



ONTAP® 9

SMB/CIFS Configuration Express Guide

June 2021 | 215-11170_2021-06_en-us
doccomments@netapp.com

Updated for ONTAP 9.9.1

 **NetApp**®

Contents

- Deciding whether to use the SMB/CIFS Configuration Express Guide..... 3**

- SMB/CIFS configuration workflow..... 4**
 - Creating an aggregate..... 4
 - Deciding where to provision the new volume..... 5

- Creating a new CIFS-enabled SVM..... 6**
 - Creating a new SVM with a CIFS volume and share..... 6
 - Mapping the SMB server on the DNS server..... 9
 - Verifying SMB client access..... 9
 - Configuring and verifying CIFS client access..... 10

- Configuring SMB/CIFS access to an existing SVM..... 11**
 - Adding CIFS access to an existing SVM..... 11
 - Mapping the SMB server on the DNS server..... 12
 - Verifying SMB client access..... 13
 - Configuring and verifying CIFS client access..... 13

- Adding a CIFS volume to a CIFS-enabled SVM..... 14**
 - Creating and configuring a volume..... 14
 - Creating a share and setting its permissions..... 15
 - Verifying SMB client access..... 15
 - Configuring and verifying CIFS client access..... 16

- Where to find additional information..... 17**

- Copyright, trademark, and machine translation..... 18**
 - Copyright..... 18
 - Trademark..... 18
 - Machine translation..... 18

Deciding whether to use the SMB/CIFS Configuration Express Guide

This guide describes how to quickly set up SMB/CIFS 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:

- 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 System Manager, not the ONTAP command-line interface or an automated scripting tool.

[Cluster management using System Manager](#)

- You want to use the *legacy* OnCommand System Manager UI for ONTAP 9.7 and earlier releases, not the ONTAP System Manager UI for ONTAP 9.7 and later.

[ONTAP System Manager documentation](#)

- Your data network uses the default IPspace, the default broadcast domain, and the default failover group.

If your data network is flat, 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.

- NTFS file permissions will be used to secure the new volume.

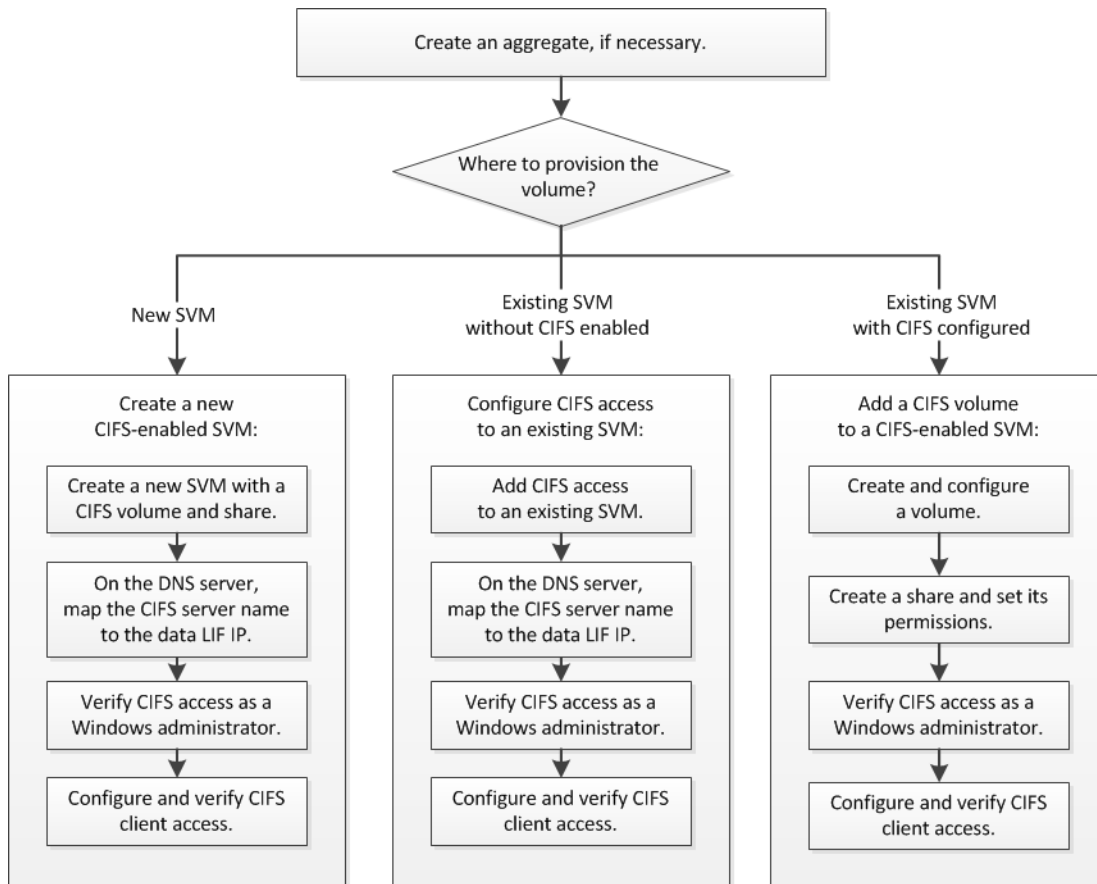
If this guide is not suitable for your situation, you should see the following documentation instead:

- *[SMB/CIFS management](#)*
- *[Network management](#)*
- *[NetApp Technical Report 4616: NFS Kerberos in ONTAP with Microsoft Active Directory](#)*
- *[NetApp Technical Report 4835: How to Configure LDAP in ONTAP](#)*
- *[NetApp Documentation: OnCommand Workflow Automation \(current releases\)](#)*

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

SMB/CIFS configuration workflow

Configuring SMB/CIFS involves optionally creating an aggregate and then choosing a workflow that is specific to your goal—creating a new CIFS-enabled SVM, configuring CIFS access to an existing SVM, or simply adding a CIFS volume to an existing SVM that is already fully configured for CIFS access.



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

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:

New Usable Capacity:

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

Choices

- If you want to provision a volume on a new SVM, create a new CIFS-enabled SVM.
[Creating a new CIFS-enabled SVM](#)
You must choose this option if CIFS is not enabled on an existing SVM.
- If you want to provision a volume on an existing SVM on which CIFS is enabled but not configured, configure CIFS/SMB access on the existing SVM.
[Configuring CIFS/SMB access on an existing SVM](#)
You should choose this option if you created the SVM for SAN access by using the relevant Express Guide.
- If you want to provision a volume on an existing SVM that is fully configured for CIFS access, add a CIFS volume to the CIFS-enabled SVM.
[Adding a CIFS volume to a CIFS-enabled SVM](#)

Creating a new CIFS-enabled SVM

Setting up a new CIFS-enabled SVM involves creating the new SVM with a CIFS volume and share, adding a mapping on the DNS server, and verifying CIFS access from a Windows administration host. You can then configure CIFS client access.

Steps

1. *Creating a new SVM with a CIFS volume and share* on page 6
2. *Mapping the SMB server on the DNS server* on page 9
3. *Verifying SMB client access* on page 9
4. *Configuring and verifying CIFS client access* on page 10

Creating a new SVM with a CIFS volume and share

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

Before you begin

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

Steps

1. Navigate to the **SVMs** window.
2. Click **Create**.
3. In the **Storage Virtual Machine (SVM) Setup** dialog box, create the SVM:
 - a. Specify a unique name for the SVM.
The name must either be a fully qualified domain name (FQDN) or follow another convention that ensures unique names across a cluster.
 - b. Select all the protocols that you have licenses for and that you will eventually use on the SVM, even if you do not want to configure all the protocols immediately.
If NFS access is required eventually, you must select **NFS** now so that CIFS and NFS clients can share the same data LIF.
 - c. Keep the default language setting, C.UTF-8.

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

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

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

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

Storage Virtual Machine (SVM) Setup

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:

- e. 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:

- f. Click **Submit & Continue**.

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

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

Data LIF Configuration

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

Data Interface details for CIFS

Assign IP Address: Without a subnet

IP Address: 10.224.107.199 [Change](#)

Port: abccorp_1:e0b [Browse...](#)

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.

CIFS Server Configuration

CIFS Server Name: vs0.example.com

Active Directory: AUTH.SEC.EXAMPLE.COM

Organizational Unit: CN=Computers

Administrator Name: adadmin

Administrator Password:

6. Create a volume for CIFS/SMB access and provision a share on it:
 - a. Name the share that CIFS/SMB clients will use to access the volume.
The name you enter for the share will also be used as the volume name.
 - b. Specify a size for the volume.

Provision a volume for CIFS storage (Optional).

Share Name: Eng

Size: 10 GB

Permission: Administrators - Full Control [Change](#)

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

7. Optional: Restrict access to the share by modifying the share ACL:
 - a. In the **Permission** field, click **Change**.
 - b. Select the Everyone group, and click **Remove**.
 - c. Optional: Click **Add**, and enter the name of an administrator group defined in the Windows Active Directory domain that includes the SVM.
 - d. Select the new administrator group, and then select **Full Control**.
 - e. Click **Save and Close**.

8. Click **Submit & Continue**.
The following objects are created:

- A data LIF named after the SVM with the suffix "_cifs_lif1"
- A CIFS server that is part of the AD domain

- A volume that is located on the aggregate with the most available space and has a name that matches the name of the share and ends in the suffix "_CIFS_volume"
 - A share on the volume
9. For all other protocol configuration pages that are displayed, click **Skip** and configure the protocol later.
 10. When the **SVM Administration** page is displayed, configure or defer configuring a separate administrator for this SVM:
 - Click **Skip** and configure an administrator later if required.
 - Enter the requested information and then click **Submit & Continue**.
 11. Review the **Summary** page, record any information you might require later and then click **OK**.

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

Result

A new SVM is created with a CIFS server containing a new volume that is shared.

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.

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.

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.

Configuring and verifying CIFS client access

When you are ready, you can give select clients access to the share by setting NTFS file permissions in Windows Explorer and modifying the share ACL in System Manager. Then you should test that the affected users or groups can access the volume.

Steps

1. Decide which clients and users or groups will be given access to the share.
2. On a Windows client, use an administrator role to give the users or groups permissions to the files and folders.
 - a. Log in to a Windows client as an administrator who has sufficient administrative rights to manage NTFS permissions.
 - b. In Windows Explorer, right-click the drive, and then select **Properties**.
 - c. Select the **Security** tab, and adjust the security settings for the groups and users as required.
3. In System Manager, modify the share ACL to give Windows users or groups access to the share.
 - a. Navigate to the **Shares** window.
 - b. Select the share, and click **Edit**.
 - c. Select the **Permissions** tab, and give the users or groups access to the share.
4. On a Windows client, log in as one of the users who now has access to the share and files, and verify that you can access the share and create a file.

Configuring SMB/CIFS access to an existing SVM

Adding access for SMB/CIFS clients to an existing SVM involves adding CIFS configurations to the SVM, adding a mapping on the DNS server, and verifying CIFS access from a Windows administration host. You can then configure CIFS client access.

Steps

1. *Adding CIFS access to an existing SVM* on page 11
2. *Mapping the SMB server on the DNS server* on page 12
3. *Verifying SMB client access* on page 13
4. *Configuring and verifying CIFS client access* on page 13

Adding CIFS access to an existing SVM

Adding CIFS/SMB access to an existing SVM involves creating a data LIF, configuring a CIFS server, provisioning a volume, sharing the volume, and configuring the share permissions.

Before you begin

- You must know which of the following networking components the SVM will use:
 - The node and the specific port on that node where the data logical interface (LIF) will be created
 - The subnet from which the data LIF's IP address will be provisioned, or optionally the specific IP address you want to assign to the data LIF
 - The Active Directory (AD) domain that this SVM will join, along with the credentials required to add the SVM to it
- Any external firewalls must be appropriately configured to allow access to network services.
- The CIFS protocol must be allowed on the SVM.
This is the case if you created the SVM while following another Express Guide to configure a SAN protocol.

Steps

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

Protocols: CIFS FC/FCoE

Data LIF Configuration

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

Data Interface details for CIFS

Assign IP Address: Without a subnet ▼

IP Address: 10.224.107.199 Change

? Port: abccorp_1:e0b Browse...

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.

— **CIFS Server Configuration** —

CIFS Server Name:

Active Directory:

Organizational Unit:

Administrator Name:

Administrator Password:

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:

Size: GB

Permission: [Change](#)

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

5. Optional: Restrict access to the share by modifying the share ACL:
 - a. In the **Permission** field, click **Change**.
 - b. Select the Everyone group, and click **Remove**.
 - c. Optional: Click **Add**, and enter the name of an administrator group defined in the Windows Active Directory domain that includes the SVM.
 - d. Select the new administrator group, and then select **Full Control**.
 - e. Click **Save and Close**.
6. Click **Submit & Close**, and then click **OK**.

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.

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.
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.

Configuring and verifying CIFS client access

When you are ready, you can give select clients access to the share by setting NTFS file permissions in Windows Explorer and modifying the share ACL in System Manager. Then you should test that the affected users or groups can access the volume.

Steps

1. Decide which clients and users or groups will be given access to the share.
2. On a Windows client, use an administrator role to give the users or groups permissions to the files and folders.
 - a. Log in to a Windows client as an administrator who has sufficient administrative rights to manage NTFS permissions.
 - b. In Windows Explorer, right-click the drive, and then select **Properties**.
 - c. Select the **Security** tab, and adjust the security settings for the groups and users as required.
3. In System Manager, modify the share ACL to give Windows users or groups access to the share.
 - a. Navigate to the **Shares** window.
 - b. Select the share, and click **Edit**.
 - c. Select the **Permissions** tab, and give the users or groups access to the share.
4. On a Windows client, log in as one of the users who now has access to the share and files, and verify that you can access the share and create a file.

Adding a CIFS volume to a CIFS-enabled SVM

Adding a CIFS volume to a CIFS-enabled SVM involves creating and configuring a volume, creating a share and setting its permissions, and verifying access from a Windows administration host. You can then configure CIFS client access.

Before you begin

CIFS must be completely set up on the SVM.

Steps

1. [Creating and configuring a volume](#) on page 14
2. [Creating a share and setting its permissions](#) on page 15
3. [Verifying SMB client access](#) on page 15
4. [Configuring and verifying CIFS client access](#) on page 16

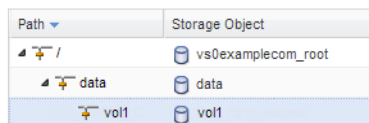
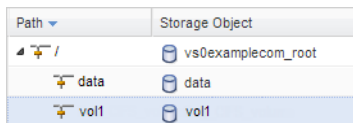
Creating and configuring a volume

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

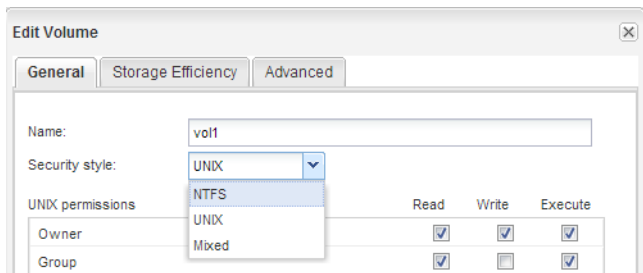
1. Navigate to the **Volumes** window.
2. Click **Create > Create FlexVol**.
The Create Volume dialog box is displayed.
3. If you want to change the default name, which ends in a date and time stamp, specify a new name, such as **vol1**.
4. Select an aggregate for the volume.
5. Specify the size of the 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.
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.



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

- a. In the **Volume** window, select the volume you just created, and click **Edit**.
The Edit Volume dialog box is displayed, showing the volume's current security style, which is inherited from the security style of the SVM root volume.
- b. Make sure the security style is NTFS.



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.

After you finish

You should verify access as a Windows administrator.

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.
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.

Configuring and verifying CIFS client access

When you are ready, you can give select clients access to the share by setting NTFS file permissions in Windows Explorer and modifying the share ACL in System Manager. Then you should test that the affected users or groups can access the volume.

Steps

1. Decide which clients and users or groups will be given access to the share.
2. On a Windows client, use an administrator role to give the users or groups permissions to the files and folders.
 - a. Log in to a Windows client as an administrator who has sufficient administrative rights to manage NTFS permissions.
 - b. In Windows Explorer, right-click the drive, and then select **Properties**.
 - c. Select the **Security** tab, and adjust the security settings for the groups and users as required.
3. In System Manager, modify the share ACL to give Windows users or groups access to the share.
 - a. Navigate to the **Shares** window.
 - b. Select the share, and click **Edit**.
 - c. Select the **Permissions** tab, and give the users or groups access to the share.
4. On a Windows client, log in as one of the users who now has access to the share and files, and verify that you can access the share and create a file.

Where to find additional information

After you have successfully tested CIFS client access, you can perform advanced CIFS 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.
- [*NetApp Technical Report 4191: Best Practices Guide for Clustered Data ONTAP 8.2 Windows File Services*](#)
Provides a brief overview of SMB implementation and other Windows File Services features with recommendations and basic troubleshooting information for ONTAP.
- [*NetApp Technical Report 3740: SMB 2 Next-Generation CIFS Protocol in Data ONTAP*](#)
Describes SMB 2 features, configuration details, and its implementation in ONTAP.

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, trademark, and machine translation

Copyright

Copyright © 2021 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.

<https://www.netapp.com/company/legal/trademarks/>

Machine translation

See important information about localized content at [netapp.com](https://www.netapp.com).

<https://www.netapp.com/company/legal/machine-translation/>