ONTAP® 9

SMB/CIFS and NFS Multiprotocol Configuration Express Guide

February 2019 | 215-11171_K0
doccomments@netapp.com
Updated for ONTAP 9.5
Contents

Deciding whether to use this guide ............................................................. 4
Multiprotocol configuration workflow ....................................................... 5
  Creating an aggregate ........................................................................................ 5
  Deciding where to provision the new volume .................................................. 6
    Creating a basic SVM ..................................................................................... 7
    Adding CIFS and NFS access to an existing SVM ....................................... 10
  Opening the export policy of the SVM root volume (Creating a new
    NFS-enabled SVM) ................................................................................. 13
    Mapping the SMB server on the DNS server .......................................... 14
    Configuring LDAP (Creating a new NFS-enabled SVM) .......................... 15
    Mapping UNIX and Windows user names .............................................. 17
  Creating and configuring a volume .............................................................. 19
  Creating a share and setting its permissions .............................................. 21
  Creating an export policy for the volume ................................................... 21
  Verifying SMB client access ...................................................................... 23
  Verifying NFS access from a UNIX administration host .............................. 23
  Configuring and verifying CIFS and NFS client access .............................. 24
Where to find additional information ....................................................... 26
Copyright .................................................................................................... 28
Trademark .................................................................................................. 29
How to send comments about documentation and receive update
  notifications ............................................................................................... 30
Index ......................................................................................................... 31
Deciding whether to use the SMB/CIFS and NFS Multiprotocol Configuration Express Guide

This guide describes how to quickly set up both SMB/CIFS and 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 through 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 ONTAP command-line interface or an automated scripting tool.

Cluster management using System Manager

• Your data network uses the default IPspace, the default broadcast domain, and the default failover group.
  If your data network is flat, using these default objects ensures that LIFs will fail over correctly in the event of a link failure. If you are not using the default objects, you should refer to the Network Management Guide for information on how to configure LIF path failover.
• LDAP, if used, is provided by Active Directory.

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

• NFS management
• SMB/CIFS management
• Network and LIF management
• NetApp Technical Report 4073: Secure Unified Authentication
• 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.
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.

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 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]

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 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.

Choices

- 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*

  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 CIFS and NFS multiprotocol access, you can directly create and configure the volume.
  
  *Creating and configuring a volume*
Creating 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.
   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**

**SVM Details**

- **Specify a unique name and the data protocols for the SVM**
  - SVM Name: vs0.example.com
- **IP space**: Default
- **Data Protocols**: CIFS, NFS, iSCSI, FCoE
- **Default Language**: CUTF-8 (cutf_8)
- **Security Style**: NFS
- **Root Aggregate**: data_01_aggr

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**

- **Search Domains**: example.com
- **Name Servers**: 192.0.2.140, 192.0.2.141, 192.0.2.147

Click **Submit & Continue**.

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

4. In the **Data LIF Configuration** section of the **Configure CIFS/NFS protocol** page, specify the details of the LIF that clients will use to access data:

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

   b. Click **Browse** and select a node and port that will be associated with the LIF.
5. In the **CIFS Server Configuration** section, define the CIFS server and configure it to access the AD domain:

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

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

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

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

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

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

7. If the **NIS Configuration** area is collapsed, expand it.

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

9. Skip the **Provision a volume for NFS Storage** area because it provisions a volume for NFS access only—not for multiprotocol access.
10. Click **Submit & Continue**.
   The following objects are created:
   - A data LIF named after the SVM with the suffix “_cifs_nfs_lif1”
   - A CIFS server that is part of the AD domain
   - An NFS server

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

12. When the **SVM Administration** page is displayed, configure or defer configuring a separate administrator for this SVM:
   - Click **Skip** and configure an administrator later if required.
   - Enter the requested information and then click **Submit & Continue**.

13. Review the **Summary** page, record any information you might require later and then click **OK**.
   The DNS administrator needs to know the CIFS server name and the IP address of the data LIF. Windows clients need to know the name of the CIFS server. NFS clients need to know the IP address of the data LIF.

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

**After you finish**
You must now open the export policy of the SVM root volume.

**Related tasks**
*Opening the export policy of the SVM root volume (Creating a new NFS-enabled SVM)* on page 13

**Adding 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 created the SVM while following another Express Guide to configure a SAN protocol.

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

**Steps**

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

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

3. In the CIFS Server Configuration section, define the CIFS server and configure it to access the AD domain:
   a. Specify a name for the CIFS server that is unique in the AD domain.
   b. Specify the FQDN of the AD domain that the CIFS server can join.
   c. If you want to associate an organizational unit (OU) within the AD domain other than CN=Computers, enter the OU.
   d. Specify the name and password of an administrative account that has sufficient privileges to add the CIFS server to the OU.
   e. If you want to avoid unauthorized access to all the shares on this SVM, select the option to encrypt data using SMB 3.0.
4. Create a volume for CIFS/SMB access and provision a share on it:
   a. Name the share that CIFS/SMB clients will use to access the volume.
      The name you enter for the share will also be used as the volume name.
   b. Specify a size for the volume.

   ![Provision volume for CIFS storage](image)

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

Opening the export policy of the SVM root volume (Creating 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.
Result
NFSv3 clients can now access any volumes created on the SVM.

Mapping 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.

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

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

Steps

1. Navigate to the SVMs window.
2. Select the required SVM
3. Click the SVM Settings tab.
4. Set up an LDAP client for the SVM to use:
   
a. In the Services pane, click LDAP Client.
   
b. In the LDAP Client Configuration window, click Add.
   
c. In the General tab of the Create LDAP Client window, type the name of the LDAP client configuration, such as vs0client1.
   
d. Add either the AD domain or the AD servers.
   
e. Click Binding, and specify the authentication level, the Bind user and password, the base DN, and the port.
f. Click **Save and Close**.

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

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

The SVM uses the new LDAP client.

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

Mapping 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.

   **Example**

   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](image)

   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.

   **Example**

   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](image)

   d. Because the position of each rule determines the order in which the rules are applied, you should review the result and confirm that the order matches your expectations.
e. Repeat steps 5.b through 5.d 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.

   Example
   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.

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

After you finish
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.

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. 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.

   **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. 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.**
Creating a share and setting its permissions

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

About this task

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

Steps

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

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

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

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. 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.
Verifying 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.
   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.

Verifying 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.
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:
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 CIFS and NFS client access

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

**Steps**

1. Decide which clients and users or groups will be given access to the share.

2. Set file permissions using a method that corresponds to the volume's security style:

   **If the volume's security style is this...**

   **Do this...**

   **NTFS**
   
   a. Log in to a Windows client as an administrator who has sufficient administrative rights to manage NTFS permissions.

   b. In Windows Explorer, right-click the drive, and then select **Properties**.

   c. Select the Security tab, and adjust the security settings for the groups and users as required.

   **UNIX**

   On a UNIX administration host, use the root user to set UNIX ownership and permissions on the volume.
3. In System Manager, modify the share ACL to give Windows users or groups access to the share.
   a. Navigate to the Shares window.
   b. Select the share, and click Edit.
   c. Select the Permissions tab, and give the users or groups access to the share.

4. In System Manager, add rules to the export policy to permit NFS clients to access the share.
   a. Select the storage virtual machine (SVM), and click SVM Settings.
   b. In the Policies pane, click Export Policies.
   c. Select the export policy that is applied to the volume.
   d. In the Export Rules tab, click Add, and specify a set of clients.
   e. Select 2 for the Rule Index so that this rule executes after the rule that allows access to the administration host.
   f. Select CIFS and NFSv3.
   g. Specify the access details that you want, and click OK.

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.

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

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

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

CIFS/SMB configuration

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

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

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

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

- **NetApp KB Article 4550: Clustered Data ONTAP CIFS Expert Recommended articles**
  Lists all common CIFS/SMB protocol operational and troubleshooting workflows

NFS configuration

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

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

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

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

  Explains how to configure 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.

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

Root volume protection

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

- **Data protection**
Describes how to create a load-sharing mirror to protect the SVM root volume, which is a NetApp best practice for NAS-enabled SVMs. Also describes how to quickly recover from volume failures or losses by promoting the SVM root volume from a load-sharing mirror.
Copyright © 2019 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.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, 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).
Trademark

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

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.

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.

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., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
• Telephone: +1 (408) 822-6000
• Fax: +1 (408) 822-4501
• Support telephone: +1 (888) 463-8277
Index

A
access
  additional documentation 26
  verifying CIFS access by clients 24
  verifying NFS access by administrators 23
  verifying NFS access by clients 24
ACLs 21
  See also share ACLs
aggregates
  creating new when provisioning a volume 5
  selecting for new volumes 19

C
CIFS
  additional documentation 26
  mapping user names 17
  setup overview 5
CIFS servers
  mapping on DNS servers 14
CIFS shares 24
  See also shares
clients
  adding an LDAP configuration, Creating a new NFS-enabled SVM 15
comments
  how to send feedback about documentation 30
configuring
  multiprotocol access 5, 10
creating
  shares on existing SVMs 21

D
DNS servers
  mapping SMB server names on 14
documentation
  additional information about protocol access 26
  how to receive automatic notification of changes to 30
  how to send feedback about 30

E
export policies
  allowing NFS access to volumes on existing SVMs 21
  defining for root volumes 13
exports
  setting UNIX file permissions 24
  verifying administrator access to 23
  verifying client access 24
express guides
  additional documentation 26
  CIFS/SMB configuration workflow 10
  multiprotocol configuration workflow 5, 10
  NFS configuration workflow 5, 10

F
feedback
  how to send comments about documentation 30
file permissions
  setting for NTFS 24
  setting for UNIX 24
files
  controlling access to, using NTFS permissions 24
  controlling access to, using UNIX permissions 24

I
information
  how to send feedback about improving documentation 30

L
LDAP
  configuring 15

M
mapping
  user names on different platforms 17
multiprotocol access
  additional documentation 26
  setup overview 5

N
name mapping
  giving LDAP priority 15
name services
  giving LDAP priority, Creating a new NFS-enabled SVM 15
name switches
  giving LDAP priority 15
NetBIOS aliases
  mapping on DNS servers 14
NFS
  additional documentation 26
  mapping user names 17
  setup overview 5
NFS exports 24
  See also exports
NTFS
  setting file permissions 24
  setting security style 19

P
permissions
configuring export policy rules to allow NFS clients access to volumes on existing SVMs
configuring share ACLs on existing SVMs
setting NTFS file permissions
setting UNIX file permissions
policies
adding export rules
Creating a new NFS-enabled SVM
provisioning volume
deciding where to
requirements
R
root volumes
opening the export policies of
S
security style
changing
setup
CIFS, overview of
multiprotocol access, overview of
NFS, overview of
SMB/CIFS, overview of
share ACLs
defining on existing SVMs
shares
creating on existing SVMs
setting NTFS file permissions
verifying client access
verifying SMB client access
SMB
verifying share client access
SMB servers
mapping on DNS servers
SMB/CIFS
deciding whether to use this guide to set up SMB/CIFS and NFS
suggestions
how to send feedback about documentation
SVMs
adding LDAP clients
Creating a new NFS-enabled SVM
creating export policies to allow NFS client access to existing volumes
creating multiprotocol volumes on
creating to support CIFS and NFS
T
technical reports
additional information about file access
testing
See also verifying
Twitter
how to receive automatic notification of documentation changes
U
UNIX
mapping users to Windows
setting file permissions
setting security style
users
mapping names to different platforms
V
verifying
CIFS access by clients
NFS access by administrators
NFS access by clients
volumes
creating new aggregates to provide physical storage
creating on existing SVMs
modifying junction path of
W
Windows
mapping users to UNIX
workflows
multiprotocol configuration