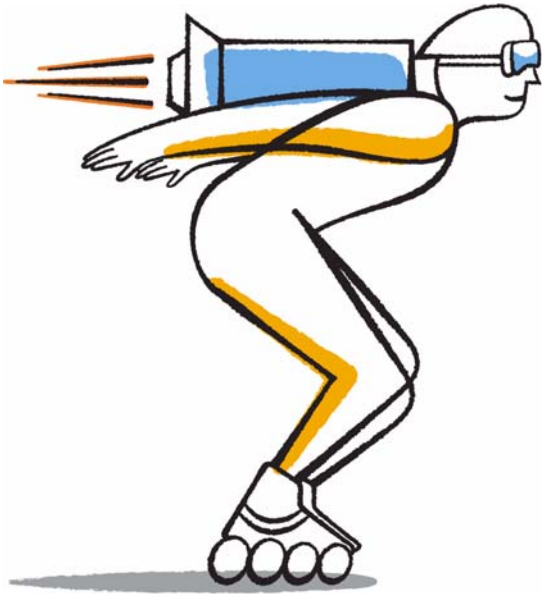
Data ONTAP® 8.1

CIFS/SMB Express Guide
For 7-Mode Administrators Learning Cluster-Mode



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: doccomments@netapp.com

Part number: 215-07234_B0
Updated for Data ONTAP 8.1.1
January 2013

Contents

Deciding whether to use this guide

This guide describes how to set up CIFS access for clients with Data ONTAP operating in Cluster-Mode. It includes information to help administrators who are familiar with Data ONTAP operating in 7-Mode.

You should use this guide if you want a standard configuration following NetApp best practices, and you do not want information about all the available options or a lot of conceptual background for the tasks.

- This guide assumes that your storage system has been successfully installed and a cluster has been created.
- This guide assumes you have downloaded and are running OnCommand System Manager 2.0.2 or later for all applicable tasks.

  It does not include procedures using the Data ONTAP CLI except when the CLI is the only way to complete a task.
- This guide describes how to configure a system with FlexVol volumes only.

  It does not include information about configuring Infinite Volumes.

If these assumptions are not correct for your installation, or if you want more conceptual background information, you should see the following documentation instead:

- *Data ONTAP Software Setup Guide for Cluster-Mode* (for new systems)
- *Data ONTAP System Administration Guide for Cluster-Mode* (for Vserver creation)
- *Data ONTAP File Access and Protocols Management Guide for Cluster-Mode* (for NFS and CIFS)
- *OnCommand System Manager Help* (available both from within the product and as a PDF download)

This documentation is available from the Product Documentation section of the NetApp Support Site.

Related information

Documentation on the NetApp Support Site: support.netapp.com

Mode differences in CIFS setup

CIFS setup in a Cluster-Mode environment differs from CIFS setup in 7-Mode in a few important ways.

CIFS server In a Cluster-Mode environment, you must create a CIFS server to enable access to your storage system by CIFS clients. When you use the Vserver create wizard, the CIFS server is created for you if you select CIFS as a protocol.

Export policies In Cluster-Mode, every volume has an export policy. This is a change from 7-Mode, where exports are used only with NFS clients.

Export policies permit you to control access to volumes in ways that are not possible with share-level controls. For example, you can define an export policy that prevents connections from clients in specific subnets, or can create access rules that apply equally to NFS and CIFS clients.

If you prefer to use traditional methods of controlling access for CIFS clients, you can define an open export policy and use Windows-based authentication and share-level access controls.

Default CIFS shares When you set up CIFS, Data ONTAP creates default CIFS shares for interprocess communication and administrative purposes. The administrative IPC$ share is created in both 7-Mode and Cluster-Mode environments. However, the ETC$ share that is created in 7-Mode is not created in Cluster-Mode because the `/etc` directory that it maps to does not exist in Cluster-Mode.

Home directory shares As in a 7-Mode environment, in Cluster-Mode you can use the Data ONTAP home directory functionality to create users' home directories and automatically offer each user a dynamic share to their home directory without creating an individual CIFS share for each user.

However, home directory shares are defined differently in Cluster-Mode than they are in 7-Mode. In Cluster-Mode, home directory share names are specified when you create or modify a share, and use patterns to match users to shares. This permits you more flexibility than the static configuration options that are available to you in 7-Mode using the `options cifs.home_dir_namestyle` registry option.

Related concepts

How export policies are used with CIFS access on page 6
How Data ONTAP enables dynamic CIFS home directories on page 7

How export policies are used with CIFS access

Export policies determine access to Vserver volumes with CIFS. To access data in a Vserver using CIFS, an export policy that allows CIFS access is created on a Vserver and then associated with volumes containing CIFS shares.

An export policy has a rule or rules applied to it that specify which clients are allowed access to the data and what authentication protocols are supported for read-only and read/write access. Client access can be configured to allow access to all clients, a subnet of clients, or a specific client. CIFS access can be configured to allow authentication using Kerberos and/or NTLM authentication when determining read-only and read/write access to data.

Export rules apply to client machines not to Windows users and groups. Export rules do not replace Windows user and group-based authentication and authorization. Export rules provide another layer of access security in addition to share and file-access permissions.

The administrator can configure rules that provide access to both NFS and CIFS hosts and associate that rule with an export policy, which can then be associated with the volume that contains data to which CIFS and NFS hosts both need access. Alternatively, if there are some volumes where only CIFS clients require access, the administrator can configure an export policy with rules that only allow access using the CIFS protocol and using only Kerberos and/or NTLM read-only and write authentication access rights. The export policy is then associated to the volumes where only CIFS access is desired.

> **Note:** If an export policy with rules that allow access to the desired clients over CIFS and allows access rights using Kerberos and/or NTLM is not associated to the volume containing the CIFS shares, hosts cannot access data using CIFS (even if share ACLs and file permissions are configured to allow access to the requestor).

Additional information about export policies

If you want to implement a custom export policy, you require additional information about how export policies work and how to implement them. This information is available in other guides.

When you require more information about export policies

For volumes that contain CIFS shares, the default export policy might meet your requirements. If it does, you do not have to create a custom export policy, and do not require additional information about how to configure one.

A default export policy with a single rule is created and applied to the root volume of the Vserver when you create a Vserver in System Manager. This default export policy permits access to any client, using any access protocol, including CIFS. Users are granted read-only and read/write access, but no one is permitted root access.

For volumes that contain CIFS shares, an open export policy like the default policy is appropriate if you control access to data on the volume using Windows-based authentication and share level access controls.

Sometimes you might want to implement a custom export policy that is more restrictive than the default policy. For example, if you permit both NFS and CIFS access to a volume, you might want to create a custom export policy with separate rules for NFS and CIFS clients.

Information about creating a custom export policy

If you choose to create a custom export policy, you should see the following guides for more information so that you can implement the policy correctly:

Data ONTAP NFSv3 Express Guide
Includes a summary of how export policies work, information about how to create export policies in System Manager, a comparison of 7-Mode exports and Cluster-Mode export policies, and example export policies.

Data ONTAP File Access and Protocols Management Guide for Cluster-Mode
Includes complete information about how export policies work in both NFS and CIFS environments, and information about how to create export policies at the command line.

How Data ONTAP enables dynamic CIFS home directories

Data ONTAP CIFS home directories enable you to configure a share that maps to different directories based on the user that connects to it and a set of variables. Instead of having to create separate shares for each user, you can configure a single share with a few home directory parameters to define a user's relationship between an entry point (the share) and their home directory (a directory on the Vserver).

There are four variables that determine how a user is mapped to a directory:

Share name
This is the name of the share that you create that the user connects to. It can be static (for example, home), dynamic (for example, *`%w`*), or a combination of the two. You must set the home directory property for this share.

The share name can use the following dynamic names:

- *`%w`* (the user's Windows user name)
- *`%d`* (the user's Windows domain name)
- *`%u`* (the user's mapped UNIX user name)

Share path
This is the relative path, defined by the share and therefore associated with one of the share names, that is appended to each search path to generate the user's entire home directory path from the root of the Vserver. It can be static (for example, `home`), dynamic (for example, `%w`), or a combination of the two (for example, `eng/%w`).

Search paths This is the set of absolute paths from the root of a Vserver that you specify to tell Data ONTAP where to search for home directories. You specify one or more search paths by using the `vserver cifs home-directory search-path add` command. If you specify multiple search paths, Data ONTAP tries them in the order specified until it finds a valid path.

Directory This is the user's home directory that you create for the user. It is usually the user's name. You must create it in one of the directories defined by the search paths.

As an example, consider the following setup:

- User: John Smith
- User domain: acme
- User name: jsmith
- Vserver name: vs1
- Home directory share name #1: home - share path: `%w`
- Home directory share name #2: *`%w`* - share path: `%d/%w`
- Search path #1: `/aggr0home/home`
- Search path #2: `/aggr1home/home`
- Search path #3: `/aggr2home/home`
- Home directory: `/aggr1home/home/jsmith`

Scenario 1: The user connects to `\\vs1\home`. This matches the first home directory share name and generates the relative path `jsmith`. Data ONTAP now searches for a directory named `jsmith` by checking each search path in order:

- `/aggr0home/home/jsmith` does not exist; moving on to search path #2.
- `/aggr1home/home/jsmith` does exist, therefore search path #3 is not checked; the user is now connected to his home directory.

Scenario 2: The user connects to `\\vs1\jsmith`. This matches the second home directory share name and generates the relative path `acme/jsmith`. Data ONTAP now searches for a directory named `acme/jsmith` by checking each search path in order:

- `/aggr0home/home/acme/jsmith` does not exist; moving on to search path #2.
- `/aggr1home/home/acme/jsmith` does not exist; moving on to search path #3.
- `/aggr2home/home/acme/jsmith` does not exist; the home directory does not exist, therefore the connection fails.

Worksheet: Cluster and network information

You can use a worksheet to collect the information that you require to set up CIFS access for clients. You must obtain the IP addresses and other information about your cluster and network from your storage and network administrators before you begin.

Information for Vserver configuration

DNS

When you create the Vserver, you must configure Domain Name Service (DNS) using a DNS server that contains records for the Active Directory service.

		Host name	**IP address**
	Primary domain server		
	Search domains (optional: up to 5)		
1			
2			
3			
4			
5			
	Name servers (at least 1; up to 3)		
1			
2			
3			

Data interfaces

You must create at least one data interface on the Vserver for use by the CIFS protocol. You should create a data interface on each node that hosts volumes used by the Vserver.

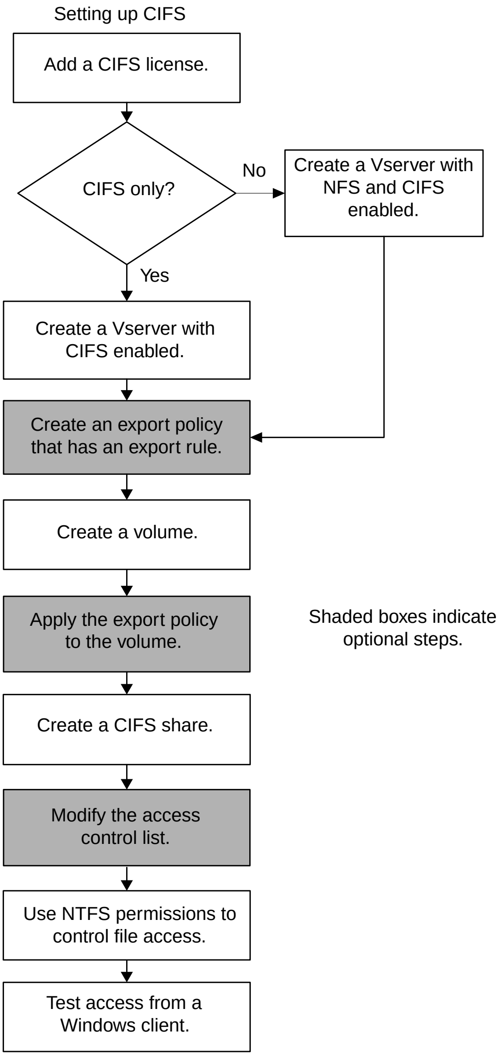
Protocol	**Interface name**	**Home node:port**	**IP address**	**Netmask**	**Gateway**
CIFS					
CIFS					

CIFS server setup

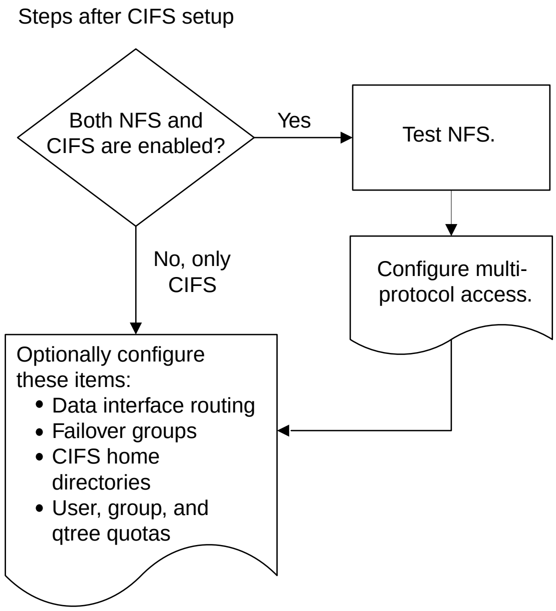
	Description	Value
CIFS server name	Name of the CIFS server that you are setting up on the storage system	
Fully qualified domain name	Windows Active Directory (AD) Domain for the storage system to join	
Admin name	User with privileges to join the Windows AD domain	
Admin password	Password of that user	

Setting up CIFS

You should review the steps involved in setting up CIFS, including the optional tasks that you might choose to perform after the setup. Creating a Vserver that supports both NFS and CIFS during setup is only necessary if you plan to enable multi-protocol access to data.


Setting up CIFS
Add a CIFS license.
CIFS only?
No
Create a Vserver with NFS and CIFS enabled.
Yes
Create a Vserver with CIFS enabled.
Create an export policy that has an export rule.
Create a volume.
Apply the export policy to the volume.
Shaded boxes indicate optional steps.
Create a CIFS share.
Modify the access control list.
Use NTFS permissions to control file access.
Test access from a Windows client.

Next steps


Steps after CIFS setup
Both NFS and CIFS are enabled?
Yes
Test NFS.
Configure multi-protocol access.
No, only CIFS
Optionally configure these items:
• Data interface routing
• Failover groups
• CIFS home directories
• User, group, and qtree quotas

Related references

Next steps: Multi-protocol access and optional configuration on page 29

Adding a CIFS license

You must ensure that the storage system has a CIFS license. A CIFS license is required to enable CIFS access to the storage system.

About this task

If you need to purchase a license, contact your NetApp or sales partner representative.

Steps

1. Start System Manager, and in the **Home** tab, double-click the appropriate storage system.

   The left navigation pane displays the cluster hierarchy.
2. Ensure your cluster is selected, and then click **Configuration** > **System Tools** > **Licenses**.
3. Click **Add**.
4. In the **Add License** dialog box, enter the CIFS license code and click **Add**.

Creating a Vserver with CIFS enabled

The Vserver is the basic building block of all Cluster-Mode configurations. The Vserver contains the volume, CIFS server, and logical interfaces that are used to access data using CIFS.

Before you begin

- The cluster should have at least one data aggregate available that you can use when creating the Vserver.
- You must have set the time zone and synchronized the time across the cluster by configuring NTP.

  You can verify this in System Manager by selecting the cluster and clicking **Configuration > System Tools > DateTime**.

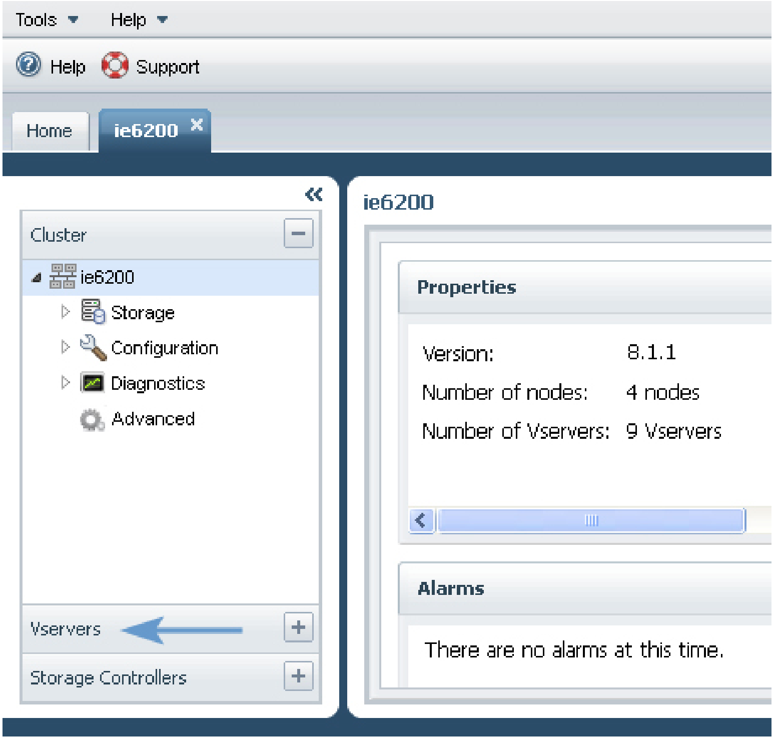
  > **Note:** You should use the Windows Active Directory domain controller as an NTP time server.

About this task

If you want to create a Vserver that has both CIFS and NFS enabled, do **not** use this procedure. Follow the procedure to create a Vserver that supports CIFS and NFS instead.

Steps

1. Start System Manager, and in the **Home** tab, double-click the appropriate storage system.
2. In the left navigation pane, click **Vservers**.



Version: 8.1.1

Number of nodes: 4 nodes

Number of Vservers: 9 Vservers

There are no alarms at this time.

3. In the right pane, click **Create**.
4. Follow the instructions in the **Create Vserver** wizard:

   a) When prompted to select a protocol, select **CIFS**.

   b) Complete the **Configure DNS** screen.

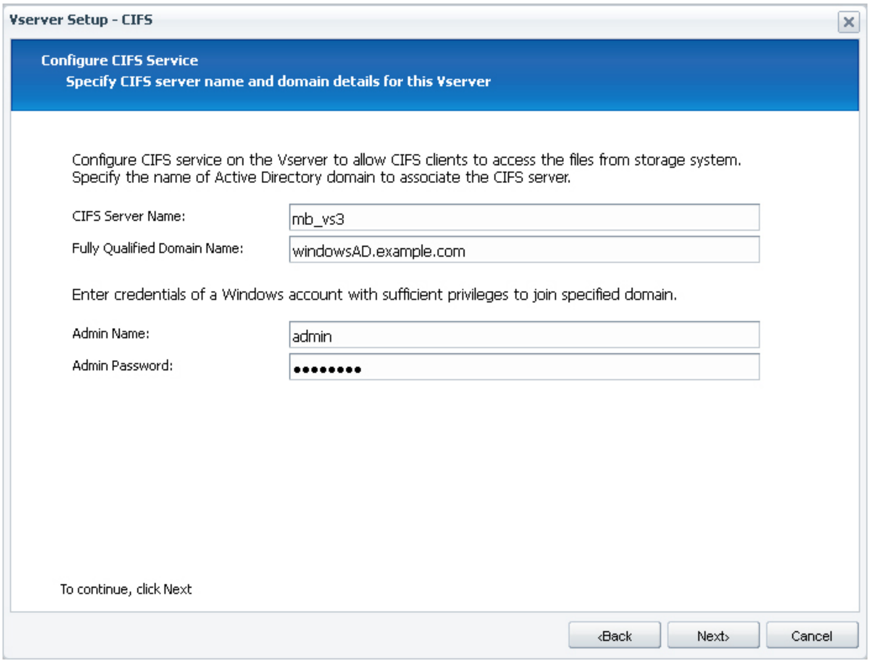
   You should use the Windows Active Directory (AD) Domain Controller as the primary domain server for the storage system. You also have to enter information about at least one additional name server.

   c) Create one or more data interfaces.

   Data interfaces are used by NFS and CIFS clients to access the storage system. You can enable one protocol or both protocols.

   d) When prompted, configure the CIFS service for the Vserver by entering all of the following information:

   - The CIFS server name
     The name must be 15 characters or fewer, and must **not** contain any of the following characters: @ # * ( ) = + [ ] | ; : " , < > / ?
   - The FQDN of an Active Directory (AD) domain that the CIFS server can join
   - The user name and password of an administrator with sufficient privileges to allow the CIFS server to join the domain


Vserver Setup - CIFS
Configure CIFS Service
Specify CIFS server name and domain details for this Vserver

Configure CIFS service on the Vserver to allow CIFS clients to access the files from storage system. Specify the name of Active Directory domain to associate the CIFS server.

CIFS Server Name: mb_vs3

Fully Qualified Domain Name: windowsAD.example.com

Enter credentials of a Windows account with sufficient privileges to join specified domain.

Admin Name: admin

Admin Password: ●●●●●●●●●

To continue, click Next

e) Select **Local User** and create a test local UNIX user and group on the Vserver.

This test UNIX user should be given the name of the Windows user that you plan to use to test CIFS access after the storage system's configuration is complete. The Windows user will be mapped to this UNIX user at connection time.

Note: Do not use the following default UNIX names or IDs:

- pcuser (User ID 65534), group pcuser (Group ID 65534)
- nobody (User ID 65535), group nobody (Group ID 65535)
- root (User ID 0) , group daemon (Group ID 1)

5. After completing the wizard, select the new Vserver in the left navigation pane and view its storage and configuration.

6. Update the security style of the root volume of the Vserver to be NTFS.

By default, all the volumes you create on the Vserver inherit the security style of the root volume.

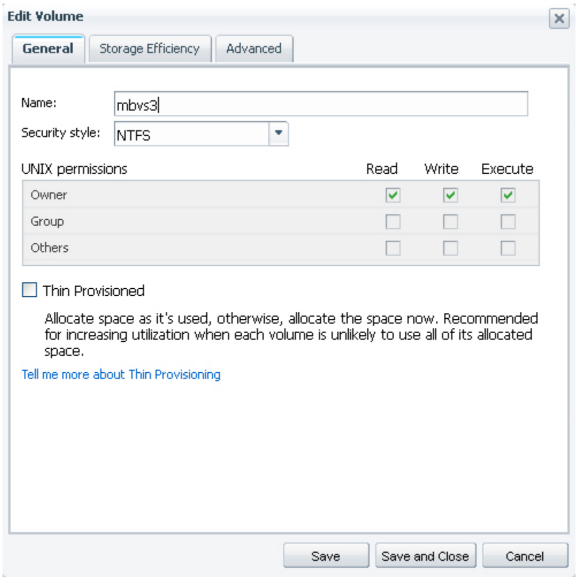
a) From the left navigation pane, click **Storage** > **Volumes**.

The single volume shown in the right pane is the root volume of the Vserver.

b) Click **Edit**.

c) In the **General** tab of the **Edit Volume** dialog box, select **NTFS** for the Security style.

d) Click **Save and Close**.



Name: mbvs3

Security style: NTFS

UNIX permissions	Read	Write	Execute
Owner	☑	☑	☑
Group	□	□	□
Others	□	□	□

□ Thin Provisioned

Allocate space as it's used, otherwise, allocate the space now. Recommended for increasing utilization when each volume is unlikely to use all of its allocated space.

Tell me more about Thin Provisioning

Result

Your Vserver is created with the following:

- A CIFS server that belongs to the specified Active Directory domain
- DNS enabled
- One or more logical data interfaces for client access to data
- Default users and groups (pcuser/pcuser, nobody/nobody, root/daemon)

  The default users and groups are used internally by Data ONTAP to map users that are not explicitly mapped to a local UNIX user, on volumes with UNIX/Mixed security style. If a Windows user accesses a volume that uses the NTFS security style, then NTFS ACLs are used for the authorization process.
- Default CIFS shares `admin$` and `ipc$`
- A default name mapping that maps Windows user names to UNIX user names
- A test local user and group to use when verifying system operation

The Vserver is started automatically. It contains a root volume under which you can junction additional volumes for data storage.

Related tasks

Creating a Vserver with CIFS and NFS enabled on page 17

Creating a Vserver with CIFS and NFS enabled

The Vserver is the basic building block of all Cluster-Mode configurations. The Vserver contains the volume, NFS and CIFS servers, and logical interfaces that are used to access data.

Before you begin

- The cluster should have at least one data aggregate available that you can use when creating the Vserver.
- You must have set the time zone and synchronized the time across the cluster by configuring NTP.

  You can verify that NTP is configured in System Manager by selecting the cluster and clicking **Configuration > System Tools > DateTime**.

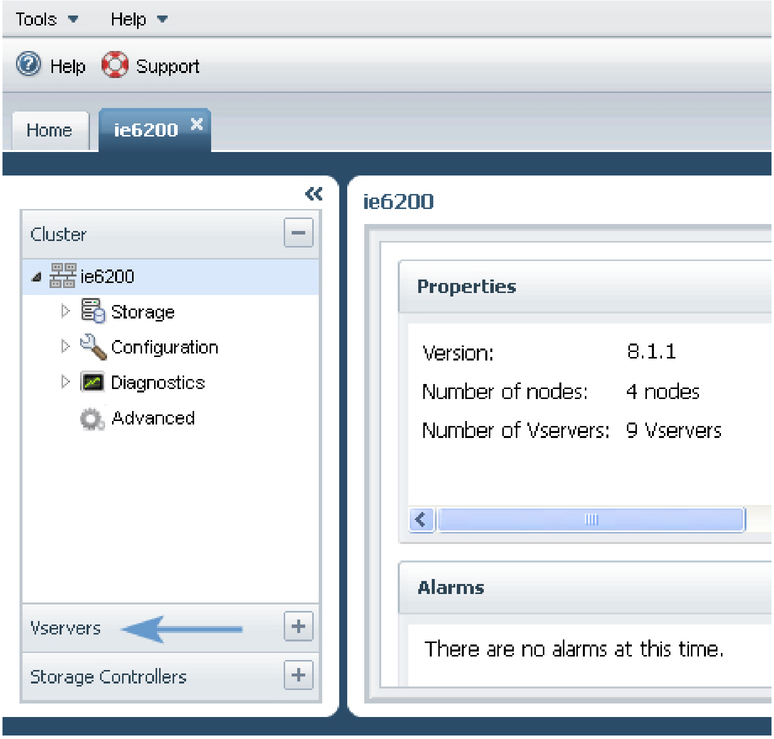
  > **Note:** You should use the Windows Active Directory domain controller as an NTP time server.

About this task

- If you have already created a Vserver with CIFS enabled, skip this procedure.
- If you want to create a Vserver that has only CIFS enabled, do **not** follow this procedure. Follow the procedure to create a Vserver with CIFS enabled instead.

Steps

1. Start System Manager, and in the **Home** tab, double-click the appropriate storage system.
2. In the left navigation pane, click **Vservers**.



Version: 8.1.1

Number of nodes: 4 nodes

Number of Vservers: 9 Vservers

There are no alarms at this time.

3. In the right pane, click **Create**.

4. Follow the instructions in the **Create Vserver** wizard:

a) When prompted to select a protocol, select **NFS** and **CIFS**.

b) Complete the **Configure DNS** screen.

You should use the Windows Active Directory (AD) Domain Controller as the primary domain server for the storage system. You also have to enter information about at least one additional name server.

c) Create one or more data interfaces.

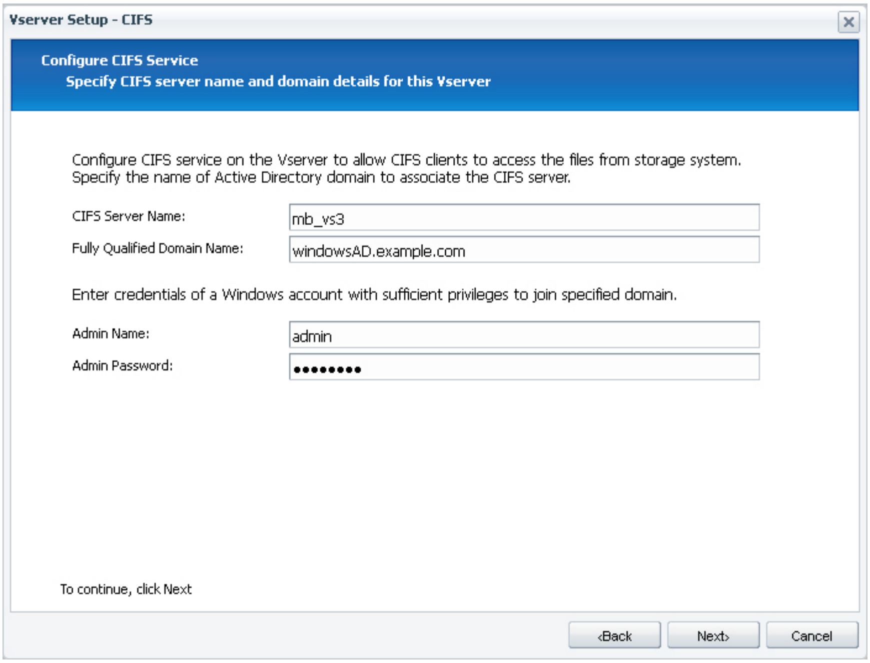
Data interfaces are used by NFS and CIFS clients to access the storage system. You should enable both NFS and CIFS for the data interfaces.

d) When prompted, configure the CIFS server for the Vserver by entering all of the following information:

- The CIFS server name

  The name must be 15 characters or fewer, and must **not** contain any of the following characters: @ # * ( ) = + [ ] | ; : " , < > / ?
- The fully qualified domain name of an Windows AD server whose domain the CIFS server can join

- The user name and password of an administrator with sufficient privileges to allow the CIFS server to join the AD server's domain



Configure CIFS Service

Specify CIFS server name and domain details for this Vserver

Configure CIFS service on the Vserver to allow CIFS clients to access the files from storage system.
Specify the name of Active Directory domain to associate the CIFS server.

CIFS Server Name: mb_vs3

Fully Qualified Domain Name: windowsAD.example.com

Enter credentials of a Windows account with sufficient privileges to join specified domain.

Admin Name: admin

Admin Password: ●●●●●●●●

To continue, click Next

e) When prompted, select **NFS version 3**.

f) Select **Local Users** and click **Next**.

To simplify the setup process, do not select NIS or LDAP at this time.

g) Create one or more test local users and group on the Vserver.

To test CIFS access, you should create a UNIX user that has the name of a Windows user that you plan to use to test CIFS access. The Windows user will be mapped to this UNIX user. To test NFS access, you should create a test UNIX user that you can use from an NFS client.

Note: Do not use the following default UNIX names or IDs:

- pcuser (User ID 65534), group pcuser (Group ID 65534)
- nobody (User ID 65535), group nobody (Group ID 65535)
- root (User ID 0) , group daemon (Group ID 1)

5. After completing the wizard, select the new Vserver in the left navigation pane and view its storage and configuration.

6. If most of the volumes that you create on this Vserver will be accessed by CIFS clients, update the security style of the root volume to be NTFS.

By default, all the volumes you create on the Vserver inherit the security style of the root volume.

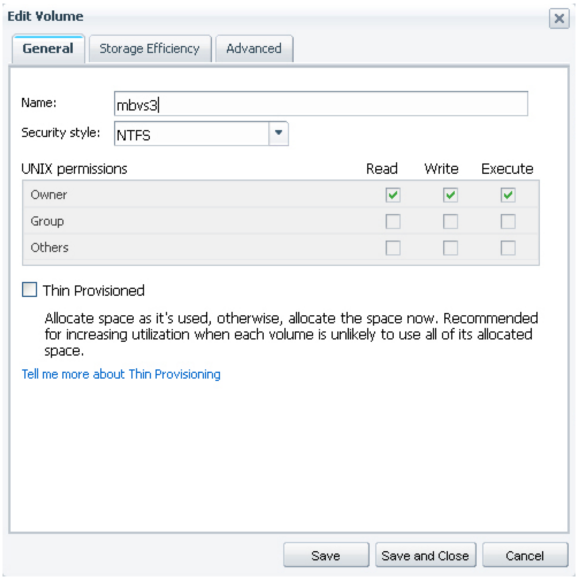
a) From the left navigation pane, click **Storage > Volumes**.

The single volume shown in the right pane is the root volume of the Vserver.

b) Click **Edit**.

c) In the **General** tab of the **Edit Volume** dialog box, select **NTFS** for the Security style.

d) Click **Save and Close**.



Name: mbvs3

Security style: NTFS

UNIX permissions	Read	Write	Execute
Owner	☑	☑	☑
Group	□	□	□
Others	□	□	□

□ Thin Provisioned

Allocate space as it's used, otherwise, allocate the space now. Recommended for increasing utilization when each volume is unlikely to use all of its allocated space.

Tell me more about Thin Provisioning

Result

Your Vserver is created with the following:

- An NFS server that supports NFS version 3
- A CIFS server that belongs to the specified Active Directory domain
- DNS enabled
- One or more logical data interfaces for client access to data
- Default users and groups (pcuser/pcuser, nobody/nobody, root/daemon)
  The default users and groups are used internally by Data ONTAP to map users that are not explicitly mapped to a local UNIX user, on volumes with UNIX/Mixed security style. If a Windows user accesses a volume that uses the NTFS security style, then NTFS ACLs are used for the authorization process.
- Default CIFS shares `admin$` and `ipc$`
- A default name mapping that maps Windows user names to UNIX user names
- A test local user and group to use when verifying system operation

The Vserver is started automatically. It contains a root volume under which you can junction additional volumes for data storage.

Related tasks

Creating a Vserver with CIFS enabled on page 13

Creating an export policy in System Manager

Export policies contain a set of rules to specify the access that clients have to volumes in a Vserver.

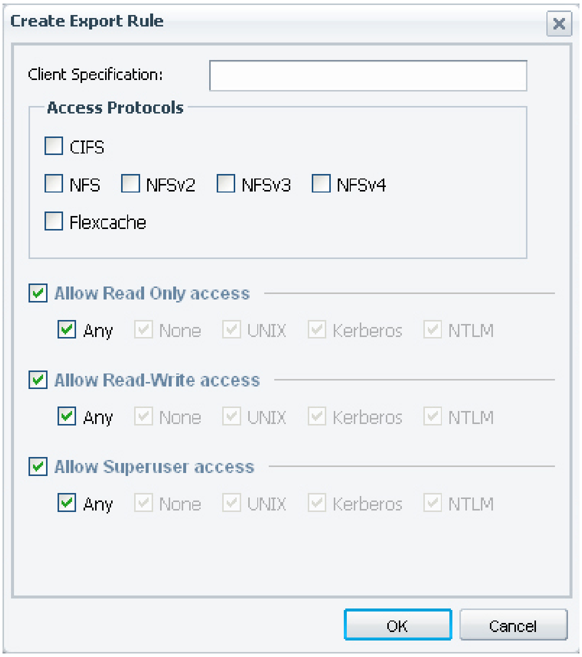
About this task

If you permit access using CIFS only, the default export policy and rule that is created by System Manager might meet your requirements. If it does, you do not need to create a custom export policy.

Steps

1. From the **Home** tab, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.
3. In the navigation pane, select the Vserver and click **Policies** > **Export Policies**.
4. Click **Create Policy** and specify a policy name.
5. Click **Add** to add an export rule to the policy.
6. In the **Create Export Rule** dialog box, perform the following steps:
    a) Specify the client that requires access to the data.

       You can enter 0.0.0.0/0 to enable access by all clients.



Create Export Rule

Client Specification:

Access Protocols

□ CIFS

□ NFS □ NFSv2 □ NFSv3 □ NFSv4

□ Flexcache

☑ Allow Read Only access

☑ Any ☑ None ☑ UNIX ☑ Kerberos ☑ NTLM

☑ Allow Read-Write access

☑ Any ☑ None ☑ UNIX ☑ Kerberos ☑ NTLM

☑ Allow Superuser access

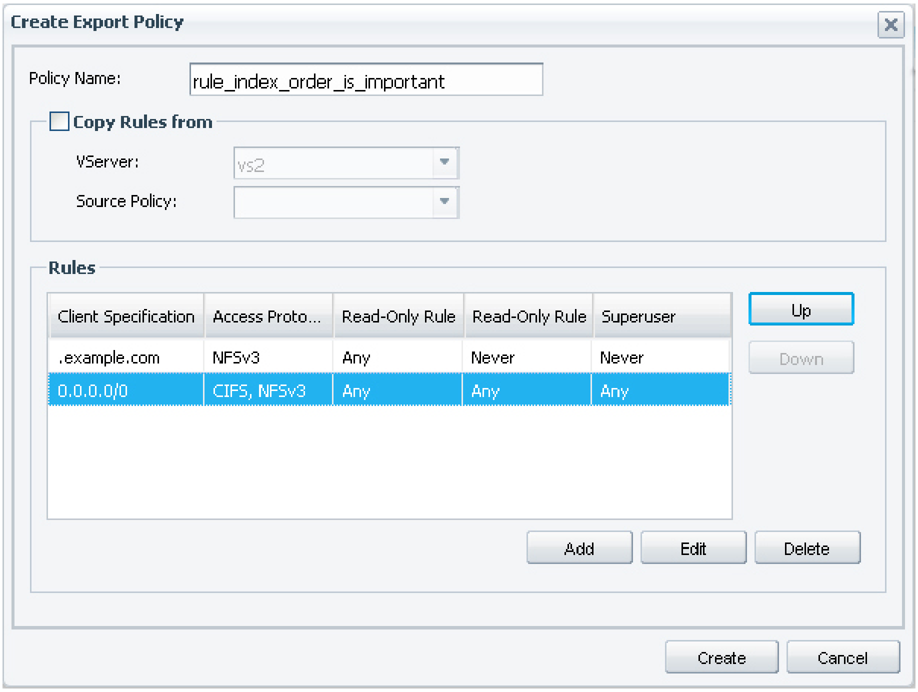
☑ Any ☑ None ☑ UNIX ☑ Kerberos ☑ NTLM

b) Select **CIFS** or **NFSv3** or select both.
c) Select one or more access types and its security type.
d) Click **OK**.

   The first rule is added to the export policy.

7. Click **Add** and complete the dialog box to add another export rule to the policy.

   The export policy now has two rules that are processed in the order that they are shown.



Policy Name: rule_index_order_is_important

☐ Copy Rules from

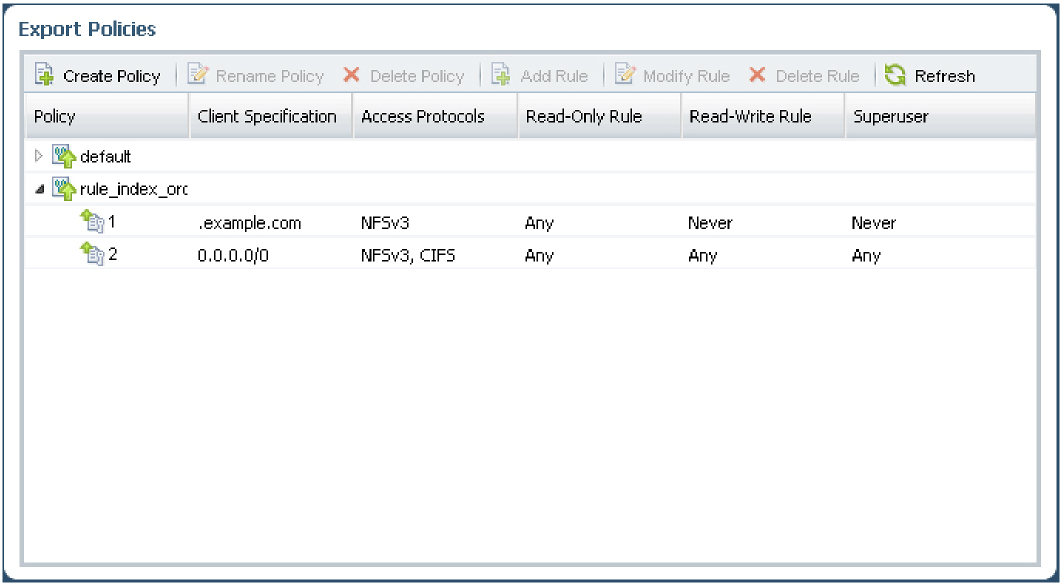
VServer: vs2

Source Policy:

Rules

Client Specification	Access Proto...	Read-Only Rule	Read-Only Rule	Superuser
.example.com	NFSv3	Any	Never	Never
0.0.0.0/0	CIFS, NFSv3	Any	Any	Any

8. To change which rule is evaluated first, select a rule and click **Up** or **Down** to change its position in the list.
9. Click **Create** to create the export policy.



Policy	Client Specification	Access Protocols	Read-Only Rule	Read-Write Rule	Superuser
▷ default					
◢ rule_index_orc					
1	.example.com	NFSv3	Any	Never	Never
2	0.0.0.0/0	NFSv3, CIFS	Any	Any	Any

When a client attempts to connect, the storage system checks the client against the first export rule. If the client matches the specification, the first rule is applied and the other rules are not checked. Rule processing stops after a match is found. Therefore, if you swap the order of the two rules shown in this export policy, then all clients, including those in example.com, are given full access to the volume.

Related concepts

How export policies are used with CIFS access on page 6

Related references

Additional information about export policies on page 6

Creating a volume

You can create a FlexVol volume for your data using the Create Volume dialog box. You should always create a volume for your data, rather than storing data in the root volume of a Vserver.

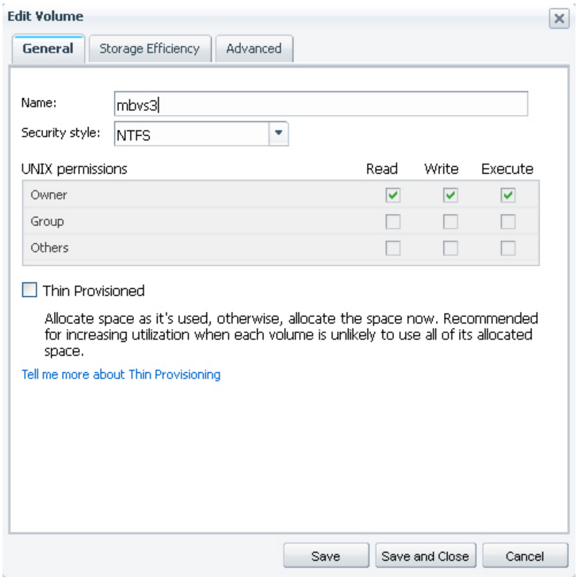
Steps

1. From the **Home** tab, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.
3. In the navigation pane, select the Vserver and click **Storage > Volumes**.
4. Click **Create**.
5. If you want to change the default name, specify a new name.
6. Select the containing aggregate for the volume.
7. Specify the size of the volume, and accept the default value for the snapshot reserve.

   The default space reserved for Snapshot copies is five percent for NAS volumes on storage systems running Data ONTAP 8.1.
8. Click **Create**.
9. Verify that the volume you created is included in the list of volumes in the **Volume** window.
10. Verify that the volume you created is junctioned under the root volume by going to **Storage > Namespace**.
11. Check the security style of the volume, and update it if it does not meet your requirements.

    If the volume will be accessed by CIFS clients, you should select NTFS as the security style of the volume. If the volume will be accessed exclusively by NFS clients, the security style should be UNIX.

a) Select the volume you created, and click **Edit**.
b) In the **General** tab, check and update the value for **Security Style** if necessary.
c) Click **Save and Close**.



Name: mbvs3

Security style: NTFS

UNIX permissions	Read	Write	Execute
Owner	☑	☑	☑
Group	□	□	□
Others	□	□	□

□ Thin Provisioned

Allocate space as it's used, otherwise, allocate the space now. Recommended for increasing utilization when each volume is unlikely to use all of its allocated space.

Tell me more about Thin Provisioning

If the volume has UNIX style security, by default it is granted UNIX 700 "read write execute" permissions for the Owner.

Applying export policies to volumes

When a volume is created, it automatically inherits the default export policy of the root volume of the Vserver. This procedure describes how to apply your customized export policy.

Steps

1. From the **Home** tab, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.
3. In the navigation pane, select the Vserver and click **Storage** > **Namespace**.
4. Select the volume and click **Change Export Policy**.
5. Select the export policy and click **Change**.
6. Verify that the Export Policy column in the **Namespace** window displays the export policy that you applied to the volume.

Creating test CIFS shares and controlling access

You should create a test CIFS share and adjust share access permissions or NTFS file and folder permissions to meet your requirements.

Access to data stored on CIFS shares can be controlled using share access controls, NTFS file and folder permissions, or a combination of the two. Most CIFS administrators choose to use NTFS file and folder permissions, while leaving share access controls unrestricted.

Creating a CIFS share

You can create a share that enables you to specify a folder, qtree, or volume that CIFS users can access.

Steps

1. From the **Home** tab, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.
3. In the navigation pane, select the Vserver and click **Storage > Shares**.
4. Click **Create Share**.
5. Click **Browse** and select the folder, qtree, or volume that should be shared.
6. Specify a name for the new CIFS share.
7. Provide a description for the share and click **Create**.

Result

The share is created with the access permissions set to Full Control for Everyone in the group.

Modifying the access control list of CIFS shares

If the default access permissions for CIFS shares do not meet your requirements, you can update them by editing the share.

About this task

By default, CIFS shares are created with access permissions that permit Full Control by Everyone. You can update these permissions to be more restrictive, or leave the access controls unrestricted and update the NTFS file and folder permissions instead.

Steps

1. From the **Home** tab, double-click the appropriate storage system.
2. Expand the **Vservers** hierarchy in the left navigation pane.

3. In the navigation pane, select the Vserver and click **Storage** > **Shares**.
4. Select the share whose access you want to change, and click **Edit**.
5. In the **Permissions** tab, click **Add**.
6. Enter the name of a User or Group defined in the Windows Active Directory domain that includes the Vserver.
7. With the new user or group selected, select the permissions that you require, and click **Save**.
8. Verify that the updated share access permission is listed in the **Share Access Control** window.

Related tasks

Controlling access to files using NTFS permissions on page 27

Controlling access to files using NTFS permissions

You can control access to folders and files on the CIFS share using NTFS file permissions.

Steps

1. From a Windows computer, go to **Start** > **All Programs** > **Accessories**, and select **Windows Explorer**.
2. From the **Tools** menu, select **Map network drive**.
3. Complete the **Map network drive** dialog box:

   a) Select a **Drive** letter.

   b) In the **Folder** box, type the IP address of the CIFS data interface you created for the Vserver, and the name of the share.

   #### Example

   If your data interface has the IP address 192.0.2.129 and your share is named share1, you should enter `\\192.0.2.129\share1`.

   > **Note:** You can specify the name of the CIFS server instead of the IP address if you have configured WINS, or the FQDN if you have manually added the CIFS server name to your DNS server.

   c) Select **Connect using a different credentials**, and enter the domain/user name and password of an administrative user authorized to join the domain.

   d) Click **Finish**.

   The drive you selected is mounted and ready.
4. Adjust the NTFS permissions for the drive, or a file or folder that you create on the drive.

   a) Right-click the drive, folder, or file, and select **Properties**.

   b) Select the **Security** tab, and adjust the security settings for the groups and users as required.

5. Remove the drive mapping by selecting **Tools > Disconnect network drive**.

Testing access from a Windows client

You should verify that you have configured CIFS correctly by accessing the CIFS share from a Windows client and writing and reading data to it.

Before you begin

- The export policy must permit read/write access from the Windows computer that you are using for the test.
- You must be logged in as a Windows user that is authenticated to the AD domain that includes the Vserver.
- The share access permissions and NTFS folder or file permissions that you configured for the share must permit read/write access by the test user.

Steps

1. From a Windows computer, go to **Start > All Programs > Accessories**, and select **Windows Explorer**.
2. From the **Tools** menu, select **Map network drive**.
3. Complete the **Map network drive** dialog box:
   a) Select a **Drive** letter.
   b) In the **Folder** box, type the IP address of the CIFS data interface and the name of the share.

      Example

      If your data interface has the IP address 192.0.2.129 and your share is named share1, you should enter `\\192.0.2.129\share1`.

      Note: You can specify the name of the CIFS server instead of the IP address if you have configured WINS, or the FQDN if you have manually added the CIFS server name to your DNS server.

   c) Click **Finish**.
4. Create a test file on the Windows computer, and save it to the newly created drive.

   Example

   Use Notepad to create a text file called `test.txt`.

   If the CIFS server, export policy, and access permissions for your share are configured correctly, the file is saved successfully to the CIFS share.
5. Delete the test file by removing it to the **Recycle Bin**.

Next steps: Multi-protocol access and optional configuration

If you have configured a Vserver that has both NFS and CIFS enabled, you must perform some additional steps to enable multi-protocol access to data. There are also optional tasks that can help you better configure your storage system for your CIFS-only or multi-protocol environment.

Multi-protocol access to data

If you want to enable multi-protocol access to your Vserver by both NFS and CIFS clients, you must complete all of the tasks outlined in the following table.

By working through this guide, you have already completed some tasks. To perform the next steps, you must use the specified guides.

Task	**Reference**
Create a Vserver with both NFS and CIFS enabled.	This guide
Create an export policy.	
Create a volume and apply the export policy to the volume.	
Create a CIFS share and update access permissions.	
Test CIFS access from a Windows client.	
Test NFS access from an NFS client.	*Data ONTAP NFSv3 Express Guide*
Configure NIS or local users and groups and then test authentication.	*Data ONTAP NFSv3 Express Guide*
Enable multi-protocol access to files.	*Data ONTAP Multi-protocol Express Guide*

Optional configuration

You can complete the following optional tasks after CIFS access has been configured and tested:

Task	**Reference**
Configure routing groups and routes for the Vserver's data interfaces.	*Data ONTAP Network Management Guide for Cluster-Mode*
Configure failover groups for data interfaces.	*Data ONTAP Network Management Guide for Cluster-Mode*

Task	**Reference**
Create CIFS home directories.	*Data ONTAP File Access and Protocols Management Guide for Cluster-Mode*
Create user, group, or qtree quotas.	*Data ONTAP Logical Storage Management Guide for Cluster-Mode*

Where to find additional information

There are documents and tools to help you learn about the additional setup and configuration steps your cluster might require.

Technical Reports

TR-3967 Deployment and Best Practices Guide for Data ONTAP 8.1 Cluster-Mode Windows File Services
Describes setting up CIFS in a Cluster-Mode environment, including best practices and troubleshooting information.

Documentation References

Data ONTAP 7-Mode to Cluster-Mode Command Map
Provides a mapping of 7-Mode commands to Cluster-Mode commands.

Data ONTAP File Access and Protocols Management Guide for Cluster-Mode
Describes how to manage file access on NetApp systems with CIFS and NFS protocols.

Data ONTAP Logical Storage Management Guide for Cluster-Mode
Describes how to efficiently manage your logical storage resources using volumes, FlexClone volumes, files and LUNs, deduplication, compression, qtrees, and quotas.

Data ONTAP Network Management Guide for Cluster-Mode
Describes how to connect your cluster to your Ethernet networks and how to manage logical interfaces (LIFs).

Data ONTAP System Administration Guide for Cluster-Mode
Describes general system administration for NetApp systems running Data ONTAP operating in Cluster-Mode.

Tool references

Interoperability Matrix Tool (IMT)
Lists supported combinations of hardware components, software versions, firmware, and drivers.

Related information

All documents and tools are available on the NetApp Support Site: support.netapp.com

Copyright information

Trademark information

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

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