

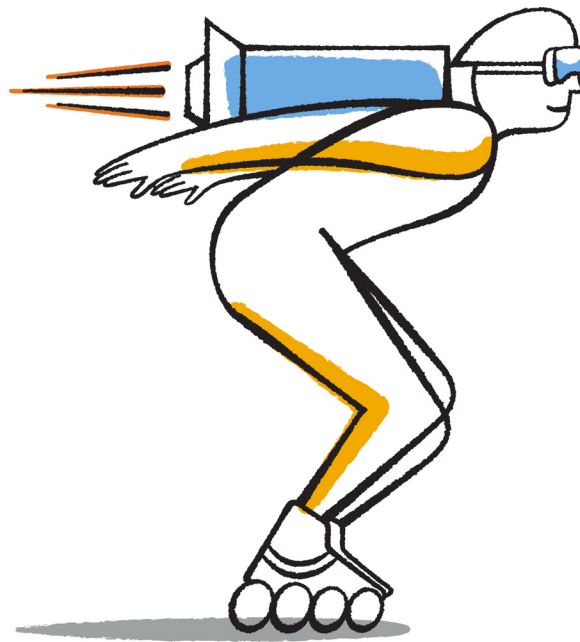


NetApp®

Updated for 8.3.1

Clustered Data ONTAP® 8.3

NFS Configuration Express Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: docomments@netapp.com

Part number: 215-09057_B0
June 2015

Contents

Deciding whether to use this guide	4
NFS configuration workflow	5
Creating an aggregate	5
Deciding where to provision the new volume	6
Creating a new NFS-enabled SVM	7
Creating a new SVM with an NFS volume and export	7
Opening the export policy of the SVM root volume	11
Configuring LDAP	12
Verifying NFS access from a UNIX administration host	14
Configuring and verifying NFS client access	15
Configuring NFS access to an existing SVM	17
Adding NFS access to an existing SVM	17
Opening the export policy of the SVM root volume	19
Configuring LDAP	20
Verifying NFS access from a UNIX administration host	22
Configuring and verifying NFS client access	23
Adding an NFS volume to an NFS-enabled SVM	25
Creating and configuring a volume	25
Creating an export policy for the volume	26
Verifying NFS access from a UNIX administration host	28
Configuring and verifying NFS client access	29
Where to find additional information	31
Copyright information	32
Trademark information	33
How to send comments about documentation and receive update notifications	34
Index	35

Deciding whether to use this guide

This guide describes how to quickly set up NFS access to a new volume on either a new or existing Storage Virtual Machine (SVM).

You should use this guide if you want to configure access to a volume in the following way:

- NFS access will be via NFSv3, not NFSv4 or NFSv4.1.
- 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 OnCommand System Manager, not the Data ONTAP command-line interface or an automated scripting tool.
- You want to create FlexVol volumes, not Infinite Volumes.
- UNIX file permissions will be used to secure the new volume.
- LDAP, if used, is provided by Active Directory.

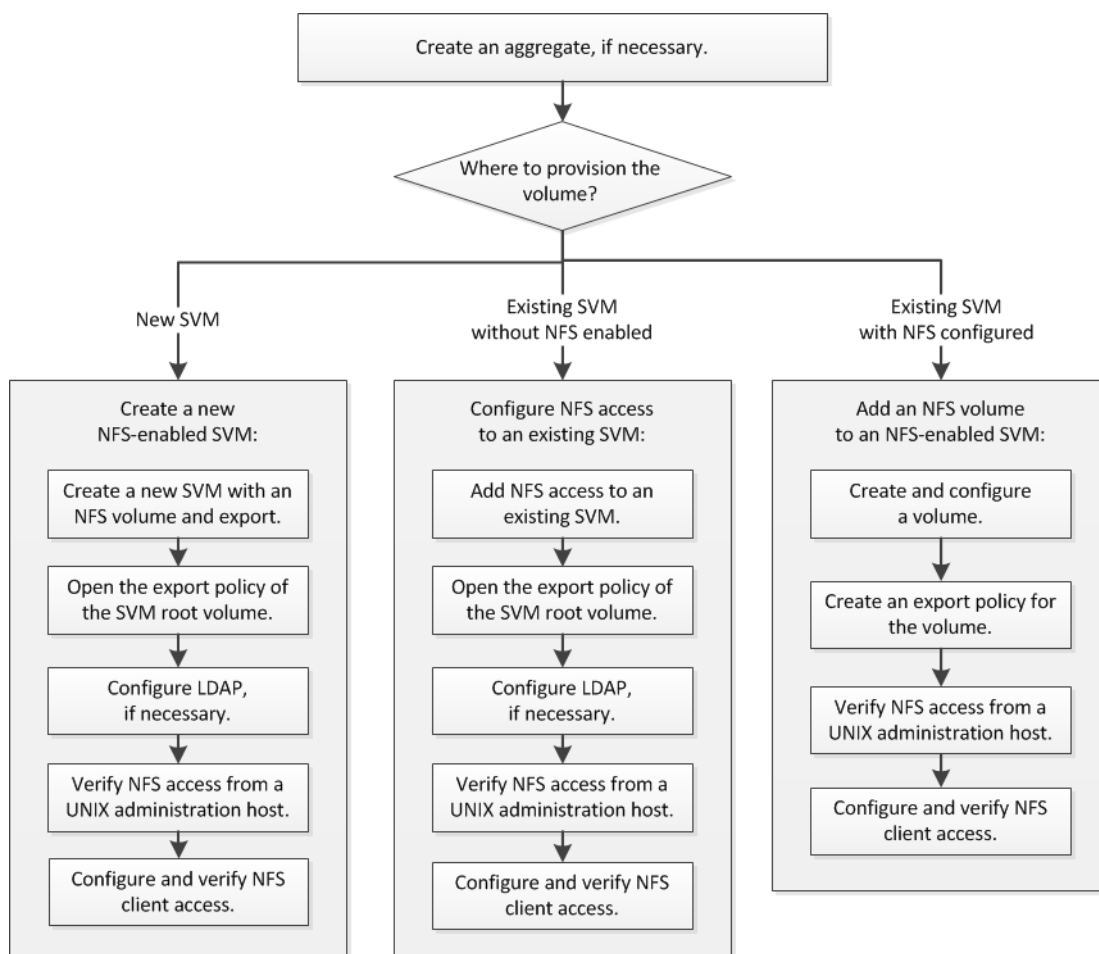
If this guide is not suitable for your situation, you should see the following documentation instead:

- [*Clustered Data ONTAP 8.3 File Access Management Guide for NFS*](#)
- [*NetApp Technical Report 4067: Clustered Data ONTAP Best Practice and NFS Implementation Guide*](#)
- [*NetApp Technical Report 4073: Secure Unified Authentication with NetApp Storage Systems: Kerberos, NFSv4, and LDAP for User Authentication over NFS \(with a Focus on Clustered Data ONTAP\)*](#)
- [*NetApp Technical Report 3580: NFSv4 Enhancements and Best Practices Guide: Data ONTAP Implementation*](#)
- [*NetApp Technical Report 4379: Name Services Best Practice Guide Clustered Data ONTAP*](#)
- [*NetApp Documentation: OnCommand Workflow Automation \(current releases\)*](#)

OnCommand Workflow Automation enables you to run prepackaged workflows that automate management tasks such as the workflows described in Express Guides.

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.



Creating 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 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. In the navigation pane, expand the **Cluster** hierarchy and click **Storage > Aggregates**.
3. Click **Create**.
4. Follow the instructions on the screen to create the aggregate using the default RAID-DP configuration, and then click **Create**.

Create Aggregate

To create an aggregate, select a disk type then specify the number of disks.

Name:

Disk Type:

Number of Disks: Max: 8 (excluding 1 hot spare), min: 5 for RAID-DP

RAID Configuration: RAID-DP; RAID group size of 16 disks

New Usable Capacity: 4.968 TB (Estimated)

Result

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

Deciding 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.

Choices

- If you want a new SVM, see [Creating a new NFS-enabled SVM](#) on page 7.
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 that has NFS enabled but not configured, see [Configuring NFS access to an existing SVM](#) on page 17.
You should choose this option if you created the SVM for SAN access by using the relevant Express Guide.
- If you want to provision a volume on an existing SVM that is fully configured for NFS access, see [Adding an NFS volume to an NFS-enabled SVM](#) on page 25.

Creating 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.

Steps

1. [Creating a new SVM with an NFS volume and export](#) on page 7
2. [Opening the export policy of the SVM root volume](#) on page 11
3. [Configuring LDAP](#) on page 12
4. [Verifying NFS access from a UNIX administration host](#) on page 14
5. [Configuring and verifying NFS client access](#) on page 15

Creating a new SVM with an NFS volume and export

You can use a wizard that guides you through the process of creating the SVM, configuring DNS, creating a data 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:
 - IPspace, if the network has more than one IPspace
You cannot change the IPspace after the SVM is created.
 - 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, and 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 NIS, LDAP, 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. Expand the **Storage Virtual Machines** hierarchy in the left navigation pane, and then click **Create**.
2. In the **Storage Virtual Machine (SVM) Setup** window, create the SVM:
 - a. Specify a unique name for the SVM.

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

- b. Select the IPspace to which the SVM will belong.

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

- c. 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.

- d. 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.

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

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

- f. Optional: Select the root aggregate to contain the SVM root volume.

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

SVM Details

? Specify a unique name and the data protocols for the SVM

SVM Name:

? IPspace:

? Volume Type: FlexVol volumes Infinite Volume

An SVM can contain either multiple FlexVol volumes or a single Infinite Volume.
You cannot change the volume type of the SVM after you set it.

? Data Protocols: CIFS NFS iSCSI FC/FCoE

? Default Language:

The language of the SVM determines the character set used to display the file names and data for all NAS volumes in the SVM. Therefore, you must set the language with correct value.

? Security Style:

Root Aggregate:

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

DNS Configuration

Specify the DNS domain and name servers. DNS details are required to configure CIFS protocol.

? Search Domains:

? Name Servers:

- h. Click **Submit & Continue**.

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

3. 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:

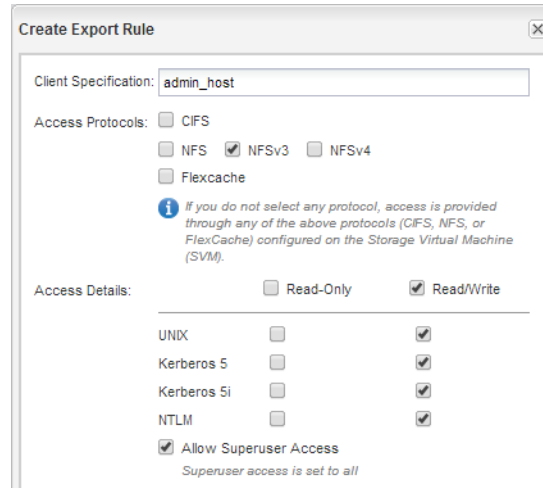
- a. Assign an IP address to the LIF automatically from a subnet you specify or manually enter the address.
- b. Click **Browse** and select a node and port that will be associated with the LIF.

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

6. 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.



Create Export Rule

Client Specification:

Access Protocols:

CIFS

NFS NFSv3 NFSv4

Flexcache

i If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

Read-Only Read/Write

UNIX	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Allow Superuser Access
Superuser access is set to all

Example

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.

7. 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
8. For all other protocol configuration pages that are displayed, click **Skip** and configure the protocol later.
 9. 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**.
 10. 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.

Result

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

Opening the export policy of the SVM root volume

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 open all NFS access in the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes.

Steps

1. In the navigation pane, select the SVM and click **Policies > Export Policies**.
2. Select the export policy named **default**, which is applied to the SVM root volume.
3. In the lower pane, click **Add**.
4. 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**.

The screenshot shows the 'Create Export Rule' dialog box with the following configuration:

- Client Specification:** 0.0.0.0/0
- Rule Index:** 1
- Access Protocols:**
 - CIFS
 - NFS
 - NFSv3
 - NFSv4
 - Flexcache
- Information:** If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).
- Access Details:**
 - Read-Only
 - Read/Write
- Authentication:**
 - UNIX
 - Kerberos 5
 - Kerberos 5i
 - NTLM
- Other Options:**
 - Allow Superuser Access

Superuser access is set to all

Result

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

Configuring LDAP

If you want the SVM to get user information from Active Directory based 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 and other documentation to configure LDAP.

NetApp Technical Report 4073: Secure Unified Authentication with NetApp Storage Systems: Kerberos, NFSv4, and LDAP for User Authentication over NFS (with a Focus on Clustered Data 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

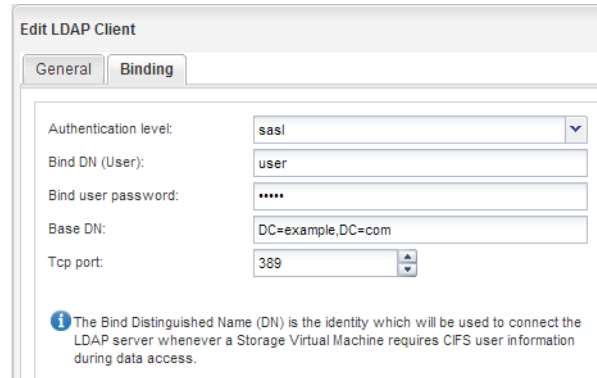
- Set up an LDAP client for the SVM to use:
 - In the navigation pane, expand the SVM, and click **Configuration > Services > LDAP Client**.
 - In the **LDAP Client** window, click **Add**.
 - In the **General** tab of the **Create LDAP Client** window, type the name of the LDAP client configuration, such as `vs0client1`.
 - Add either the AD domain or the AD servers.

The screenshot shows the 'Create LDAP Client' window with the following details:

- Title:** Create LDAP Client
- Tabs:** General (selected), Binding
- LDAP Client Configuration:** vs0client1
- Servers Section:**
 - Active Directory Domain:** example.com
 - Preferred Active Directory Servers:**

Server	Actions
192.0.2.145	Add, Delete, Up, Down
 - Active Directory Servers:**

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



Edit LDAP Client

General Binding

Authentication level: sasl

Bind DN (User): user

Bind user password: ****

Base DN: DC=example,DC=com

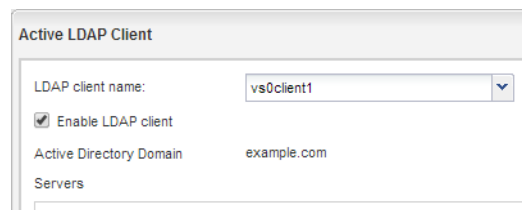
Top port: 389

i The Bind Distinguished Name (DN) is the identity which will be used to connect the LDAP server whenever a Storage Virtual Machine requires CIFS user information during data access.

f. Click **Save and Close**.

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

2. 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**.



Active LDAP Client

LDAP client name: vs0client1

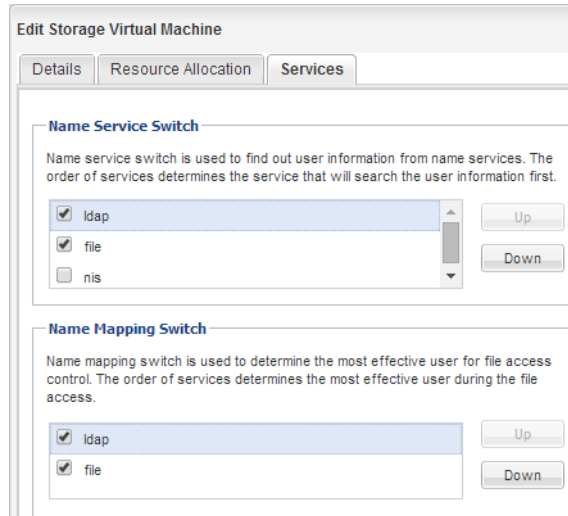
Enable LDAP client

Active Directory Domain: example.com

Servers

The SVM uses the new LDAP client.

3. Give LDAP priority over other sources of user information, such as NIS and local users and groups:
 - a. In the navigation pane, select the cluster to display the list of SVMs.
 - b. In the right window, select the SVM and click **Edit**.
 - c. Click the **Services** tab.
 - d. Under **Name Service Switch**, select **LDAP** and move it to the top of the list.
 - e. Either clear **NIS** or move it further down the order as required.
 - f. Under **Name Mapping Switch**, select **LDAP** and move it to the top of the list.
 - g. Click **Save and Close**.



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

Verifying NFS access from a UNIX administration host

After you configure NFS access to an 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.

Example

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.

Example

```
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 ..
```

Result

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

Configuring and verifying NFS client access

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. In the navigation pane, select the Storage Virtual Machine (SVM), and click **Policies > Export Policies**.
 - b. Select the export policy with the same name as the volume.
 - c. In the **Export Rules** tab, click **Add**, and specify a set of clients.
 - d. Select **2** for the **Rule Index** so that this rule executes after the rule that allows access to the administration host.
 - e. Select **NFSv3**.
 - f. Specify the access details that you want, and click **OK**.

Example

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**.

Create Export Rule

Client Specification: 10.1.1.0/24

Rule Index: 2

Access Protocols:

- CIFS
- NFS
- NFSv3
- NFSv4
- Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

	<input checked="" type="checkbox"/> Read-Only	<input checked="" type="checkbox"/> Read/Write
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Allow Superuser Access		

Superuser access is set to all

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.

Configuring 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.

Steps

1. [Adding NFS access to an existing SVM](#) on page 17
2. [Opening the export policy of the SVM root volume](#) on page 19
3. [Configuring LDAP](#) on page 20
4. [Verifying NFS access from a UNIX administration host](#) on page 22
5. [Configuring and verifying NFS client access](#) on page 23

Adding 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:
 - 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, and optionally the specific IP address you want to assign to the data LIF
- Any external firewalls must be appropriately configured to allow access to network services.
- The NFS protocol must be allowed on the SVM.
This is the case if you created the SVM while following another Express Guide to configure a SAN protocol.

Steps

1. Navigate to the area where you can configure the protocols of the SVM:
 - a. In the navigation pane, expand the **Storage Virtual Machines** hierarchy and select the cluster.
 - b. In the list of SVMs, select the SVM that you want to configure.
 - c. In the **Details** pane, next to **Protocols**, click **NFS**.

Protocols: NFS FCIFCDE

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.

Data LIF Configuration

Retain the CIFS data LIF's configuration for NFS clients.

Data interface details for CIFS

Subnet:

Auto-select the IP address from this subnet

Use a specific IP address:

Port: [Browse...](#)

3. If your site uses NIS for name services or name mapping, specify the domain and IP addresses of the NIS servers.

NIS Configuration (Optional)

Configure NIS domain on the SVM to authorize NFS users.

Domain Name(s):

IP Address(es):

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.

Provision a volume for NFS storage.

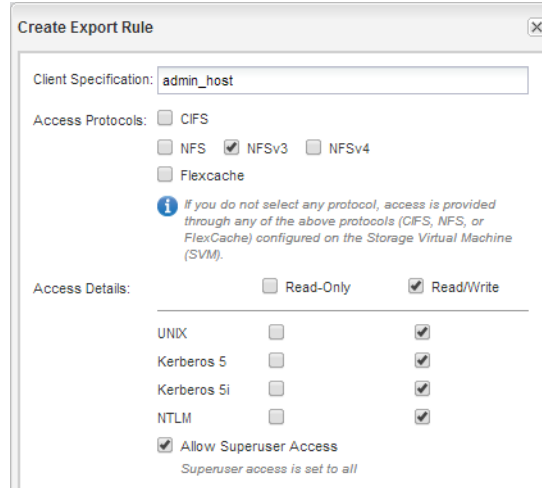
Export Name:

Size:

Permission: [Change](#)

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.



Create Export Rule

Client Specification:

Access Protocols:

- CIFS
- NFS NFSv3 NFSv4
- Flexcache

! If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

- Read-Only Read/Write

- UNIX
- Kerberos 5
- Kerberos 5i
- NTLM
- Allow Superuser Access
Superuser access is set to all

Example

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**.

Opening the export policy of the SVM root volume

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 open all NFS access in the default export policy, and later restrict access to individual volumes by creating custom export policies for individual volumes.

Steps

1. In the navigation pane, select the SVM and click **Policies > Export Policies**.
2. Select the export policy named **default**, which is applied to the SVM root volume.
3. In the lower pane, click **Add**.
4. 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**.

Create Export Rule

Client Specification: 0.0.0.0/0

Rule Index: 1

Access Protocols: CIFS NFS NFSv3 NFSv4 Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details: Read-Only Read/Write

UNIX Kerberos 5 Kerberos 5i NTLM Allow Superuser Access
Superuser access is set to all

Result

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

Configuring LDAP

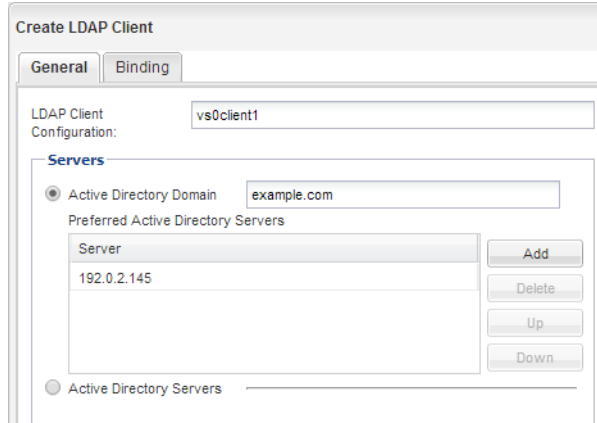
If you want the SVM to get user information from Active Directory based LDAP, you must create an LDAP client, enable it for the SVM, and give LDAP priority over other sources of user information.

Before you begin

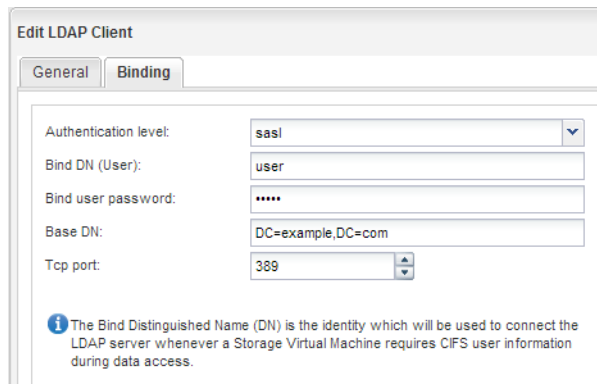
- The LDAP configuration must be using Active Directory (AD).
If you use another type of LDAP, you must use the command-line interface and other documentation to configure LDAP.
[NetApp Technical Report 4073: Secure Unified Authentication with NetApp Storage Systems: Kerberos, NFSv4, and LDAP for User Authentication over NFS \(with a Focus on Clustered Data ONTAP\)](#)
- 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

- Set up an LDAP client for the SVM to use:
 - In the navigation pane, expand the SVM, and click **Configuration > Services > LDAP Client**.
 - In the **LDAP Client** window, click **Add**.
 - In the **General** tab of the **Create LDAP Client** window, type the name of the LDAP client configuration, such as `vs0client1`.
 - Add either the AD domain or the AD servers.



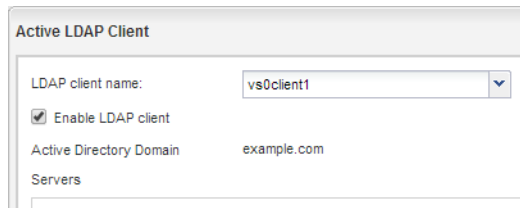
- e. Click **Binding**, and specify the authentication level, the Bind user and password, the base DN, and the port.



- f. Click **Save and Close**.

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

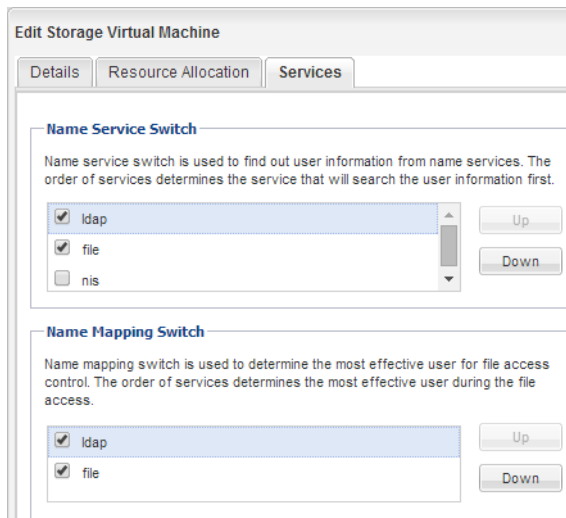
2. Enable the new LDAP client for the SVM:
 - a. In the navigation pane, click **LDAP Configuration**.
 - b. Click **Edit**.
 - c. Ensure that the client you just created is selected in **LDAP client name**.
 - d. Select **Enable LDAP client**, and click **OK**.



The SVM uses the new LDAP client.

3. Give LDAP priority over other sources of user information, such as NIS and local users and groups:

- a. In the navigation pane, select the cluster to display the list of SVMs.
- b. In the right window, select the SVM and click **Edit**.
- c. Click the **Services** tab.
- d. Under **Name Service Switch**, select **LDAP** and move it to the top of the list.
- e. Either clear **NIS** or move it further down the order as required.
- f. Under **Name Mapping Switch**, select **LDAP** and move it to the top of the list.
- g. Click **Save and Close**.



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

Verifying NFS access from a UNIX administration host

After you configure NFS access to an 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.

Example

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.

Example

```
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 ..
```

Result

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

Configuring and verifying NFS client access

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.

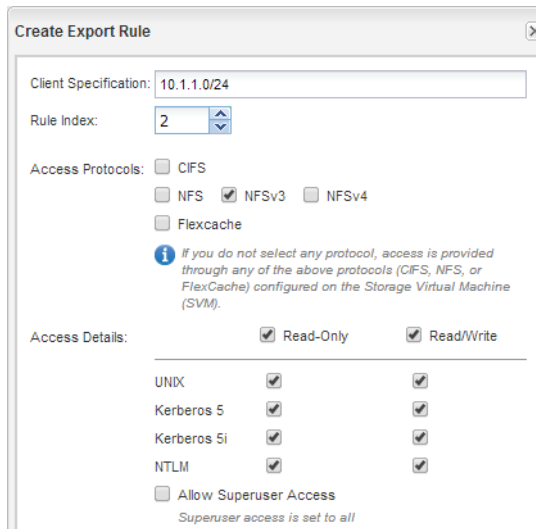
Steps

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. In the navigation pane, select the Storage Virtual Machine (SVM), and click **Policies > Export Policies**.
 - b. Select the export policy with the same name as the volume.

- c. In the **Export Rules** tab, click **Add**, and specify a set of clients.
- d. Select **2** for the **Rule Index** so that this rule executes after the rule that allows access to the administration host.
- e. Select **NFSv3**.
- f. Specify the access details that you want, and click **OK**.

Example

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**.



Create Export Rule

Client Specification: 10.1.1.0/24

Rule Index: 2

Access Protocols: CIFS
 NFS NFSv3 NFSv4
 Flexcache

! If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details: Read-Only Read/Write

UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Allow Superuser Access		

Superuser access is set to all

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.

Adding 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.

Steps

1. [Creating and configuring a volume](#) on page 25
2. [Creating an export policy for the volume](#) on page 26
3. [Verifying NFS access from a UNIX administration host](#) on page 28
4. [Configuring and verifying NFS client access](#) on page 29

Creating and configuring 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. In the navigation pane, select the SVM, and click **Storage > Volumes**.
2. Click **Create**.
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.

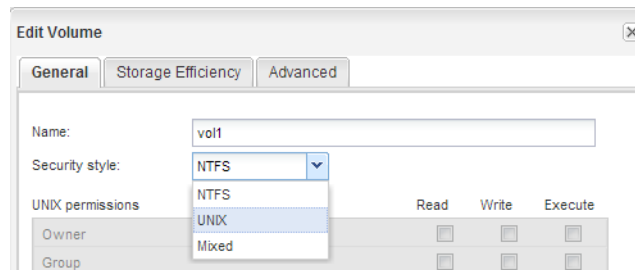
7. Optional: If you do not want the volume to be located at the root of the SVM, modify the place of the new volume in the existing namespace:
 - a. Select **Storage > Namespace**.
 - b. Select the new volume, click **Unmount**, and then confirm the action in the **Unmount Volume** dialog box.
 - c. 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.

Example

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. Click **Storage > Volumes**, 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. Ensure the security style is UNIX.



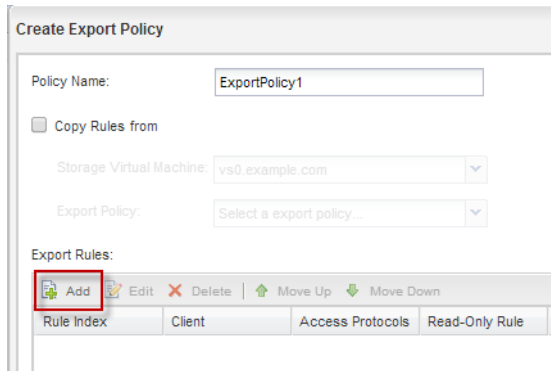
Creating an export policy for the volume

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.

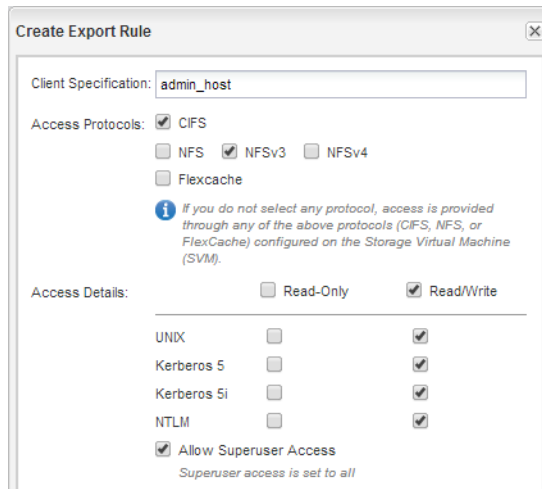
Steps

1. In the navigation pane, expand the SVM and then click **Policies > Export Policies**.

2. Create a new export policy:
 - a. In the **Export Policies** window, 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.



3. 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.

4. Apply the new export policy to the new volume so that the administrator host can access the volume:
 - a. In the left navigation pane, click **Storage > Namespace**.
 - b. Select the volume and click **Change Export Policy**.

- c. Select the new policy and click **Change**.

Related tasks

[Verifying NFS access from a UNIX administration host](#) on page 14

Verifying NFS access from a UNIX administration host

After you configure NFS access to an 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.

Example

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.

Example

```
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 ..
```

Result

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

Configuring and verifying NFS client access

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. In the navigation pane, select the Storage Virtual Machine (SVM), and click **Policies > Export Policies**.
 - b. Select the export policy with the same name as the volume.
 - c. In the **Export Rules** tab, click **Add**, and specify a set of clients.
 - d. Select **2** for the **Rule Index** so that this rule executes after the rule that allows access to the administration host.
 - e. Select **NFSv3**.
 - f. Specify the access details that you want, and click **OK**.

Example

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**.

Create Export Rule

Client Specification: 10.1.1.0/24

Rule Index: 2

Access Protocols:

- CIFS
- NFS
- NFSv3
- NFSv4
- Flexcache

If you do not select any protocol, access is provided through any of the above protocols (CIFS, NFS, or FlexCache) configured on the Storage Virtual Machine (SVM).

Access Details:

	<input checked="" type="checkbox"/> Read-Only	<input checked="" type="checkbox"/> Read/Write
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5i	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
NTLM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/> Allow Superuser Access		

Superuser access is set to all

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.

Where to find additional information

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

NFS configuration

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

- [*Clustered Data ONTAP 8.3 File Access Management Guide for NFS*](#)
Describes how to configure and manage file access using the NFS protocol.
- [*NetApp Technical Report 4067: Clustered Data ONTAP Best Practice and NFS Implementation Guide*](#)
Serves as an NFSv3 and NFSv4 operational guide and provides an overview of Data ONTAP operating system with a focus on NFSv4.
- [*NetApp Technical Report 4379: Name Services Best Practice Guide Clustered Data ONTAP*](#)
Explains how to configure LDAP, NIS, DNS, and local file configuration for authentication purposes.
- [*NetApp Technical Report 4073: Secure Unified Authentication with NetApp Storage Systems: Kerberos, NFSv4, and LDAP for User Authentication over NFS \(with a Focus on Clustered Data ONTAP\)*](#)
Explains how to configure clustered Data ONTAP for use with UNIX-based Kerberos version 5 (krb5) servers for NFS storage authentication and Windows Server Active Directory (AD) as the KDC and Lightweight Directory Access Protocol (LDAP) identity provider.
- [*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 Data ONTAP.

SAN protocol configuration

If you want to provide SAN access to the SVM, you can use any of the FC or iSCSI configuration express guides, which are available for multiple host operating systems.

[*NetApp Documentation: Clustered Data ONTAP Express Guides*](#)

Root volume protection

After configuring protocols on the SVM, you should ensure that its root volume is protected by using the following express guide:

- [*Clustered Data ONTAP 8.3 SVM Root Volume Protection Express Guide*](#)
Describes how to quickly create load-sharing mirrors on every node of a Data ONTAP 8.3 cluster 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.

Copyright information

Copyright © 1994–2015 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email to docomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index

A

- about this guide
 - deciding whether to use [4](#)
- access
 - additional documentation [31](#)
 - verifying NFS access by administrators [14](#), [22](#), [28](#)
 - verifying NFS access by clients [15](#), [23](#), [29](#)
 - See also* permissions
- aggregates
 - creating [5](#)
 - selecting for new data volumes during SVM creation [7](#)
 - selecting for new volumes [25](#)
 - selecting for SVM [7](#)
- audience
 - for the guide [4](#)

C

- clients
 - adding an LDAP configuration [12](#), [20](#)
- comments
 - how to send feedback about documentation [34](#)
- configuring
 - LDAP [12](#), [20](#)
 - NFS access [5](#), [17](#), [25](#)
- creating
 - aggregates [5](#)
 - export policies for volumes on existing SVMs [26](#)
 - exports while creating new SVMs [7](#)
 - SVMs [7](#)
 - volumes on existing SVMs [25](#)
 - volumes while creating new SVMs [7](#)

D

- data LIFs
 - creating [7](#)
- documentation
 - additional information about protocol access [31](#)
 - how to receive automatic notification of changes to [34](#)
 - how to send feedback about [34](#)

E

- export policies
 - creating for volumes on existing SVMs [26](#)
 - defining for root volumes [11](#), [19](#)
 - defining for volumes on existing SVMs [26](#)
 - defining while creating new SVMs [7](#)
- exports
 - creating while creating new SVMs [7](#)
 - setting UNIX file permissions [15](#), [23](#), [29](#)
 - verifying administrator access to [14](#), [22](#), [28](#)
 - verifying client access [15](#), [23](#), [29](#)
- express guides

- additional documentation [31](#)
- NFS configuration workflow [5](#), [17](#), [25](#)
- requirements for using this guide [4](#)

F

- feedback
 - how to send comments about documentation [34](#)
- file permissions
 - setting for UNIX [15](#), [23](#), [29](#)
- files
 - controlling access to, using UNIX permissions [15](#), [23](#), [29](#)
- FlexVol volumes
 - See* volumes

I

- information
 - how to send feedback about improving documentation [34](#)

L

- LDAP
 - configuring [12](#), [20](#)

N

- name services
 - giving LDAP priority [12](#), [20](#)
- NFS
 - additional documentation [31](#)
 - requirements for using this guide to set up NFS [4](#)
 - setup overview [5](#)
- NFS exports
 - See* exports
- NIS
 - identifying [7](#)

P

- permissions
 - configuring export policy rules for volumes on existing SVMs [26](#)
 - configuring export rules while creating new SVMs [7](#)
 - setting UNIX file permissions [15](#), [23](#), [29](#)
- policies
 - adding export rules [15](#), [23](#), [29](#)
 - creating export, for volumes on existing SVMs [26](#)
 - defining export, for volumes on existing SVMs [26](#)
 - See also* export policies
- provisioning
 - volumes on new SVMs [7](#)

R

- root volumes
 - opening the export policies of [11](#), [19](#)

S

- security style
 - changing [25](#)
- setup
 - NFS, overview of [5](#), [17](#), [25](#)
- subnets
 - choosing [7](#)
- suggestions
 - how to send feedback about documentation [34](#)
- SVMs
 - adding LDAP clients [12](#), [20](#)
 - creating export policies for volumes on existing [26](#)
 - creating NFS volumes on [25](#)
 - creating to support NFS [7](#)
 - provisioning volumes on new [7](#)

T

- technical reports
 - additional information about file access [31](#)
- testing

See [verifying](#)

- twitter
 - how to receive automatic notification of documentation changes [34](#)

U

- UNIX
 - security style, setting [25](#)
 - setting file permissions [15](#), [23](#), [29](#)

V

- verifying
 - NFS access by administrators [14](#), [22](#), [28](#)
 - NFS access by clients [15](#), [23](#), [29](#)
- volumes
 - creating export policies for, on existing SVMs [26](#)
 - creating on existing SVMs [25](#)
 - modifying junction path of [25](#)
 - provisioning on new SVMs [7](#)

W

- workflows
 - NFS configuration [5](#), [17](#), [25](#)