



# Multiprotocol configuration workflow

## System Manager Classic

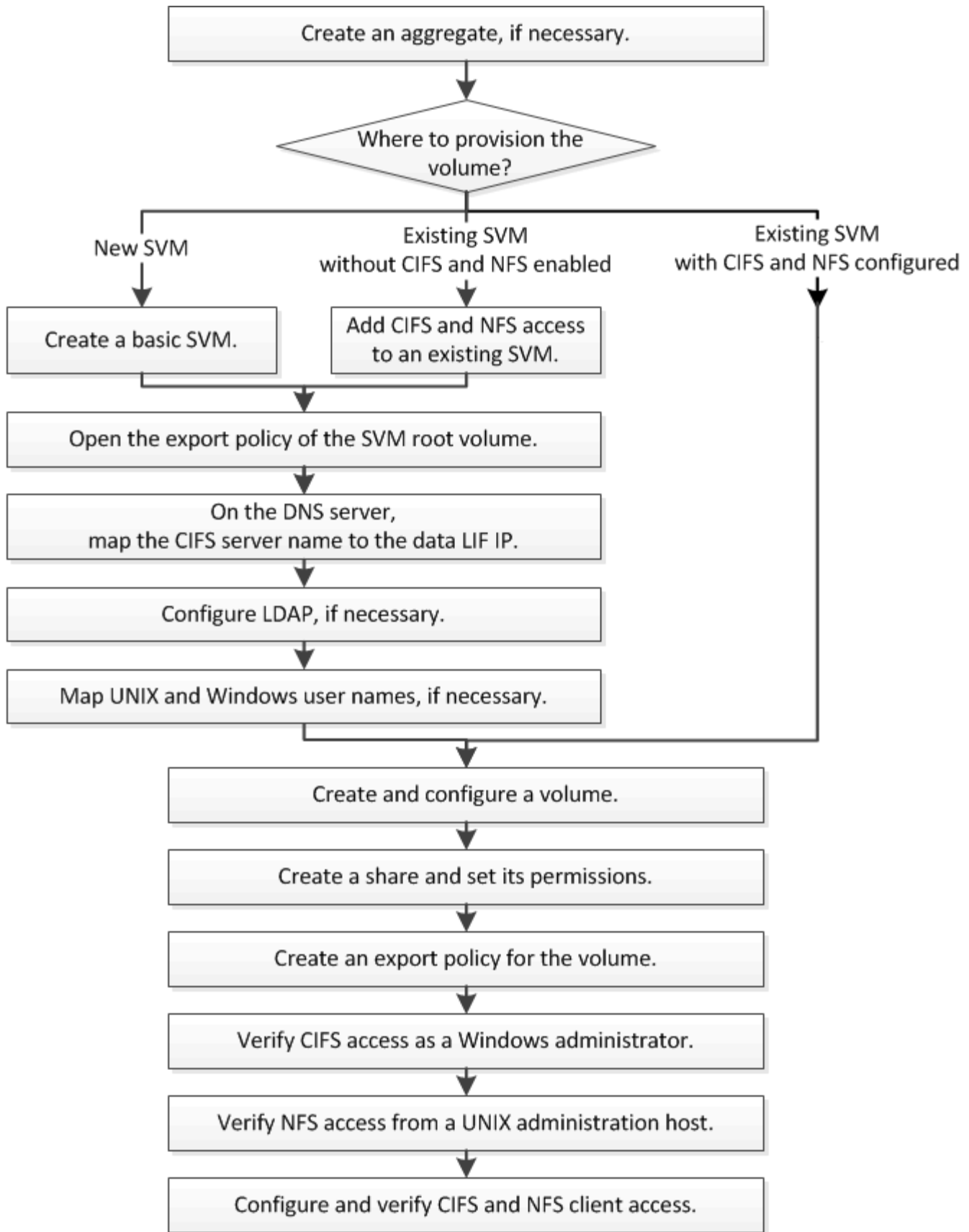
NetApp  
June 22, 2024

# Table of Contents

- Multiprotocol configuration workflow ..... 1
- Create an aggregate ..... 2
- Decide where to provision the new volume ..... 3
- Create and configure a volume ..... 17
- Create a share and set its permissions ..... 18
- Create an export policy for the volume ..... 19
- Verify SMB client access ..... 20
- Verify NFS access from a UNIX administration host ..... 21
- Configure and verify CIFS and NFS client access ..... 22

# 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

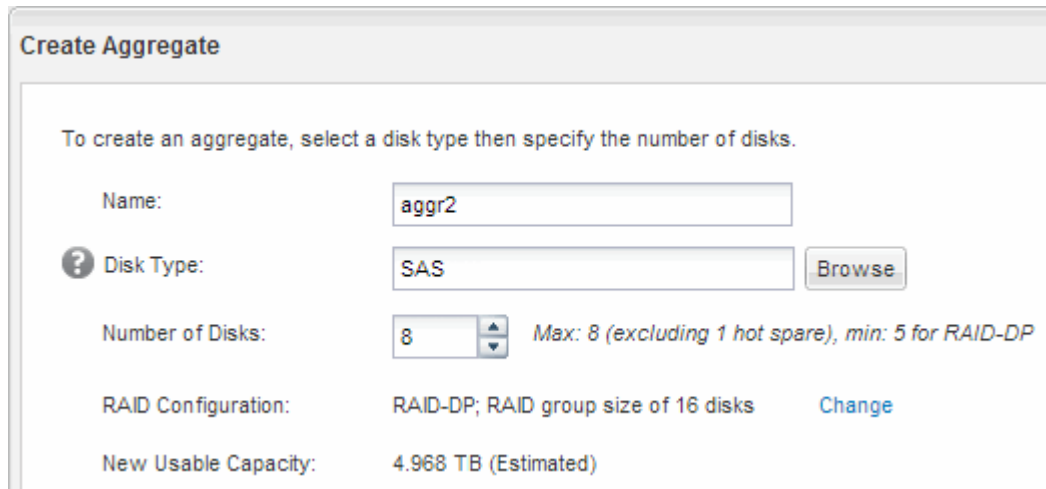
provide physical storage to the volume which you are provisioning.

### 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**.



**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)

### Results

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

## Decide where to provision the new volume

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

### Procedure

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

#### [Creating a basic SVM](#)

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

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

#### [Adding CIFS and NFS access on an existing SVM](#)

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

### Creating and configuring a volume

## Create a basic SVM

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

### Before you begin

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

### About this task

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

### Steps

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

The name must either be a fully qualified domain name (FQDN) or follow another convention that ensures unique names across a cluster.
  - b. Select all the protocols that you have licenses for and that you will eventually use on the SVM, even if you do not want to configure all the protocols immediately.
  - c. Keep the default language setting, C.UTF-8.



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

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

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

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

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

### Storage Virtual Machine (SVM) Setup

1  
Enter SVM basic details

#### SVM Details

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

SVM Name:

? IPspace:

? Data Protocols:  CIFS  NFS  iSCSI  FC/FCoE  NVMe

? Default Language:   
The language of the SVM specifies the default language encoding setting for the SVM and its volumes. Using a setting that incorporates UTF-8 character encoding is recommended.

? Security Style:

Root Aggregate:

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

#### DNS Configuration

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

? Search Domains:

? Name Servers:

- 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.


The screenshot shows the 'Data LIF Configuration' section. It includes a checkbox labeled 'Retain the CIFS data LIF's configuration for NFS clients.' Below this, the text 'Data Interface details for CIFS' is displayed. There are two main input areas: 'Assign IP Address:' with a dropdown menu set to 'Without a subnet' and a 'Change' link next to the IP address '10.224.107.199'; and 'Port:' with a text input field containing 'abccorp\_1:e0b' and a 'Browse...' button.

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.

The screenshot shows the 'CIFS Server Configuration' section. It contains five input fields: 'CIFS Server Name' with 'vs0.example.com', 'Active Directory' with 'AUTH.SEC.EXAMPLE.COM', 'Organizational Unit' with 'CN=Computers', 'Administrator Name' with 'adadmin', and 'Administrator Password' with a masked password represented by seven dots.

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.




—  **NIS Configuration {Optional}** —

Configure NIS domain on the SVM to authorize NFS users.

Domain Names:

IP Addresses:

 Database Type:  group  passwd  netgroup

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

10. Click **Submit & Continue**.

The following objects are created:

- A data LIF named after the SVM with the suffix “\_cifs\_nfs\_lif1”
- A CIFS server that is part of the AD domain
- An NFS server

11. For all other protocol configuration pages that are displayed, click **Skip** and configure the protocol later.

12. When the **SVM Administration** page is displayed, configure or defer configuring a separate administrator for this SVM:

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

13. Review the **Summary** page, record any information you might require later and then click **OK**.

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

## Results

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

## What to do next

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

## Related information

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

## Add CIFS and NFS access to an existing SVM

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

### Before you begin

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

- The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
- The Active Directory (AD) domain that this SVM will join, along with the credentials required to add the SVM to it
- NIS information if your site uses NIS for name services or name mapping
- Any external firewalls must be appropriately configured to allow access to network services.
- The time on the AD domain controllers, clients, and SVM must be synchronized within five minutes of each other.
- The CIFS and NFS protocols must be allowed on the SVM.

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

### About this task

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

### Steps

1. Navigate to the area where you can configure the protocols of the SVM:

- Select the SVM that you want to configure.
- In the **Details** pane, next to **Protocols**, click **CIFS**.

Protocols: NFS CIFS FC/FCoE

2. In the **Data LIF Configuration** section of the **Configure CIFS protocol** dialog box, create a data LIF for the SVM:

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

- Specify a name for the CIFS server that is unique in the AD domain.
- Specify the FQDN of the AD domain that the CIFS server can join.
- If you want to associate an organizational unit (OU) within the AD domain other than CN=Computers, enter the OU.
- Specify the name and password of an administrative account that has sufficient privileges to add the CIFS server to the OU.
- If you want to avoid unauthorized access to all the shares on this SVM, select the option to encrypt

data using SMB 3.0.

▲ **CIFS Server Configuration**

CIFS Server Name:	<input type="text" value="vs0.example.com"/>
Active Directory:	<input type="text" value="AUTH.SEC.EXAMPLE.COM"/>
Organizational Unit:	<input type="text" value="CN=Computers"/>
Administrator Name:	<input type="text" value="adadmin"/>
Administrator Password:	<input type="password" value="••••••"/>

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.

Provision a volume for CIFS storage (Optional).

Share Name:	<input type="text" value="Eng"/>
Size:	<input type="text" value="10"/> <input type="text" value="GB"/> ▼
Permission:	<input type="text" value="Administrators - Full Control"/> <a href="#">Change</a>

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

5. Skip the **Provision a volume for CIFS Storage** area, because it provisions a volume for only CIFS access—not for multiprotocol access.

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

7. Enable NFS:

a. From the SVMs tab, select the SVM for which you want to enable NFS and click **Manage**.

b. In the **Protocols** pane, click **NFS** and then click **Enable**.

8. If your site uses NIS for name services or name mapping, configure NIS:

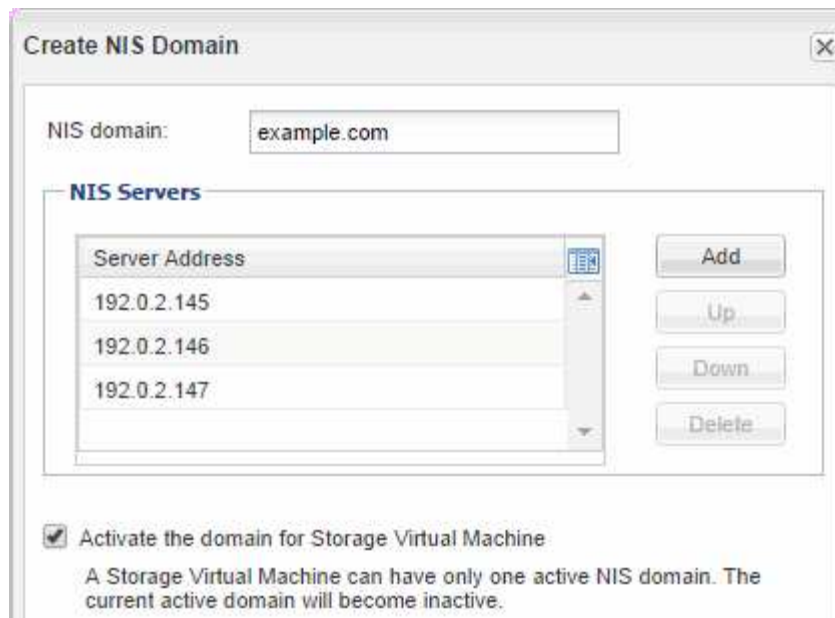
a. In the **Services** window, click **NIS**.

b. In the **NIS** window, click **Create**.

c. Specify the domain of the NIS servers.

d. Add the IP addresses of the NIS servers.

e. Select **Activate the domain for Storage Virtual Machine**, and then click **Create**.



### What to do next

Open the export policy of the SVM root volume.

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

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

#### About this task

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

#### Steps

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

**Create Export Rule** [X]

Client Specification: 0.0.0.0/0

Rule Index: 1

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:

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

*Superuser access is set to all*

## 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.

**Create LDAP Client**

**General** | Binding

LDAP Client Configuration:

**Servers**

Active Directory Domain

Preferred Active Directory Servers

Server
192.0.2.145

Active Directory Servers

- e. 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:  ▼

Bind DN (User):

Bind user password:

Base DN:

Tcp port:  ▲▼

**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.

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**.

**Active LDAP Client**

LDAP client name: vs0client1

Enable LDAP client

Active Directory Domain: example.com

Servers

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**.

**Edit Storage Virtual Machine**

Details Resource Allocation **Services**

Name service switches are used to look up and retrieve user information to provide proper access to clients. The order of the services listed determines in which order the name service sources are consulted to retrieve information.

Name Service Switch

hosts:	files	dns	
namemap:	ldap	files	
group:	ldap	files	nis
netgroup:	ldap	files	nis
passwd:	ldap	files	nis

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

## Map UNIX and Windows user names

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



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

### About this task

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

### Steps

1. Decide on a method of name mapping—name mapping conversion rules, default user mappings, or both—by considering the following factors:

- Conversion rules use regular expressions to convert one user name to another, which is useful if you want to control or track access at an individual level.

For example, you can map UNIX users to Windows users in a domain, and vice versa.

- Default users enable you to assign a user name to all users who are not mapped by implicit mappings or name mapping conversion rules.

Each SVM has a default UNIX user named “pcuser” but does not have a default Windows user.

2. Navigate to the **SVMs** window.
3. Select the SVM that you want to configure.
4. Click the **SVM Settings** tab.
5. **Optional:** Create a name mapping that converts UNIX user accounts to Windows user accounts, and vice versa:
  - a. In the **Host Users and Groups** pane, click **Name Mapping**.
  - b. Click **Add**, retain the default **Windows to UNIX** direction, and then create a regular expression that produces a UNIX credential when a Windows user tries to access a file that uses UNIX file permissions.

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

Add Name Mapping Entry	
Direction:	Windows to UNIX
Position:	1
Pattern:	ENG\\(.+)
Replacement:	\\1

- 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.

**Add Name Mapping Entry**

Direction:

Position:

Pattern:

Replacement:

- 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.

**Name Mapping**

Position	Pattern	Replacement
<b>UNIX to Windows</b>		
2	(.)	ENG\\1
<b>Windows to UNIX</b>		
1	ENG\\(.+)	\\1

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

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

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

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

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

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

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

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

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

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

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

**What to do next**

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

# Create and configure a volume

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

## Steps

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

The Create Volume dialog box is displayed.

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

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

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

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

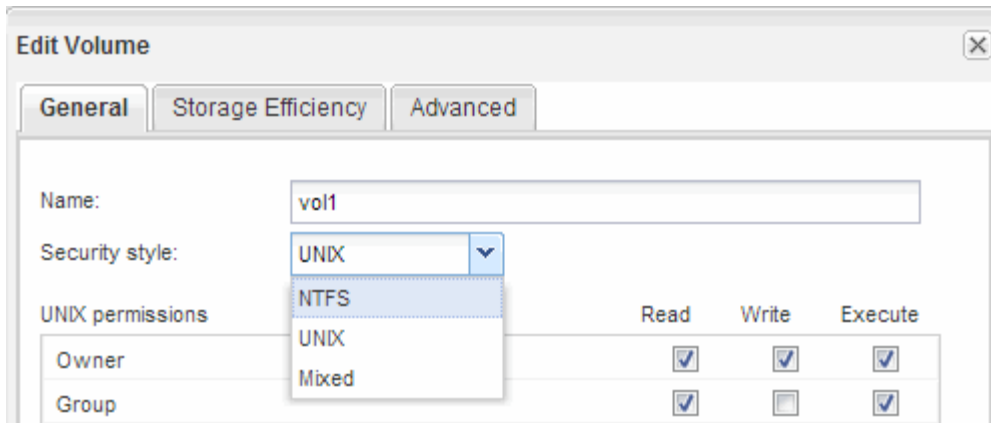
Path	Storage Object
/	vs0examplecom_root
data	data
vol1	vol1

Path	Storage Object
/	vs0examplecom_root
data	data
data/ vol1	vol1

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**.

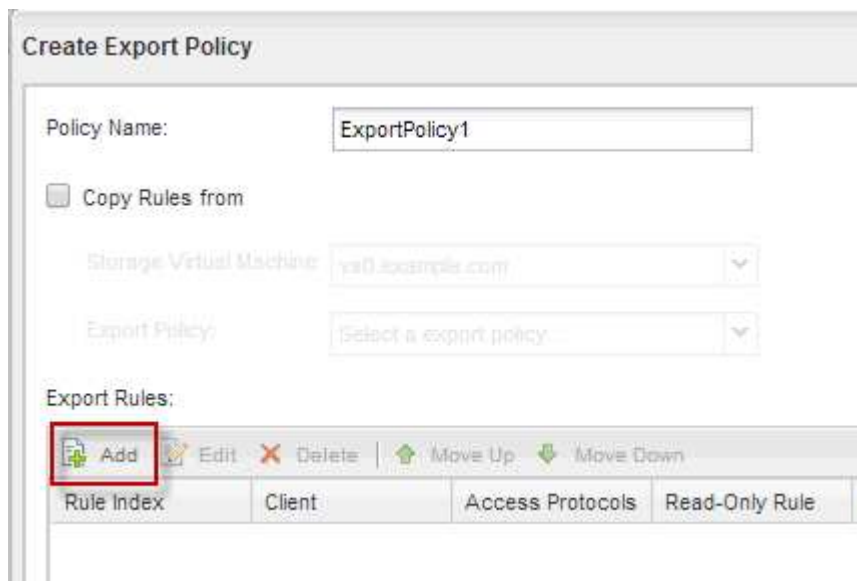
The updated share access permissions are listed in the Share Access Control pane.

# Create an export policy for the volume

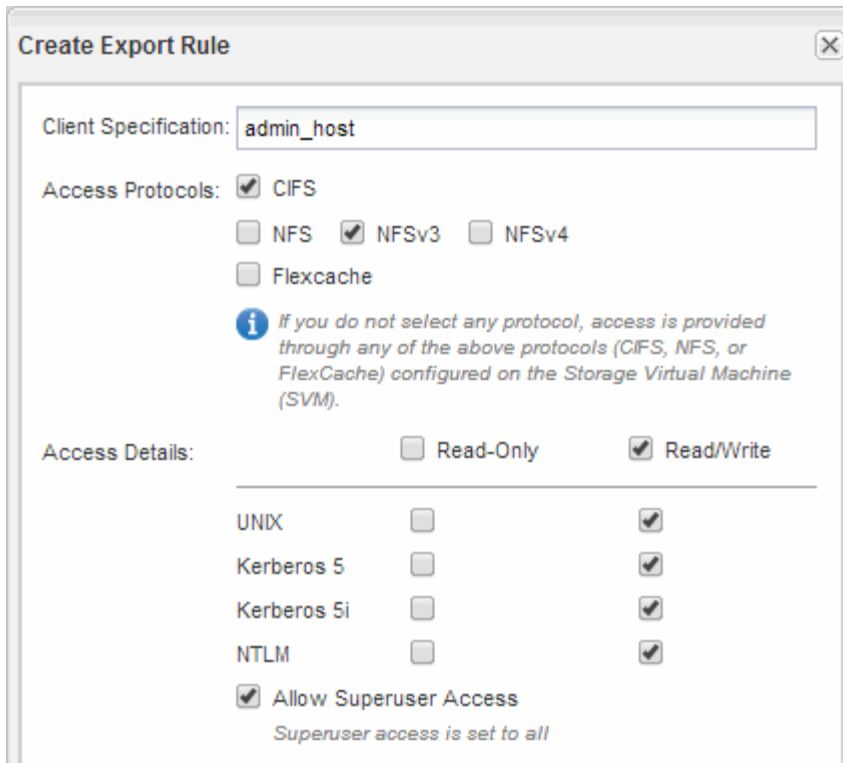
Before any NFS clients can access a volume, you must create an export policy for the volume, add a rule that permits access by an administration host, and apply the new export policy to the volume.

## 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	<ol style="list-style-type: none"> <li>a. Log in to a Windows client as an administrator who has sufficient administrative rights to manage NTFS permissions.</li> <li>b. In Windows Explorer, right-click the drive, and then select <b>Properties</b>.</li> <li>c. Select the Security tab, and adjust the security settings for the groups and users as required.</li> </ol>
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**.

**Create Export Rule**

Client Specification:

Rule Index:

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
<hr/>		
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*

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.

## Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.