



# **Configure SMB client access to shared storage**

**ONTAP 9**

NetApp  
December 04, 2021

# Table of Contents

- Configure SMB client access to shared storage ..... 1
- Configure SMB client access to shared storage ..... 1
- Create a volume or qtree storage container..... 1
- Requirements and considerations for creating an SMB share..... 3
- Create an SMB share..... 4
- Verify SMB client access ..... 5
- Create SMB share access control lists ..... 6
- Configure NTFS file permissions in a share..... 8
- Verify user access ..... 9

# Configure SMB client access to shared storage

## Configure SMB client access to shared storage

To provide SMB client access to shared storage on an SVM, you must create a volume or qtree to provide a storage container, and then create or modify a share for that container. You can then configure share and file permissions, and test access from client systems.

### Before you begin

- SMB must be completely set up on the SVM.
- Any updates to your name services configuration must be complete.
- Any additions or modifications to an Active Directory domain or workgroup configuration must be complete.

## Create a volume or qtree storage container

### Create a volume

You can create a volume and specify its junction point and other properties by using the `volume create` command.

### Before you begin

The SVM security style must be NTFS, and SMB should be set up and running.

### About this task

A volume must include a *junction path* for its data to be made available to clients. You can specify the junction path when you create a new volume. If you create a volume without specifying a junction path, you must *mount* the volume in the SVM namespace using the `volume mount` command.

### Steps

1. Create the volume with a junction point: `volume create -vserver vservice_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path junction_path`

The choices for `-junction-path` are the following:

- Directly under root, for example, `/new_vol`

You can create a new volume and specify that it be mounted directly to the SVM root volume.

- Under an existing directory, for example, `/existing_dir/new_vol`

You can create a new volume and specify that it be mounted to an existing volume (in an existing hierarchy), expressed as a directory.

If you want to create a volume in a new directory (in a new hierarchy under a new volume), for example, `/new_dir/new_vol`, then you must first create a new parent volume that is junctioned to the SVM root volume. You would then create the new child volume in the junction path of the new parent volume (new directory).

2. Verify that the volume was created with the desired junction point: `volume show -vserver vserver_name -volume volume_name -junction`

## Examples

The following command creates a new volume named `users1` on the SVM `vs1.example.com` and the aggregate `aggr1`. The new volume is made available at `/users`. The volume is 750 GB in size, and its volume guarantee is of type `volume` (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
          Junction
Vserver   Volume  Active  Junction Path  Junction
-----
vs1.example.com  users1  true    /users         RW_volume
```

The following command creates a new volume named "home4" on the SVM "vs1.example.com" and the aggregate "aggr1". The directory `/eng/` already exists in the namespace for the `vs1` SVM, and the new volume is made available at `/eng/home`, which becomes the home directory for the `/eng/` namespace. The volume is 750 GB in size, and its volume guarantee is of type `volume` (by default).

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
          Junction
Vserver   Volume  Active  Junction Path  Junction
-----
vs1.example.com  home4  true    /eng/home      RW_volume
```

## Create a qtree

You can create a qtree to contain your data and specify its properties by using the `volume qtree create` command.

### Before you begin

- The SVM and the volume that will contain the new qtree must already exist.
- The SVM security style must be NTFS, and SMB should be set up and running.

### Steps

1. Create the qtree: `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

You can specify the volume and qtree as separate arguments or specify the qtree path argument in the format `/vol/volume_name/_qtree_name`.

2. Verify that the qtree was created with the desired junction path: 

```
volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }
```

### Example

The following example creates a qtree named qt01 located on SVM vs1.example.com that has a junction path `/vol/data1`:

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                Vserver Name: vs1.example.com
                Volume Name: data1
                Qtree Name: qt01
Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                Security Style: ntfs
                Oplock Mode: enable
                Unix Permissions: ---rwxr-xr-x
                Qtree Id: 2
                Qtree Status: normal
                Export Policy: default
Is Export Policy Inherited: true
```

## Requirements and considerations for creating an SMB share

Before creating an SMB share, you must understand requirements for share paths and share properties, particularly for home directories.

Creating an SMB share entails specifying a directory path structure (using the `-path` option in the `vserver cifs share create` command) that clients will access. The directory path corresponds to the junction path for a volume or qtree that you created in the SVM namespace. The directory path and corresponding junction path must exist before creating your share.

Share paths have the following requirements:

- A directory path name can be up to 255 characters long.
- If there is a space in the path name, the entire string must be put in quotes (for example, `"/new volume/mount here"`).

- If the UNC path (`\\servername\sharename\filepath`) of the share contains more than 256 characters (excluding the initial “\” in the UNC path), then the **Security** tab in the Windows Properties box is unavailable.

This is a Windows client issue rather than an ONTAP issue. To avoid this issue, do not create shares with UNC paths with more than 256 characters.

Share property defaults can be changed:

- The default initial properties for all shares are `oplocks`, `browsable`, `changenotify`, and `show-previous-versions`.
- It is optional to specify share properties when you create a share.

However, if you do specify share properties when you create the share, the defaults are not used. If you use the `-share-properties` parameter when you create a share, you must specify all of the share properties that you want to apply to the share using a comma-delimited list.

- To designate a home directory share, use the `homedirectory` property.

This feature enables 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 SVM).



You cannot add or remove this property after creating the share.

Home directory shares have the following requirements:

- Before creating SMB home directories, you must add at least one home directory search path by using the `vserver cifs home-directory search-path add` command.
- Home directory shares specified by the value of `homedirectory` on the `-share-properties` parameter must include the `%w` (Windows user name) dynamic variable in the share name.

The share name can additionally contain the `%d` (domain name) dynamic variable (for example, `%d/%w`) or a static portion in the share name (for example, `home1_%w`).

- If the share is used by administrators or users to connect to other users’ home directories (using options to the `vserver cifs home-directory modify` command), the dynamic share name pattern must be preceded by a tilde (`~`).

[SMB management](#) and `vserver cifs share man` pages have additional information.

## Create an SMB share

You must create an SMB share before you can share data from an SMB server with SMB clients. When you create a share, you can set share properties, such as designating the share as a home directory. You can also customize the share by configuring optional settings.

**Before you begin**

The directory path for the volume or qtree must exist in the SVM namespace before creating the share.

### About this task

When you create a share, the default share ACL (default share permissions) is `Everyone / Full Control`. After testing access to the share, you should remove the default share ACL and replace it with a more secure alternative.

### Steps

1. If necessary, create the directory path structure for the share.

The `vserver cifs share create` command checks the path specified in the `-path` option during share creation. If the specified path does not exist, the command fails.

2. Create an SMB share associated with the specified SVM: `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. Verify that the share was created: `vserver cifs share show -share-name share_name`

### Examples

The following command creates an SMB share named "SHARE1" on SVM `vs1.example.com`. Its directory path is `/users`, and it is created with default properties.

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1
```

Vserver	Share	Path	Properties	Comment	ACL
vs1.example.com	SHARE1	/users	oplocks	-	Everyone / Full Control
			browsable		
			changenotify		
			show-previous-versions		

## Verify SMB client access

You should verify that you have configured SMB correctly by accessing and writing data to the share. You should test access using the SMB server name and any NetBIOS aliases.

### Steps

1. Log in to a Windows client.
2. Test access using the SMB server name:
  - a. In Windows Explorer, map a drive to the share in the following format: `\\SMB_Server_Name\Share_Name`

If the mapping is not successful, it is possible that the DNS mapping has not yet propagated throughout the network. You must test access using the SMB server name later.

If the SMB server is named `vs1.example.com` and the share is named `SHARE1`, you should enter the following: `\\vs0.example.com\SHARE1`

b. On the newly created drive, create a test file, and then delete the file.

You have verified write access to the share using the SMB server name.

3. Repeat Step 2 for any NetBIOS aliases.

## Create SMB share access control lists

Configuring share permissions by creating access control lists (ACLs) for SMB shares enables you to control the level of access to a share for users and groups.

### Before you begin

You must have decided which users or groups will be given access to the share.

### About this task

You can configure share-level ACLs by using local or domain Windows user or group names.

Before creating a new ACL, you should delete the default share ACL `Everyone / Full Control`, which poses a security risk.

In workgroup mode, the local domain name is the SMB server name.

### Steps

1. Delete the default share ACL:  
`vserver cifs share access-control delete -vserver vserver_name -share share_name -user-or-group everyone`
2. Configure the new ACL:

If you want to configure ACLs by using a...	Enter the command...
Windows user	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_domain_name\\user_name -permission access_right</pre>
Windows group	<pre>vserver cifs share access-control create -vserver vserver_name -share share_name -user-group-type windows -user-or-group Windows_group_name -permission access_right</pre>

3. Verify that the ACL applied to the share is correct by using the `vserver cifs share access-control show` command.



## Example

The following command gives Change permissions to the "Sales Team" Windows group for the "sales" share on the "vs1.example.com" SVM:

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show

Vserver          Share          User/Group          User/Group  Access
Permission       Name           Name                Type
-----
vs1.example.com  c$             BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales          DOMAIN\"Sales Team"    windows     Change
```

The following commands give Change permission to the local Windows group named "Tiger Team" and Full\_Control permission to the local Windows user named "Sue Chang" for the "datavol5" share on the "vs1" SVM:

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1

Vserver          Share          User/Group          User/Group  Access
Permission       Name           Name                Type
-----
vs1              c$             BUILTIN\Administrators  windows
Full_Control
vs1              datavol5       DOMAIN\"Tiger Team"    windows     Change
vs1              datavol5       DOMAIN\"Sue Chang"     windows
```

# Configure NTFS file permissions in a share

To enable file access to the users or groups who have access to a share, you must configure NTFS file permissions on files and directories in that share from a Windows client.

## Before you begin

The administrator performing this task must have sufficient NTFS permissions to change permissions on the selected objects.

## About this task

[SMB management](#) and your Windows documentation contain information about how to set standard and advanced NTFS permissions.

## Steps

1. Log in to a Windows client as an administrator.
2. From the **Tools** menu in Windows Explorer, select **Map network drive**.
3. Complete the **Map Network Drive** box:
  - a. Select a **Drive** letter.
  - b. In the **Folder** box, type the SMB server name containing the share that contains the data to which you want to apply permissions and the name of the share.

If your SMB server name is SMB\_SERVER01 and your share is named "SHARE1", you would enter \\SMB\_SERVER01\SHARE1.



You can specify the IP address of the data interface for the SMB server instead of the SMB server name.

- c. Click **Finish**.

The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

4. Select the file or directory for which you want to set NTFS file permissions.
5. Right-click the file or directory, and then select **Properties**.
6. Select the **Security** tab.

The Security tab displays the list of users and groups for which NTFS permission are set. The Permissions for <Object> box displays a list of Allow and Deny permissions in effect for the selected user or group.

7. Click **Edit**.

The Permissions for <Object> box opens.

8. Perform the desired actions:

If you want to....	Do the following...
Set standard NTFS permissions for a new user or group	<p>a. Click <b>Add</b>.</p> <p>The Select User, Computers, Service Accounts, or Groups window opens.</p> <p>b. In the <b>Enter the object names to select</b> box, type the name of the user or group on which you want to add NTFS permission.</p> <p>c. Click <b>OK</b>.</p>
Change or remove standard NTFS permissions from a user or group	In the <b>Group or user names</b> box, select the user or group that you want to change or remove.

9. Perform the desired actions:

If you want to...	Do the following
Set standard NTFS permissions for a new or existing user or group	In the <b>Permissions for &lt;Object&gt;</b> box, select the <b>Allow</b> or <b>Deny</b> boxes for the type of access that you want to allow or not allow for the selected user or group.
Remove a user or group	Click <b>Remove</b> .



If some or all of the standard permission boxes are not selectable, it is because the permissions are inherited from the parent object. The **Special permissions** box is not selectable. If it is selected, it means that one or more of the granular advanced rights has been set for the selected user or group.

10. After you finish adding, removing, or editing NTFS permissions on that object, click **OK**.

## Verify user access

You should test that the users you configured can access the SMB share and the files it contains.

### Steps

1. On a Windows client, log in as one of the users who now has access to the share.
2. From the **Tools** menu in Windows Explorer, select **Map network drive**.
3. Complete the **Map Network Drive** box:
  - a. Select a **Drive** letter.
  - b. In the **Folder** box, type the share name you will provide to users.

If your SMB server name is SMB\_SERVER01 and your share is named "SHARE1", you would enter \\SMB\_SERVER01\share1.

c. Click **Finish**.

The drive you selected is mounted and ready with the Windows Explorer window displaying files and folders contained within the share.

4. Create a test file, verify that it exists, write text to it, and then remove the test file.

## Copyright Information

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.

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

## Trademark Information

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