Provision NAS storage

System Manager Classic

NetApp
January 13, 2022

Table of Contents

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…	See this content…
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

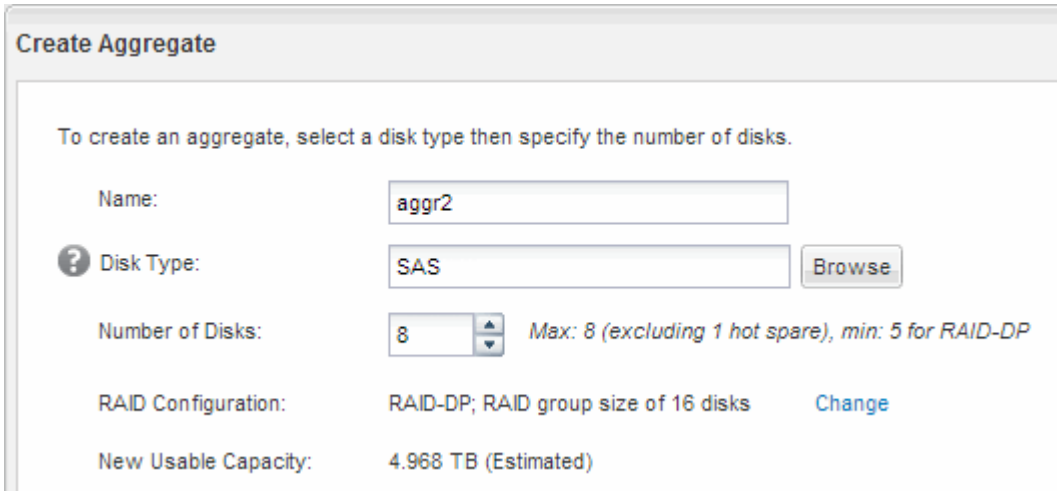
If you do not want to use an existing aggregate, you can create a new aggregate to provide physical storage to the volume which you are provisioning.

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 when you did not follow the procedure in this content 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.

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.

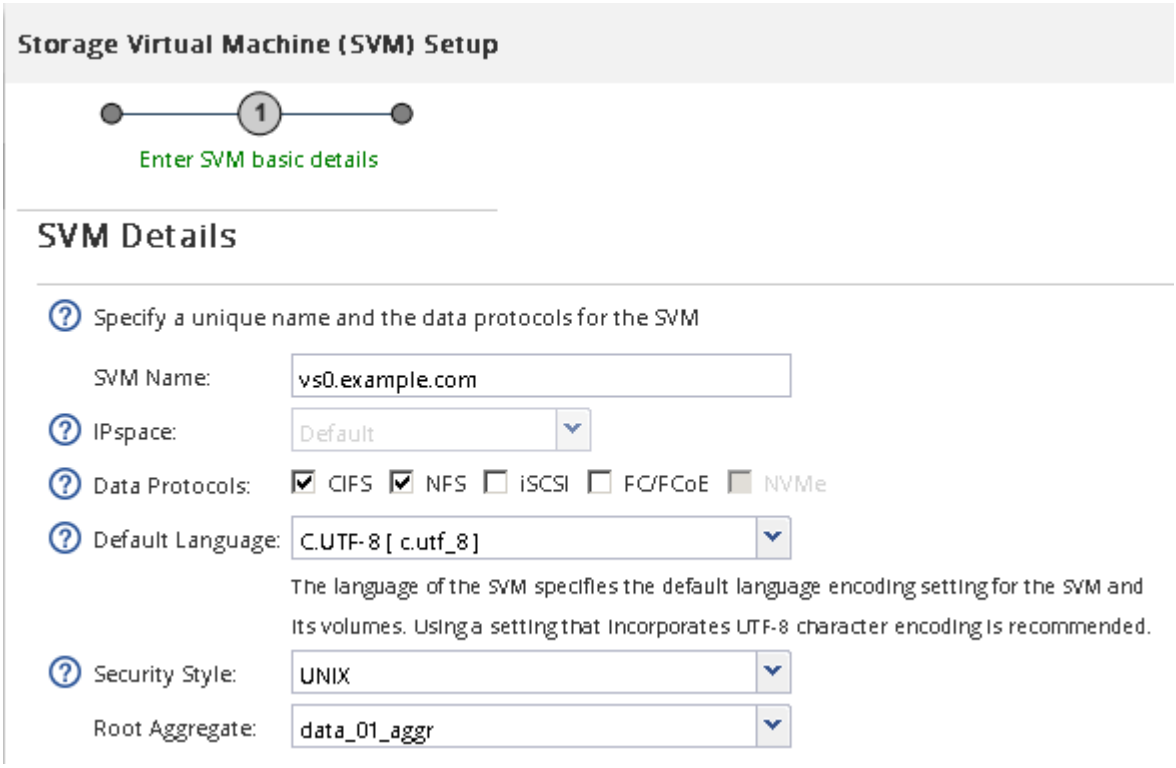
This language is inherited by the volume that you create later, and a volume's language cannot be changed.

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

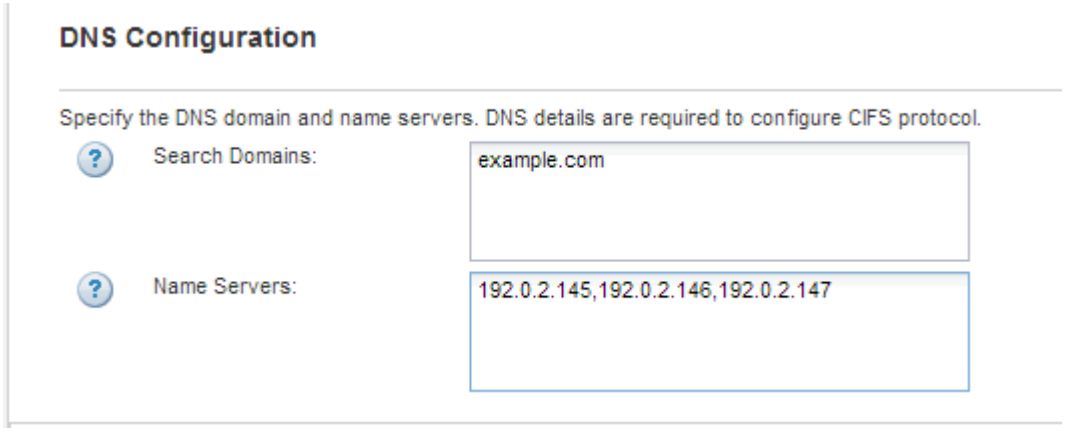
Selecting the CIFS protocol sets the security style to NTFS by default.

e. 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.



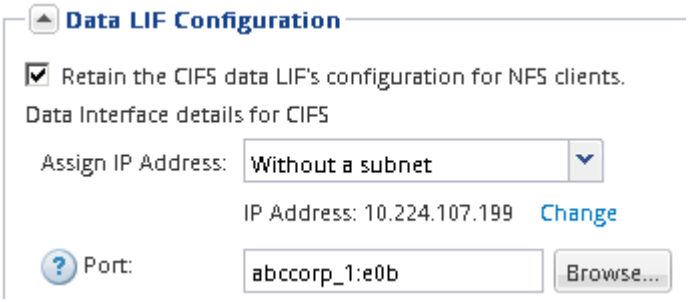
f. In the **DNS Configuration** area, ensure that the default DNS search domain and name servers are the ones that you want to use for this SVM.



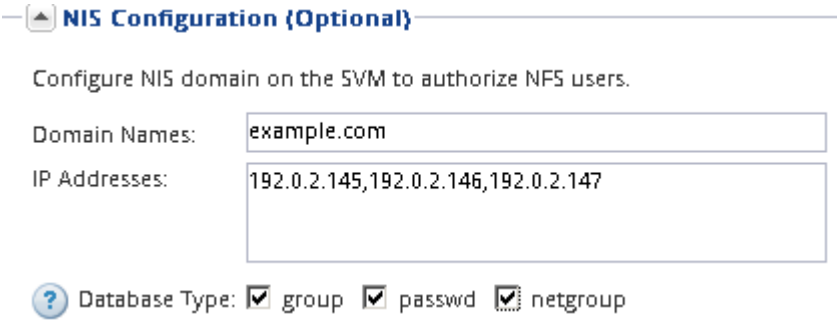
g. Click **Submit & Continue**.

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

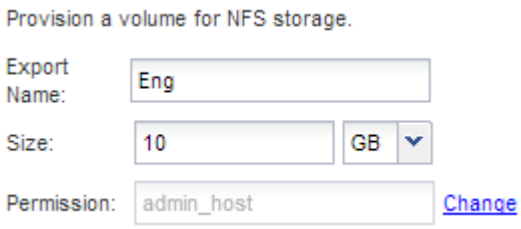
4. In the **Data LIF Configuration** section of the **Configure CIFS/NFS protocol** page, specify the details of the LIF that clients will use to access data:
   a. Assign an IP address to the LIF automatically from a subnet you specify or manually enter the address.
   b. Click **Browse** and select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

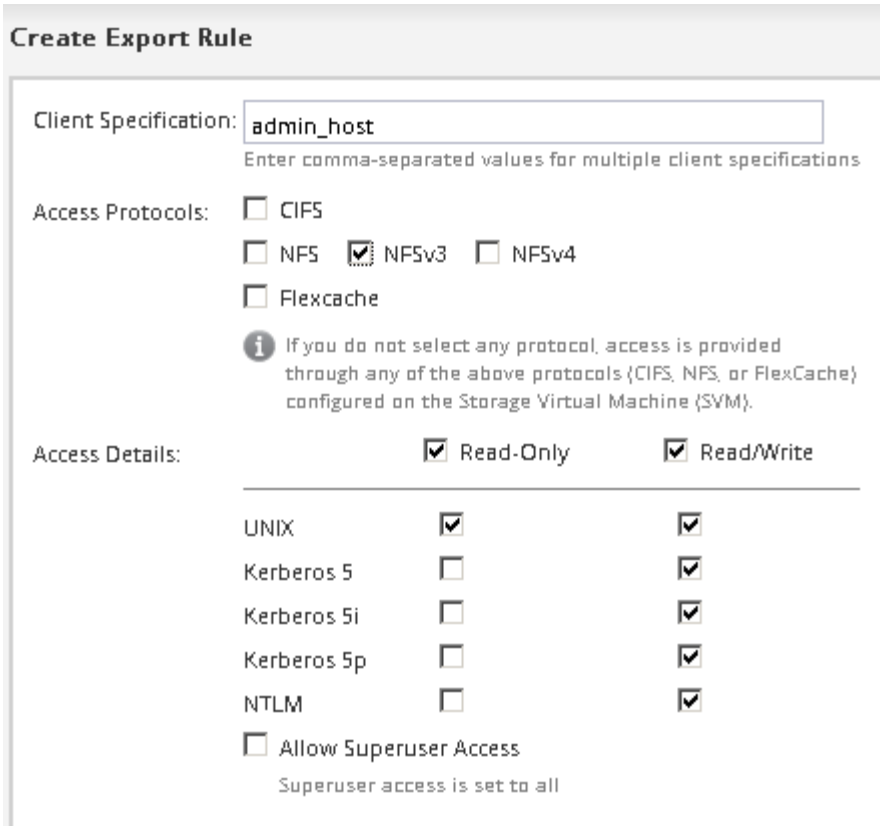


7. Create and export a volume for NFS access:
   a. For **Export Name**, type a name that will be both the export name and the beginning of the volume name.
   b. Specify a size for the volume that will contain the files.



   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)

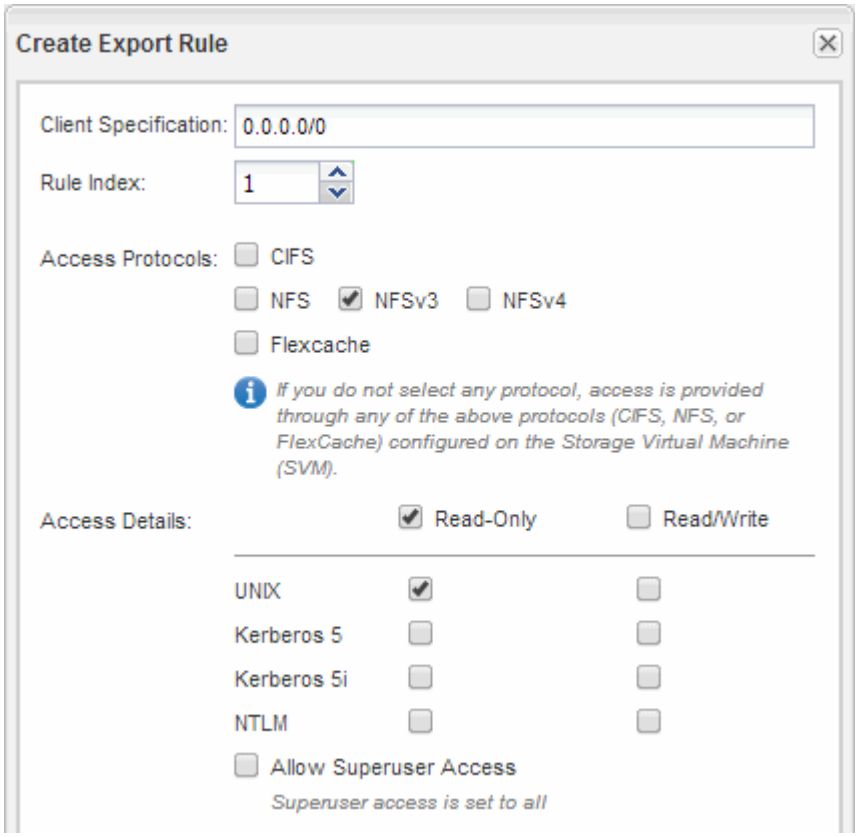
You must add a rule to the default export policy to allow all clients access through NFSv3. Without such a rule, all NFS clients are denied access to the storage virtual machine (SVM) and its volumes.

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

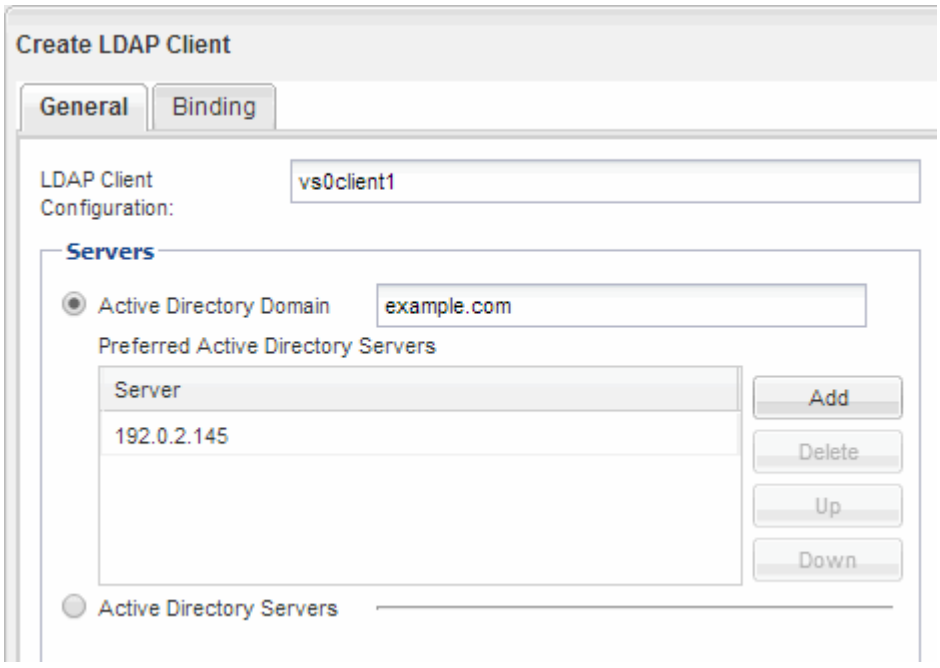
1. Navigate to the **SVMs** window.
2. Select the required SVM
3. Click the **SVM Settings** tab.
4. Set up an LDAP client for the SVM to use:

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

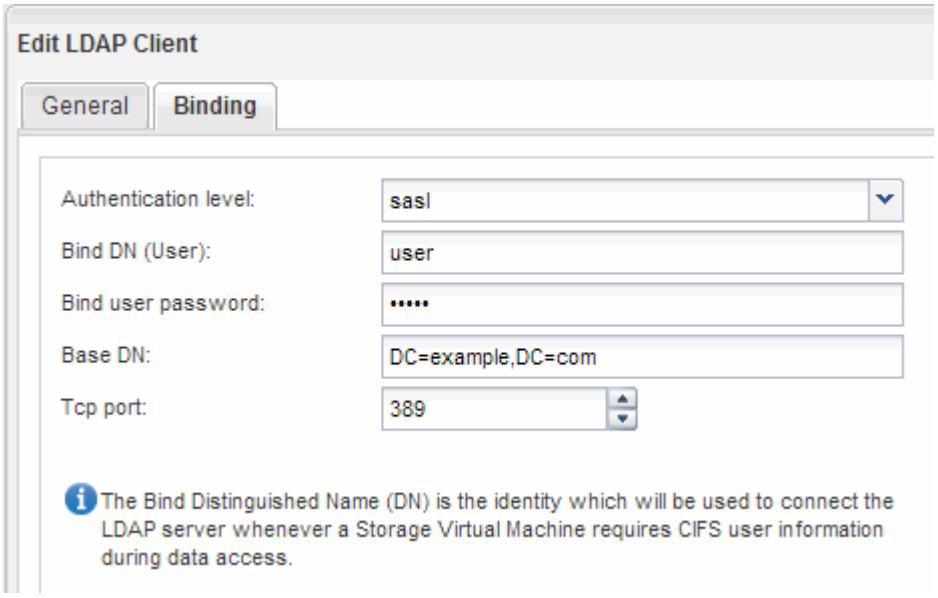
   b. In the **LDAP Client Configuration** window, click **Add**.

   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.

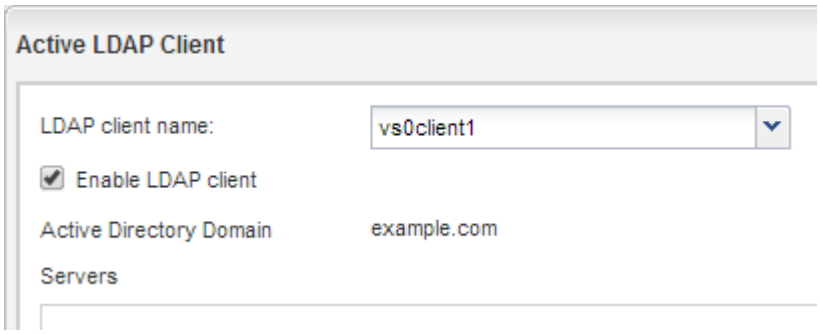
5. Enable the new LDAP client for the SVM:

   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:

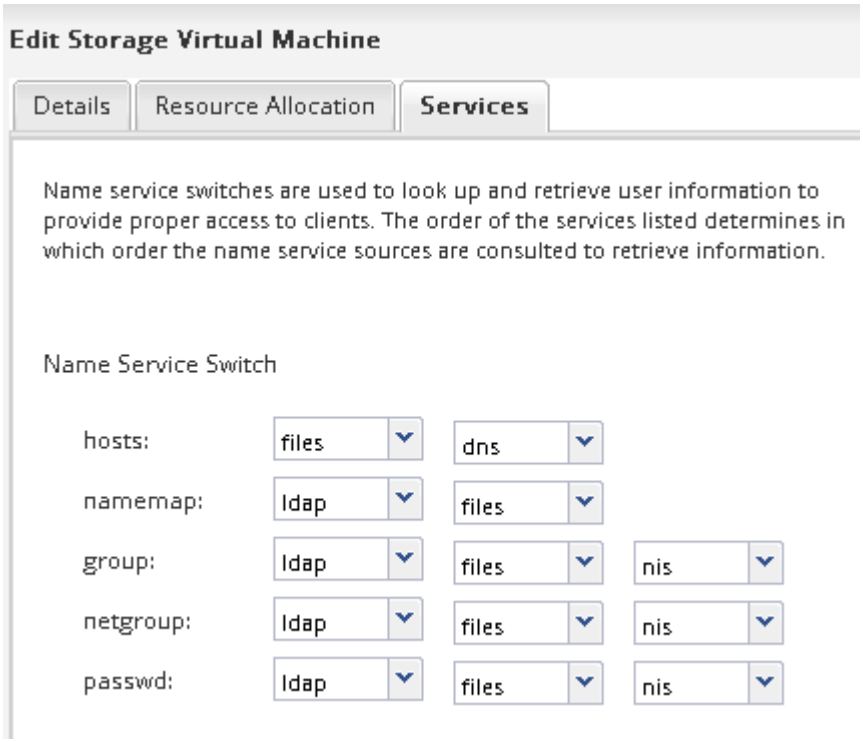
   a. Navigate to the **SVMs** window.

   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

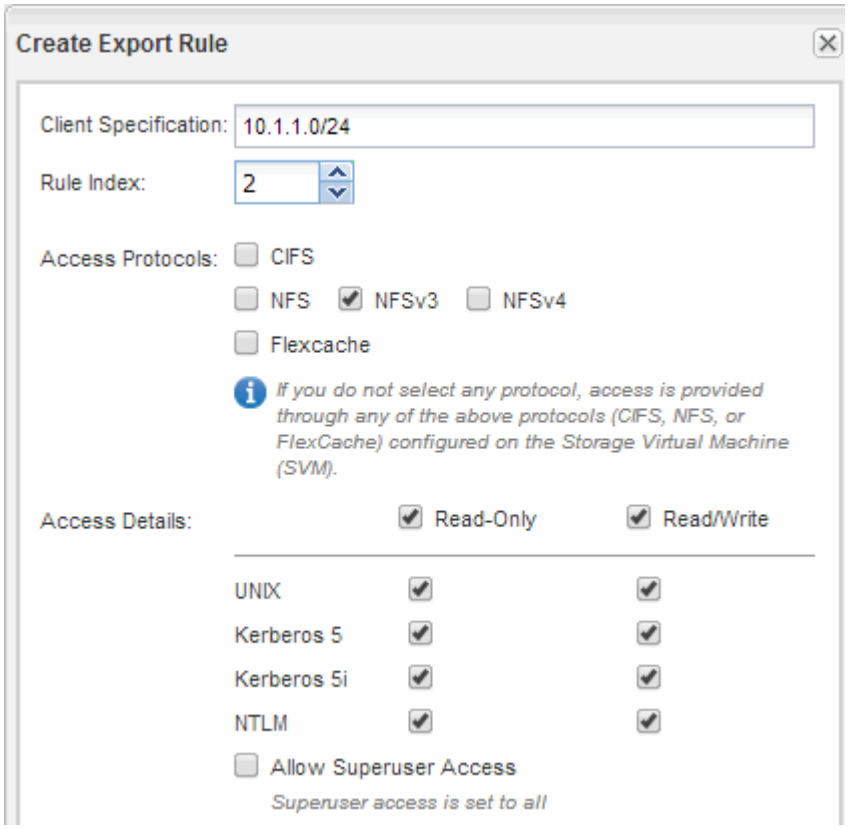
1. Decide which clients and users or groups will be given access to the share.
2. On a UNIX administration host, use the root user to set UNIX ownership and permissions on the volume.
3. In System Manager, add rules to the export policy to permit NFS clients to access the share.
   a. Select the storage 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

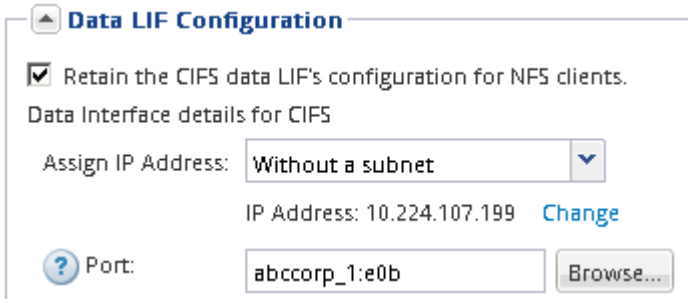
    - The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
- Any external firewalls must be appropriately configured to allow access to network services.
- The NFS protocol must be allowed on the SVM.

For more information, see the Network management documentation.

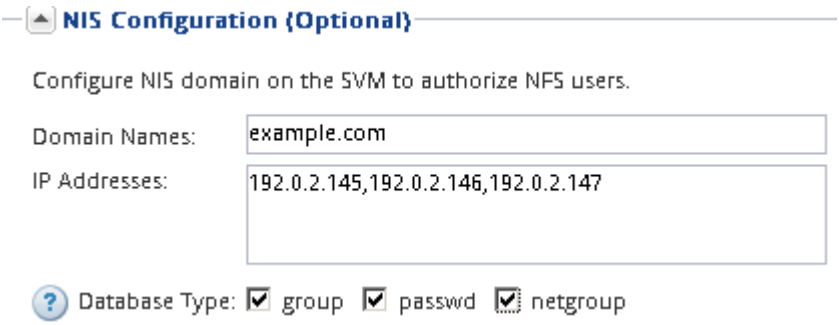
Steps

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.

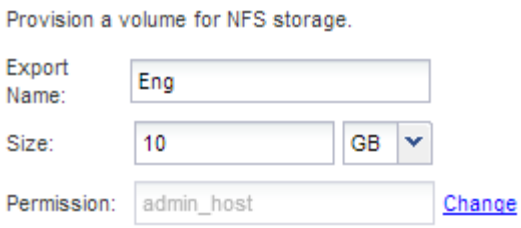


3. If your site uses NIS for name services or name mapping, specify the domain and IP addresses of the NIS servers and select the database types for which you want to add the NIS name service source.



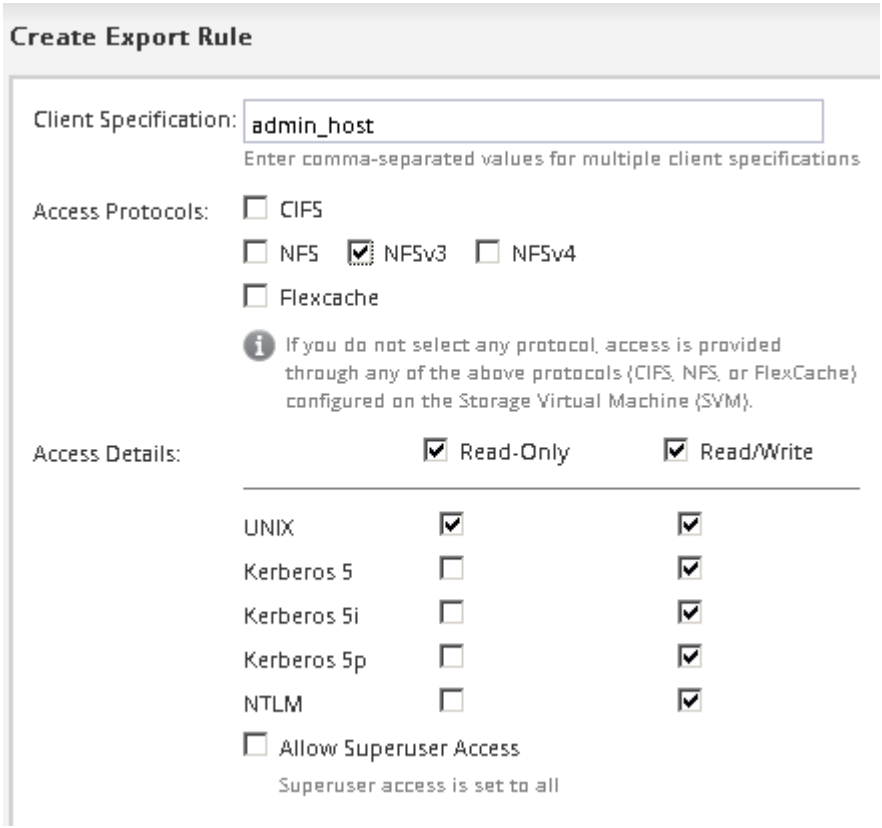
If NIS services are not available, do not attempt to configure it. Improperly configured NIS services can cause datastore access issues.

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)

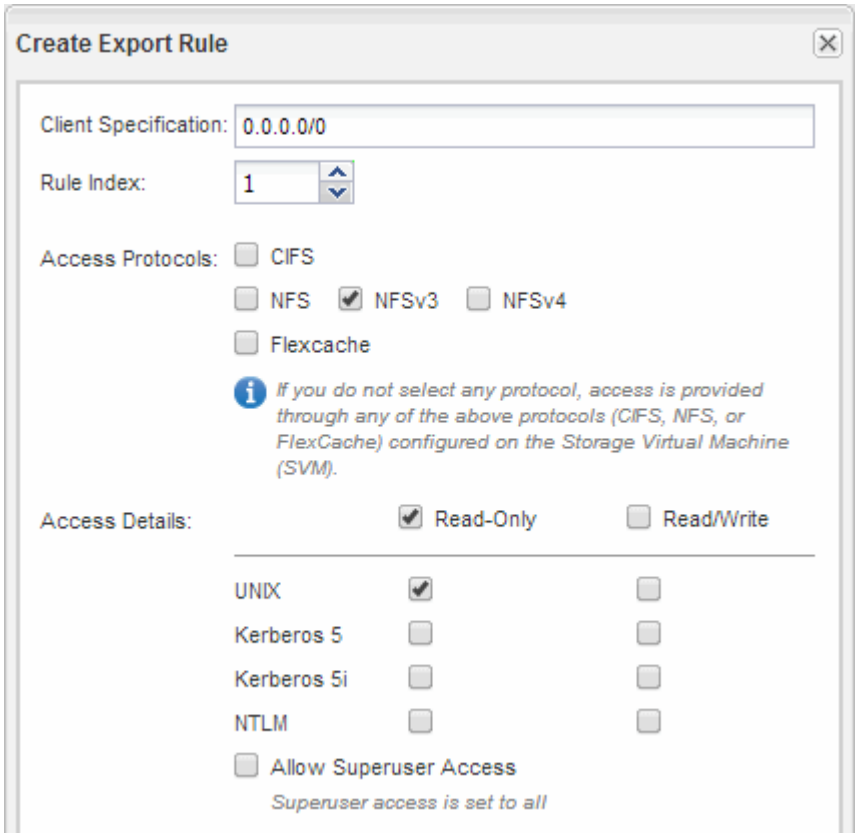
You must add a rule to the default export policy to allow all clients access through NFSv3. Without such a rule, all NFS clients are denied access to the storage virtual machine (SVM) and its volumes.

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

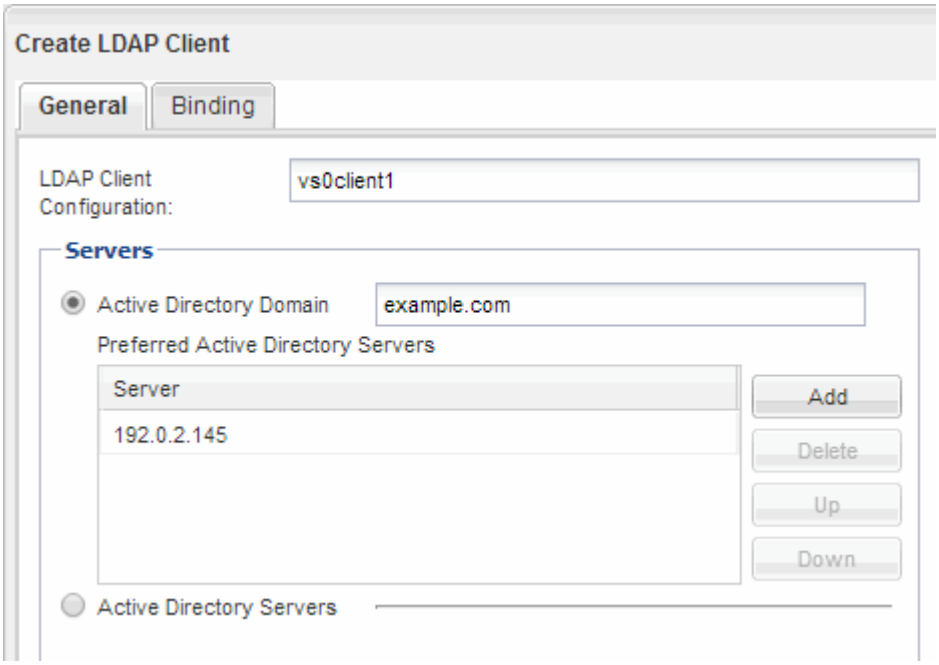
1. Navigate to the **SVMs** window.
2. Select the required SVM
3. Click the **SVM Settings** tab.
4. Set up an LDAP client for the SVM to use:

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

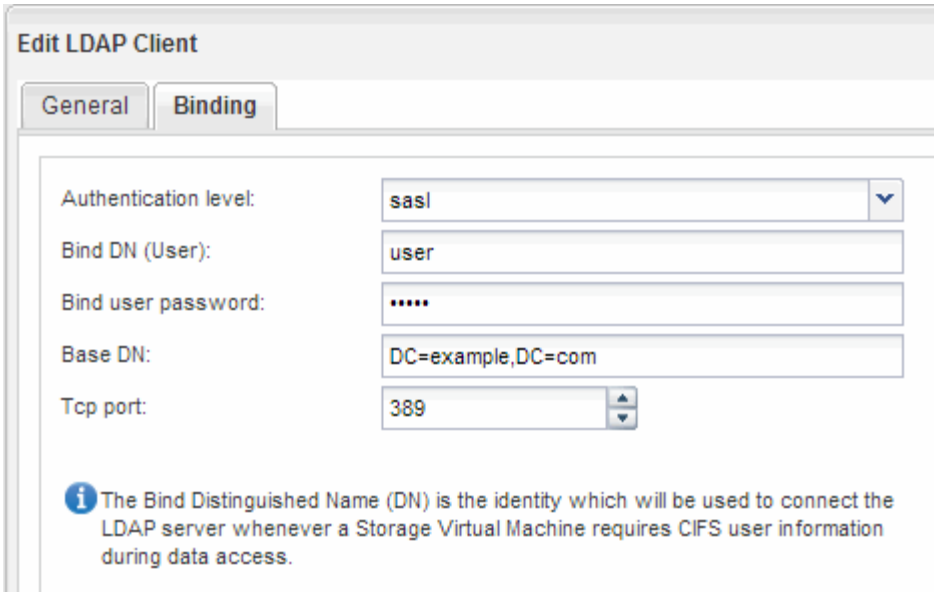
   b. In the **LDAP Client Configuration** window, click **Add**.

   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.

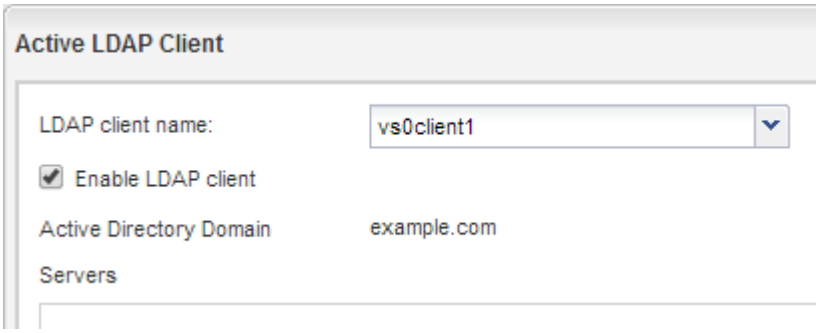
5. Enable the new LDAP client for the SVM:

   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:

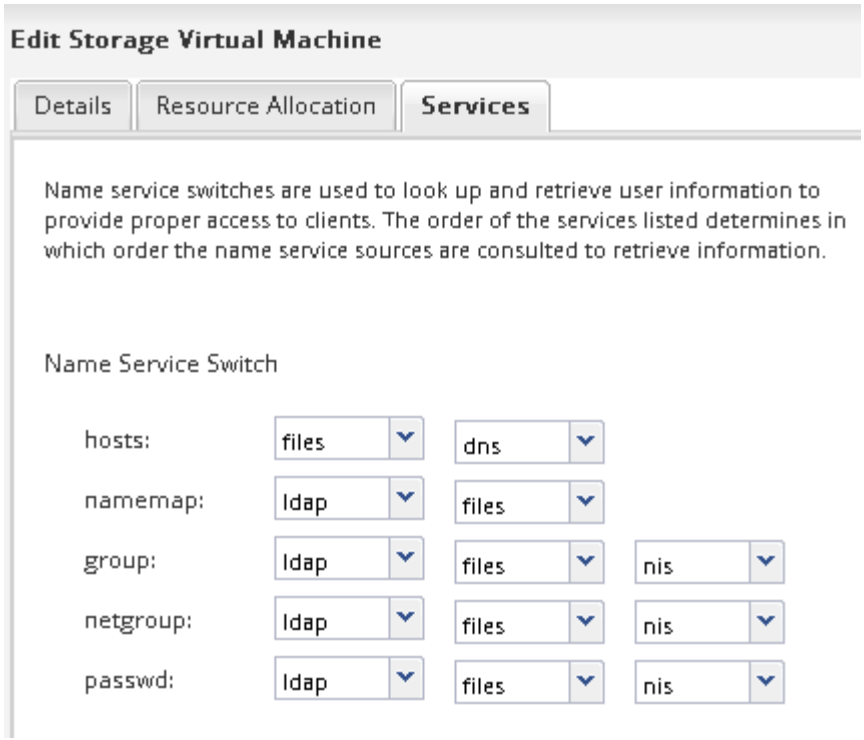
   a. Navigate to the **SVMs** window.

   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

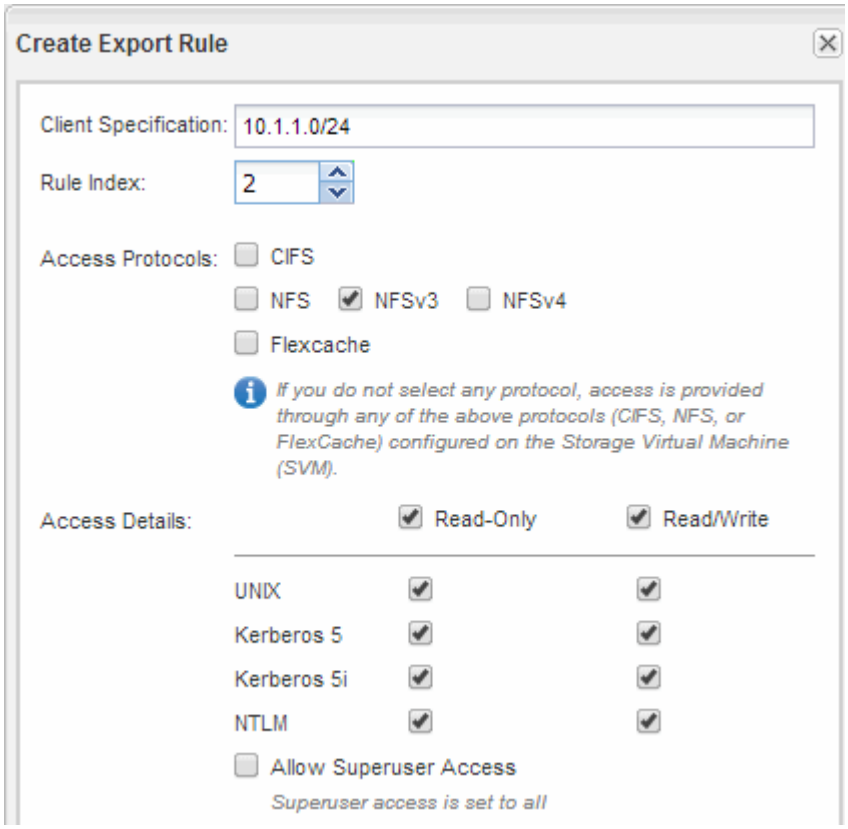
1. Decide which clients and users or groups will be given access to the share.
2. On a UNIX administration host, use the root user to set UNIX ownership and permissions on the volume.
3. In System Manager, add rules to the export policy to permit NFS clients to access the share.
   a. Select the storage 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.

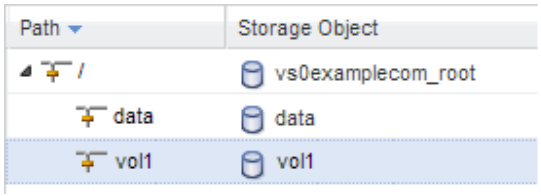
3. If you want to change the default name, which ends in a date and time stamp, specify a new name, such as `vol1`.
4. Select an aggregate for the volume.
5. Specify the size of the volume.
6. Click **Create**.

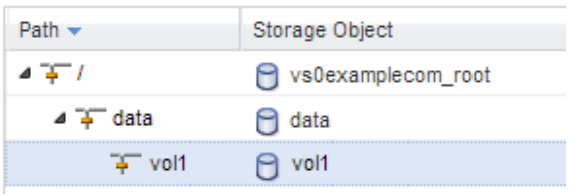
   Any new volume created in System Manager is mounted by default at the root volume using the volume name as the junction name. NFS clients use the junction path and the junction name when mounting the volume.

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.



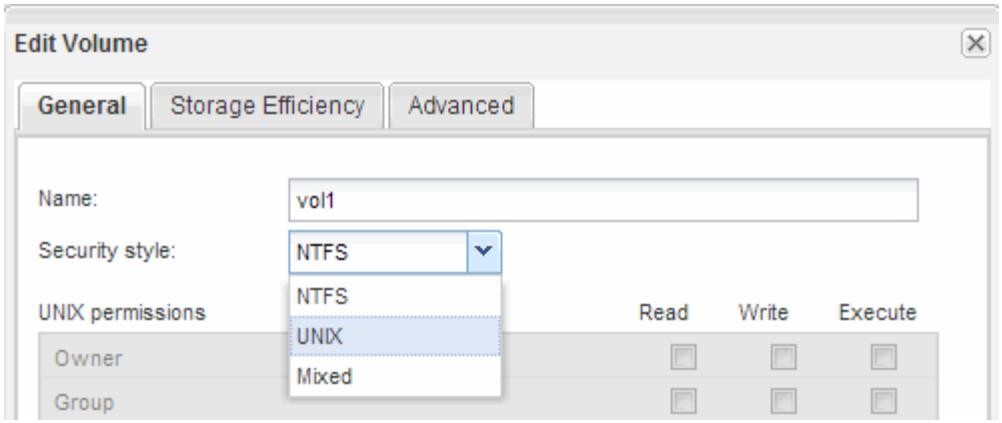


8. Review the volume’s security style and change it, if necessary:

   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.

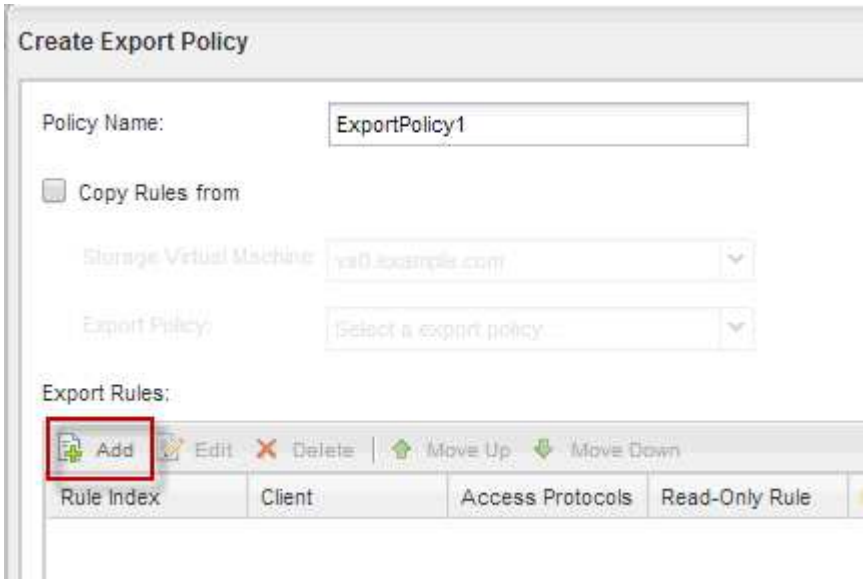


Create an export policy for the volume

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

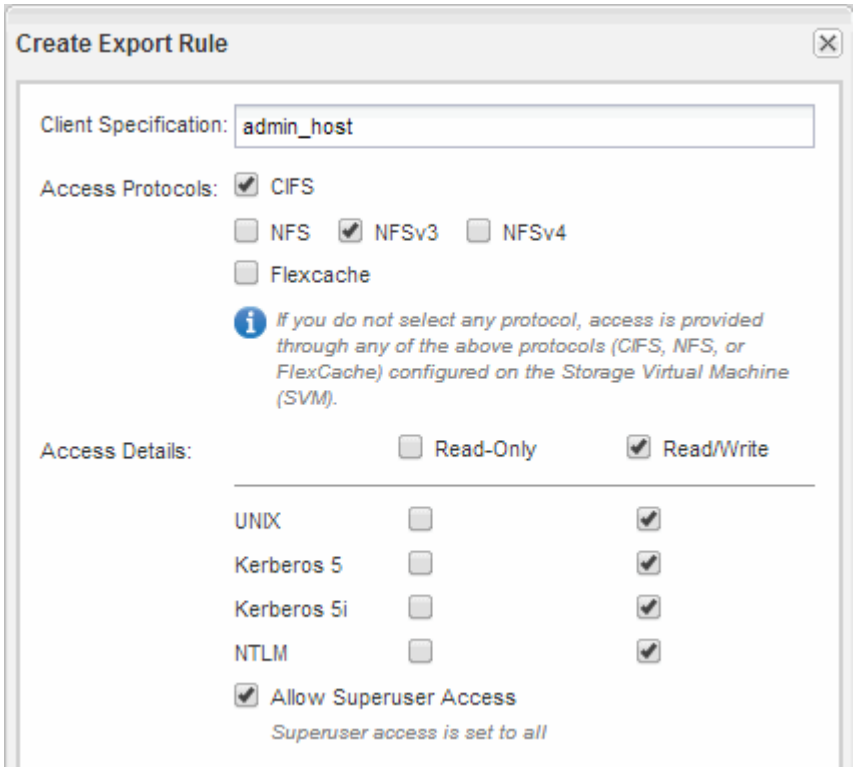
1. Navigate to the **SVMs** window.
2. Click the **SVM Settings** tab.
3. Create a new export policy:
   a. In the **Policies** pane, click **Export Policies** and then click **Create**.
   b. In the **Create Export Policy** window, specify a policy name.
   c. Under **Export Rules**, click **Add** to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

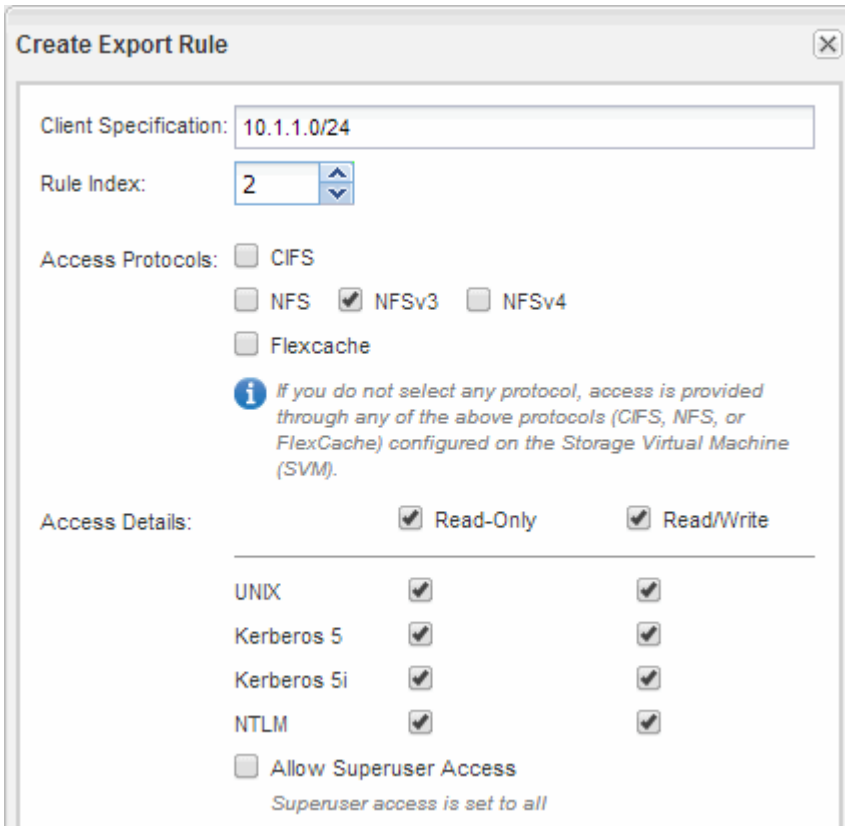
Configure and verify NFS client access (Add an NFS volume to an NFS-enabled SVM)

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

This content describes how to quickly set up NFS access for ESXi hosts to datastores using ONTAP volumes.

You should use this content if you want to configure NFS access for ESXi hosts to a volume in the following way:

- You are working with clusters running ONTAP 9.
- 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 to provision a datastore and create a volume.
- 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

- 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.

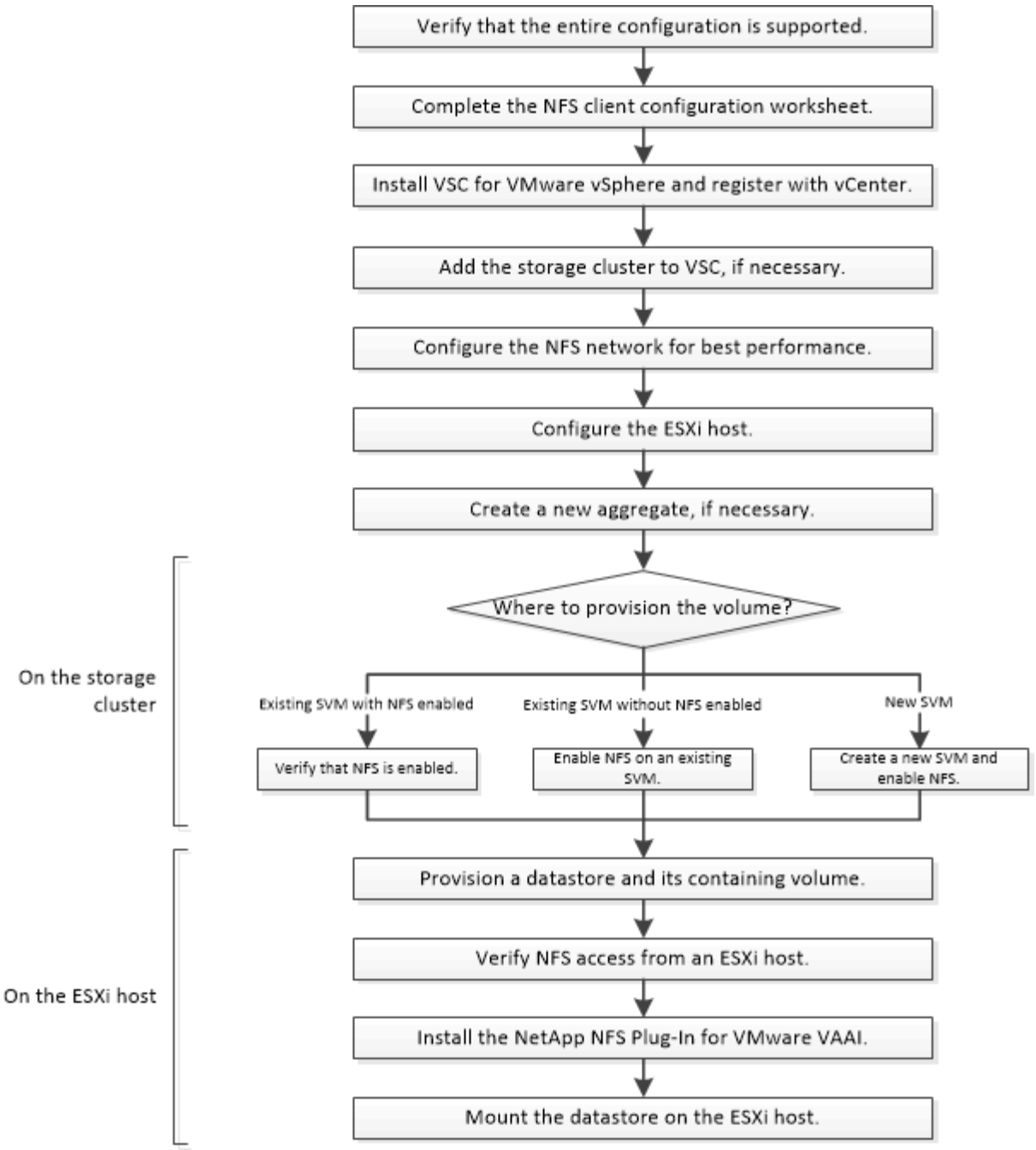
- NFS access will be through NFSv3 and NFSv4 for use with VMware VAAI.

If this content is not suitable for your situation, you should see the following documentation instead:

- NFS management
- NetApp Technical Report 4067: NFS Best Practice and Implementation
- NetApp Technical Report 4668: Name Services Best Practices
- NetApp Technical Report 4597: VMware vSphere with ONTAP

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.

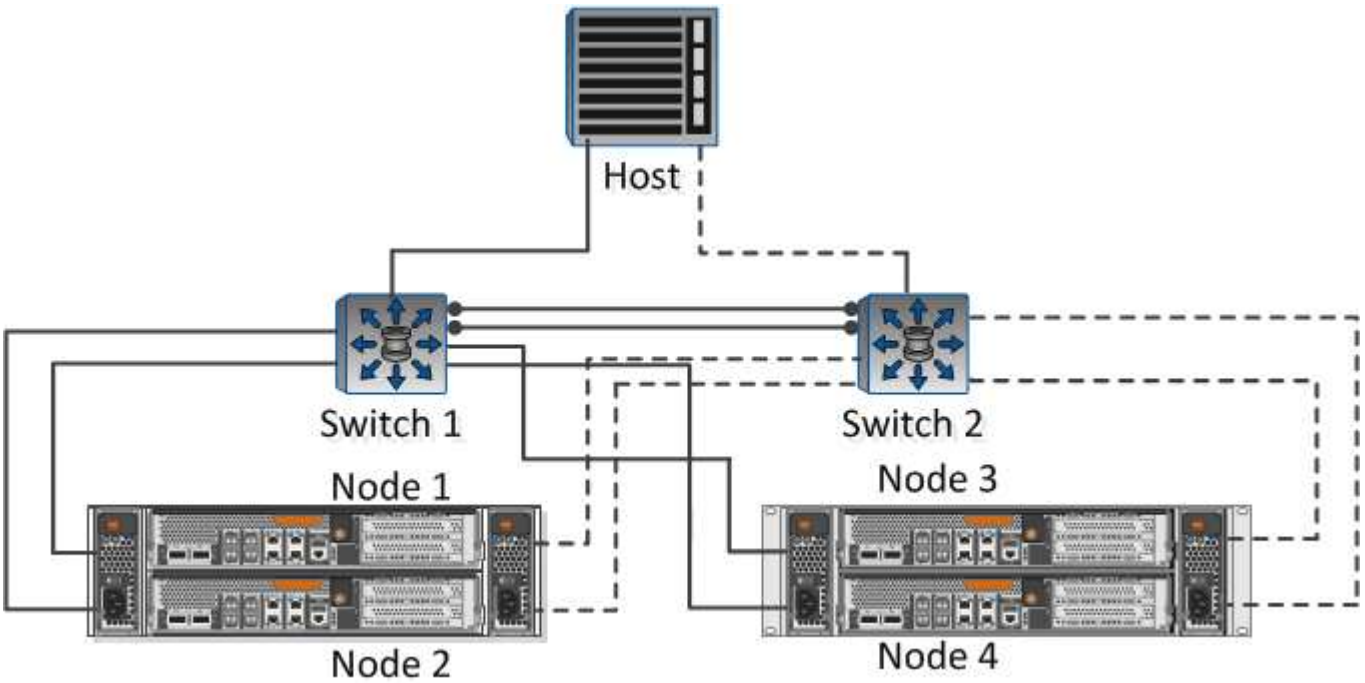
Complete the NFS client configuration worksheet

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)

information

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

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

Install

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

- 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 tool.

   NetApp Support

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

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.

For more information, .

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

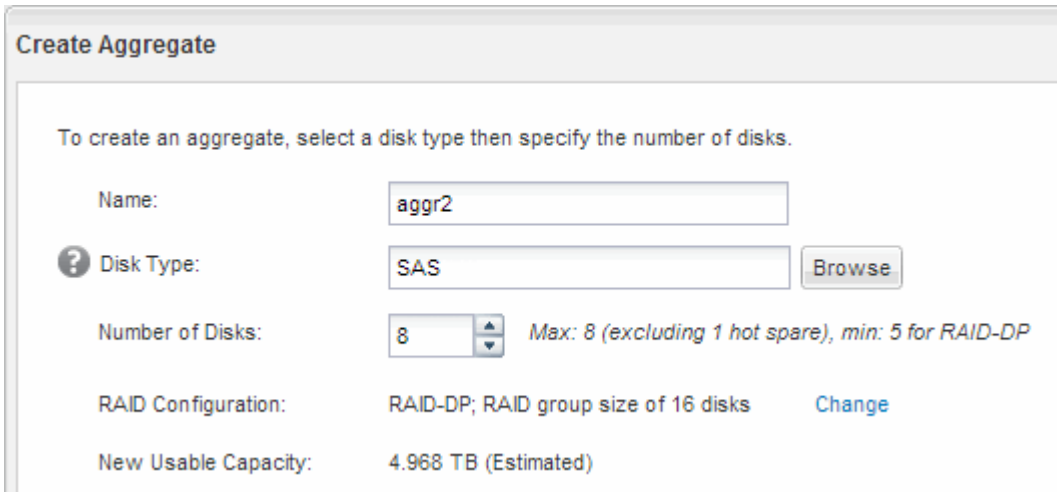
If you have an existing aggregate that you want to use for the new volume, you can skip this procedure.

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 when you followed the procedure in this content 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

Setting up a new 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 :

   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 , you should select them even if you do not want to configure them immediately.

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

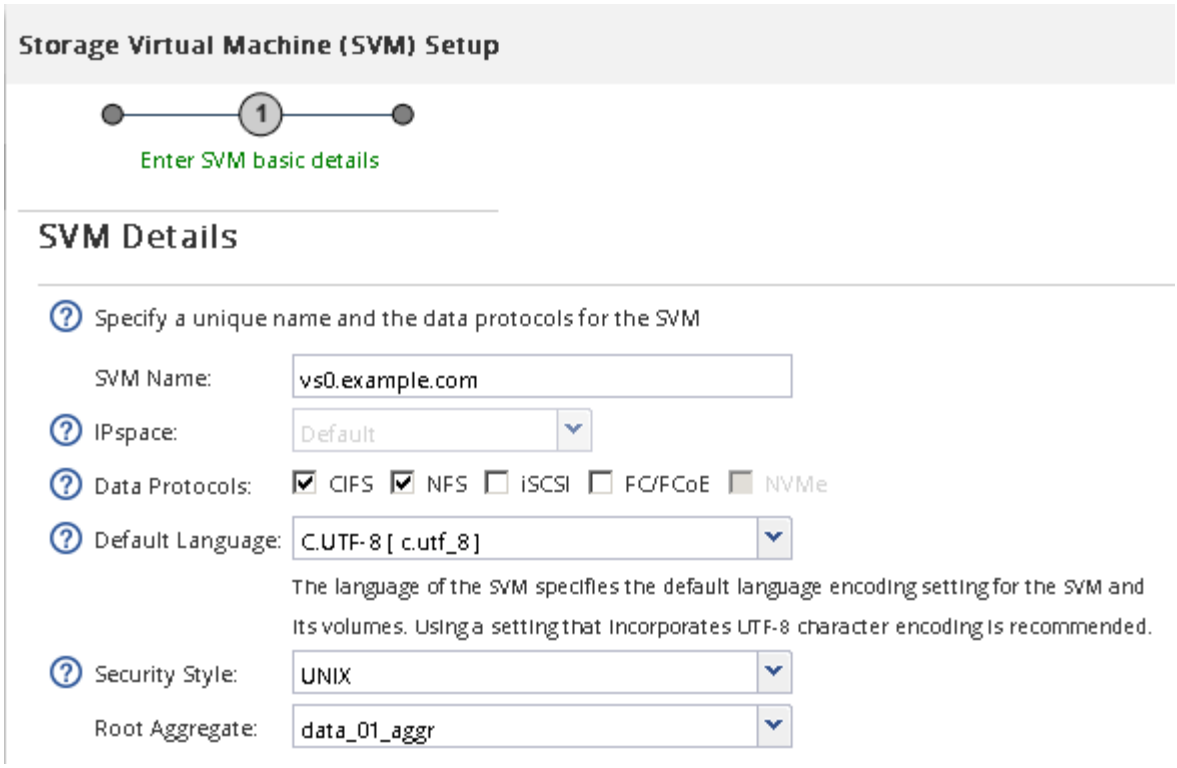
      This language is inherited by the volume that you create later, and a volume's language cannot be changed.

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

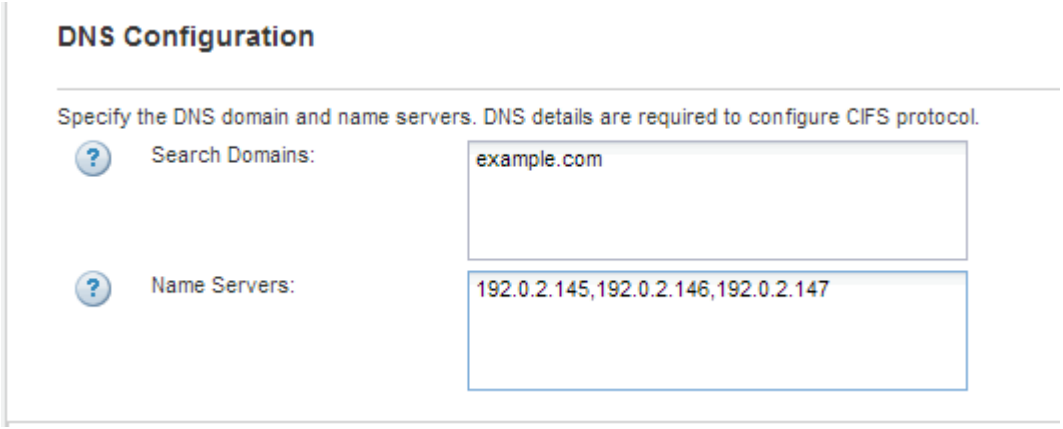
      Selecting the CIFS protocol sets the security style to NTFS by default.

   e. 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. 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.



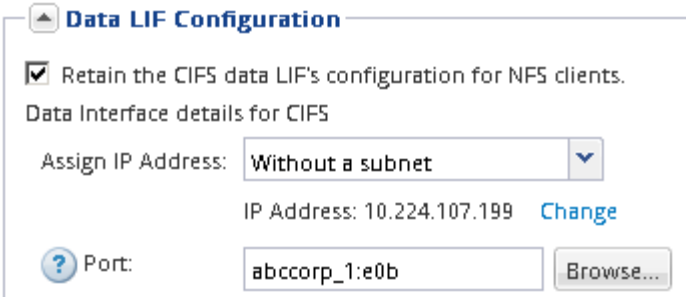
g. Click **Submit & Continue**.

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 is created with NFS enabled.

Add NFS access to an existing

To add NFS access to an existing , 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

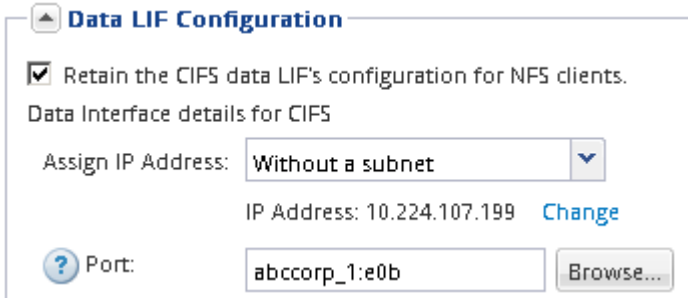
- You must know which of the following networking components the will use:
  - The node and the specific port on that node where the data LIF will be created
  - The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
- 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 when you did not follow the procedure in this content to create the SVM while configuring a different protocol.

Steps

1. Navigate to the **Details** pane where you can configure the protocols of the :
   a. Select the 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

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

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.

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 , 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

Where to find additional information

After you have successfully tested NFS client access, you can perform additional NFS configuration or add SAN access. When protocol access is complete, you should protect the root volume of the . There is comprehensive content and technical reports to help you achieve these goals.

NFS configuration

You can further configure NFS access using the following content and technical reports:

- NFS configuration

  Describes how to use CLI commands to configure advanced NFS client access to files contained in a new volume or qtree.

- NFS management

  Describes how to manage file access using the NFS protocol, including authentication, authorization, and security.

- NetApp Technical Report 4597: VMware vSphere with ONTAP

  Describes the best practices that should be followed when using ONTAP and VMware vSphere server virtualization environments.

- NetApp Technical Report 4668: Name Services Best Practices

  Provides a comprehensive list of best practices, limits, recommendations, and considerations when configuring LDAP, NIS, DNS, and local user and group files for authentication purposes.

- NetApp Technical Report 4067: NFS Best Practice and Implementation

  Provides an overview of ONTAP with a focus on NFSv4.

Root volume protection

After configuring protocols on the SVM, you should ensure that its root volume is protected:

- Data protection

  Describes how to create a load-sharing mirror to protect the root volume, which is a NetApp best practice for NAS-enabled SVMs. Also describes how to quickly recover from volume failures or losses by promoting the SVM root volume from a load-sharing mirror.

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:

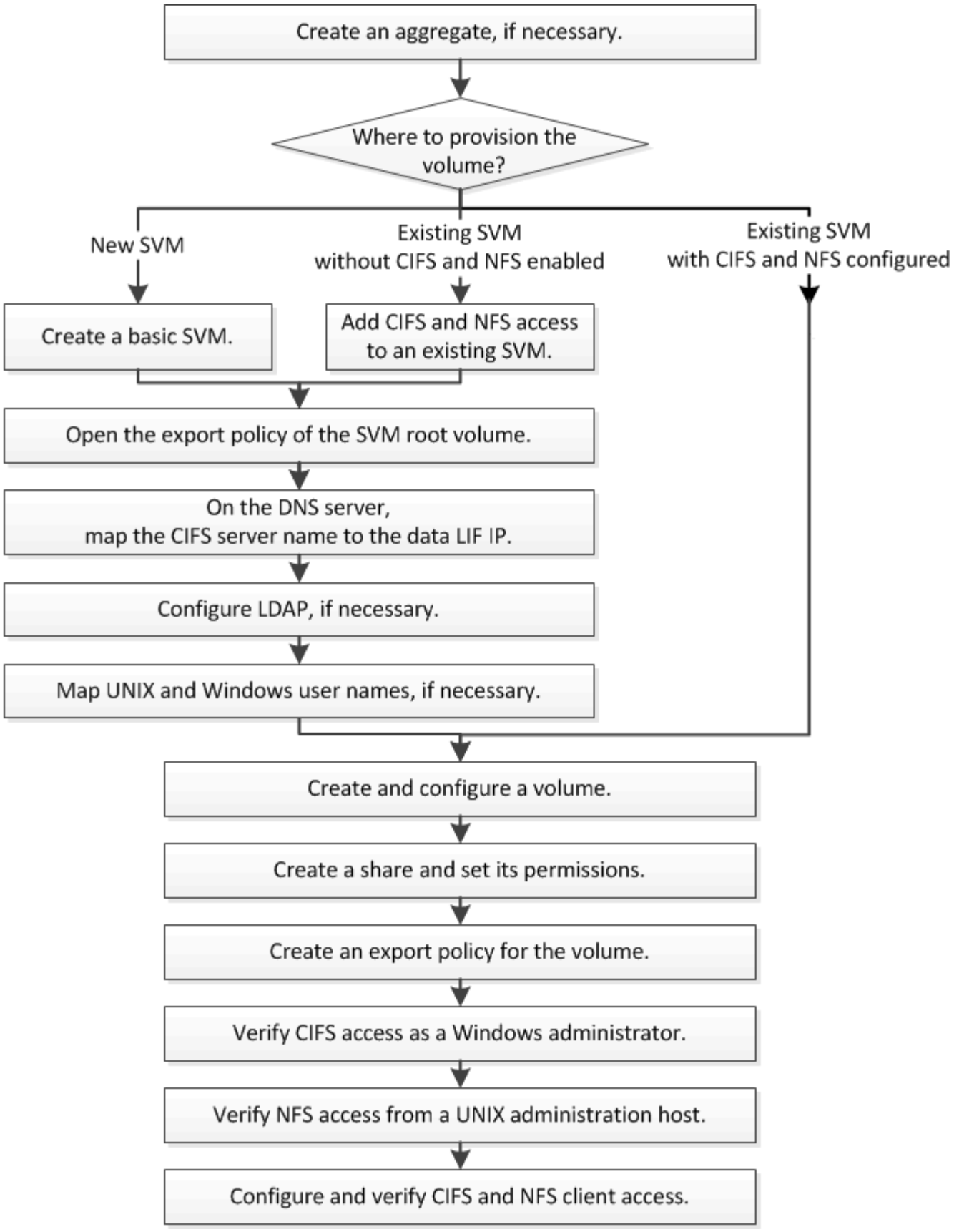
- NFS management
- SMB management

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
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

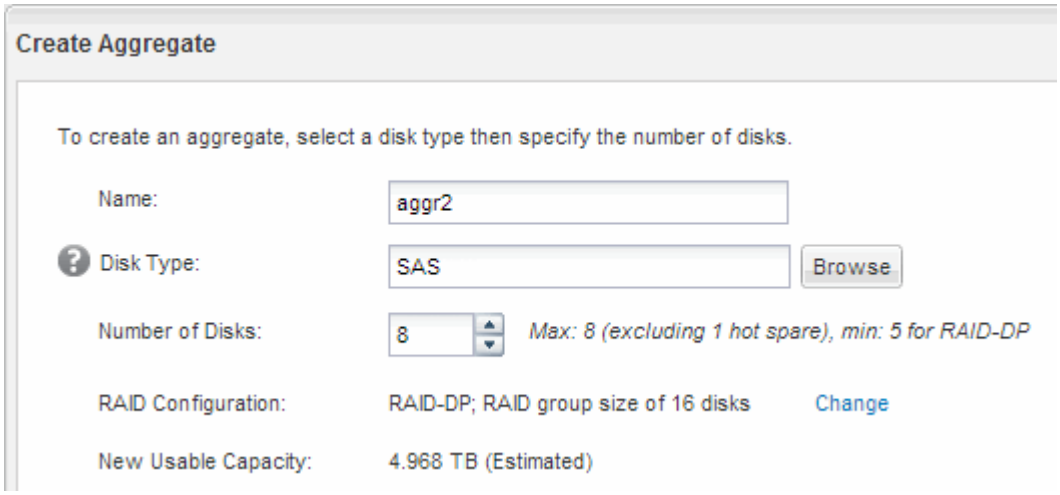
provide physical storage to the volume which you are provisioning.

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.

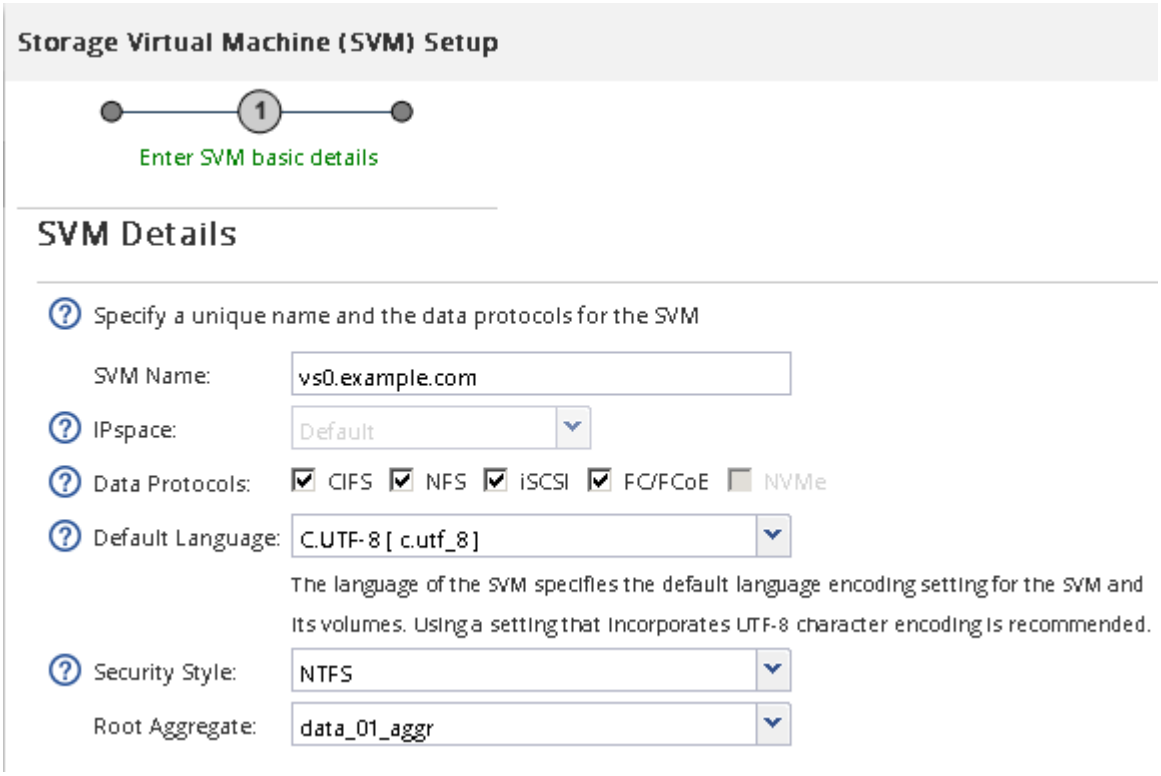
If you support international character display in both NFS and SMB/CIFS clients, consider using the **UTF8MB4** language code, which is available beginning with ONTAP 9.5.

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

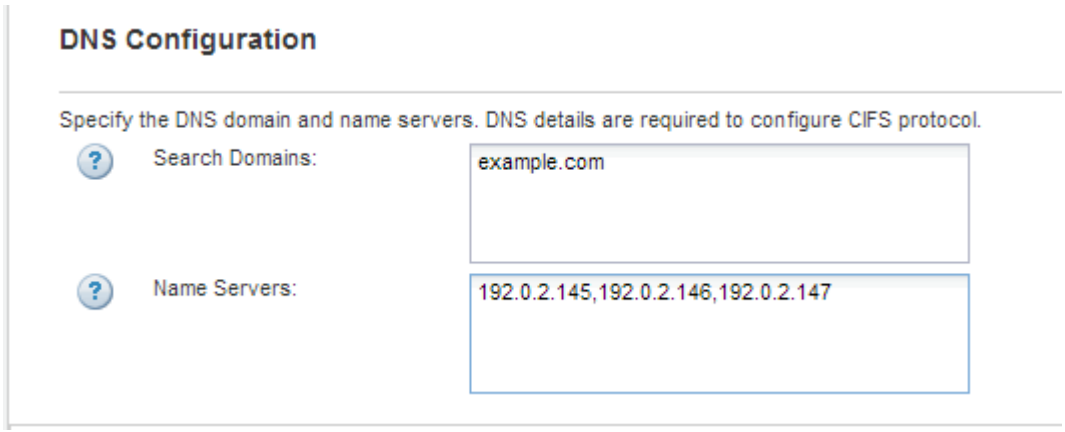
   Selecting the CIFS protocol sets the security style to NTFS by default.

e. 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.



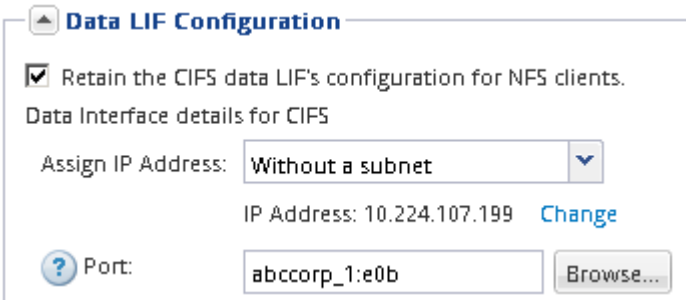
f. In the **DNS Configuration** area, ensure that the default DNS search domain and name servers are the ones that you want to use for this SVM.



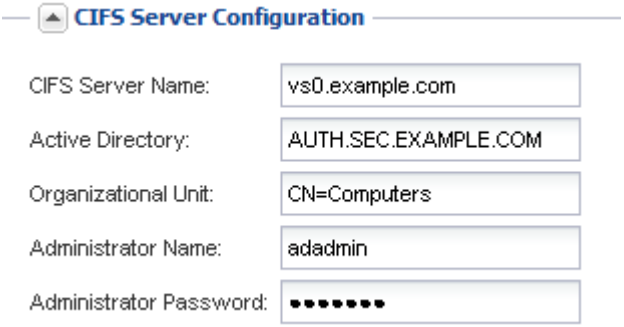
g. Click **Submit & Continue**.

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

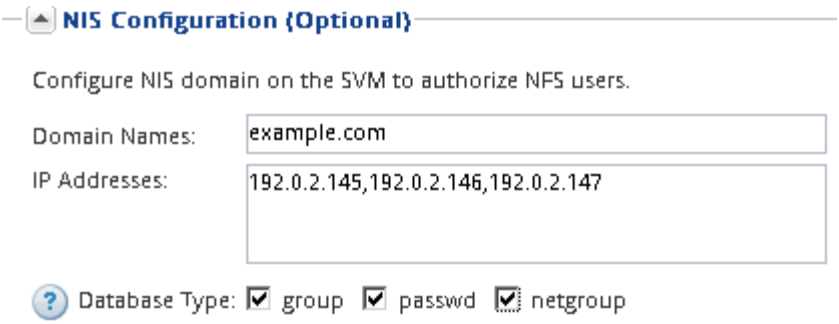
4. In the **Data LIF Configuration** section of the **Configure CIFS/NFS protocol** page, specify the details of the LIF that clients will use to access data:
   a. Assign an IP address to the LIF automatically from a subnet you specify or manually enter the address.
   b. Click **Browse** and select 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 when you did not follow the procedure in this content to create the SVM while configuring a different protocol.

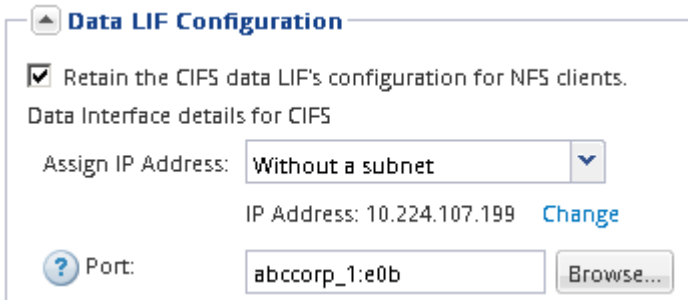
About this task

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

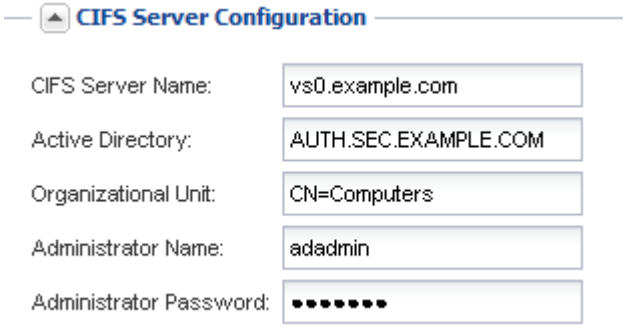
1. Navigate to the area where you can configure the protocols of the SVM:
   a. Select the SVM that you want to configure.
   b. In the **Details** pane, next to **Protocols**, click **CIFS**.

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.

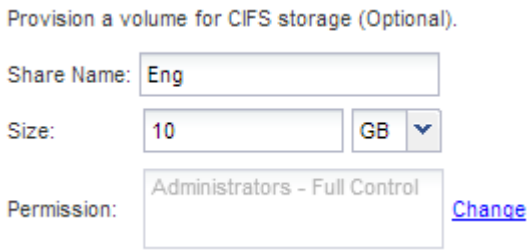


4. Create a volume for CIFS/SMB access and provision a share on it:

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

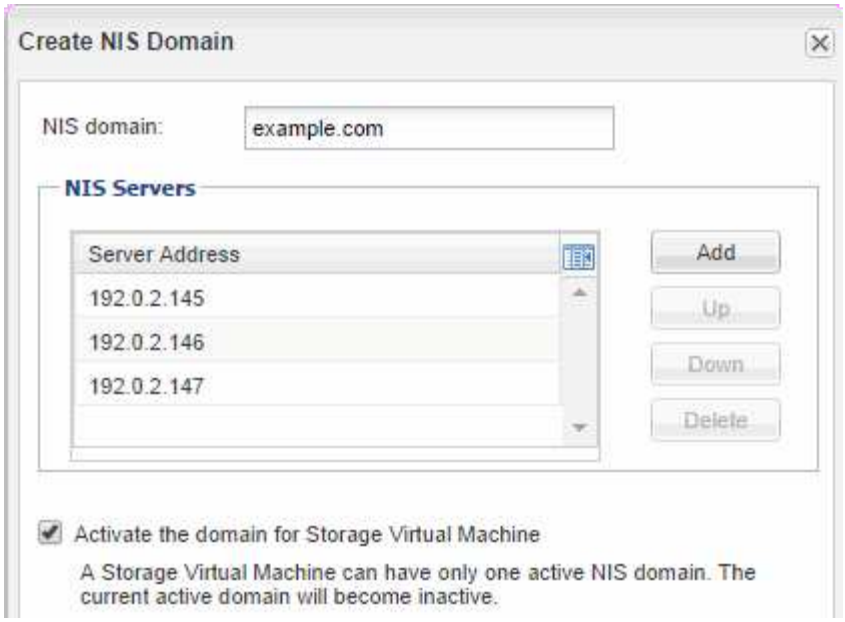
      The name you enter for the share will also be used as the volume name.

   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

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

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

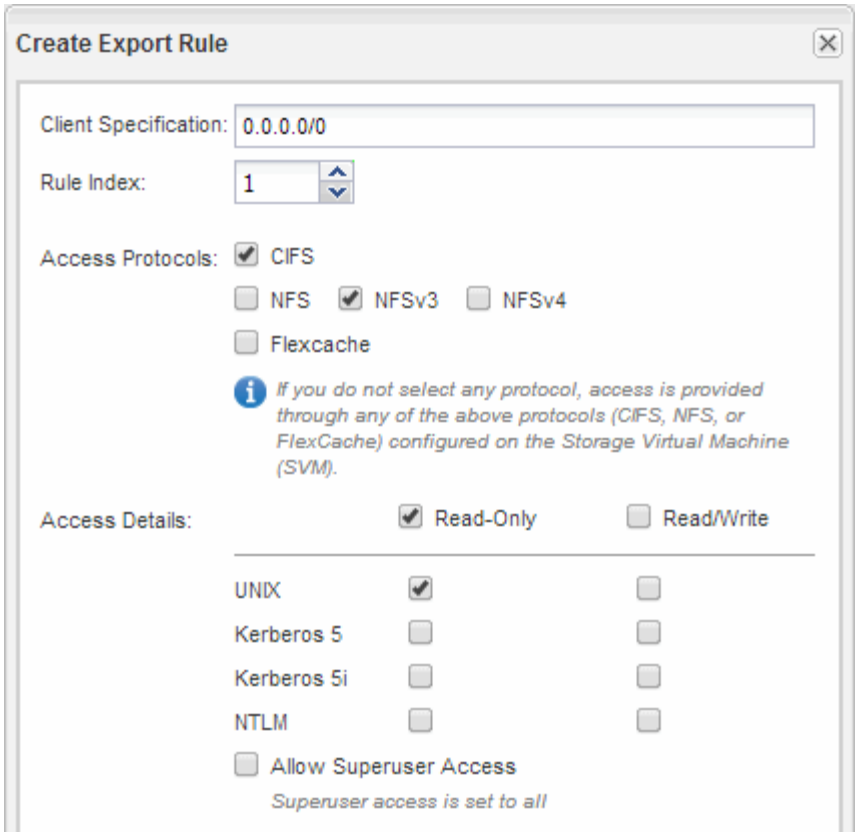
You must add a rule to the default export policy to allow all clients access through NFSv3. Without such a rule, all NFS clients are denied access to the storage virtual machine (SVM) and its volumes.

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

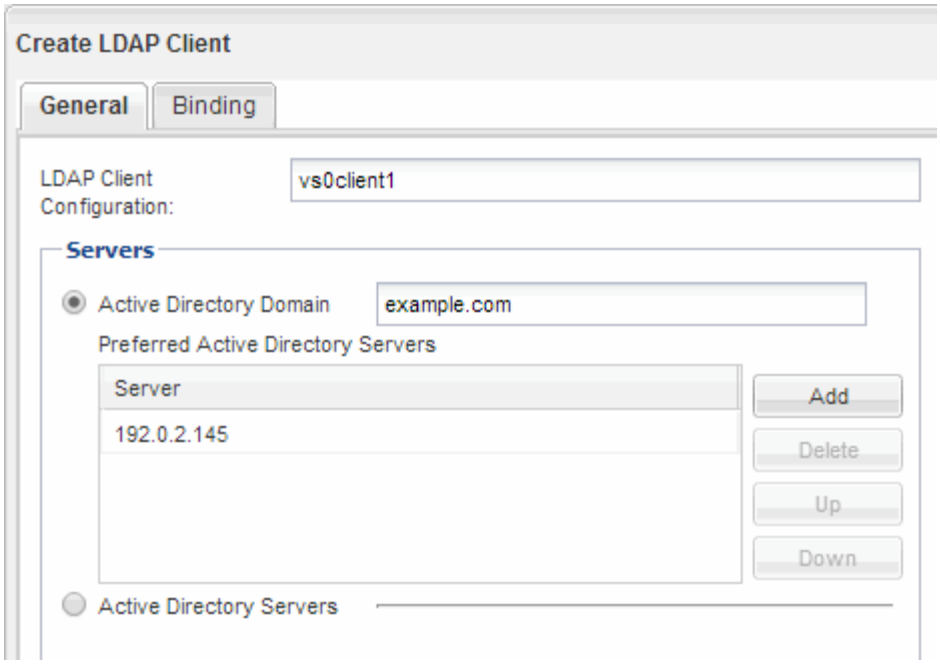
  NetApp Technical Report 4616: NFS Kerberos in ONTAP with Microsoft Active Directory

  NetApp Technical Report 4835: How to Configure LDAP in ONTAP

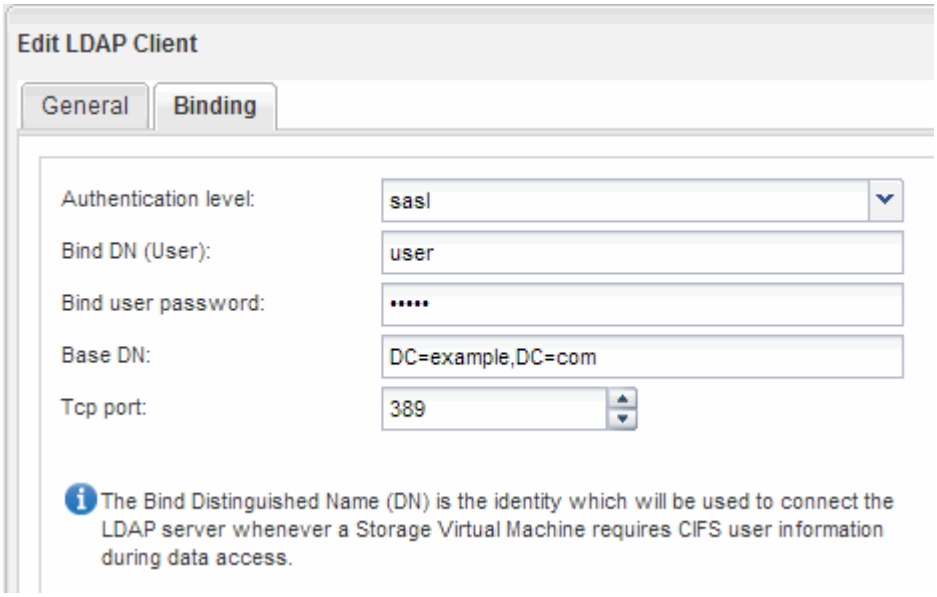
- You must know the AD domain and servers, as well as the following binding information: the authentication level, the Bind user and password, the base DN, and the LDAP port.

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.

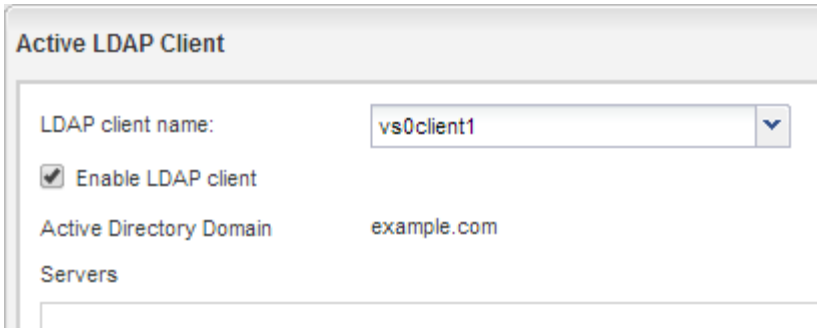


f. Click **Save and Close**.

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

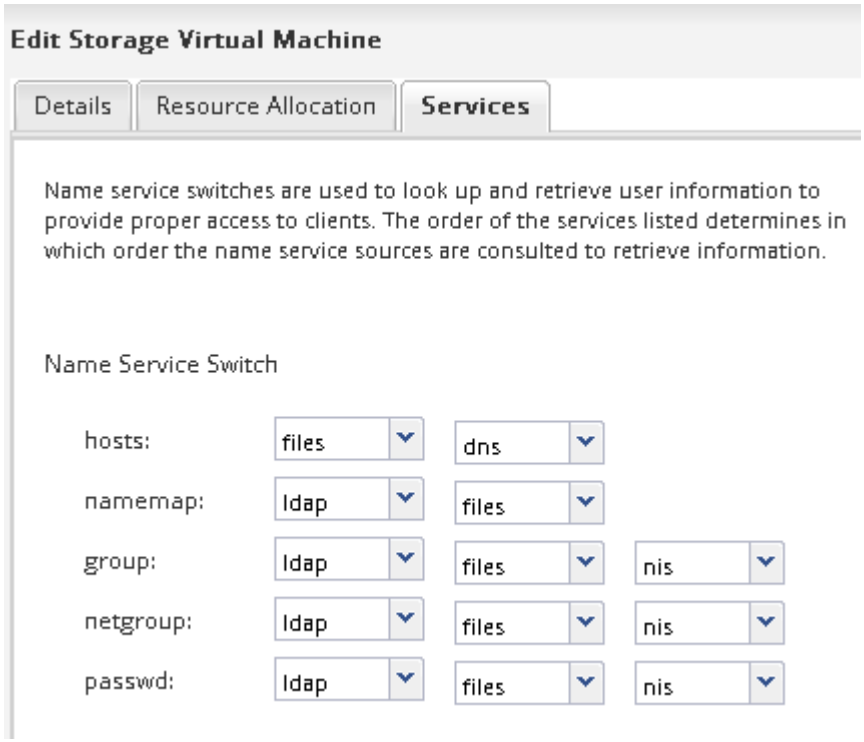
5. Enable the new LDAP client for the SVM:

   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.

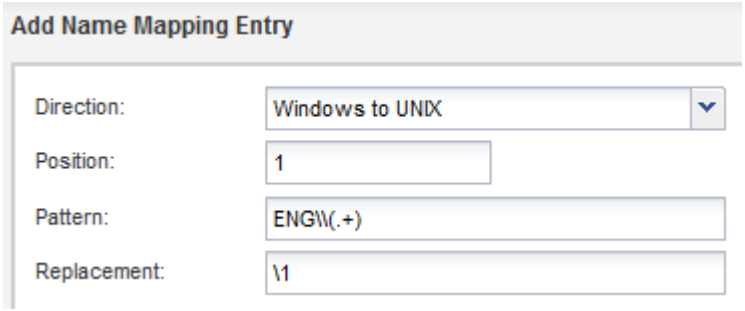
Steps

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.

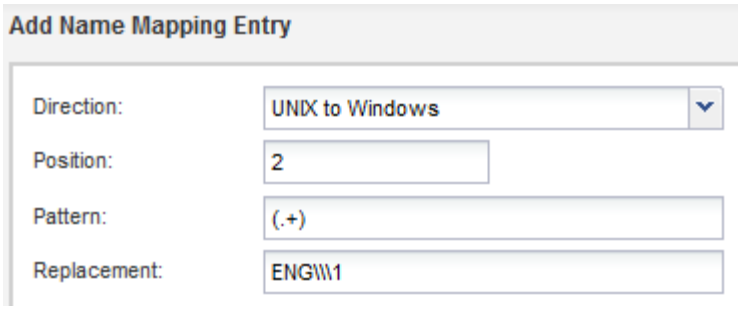
     Each SVM has a default UNIX user named “pcuser” but does not have a default Windows user.
2. Navigate to the **SVMs** window.
3. Select the SVM that you want to configure.
4. Click the **SVM Settings** tab.
5. Create a name mapping that converts UNIX user accounts to Windows user accounts, and vice versa:
   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.

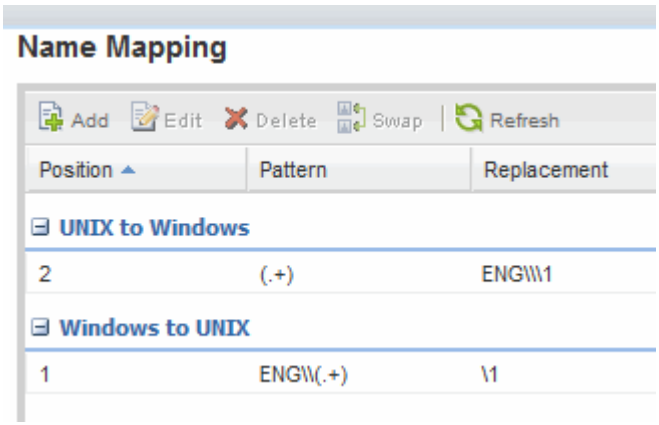
      

   c. Click**Add**, select the **UNIX to Windows** direction, and then create the corresponding mapping that produces a Windows credential when a UNIX user tries to access a file that has NTFS file permissions.

      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 #SUBSTEP_8BDAF68A77864AAFAF680961CE879940 through #SUBSTEP_E730068645DB4303B61744DB632A9803 to map all of the domains and names on the SVM.

6. 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. 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**.

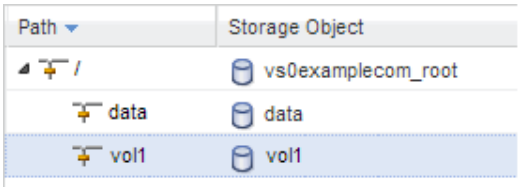
   The Create Volume dialog box is displayed.

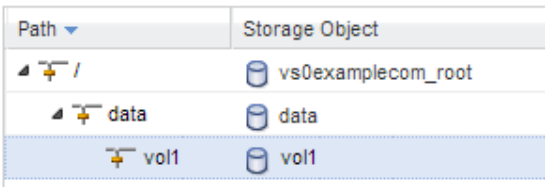
3. If you want to change the default name, which ends in a date and time stamp, specify a new name, such as `vol1`.
4. Select an aggregate for the volume.
5. Specify the size of the volume.
6. Click **Create**.

   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. 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.

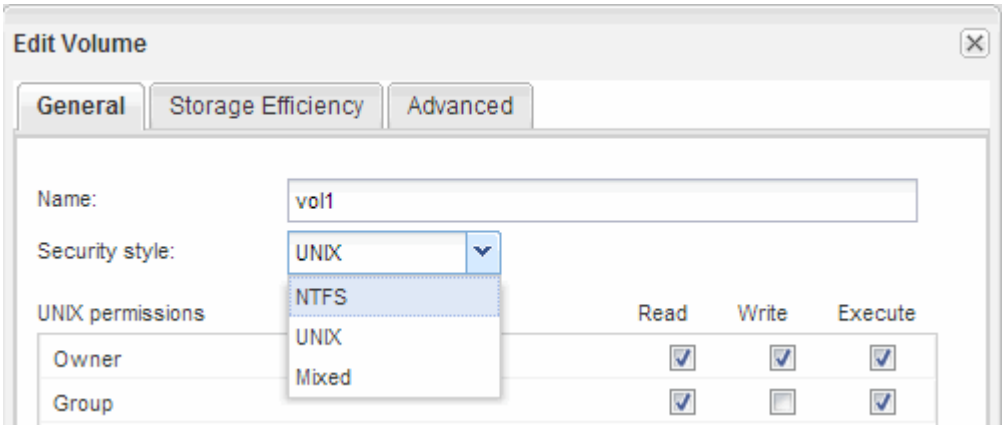




8. Review the volume's security style and change it, if necessary:
   a. In the **Volume** window, select the volume you just created, and click **Edit**.

      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**.

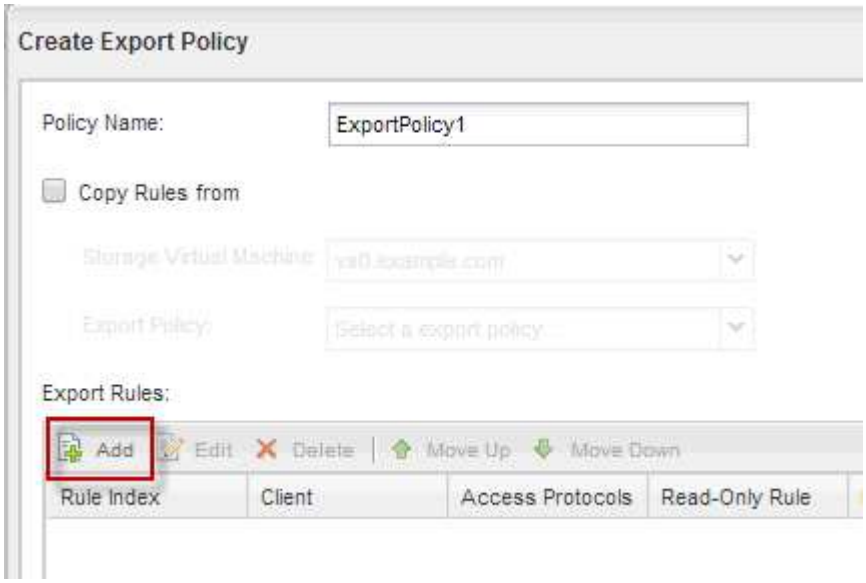
   The updated share access permissions are listed in the Share Access Control pane.

Create an export policy for the volume

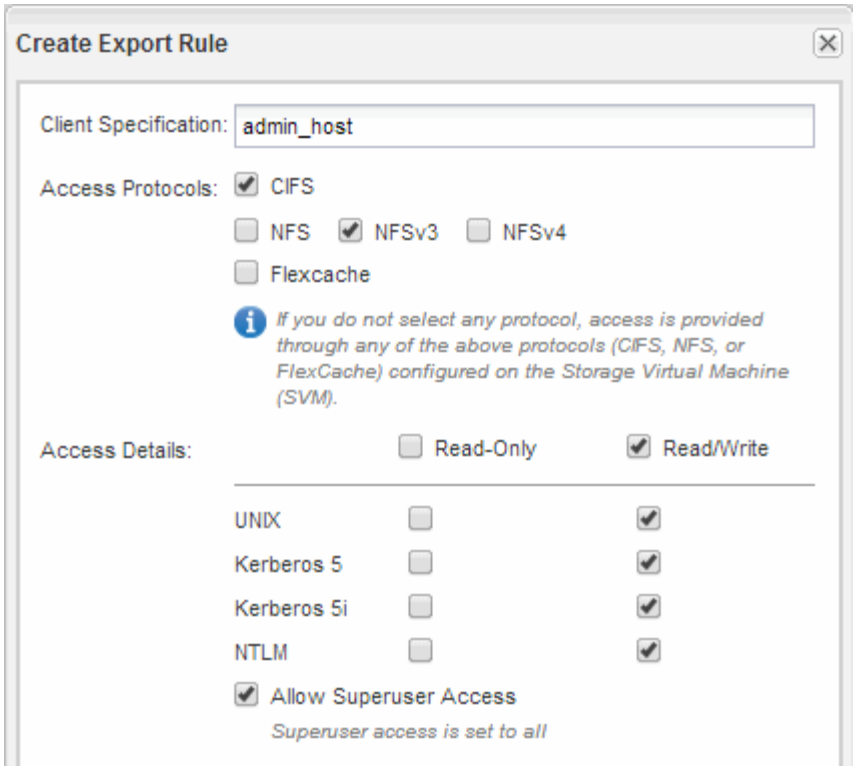
Before any NFS clients can access a volume, you must create an export policy for the volume, add a rule that permits access by an administration host, and apply the new export policy to the volume.

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.

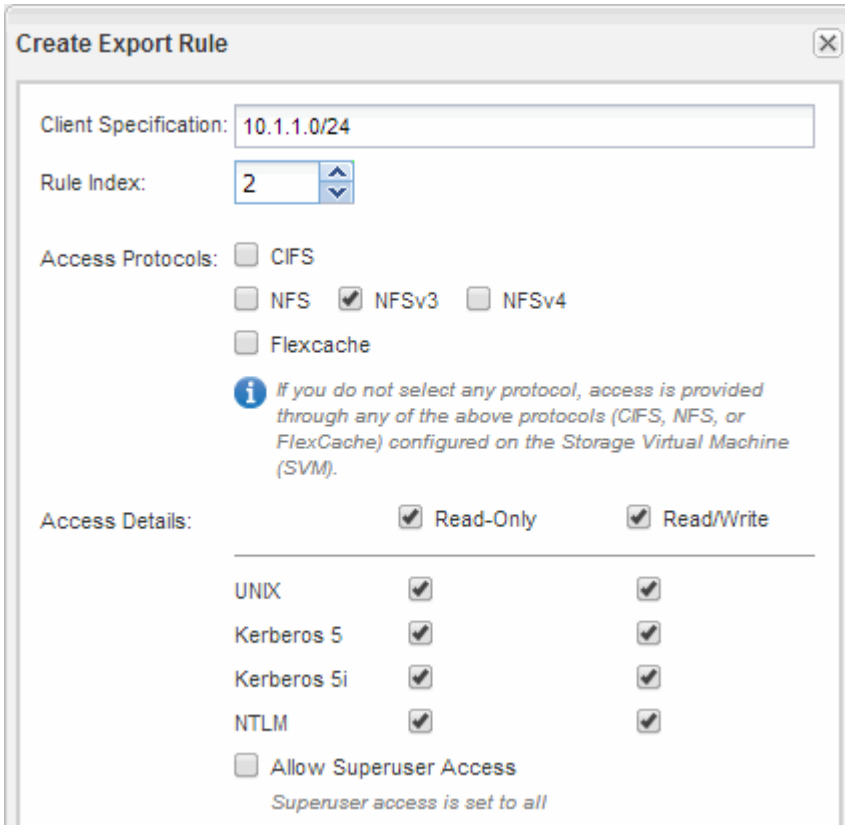
d. In the **Export Rules** tab, click **Add**, and specify a set of clients.

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.

Where to find additional information

After you have successfully tested CIFS and NFS client access, you can perform advanced CIFS and NFS configuration or add SAN access. When protocol access is complete, you should protect the root volume of SVM. There is comprehensive content and technical reports to help you achieve these goals.

CIFS/SMB configuration

You can further configure CIFS access using the following content and technical reports:

- CIFS management

  Describes how to configure and manage file access using the CIFS/SMB protocol.

- NetApp Technical Report 4191: Best Practices Guide for Clustered Data ONTAP 8.2 Windows File Services

  Provides a brief overview of SMB implementation and other Windows File Services features with recommendations and basic troubleshooting information for ONTAP.

- NetApp Technical Report 3740: SMB 2 Next-Generation CIFS Protocol in Data ONTAP

  Describes SMB 2 features, configuration details, and its implementation in ONTAP.

NFS configuration

You can further configure NFS access using the following content and technical reports:

- NFS management

  Describes how to configure and manage file access using the NFS protocol.

- NetApp Technical Report 4067: NFS Best Practice and Implementation

  Serves as an NFSv3 and NFSv4 operational guide and provides an overview of ONTAP operating system with a focus on NFSv4.

- NetApp Technical Report 4668: Name Services Best Practices

  Provides a comprehensive list of best practices, limits, recommendations, and considerations when configuring LDAP, NIS, DNS, and local user and group files for authentication purposes.

- NetApp Technical Report 4616: NFS Kerberos in ONTAP with Microsoft Active Directory
- NetApp Technical Report 4835: How to Configure LDAP in ONTAP
- NetApp Technical Report 3580: NFSv4 Enhancements and Best Practices Guide Data ONTAP Implementation

  Describes the best practices that should be followed while implementing NFSv4 components on AIX, Linux, or Solaris clients attached to systems running ONTAP.

Root volume protection

After configuring protocols on the SVM, you should ensure that its root volume is protected:

- Data protection

  Describes how to create a load-sharing mirror to protect the SVM root volume, which is a NetApp best practice for NAS-enabled SVMs. Also describes how to quickly recover from volume failures or losses by promoting the SVM root volume from a load-sharing mirror

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.

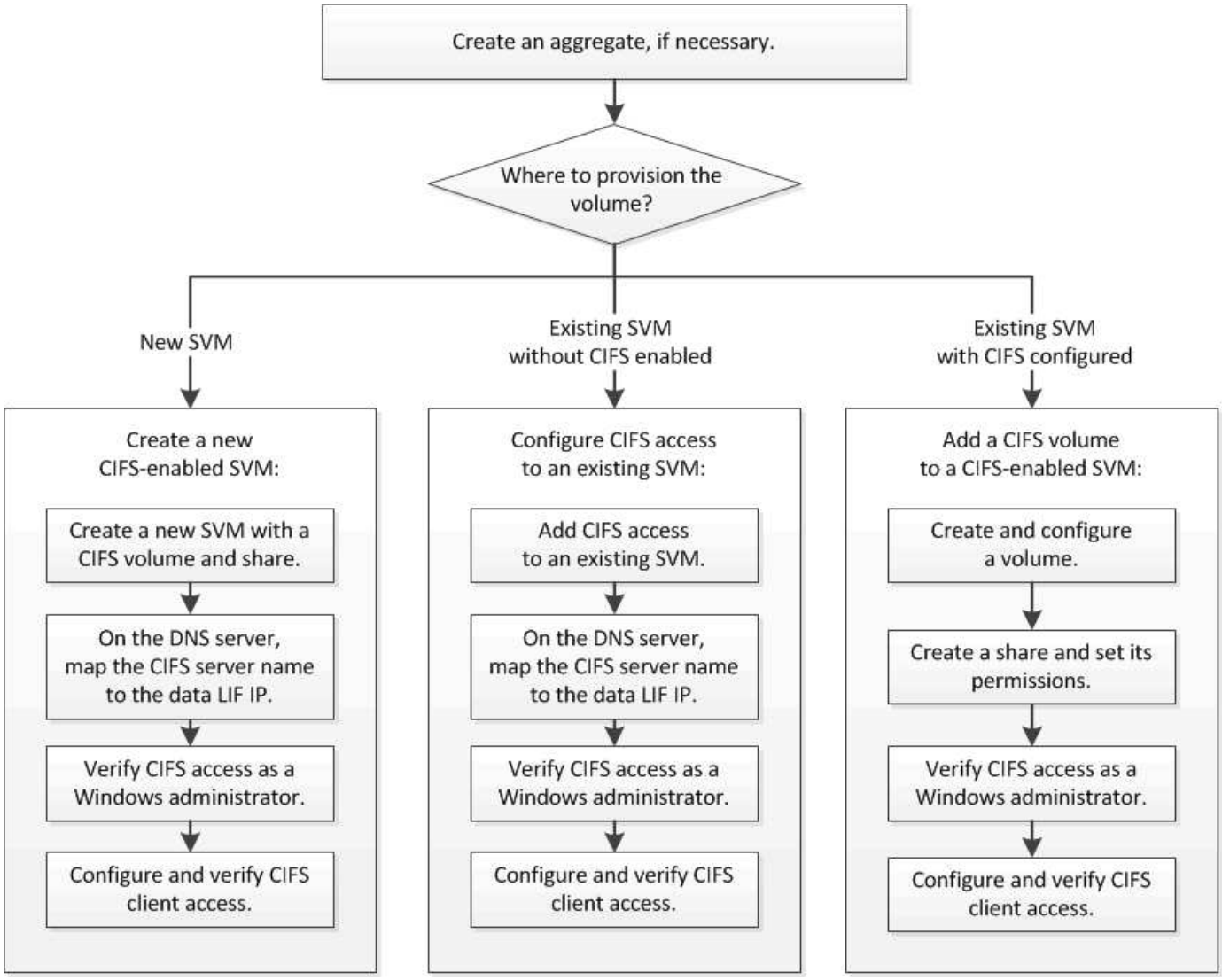
If you want details about the range of ONTAP SMB protocol capabilities, consult the SMB reference overview.

Other ways to do this in ONTAP

To perform these tasks with…	See this content…
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

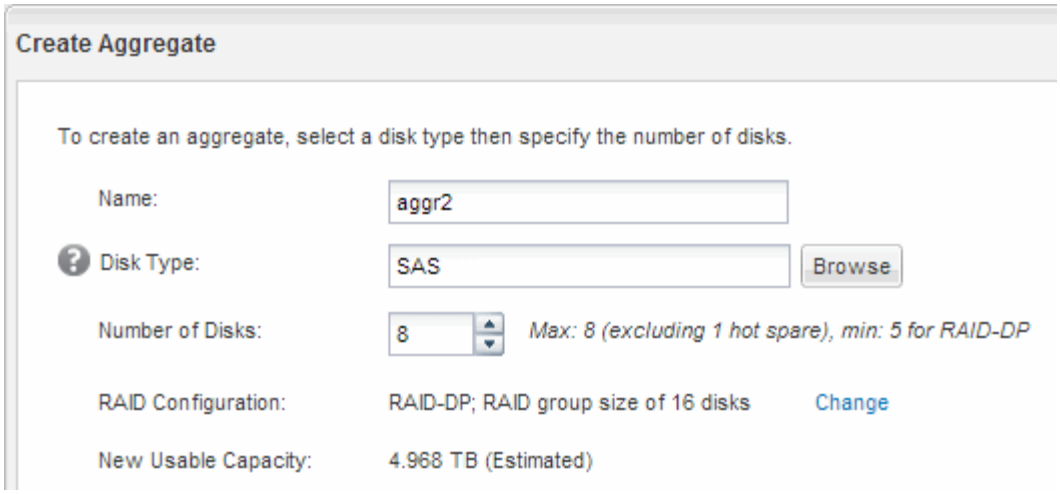
If you do not want to use an existing aggregate, you can create a new aggregate to provide physical storage to the volume which you are provisioning.

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 created the SVM for SAN access by using the procedure in this content.

- 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.

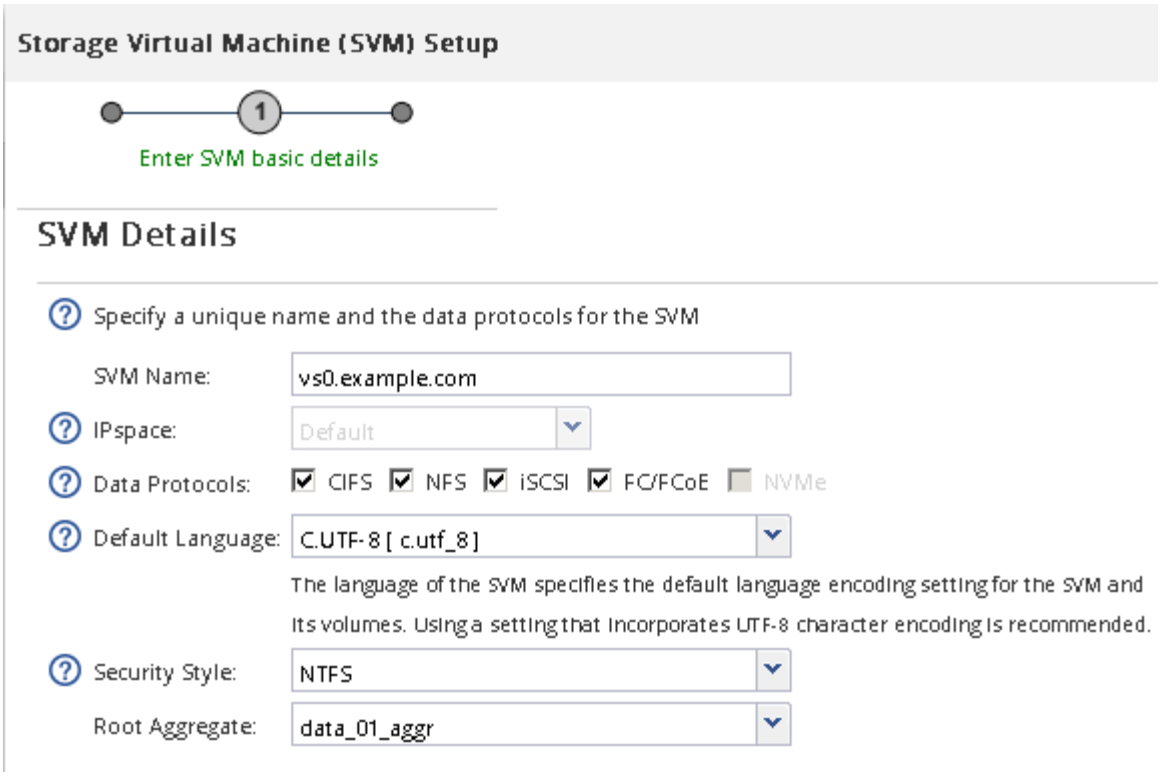
      

      If you support international character display in both NFS and SMB/CIFS clients, consider using the **UTF8MB4** language code, which is available beginning with ONTAP 9.5.

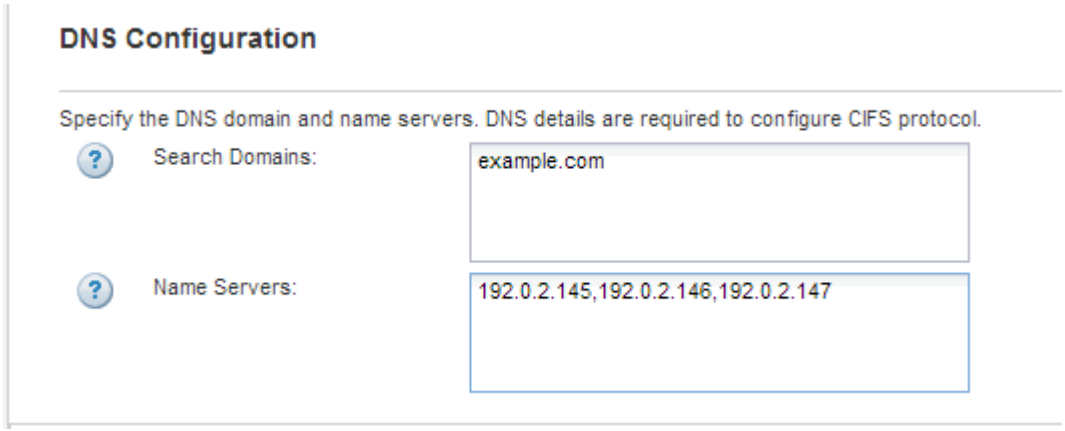
      This language is inherited by the volume that you create later, and a volume's language cannot be changed.

   d. 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.



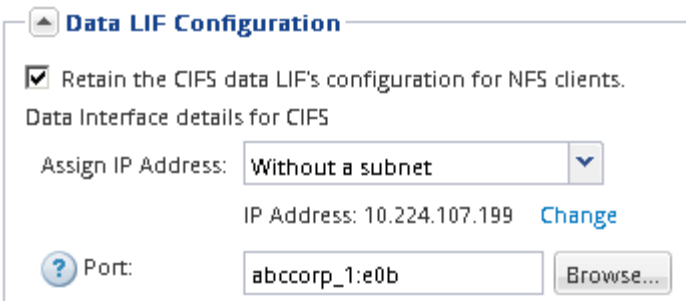
e. In the **DNS Configuration** area, ensure that the default DNS search domain and name servers are the ones that you want to use for this SVM.



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:

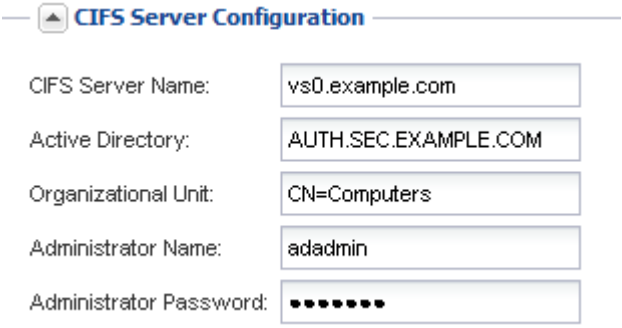
   a. Specify a name for the CIFS server that is unique in the AD domain.

   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.

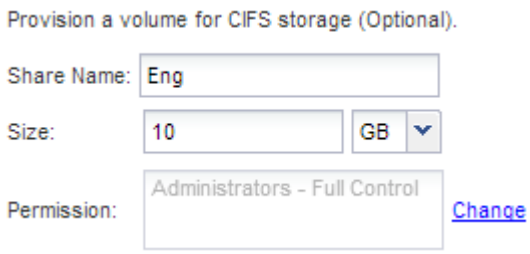


6. Create a volume for CIFS/SMB access and provision a share on it:

   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. 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. 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.

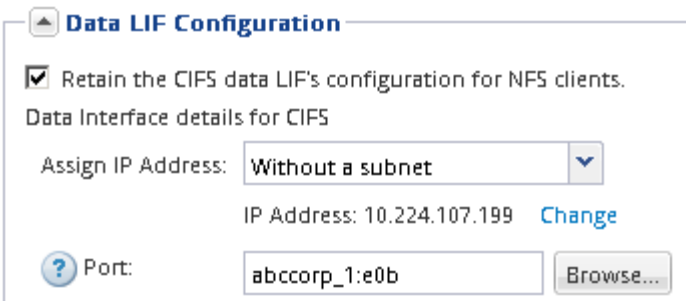
  This is the case if you did not created the SVM following the procedure in this content to configure a SAN protocol.

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:

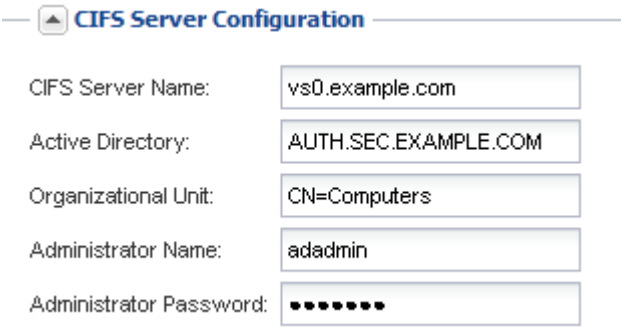
   a. Specify a name for the CIFS server that is unique in the AD domain.

   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.

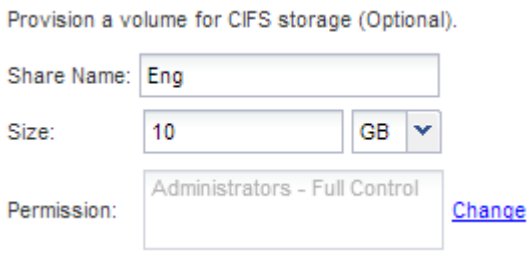


4. Create a volume for CIFS/SMB access and provision a share on it:

   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. 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. 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. 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.

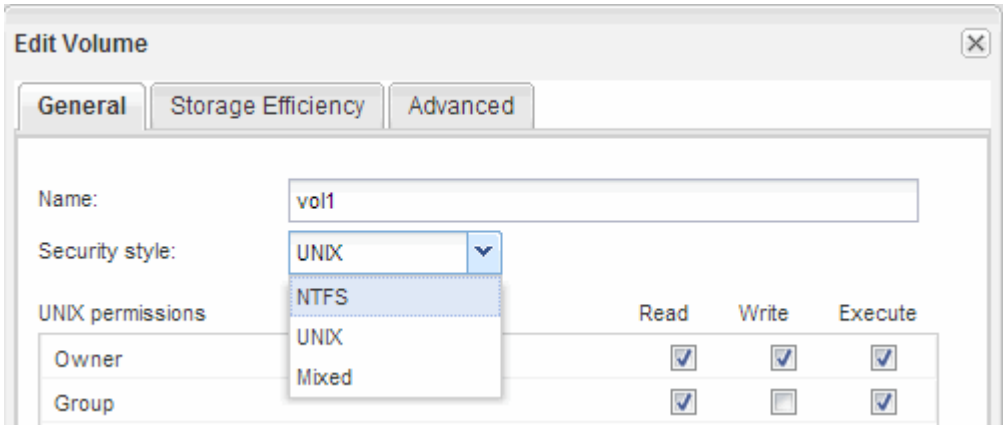
   + image::../media/namespace_1_before_smb.gif[This graphic is described by the surrounding text.]

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. 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.

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.