is enabled or disabled for continuous availability. Starting with System Manager 9.6, continuous availability is supported for FlexGroup volumes.

  - Access-Based Enumeration

    Specifies whether access-based enumeration (ABE) is enabled or disabled on the share.

  - BranchCache

    Specifies whether BranchCache is enabled or disabled on the share.

  - SMB Encryption

    Specifies whether data encryption using SMB 3.0 is enabled at the storage virtual machine (SVM) level or at the share level. If SMB encryption is enabled at the SVM level, SMB encryption applies for all of the shares and the value is shown as Enabled (at the SVM level).

  - Previous Versions

    Specifies whether the previous versions can be viewed and restored from the client.

- **Share access control**

  Displays the access rights of the domain users, domain groups, local users, and local groups for the share.

Related information

Setting up CIFS

Manage LUNs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage LUNs.

You can access all the LUNs in the cluster by using the LUNs tab or you can access the LUNs specific to the SVM by using **SVMs** > **LUNs**.

The LUNs tab is displayed only if you have enabled the FC/FCoE and iSCSI licenses.

Related information

SAN administration

Create FC SAN optimized LUNs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create one or more FC SAN optimized LUNs during the initial setup of a cluster on an AFF platform.

Before you begin

- You must ensure that only one storage virtual machine (SVM) has been created with the name AFF_SAN_DEFAULT_SVM, and that this SVM does not contain any LUNs.
- You must have verified that the hardware setup has been completed successfully.

  ONTAP 9 Documentation Center

About this task

- This method is available only during the initial setup of a cluster with two or more nodes.

  System Manager uses only the first two nodes to create LUNs.

- Each LUN is created on a separate volume.
- Volumes are thin provisioned.
- Space reservation is disabled on the created LUNs.
- Most of the cluster configurations are already completed at the factory and are optimized for optimum storage efficiency and performance.

  You must not modify these configurations.

Steps

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

   After you create LUNs using this method, you cannot use this method again.

   If you close the dialog box without creating LUNs, you must navigate to the LUNs tab and click **Create** to

access the dialog box again.

2. In the **LUN details** area of the **Create LUNs** dialog box, specify the application type:

If the application type is…	Then…
Oracle	a. Specify the database name and size. b. If you have deployed Oracle Real Application Clusters (RAC), then select the **Oracle RAC** check box. Only two RAC nodes are supported. You must ensure that Oracle RAC has a minimum of two initiators added to the initiator group.
SQL	Specify the number of databases and the size of each database.
Other	a. Specify the name and size of each LUN. b. If you want to create more LUNs, click **Add more LUNs**, and then specify the name and size for each LUN.

   Data, log, binary, and temporary LUNs are created based on the selected application type.

3. In the **Map to these Initiators** area, perform these steps:

   a. Specify the initiator group name and the type of operating system.

   b. Add the host initiator WWPN by selecting it from the drop-down list or by typing the initiator in the text box.

   c. Add the alias for the initiator.

   Only one initiator group is created.

4. Click **Create**.

   A summary table is displayed with the LUNs that are created.

5. Click **Close**.

Related information

ONTAP 9 Documentation Center

Application-specific LUN settings with System Manager - ONTAP 9.7 and earlier

ONTAP System Manager classic (available in ONTAP 9.7 and earlier) supports Oracle, SQL, and other application types while creating FC SAN optimized LUNs on an AFF cluster. LUN settings such as the LUN size are determined by rules specific to the application type. For SQL and Oracle, LUN settings are automatically created.

If your cluster contains two or more nodes, System Manager uses only the first two nodes selected by the API to create LUNs. Data aggregates are already created in each of the two nodes. The size of each volume created is equal to the available capacity of the aggregate. The volumes are thin-provisioned and space reservation is disabled on the LUNs.

Storage efficiency policy is enabled by default with the schedule set to “daily” and quality of service (QoS) set to “best_effort”. By default, access time (atime) update is enabled on the cluster. However, access time updates are disabled by System Manager while creating volumes and therefore every time a file is read or written, the access time field in the directory is not updated.

Enabling the access time update causes performance degradation to the data-serving capability of the cluster.

LUN settings for SQL

By default, LUNs and volumes are provisioned for a single instance of the SQL server with 2 databases of 1 TB each and 24 physical cores. Space is provisioned for LUNs and volumes according to specific rules for the SQL server. Load balancing is performed for LUNs across the HA pair. You can modify the number of databases. For each database, eight data LUNs and one log LUN is created. One temporary LUN is created for each SQL instance.

The following table provides information about how space is provisioned for the default values of SQL:

Node	Aggregate	LUN type	Volume name	LUN name	Formula for LUN size	LUN size (GB)
node1	node1_aggr1	data	db01_data01	db01_data01	Database size ÷ 8	125
		data	db01_data02	db01_data02	Database size ÷ 8	125
		data	db01_data03	db01_data03	Database size ÷ 8	125
		data	db01_data04	db01_data04	Database size ÷ 8	125
		data	db02_data01	db02_data01	Database size ÷ 8	125
		data	db02_data02	db02_data02	Database size ÷ 8	125
		data	db02_data03	db02_data03	Database size ÷ 8	125
		data	db02_data04	db02_data04	Database size ÷ 8	125

Node	Aggregate	LUN type	Volume name	LUN name	Formula for LUN size	LUN size (GB)
		log	db01_log	db01_log	Database size ÷ 20	50
		temp	sql_temp	sql_temp	Database size ÷ 3	330
node2	node2_aggr1	data	db01_data05	db01_data05	Database size ÷ 8	125
		data	db01_data06	db01_data06	Database size ÷ 8	125
		data	db01_data07	db01_data07	Database size ÷ 8	125
		data	db01_data08	db01_data08	Database size ÷ 8	125
		data	db02_data05	db02_data05	Database size ÷ 8	125
		data	db02_data06	db02_data06	Database size ÷ 8	125
		data	db02_data07	db02_data07	Database size ÷ 8	125
		data	db02_data08	db02_data08	Database size ÷ 8	125
		log	db02_log	db02_log	Database size ÷ 20	50

LUN settings for Oracle

By default, LUNs and volumes are provisioned for one database of 2 TB. Space is provisioned for LUNs and volumes according to specific rules for Oracle. By default, Oracle Real Application Clusters (RAC) is not selected.

The following table provides information about how space is provisioned for the default values of Oracle:

Node	Aggregate	LUN type	Volume name	LUN name	Formula for LUN size	LUN size (GB)
node1	node1_aggr1	data	ora_vol01	ora_lundata01	Database size ÷ 8	250

Node	Aggregate	LUN type	Volume name	LUN name	Formula for LUN size	LUN size (GB)
		data	ora_vol02	ora_lundata02	Database size ÷ 8	250
		data	ora_vol03	ora_lundata03	Database size ÷ 8	250
		data	ora_vol04	ora_lundata04	Database size ÷ 8	250
		log	ora_vol05	ora_lunlog1	Database size ÷ 40	50
		binaries	ora_vol06	ora_orabin1	Database size ÷ 40	50
node2	node2_aggr1	data	ora_vol07	ora_lundata05	Database size ÷ 8	250
		data	ora_vol08	ora_lundata06	Database size ÷ 8	250
		data	ora_vol09	ora_lundata07	Database size ÷ 8	250
		data	ora_vol10	ora_lundata08	Database size ÷ 8	250
		log	ora_vol11	ora_lunlog2	Database size ÷ 40	50

For Oracle RAC, LUNs are provisioned for grid files. Only two RAC nodes are supported for Oracle RAC.

The following table provides information about how space is provisioned for the default values of Oracle RAC:

Node	Aggregate	LUN type	Volume name	LUN name	Formula for LUN size	LUN size (GB)
node1	node1_aggr1	data	ora_vol01	ora_lundata01	Database size ÷ 8	250
		data	ora_vol02	ora_lundata02	Database size ÷ 8	250
		data	ora_vol03	ora_lundata03	Database size ÷ 8	250

Node	Aggregate	LUN type	Volume name	LUN name	Formula for LUN size	LUN size (GB)
		data	ora_vol04	ora_lundata04	Database size ÷ 8	250
		log	ora_vol05	ora_lunlog1	Database size ÷ 40	50
		binaries	ora_vol06	ora_orabin1	Database size ÷ 40	50
		grid	ora_vol07	ora_lungrid1	10 GB	10
node2	node2_aggr1	data	ora_vol08	ora_lundata05	Database size ÷ 8	250
		data	ora_vol09	ora_lundata06	Database size ÷ 8	250
		data	ora_vol10	ora_lundata07	Database size ÷ 8	250
		data	ora_vol11	ora_lundata08	Database size ÷ 8	250
		log	ora_vol12	ora_lunlog2	Database size ÷ 40	50
		binaries	ora_vol13	ora_orabin2	Database size ÷ 40	50

LUN settings for other application type

Each LUN is provisioned in a volume. The space is provisioned in the LUNs based on the specified size. Load balancing is performed across the nodes for all the LUNs.

Create LUNs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create LUNs for an existing aggregate, volume, or qtree when there is available free space. You can create a LUN in an existing volume or create a new FlexVol volume for the LUN. You can also enable storage Quality of Service (QoS) to manage the workload performance.

About this task

If you specify the LUN ID, System Manager checks the validity of the LUN ID before adding it. If you do not specify a LUN ID, ONTAP software automatically assigns one.

While selecting the LUN multiprotocol type, you should have considered the guidelines for using each type. The LUN Multiprotocol Type, or operating system type, determines the layout of data on the LUN, and the minimum and maximum sizes of the LUN. After the LUN is created, you cannot modify the LUN host operating system type.

In a MetroCluster configuration, System Manager displays only the following aggregates for creating FlexVol volumes for the LUN:

- In normal mode, when you create volumes on sync-source SVMs or data-serving SVMs in the primary site, only those aggregates that belong to the cluster in the primary site are displayed.
- In switched-over mode, when you create volumes on sync-destination SVMs or data-serving SVMs in the surviving site, only switched-over aggregates are displayed.

Steps

1. Click **Storage** > **LUNs**.
2. In the **LUN Management** tab, click **Create**.
3. Browse and select an SVM in which you want to create the LUNs.
4. In the **Create LUN Wizard**, specify the name, size, type, description for the LUN, and select the **Space Reserve**, and then click **Next**.
5. Create a new FlexVol volume for the LUN or select an existing volume or qtree, and then click **Next**.
6. Add initiator groups if you want to control host access to the LUN, and then click **Next**.
7. Select the **Manage Storage Quality of Service** check box if you want to manage the workload performance of the LUN.
8. Create a new storage QoS policy group or select an existing policy group to control the input/output (I/O) performance of the LUN:

If you want to…	Do this…
Create a new policy group	a. Select **New Policy Group** b. Specify the policy group name. c. Specify the minimum throughput limit. ◦ In System Manager 9.5, you can set the minimum throughput limit only on a performance-based All Flash Optimized personality. In System Manager 9.6, you can also set the minimum throughput limit for ONTAP Select Premium systems. ◦ You cannot set the minimum throughput limit for volumes on a FabricPool-enabled aggregate. ◦ If you do not specify the minimum throughput value or if the minimum throughput value is set to 0, the system automatically displays “None” as the value. This value is case-sensitive. d. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group does not exceed the specified throughput limit. ◦ The minimum throughput limit and the maximum throughput limit must be of the same unit type. ◦ If you do not specify the minimum throughput limit, then you can set the maximum throughput limit in IOPS and B/s, KB/s, MB/s, and so on. ◦ If you do not specify the maximum throughput value, the system automatically displays “Unlimited” as the value and this value is case-sensitive. The unit that you specify does not affect the maximum throughput.

If you want to…	Do this…
Select an existing policy group	a. Select **Existing Policy Group**, and then click **Choose** to select an existing policy group from the Select Policy Group dialog box. b. Specify the minimum throughput limit. ◦ In System Manager 9.5, you can set the minimum throughput limit only on a performance-based All Flash Optimized personality. In System Manager 9.6, you can also set the minimum throughput limit for ONTAP Select Premium systems. ◦ You cannot set the minimum throughput limit for volumes on a FabricPool-enabled aggregate. ◦ If you do not specify the minimum throughput value or if the minimum throughput value is set to 0, the system automatically displays “None” as the value. This value is case-sensitive. c. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group does not exceed the specified throughput limit. ◦ The minimum throughput limit and the maximum throughput limit must be of the same unit type. ◦ If you do not specify the minimum throughput limit, then you can set the maximum throughput limit in IOPS and B/s, KB/s, MB/s, and so on. ◦ If you do not specify the maximum throughput value, the system automatically displays “Unlimited” as the value and this value is case-sensitive. The unit that you specify does not affect the maximum throughput. If the policy group is assigned to more than one object, the maximum throughput that you specify is shared among the objects.

9. Review the specified details in the **LUN summary** window, and then click **Next**.
10. Confirm the details, and then click **Finish** to complete the wizard.

Related information

LUNs window

Guidelines for using LUN multiprotocol type

Delete LUNs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to delete LUNs and return the space used by the LUNs to their containing aggregates or volumes.

Before you begin

- The LUN must be offline.
- The LUN must be unmapped from all initiator hosts.

Steps

1. Click **Storage** > **LUNs**.
2. In the **LUN Management** tab, select one or more LUNs that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

Related information

LUNs window

Manage initiator groups with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage an initiator group. Initiator groups enable you to control host access to specific LUNs. You can use portsets to limit which LIFs an initiator can access.

Create initiator groups

Steps

1. Click **Storage** > **LUNs**.
2. In the **Initiator Groups** tab, click **Create**.
3. In the **General** tab of the **Create Initiator Group** dialog box, specify the initiator group name, operating system, host alias name, portset, and supported protocol for the group.
4. Click **Create**.

Delete initiator groups

You can use the Initiator Groups tab in System Manager to delete initiator groups.

Before you begin

All the LUNs mapped to the initiator group must be manually unmapped.

Steps

1. Click **Storage** > **LUNs**.
2. In the **Initiator Groups** tab, select one or more initiator groups that you want to delete, and then click **Delete**.

3. Click **Delete**.
4. Verify that the initiator groups you deleted are no longer displayed in the **Initiator Groups** tab.

Add initiators

You can use System Manager to add initiators to an initiator group. An initiator provides access to a LUN when the initiator group that it belongs to is mapped to that LUN.

Steps

1. Click **Storage** > **LUNs**.
2. In the **LUN Management** tab, select the initiator group to which you want to add initiators and click **Edit**.
3. In the **Edit Initiator Group** dialog box, click **Initiators**.
4. Click **Add**.
5. Specify the initiator name and click **OK**.
6. Click **Save and Close**.

Delete initiators from an initiator group

You can use the Initiator Groups tab in System Manager to delete an initiator. To delete an initiator from an initiator group, you must disassociate the initiator from the initiator group.

Before you begin

All of the LUNs that are mapped to the initiator group that contains the initiator that you want to delete must be manually unmapped.

Steps

1. Click **Storage** > **LUNs**.
2. In the **Initiator Groups** tab, select the initiator group from which you want to delete the initiator, and then click **Edit**.
3. In the **Edit Initiator Group** dialog box, click the **Initiators** tab.
4. Select and delete the initiator from the text box, and click **Save**.

   The initiator is disassociated from the initiator group.

Related information

LUNs window

Manage portsets with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create, delete and edit portsets.

Create portsets

You can use ONTAP System Manager classic to create portsets to limit access to your LUNs.

Steps

1. Click **Storage** > **LUNs**.

2. In the **Portsets** tab, click **Create**.
3. In the **Create Portset** dialog box, select the type of protocol.
4. Choose the network interface that you want to associate with the portset.
5. Click **Create**.

Delete portsets

You can use System Manager to delete a portset when it is no longer required.

Steps

1. Click **Storage** > **LUNs**.
2. In the **Portsets** tab, select one or more portsets and click **Delete**.
3. Confirm the deletion by clicking **Delete**.

Edit portsets

You can use the Portsets tab in System Manager to edit settings related to portsets.

Steps

1. Click **Storage** > **LUNs**.
2. In the **Portsets** tab, select the portset you want to edit and click **Edit**.
3. In the **Edit Portset** dialog box, make the necessary changes.
4. Click **Save and Close**.

Related information

Configuring iSCSI protocol on SVMs

Clone LUNs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create a temporary copy of a LUN for testing or to make a copy of your data available to additional users without providing them access to the production data. LUN clones enable you to create multiple readable and writable copies of a LUN.

Before you begin

- You must have installed the FlexClone license on the storage system.
- When space reservation is disabled on a LUN, the volume that contains the LUN must have enough space to accommodate changes to the clone.

About this task

- When you create a LUN clone, automatic deletion of the LUN clone is enabled by default in System Manager.

  The LUN clone is deleted when ONTAP triggers automatic deletion to conserve space.

- You cannot clone LUNs that are on SnapLock volumes.

Steps

1. Click **Storage** > **LUNs**.
2. In the **LUN Management** tab, select the LUN that you want to clone, and then click **Clone**.
3. If you want to change the default name, specify a new name for the LUN clone.
4. Click **Clone**.
5. Verify that the LUN clone that you created is listed in the **LUNs** window.

Related information

LUNs window

Edit LUNs with System Manager - ONTAP 9.7 and earlier

You can use the LUN properties dialog box in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to change the name, description, size, space reservation setting, or the mapped initiator hosts of a LUN.

About this task

When you resize a LUN, you have to perform the steps on the host side that are recommended for the host type and the application that is using the LUN.

Steps

1. Click **Storage** > **LUNs**.
2. In the **LUN Management** tab, select the LUN that you want to edit from the list of LUNs, and click **Edit**.
3. Make the required changes.
4. Click **Save and Close**.

Related information

LUNs window

Bring LUNs online with System Manager - ONTAP 9.7 and earlier

You can use the **LUN Management** tab in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to bring selected LUNs online and make them available to the host.

Before you begin

Any host application accessing the LUN must be quiesced or synchronized.

Steps

1. Click **Storage** > **LUNs**.
2. In the **LUN Management** tab, select one or more LUNs that you want to bring online.
3. Click **Status** > **Online**.

Related information

LUNs window

Take LUNs offline with System Manager - ONTAP 9.7 and earlier

You can use the **LUN Management** tab in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to take selected LUNs offline and make them unavailable for block protocol access.

Before you begin

Any host application accessing the LUN must be quiesced or synchronized.

Steps

1. Click **Storage** > **LUNs**.
2. In the **LUN Management** tab, select one or more LUNs that you want to take offline.
3. Click **Status** > **Offline**.

Related information

LUNs window

Move LUNs with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to move a LUN from its containing volume to another volume or qtree within a storage virtual machine (SVM). You can move the LUN to a volume that is hosted on an aggregate containing high-performance disks, thereby improving the performance when accessing the LUN.

About this task

- You cannot move a LUN to a qtree within the same volume.
- If you have created a LUN from a file using the command-line interface (CLI), you cannot move the LUN using System Manager.
- The LUN move operation is nondisruptive; it can be performed when the LUN is online and serving data.
- You cannot use System Manager to move the LUN if the allocated space in the destination volume is not sufficient to contain the LUN, and even if autogrow is enabled on the volume.

  You should use the CLI instead.

- You cannot move LUNs on SnapLock volumes.

Steps

1. Click **Storage** > **LUNs**.
2. In the **LUN Management** tab, select the LUN that you want to move from the list of LUNs, and then click **Move**.
3. **Optional:** In the **Move Options** area of the **Move LUN** dialog box, specify a new name for the LUN if you want to change the default name.
4. Select the storage object to which you want to move the LUN and perform one of the following actions:

If you want to move the LUN to…	Then…
A new volume	a. Select an aggregate in which you want to create the new volume. b. Specify a name for the volume.
An existing volume or qtree	a. Select a volume to which you want to move the LUN. b. If the selected volume contains any qtrees, select the qtree to which you want to move the LUN.

5. Click **Move**.
6. Confirm the LUN move operation, and click **Continue**.

   For a brief period of time, the LUN is displayed on both the origin and destination volume. After the move operation is complete, the LUN is displayed on the destination volume.

   The destination volume or qtree is displayed as the new container path for the LUN.

Assign LUNs to storage QoS with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to limit the throughput of LUNs by assigning them to storage Quality of Service (QoS) policy groups. You can assign storage QoS for new LUNs or modify storage QoS details for LUNs that are already assigned to a policy group.

About this task

- You cannot assign storage QoS to a LUN if the following storage objects are assigned to a policy group:
  - Parent volume of the LUN
  - Parent storage virtual machine (SVM) of the LUN
- You can assign storage QoS or modify the QoS details for a maximum of 10 LUNs simultaneously.

Steps

1. Click **Storage** > **LUNs**.
2. In the **LUN Management** tab, select one or more LUNs for which you want to assign storage QoS.
3. Click **Storage QoS**.
4. In the **Quality of Service Details** dialog box, select the **Manage Storage Quality of Service** check box if you want to manage the workload performance of the LUN.

   If some of the LUNs that you selected are already assigned to a policy group, the changes that you make might affect the performance of these LUNs.

5. Create a new storage QoS policy group or select an existing policy group to control the input/output (I/O) performance of the LUN:

If you want to…	Do this…
Create a new policy group	a. Select **New Policy Group**. b. Specify the policy group name. c. Specify the minimum throughput limit. ◦ In System Manager 9.5, you can set the minimum throughput limit only on a performance-based All Flash Optimized personality. In System Manager 9.6, you can also set the minimum throughput limit for ONTAP Select Premium systems. ◦ You cannot set the minimum throughput limit for volumes on a FabricPool-enabled aggregate. ◦ If you do not specify the minimum throughput value or if the minimum throughput value is set to 0, the system automatically displays “None” as the value. This value is case-sensitive. d. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group does not exceed the specified throughput limit. ◦ The minimum throughput limit and the maximum throughput limit must be of the same unit type. ◦ If you do not specify the minimum throughput limit, then you can set the maximum throughput limit in IOPS and B/s, KB/s, MB/s, and so on. ◦ If you do not specify the maximum throughput value, the system automatically displays “Unlimited” as the value and this value is case-sensitive. The unit that you specify does not affect the maximum throughput.

If you want to…	Do this…
Select an existing policy group	a. Select **Existing Policy Group**, and then click **Choose** to select an existing policy group from the Select Policy Group dialog box. b. Specify the minimum throughput limit. ◦ In System Manager 9.5, you can set the minimum throughput limit only on a performance-based All Flash Optimized personality. In System Manager 9.6, you can also set the minimum throughput limit for ONTAP Select Premium systems. ◦ You cannot set the minimum throughput limit for volumes on a FabricPool-enabled aggregate. ◦ If you do not specify the minimum throughput value or if the minimum throughput value is set to 0, the system automatically displays “None” as the value. This value is case-sensitive. c. Specify the maximum throughput limit to ensure that the workload of the objects in the policy group does not exceed the specified throughput limit. ◦ The minimum throughput limit and the maximum throughput limit must be of the same unit type. ◦ If you do not specify the minimum throughput limit, then you can set the maximum throughput limit in IOPS and B/s, KB/s, MB/s, and so on. ◦ If you do not specify the maximum throughput value, the system automatically displays “Unlimited” as the value and this value is case-sensitive. The unit that you specify does not affect the maximum throughput. If the policy group is assigned to more than one object, the maximum throughput that you specify is shared among the objects.

6. **Optional:** Click the link that specifies the number of LUNs to review the list of selected LUNs, and click **Discard** if you want to remove any LUNs from the list.

   The link is displayed only when multiple LUNs are selected.

7. Click **OK**.

Edit initiator groups with System Manager - ONTAP 9.7 and earlier

You can use the **Edit Initiator Group** dialog box in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to change the name of an existing initiator group and its operating system. You can add initiators to or remove initiators from the initiator group. You can also change the portset associated with the initiator group.

Steps

1. Click **Storage** > **LUNs**.
2. In the **Initiator Groups** tab, select the initiator group that you want to modify, and then click **Edit**.
3. Make the necessary changes.
4. Click **Save and Close**.
5. Verify the changes you made to the initiator group in the **Initiator Groups** tab.

Related information

LUNs window

Edit initiators with System Manager - ONTAP 9.7 and earlier

You can use the **Edit Initiator Group** dialog box in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to change the name of an existing initiator in an initiator group.

Steps

1. Click **Storage** > **LUNs**.
2. In the **Initiator Groups** tab, select the initiator group to which the initiator belongs, and then click **Edit**.
3. In the **Edit Initiator Group** dialog box, click **Initiators**.
4. Select the initiator that you want to edit and click **Edit**.
5. Change the name and click **OK**.
6. Click **Save and Close**.

Related information

LUNs window

View LUN information with System Manager - ONTAP 9.7 and earlier

You can use the **LUN Management** tab in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to view details about a LUN, such as its name, status, size, and type.

Steps

1. Click **Storage** > **LUNs**.
2. In the **LUN Management** tab, select the LUN that you want to view information about from the displayed

list of LUNs.

3. Review the LUN details in the **LUNs** window.

View initiator groups with System Manager - ONTAP 9.7 and earlier

You can use the **Initiator Groups** tab in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to view all the initiator groups and the initiators mapped to these initiator groups, and the LUNs and LUN ID mapped to the initiator groups.

Steps

1. Click **Storage** > **LUNs**.
2. Click **Initiator Groups** and review the initiator groups that are listed in the upper pane.
3. Select an initiator group to view the initiators that belong to it, which are listed in the **Initiators** tab in the lower pane.
4. Select an initiator group to view the LUNs mapped to it, which are listed in the **Mapped LUNs** in the lower pane.

Guidelines for working with FlexVol volumes that contain LUNs with System Manager - ONTAP 9.7 and earlier

In ONTAP System Manager classic (available in ONTAP 9.7 and earlier), when you work with FlexVol volumes that contain LUNs, you must change the default settings for Snapshot copies. You can also optimize the LUN layout to simplify administration.

Snapshot copies are required for many optional features such as SnapMirror, SyncMirror, dump and restore, and ndmpcopy.

When you create a volume, ONTAP automatically performs the following:

- Reserves 5 percent of the space for Snapshot copies
- Schedules Snapshot copies

Because the internal scheduling mechanism for creating Snapshot copies within ONTAP does not ensure that the data within a LUN is in a consistent state, you should change these Snapshot copy settings by performing the following tasks:

- Turn off the automatic Snapshot copy schedule.
- Delete all of the existing Snapshot copies.
- Set the percentage of space reserved for Snapshot copies to zero.

You should use the following guidelines to create volumes that contain LUNs:

- Do not create any LUNs in the system's root volume.

  ONTAP uses this volume to administer the storage system. The default root volume is /vol/vol0.

- You should use a SAN volume to contain the LUN.
- You should ensure that no other files or directories exist in the volume that contains the LUN.

  If this is not possible and you are storing LUNs and files in the same volume, you should use a separate

qtree to contain the LUNs.

- If multiple hosts share the same volume, you should create a qtree on the volume to store all of the LUNs for the same host.

  This is a best practice that simplifies LUN administration and tracking.

- To simplify management, you should use naming conventions for LUNs and volumes that reflect their ownership or the way that they are used.

Related information

ONTAP 9 Documentation Center

Understanding space reservations for LUNs in System Manager - ONTAP 9.7 and earlier

Understanding how the space reservation setting (combined with the volume guarantee) in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) affects how space is set aside for LUNs helps you to understand the ramifications of disabling space reservations. It also helps you to understand why certain combinations of LUN and volume settings are not useful.

When a LUN has space reservations enabled (a space-reserved LUN), and its containing volume has a volume guarantee, free space from the volume is set aside for the LUN at creation time; the size of this reserved space is governed by the size of the LUN. Other storage objects in the volume (other LUNs, files, Snapshot copies, and so on) are prevented from using this space.

When a LUN has space reservations disabled (a non-space-reserved LUN), no space is set aside for that LUN at creation time. The storage required by any write operation to the LUN is allocated from the volume when it is needed, provided sufficient free space is available.

If a space-reserved LUN is created in a none-guaranteed volume, the LUN behaves the same as a non-space-reserved LUN. This is because a none-guaranteed volume has no space to allocate to the LUN; the volume itself can only allocate space as it is written to, due to its none guarantee. Therefore, creating a space-reserved LUN in a none-guaranteed volume is not recommended; employing this configuration combination might provide write guarantees that are in fact impossible.

When the space reserve is set to “Default”, the ONTAP space reservation settings apply to the LUNs. ONTAP space reservation settings also apply to the container volumes if new volumes are created.

Guidelines for using LUN multiprotocol type in System Manager - ONTAP 9.7 and earlier

In ONTAP System Manager classic (available in ONTAP 9.7 and earlier), the LUN multiprotocol type, or operating system type, specifies the operating system of the host accessing the LUN. It also determines the layout of data on the LUN, and the minimum and maximum size of the LUN.

Not all ONTAP versions support all LUN multiprotocol types. For the latest information, see the Interoperability Matrix Tool.

The following table describes the LUN multiprotocol type values and the guidelines for using each type:

LUN multiprotocol type	When to use
AIX	If your host operating system is AIX.
HP-UX	If your host operating system is HP-UX.
Hyper-V	If you are using Windows Server 2008 or Windows Server 2012 Hyper-V and your LUNs contain virtual hard disks (VHDs). If you are using hyper_v for your LUN type, you should also use hyper_v for your igroup OS type. For raw LUNs, you can use the type of child operating system that the LUN multiprotocol type uses.
Linux	If your host operating system is Linux.
NetWare	If your host operating system is NetWare.
OpenVMS	If your host operating system is OpenVMS.
Solaris	If your host operating system is Solaris and you are not using Solaris EFI labels.
Solaris EFI	If you are using Solaris EFI labels. Using any other LUN multiprotocol type with Solaris EFI labels might result in LUN misalignment problems.
VMware	If you are using an ESX Server and your LUNs will be configured with VMFS. If you configure the LUNs with RDM, you can use the guest operating system as the LUN multiprotocol type.
Windows 2003 MBR	If your host operating system is Windows Server 2003 using the MBR partitioning method.
Windows 2003 GPT	If you want to use the GPT partitioning method and your host is capable of using it. Windows Server 2003, Service Pack 1 and later are capable of using the GPT partitioning method, and all 64-bit versions of Windows support it.

LUN multiprotocol type	When to use
Windows 2008 or later	If your host operating system is Windows Server 2008 or later; both MBR and GPT partitioning methods are supported.
Xen	If you are using Xen and your LUNs will be configured with Linux LVM with Dom0. For raw LUNs, you can use the type of guest operating system that the LUN multiprotocol type uses.

Related information

Creating LUNs

NetApp Interoperability

Solaris Host Utilities 6.1 Installation and Setup Guide

Solaris Host Utilities 6.1 Quick Command Reference

Solaris Host Utilities 6.1 Release Notes

LUNs window in System Manager - ONTAP 9.7 and earlier

You can use the LUNs window in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create and manage LUNs and to display information about LUNs. You can also add, edit, or delete initiator groups and initiator IDs.

LUN Management tab

This tab enables you to create, clone, delete, move, or edit the settings of LUNs. You can also assign LUNs to a Storage Quality of Service (QoS) policy group.

Command buttons

- **Create**

  Opens the Create LUN wizard, which enables you to create LUNs.

  In a cluster on an AFF platform that does not contain any existing LUNs, the Create FC SAN optimized LUNs dialog box is opened, which enables you to set up one or more FC SAN optimized LUNs.

- **Clone**

  Opens the Clone LUN dialog box, which enables you to clone the selected LUNs.

- **Edit**

  Opens the Edit LUN dialog box, which enables you to edit the settings of the selected LUN.

- **Delete**

  Deletes the selected LUN.

- **Status**

  Enables you to change the status of the selected LUN to either Online or Offline.

- **Move**

  Opens the Move LUN dialog box, which enables you to move the selected LUN to a new volume or an existing volume or qtree within the same storage virtual machine (SVM).

- **Storage QoS**

  Opens the Quality of Service details dialog box, which enables you to assign one or more LUNs to a new or existing policy group.

- **Refresh**

  Updates the information in the window.

LUNs list

- **Name**

  Displays the name of the LUN.

- **SVM**

  Displays the name of the storage virtual machine (SVM) in which the LUN is created.

- **Container Path**

  Displays the name of the file system (volume or qtree) that contains the LUN.

- **Space Reservation**

  Specifies whether space reservation is enabled or disabled.

- **Available Size**

  Displays the space available in the LUN.

- **Total Size**

  Displays the total space in the LUN.

- **%Used**

  Displays the total space (in percentage) that is used.

- **Type**

  Specifies the LUN type.

- **Status**

  Specifies the status of the LUN.

- **Policy Group**

  Displays the name of the Storage QoS policy group to which the LUN is assigned. By default, this column is hidden.

- **Application**

  Displays the name of the application that is assigned to the LUN.

- **Description**

  Displays the description of the LUN.

Details area

The area below the LUNs list displays details related to the selected LUN.

- **Details tab**

  Displays details related to the LUN such as the LUN serial number, whether the LUN is a clone, LUN description, the policy group to which the LUN is assigned, minimum throughput of the policy group, maximum throughput of the policy group, details about the LUN move operation, and the application assigned to the LUN. You can also view details about the initiator groups and initiators that are associated with the selected LUN.

- **Performance tab**

  Displays performance metrics graphs of the LUNs, including data rate, IOPS, and response time.

  Changing the client time zone or the cluster time zone impacts the performance metrics graphs. Refresh your browser to see the updated graphs.

Initiator Groups tab

This tab enables you to create, delete, or edit the settings of initiator groups and initiator IDs.

Command buttons

- **Create**

  Opens the Create Initiator Group dialog box, which enables you to create initiator groups to control host access to specific LUNs.

- **Edit**

  Opens the Edit Initiator Group dialog box, which enables you to edit the settings of the selected initiator group.

- **Delete**

  Deletes the selected initiator group.

- **Refresh**

  Updates the information in the window.

Initiator Groups list

- **Name**

  Displays the name of the initiator group.

- **Type**

  Specifies the type of protocol supported by the initiator group. The supported protocols are iSCSI, FC/FCoE, or Mixed (iSCSI and FC/FCoE).

- **Operating System**

  Specifies the operating system for the initiator group.

- **Portset**

  Displays the portset that is associated with the initiator group.

- **Initiator Count**

  Displays the number of initiators added to the initiator group.

Details area

The area below the Initiator Groups list displays details about the initiators that are added to the selected initiator group and the LUNs that are mapped to the initiator group.

Portsets tab

This tab enables you to create, delete, or edit the settings of portsets.

Command buttons

- **Create**

  Opens the Create Portset dialog box, which enables you to create portsets to limit access to your LUNs.

- **Edit**

  Opens the Edit Portset dialog box, which enables you to select the network interfaces that you want to associate with the portset.

- **Delete**

  Deletes the selected portset.

- **Refresh**

  Updates the information in the window.

Portsets list

- **Portset Name**

  Displays the name of the portset.

- **Type**

  Specifies the type of protocol supported by the portset. The supported protocols are iSCSI, FC/FCoE, or Mixed (iSCSI and FC/FCoE).

- **Interface Count**

  Displays the number of network interfaces that are associated with the portset.

- **Initiator Group Count**

  Displays the number of initiator groups that are associated with the portset.

Details area

The area below the Portsets list displays details about the network interfaces and initiator groups associated with the selected portset.

Related information

Creating LUNs

Deleting LUNs

Creating initiator groups

Editing LUNs

Editing initiator groups

Editing initiators

Bringing LUNs online

Taking LUNs offline

Cloning LUNs

Manage Qtrees with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create, edit, and delete Qtrees.

Create qtrees

Qtrees enable you to manage and partition your data within a volume. You can use the Create Qtree dialog box in System Manager to add a new qtree to a volume on your storage system.

Steps

1. Click **Storage** > **Qtrees**.
2. From the drop-down menu in the **SVM** field, select the storage virtual machine (SVM) on which you want to create a qtree.
3. Click **Create**.
4. In the **Details** tab of the **Create Qtree** dialog box, type a name for the qtree.
5. Select the volume to which you want to add the qtree.

   The Volume browse list includes only the volumes that are online.

6. If you want to disable opportunistic locks (oplocks) for the qtree, clear the **Enable Oplocks for files and directories in this Qtree** check box.

   By default, oplocks are enabled for each qtree.

7. If you want to change the default inherited security style, select a new security style.

   The default security style of the qtree is the security style of the volume that contains the qtree.

8. If you want to change the default inherited export policy, either select an existing export policy or create an export policy.

   The default export policy of the qtree is the export policy that is assigned to the volume that contains the qtree.

9. If you want to restrict the disk space usage, click the **Quotas** tab.
   a. If you want to apply quotas on the qtree, click **Qtree quota**, and then specify the disk space limit.
   b. If you want to apply quotas for all the users on the qtree, click **User quota**, and then specify the disk space limit.
10. Click **Create**.
11. Verify that the qtree that you created is included in the list of qtrees in the **Qtrees** window.

Delete qtrees

You can delete a qtree and reclaim the disk space that the qtree uses within a volume by using System Manager. When you delete a qtree, all of the quotas that are applicable to that qtree are no longer applied by ONTAP.

Before you begin

- The qtree status must be normal.
- The qtree must not contain any LUN.

Steps

1. Click **Storage** > **Qtrees**.
2. In the **Qtrees** window, select one or more qtrees that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.
4. Verify that the qtree that you deleted is no longer included in the list of qtrees in the **Qtrees** window.

Edit qtrees

You can use System Manager to modify the properties of a qtree such as the security style, enable or disable opportunistic locks (oplocks), and assign a new or existing export policy.

Steps

1. Click **Storage** > **Qtrees**.
2. Select the qtree that you want to edit, and then click **Edit**.
3. In the **Edit Qtree** dialog box, edit the following properties as required:
   - Oplocks
   - Security style
   - Export policy
4. Click **Save**.
5. Verify the changes that you made to the selected qtree in the **Qtrees** window.

Assign export policies to qtrees

Instead of exporting an entire volume, you can export a specific qtree on a volume to make it directly accessible to clients. You can use System Manager to export a qtree by assigning an export policy to the qtree. You can assign an export policy to one or more qtrees from the Qtrees window.

Steps

1. Click **Storage** > **Qtrees**.
2. From the drop-down menu in the SVM field, select the storage virtual machine (SVM) on which the qtrees that you want to export reside.
3. Select one or more qtrees for which you want to assign an export policy, and then click **Change Export Policy**.
4. In the **Export Policy** dialog box, either create an export policy or select an existing export policy.

   Creating an export policy

5. Click **Save**.
6. Verify that the export policy and its related export rules that you assigned to the qtrees are displayed in the **Details** tab of the appropriate qtrees.

View qtree information

You can use the Qtrees window in System Manager to view the volume that contains the qtree, the name, security style, and status of the qtree, and the oplocks status.

Steps

1. Click **Storage** > **Qtrees**.
2. From the drop-down menu in the **SVM** field, select the storage virtual machine (SVM) on which the qtree about which you want to view information resides.
3. Select the qtree from the displayed list of qtrees.
4. Review the qtree details in the **Qtrees** window.

Qtree options

A qtree is a logically defined file system that can exist as a special subdirectory of the root directory within a FlexVol volume. Qtrees are used to manage and partition data within the volume.

If you create qtrees on a FlexVol that contains volumes, the qtrees appear as directories. Therefore, you need to be careful to not delete the qtrees accidentally when deleting volumes.

You can specify the following options when creating a qtree:

- Name of the qtree
- Volume in which you want the qtree to reside
- Oplocks

  By default, oplocks are enabled for the qtree. If you disable oplocks for the entire storage system, oplocks are not set even if you enable oplocks for each qtree.

- Security style

  The security style can be UNIX, NTFS, or Mixed (UNIX and NTFS). By default, the security style of the qtree is the same as that of the selected volume.

- Export policy

  You can create a new export policy or select an existing policy. By default, the export policy of the qtree is same as that of the selected volume.

- Space usage limits for qtree and user quotas

Qtrees window

You can use the Qtrees window to create, display, and manage information about qtrees.

Command buttons

- **Create**

  Opens the Create Qtree dialog box, which enables you to create a new qtree.

- **Edit**

  Opens the Edit Qtree dialog box, which enables you to change the security style and to enable or disable oplocks (opportunistic locks) on a qtree.

- **Change Export Policy**

  Opens the Export Policy dialog box, which enables you to assign one or more qtrees to new or existing export policies.

- **Delete**

  Deletes the selected qtree.

  This button is disabled unless the status of the selected qtree is normal.

- **Refresh**

  Updates the information in the window.

Qtree list

The qtree list displays the volume in which the qtree resides and the qtree name.

- **Name**

  Displays the name of the qtree.

- **Volume**

  Displays the name of the volume in which the qtree resides.

- **Security Style**

  Specifies the security style of the qtree.

- **Status**

  Specifies the current status of the qtree.

- **Oplocks**

  Specifies whether the oplocks setting is enabled or disabled for the qtree.

- **Export Policy**

  Displays the name of the export policy to which the qtree is assigned.

Details area

- **Details tab**

  Displays detailed information about the selected qtree, such as the mount path of the volume containing the qtree, details about the export policy, and the export policy rules.

Related information

ONTAP concepts

Logical storage management

NFS management

SMB/CIFS management

Manage Quotas with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create, edit, and delete quotas.

Create quotas

Quotas enable you to restrict or track the disk space and number of files that are used by a user, group, or qtree. You can use the Add Quota wizard in System Manager to create a quota and to apply the quota to a specific volume or qtree.

About this task

Using System Manager, the minimum value that you can specify for the hard limit and soft limit on the number of files that the quota can own is 1000. If you want to specify a value lower than 1000, you should use the command-line interface (CLI).

Steps

1. Click **Storage** > **Quotas**.
2. From the drop-down menu in the **SVM** field, select the storage virtual machine (SVM) on which you want to create a quota.
3. In the **User Defined Quotas** tab, click **Create**.

   The Create Quota Wizard is displayed.
4. Type or select information as prompted by the wizard.
5. Confirm the details, and then click **Finish** to complete the wizard.

What to do next

You can use the local user name or RID to create user quotas. If you create the user quota or group quota by using the user name or group name, then the `/etc/passwd`file and the`/etc/group`file must be updated, respectively.

Delete quotas

You can use System Manager to delete one or more quotas when your users and their storage requirements and limitations change.

Steps

1. Click **Storage** > **Quotas**.
2. From the drop-down menu in the **SVM** field, select the storage virtual machine (SVM) on which the quotas that you want to delete reside.
3. Select one or more quotas that you want to delete, and then click **Delete**.
4. Select the confirmation check box, and then click **Delete**.

Edit quota limits

You can use System Manager to edit the disk space threshold, the hard limit and soft limit on the amount of disk space that the quota target can use, and the hard limit and soft limit on the number of files that the quota target can own.

Steps

1. Click **Storage** > **Quotas**.
2. From the drop-down menu in the **SVM** field, select the storage virtual machine (SVM) on which the quota that you want to edit resides.

3. Select the quota that you want to edit, and click **Edit Limits**.
4. In the **Edit Limits** dialog box, edit the quota settings as required.

   One hundred (100) is the minimum value that you can specify for the hard limit and soft limit on the number of files that the quota can own. If you want to specify a value lower than 100, you should use the command-line interface (CLI).

5. Click **Save and Close**.
6. Verify the changes that you made to the selected quota in the **User Defined Quotas** tab.

Activate or deactivate quotas

You can use System Manager to activate or deactivate quotas on one or more volumes that you select on your storage system. You can activate or deactivate quotas when you users and their storage requirements and limitations change.

Steps

1. Click **Storage** > **Quotas**.
2. From the drop-down menu in the SVM field, select the storage virtual machine (SVM) on which the quotas that you want to activate or deactivate reside.
3. In the **Quota Status on Volumes** tab, select one or more volumes for which you want to activate or deactivate quotas.
4. Click **Activate** or **Deactivate**, as required.
5. If you are deactivating a quota, select the confirmation check box, and then click **OK**.
6. Verify the quota status on the volumes in the **Status** column.

Resize quotas

You can use the Resize Quota dialog box in System Manager to adjust the active quotas in the specified volume so that they reflect the changes that you have made to a quota.

Before you begin

Quotas must be enabled for the volumes for which you want to resize quotas.

Steps

1. Click **Storage** > **Quotas**.
2. In the **Quota Status on Volumes** tab of the **Quotas** window, select one or more volumes for which you want to resize the quotas.
3. Click **Resize**.

View quota information

You can use the Quotas window in System Manager to view quota details such as the volume and qtrees to which the quota is applied, the type of quota, the user or group to which the quota is applied, and the space and file usage.

Steps

1. Click **Storage** > **Quotas**.
2. From the drop-down menu in the **SVM** field, select the storage virtual machine (SVM) on which the quota

that you want to view information about resides.

3. Perform the appropriate action:

If…	Then…
You want to view details of all of the quotas that you created	Click the **User Defined Quotas** tab.
You want to view details of the quotas that are currently active	Click the **Quota Report** tab.

4. Select the quota that you want to view information about from the displayed list of quotas.
5. Review the quota details.

Types of quotas

Quotas can be classified on the basis of the targets to which they are applied.

The following are the types of quotas based on the targets to which they are applied:

- **User quota**

  The target is a user.

  The user can be represented by a UNIX user name, UNIX UID, a Windows SID, a file or directory whose UID matches the user, Windows user name in pre-Windows 2000 format, and a file or directory with an ACL owned by the user's SID. You can apply it to a volume or a qtree.

- **Group quota**

  The target is a group.

  The group is represented by a UNIX group name, a GID, or a file or directory whose GID matches the group. ONTAP does not apply group quotas based on a Windows ID. You can apply a quota to a volume or a qtree.

- **Qtree quota**

  The target is a qtree, specified by the path name to the qtree.

  You can determine the size of the target qtree.

- **Default quota**

  Automatically applies a quota limit to a large set of quota targets without creating separate quotas for each target.

  Default quotas can be applied to all three types of quota target (users, groups, and qtrees). The quota type is determined by the value of the type field.

Quota limits

You can apply a disk space limit or limit the number of files for each quota type. If you do not specify a limit for a quota, none is applied.

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

Hard quotas impose a hard limit on system resources; any operation that would result in exceeding the limit fails. The following settings create hard quotas:

- Disk Limit parameter
- Files Limit parameter

Soft quotas send a warning message when resource usage reaches a certain level, but do not affect data access operations, so you can take appropriate action before the quota is exceeded. The following settings create soft quotas:

- Threshold for Disk Limit parameter
- Soft Disk Limit parameter
- Soft Files Limit parameter

Threshold and Soft Disk quotas enable administrators to receive more than one notification about a quota. Typically, administrators set the Threshold for Disk Limit to a value that is only slightly smaller than the Disk Limit, so that the threshold provides a "final warning" before writes start to fail.

- **Disk space hard limit**

  Disk space limit applied to hard quotas.

- **Disk space soft limit**

  Disk space limit applied to soft quotas.

- **Threshold limit**

  Disk space limit applied to threshold quotas.

- **Files hard limit**

  The maximum number of files on a hard quota.

- **Files soft limit**

  The maximum number of files on a soft quota.

Quota management

System Manager includes several features that help you to create, edit, or delete quotas. You can create a user, group, or tree quota and you can specify quota limits at the disk and file levels. All quotas are established on a per-volume basis.

After creating a quota, you can perform the following tasks:

- Enable and disable quotas
- Resize quotas

Quotas window

You can use the Quotas window to create, display, and manage information about quotas.

Tabs

- **User Defined Quotas**

  You can use the **User Defined Quotas** tab to view details of the quotas that you create and to create, edit, or delete quotas.

- **Quota Report**

  You can use the Quota Report tab to view the space and file usage and to edit the space and file limits of quotas that are active.

- **Quota Status on Volumes**

  You can use the Quota Status on Volumes tab to view the status of a quota and to turn quotas on or off and to resize quotas.

Command buttons

- **Create**

  Opens the Create Quota wizard, which enables you to create quotas.

- **Edit Limits**

  Opens the Edit Limits dialog box, which enables you to edit settings of the selected quota.

- **Delete**

  Deletes the selected quota from the quotas list.

- **Refresh**

  Updates the information in the window.

User Defined Quotas list

The quotas list displays the name and storage information for each quota.

- **Volume**

  Specifies the volume to which the quota is applied.

- **Qtree**

  Specifies the qtree associated with the quota. “All Qtrees” indicates that the quota is associated with all the qtrees.

- **Type**

  Specifies the quota type: user, or group, or tree.

- **User/Group**

  Specifies a user or a group associated with the quota. "All Users" indicates that the quota is associated with all the users. "All groups" indicates that the quota is associated with all the groups.

- **Quota Target**

  Specifies the type of target that the quota is assigned to. The target can be qtree, user, or group.

- **Space Hard Limit**

  Specifies the disk space limit applied to hard quotas.

  This field is hidden by default.

- **Space Soft Limit**

  Specifies the disk space limit applied to soft quotas.

  This field is hidden by default.

- **Threshold**

  Specifies the disk space limit applied to threshold quotas.

  This field is hidden by default.

- **File Hard Limit**

  Specifies the maximum number of files in a hard quota.

  This field is hidden by default.

- **File Soft Limit**

  Specifies the maximum number of files in a soft quota.

  This field is hidden by default.

Details area

The area below the quotas list displays quota details such as the quota error, space usage and limits, and file usage and limits.

Related information

Logical storage management

Configure the CIFS protocol with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to

enable and configure CIFS servers to allow CIFS clients to access files on the cluster.

Set up CIFS

You can use System Manager to enable and configure CIFS servers to allow CIFS clients to access the files on the cluster.

Before you begin

- The CIFS license must be installed on your storage system.
- While configuring CIFS in the Active Directory domain, the following requirements must be met:
  - DNS must be enabled and configured correctly.
  - The storage system must be able to communicate with the domain controller by using the fully qualified domain name (FQDN).
  - The time difference (clock skew) between the cluster and the domain controller must not be more than five minutes.
- If CIFS is the only protocol that is configured on the storage virtual machine (SVM), the following requirements must be met:
  - The root volume security style must be NTFS.

    By default, System Manager sets the security style as UNIX.
  - Superuser access must be set to `Any` for the CIFS protocol.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Configuration** tab, click **Set up**.
4. In the **General** tab of the **CIFS Server Setup** dialog box, specify the NetBIOS name and the Active Directory domain details.
5. Click the **Options** tab, and then perform the following actions:
   - In the SMB settings area, select or clear the SMB signing check box and the SMB encryption check box, as required.
   - Specify the default UNIX user.
   - In the WINS Servers area, add the required IP address.
6. Click **Set up**.

Edit the general properties for CIFS

You can modify the general properties for CIFS such as the default UNIX user and default Windows user by using System Manager. You can also enable or disable SMB signing for the CIFS server.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Configuration** tab, click **Options**.
4. In the **CIFS Options** dialog box, modify the following CIFS server properties, as required:

- UNIX user
- Windows user
- IP address
- Enable or disable SMB signing

  Enabling SMB signing prevents the data from being compromised. However, you might encounter performance degradation in the form of increased CPU usage on both the clients and the server, although the network traffic remains the same. You can disable SMB signing on any of your Windows clients that do not require protection against replay attacks.

  For information about disabling SMB signing on Windows clients, see the Microsoft Windows documentation.

- Enable or disable SMB 3.0 encryption

  You should enable SMB Multichannel to establish multiple channels between an SMB 3.0 session and transport connections.

5. Click either **Save** or **Save and Close**.

Related information

Creating a CIFS share

CIFS window

Editing volume properties

Modifying export policy rules

SMB/CIFS management

Manage home directory paths - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to specify one or more paths that can be used by the storage system to resolve the location of the CIFS home directories of users.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Home Directories** area of the **Configuration** tab, click **Manage**.
4. In the **Manage Home Directories** dialog box, specify the paths that are to be used by the storage system to search for the CIFS home directories of users.
5. Click **Add**, and then click **Save and Close**.

Delete home directory paths

You can use System Manager to delete a home directory path when you do not want the storage system to use the path to resolve the location of the CIFS home directories of users.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Home Directories** area of the **Configuration** tab, click **Manage**.
4. In the **Manage Home Directories** dialog box, select the home directory path that you want to delete, and then click **Delete**.
5. Click **Save and Close**.

Related information

Reset CIFS domain controllers with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to reset the CIFS connection to domain controllers for the specified domain. Failure to reset the domain controller information can cause a connection failure.

About this task

You have to update the discovery information of the storage system's available domain controller after you add or delete a domain from the list of preferred domain controllers. You can update the storage system's available domain controller discovery information in ONTAP through the command-line interface (CLI).

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Domain** tab, click **Reset**.

Related information

CIFS window

Manage the CIFS group policy configuration with System Manager - ONTAP 9.7 and earlier

You can use the CIFS window in ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to update and manage the group policy.

Update the CIFS group policy configuration

You have to update the group policy after the policy configuration is changed through the command-line interface (CLI).

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. Click the **Domain** tab.
4. In the **Group Policy** area, select the group policy configuration that you want to update, and then click **Update**.

Enable or disable a CIFS group policy configuration

You can enable or disable the CIFS group policy configuration from the CIFS window in System Manager.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. Click the **Domain** tab.
4. In the **Group Policy** area, select the group policy configuration that you want to enable or disable, and then click **Enable** or **Disable**, as required.

Reload CIFS group policy

You have to reload a CIFS group policy if the status of the policy is changed. You can use the CIFS window in System Manager to reload the group policy.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. Click the **Domain** tab.
4. In the **Group Policy** area, select the group policy configuration that you want to reload, and then click **Reload**.

Configure BranchCache with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to configure BranchCache on a CIFS-enabled storage virtual machine (SVM) to enable the caching of content on computers that are local to the requesting clients.

Before you begin

- CIFS must be licensed, and a CIFS server must be configured.
- For BranchCache version 1, SMB 2.1 or later must be enabled.
- For BranchCache version 2, SMB 3.0 must be enabled, and the remote Windows clients must support BranchCache 2.

About this task

- You can configure BranchCache on SVMs.
- You can create an all-shares BranchCache configuration if you want to offer caching services for all of the content that is contained within all of the SMB shares on the CIFS server.
- You can create a per-share BranchCache configuration if you want to offer caching services for the content that is contained within selected SMB shares on the CIFS server.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **BranchCache** tab, click **Set Up**.
4. In the **BranchCache Setup** dialog box, enter the following information:

a. Specify the path to the hash store.

   The path can be to an existing directory where you want the hash data to be stored. The destination path must be read-writable. Read-only paths such as Snapshot directories are not allowed.

b. Specify the maximum size (in KB, MB, GB, TB, or PB) for a hash data store.

   If the hash data exceeds this value, older hashes are deleted to provide space for newer hashes. The default size for a hash store is 1 GB.

c. Specify the operating mode for the BranchCache configuration.

   The default operating mode is set to all shares.

d. Specify a server key to prevent clients from impersonating the BranchCache server.

   You can set the server key to a specific value so that if multiple servers are providing BranchCache data for the same files, clients can use hashes from any server using that same server key. If the server key contains any spaces, you must enclose the server key in quotation marks.

e. Select the required BranchCache version.

   By default, all of the versions that are supported by the client are selected.

5. Click **Set Up**.

Modify the BranchCache settings

You can use the CIFS window in System Manager to modify the BranchCache settings that are configured for a CIFS-enabled storage virtual machine (SVM). You can change the hash store path, the hash store size, the operating mode, and the BranchCache versions that are supported.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **BranchCache** tab, click **Edit**.
4. In the **Modify BranchCache Settings** dialog box, modify the required information:
   - Hash store path

     If you modify the hash store path, you are provided with an option to retain the cached hash data from the previous hash store.

   - Hash store size
   - Operating mode
   - BranchCache version
5. Click **Modify**.

Delete the BranchCache configuration

You can use System Manager to delete the BranchCache configuration if you no longer want to offer caching services on the storage virtual machine (SVM) that is configured for BranchCache.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **BranchCache** tab, click **Delete**.
4. Select the confirmation check box, and then click **Delete**.

   You can also remove existing hashes from the hash store.

Manage preferred domain controllers with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage preferred domain controllers.

Add preferred domain controllers

System Manager automatically discovers domain controllers through DNS. Optionally, you can add one or more domain controllers to the list of preferred domain controllers for a specific domain.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Domain** tab, click **Add** in the **Preferred Domain Controllers** area.
4. Enter the fully qualified domain name (FQDN) and the IP addresses of the domain controllers that you want to add.

   You can add multiple domain controllers by entering the IP addresses of the domain controllers, separated by commas.

5. Click **Save**.
6. Verify that the domain controller that you added is displayed in the list of preferred domain controllers.

Edit preferred domain controllers

You can use System Manager to modify the IP address of the preferred domain controllers that are configured for a specific domain.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Preferred Domain Controllers** area of the **Domain** tab, double-click the domain controller that you want to edit.
4. Modify the IP addresses of the domain controller, and then click **Save**.

Delete preferred domain controllers

You can use System Manager to delete a preferred domain controller to which the storage virtual machine (SVM) computer account is associated. You can do this when you no longer want to use a particular domain controller.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Domain** tab, select the domain that you want to delete from the **Preferred Domain Controllers** area, and then click **Delete**.
4. Select the confirmation check box, and then click **Delete**.

View CIFS domain information with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to view information about the domain controllers and servers that are connected to the storage system.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. Click the **Domain** tab.
4. Review the information about the connected domain controllers and servers.

CIFS window in System Manager - ONTAP 9.7 and earlier

You can use the CIFS window in ONTAP System Manager (available in ONTAP 9.7 and earlier) to configure the CIFS server, to manage domain controllers, to manage symbolic UNIX mappings, and to configure BranchCache.

Configuration tab

The Configuration tab enables you to create and manage the CIFS server.

- **Server**

  Specifies the status of the CIFS server, name of the server, authentication mode, name of the active directory domain, and status of SMB multichannel.

- **Home Directories**

  Specifies home directory paths and the style for determining how PC user names are mapped to home directory entries.

- **Command buttons**
  - Setup

    Opens the CIFS Setup wizard, which enables you to set up CIFS on your storage virtual machine (SVM).

  - Options

    Displays the CIFS Options dialog box, which enables you to enable or disable SMB 3.0 signing, to enable or disable SMB 3.0 encryption, and to add Windows Internet Name Service (WINS) servers.

SMB signing prevents the network traffic between the CIFS server and the client from being compromised.

- Delete

  Enables you to delete the CIFS server.

- Refresh

  Updates the information in the window.

Domain tab

The Domain tab enables you to view and reset your CIFS domain controllers, and to add or delete preferred domain controllers. You can also use this tab to manage CIFS group policy configurations.

- **Servers**

  Displays information about discovered authentication servers and your preferred domain controllers on the CIFS-enabled SVM.

  You can also reset the information about the discovered servers, add a preferred domain controller, delete a domain controller, or refresh the list of domain controllers.

- **Group Policy**

  Enables you to view, enable, or disable group policy configurations on the CIFS server. You can also reload a group policy if the status of the policy is changed.

Symlinks tab

The Symlinks tab enables you to manage the mappings of UNIX symbolic links for CIFS users.

- **Path Mappings**

  Displays the list of symbolic link mappings for CIFS.

- **Command buttons**
  - Create

    Opens the Create New Symlink Path Mappings dialog box, which enables you to create a UNIX symbolic link mapping.

  - Edit

    Opens the Edit Symlink Path Mappings dialog box, which enables you to modify the CIFS share and path.

  - Delete

    Enables you to delete the symbolic link mapping.

  - Refresh

    Updates the information in the window.

BranchCache tab

The BranchCache tab enables you to set up and manage BranchCache settings on CIFS-enabled SVMs.

You can view the status of the BranchCache service, the path to the hash store, the size of the hash store, and the operating mode, server key, and version of BranchCache.

- **Command buttons**
  - Setup

    Opens the BranchCache Setup dialog box, which enables you to configure BranchCache for the CIFS server.

  - Edit

    Opens the Modify BranchCache Settings dialog box, which enables you to modify the properties of the BranchCache configuration.

  - Delete

    Enables you to delete the BranchCache configuration.

  - Refresh

    Updates the information in the window.

Related information

Setting up CIFS

Editing the general properties for CIFS

Adding home directory paths

Deleting home directory paths

Resetting CIFS domain controllers

Configure the NFS protocol with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to authenticate NFS clients to access data on the SVM.

Edit NFS settings

You can use System Manager to edit the NFS settings such as enabling or disabling NFSv3, NFSv4, and NFSv4.1, enabling or disabling read and write delegations for NFSv4 clients, and enabling NFSv4 ACLs. You can also edit the default Windows user.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **NFS**.

4. In the **NFS** window, click **Edit**.
5. In the **Edit NFS Settings** dialog box, make the required changes.
6. Click **Save and Close**.

NFS window

You can use the NFS window to display and configure your NFS settings.

- **Server Status**

  Displays the status of the NFS service. The service is enabled if the NFS protocol is configured on the storage virtual machine (SVM).

  If you have upgraded to ONTAP 8.3 or later from an NFS-enabled storage system running Data ONTAP 8.1.x, the NFS service is enabled in ONTAP 8.3 or later. However, you must enable support for NFSv3 or NFSv4 because NFSv2 is no longer supported.

Command buttons

- **Enable**

  Enables the NFS service.

- **Disable**

  Disables the NFS service.

- **Edit**

  Opens the Edit NFS Settings dialog box, which enables you to edit NFS settings.

- **Refresh**

  Updates the information in the window.

Related information

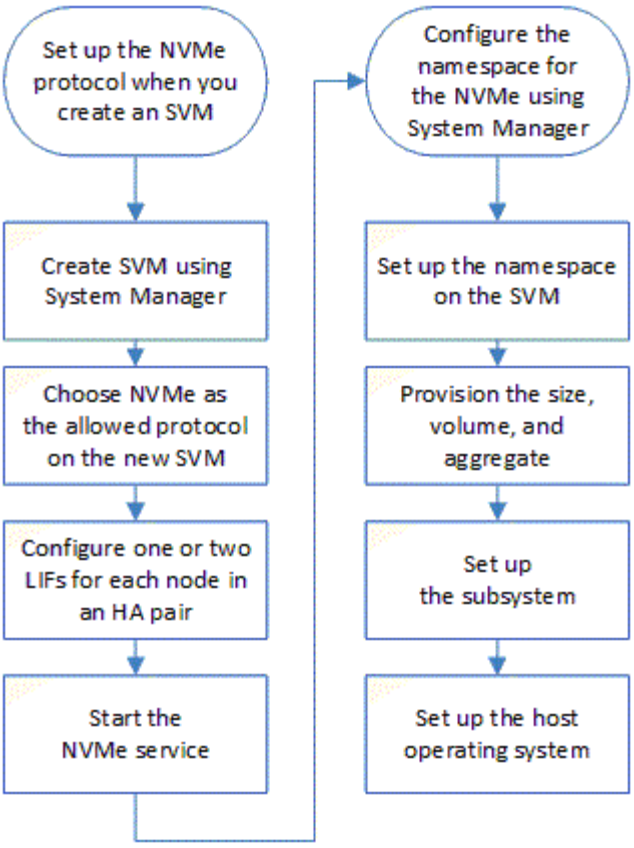
NFS management

Set up NVMe with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to set up the NVMe protocol for an SVM. When the NVMe protocol is enabled on the SVM, you can then provision a namespace or namespaces and assign them to a host and a subsystem.

Beginning with ONTAP 9.5, you must configure at least one NVMe LIF for each node in an HA pair that uses the NVMe protocol. You can also define a maximum of two NVMe LIFs per node. You configure the NVMe LIFs when you create or edit the SVM settings using System Manager.

The following illustration shows the workflow for setting up NVMe:



Create an NVMe namespace with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create one or more NVMe namespaces and connect each to a host or set of hosts in a storage virtual machine (SVM). The NVMe namespace is a quantity of memory that can be formatted into logical blocks. Each namespace can be mapped to an NVMe subsystem.

Before you begin

The SVM must already be configured with the NVMe protocol. To map a namespace, at least one LIF with the data protocol NVMe must exist in the node that owns the namespace.

Steps

1. Click **Storage** > **NVMe** > **NVMe namespaces**.
2. Select the SVM that will contain the namespace.
3. Ensure that at least one NVMe LIF is configured for each node of the HA pair. You can create a maximum of two NVMe LIFs per node.
4. Configure the size of the namespace (between 1MB and 16TB).
5. Enter the block size.

   For System Manager 9.5, the block size defaults to 4 KB, and this field is not shown.

   For System Manager 9.6, you can specify a block size of 4 KB or 512 Bytes.

6. Select the existing volume or create a new volume by choosing the aggregate.

Click on the + symbol to set up additional namespaces (max 250) within the SVM.

7. Select the NVMe subsystem that will be associated with this namespace.

   You can choose from the following options:

   - None: No subsystems are mapped.
   - Use an existing subsystem: The subsystems listed are based on the selected SVM.
   - Create a new subsystem: You can choose to create a new subsystem and map to all the new namespaces.

8. Select the host operating system.
9. Click **Submit**.

Related information

NVMe namespaces window

Edit an NVMe namespace with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager Classic (available in ONTAP 9.7 and earlier) to edit the namespace by changing the subsystem that the namespace is mapped to.

About this task

You can only modify the NVMe subsystem settings in this window; you cannot edit the other namespace details.

Steps

1. Click **NVMe** > **NVMe namespaces**.
2. In the **NVMe namespaces window**, select the namespace you want to edit.
3. Select a subsystem option:
   - None: Choosing this option unmaps the existing subsystem mapping for this namespace only. This option is preselected if no subsystem mapping is present for the selected namespace.
   - Use an existing subsystem: This option is preselected if subsystem-to-namespace mapping is present. Choosing a different subsystem maps the new subsystem by unmapping the previously mapped subsystem.

Clone an NVMe namespace with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to quickly create another namespace of the same configuration by choosing to clone a namespace. You can map the newly cloned namespace to another host NQN.

Before you begin

You must have a FlexClone license to clone a namespace.

About this task

You can clone a namespace with the selected host mapping and associate it with another subsystem.

Steps

1. Click **NVMe** > **NVMe namespaces**.
2. In the **NVMe namespaces window**, select the namespace you want to clone.
3. You can rename the cloned namespace if you need a specific name but it is not required.

   The dialog provides a default name of the namespace to-be-cloned.

4. Modify the subsystem mapping for the cloned namespace.
5. Click **OK**.

   The online, mapped namespace is cloned inside the same SVM with a different name. Host mapping will not be cloned.

Start and stop the NVMe service with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to start the NVMe service to bring the adapters online. The NVMe service enables you to manage NVMe adapters for use with namespaces. You can stop the NVMe service to take the NVMe adapters offline and to disable access to the namespaces.

Before you begin

NVMe capable adapters must be present before you start the NVMe service.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM settings**.
3. In the **Protocols** menu, click **NVMe**.
4. Click **Start** or **Stop** service as required.

Manage NVMe subsystems with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create and manage an NVMe subsystem. You can associate the NVMe subsystem with different hosts and namespaces within the vserver. Also, each vserver can support more than one NVMe subsystem. However, you cannot configure a NVMe subsystem to be used on multiple vservers.

Create NVMe subsystems

You can use System Manager to create an NVMe subsystem.

Steps

1. Click **Create** in the **NVMe Subsystems** window.
2. Provide entries in the **NVMe Subsystems: Create** window for the following fields:
   - **SVM**

     From the drop-down menu, select the SVM on which you want to create the subsystem.

   - **Name**

Enter a name for the subsystem. The subsystem name cannot already exist in the SVM. The name is case-sensitive and is limited to 96 characters. Special characters are allowed.

- **Host OS**

  From the drop-down menu, select the type of Host OS of the subsystem.

- **Host NQN**

  Enter the Host NQN attached to the controller. You can enter more than one Host NQN by separating them with commas.

3. Click **Save**.

   The NVMe subsystem is created, and the NVMe Subsystemswindow is displayed.

Edit NVMe subsystems details

You can use System Manager to edit the details of an NVMe subsystem.

Steps

1. Find the NVMe subsystem you want to edit in the **NVMe Subsystem** window.
2. Check the box to the left of the name of the subsystem you want to edit.
3. Click **Edit**.

   The current details of the NVMe subsystem are displayed in the NVMe Subsystems: Editwindow.

4. You can modify only the information in the **Host NQN** field.

   - **Host NQN**

     Modify the Host NQN attached to the controller. You can enter more than one Host NQN by separating them with commas.

   The **Associated NVMe Namespaces** table displays below the Host NQN field. For each namespace, that table lists the namespace path and namespace ID.

5. Click **Save**.

   The NVMe subsystem details are updated, and the NVMe Subsystems window is displayed.

Delete an NVMe subsystem

You can use System Manager to delete an NVMe subsystem from a cluster.

About this task

The following actions occur when you delete an NVMe subsystem:

- If the NVMe subsystem has configured hosts, then mapped hosts will be removed.
- If the NVMe subsystem has mapped namespaces, then they will be unmapped.

Steps

1. Find the NVMe subsystem you want to delete on the **NVMe Subsystem** window.
2. Check the box to the left of the name of the subsystem you want to delete.
3. Click **Delete**.

   A Warning message is displayed.

4. Click the **Delete the NVMe Subsystem** check box to confirm the deletion, then click **Yes**.

   The NVMe subsystem is deleted from the cluster, and the NVMe Subsystems window is displayed.

NVMe Subsystems window

The NVMe Subsystems window displays by default an inventory list of NVMe subsystems in a cluster. You can filter the list to display only subsystems that are specific to an SVM. The window also enables you to create, edit, or delete NVMe subsystems. You can access this window by selecting **Storage** > **NVMe** > **Subsystems**.

- NVMe Subsystems table
- Toolbar

NVMe Subsystems table

The NVMe Subsystems table lists the inventory of NVMe subsystems in a cluster. You can refine the list by using the drop-down menu in the **SVM** field to select an SVM to display only the NVMe subsystems associated with that SVM. The **Search** field and **Filtering** drop-down menu enable you to further customize the list.

The NVMe Subsystems table contains the following columns:

- **(check box)**

  Enables you to specify on which subsystems you want to perform actions.

  Click the check box to select the subsystem, then click the action in the toolbar that you want to perform.

- **Name**

  Displays the name of the subsystem.

  You can search for a subsystem by entering its name in the **Search** field.

- **Host OS**

  Displays the name of the host OS associated with the subsystem.

- **Host NQN**

  Displays the NVMe Qualified Name (NQN) attached to the controller. If multiple NQNs are displayed, they are separated by commas.

- **Associated NVMe Namespaces**

  Displays the number of the NVM namespaces associated with the subsystem. You can hover over the number to display the associated namespaces paths. Click on a path to display the Namespace Details window.

Toolbar

The toolbar is located above the column header. You can use the fields and buttons in the toolbar to perform various actions.

- **Search**

  Enables you to search on values that might be found in the **Name** column.

- **Filtering**

  Allows you to select from a drop-down menu that lists various methods of filtering the list.

- **Create**

  Opens the Create NVMe Subsystem dialog box, which enables you to create an NVMe subsystem.

- **Edit**

  Opens the Edit NVMe Subsystem dialog box, which enables you to edit an existing NVMe subsystem.

- **Delete**

  Opens the Delete NVMe Subsystem confirmation dialog box, which enables you to delete an existing NVMe subsystem.

Configure the iSCSI protocol with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to configure the iSCSI protocol that enables you to transfer block data to hosts using SCSI protocol over TCP/IP.

Create iSCSI aliases

An iSCSI alias is a user-friendly identifier that you assign to an iSCSI target device (in this case, the storage system) to make it easier to identify the target device in user interfaces. You can use System Manager to create an iSCSI alias.

About this task

An iSCSI alias is a string of 1 to 128 printable characters.An iSCSI alias must not include spaces.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. In the **Service** tab of the **iSCSI** window, click **Edit**.
5. In the **Edit iSCSI Service Configuration** dialog box, enter an iSCSI alias in the **Target Alias** field, and then click **OK**.

Enable or disable the iSCSI service on storage system interfaces

You can use System Manager to control which network interfaces are used for iSCSI communication by enabling or disabling the interfaces. When the iSCSI service is enabled, iSCSI connections and requests are accepted over those network interfaces that are enabled for iSCSI, but not over disabled interfaces.

Before you begin

You must have terminated any outstanding iSCSI connections and sessions that are currently using the interface. By default, the iSCSI service is enabled on all of the Ethernet interfaces after you enable the iSCSI license.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. In the **iSCSI Interfaces** area, select the interface on which you want to enable or disable the iSCSI service.
5. Click **Enable** or **Disable**, as required.

Add the security method for iSCSI initiators

You can use System Manager to add an initiator and to specify the security method that is used to authenticate the initiator.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. In the **iSCSI** window, click the **Initiator Security** tab.
5. Click **Add** in the **Initiator Security** area.
6. Specify the initiator name and the security method for authenticating the initiator.

   For CHAP authentication, you must provide the user name and password, and then confirm your password for inbound settings. For outbound settings, this login information is optional.

7. Click **OK**.

Edit default security settings

You can use the Edit Default Security dialog box in System Manager to edit the default security settings for the iSCSI initiators that are connected to the storage system.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. In the **Default Security** area of the **Initiator Security** tab, click **Edit**.
5. In the **Edit Default Security** dialog box, change the security type.

For CHAP authentication, you must provide the user name and password, and then confirm your password for inbound settings. For outbound settings, this login information is optional.

6. Click **OK**.

Change the default iSCSI initiator authentication method

You can use System Manager to change the default iSCSI authentication method, which is the authentication method that is used for any initiator that is not configured with a specific authentication method.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. In the **Initiator Security** tab, click **Edit** in the **Default Security** area.
5. Change the security type.

   For CHAP authentication, you must provide the user name and password, and then confirm your password for inbound settings. For outbound settings, this login information is optional.

6. Click **OK**.

Set the default security for iSCSI initiators

You can use System Manager to remove the authentication settings for an initiator and to use the default security method to authenticate the initiator.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. In the **Initiator Security** tab, select the initiator for which you want to change the security setting.
5. Click **Set Default** in the **Initiator Security** area, and then click **Set Default** in the confirmation dialog box.

Start or stop the iSCSI service

You can use System Manager to start or stop the iSCSI service on your storage system.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. Click **Start** or **Stop**, as required.

View initiator security information

You can use System Manager to view the default authentication information and all the initiator-specific authentication information.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **iSCSI**.
4. In the **Initiator Security** tab of the **iSCSI** window, review the details.

iSCSI window

You can use the iSCSI window to start or stop the iSCSI service, change a storage system iSCSI node name, and create or change the iSCSI alias of a storage system. You can also add or change the initiator security setting for an iSCSI initiator that is connected to your storage system.

Tabs

- **Service**

  You can use the **Service** tab to start or stop the iSCSI service, change a storage system iSCSI node name, and create or change the iSCSI alias of a storage system.

- **Initiator Security**

  You can use the **Initiator Security** tab to add or change the initiator security setting for an iSCSI initiator that is connected to your storage system.

Command buttons

- **Edit**

  Opens Edit iSCSI Service Configurations dialog box, which enables you to change iSCSI node name and iSCSI alias of the storage system.

- **Start**

  Starts the iSCSI service.

- **Stop**

  Stops the iSCSI service.

- **Refresh**

  Updates the information in the window.

Details area

The details area displays information about the status of the iSCSI service, iSCSI target node name, and iSCSI target alias. You can use this area to enable or disable the iSCSI service on a network interface.

Related information

SAN administration

Configure the FC/FCoE protocol with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to configure FC/FCoE protocols.

Start or stop the FC or FCoE service

The FC service enables you to manage FC target adapters for use with LUNs. You can use System Manager to start the FC service to bring the adapters online and to enable access to the LUNs on the storage system. You can stop the FC service to take the FC adapters offline and to disable access to the LUNs.

Before you begin

- The FC license must be installed.
- An FC adapter must be present in the target storage system.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **FC/FCoE**.
4. Click **Start** or **Stop**, as required.

Change an FC or FCoE node name

If you replace a storage system chassis and reuse it in the same Fibre Channel SAN, the node name of the replaced storage system might be duplicated in certain cases. You can change the node name of the storage system by using System Manager.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Protocols** pane, click **FC/FCoE**.
4. Click **Edit**.
5. Type the new name, and then click **OK**.

The FCoE protocol

Fibre Channel over Ethernet (FCoE) is a new model for connecting hosts to storage systems. Like the traditional FC protocol, FCoE maintains existing FC management and controls, but it uses a 10-gigabit Ethernet network as the hardware transport.

Setting up an FCoE connection requires one or more supported converged network adapters (CNAs) in the host, connected to a supported data center bridging (DCB) Ethernet switch. The CNA is a consolidation point and effectively serves as both an HBA and an Ethernet adapter.

In general, you can configure and use FCoE connections the same way you use traditional FC connections.

FC/FCoE window

You can use the FC/FCoE window to start or stop the FC service.

Command buttons

- **Edit**

  Opens the Edit Node Name dialog box, which enables you to change the FC or FCoE node name.

- **Start**

  Starts the FC/FCoE service.

- **Stop**

  Stops the FC/FCoE service.

- **Refresh**

  Updates the information in the window.

FC/FCoE details

The details area displays information about the status of FC/FCoE service, the node name, and the FC/FCoE adapters.

Related information

Configuring FC protocol and FCoE protocol on SVMs

SAN administration

Manage export policies with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create, edit, and manage export policies.

Create an export policy

You can use System Manager to create an export policy so that clients can access specific volumes.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Export Policies**.
4. Click **Create**.
5. In the **Create Export Policy** dialog box, specify a name for the export policy.
6. If you want to create an export policy by copying the rules from an existing export policy, select the **Copy Rules from** check box, and then select the storage virtual machine (SVM) and the export policy.

   You should not select the destination SVM for disaster recovery from the drop-down menu to create an export policy.

7. In the **Export Rules**area, click **Add** to add rules to the export policy.

8. Click **Create**.
9. Verify that the export policy that you created is displayed in the **Export Policies** window.

Rename export policies

You can use System Managerto rename an existing export policy.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Export Policies**.
4. Select the export policy that you want to rename, and then click **Rename Policy**.
5. In the **Rename Policy** dialog box, specify a new policy name, and then click **Modify**.
6. Verify the changes that you made in the **Export Policies** window.

Delete export policies

You can use System Manager to delete export policies that are no longer required.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Export Policies**.
4. Select the export policy that you want to delete, and then click **Delete Policy**.
5. Select the confirmation check box, and then click **Delete**.

Add rules to an export policy

You can use System Manager to add rules to an export policy, which enables you to define client access to data.

Before you begin

You must have created the export policy to which you want to add the export rules.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Export Policies**.
4. Select the export policy to which you want to add rules, and from the **Export Rules** tab, click **Add**.
5. In the **Create Export Rule** dialog box, perform the following steps:
   a. Specify the client that requires access to the data.

      You can specify multiple clients as comma-separated values.

      You can specify the client in any of the following formats:

      - As a host name; for instance, host1

- As an IPv4 address; for instance, 10.1.12.24
- As an IPv4 address with a network mask; for instance, 10.1.16.0/255.255.255.0
- As an IPv6 address; for instance, FE80::0202:B3FF:FE1E:8329
- As an IPv6 address with a network mask; for instance, 2001:db8::/32
- As a netgroup, with the netgroup name preceded by an at symbol (@); for instance, @netgroup
- As a domain name preceded by a period (.); for instance, .example.com

> You must not enter an IP address range, such as 10.1.12.10 through 10.1.12.70. Entries in this format are interpreted as a text string and are treated as a host name.

You can enter the IPv4 address `0.0.0.0/0` to provide access to all of the hosts.

b. If you want to modify the rule index number, select the appropriate rule index number.
c. Select one or more access protocols.

   If you do not select any access protocol, the default value “Any” is assigned to the export rule.

d. Select one or more security types and access rules.

6. Click **OK**.
7. Verify that the export rule that you added is displayed in the **Export Rules** tab for the selected export policy.

Modify export policy rules

You can use System Manager to modify the specified client, access protocols, and access permissions of an export policy rule.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Export Policies**.
4. In the **Export Policies** window, select the export policy for which you want to edit the export rule, and in the **Export Rules** tab, select the rule that you want to edit, and then click **Edit**.
5. Modify the following parameters as required:
   - Client specification
   - Access protocols
   - Access details
6. Click **OK**.
7. Verify that the updated changes for the export rule are displayed in the **Export Rules** tab.

Delete export policy rules

You can use System Manager to delete export policy rules that are no longer required.

Steps

1. Click **Storage** > **SVMs**.

2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Export Policies**.
4. Select the export policy for which you want to delete the export rule.
5. In the **Export Rules** tab, select the export rule that you want to delete, and then click **Delete**.
6. In the confirmation box, click **Delete**.

How export policies control client access to volumes or qtrees

Export policies contain one or more *export rules* that process each client access request. The result of the process determines whether the client is denied or granted access and what level of access. An export policy with export rules must exist on the storage virtual machine (SVM) for clients to access data.

You associate exactly one export policy with each volume or qtree to configure client access to the volume or qtree. The SVM can contain multiple export policies. This enables you to do the following for SVMs with multiple volumes or qtrees:

- Assign different export policies to each volume or qtree of the SVM for individual client access control to each volume or qtree in the SVM.
- Assign the same export policy to multiple volumes or qtrees of the SVM for identical client access control without having to create a new export policy for each volume or qtree.

If a client makes an access request that is not permitted by the applicable export policy, the request fails with a permission-denied message. If a client does not match any rule in the export policy, then access is denied. If an export policy is empty, then all accesses are implicitly denied.

You can modify an export policy dynamically on a system running ONTAP.

Export Policies window

You can use the Export Policies window to create, view, and manage information about export policies and its related export rules.

Export Policies

The Export Policies window enables you to view and manage the export policies created for the storage virtual machine (SVM).

- **Command buttons**
  - Create

    Opens the Create Export Policy dialog box, which enables you to create an export policy and add export rules. You can also copy export rules from an existing SVM.

  - Rename

    Opens the Rename Policy dialog box, which enables you to rename the selected export policy.

  - Delete

    Opens the Delete Export Policy dialog box, which enables you to delete the selected export policy.

  - Refresh

Updates the information in the window.

Export Rules tab

The Export Rules tab enables you to view information about the export rules created for a particular export policy. You can also add, edit, and delete rules.

- **Command buttons**
  - Add

    Opens the Create Export Rule dialog box, which enables you to add an export rule to the selected export policy.

  - Edit

    Opens the Modify Export Rule dialog box, which enables you to modify the attributes of the selected export rule.

  - Delete

    Opens the Delete Export Rule dialog box, which enables you to delete the selected export rule.

  - Move Up

    Moves up the rule index of the selected export rule.

  - Move Down

    Moves down the rule index of the selected export rule.

  - Refresh

    Updates the information in the window.

- **Export rules list**
  - Rule Index

    Specifies the priority based on which the export rules are processed. You can use the Move Up and Move Down buttons to choose the priority.

  - Client

    Specifies the client to which the rule applies.

  - Access Protocols

    Displays the access protocol that is specified for the export rule.

    If you have not specified any access protocol, the default value “Any” is considered.

  - Read-Only Rule

    Specifies one or more security types for read-only access.

- Read/Write Rule

  Specifies one or more security types for read/write access.

- Superuser Access

  Specifies the security type or types for superuser access.

Assigned Objects tab

The Assigned Objects tab enables you to view the volumes and qtrees that are assigned to the selected export policy. You can also view whether the volume is encrypted or not.

Related information

Setting up CIFS

Manage efficiency policies with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create, edit, and delete efficiency policies.

Add efficiency policies

You can use System Manager to add efficiency policies for running the deduplication operation on a volume on a specified schedule or when the change in volume data reaches a specified threshold value.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Efficiency Policies**.
4. Click **Add**, and then specify the policy name.
5. Specify how the storage efficiency policy should be run:
   - Select **Schedule**, and specify the schedule name and the schedule details.

     You can specify the maximum run-time duration of the efficiency policy, if required.

   - Select **ChangeLog Threshold**, and specify the threshold value (in percent) for the change in volume data.
6. **Optional:** Select the **Set QoS policy to background** check box to reduce performance impact on client operations.
7. Click **Add**.

Edit efficiency policies

You can use System Manager to modify the attributes of an efficiency policy such as the policy name, schedule name, and maximum runtime.

Steps

1. Click **Storage** > **SVMs**.

2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Efficiency Policies**.
4. In the **Efficiency Policies** window, select the policy that you want to edit, and then click **Edit**.
5. In the **Edit Efficiency Policy** dialog box, make the required changes.
6. Click **Save**.

Delete efficiency policies

You can use System Managerto delete an efficiency policy that is no longer required.

Before you begin

The efficiency policy must be disabled.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Efficiency Policies**.
4. Select the efficiency policy that you want to delete, and then click **Delete**.
5. Select the confirmation check box, and then click **Delete**.

Enable or disable efficiency policies

You can use System Manager to enable or disable an efficiency policy.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **Efficiency Policies**.
4. Select one or more efficiency policies that you want to enable or disable.
5. Click **Status** > **Enable** or **Status** > **Disable**, as required.
6. If you are disabling an efficiency policy, select the confirmation check box, and then click **OK**.

What an efficiency policy is

An efficiency policy is a job schedule for a deduplication operation on a FlexVol volume.

You can run deduplication on a FlexVol volume either by scheduling the operations to start at a specific time or by specifying that the operations are triggered if a threshold percentage is exceeded. You can schedule a deduplication operation by creating job schedules that are enclosed within the efficiency policies. The volume efficiency policies support only job schedules that are of type cron. Alternately, you can specify a threshold percentage. When new data exceeds the specified percentage, the deduplication operation is started.

Understanding predefined efficiency policies

You can configure a volume with efficiency policies to achieve additional space savings. You can configure a volume to run inline compression without a scheduled or manually started background efficiency operation configured on the volume.

When you create an SVM, the following efficiency policies are created automatically and cannot be deleted:

- Default

  You can configure a volume with the efficiency policy to run the scheduled deduplication operations on the volume.

- Inline-only

  You can configure a volume with the inline-only efficiency policy and enable inline compression, to run inline compression on the volume without any scheduled or manually started background efficiency operations.

For more information about the inline-only and default efficiency policies, see the man pages.

Efficiency Policies window

You can use the Efficiency Policies window to create, display, and manage information about efficiency policies.

Command buttons

- **Add**

  Opens the Add Efficiency Policy dialog box, which enables you to run a deduplication operation on a volume for a specified duration (schedule-based) or when the change in volume data reaches a specified threshold value (threshold-based).

- **Edit**

  Opens the Edit Efficiency Policy dialog box, which enables you to modify the schedule, threshold value, QoS type, and maximum run time for a deduplication operation.

- **Delete**

  Opens the Delete Efficiency Policy dialog box, which enables you to delete the selected efficiency policy.

- **Status**

  Open a drop-down menu, which provides options to enable or disable the selected efficiency policy.

- **Refresh**

  Updates the information in the window.

Efficiency policies list

- **Auto**

  Specifies that deduplication is continuously performed in the background. This policy is set for all newly created volumes and for all upgraded volumes that have not been manually configured for background deduplication. If you change the policy to “default” or any other policy, the “auto” policy is disabled.

  If a volume moves from a non-AFF system to an AFF system, the “auto” policy is enabled on the destination node by default. If a volume moves from an AFF node to a non-AFF node, the “auto” policy on

the destination node is replaced by the “inline-only” policy by default.

- **Policy**

  Specifies the name of an efficiency policy.

- **Status**

  Specifies the status of an efficiency policy. The status can be one of the following:

  - Enabled

    Specifies that the efficiency policy can be assigned to a deduplication operation.

  - Disabled

    Specifies that the efficiency policy is disabled. You can enable the policy by using the status drop-down menu and assign it later to a deduplication operation.

- **Run By**

  Specifies whether the storage efficiency policy is run based on a schedule or based on a threshold value (change log threshold).

- **QoS Policy**

  Specifies the QoS type for the storage efficiency policy. The QoS type can be one of the following:

  - Background

    Specifies that the QoS policy is running in the background, which reduces potential performance impact on the client operations.

  - Best-effort

    Specifies that the QoS policy is running on a best-effort basis, which enables you to maximize the utilization of system resources.

- **Maximum Runtime**

  Specifies the maximum run-time duration of an efficiency policy. If this value is not specified, the efficiency policy is run till the operation is complete.

Details area

The area below the efficiency policy list displays additional information about the selected efficiency policy, including the schedule name and the schedule details for a schedule-based policy, and the threshold value for a threshold-based policy.

Manage QoS policy groups with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create storage Quality of Service (QoS) policy groups to limit the throughput of workloads and to monitor workload performance.

Create QoS policy groups

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **QoS Policy Groups**.
4. In the **QoS Policy Groups** window, click **Create**.
5. In the **Create Policy Group** dialog box, specify a group name for the policy.
6. Specify the minimum throughput limit.
   - In System Manager 9.5, you can set the minimum throughput limit only on a performance-based All Flash Optimized personality. In System Manager 9.6, you can also set the minimum throughput limit for ONTAP Select Premium systems.
   - You cannot set the minimum throughput limit for volumes on a FabricPool-enabled aggregate.
   - If you do not specify the minimum throughput value or if the minimum throughput value is set to 0, the system automatically displays “None” as the value.

     This value is case-sensitive.
7. Specify the maximum throughput limit.
   - The minimum throughput limit and the maximum throughput limit must be of the same unit type.
   - If you do not specify the minimum throughput limit, you can set the maximum throughput limit in IOPS and B/s, KB/s, MB/s, and so on.
   - If you do not specify the maximum throughput limit, the system automatically displays “Unlimited” as the value.

     This value is case-sensitive. The unit that you specify does not affect the maximum throughput.
8. Click **OK**.

Delete QoS policy groups

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to delete a Storage Quality of Service (QoS) policy group that is no longer required.

Before you begin

You must have unassigned all of the storage objects that are assigned to the policy group.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **QoS Policy Groups**.
4. In the **QoS Policy Groups** window, select the policy group that you want to delete, and then click **Delete**.
5. In the confirmation dialog box, click **Delete**.

Edit QoS policy groups

You can use the Edit Policy Group dialog box in ONTAP System Manager classic (available in ONTAP 9.7 and

earlier) to modify the name and maximum throughput of an existing storage Quality of Service (QoS) policy group.

About this task

- In System Manager 9.5, you can set the minimum throughput limit only on a performance-based All Flash Optimized personality. In System Manager 9.6, you can also set the minimum throughput limit for ONTAP Select Premium systems.
- You cannot set the minimum throughput limit for volumes on a FabricPool-enabled aggregate.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Policies** pane, click **QoS Policy Groups**.
4. Select the QoS policy group that you want to edit, and then click **Edit**.
   - The minimum throughput limit and the maximum throughput limit must be of the same unit type.
   - If you do not specify the minimum throughput limit, you can set the maximum throughput limit in IOPS and B/s, KB/s, MB/s, and so on.
   - If you do not specify the maximum throughput limit, the value is set to unlimited, and the unit that you specify does not affect the maximum throughput.
5. In the **Edit Policy Group** dialog box, edit the QoS policy group details, and then click **Save**.

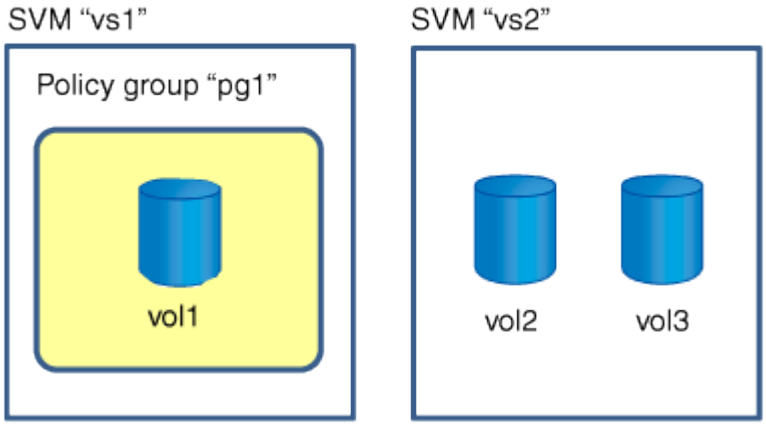
Rules for assigning storage objects to policy groups

You should be aware of rules that dictate how you can assign storage objects to Storage QoS policy groups.

Storage objects and policy groups must belong to the same SVM

A storage object must be contained by the SVM to which the policy group belongs. You specify the SVM to which the policy group belongs when you create the policy group. Multiple policy groups can belong to the same SVM.

In the following illustration, the policy group pg1 belongs to SVM vs1. You cannot assign volumes vol2 or vol3 to policy group pg1 because those volumes are contained by a different SVM.

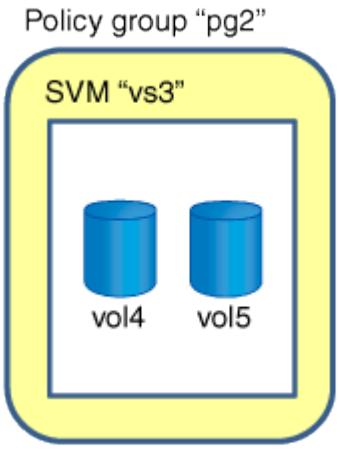


Nested storage objects cannot belong to policy groups

You cannot assign a storage object to a policy group if its containing object or its child objects belong to a policy group. The following table lists the restrictions.

If you assign the…	Then you cannot assign…
SVM to a policy group	Any storage objects contained by the SVM to a policy group
Volume to a policy group	The volume's containing SVM or any child LUNs to a policy group
LUN to a policy group	The LUN's containing volume or SVM to a policy group
File to a policy group	The file's containing volume or SVM to a policy group

In the following illustration, the SVM vs3 is assigned to policy group pg2. You cannot assign volumes vol4 or vol5 to a policy group because an object in the storage hierarchy (SVM vs3) is assigned to a policy group.



Manage NIS services with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to add, edit, and manage Network Information Service (NIS) domains.

Add NIS domains

You can maintain host information centrally by using NIS. You can use System Manager to add the NIS domain name of your storage system. Only one NIS domain can be active on a storage virtual machine (SVM) at any given time.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Services** pane, click **NIS**.

4. Click **Create**.
5. Type the NIS domain name, and then add one or more NIS servers.
6. Click **Create**.

Edit NIS domains

You can use System Manager to modify NIS domains based on the requirement for storage virtual machine (SVM) authentication and authorization.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Services** pane, click **NIS**.
4. Select the NIS domain, and then click **Edit**.
5. Make the required changes, and then click **Edit**.

NIS window

The NIS window enables you to view the current NIS settings for your storage system.

Command buttons

- **Create**

  Opens the Create NIS Domain dialog box, which enables you to create NIS domains.

- **Edit**

  Opens the Edit NIS Domain dialog box, which enables you to add, delete, or modify NIS servers.

- **Delete**

  Deletes the selected NIS domain.

- **Refresh**

  Updates the information in the window.

Related information

NFS configuration

Configure LDAP client services with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to add, edit, and delete LDAP client configurations.

Add an LDAP client configuration

You can use System Manager to add an LDAP client configuration at the cluster level or the storage virtual machine (SVM) level if you want to use LDAP services. You must first set up an LDAP client to use LDAP

services.

About this task

At the SVM level, you can add an LDAP client only for a selected SVM.

Steps

1. Add an LDAP client configuration by using one of the following methods:
   - Cluster level: click ⚙ > **LDAP**.
   - SVM level: click **SVM** > **SVM Settings** > **LDAP Client**.
2. Click **Add**.
3. Type the name of the LDAP client.
4. Add either the Active Directory domain or the LDAP server.
5. Click ⚙ (advanced options), select the **Schema**, and click **Apply**.
6. Specify the **Base DN** and **TCP Port**.
7. Click **Binding**, and then specify the authentication details.
8. Click **Save and Close**.
9. Verify that the LDAP client that you added is displayed.

Delete an LDAP client configuration

You can use System Manager to delete an LDAP client configuration at the cluster level or the storage virtual machine (SVM) level.

About this task

At the SVM level, you can delete an LDAP client only for a selected SVM.

Steps

1. To delete an LDAP client configuration:
   - Cluster level: Click ⚙ > **LDAP**.
   - SVM level: Click **SVM** > **SVM Settings** > **LDAP Client**.
2. Select the LDAP client that you want to delete, and then click **Delete**.
3. Select the confirmation check box, and then click **Delete**.
4. Verify that the LDAP client that you deleted is no longer displayed.

Edit an LDAP client configuration

You can use System Manager to edit an LDAP client configuration at the cluster level or the storage virtual machine (SVM) level.

About this task

At the SVM level, you can edit an LDAP client only for a selected SVM.

Steps

1. To edit an LDAP client configuration:
   - Cluster level: Click ⚙ > **LDAP**.

- SVM level: Click **SVM** > **SVM Settings** > **LDAP Client**.

2. Select the LDAP client that you want to modify, and then click **Edit**.
3. In the **Edit LDAP Client** dialog box, edit the LDAP client configuration as required.
4. Click **Save and Close**.
5. Verify that the changes that you made to the LDAP client configuration are displayed.

LDAP Client window

You can use the LDAP Client window to create LDAP clients for user authentication, file access authorization, user search, and mapping services between NFS and CIFS at the storage virtual machine (SVM) level.

Command buttons

- **Add**

  Opens the Create LDAP Client dialog box, which enables you to create and configure LDAP clients.

- **Edit**

  Opens the Edit LDAP Client dialog box, which enables you to edit LDAP client configurations. You can also edit active LDAP clients.

- **Delete**

  Opens the Delete LDAP Client(s) dialog box, which enables you to delete LDAP client configurations. You can also delete an active LDAP client.

- **Refresh**

  Updates the information in the window.

LDAP client list

Displays (in tabular format) details about LDAP clients.

- **LDAP Client Configuration**

  Displays the name of the LDAP client configuration that you specified.

- **Storage Virtual Machine**

  Displays the name of the SVM for each LDAP client configuration.

- **Schema**

  Displays the schema for each LDAP client.

- **Minimum Bind Level**

  Displays the minimum bind level for each LDAP client.

- **Active Directory Domain**

Displays the Active Directory domain for each LDAP client configuration.

- **LDAP Servers**

  Displays the LDAP server for each LDAP client configuration.

- **Preferred Active Directory Servers**

  Displays the preferred Active Directory server for each LDAP client configuration.

Related information

LDAP

Manage LDAP configurations with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage LDAP configurations.

Edit active LDAP clients

You can use System Manager to associate an active LDAP client with a storage virtual machine (SVM), which enables you to use LDAP as a name service or for name mapping.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Services** pane, click **LDAP Configuration**.
4. In the **LDAP Configuration** window, click **Edit**.
5. In the **Active LDAP Client** dialog box, select the LDAP client that you want to edit, and perform the following actions:
   - Modify the Active Directory domain servers.
   - Modify the preferred Active Directory servers.
6. Click **OK**.
7. Verify that the changes that you made are updated in the **LDAP Configuration** window.

Delete active LDAP clients

You can use System Manager to delete an active LDAP client when you do not want a storage virtual machine (SVM) to be associated with it.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. Click the **SVM Settings** tab.
4. In the **Services** pane, click **LDAP Configuration**.
5. Click **Delete**.

6. Select the confirmation check box, and then click **Delete**.

LDAP Configuration window

You can use the LDAP Configuration window to edit or delete active LDAP clients at the storage virtual machine (SVM) level.

Command buttons

- **Edit**

  Opens the Active LDAP Client dialog box, which enables you to edit the properties of the active LDAP client, such as Active Directory domain servers and preferred Active Directory servers.

- **Delete**

  Opens the Delete Active LDAP Client dialog box, which enables you to delete the active LDAP client.

- **Refresh**

  Updates the information in the window.

LDAP Configuration area

Displays the details about the active LDAP client.

- **LDAP client name**

  Displays the name of the active LDAP client.

- **Active Directory Domain Servers**

  Displays the Active Directory domain for the active LDAP client.

- **Preferred Active Directory Servers**

  Displays the preferred Active Directory server for the active LDAP client.

Manage Kerberos realm services with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create and manage Kerberos realm services.

Create a Kerberos realm configuration

If you want to use Kerberos authentication for client access, you must configure the storage virtual machine (SVM) to use an existing Kerberos realm. You can use System Manager to create a Kerberos realm configuration, which enables SVMs to use Kerberos security services for NFS.

Before you begin

- The CIFS license must be installed if CIFS shares are used, and the NFS license must be installed if an LDAP server is used.
- Active Directory (Windows 2003 or Windows 2008) with DES MD5 encryption capability must be available.

- You must have set the time zone and synchronized the time across the cluster by configuring NTP.

  This prevents authentication errors, and ensures that the timestamps in log files are consistent across the cluster.

About this task

While creating a Kerberos realm, you must set the following attributes in the Create Kerberos Realm wizard:

- Kerberos realm
- KDC IP address and port number

  The default port number is 88.

- Kerberos Key Distribution Center (KDC) vendor
- Administrative server IP address if the KDC vendor is not Microsoft
- Password server IP address
- Active Directory server name and IP address if the KDC vendor is Microsoft

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Services** pane, click **Kerberos Realm**.
4. In the **Kerberos Realm** window, click **Create**.
5. Type or select information as prompted by the wizard.
6. Confirm the details, and then click **Finish** to complete the wizard.

Edit a Kerberos realm configuration

You can use System Manager to edit a Kerberos realm configuration at the storage virtual machine (SVM) level.

About this task

You can modify the following attributes by using the Kerberos Realm Edit wizard:

- The KDC IP address and port number
- The IP address of the administrative server if the KDC vendor is not Microsoft
- The IP address of the password server
- The Active Directory server name and IP address if the KDC vendor is Microsoft

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Services** pane, click **Kerberos Realm**.
4. In the **Kerberos Realm** window, select the Kerberos realm configuration that you want to modify, and then click **Edit**.
5. Type or select information as prompted by the wizard.

6. Confirm the details, and then click **Finish** to complete the wizard.

Delete Kerberos realm configurations

You can use System Manager to delete a Kerberos realm configuration.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Services** pane, click **Kerberos Realm**.
4. In the **Kerberos Realm** window, select one or more Kerberos realm configurations that you want to delete, and then click **Delete**.
5. Select the confirmation check box, and then click **Delete**.

Use Kerberos with NFS for strong security

You can use Kerberos to provide strong authentication between SVMs and NFS clients to provide secure NFS communication. Configuring NFS with Kerberos increases the integrity and security of NFS client communications with the storage system.

Kerberos authentication for CIFS

With Kerberos authentication, upon connection to your CIFS server, the client negotiates the highest possible security level. However, if the client cannot use Kerberos authentication, Microsoft NTLM or NTLM V2 is used to authenticate with the CIFS server.

Kerberos Realm window

You can use the Kerberos Realm window to provide authentication between storage virtual machines (SVMs) and NFS clients to ensure secure NFS communication.

Command buttons

- **Create**

  Opens the Kerberos Realm Create wizard, which enables you to configure a Kerberos realm to retrieve user information.

- **Edit**

  Opens the Kerberos Realm Edit wizard, which enables you to edit a Kerberos realm configuration based on the requirement for SVM authentication and authorization.

- **Delete**

  Opens the Delete Kerberos Realm(s) dialog box, which enables you to delete Kerberos realm configuration.

- **Refresh**

  Updates the information in the window.

Kerberos Realm list

Provides details about the Kerberos realms, in tabular format.

- **Realm**

  Specifies the name of the Kerberos realm.

- **KDC Vendor**

  Specifies the name of the Kerberos Distribution Center (KDC) vendor.

- **KDC IP Address**

  Specifies the KDC IP address used by the configuration.

Details area

The details area displays information such as the KDC IP address and port number, KDC vendor, administrative server IP address and port number, Active Directory server and server IP address of the selected Kerberos realm configuration.

Related information

Setting the time zone for a cluster

NetApp Technical Report 4067: NFS in NetApp ONTAP

NetApp Technical Report 4616: NFS Kerberos in ONTAP with Microsoft Active Directory

NetApp Technical Report 4835: How to Configure LDAP in ONTAP

NFS management

Manage DNS/DDNS services with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage DNS/DDNS services.

Enable or disable DDNS

You can use System Manager to enable or disable DDNS on a storage system.

About this task

- DNS is enabled by default.
- DDNS is disabled by default.
- System Manager does not perform any validation checks for the DNS and DDNS settings.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Services** pane, click **DNS/DDNS**.

4. In the **DNS/DDNS Services** window, click **Edit**.
5. In the **Edit DNS/DDNS Settings** dialog box, enable DDNS by selecting the **DDNS service** check box.

   You can disable DDNS by clearing the **DDNS service** check box.

6. Click **OK**.

Edit DNS and DDNS settings

You can maintain host information centrally by using DNS. You can use System Manager to add or modify the DNS domain name of your storage system. You can also enable DDNS on your storage system to update the name server automatically in the DNS server.

Before you begin

You must have set up a CIFS server or an Active Directory account for the storage virtual machine (SVM) for secure DDNS to work.

About this task

System Manager does not perform any validation checks for the DNS and DDNS settings.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Services** pane, click **DNS/DDNS**.
4. Click **Edit**.
5. In the **DNS Domains and Name Servers** area, add or modify the DNS domain names and the IP addresses.
6. Select the **DDNS service** check box to enable DDNS.
   a. Select the **Enable Secure DDNS** check box to enable secure DDNS.
   b. Specify the fully qualified domain name (FQDN) and the time to live value for the DDNS service.

      By default, time to live is set to 24 hours and FQDN is set to `SVM name. domain name`.

7. Click **OK** to save the changes that you made.

DNS/DDNS Services window

The DNS/DDNS Services window enables you to view and edit the current DNS and DDNS settings for your system.

Command buttons

- **Edit**

  Opens the Edit DNS/DDNS Settings dialog box, which you can use to add or modify DNS or DDNS details. You can also enable or disable DDNS.

- **Refresh**

  Updates the information in the window.

Create and manage SVM user accounts with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create and manage storage virtual machine (SVM) user accounts.

Add SVM user accounts

You can use System Manager to add a storage virtual machine (SVM) user account and to specify a user login method for accessing the storage system.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **SVM User Details** pane, click **Users**.
4. Click **Add**.
5. Specify a user name and password for connecting to the storage system, and confirm the password.
6. Add one or more user login methods, and then click **Add**.

   A login method for the new vsadmin account is automatically included that uses HTTP as the application and is authenticated with a certificate.

Change the password for SVM user accounts

You can use System Manager to reset the password for a storage virtual machine (SVM) user account.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **SVM User Details** pane, click **Users**.
4. Select the user account for which you want to modify the password, and then click **Reset Password**.
5. In the **Reset Password** dialog box, type the new password, confirm the new password, and then click **Change**.

Edit SVM user accounts

You can use System Manager to edit a storage virtual machine (SVM) user account by modifying the user login methods for accessing the storage system.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **SVM User Details** pane, click **Users**.
4. Select the user account that you want to edit, and then click **Edit**.
5. Modify one or more user login methods, and then click **Modify**.

Lock or unlock SVM user accounts

You can use System Manager to lock or unlock storage virtual machine (SVM) user accounts.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **SVM User Details** pane, click **Users**.
4. In the **Users** window, select the user account for which you want to modify the account status, and then click either **Lock** or **Unlock**, as required.

Users window

You can use the Users window to manage user accounts, to reset the password of a user, and to view information about all of the user accounts.

Command buttons

- **Add**

  Opens the Add User dialog box, which enables you to add user accounts.

- **Edit**

  Opens the Modify User dialog box, which enables you to modify user login methods.

  It is a best practice to use a single role for all of the access and authentication methods of a user account.

- **Delete**

  Enables you to delete a selected user account.

- **Change Password**

  Opens the Change Password dialog box, which enables you to reset a selected user's password.

- **Lock**

  Locks the user account.

- **Refresh**

  Updates the information in the window.

Users list

The area below the users list displays detailed information about the selected user.

- **User**

  Displays the name of the user account.

- **Account Locked**

  Displays whether the user account is locked.

User Login Methods area

- **Application**

  Displays the access method that a user can use to access the storage system. The supported access methods include the following:

  - System console (console)
  - HTTP(S) (http)
  - ONTAP API (ontapi)
  - Service Processor (service-processor)
  - SSH (ssh)

- **Authentication**

  Displays the default supported authentication method, which is “password”.

- **Role**

  Displays the role of a selected user.

Local UNIX users and groups with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to maintain a list of local UNIX users and groups for each storage virtual machine (SVM).

UNIX window

You can use the UNIX window to maintain a list of local UNIX users and groups for each storage virtual machine (SVM). You can use local UNIX users and groups for authentication and name mappings.

Groups tab

You can use the Groups tab to add, edit, or delete UNIX groups that are local to an SVM.

Command buttons

- **Add Group**

  Opens the Add Group dialog box, which enables you to create UNIX groups that are local to SVMs. Local UNIX groups are used with local UNIX users.

- **Edit**

  Opens the Edit Group dialog box, which enables you to edit a group ID.

- **Delete**

Deletes the selected group.

- **Refresh**

  Updates the information in the window.

Groups list

- **Group Name**

  Displays the name of the group.

- **Group ID**

  Displays the ID of the group.

Users tab

You can use the **Users** tab to add, edit, and delete UNIX users that are local to SVMs.

Command buttons

- **Add User**

  Opens the Add User dialog box, which enables you to create UNIX users that are local to SVMs.

- **Edit**

  Opens the Edit User dialog box, which enables you to edit the User ID, UNIX group to which the user belongs, and the full name of the user.

- **Delete**

  Deletes the selected user.

- **Refresh**

  Updates the information in the window.

Users list

- **User Name**

  Displays the name of the user.

- **User ID**

  Displays the ID of the user.

- **Full Name**

  Displays the full name of the user.

- **Primary Group ID**

Displays the ID of the group to which the user belongs.

- **Primary Group Name**

  Displays the name of the group to which the user belongs.

Local windows group

Manage local Windows groups with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage local Windows groups. You can modify group properties, memberships, accounts and assign specific privileges to groups.

Edit local Windows group properties

You can manage local group memberships by adding and removing a local user, an Active Directory user, or an Active Directory group by using System Manager. You can modify the privileges that are assigned to a group and the description of a group to easily identify the group.

About this task

You must keep the following in mind when adding members to or removing members from a local Windows group:

- You cannot add users to or remove users from the special *Everyone* group.
- You cannot add a local Windows group to another local Windows group.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Host Users and Groups** pane, click **Windows**.
4. In the **Groups** tab, click **Edit**.
5. Specify a name for the group and a description to identify the new group.
6. Assign a set of privileges to the group.

   You can select the privileges from the predefined set of supported privileges.

7. Click **Add** to add users to the group.
8. In the **Add Members** window, perform one of the following actions:
   - Specify the Active Directory user or Active Directory group to be added to a particular local group.
   - Select the users from the list of available local users in the storage virtual machine (SVM).
9. Click **Edit**.

Results

The local Windows group settings are modified, and the changes are displayed in the **Groups** tab.

Create a local Windows group

You can use System Manager to create local Windows groups that can be used for authorizing access to the data contained in the storage virtual machine (SVM) over an SMB connection. You can also assign the privileges that define the user rights or capabilities that a member of the group has when performing administrative activities.

Before you begin

CIFS server must be configured for the SVM.

About this task

- You can specify a group name with or without the local domain name.

  The local domain is the name of the CIFS server for the SVM. For example, if the CIFS server name of the SVM is “CIFS_SERVER” and you want to create an “engineering” group, you can specify either “engineering” or “CIFS_SERVER\engineering” as the group name.

  The following rules apply when using a local domain as part of the group name:

  - You can specify only the local domain name for the SVM to which the group is applied.

    For example, if the local CIFS server name is “CIFS_SERVER”, you cannot specify “CORP_SERVER\group1” as the group name.

  - You cannot use “BUILTIN” as a local domain in the group name.

    For example, you cannot create a group with “BUILTIN\group1” as the name.

  - You cannot use an Active Directory domain as a local domain in the group name.

    For example, you cannot create a group named “AD_DOM\group1”, where “AD_DOM” is the name of an Active Directory domain.

- You cannot use a group name that already exists.
- The group name that you specify must meet the following requirements:
  - Must not exceed 256 characters
  - Must not end in a period
  - Must not include commas
  - Must not include any of the following printable characters: " / \ [ ] : | < > + = ; ? * @
  - Must not include characters in the ASCII range 1 through 31, which are non-printable

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Host Users and Groups** pane, click **Windows**.
4. In the **Groups** tab, click **Create**.
5. In the **Create Group** dialog box, specify a name for the group and a description that helps you to identify the new group.
6. Assign a set of privileges to the group.

You can select the privileges from the predefined set of supported privileges.

7. Click **Add** to add users to the group.
8. In the **Add Members to Group** dialog box, perform one of the following actions:
   - Specify the Active Directory user or Active Directory group to be added to a particular local group.
   - Select the users from the list of available local users in the SVM.
   - Click **OK**.
9. Click **Create**.

Results

The local Windows group is created and is listed in the Groups window.

Add user accounts to a Windows local group

You can add a local user, an Active Directory user, or an Active Directory group (if you want users to have the privileges that are associated with that group) to a Windows local group by using System Manager.

Before you begin

- The group must exist before you can add a user to the group.
- The user must exist before you can add the user to a group.

About this task

You must keep the following in mind when adding members to a local Windows group:

- You cannot add users to the special *Everyone* group.
- You cannot add a local Windows group to another local Windows group.
- You cannot add a user account that contains a space in the user name by using System Manager.

  You can either rename the user account or add the user account by using the command-line interface (CLI).

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Host Users and Groups** pane, click **Windows**.
4. In the **Groups** tab, select the group to which you want to add a user, and then click **Add Members**.
5. In the **Add Members** window, perform one of the following actions:
   - Specify the Active Directory user or Active Directory group to be added to a particular local group.
   - Select the users from the list of available local users in the storage virtual machine (SVM).
6. Click **OK**.

Results

The user that you added is listed in the Userstab of the **Groups** tab.

Rename a local Windows group

You can use System Manager to rename a local Windows group to identify the group more easily.

About this task

- The new group name must be created in the same domain as the old group name.
- The group name must meet the following requirements:
  - Must not exceed 256 characters
  - Must not end in a period
  - Must not include commas
  - Must not include any of the following printable characters: " / \ [ ] : | < > + = ; ? * @
  - Must not include characters in the ASCII range 1 through 31, which are non-printable

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Host Users and Groups** pane, click **Windows**.
4. In the **Groups** tab, select the group that you want to rename, and then click **Rename**.
5. In the **Rename Group** window, specify a new name for the group.

Results

The local group name is changed, and the group is listed with the new name in the Groups window.

Delete a local Windows group

You can use System Manager to delete a local Windows group from a storage virtual machine (SVM) if the group is no longer required for determining access rights to the data contained on the SVM or for assigning SVM user rights (privileges) to group members.

About this task

- Removing a local group removes the membership records of the group.
- The file system is not altered.

  Windows Security Descriptors on files and directories that refer to this group are not adjusted.
- The special “Everyone” group cannot be deleted.
- Built-in groups such as BUILTIN\Administrators and BUILTIN\Users cannot be deleted.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Host Users and Groups** pane, click **Windows**.
4. In the **Groups** tab, select the group that you want to delete, and then click **Delete**.
5. Click **Delete**.

Results

The local group is deleted along with its membership records.

Create a local Windows user account

You can use System Manager to create a local Windows user account that can be used to authorize access to the data contained in the storage virtual machine (SVM) over an SMB connection. You can also use local Windows user accounts for authentication when creating a CIFS session.

Before you begin

- The CIFS server must be configured for the SVM.

About this task

A local Windows user name must meet the following requirements:

- Must not exceed 20 characters
- Must not end in a period
- Must not include commas
- Must not include any of the following printable characters: " / \ [ ] : | < > + = ; ? * @
- Must not include characters in the ASCII range 1 through 31, which are non-printable

The password must meet the following criteria:

- Must be at least six characters in length
- Must not contain the user account name
- Must contain characters from at least three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Special characters: ~ ! @ # 0 ^ & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Host Users and Groups** pane, click **Windows**.
4. In the **Users** tab, click **Create**.
5. Specify a name for the local user.
6. Specify the full name of the local user and a description that helps you to identify this new user.
7. Enter a password for the local user, and confirm the password.

   The password must meet the password requirements.

8. Click **Add** to assign group memberships to the user.
9. In the **Add Groups** window, select the groups from the list of available groups in the SVM.
10. Select **Disable this account** to disable this account after the user is created.
11. Click **Create**.

Results

The local Windows user account is created and is assigned membership to the selected groups. The user account is listed in the **Users** tab.

Edit local Windows user properties

You can use System Manager to modify a local Windows user account if you want to change an existing user's full name or description, or if you want to enable or disable the user account. You can also modify the group memberships that are assigned to the user account.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Host Users and Groups** pane, click **Windows**.
4. In the **Users** tab, click **Edit**.
5. In the **Modify User** window, make the required changes.
6. Click **Modify**.

Results

The attributes of the local Windows user account are modified and are displayed in the **Users** tab.

Assign group memberships to a user account

You can use System Manager to assign group membership to a user account if you want a user to have the privileges that are associated with a particular group.

Before you begin

- The group must exist before you can add a user to the group.
- The user must exist before you can add the user to a group.

About this task

You cannot add users to the special *Everyone* group.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Host Users and Groups** pane, click **Windows**.
4. In the **Users** tab, select the user account to which you want to assign group memberships, and then click **Add to Group**.
5. In the **Add Groups** window, select the groups to which you want to add the user account.
6. Click **OK**.

Results

The user account is assigned membership to all of the selected groups, and the user has the privileges that are associated with these groups.

Rename a local Windows user

You can use System Manager to rename a local Windows user account to identify the local user more easily.

About this task

- The new user name must be created in the same domain as the previous user name.
- The user name that you specify must meet the following requirements:
  - Must not exceed 20 characters
  - Must not end in a period
  - Must not include commas
  - Must not include any of the following printable characters: " / \ [ ] : | < > + = ; ? * @
  - Must not include characters in the ASCII range 1 through 31, which are non-printable

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Host Users and Groups** pane, click **Windows**.
4. In the **Users** tab, select the user that you want to rename, and then click **Rename**.
5. In the **Rename User** window, specify a new name for the user.
6. Confirm the new name, and then click **Rename**.

Results

The user name is changed, and the new name is listed in the **Users** tab.

Reset the password of a Windows local user

You can use System Manager to reset the password of a Windows local user. For example, you might want to reset the password if the current password is compromised or if the user has forgotten the password.

About this task

The password that you set must meet the following criteria:

- Must be at least six characters in length
- Must not contain the user account name
- Must contain characters from at least three of the following four categories:
  - English uppercase characters (A through Z)
  - English lowercase characters (a through z)
  - Base 10 digits (0 through 9)
  - Special characters: ~ ! @ # 0 ^ & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Host Users and Groups** pane, click **Windows**.

4. In the **Users** tab, select the user whose password you want to reset, and then click **Set Password**.
5. In the **Reset Password** dialog box, set a new password for the user.
6. Confirm the new password, and then click **Reset**.

Delete a local Windows user account

You can use System Manager to delete a local Windows user account from a storage virtual machine (SVM) if the user account is no longer required for local CIFS authentication to the CIFS server of the SVM or for determining access rights to the data contained in the SVM.

About this task

- Standard users such as Administrator cannot be deleted.
- ONTAP removes references to the deleted local user from the local-group database, from the local-user-membership, and from the user-rights database.

Steps

1. Click **Storage** > **SVMs**.
2. Select the SVM, and then click **SVM Settings**.
3. In the **Host Users and Groups** pane, click **Windows**.
4. In the **Users** tab, select the user account that you want to delete, and then click **Delete**.
5. Click **Delete**.

Results

The local user account is deleted along with its group membership entries.

The Windows window

You can use System Manager to use the Windows window. The Windows window helps you to maintain a list of local Windows users and groups for each storage virtual machine (SVM) on the cluster. You can use local Windows users and groups for authentication and name mappings.

Users tab

You can use the Users tab to view the Windows users that are local to an SVM.

Command buttons

- **Create**

  Opens the Create User dialog box, which enables you to create a local Windows user account that can be used to authorize access to data contained in the SVM over an SMB connection.

- **Edit**

  Opens the Edit User dialog box, which enables you to edit local Windows user properties, such as group memberships and the full name. You can also enable or disable the user account.

- **Delete**

  Opens the Delete User dialog box, which enables you to delete a local Windows user account from an SVM if it is no longer required.

- **Add to Group**

  Opens the Add Groups dialog box, which enables you to assign group membership to a user account if you want the user to have privileges associated with that group.

- **Set Password**

  Opens the Reset Password dialog box, which enables you to reset the password of a Windows local user. For example, you might want to reset the password if the password is compromised or if the user has forgotten the password.

- **Rename**

  Opens the Rename User dialog box, which enables you to rename a local Windows user account to more easily identify it.

- **Refresh**

  Updates the information in the window.

Users list

- **Name**

  Displays the name of the local user.

- **Full Name**

  Displays the full name of the local user.

- **Account Disabled**

  Displays whether the local user account is enabled or disabled.

- **Description**

  Displays the description for this local user.

Users Details Area

- **Group**

  Displays the list of groups in which the user is a member.

Groups tab

You can use the Groups tab to add, edit, or delete Windows groups that are local to an SVM.

Command buttons

- **Create**

  Opens the Create Group dialog box, which enables you to create local Windows groups that can be used for authorizing access to data contained in SVMs over an SMB connection.

- **Edit**

  Opens the Edit Group dialog box, which enables you to edit the local Windows group properties, such as privileges assigned to the group and the description of the group.

- **Delete**

  Opens the Delete Group dialog box, which enables you to delete a local Windows group from an SVM if it is no longer required.

- **Add Members**

  Opens the Add Members dialog box, which enables you to add local or Active Directory users, or Active Directory groups to the local Windows group.

- **Rename**

  Opens the Rename Group dialog box, which enables you to rename a local Windows group to more easily identify it.

- **Refresh**

  Updates the information in the window.

Groups list

- **Name**

  Displays the name of the local group.

- **Description**

  Displays the description for this local group.

Groups Details Area

- **Privileges**

  Displays the list of privileges associated with the selected group.

- **Users**

  Displays the list of local users associated with the selected group.

Name mapping with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to specify name mapping entries to map users from different platforms.

Name mapping conversion rules

An ONTAP system keeps a set of conversion rules for each SVM. Each rule consists of two pieces: a *pattern* and a *replacement*. Conversions start at the beginning of the appropriate list and perform a substitution based

on the first matching rule. The pattern is a UNIX-style regular expression. The replacement is a string containing escape sequences representing subexpressions from the pattern, as in the UNIX `sed` program.

Name Mapping window

You can use the Name Mapping window to specify the name mapping entries to map users from different platforms.

Name Mappings

You can create and use name mappings to map your UNIX users to Windows users, Windows users to UNIX users, or Kerberos users to UNIX users.

Command buttons

- **Add**

  Opens the Add Name Mapping Entry dialog box, which enables you to create a name mapping on storage virtual machines (SVMs).

- **Edit**

  Opens the Edit Name Mapping Entry dialog box, which enables you to edit a name mapping on SVMs.

- **Delete**

  Opens the Delete Name Mapping Entries dialog box, which enables you to delete a name mapping entry.

- **Swap**

  Opens the Swap Name Mapping Entries dialog box, which enables you to interchange positions of the two selected name mapping entries.

- **Refresh**

  Updates the information in the window.

Name mappings list

- **Position**

  Specifies the name mapping's position in the priority list. Name mappings are applied in the order in which they occur in the priority list.

- **Pattern**

  Specifies the user name pattern that must be matched.

- **Replacement**

  Specifies the replacement pattern for the user name.

- **Direction**

  Specifies the direction of the name mapping. Possible values are krb_unix for a Kerberos-to-UNIX name

mapping, win_unix for a Windows-to-UNIX name mapping, and unix_win for a UNIX-to-Windows name mapping.

Command buttons

- **Add**

  Opens the Add Group Mapping Entry dialog box, which enables you to create a group mapping on SVMs.

- **Edit**

  Opens the Edit Group Mapping Entry dialog box, which enables you to edit the group mapping on SVMs.

- **Delete**

  Opens the Delete Group Mapping Entries dialog box, which enables you to delete a group mapping entry.

- **Swap**

  Opens the Swap Group Mapping Entries dialog box, which enables you to interchange positions of the two selected group mapping entries.

- **Refresh**

  Updates the information in the window.

Group mappings list

- **Position**

  Specifies the group mapping's position in the priority list. Group mappings are applied in the order in which they occur in the priority list.

- **Pattern**

  Specifies the user name pattern that must be matched.

- **Replacement**

  Specifies the replacement pattern for the user names.

- **Direction**

  Specifies the direction of the group mapping. Possible values are `krb_unix` for a Kerberos-to-UNIX group mapping, `win_unix` for a Windows-to-UNIX group mapping, and `unix_win` for a UNIX-to-Windows group mapping.

Related information

SMB/CIFS management

Mirror relationships

Manage mirror relationships with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage mirror relationships. You can update, create, quiesce, initialize, reestablish, delete and edit mirror relationships in addition to resuming quiesced mirror relationships.

Delete relationships

You can use System Manager to delete a mirror relationship and permanently end the mirror relationship between the source and destination volumes. When a mirror relationship is deleted, the base Snapshot copy on the source volume is deleted.

About this task

It is a best practice to break the mirror relationship before deleting the relationship.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship that you want to delete and click **Delete**.
3. Select the confirmation check boxes to delete the mirror relationship and to release the base Snapshot copies, and then click **Delete**.

Results

The relationship is deleted, and the base Snapshot copy on the source volume is deleted.

Resynchronize relationships

You can use System Manager to reestablish a mirror relationship that was broken earlier. You can perform a resynchronization operation to recover from a disaster that disabled the source volume.

Before you begin

The source cluster and destination cluster and the source SVM and destination SVM must be in peer relationships.

About this task

- When you perform a resynchronization operation, the contents on the mirror destination are overwritten by the contents on the source volume.

  - For SnapLock compliance volumes, all data changes in the active file system with reference to the common Snapshot copy are preserved in a locked Snapshot copy until the expiry time that is set for the current volume.

    If the volume expiry time is in the past or has not been set, then the Snapshot copy and the common Snapshot copy are locked for a duration of 30 days. All of the intermediate Snapshot copies between the common Snapshot copy and the latest locked Snapshot copy are deleted.

  - For all volumes other than SnapLock compliance volumes, the resynchronization operation might cause loss of newer data that is written to the destination volume after the base Snapshot copy was created.

- If the Last Transfer Error field in the Protection window recommends a resynchronization operation, you must first break the relationship, and then perform the resynchronization operation.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship that you want to resynchronize.
3. Click **Operations** > **Resync**.
4. Select the confirmation checkbox, and then click **Resync**.

Resume quiesced relationships

You can use System Manager to resume a quiesced mirror relationship. When you resume the relationship, normal data transfer to the mirror destination is resumed and all the mirror activities are restarted.

About this task

If you have quiesced a broken mirror relationship from the command-line interface (CLI), you cannot resume the relationship from System Manager. You must use the CLI to resume the relationship.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship that you want to resume.
3. Click **Operations** > **Resume**.
4. Select the confirmation check box and click **Resume**.

Results

Data transfer to the mirror destination resumes for the selected mirror relationship.

Update relationships

You can use System Manager to initiate an unscheduled mirror update of the destination. You might have to perform a manual update to prevent data loss due to an upcoming power outage, scheduled maintenance, or data migration.

Before you begin

The mirror relationship must be in a Snapmirrored state.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship for which you want to update the data, and click **Operations** > **Update**.
3. Choose one of the following options:
   - Select **On demand** to perform an incremental transfer from the recent common Snapshot copy between the source and destination volumes.
   - Select **Select Snapshot copy** and specify the Snapshot copy that you want to transfer.
4. **Optional:** Select **Limit transfer bandwidth to** to limit the network bandwidth used for transfers and specify the maximum transfer speed.
5. Click **Update**.
6. Verify the transfer status in the **Details** tab.

Quiesce relationships

You can use System Manager to quiesce a mirror destination to stabilize it before creating a Snapshot copy. The quiesce operation enables active mirror transfers to finish and disables future transfers for the mirroring relationship.

About this task

You can quiesce only mirror relationships that are in the Snapmirrored state.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship that you want to quiesce.
3. Click **Operations** > **Quiesce**.
4. Select the confirmation check box and click **Quiesce**.

Initialize relationships

When you start a mirror relationship, you must initialize that relationship. Initializing a relationship consists of a complete baseline transfer of data from the source volume to the destination. You can use System Manager to initialize a mirror relationship if you have not already initialized the relationship while creating it.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship that you want to initialize.
3. Click **Operations** > **Initialize**.
4. Select the confirmation check box and click **Initialize**.
5. Verify the status of the mirror relationship in the **Protection** window.

Results

A Snapshot copy is created and transferred to the destination. This Snapshot copy is used as a baseline for subsequent incremental Snapshot copies.

Edit relationships

You can use System Manager to edit a mirror relationship either by selecting an existing policy or schedule in the cluster, or by creating a policy or schedule.

About this task

- You cannot edit a mirror relationship that is created between a volume in Data ONTAP 8.2.1 and a volume in ONTAP 8.3 or later.
- You cannot edit the parameters of an existing policy or schedule.
- You can modify the relationship type of a version-flexible mirror relationship, vault relationship, or mirror and vault relationship by modifying the policy type.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship for which you want to modify the policy or schedule, and then click **Edit**.
3. In the **Edit Relationship** dialog box, select an existing policy or create a policy:

If you want to…	Do the following…
Select an existing policy	Click **Browse**, and then select an existing policy.
Create a policy	a. Click **Create Policy**. b. Specify a name for the policy. c. Set the priority for scheduled transfers. Low indicates that the transfer has the least priority and is usually scheduled after normal priority transfers. By default, the priority is set to Normal. d. Select the **Transfer All Source Snapshot Copies** check box to include the "all_source_snapshots" rule to the mirror policy, which enables you to back up all of the Snapshot copies from the source volume. e. Select the **Enable Network Compression** check box to compress the data that is being transferred. f. Click **Create**.

4. Specify a schedule for the relationship:

If…	Do the following…
You want to assign an existing schedule	From the list of schedules, select an existing schedule.
You want to create a schedule	a. Click **Create Schedule**. b. Specify a name for the schedule. c. Select either **Basic** or **Advanced**. ◦ Basic specifies only the day of the week, time, and the transfer interval. ◦ Advanced creates a cron-style schedule. d. Click **Create**.
You do not want to assign a schedule	Select **None**.

5. Click **OK** to save the changes.

Create mirror relationships from a destination SVM

You can use System Manager to create a mirror relationship from the destination storage virtual machine (SVM) and to assign a policy and schedule to the mirror relationship. The mirror copy enables quick availability of data if the data on the source volume is corrupted or lost.

Before you begin

- The source cluster must be running ONTAP 8.2.2 or later.
- The SnapMirror license must be enabled on the source cluster and destination cluster.

> For some platforms, it is not mandatory for the source cluster to have the SnapMirror license enabled if the destination cluster has the SnapMirror license and Data Protection Optimization (DPO) license enabled.

- While mirroring a volume, if you select a SnapLock volume as the source, then the SnapMirror license and SnapLock license must be installed on the destination cluster.
- The source cluster and destination cluster must be in a healthy peer relationship.
- The destination SVM must have space available.
- A source volume of type read/write (rw) must exist.
- The FlexVol volumes must be online and must be of type read/write.
- The SnapLock aggregate type must be of the same type.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which Security Assertion Markup Language (SAML) authentication is enabled, password-based authentication must be enabled on the remote cluster.

About this task

- System Manager does not support a cascade relationship.

  For example, a destination volume in a relationship cannot be the source volume in another relationship.

- You cannot create a mirror relationship between a sync-source SVM and a sync-destination SVM in a MetroCluster configuration.
- You can create a mirror relationship between sync-source SVMs in a MetroCluster configuration.
- You can create a mirror relationship from a volume on a sync-source SVM to a volume on a data-serving SVM.
- You can create a mirror relationship from a volume on a data-serving SVM to a data protection (DP) volume on a sync-source SVM.
- You can create a mirror relationship between SnapLock volumes of the same type only.

  For example, if the source volume is a SnapLock Enterprise volume, then the destination volume must also be a SnapLock Enterprise volume. You must ensure that the destination SVM has aggregates of the same SnapLock type available.

- The destination volume that is created for a mirror relationship is not thin provisioned.
- A maximum of 25 volumes can be protected in one selection.
- You cannot create a mirror relationship between SnapLock volumes if the destination cluster is running a version of ONTAP that is older than the ONTAP version that the source cluster is running.

Steps

1. Click **Protection** > **Volume Relationships**.
2. In the **Volume Relationships** window, click **Create**.
3. In the **Browse SVM** dialog box, select an SVM for the destination volume.

4. In the **Create Protection Relationship** dialog box, select **Mirror** from the **Relationship Type** drop-down list.
5. Specify the cluster, the SVM, and the source volume.

   If the specified cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the specified cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed.

6. For FlexVol volumes, specify a volume name suffix.

   The volume name suffix is appended to the source volume names to generate the destination volume names.

7. Click **Browse**, and then change the mirror policy.
8. Select a schedule for the relationship from the list of existing schedules.
9. Select **Initialize Relationship** to initialize the mirror relationship.
10. Enable FabricPool-enabled aggregates, and then select an appropriate tiering policy.
11. Click **Create**.

Results

If you chose to create a destination volume, a destination volume of type *dp* is created, with the language attribute set to match the language attribute of the source volume.

A mirror relationship is created between the source volume and the destination volume. The base Snapshot copy is transferred to the destination volume if you have opted to initialize the relationship.

Reverse resynchronizing mirror relationships

You can use System Manager to reestablish a mirror relationship that was previously broken. In a reverse resynchronization operation, you reverse the functions of the source volume and destination volume.

Before you begin

The source volume must be online.

About this task

- You can use the destination volume to serve data while you repair or replace the source volume, update the source volume, and reestablish the original configuration of the systems.
- When you perform reverse resynchronization, the contents on the mirror source are overwritten by the contents on the destination volume.

- For SnapLock compliance volumes, all data changes in the active file system with reference to the common Snapshot copy are preserved in a locked Snapshot copy until the expiry time that is set for the current volume.

  If the volume expiry time is in the past or has not been set, then the Snapshot copy and the common Snapshot copy are locked for a duration of 30 days. All of the intermediate Snapshot copies between the common Snapshot copy and the latest locked Snapshot copy are deleted.

- For all volumes other than SnapLock compliance volumes, the resynchronization operation might cause loss of newer data that is written to the source volume after the base Snapshot copy was created.

- When you perform reverse resynchronization, the mirror policy of the relationship is set to DPDefault, and the mirror schedule is set to None.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship that you want to reverse.
3. Click **Operations** > **Reverse Resync**.
4. Select the confirmation checkbox, and then click **Reverse Resync**.

Related information

Protection window

Break SnapMirror relationships with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to break a SnapMirror relationship. You must break a SnapMirror relationship if a SnapMirror source becomes unavailable and you want client applications to be able to access the data from the mirror destination. After the SnapMirror relationship is broken, the destination volume type changes from "data protection" (DP) to "read/write" (RW).

Before you begin

- The SnapMirror destination must be in the quiesced state or idle state.
- The destination volume must be mounted on the destination storage virtual machine (SVM) namespace.

About this task

- You can 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.
- You can break SnapMirror relationships between ONTAP systems and SolidFire storage systems.
- If you are breaking a FlexGroup volume relationship, you must refresh the page to view the updated status of the relationship.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship that you want to break.

3. Click **Operations** > **Break**.
4. Select the confirmation check box, and then click **Break**.

Results

The data protection SnapMirror relationship is broken. The destination volume type changes from data protection (DP), read-only, to read/write (RW). The system stores the base Snapshot copy for the data protection mirror relationship for later use.

Related information

Protection window

Abort a mirror transfer with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to abort a volume replication operation before the data transfer is complete. You can abort a scheduled update, a manual update, or an initial data transfer.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the relationship for which you want to stop the data transfer, and click **Operations** > **Abort**.
3. Click the **Yes, I want to abort the transfer** check box to confirm the operation.
4. Click the **Keep any partially transferred data** check box to retain the data that is already transferred to the destination volume.
5. Click **Abort**.

   The transfer status is displayed as “Aborting” until the operation is complete and displayed as “Idle” after the operation is complete.

Related information

Protection window

Restore a volume in a mirror relationship with System Manager - ONTAP 9.7 and earlier

For a version-independent mirror relationship, you can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to restore Snapshot copies to a source volume or to other volumes if the source data is corrupted and is no longer usable. You can replace the original data with the Snapshot copies in the destination volume.

Before you begin

- The SnapMirror license must be enabled on both the source cluster and the destination cluster or on the nodes that contain the source volume and destination volume.
- The source cluster and destination cluster must be in a healthy peer relationship.
- The source aggregate or any other aggregate that you select for the restore operation must be a 64-bit aggregate.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which Security Assertion Markup Language (SAML) authentication is enabled, password-based authentication must also

be enabled on the remote cluster.

About this task

- You cannot restore a volume that is in a mirror relationship between a source storage virtual machine (SVM) and a destination SVM in a MetroCluster configuration.
- You cannot perform a restore operation on SnapLock volumes.
- You can restore a mirror relationship between sync-source SVMs in a MetroCluster configuration.
- You can restore a mirror relationship from a volume on a sync-source SVM to a default SVM.
- You can restore a mirror relationship from a volume on a default SVM to a DP volume on a sync-source SVM.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship, and then click **Operations** > **Restore**.
3. In the **Restore** dialog box, restore the data to the source volume in the mirror relationship or select any other volume:

If you want to restore the data to…	Do this…
The source volume	a. Select **Source volume**. b. Go to Step 7.
Any other volume	Select **Other volume**, and then select the cluster and SVM from the list.

4. Restore the data to a new volume or to an existing volume:

If you want to restore the data to…	Do this…
A new volume	If you want to change the default name, displayed in the format `destination_SVM_name_destination_volume_name_` restore, specify a new name, and then select the containing aggregate for the volume.
An existing volume	Select the **Select Volume** option. You must select a volume other than the source volume, or a read/write volume with some data in it and with a common Snapshot copy. Only those volumes with the same language attribute as the source volume are listed.

5. Select either the latest Snapshot copy or the specific Snapshot copy that you want to restore.
6. Select the confirmation checkbox to restore the volume from the Snapshot copy.
7. **Optional:** Select the **Enable Network Compression** checkbox to compress the data that is being transferred during the restore operation.

8. Click **Restore**.

Vault relationships

Manage vault relationships with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to update, resume, quiesce, initialize and delete vault relationships in addition to creating vault relationships from a destination SVM.

Edit relationships

You can use System Manager to edit a vault relationship either by selecting an existing policy or schedule in the cluster, or by creating a new policy or schedule. However, you cannot edit the parameters of an existing policy or schedule.

Before you begin

The source and destination clusters must be in a healthy peer relationship.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the vault relationship for which you want to modify the policy or schedule, and then click **Edit**.
3. In the **Edit Relationship** dialog box, select the appropriate action:

If you want to…	Do the following…
Select an existing policy	Click **Browse**, and then select an existing policy. You can select a policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.

If you want to…	Do the following…
Create a new policy	a. Click **Create Policy**. b. Specify a name for the policy. c. Set the priority for scheduled transfers. Low indicates that the transfer has the least priority and is usually scheduled after normal priority transfers. By default, the priority is set to Normal. d. Select the **Enable Network Compression** check box to compress the data that is being transferred. e. Specify a SnapMirror label and destination retention count for the vault policy. You must ensure that a Snapshot copy with the same label is created on the source volume for the new SnapMirror label to be effective. f. Click **Create**.

4. Specify a schedule for the relationship:

If…	Do the following…
You want to assign an existing schedule	Select an existing schedule from the list.
You want to create a new schedule	a. Click **Create Schedule**. b. Specify a name for the schedule. c. Select one of the following options: ◦ **Basic** You can select this option to specify only the day of the week, time, and the transfer interval. ◦ **Advanced** You can select this option to specify a cron-style schedule. d. Click **Create**.
You do not want to assign a schedule	Select **None**.

5. Click **OK**.

Related information

Protection window

Initialize relationships

You can use System Manager to initialize a vault relationship if you have not already initialized it while creating the relationship. A baseline transfer of data is initiated from the source FlexVol volume to the destination FlexVol volume.

Before you begin

The source and destination clusters must be in a healthy peer relationship.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the relationship you want to initialize, and click **Operations** > **Initialize**.
3. In the **Initialize** window, click **Initialize**.

Results

A Snapshot copy is created and transferred to the destination.

This Snapshot copy is used as a baseline for subsequent incremental Snapshot copies.

Related information

Protection window

Create relationships from a destination SVM

You can use System Manager to create a vault relationship from the destination storage virtual machine (SVM), and to assign a vault policy to create a backup vault. In the event of data loss or corruption on a system, backed-up data can be restored from the backup vault destination.

Before you begin

- The source cluster must be running ONTAP 8.2.2 or later.
- SnapVault license or SnapMirror license must be enabled on both the source cluster and the destination cluster.

  For some platforms, it is not mandatory for the source cluster to have the SnapVault license or the SnapMirror license enabled if the destination cluster has the SnapVault license or the SnapMirror license, and DPO license enabled.

- The source cluster and destination cluster must be in a healthy peer relationship.
- The destination SVM must have space available.
- The source aggregate and the destination aggregate must be 64-bit aggregates.
- A source volume of type read/write (rw) must exist.
- A vault (XDP) policy must exist.

  If a vault policy does not exist, you must create a vault policy or accept the default vault policy (XDPDefault) that is automatically assigned.

- FlexVol volumes must be online and read/write.

- The SnapLock aggregate type must be the same.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which SAML authentication is enabled, password-based authentication must be enabled on the remote cluster.

About this task

- System Manager does not support a cascade relationship.

  For example, a destination volume in a relationship cannot be the source volume in another relationship.

- You cannot create a vault relationship between a sync-source SVM and a sync-destination SVM in a MetroCluster configuration.
- You can create a vault relationship between sync-source SVMs in a MetroCluster configuration.
- You can create a vault relationship from a volume on a sync-source SVM to a volume on a data-serving SVM.
- You can create a vault relationship from a volume on a data-serving SVM to a data protection (DP) volume on a sync-source SVM.
- You can create a vault relationship only between a non-SnapLock (primary) volume and a SnapLock destination (secondary) volume.
- A maximum of 25 volumes can be protected in one selection.

Steps

1. Click **Protection** > **Volume Relationships**.
2. In the **Relationships** window, click **Create**.
3. In the **Browse SVM** dialog box, select an SVM for the destination volume.
4. In the **Create Protection Relationship** dialog box, select **Vault** from the **Relationship Type** drop-down list.
5. Specify the cluster, the SVM, and the source volume.

   If the specified cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the specified cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed.

6. Enter a volume name suffix.

   The volume name suffix is appended to the source volume names to generate the destination volume names.

7. If you are creating a SnapLock volume, specify the default retention period.

   The default retention period can be set to any value between 1 day through 70 years or Infinite.

8. **Optional:** Click **Browse**, and then change the vault policy.
9. Select a schedule for the relationship from the list of existing schedules.
10. **Optional:** Select **Initialize Relationship** to initialize the vault relationship.
11. Enable SnapLock aggregates, and then select a SnapLock Compliance aggregate or a SnapLock Enterprise aggregate.
12. Enable FabricPool-enabled aggregates, and then select an appropriate tiering policy.

13. Click **Validate** to verify whether the selected volumes have matching labels.
14. Click **Create**.

Results

If you chose to create a destination volume, a volume of type *dp* is created with the following default settings:

- Autogrow is enabled.
- Deduplication is enabled or disabled according to the user preference or the source volume deduplication setting.
- Compression is disabled.
- The language attribute is set to match the language attribute of the source volume.

A vault relationship is created between the destination volume and the source volume. The base Snapshot copy is transferred to the destination volume if you have opted to initialize the relationship.

Update relationships

You can use System Manager to manually initiate an unscheduled incremental update. You might require a manual update to prevent data loss due to an upcoming power outage, scheduled maintenance, or data migration.

Before you begin

The vault relationship must be initialized.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the relationship for which you want to update the data, and click **Operations** > **Update**.
3. Choose one of the following options:
   - Select **As Per Policy** to perform an incremental transfer from the recent common Snapshot copy between the source and destination volumes.
   - Select **Select Snapshot copy** and specify the Snapshot copy that you want to transfer.
4. **Optional:** Select **Limit transfer bandwidth to** to limit the network bandwidth that is used for transfers and specify the maximum transfer speed.
5. Click **Update**.
6. Verify the transfer status in the **Details** tab.

Delete relationships

You can use System Manager to end a vault relationship between a source and destination volume, and release the Snapshot copies from the source.

About this task

Releasing the relationship permanently removes the base Snapshot copies used by the vault relationship on the source volume. To re-create the vault relationship, you must run the resynchronization operation from the source volume by using the command-line interface (CLI).

Steps

1. Click **Protection** > **Volume Relationships**.

2. Select the volume for which you want to delete the vault relationship, and click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

   You can also select the release base Snapshot copies check box to delete the base Snapshot copies used by the vault relationship on the source volume.

   If the relationship is not released, then you must use the CLI to run the release operation on the source cluster to delete the base Snapshot copies that were created for the vault relationship from the source volume.

Resume relationships

You can resume a quiesced vault relationship by using System Manager. When you resume the relationship, normal data transfer to the destination FlexVol volume is resumed and all vault activities are restarted.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the relationship for which you want to resume the data transfer, and click **Operations** > **Resume**.
3. In the **Resume** window, click **Resume**.

Results

Normal data transfers are resumed. If there is a scheduled transfer for the relationship, the transfer is started from the next schedule.

Quiesce relationships

You can use System Manager to disable data transfers to the destination FlexVol volume by quiescing the vault relationship.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the relationship for which you want to stop the scheduled data transfers, and click **Operations** > **Quiesce**.
3. In the **Quiesce** window, click **Quiesce**.

Results

If there is no transfer in progress, the transfer status is displayed as Quiesced. If a transfer is in progress, the transfer is not affected, and the transfer status is displayed as Quiescing until the transfer is complete.

Related information

Protection window

Abort a Snapshot copy transfer with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to abort or stop a data transfer that is currently in progress.

Steps

1. Click **Protection** > **Volume Relationships**.

2. Select the relationship for which you want to stop the data transfer, and click **Operations** > **Abort**.
3. Select the **Yes, I want to abort the transfer** check box to confirm the operation.
4. **Optional:** Select the **Keep any partially transferred data** check box to retain the data that is already transferred to the destination volume.
5. Click **Abort**.

Results

The transfer status is displayed as “Aborting” until the operation is complete and displayed as “Idle” after the operation is complete.

Related information

Protection window

Restore a volume in a vault relationship with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to restore Snapshot copies to a source volume or to other volumes if the source data is corrupted and is no longer usable. You can replace the original data with the Snapshot copies in the destination volume.

Before you begin

- The SnapMirror license must be enabled on both the source storage system and the destination storage system or on the nodes that contain the source volume and destination volume.
- The source cluster and destination cluster must be in a healthy peer relationship.
- The source aggregate or any other aggregate that you select for the restore operation must be a 64-bit aggregate.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which SAML authentication is enabled, password-based authentication must also be enabled on the remote cluster.

About this task

- You cannot restore a volume that is in a vault relationship between a source storage virtual machine (SVM) and a destination SVM in a MetroCluster configuration.
- You can restore a vault relationship between sync-source SVMs in a MetroCluster configuration.
- You can restore a vault relationship from a volume on a sync-source SVM to a default SVM.
- You can restore a vault relationship from a volume on a default SVM to a DP volume on a sync-source SVM.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the vault relationship, and then click **Operations** > **Restore**.
3. In the **Restore** dialog box, restore the data to the source volume in the vault relationship or select any other volume:

If you want to restore the data to…	Do this…
The source volume	a. Select **Source volume**. b. Go to Step 6.
Any other volume	Select **Other volume**, and then select the cluster and SVM from the list.

4. Restore the data to a new volume or select any existing volume:

If you want to restore the data to…	Do this…
A new volume	If you want to change the default name, displayed in the format `destination_SVM_name_destination_volume_name_` restore, specify a new name, and then select the containing aggregate for the volume.
An existing volume	Select the **Select Volume** option. You must select a volume other than the source volume, or a read/write volume with some data in it and with a common Snapshot copy. Only those volumes with the same language attribute as the source volume are listed.

5. Select either the latest Snapshot copy or the specific Snapshot copy that you want to restore.
6. Select the confirmation check box to restore the volume from the Snapshot copy.
7. **Optional:** Select the **Enable Network Compression** check box to compress the data that is being transferred during the restore operation.
8. Click **Restore**.

Related information

Protection window

Mirror and vault relationships

Manage mirror and vault relationships with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to manage mirror and vault relationships. You can edit, delete, initialize, update, quiesce, resume and break mirror and vault relationships. You can also perform resynchronization or reverse resynchronization operations in addition to creating mirror and vault relationships from a destination SVM.

Edit relationships

You can use System Manager to edit a mirror and vault relationship by modifying the selected policy or schedule. However, you cannot edit the parameters of an existing policy or schedule.

Before you begin

The source and destination clusters must be in a healthy peer relationship.

About this task

You can modify the relationship type of a version-flexible mirror relationship, vault relationship, or mirror and vault relationship by modifying the policy type.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror and vault relationship that you want to modify, and then click **Edit**.
3. In the **Edit Relationship** dialog box, select the appropriate action:

If you want to…	Do the following…
Select an existing policy	Click **Browse**, and then select an existing policy. You can select a policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.
Create a new policy	a. Click **Create Policy**. b. Specify a name for the policy. c. Set the priority for scheduled transfers. Low indicates that the transfer has the least priority and is usually scheduled after normal priority transfers. By default, the priority is set to Normal. d. Select the **Enable Network Compression** check box to compress the data that is being transferred. e. Specify a SnapMirror label and destination retention count for the vault policy. You must ensure that a Snapshot copy with the same label is created on the source volume for the new SnapMirror label to be effective. f. Click **Create**.

4. Specify a schedule for the relationship:

If…	Do the following…
You want to assign an existing schedule	Click **Browse**, and then select an existing schedule.

If…	Do the following…
You want to create a new schedule	a. Click **Create Schedule**. b. Specify a name for the schedule. c. Select one of the following options: ◦ **Basic** You can select this option to specify only the day of the week, time, and the transfer interval. ◦ **Advanced** You can select this option to specify a cron style schedule. d. Click **Create**.
You do not want to assign a schedule	Select **None**.

5. Click **OK**.

Update relationships manually

You can use System Manager to manually initiate an unscheduled incremental update. You might require a manual update to prevent data loss due to an upcoming power outage, scheduled maintenance, or data migration.

Before you begin

The mirror and vault relationship must be initialized and in a Snapmirrored state.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror relationship for which you want to update the data, and then click **Operations** > **Update**.
3. Choose one of the following options:
   - Select **As Per Policy** to perform an incremental transfer from the recent common Snapshot copy between the source and destination volumes.
   - Select **Select Snapshot copy** and specify the Snapshot copy that you want to transfer.
4. Select **Limit transfer bandwidth to** to limit the network bandwidth that is used for transfers, and then specify the maximum transfer speed.
5. Click **Update**.
6. Verify the transfer status in the **Details** tab.

Initialize relationships

You can use System Manager to initialize a mirror and vault relationship if you have not already initialized the relationship while creating it. When you initialize a relationship, a complete baseline transfer of data is performed from the source volume to the destination.

Before you begin

The source and destination clusters must be in a healthy peer relationship.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror and vault relationship that you want to initialize, and then click **Operations** > **Initialize**.
3. Select the confirmation check box, and then click **Initialize**.
4. Verify the status of the relationship in the **Protection** window.

Results

A Snapshot copy is created and transferred to the destination.

This Snapshot copy is used as a baseline for subsequent incremental Snapshot copies.

Create a relationship from a destination SVM

You can use System Manager to create a mirror and vault relationship from the destination storage virtual machine (SVM). Creating this relationship enables you to better protect your data by periodically transferring data from the source volume to the destination volume. It also enables you to retain data for long periods by creating backups of the source volume.

Before you begin

- The destination cluster must be running ONTAP 8.3.2 or later.
- SnapMirror license must be enabled on the source cluster and destination cluster.

For some platforms, it is not mandatory for the source cluster to have the SnapMirror license enabled if the destination cluster has the SnapMirror license and Data Protection Optimization (DPO) license enabled.

- The source cluster and destination cluster must be in a healthy peer relationship.
- The destination SVM must have space available.
- The source aggregate and destination aggregate must be 64-bit aggregates.
- A source volume of type read/write (rw) must already exist.
- The SnapLock aggregate type must be the same.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which SAML authentication is enabled, password-based authentication must be enabled on the remote cluster.

About this task

- System Manager does not support a cascade relationship.

  For example, a destination volume in a relationship cannot be the source volume in another relationship.

- You cannot create a mirror and vault relationship between a sync-source SVM and a sync-destination SVM in a MetroCluster configuration.
- You can create a mirror and vault relationship between sync-source SVMs in a MetroCluster configuration.
- You can create a mirror and vault relationship from a volume on a sync-source SVM to a volume of a data-serving SVM.
- You can create a mirror and vault relationship from a volume on a data-serving SVM to a DP volume on a

sync-source SVM.

- A maximum of 25 volumes can be protected in one selection.

Steps

1. Click **Protection** > **Volume Relationships**.
2. In the **Relationships** window, click **Create**.
3. In the **Browse SVM** dialog box, select an SVM for the destination volume.
4. In the **Create Protection Relationship** dialog box, select **Mirror and Vault** from the **Relationship Type** drop-down list.
5. Specify the cluster, the SVM, and the source volume.

   If the specified cluster is running a version of ONTAP software earlier than ONTAP 9.3, then only peered SVMs are listed. If the specified cluster is running ONTAP 9.3 or later, peered SVMs and permitted SVMs are listed.

6. Enter a volume name suffix.

   The volume name suffix is appended to the source volume names to generate the destination volume names.

7. **Optional:** Click **Browse**, and then change the mirror and vault policy.

   You can select the policy that has the maximum number of matching labels with the Snapshot policy that is attached to the source volume.

8. Select a schedule for the relationship from the list of existing schedules.
9. **Optional:** Select **Initialize Relationship** to initialize the relationship.
10. Enable FabricPool-enabled aggregates, and then select an appropriate tiering policy.
11. Click **Validate** to verify whether the selected volumes have matching labels.
12. Click **Create**.

Resynchronize relationships

You can use System Manager to reestablish a mirror and vault relationship that was broken earlier. You can perform a resynchronization operation to recover from a disaster that disabled the source volume.

Before you begin

The source and destination clusters and the source and destination storage virtual machines (SVMs) must be in peer relationships.

About this task

You should be aware of the following before performing a resynchronization operation:

- When you perform a resynchronization operation, the contents on the destination volume are overwritten by the contents on the source.

  The resynchronization operation can cause loss of newer data written to the destination volume after the base Snapshot copy was created.

- If the Last Transfer Error field in the Protection window recommends a resynchronization operation, you

must first break the relationship and then perform the resynchronization operation.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror and vault relationship that you want to resynchronize, and then click **Operations** > **Resync**.
3. Select the confirmation check box, and then click **Resync**.

Reverse resynchronize relationships

You can use System Manager to reestablish a mirror and vault relationship that was previously broken. In a reverse resynchronization operation, the functions of the source and destination volumes are reversed. You can 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.

Before you begin

The source volume must be online.

About this task

- When you perform reverse resynchronization, the contents on the source volume are overwritten by the contents on the destination volume.

  The reverse resynchronization operation can cause data loss on the source volume.

- When you perform reverse resynchronization, the policy of the relationship is set to MirrorAndVault and the schedule is set to None.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror and vault relationship that you want to reverse, and then click **Operations** > **Reverse Resync**.
3. Select the confirmation check box, and then click **Reverse Resync**.

Break relationships

You can use System Manager to break a mirror and vault relationship if a source volume becomes unavailable and you want client applications to access the data from the destination volume. You can use the destination volume to serve data while you repair or replace the source volume, update the source volume, and reestablish the original configuration of the systems.

Before you begin

- The mirror and vault relationship must be in the quiesced state or idle state.
- The destination volume must be mounted on the destination storage virtual machine (SVM) namespace.

About this task

You can break mirror relationships between ONTAP systems and SolidFire storage systems.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror and vault relationship that you want to break, and then click **Operations** > **Break**.

3. Select the confirmation check box, and then click **Break**.

Results

The mirror and vault relationship is broken. The destination volume type changes from data protection (DP) read-only to read/write. The system stores the base Snapshot copy for the mirror and vault relationship for later use.

Resume relationships

If you have a quiesced mirror and vault relationship, you can use System Manager to resume the relationship. When you resume the relationship, normal data transfer to the destination volume is resumed and all the protection activities are restarted.

About this task

If you have quiesced a broken mirror and vault relationship from the command-line interface (CLI), you cannot resume the relationship from System Manager. You must use the CLI to resume the relationship.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror and vault relationship that you want to resume, and then click **Operations** > **Resume**.
3. Select the confirmation check box, and then click **Resume**.

Results

Normal data transfers are resumed. If there is a scheduled transfer for the relationship, the transfer is started from the next schedule.

Delete relationships

You can use System Manager to end a mirror and vault relationship between a source and destination volume, and release the Snapshot copies from the source volume.

About this task

- It is a best practice to break the mirror and vault relationship before deleting the relationship.
- To re-create the relationship, you must run the resynchronization operation from the source volume by using the command-line interface (CLI).

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror and vault relationship that you want to delete and click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

   You can also select the release base Snapshot copies check box to delete the base Snapshot copies used by the mirror and vault relationship on the source volume.

   If the relationship is not released, then you must use the CLI to run the release operation on the source cluster to delete the base Snapshot copies that were created for the mirror and vault relationship from the source volume.

Results

The relationship is deleted and the base Snapshot copies on the source volume are permanently deleted.

Quiesce relationships

You can use System Manager to quiesce a destination volume to stabilize the destination before creating a Snapshot copy. The quiesce operation enables active data transfers to finish and disables future transfers for the mirror and vault relationship.

Before you begin

The mirror and vault relationship must be in a Snapmirrored state.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror and vault relationship that you want to quiesce, and then click **Operations** > **Quiesce**.
3. Select the confirmation check box, and then click **Quiesce**.

Results

If there is no transfer in progress, the transfer status is displayed as `Quiesced`. If a transfer is in progress, the transfer is not affected, and the transfer status is displayed as `Quiescing` until the transfer is complete.

Abort mirror and vault relationships with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to abort a volume replication operation if you want to stop the data transfer. You can abort a scheduled update, a manual update, or an initial data transfer.

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror and vault relationship for which you want to stop the data transfer, and then click **Operations** > **Abort**.
3. Select the **Yes, I want to abort the transfer** check box to confirm the operation.
4. **Optional:** Select the **Keep any partially transferred data** check box to retain the data that is already transferred to the destination volume.
5. Click **Abort**.

Results

The transfer status is displayed as “Aborting” until the operation is complete and displayed as “Idle” after the operation is complete.

Restore a volume in a mirror and vault relationship with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to restore Snapshot copies to a source volume or to other volumes if the source data is corrupted and is no longer usable. You can replace the original data with the Snapshot copies in the destination volume.

Before you begin

- The SnapMirror license and SnapVault license must be enabled on both the source cluster and the destination cluster or on the nodes that contain the source volume and destination volume.
- The source cluster and destination cluster must be in a healthy peer relationship.

- The source aggregate or any other aggregate that you select for the restore operation must be a 64-bit aggregate.
- If you are connecting from a cluster running ONTAP 9.2 or earlier to a remote cluster on which SAML authentication is enabled, password-based authentication must also be enabled on the remote cluster.

About this task

- You cannot restore a volume that is in a mirror and vault relationship between a source storage virtual machine (SVM) and a destination SVM in a MetroCluster configuration.
- You can restore a mirror and vault relationship for the following configurations:
  - Between sync-source SVMs in a MetroCluster configuration
  - From a volume on a sync-source SVM to a default SVM
  - From a volume on a default SVM to a DP volume on a sync-source SVM

Steps

1. Click **Protection** > **Volume Relationships**.
2. Select the mirror and vault relationship that you want to restore, and then click **Operations** > **Restore**.
3. In the **Restore** dialog box, restore the data to the source volume in the relationship or select any other volume:

If you want to restore the data to…	Do this…
The source volume	a. Select **Source volume**. b. Go to step 6.
Any other volume	Select **Other volume**, and then select the cluster and the SVM.

4. Restore the data to a new volume or to an existing volume:

If you want to restore the data to…	Do this…
A new volume	If you want to change the default name, displayed in the format "destination_SVM_name_destination_volume_name_restore", specify a new name, and then select the containing aggregate for the volume.
An existing volume	Select the **Select Volume** option. You must select a volume other than the source volume, or a read/write volume with some data in it and with a common Snapshot copy. Only those volumes with the same language attribute as the source volume are listed.

5. Select either the latest Snapshot copy or the specific Snapshot copy that you want to restore.

6. Select the confirmation check box to restore the volume from the Snapshot copy.
7. **Optional:** Select the **Enable Network Compression** check box to compress the data that is being transferred during the restore operation.
8. Click **Restore**.

Protection window with System Manager - ONTAP 9.7 and earlier

You can use the Protection window with ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create and manage mirror relationships, vault relationships, and mirror and vault relationships and to display details about these relationships. The Protection window does not display load-sharing (LS) relationships and transition data protection (TDP) relationships.

Command buttons

- **Create**

  Opens the Create Protection Relationship dialog box, which you can use to create a mirror relationship, vault relationship, or mirror and vault relationship from a destination volume.

  System Manager does not display any storage virtual machine (SVM) that is configured for disaster recovery (DR) in the Create Protection Relationship dialog box.

- **Edit**

  Opens the Edit Protection Relationship dialog box, which you can use to edit the schedule and policy of a relationship.

  For a vault relationship, mirror and vault relationship, or version-flexible mirror relationship, you can modify the relationship type by modifying the policy type.

- **Delete**

  Opens the Delete Protection Relationship dialog box, which you can use to delete a relationship.

- **Operations**

  Displays the operations that can be performed on a protection relationship.

- **Refresh**

  Updates the information in the window.

Protection relationships list

- **Source Storage Virtual Machine**

  Displays the SVM that contains the volume from which data is mirrored or vaulted in a relationship.

- **Source Volume**

  Displays the volume from which data is mirrored or vaulted in a relationship.

- **Destination Volume**

  Displays the volume to which data is mirrored or vaulted in a relationship.

- **Is Healthy**

  Displays whether the relationship is healthy or not.

- **Object Type**

  Displays the object type of the relationship, such as Volume, FlexGroup, or SVM.

- **Relationship State**

  Displays the state of the relationship, such as Snapmirrored, Uninitialized, or Broken Off.

- **Transfer Status**

  Displays the status of the relationship.

- **Relationship Type**

  Displays the type of relationship, such as mirror, vault, or mirror and vault.

- **Lag Time**

  Lag time is the difference between the current time and the timestamp of the last Snapshot copy that was successfully transferred to the destination system. The lag time will always be at least as much as the duration of the last successful transfer, unless the clocks on the source and destination systems are not synchronized. The time zone difference is automatically calculated into the lag time.

- **Policy Name**

  Displays the name of the policy that is assigned to the relationship.

- **Policy Type**

  Displays the type of policy that is assigned to the relationship. The policy type can be StrictSync, Sync, Asynchronous Mirror, Asynchronous Vault, or Asynchronous Mirror Vault.

Details area

- **Details tab**

  Displays general information about the selected relationship, such as the source cluster and destination cluster, data transfer rate, state of the relationship, details about the network compression ratio, data transfer status, type of current data transfer, type of last data transfer, latest Snapshot copy, and timestamp of the latest Snapshot copy.

- **Policy Details tab**

  Displays details about the policy that is assigned to the selected protection relationship. This tab also displays the SnapMirror label and the Snapshot copy schedules in the source volume that match the specified label.

- **Snapshot Copies tab**

  Displays the count of Snapshot copies with the SnapMirror label attribute for the selected protection relationship and the timestamp of the latest Snapshot copy.

SVM Relationships with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create and manage mirror relationships and mirror and vault relationships between SVMs. Storage virtual machine (SVM) disaster recovery (DR) provides disaster recovery capability at the SVM level by enabling the recovery of the data that is present in the constituent volumes of the SVM and the recovery of the SVM configuration.

Create SVM relationships

You can use System Manager to create SVM relationships to transfer data from the source SVM to the destination SVM. Creating an SVM relationship helps in recovering from a disaster as data is available on the source SVM and on the destination SVM.

Before you begin

- The destination cluster and source cluster must be running ONTAP 9.5 or later.
- The destination cluster must not be in a MetroCluster configurations.
- Starting with System Manager 9.6, Fabric Pool is supported.

Steps

1. Click **Protection** > **SVM Relationship** > **Create**.
2. Select the SVM relationship type from the **SVM Relationship Type** list.
3. From the **Source Storage Virtual Machine** pane, select the cluster and the SVM.
4. **Optional:** To view SVMs that do not have the required permissions, click **Navigate to the source cluster**, and then provide the required permissions.
5. From the **Destination Storage Virtual Machine** pane, specify the name of the SVM that will be created on the destination cluster.
6. Select the option to copy the source SVM configuration.
7. **Optional:** Click ⚙, update the protection policy and protection schedule, select aggregate, and then initialize the protection relationship.
8. Click **Save** to create the SVM relationship.

   The SVM Relationships: Summary window is displayed.

9. Click **Done** to complete the process.

Edit SVM relationships

You can use System Manager to modify the properties of an SVM relationship.

Steps

1. Click **Protection** > **SVM Relationship**.

2. Select the SVM relationship that you want to modify, and then click **Edit**.
3. Select the SVM relationship type.

   If the SVM relationships were created before ONTAP 9.3, then changing the SVM relationship type from mirror to mirror and vault is not allowed.

4. Modify the protection policy, the protection schedule, and the option to copy the source SVM configuration, as required.
5. Click **Save** to save the changes.

Manage SVM relationships

You can use System Manager to perform various operations on SVM relationships such as initializing SVM relationships, updating SVM relationships, activating the destination SVM, resynchronizing data from the source SVM, resynchronizing data from the destination SVM, and reactivating the source SVM.

Before you begin

- To initialize the SVM relationship, the source and destination clusters must be in a healthy peer relationship.
- To update the SVM relationship, the SVM relationship must be initialized and in a Snapmirrored state.
- To reactivate the source SVM, the resynchronize data from the destination SVM (reverse resync) operation must have been performed.
- If you had selected the option to copy the source SVM configuration while creating the SVM relationship, then to activate the SVM relationship, the source SVM must be stopped.
- SnapMirror license must be enabled on the source cluster and destination cluster.
- The source cluster and destination cluster must be in a healthy peer relationship.
- The destination cluster must have space available.
- The source SVM must have permission for SVM peering.
- You must break the SVM relationship to activate destination SVM, resync from source SVM, resync from destination SVM (Reverse Resync), and reactivate source SVM.
- To reactivate the source SVM, the SVM reverse relationship must exist and be in a Snapmirrored state.

Steps

1. Click **Protection** > **SVM Relationship**.
2. Select the SVM relationship, and then perform the appropriate action:

If you want to…	Do the following…
Initialize the SVM relationship	a. Click **Operations** > **Initialize**. The Initialize dialog box is displayed. b. Click **Initialize**.

If you want to…	Do the following…
Update the SVM relationship	a. Click **Operations** > **Update**. The Update dialog box is displayed. b. Click **Update**.
Activate the destination SVM Activating the destination SVM involves quiescing scheduled SnapMirror transfers, aborting any ongoing SnapMirror transfers, breaking the SVM relationship, and starting the destination SVM.	a. Click **Operations** > **Activate Destination SVM**. The Activate Destination SVM dialog box is displayed. b. Select the **Ok to activate destination SVM and break the relationship** checkbox. c. Click **Activate**.
Resynchronize data from the source SVM The resync operation performs a rebaseline of the SVM configuration. You can resync from the source SVM to reestablish a broken relationship between the two SVMs. When the resync is complete, the destination SVM contains the same information as the source SVM and is scheduled for further updates.	a. Click **Operations** > **Resync from Source SVM**. The Resync from Source SVM dialog box is displayed. b. Select the **Ok to delete any newer data in the destination SVM** checkbox. c. Click **Resync**.
Resynchronize data from the destination SVM (Reverse Resync) You can resync from the destination SVM to create a new relationship between the two SVMs. During this operation, the destination SVM continues to serve data with the source SVM backing up the configuration and data of the destination SVM.	a. Click **Operations** > **Resync from Destination SVM (Reverse ReSync)**. The Resync from Destination SVM (Reverse Resync) dialog box is displayed. b. If the SVM has multiple relationships, select the **This SVM has multiple relationships, Ok to release to other relationships** checkbox. c. Select the **Ok to delete the new data in the source SVM** checkbox. d. Click **Reverse Resync**.
Reactivate the source SVM Reactivating the source SVM involves protecting and recreating the SVM relationships between the source and destination SVM. If you had selected the option to copy the source SVM configuration while creating the SVM relationship, then the destination SVM will stop processing data.	a. Click **Operations** > **Reactivate Source SVM**. The Reactivate Source SVM dialog box is displayed. b. Click **Initiate Reactivation** to initiate reactivation to the destination SVM. c. Click **Done**.

SVM Relationships Window

You can use the SVM Relationships window to create and manage mirror relationships, and mirror and vault relationships between SVMs.

Command buttons

- **Create**

  Opens the SVM Disaster Recovery page, which you can use to create a mirror relationship, or mirror and vault relationship from a destination volume.

- **Edit**

  Enables you to edit the schedule and policy of a relationship.

  For mirror and vault relationship, or version-flexible mirror relationship, you can modify the relationship type by modifying the policy type.

- **Delete**

  Enables you to delete a relationship.

- **Operations**

  Provides the following options:

  - **Initialize**

    Enables you to initialize the SVM relationship to perform a baseline transfer from the source SVM to the destination SVM.

  - **Update**

    Enables you to update data from the source SVM to the destination SVM.

  - **Activate Destination SVM**

    Enables you to activate the destination SVM.

  - **Resync from Source SVM**

    Enables you to initiate resynchronization of a broken relationship.

  - **Resync from Destination SVM (Reverse Resync)**

    Enables you to resynchronize the relationship from the destination SVM to the source SVM.

  - **Reactivate Source SVM**

    Enables you to reactivate the source SVM.

- **Refresh**

  Updates the information in the window.

SVM relationships list

- **Source Storage Virtual Machine**

  Displays the SVM that contains the volume from which data is mirrored and vaulted in a relationship.

- **Destination Storage Virtual Machine**

  Displays the SVM that contains the volume to which data is mirrored and vaulted in a relationship.

- **Is Healthy**

  Displays whether the relationship is healthy or not.

- **Relationship State**

  Displays the state of the relationship, such as Snapmirrored, Uninitialized, or Broken Off.

- **Transfer Status**

  Displays the status of the relationship.

- **Relationship Type**

  Displays the type of relationship, such as mirror, or mirror and vault.

- **Lag Time**

  Lag time is the difference between the current time and the timestamp of the last Snapshot copy that was successfully transferred to the destination system. The lag time will always be at least as much as the duration of the last successful transfer, unless the clocks on the source and destination systems are not synchronized. The time zone difference is automatically calculated into the lag time.

- **Policy Name**

  Displays the name of the policy that is assigned to the relationship.

- **Policy Type**

  Displays the type of policy that is assigned to the relationship. The policy type can be StrictSync, Sync, Asynchronous Mirror, Asynchronous Vault, or Asynchronous Mirror Vault.

Details area

- **Details tab**

  Displays general information about the selected relationship, such as the source cluster and destination cluster, the protection relationship that is associated with the SVM, data transfer rate, state of the relationship, details about the network compression ratio, data transfer status, type of current data transfer, type of last data transfer, latest Snapshot copy, timestamp of the latest Snapshot copy, the status of the identity preserve, and the number of volumes protected.

- **Policy Details tab**

  Displays details about the policy that is assigned to the selected protection relationship.

Manage protection policies with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create, edit, and delete protection policies.

Create protection policies

You can use System Manager to create cluster-level asynchronous mirror policies, vault policies, or mirror and vault policies, and to apply these policies to a cluster-level data protection relationship.

Steps

1. Click **Protection** > **Protection Policies**.
2. Click **Create**.
3. In the **Create Policy** dialog box, select the type of policy that you want to create.
4. Specify the policy name and transfer priority.

   Low indicates that the transfer has the lowest priority. Low priority transfers are usually scheduled after normal priority transfers. By default, the transfer priority is set to Normal.

5. **Optional:** Select the **Enable Network Compression** check box to compress the data that is being transferred during a data transfer.
6. **Optional:** For an asynchronous mirror policy, select the **Transfer All Source Snapshot Copies** check box to include the “all_source_snapshots” rule to the mirror policy, which backs up all of the Snapshot copies from the source volume.
7. **Optional:** Click **Add Comments** to add additional comments for the policy.
8. For a vault policy or mirror vault policy, specify a SnapMirror label and a destination retention count.
9. Click **Create**.

Protection Policies window

You can use the Protection Policies window to create, manage, and display information about mirror, vault, and mirror vault policies.

Command buttons

- **Create**

  Opens the Create Policy dialog box, which enables you to create a mirror, vault, or mirror vault policy.

- **Edit**

  Opens the Edit Policy dialog box, which enables you to edit a policy.

- **Delete**

  Opens the Delete Policy dialog box, which enables you to delete a policy.

- **Refresh**

  Updates the information in the window.

Protection policies list

- **Name**

  Displays the name of the protection policy.

- **Type**

  Displays the policy type, which can be Vault, Mirror Vault, or Asynchronous Mirror.

- **Comment**

  Displays the description specified for the policy.

- **Transfer Priority**

  Displays the data transfer priority, such as Normal or Low.

Details area

- **Policy Details tab**

  Displays details of the protection policy, such as the user who created the policy, number of rules, retention count, and status of network compression.

- **Policy Rules tab**

  Displays details of the rules that are applied to the policy. The Policy Rules tab is displayed only if the selected policy contains rules.

Manage Snapshot policies with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create and manage Snapshot policies in your storage system.

About Snapshot policies

When applied to a volume, a Snapshot policy specifies a schedule or schedules according to which Snapshot copies are created and specifies the maximum number of Snapshot copies that each schedule can create. A Snapshot policy can include up to five schedules.

For vault relationships, the SnapMirror Label attribute is used to select Snapshot copies on the source volumes. Only Snapshot copies with the labels configured in the vault policy rules are replicated in backup vault operations. The Snapshot policy assigned to the source volume must include the SnapMirror Label attribute.

Create Snapshot policies

You can create a Snapshot policy in System Manager to specify the maximum number of Snapshot copies that can be automatically created and the frequency of creating them.

Steps

1. Click **Protection** > **Snapshot Policies**.

2. Click **Create**.
3. In the **Create Snapshot Policy** dialog box, specify the policy name.
4. Click **Add**, and then specify the schedule name, the maximum number of Snapshot copies that you want to retain, and the SnapMirror label name.

   The maximum number of Snapshot copies that can be retained by the specified schedules must not exceed 254.

5. Click **OK**, and then click **Create**.

Edit Snapshot policies

You can modify the details of an existing Snapshot policy, such as the schedule name, SnapMirror label, or the maximum number of Snapshot copies that are created, by using the Edit Snapshot Policy dialog box in System Manager.

Steps

1. Click **Protection** > **Snapshot Policies**.
2. In the **Snapshot Policies** window, select the Snapshot policy that you want to modify and click **Edit**.
3. In the **Edit Snapshot Policy** dialog box, select the schedule that you want to modify and click **Edit**.
4. Click **OK**.
5. Verify the changes you made to the selected Snapshot policy in the **Edit Snapshot Policy** dialog box and click **Save**.

Delete Snapshot policies

You can use System Manager to delete Snapshot policies. If you delete a Snapshot policy that is being used by one or more volumes, Snapshot copies of the volume or volumes are no longer created according to the deleted policy.

Before you begin

You must have dissociated the Snapshot policy from each volume that uses it.

Steps

1. Click **Protection** > **Snapshot Policies**.
2. Select the Snapshot policy and click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

Snapshot Policies window

You can use the Snapshot Policies window to manage Snapshot policy tasks, such as adding, editing, and deleting Snapshot policies.

Command buttons

- **Create**

  Opens the Create Snapshot Policy dialog box, which enables you to add backup schedules and specify the maximum number of Snapshot copies to be retained in a policy.

- **Edit**

  Opens the Edit Snapshot Policy dialog box, which enables you to modify the frequency at which Snapshot copies should be created and the maximum number of Snapshot copies to be retained.

- **Delete**

  Opens the Delete dialog box, which enables you to delete the selected Snapshot policy.

- **View as**

  Enables you to view the Snapshot policies either as a list or as a tree.

- **Status**

  Opens the menu, which you can use to either enable or disable the selected Snapshot policy.

- **Refresh**

  Updates the information in the window.

Snapshot policy list

- **Policy/Schedule Name**

  Specifies the name of the Snapshot policy and the schedules in the policy.

- **Storage Virtual Machine**

  Specifies the name of the storage virtual machine (SVM) to which the Snapshot copies belong.

- **Status**

  Specifies the status of the Snapshot policy, which can be Enabled or Disabled.

- **Maximum Snapshots to be retained**

  Specifies the maximum number of Snapshot copies to be retained.

- **SnapMirror Label**

  Specifies the name of the SnapMirror label attribute of the Snapshot copy generated by the backup schedule.

Manage schedules with System Manager - ONTAP 9.7 and earlier

You can use ONTAP System Manager classic (available in ONTAP 9.7 and earlier) to create and manage schedules in your storage system.

Create schedules

You can create schedules to run a job at a specific time or at regular periods by using System Manager.

About this task

When you create a schedule in a MetroCluster configuration, it is a best practice to create an equivalent schedule on the cluster in the surviving site as well.

Steps

1. Click **Protection** > **Schedules**.
2. Click **Create**.
3. In the **Create Schedule** dialog box, specify the schedule name.
4. Create a schedule based on your requirements:

If you want to create…	Do this…
A daily or a specific schedule on certain days	Select **Basic**, and specify the schedule and recurrence details (in hours and minutes).
A schedule that runs at a specific interval	Select **Interval**, and specify the schedule and recurrence details (in days, hours, and minutes).
A schedule that runs at a specific period	Select **Advanced**, and specify the schedule and recurrence details (in months, days, weekdays, hours, and minutes).

5. Click **Create**.

Edit schedules

You can make changes to a previously created cron schedule or an interval schedule if it does not meet your requirements by using System Manager. You can modify schedule details such as recurring days and hours, interval options, and advanced cron options.

About this task

When you edit a schedule in a MetroCluster configuration, it is a best practice to edit the equivalent schedule on the surviving site cluster as well.

Steps

1. Click **Protection** > **Schedules**.
2. Select the schedule that you want to modify and click **Edit**.
3. In the **Edit Schedule** dialog box, modify the schedule by performing the appropriate action:

If you select the schedule option as…	Do this..
Basic	Specify the recurring days and recurring schedule details.
Interval	Specify the interval options in days, hours, and minutes.
Advanced	Specify the advanced cron options in months, days, week days (if applicable), hours, and minutes.

4. Click **OK**.

Delete schedules

You can use System Manager to delete the schedules that run specific storage management tasks.

Steps

1. Click **Protection** > **Schedules**.
2. Select the schedule that you want to delete and click **Delete**.
3. Select the confirmation check box, and then click **Delete**.

Manage schedules

You can configure many tasks (for instance, volume Snapshot copies and mirror replications) to run on specified schedules. Schedules that are run at specified schedules are known as *cron* schedules because of their similarity to UNIX `cron` schedules. Schedules that are run at intervals are known as *interval* schedules.

You can manage schedules in the following ways:

- Creating a cron schedule or an interval schedule
- Displaying information about all the schedules
- Modifying a cron schedule or an interval schedule
- Deleting a cron schedule or an interval schedule

  You cannot delete a schedule that is currently in use by a running job.

The cluster administrator can perform all the schedule management tasks.

Schedules window

You can use the Schedules window to manage scheduled tasks, such as creating, displaying information about, modifying, and deleting schedules.

Command buttons

- **Create**

  Opens the Create Schedule dialog box, which enables you to create time-based and interval schedules.

- **Edit**

  Opens the Edit Schedule dialog box, which enables you to edit the selected schedules.

- **Delete**

  Opens the Delete Schedule dialog box, which enables you to delete the selected schedules.

- **Refresh**

  Updates the information in the window.

Schedules list

- **Name**

  Specifies the name of the schedule.

- **Type**

  Specifies the type of the schedule—time-based or interval-based.

Details area

The details area displays information about when a selected schedule is run.

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

Open source

Provides information about third-party copyright and licenses used in this product.

Notice for ONTAP 9.9.1
Notice for ONTAP 9.8
Notice for ONTAP 9.7
Notice for ONTAP 9.6
Notice for ONTAP 9.5
Notice for ONTAP 9.4
Notice for ONTAP 9.3
Notice for ONTAP 9.2
Notice for ONTAP 9.1

Copyright information

Copyright © 2024 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

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.