Create and configure SMB shares

ONTAP 9

NetApp
July 21, 2023

Table of Contents

Create and configure SMB shares

Create and configure SMB shares overview

Before users and applications can access data on the CIFS server over SMB, you must create and configure SMB shares, which is a named access point in a volume. You can customize shares by specifying share parameters and share properties. You can modify an existing share at any time.

When you create an SMB share, ONTAP creates a default ACL for the share with Full Control permissions for Everyone.

SMB shares are tied to the CIFS server on the storage virtual machine (SVM). SMB shares are deleted if either the SVM is deleted or the CIFS server with which it is associated is deleted from the SVM. If you recreate the CIFS server on the SVM, you must re-create the SMB shares.

Related information

Manage file access using SMB

SMB configuration for Microsoft Hyper-V and SQL Server

Configure character mapping for SMB file name translation on volumes

What the default administrative shares are

When you create a CIFS server on your storage virtual machine (SVM), default administrative shares are automatically created. You should understand what those default shares are and how they are used.

ONTAP creates the following default administrative shares when you create the CIFS server:

Beginning with ONTAP 9.8, the admin$ share is no longer created by default.

- ipc$
- admin$ (ONTAP 9.7 and earlier only)
- c$

Because shares that end with the $ character are hidden shares, the default administrative shares are not visible from My Computer, but you can view them by using Shared Folders.

How the ipc$ and admin$ default shares are used

The ipc$ and admin$ shares are used by ONTAP and cannot be used by Windows administrators to access data residing on the SVM.

- ipc$ share

  The ipc$ share is a resource that shares the named pipes that are essential for communication between programs. The ipc$ share is used during remote administration of a computer and when viewing a

computer's shared resources. You cannot change the share settings, share properties, or ACLs of the ipc$ share. You also cannot rename or delete the ipc$ share.

- admin$ share (ONTAP 9.7 and earlier only)

  Beginning with ONTAP 9.8, the admin$ share is no longer created by default.

  The admin$ share is used during remote administration of the SVM. The path of this resource is always the path to the SVM root. You cannot change the share settings, share properties, or ACLs for the admin$ share. You also cannot rename or delete the admin$ share.

How the c$ default share is used

The c$ share is an administrative share that the cluster or SVM administrator can use to access and manage the SVM root volume.

The following are characteristics of the c$ share:

- The path for this share is always the path to the SVM root volume and cannot be modified.
- The default ACL for the c$ share is Administrator / Full Control.

  This user is the BUILTIN\administrator. By default, the BUILTIN\administrator can map to the share and view, create, modify, or delete files and folders in the mapped root directory. Caution should be exercised when managing files and folders in this directory.

- You can change the c$ share's ACL.
- You can change the c$ share settings and share properties.
- You cannot delete the c$ share.
- The SVM administrator can access the rest of the SVM namespace from the mapped c$ share by crossing the namespace junctions.
- The c$ share can be accessed by using the Microsoft Management Console.

Related information

Configuring advanced NTFS file permissions using the Windows Security tab

SMB share naming requirements

You should keep the ONTAP share naming requirements in mind when creating SMB shares on your SMB server.

Share naming conventions for ONTAP are the same as for Windows and include the following requirements:

- The name of each share must be unique for the SMB server.
- Share names are not case-sensitive.
- The maximum share name length is 80 characters.
- Unicode share names are supported.
- Share names ending with the $ character are hidden shares.
- For ONTAP 9.7 and earlier, the admin$, ipc$, and c$ administrative shares are automatically created on

every CIFS server and are reserved share names. Beginning with ONTAP 9.8, the admin$ share is no longer automatically created.

- You cannot use the share name ONTAP_ADMIN$ when creating a share.
- Share names containing spaces are supported:
  - You cannot use a space as the first character or as the last character in a share name.
  - You must enclose share names containing a space in quotation marks.

> Single quotation marks are considered part of the share name and cannot be used in place of quotation marks.

- The following special characters are supported when you name SMB shares:

  ! @ # $ % & ' _ - . ~ ( ) { }

- The following special characters are not supported when you name SMB shares:

  □ " / \ : ; | < > , ? * =

Directory case-sensitivity requirements when creating shares in a multiprotocol environment

If you create shares in an SVM where the 8.3 naming scheme is used to distinguish between directory names where there are only case differences between the names, you must use the 8.3 name in the share path to ensure that the client connects to the desired directory path.

In the following example, two directories named “testdir” and “TESTDIR” were created on a Linux client. The junction path of the volume containing the directories is `/home`. The first output is from a Linux client and the second output is from an SMB client.

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

When you create a share to the second directory, you must use the 8.3 name in the share path. In this example, the share path to the first directory is `/home/testdir` and the share path to the second directory is `/home/TESTDI~1`.

Use SMB share properties

Use SMB share properties overview

You can customize the properties of SMB shares.

The available share properties are as follows:

Share properties	Description
`oplocks`	This property specifies that the share uses opportunistic locks, also known as client-side caching.
`browsable`	This property allows Windows clients to browse the share.
`showsnapshot`	This property specifies that Snapshot copies can be viewed and traversed by clients.
`changenotify`	This property specifies that the share supports Change Notify requests. For shares on an SVM, this is a default initial property.
`attributecache`	This property enables the file attribute caching on the SMB share to provide faster access of attributes. The default is to disable attribute caching. This property should be enabled only if there are clients connecting to shares over SMB 1.0. This share property is not applicable if clients are connecting to shares over SMB 2.x or SMB 3.0.
`continuously-available`	This property permits SMB clients that support it to open files in a persistent manner. Files opened this way are protected from disruptive events, such as failover and giveback.
`branchcache`	This property specifies that the share allows clients to request BranchCache hashes on the files within this share. This option is useful only if you specify “per-share” as the operating mode in the CIFS BranchCache configuration.
`access-based-enumeration`	This property specifies that *Access Based Enumeration* (ABE) is enabled on this share. ABE-filtered shared folders are visible to a user based on that individual user’s access rights, preventing the display of folders or other shared resources that the user does not have rights to access.

Share properties	Description
`namespace-caching`	This property specifies that the SMB clients connecting to this share can cache the directory enumeration results returned by the CIFS servers, which can provide better performance. By default, SMB 1 clients do not cache directory enumeration results. Because SMB 2 and SMB 3 clients cache directory enumeration results by default, specifying this share property provides performance benefits only to SMB 1 client connections.
`encrypt-data`	This property specifies that SMB encryption must be used when accessing this share. SMB clients that do not support encryption when accessing SMB data will not be able to access this share.

Add or remove share properties on an existing SMB share

You can customize an existing SMB share by adding or removing share properties. This can be useful if you want to change the share configuration to meet changing requirements in your environment.

Before you begin

The share whose properties you want to modify must exist.

About this task

Guidelines for adding share properties:

- You can add one or more share properties by using a comma-delimited list.
- Any share properties that you have previously specified remain in effect.

  Newly added properties are appended to the existing list of share properties.
- If you specify a new value for share properties that are already applied to the share, the newly specified value replaces the original value.
- You cannot remove share properties by using the `vserver cifs share properties add` command.

  You can use the `vserver cifs share properties remove` command to remove share properties.

Guidelines for removing share properties:

- You can remove one or more share properties by using a comma-delimited list.
- Any share properties that you have previously specified but do not remove remain in effect.

Steps

1. Enter the appropriate command:

If you want to…	Enter the command…
Add share properties	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
Remove share properties	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. Verify the share property settings: `vserver cifs share show -vserver vserver_name -share -name share_name`

Examples

The following command adds the `showsnapshot` share property to a share named “share1” on SVM vs1:

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

The following command removes the `browsable` share property from a share named “share2” on SVM vs1:

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

Related information

Commands for managing SMB shares

Optimize SMB user access with the force-group share setting

When you create a share from the ONTAP command line to data with UNIX effective security, you can specify that all files created by SMB users in that share belong to the same group, known as the *force-group*, which must be a predefined group in the UNIX group database. Using a force-group makes it easier to ensure that files can be accessed by SMB users belonging to various groups.

Specifying a force-group is meaningful only if the share is in a UNIX or mixed qtree. There is no need to set a force-group for shares in an NTFS volume or qtree because access to files in these shares is determined by Windows permissions, not UNIX GIDs.

If a force-group has been specified for a share, the following becomes true of the share:

- SMB users in the force-group who access this share are temporarily changed to the GID of the force-group.

  This GID enables them to access files in this share that are not accessible normally with their primary GID or UID.

- All files in this share created by SMB users belong to the same force-group, regardless of the primary GID of the file owner.

When SMB users try to access a file created by NFS, the SMB users' primary GIDs determine access rights.

The force-group does not affect how NFS users access files in this share. A file created by NFS acquires the GID from the file owner. Determination of access permissions is based on the UID and primary GID of the NFS user who is trying to access the file.

Using a force-group makes it easier to ensure that files can be accessed by SMB users belonging to various groups. For example, if you want to create a share to store the company's web pages and give write access to users in the Engineering and Marketing departments, you can create a share and give write access to a force-group named "webgroup1". Because of the force-group, all files created by SMB users in this share are owned by the "webgroup1" group. In addition, users are automatically assigned the GID of the "webgroup1" group when accessing the share. As a result, all the users can write to this share without you needing to manage the access rights of the users in the Engineering and Marketing departments.

Related information

Creating an SMB share with the force-group share setting

Create an SMB share with the force-group share setting

You can create an SMB share with the force-group share setting if you want SMB users that access data on volumes or qtrees with UNIX file security to be regarded by ONTAP as belonging to the same UNIX group.

Step

1. Create the SMB share: `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

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.

If you want to remove the force-group after the share is created, you can modify the share at any time and specify an empty string ("") as the value for the `-force-group-for-create` parameter. If you remove the force-group by modifying the share, all existing connections to this share continue to have the previously set force-group as the primary GID.

Example

The following command creates a "webpages" share that is accessible on the web in the `/corp/companyinfo` directory in which all files that SMB users create are assigned to the webgroup1 group:

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

Related information

Optimize SMB user access with the force-group share setting

View information about SMB shares using the MMC

You can view information about SMB shares on your SVM and perform some management tasks using the Microsoft Management Console (MMC). Before you can view the shares, you need to connect the MMC to the SVM.

About this task

You can perform the following tasks on shares contained within SVMs using the MMC:

- View shares
- View active sessions
- View open files
- Enumerate the list of sessions, files and tree connections in the system
- Close open files in the system
- Close open sessions
- Create/manage shares

The views displayed by the preceding capabilities are node specific and not cluster specific. Therefore, when you use the MMC to connect to the SMB server host name (that is, cifs01.domain.local), you are routed, based on how you have set up DNS, to a single LIF within your cluster.

The following functions are not supported in MMC for ONTAP:

- Creating new local users/groups
- Managing/viewing existing local users/groups
- Viewing events or performance logs

- Storage
- Services and applications

In instances where the operation is not supported, you might experience `remote procedure call failed` errors.

FAQ: Using Windows MMC with ONTAP

Steps

1. To open Computer Management MMC on any Windows server, in the **Control Panel**, select **Administrative Tools** > **Computer Management**.
2. Select **Action** > **Connect to another computer**.

   The Select Computer dialog box appears.

3. Type the name of the storage system or click **Browse** to locate the storage system.
4. Click **OK**.

   The MMC connects to the SVM.

5. In the navigation pane, click **Shared Folders** > **Shares**.

   A list of shares on the SVM is displayed in the right display pane.

6. To display the share properties for a share, double-click the share to open the **Properties** dialog box.
7. If you cannot connect to the storage system using MMC, you can add the user to the BUILTIN\Administrators group or BUILTIN\Power Users group by using one of the following commands on the storage system:

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

Commands for managing SMB shares

You use the `vserver cifs share` and `vserver cifs share properties` commands to manage SMB shares.

If you want to…	Use this command…
Create an SMB share	`vserver cifs share create`
Display SMB shares	`vserver cifs share show`

If you want to…	Use this command…
Modify an SMB share	`vserver cifs share modify`
Delete an SMB share	`vserver cifs share delete`
Add share properties to an existing share	`vserver cifs share properties add`
Remove share properties from an existing share	`vserver cifs share properties remove`
Display information about share properties	`vserver cifs share properties show`

See the man page for each command for more information.

Copyright information

Trademark information