NetApp

Use options to customize SMB servers
ONTAP 9

NetApp
August 16, 2023

Table of Contents

Use options to customize SMB servers

Available SMB server options

It is useful to know what options are available when considering how to customize the SMB server. Although some options are for general use on the SMB server, several are used to enable and configure specific SMB functionality. SMB server options are controlled with the `vserver cifs options modify` option.

The following list specifies the SMB server options that are available at the admin privilege level:

- **Configuring the SMB session timeout value**

  Configuring this option enables you to specify the number of seconds of idle time before an SMB session is disconnected. An idle session is a session in which a user does not have any files or directories opened on the client. The default value is 900 seconds.

- **Configuring the default UNIX user**

  Configuring this option enables you to specify the default UNIX user that the SMB server uses. ONTAP automatically creates a default user named "pcuser" (with a UID of 65534), creates a group named "pcuser" (with a GID of 65534), and adds the default user to the "pcuser" group. When you create a SMB server, ONTAP automatically configures "pcuser" as the default UNIX user.

- **Configuring the guest UNIX user**

  Configuring this option enables you to specify the name of a UNIX user to which users who log in from untrusted domains are mapped, which allows a user from an untrusted domain to connect to the SMB server. By default, this option is not configured (there is no default value); therefore, the default is to not allow users from untrusted domains to connect to the SMB server.

- **Enabling or disabling read grant execution for mode bits**

  Enabling or disabling this option enables you to specify whether to allow SMB clients to run executable files with UNIX mode bits to which they have read access, even when the UNIX executable bit is not set. This option is disabled by default.

- **Enabling or disabling the ability to delete read-only files from NFS clients**

  Enabling or disabling this option determines whether to allow NFS clients to delete files or folders with the read-only attribute set. NTFS delete semantics does not allow the deletion of a file or folder when the read-only attribute is set. UNIX delete semantics ignores the read-only bit, using the parent directory permissions instead to determine whether a file or folder can be deleted. The default setting is `disabled`, which results in NTFS delete semantics.

- **Configuring Windows Internet Name Service server addresses**

  Configuring this option enables you to specify a list of Windows Internet Name Service (WINS) server addresses as a comma-delimited list. You must specify IPv4 addresses. IPv6 addresses are not supported. There is no default value.

The following list specifies the SMB server options that are available at the advanced privilege level:

- **Granting UNIX group permissions to CIFS users**

  Configuring this option determines whether the incoming CIFS user who is not the owner of the file can be granted the group permission. If the CIFS user is not the owner of the UNIX security-style file and this parameter is set to `true`, then the group permission is granted for the file. If the CIFS user is not the owner of the UNIX security-style file and this parameter is set to `false`, then the normal UNIX rules are applicable to grant the file permission. This parameter is applicable to UNIX security-style files that have permission set as `mode bits` and is not applicable to files with the NTFS or NFSv4 security mode. The default setting is `false`.

- **Enabling or disabling SMB 1.0**

  SMB 1.0 is disabled by default on an SVM for which a SMB server is created in ONTAP 9.3.

  > (i) Beginning ONTAP 9.3, SMB 1.0 is disabled by default for new SMB servers created in ONTAP 9.3. You should migrate to a later SMB version as soon as possible to prepare for security and compliance enhancements. Contact your NetApp representative for details.

- **Enabling or disabling SMB 2.x**

  SMB 2.0 is the minimum SMB version that supports LIF failover. If you disable SMB 2.x, ONTAP also automatically disables SMB 3.X.

  SMB 2.0 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling SMB 3.0**

  SMB 3.0 is the minimum SMB version that supports continuously available shares. Windows Server 2012 and Windows 8 are the minimum Windows versions that support SMB 3.0.

  SMB 3.0 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling SMB 3.1**

  Windows 10 is the only Windows version that supports SMB 3.1.

  SMB 3.1 is supported only on SVMs. The option is enabled by default on SVMs

- **Enabling or disabling ODX copy offload**

  ODX copy offload is used automatically by Windows clients that support it. This option is enabled by default.

- **Enabling or disabling the direct-copy mechanism for ODX copy offload**

  The direct-copy mechanism increases the performance of the copy offload operation when Windows clients try to open the source file of a copy in a mode that prevents the file being changed while the copy is in progress. By default, the direct copy mechanism is enabled.

- **Enabling or disabling automatic node referrals**

  With automatic node referrals, the SMB server automatically refers clients to a data LIF local to the node that hosts the data accessed through the requested share.

- **Enabling or disabling export policies for SMB**

This option is disabled by default.

- **Enabling or disabling using junction points as reparse points**

  If this option is enabled, the SMB server exposes junction points to SMB clients as reparse points. This option is valid only for SMB 2.x or SMB 3.0 connections. This option is enabled by default.

  This option is supported only on SVMs. The option is enabled by default on SVMs

- **Configuring the number of maximum simultaneous operations per TCP connection**

  The default value is 255.

- **Enabling or disabling local Windows users and groups functionality**

  This option is enabled by default.

- **Enabling or disabling local Windows users authentication**

  This option is enabled by default.

- **Enabling or disabling VSS shadow copy functionality**

  ONTAP uses the shadow copy functionality to perform remote backups of data stored using the Hyper-V over SMB solution.

  This option is supported only on SVMs, and only for Hyper-V over SMB configurations. The option is enabled by default on SVMs

- **Configuring the shadow copy directory depth**

  Configuring this option enables you to define the maximum depth of directories on which to create shadow copies when using the shadow copy functionality.

  This option is supported only on SVMs, and only for Hyper-V over SMB configurations. The option is enabled by default on SVMs

- **Enabling or disabling multidomain search capabilities for name mapping**

  If enabled, when a UNIX user is mapped to a Windows domain user by using a wildcard (*) in the domain portion of the Windows user name (for example, *\joe), ONTAP searches for the specified user in all of the domains with bidirectional trusts to the home domain. The home domain is the domain that contains the SMB server's computer account.

  As an alternative to searching all of the bidirectionally trusted domains, you can configure a list of preferred trusted domains. If this option is enabled and a preferred list is configured, the preferred list is used to perform multidomain name mapping searches.

  The default is to enable multidomain name mapping searches.

- **Configuring the file system sector size**

  Configuring this option enables you to configure the file system sector size in bytes that ONTAP reports to SMB clients. There are two valid values for this option: `4096` and `512`. The default value is `4096`. You might need to set this value to `512` if the Windows application supports only a sector size of 512 bytes.

- **Enabling or disabling Dynamic Access Control**

  Enabling this option enables you to secure objects on the SMB server by using Dynamic Access Control (DAC), including using auditing to stage central access policies and using Group Policy Objects to implement central access policies. The option is disabled by default.

  This option is supported only on SVMs.

- **Setting the access restrictions for non-authenticated sessions (restrict anonymous)**

  Setting this option determines what the access restrictions are for non-authenticated sessions. The restrictions are applied to anonymous users. By default, there are no access restrictions for anonymous users.

- **Enabling or disabling the presentation of NTFS ACLs on volumes with UNIX effective security (UNIX security-style volumes or mixed security-style volumes with UNIX effective security)**

  Enabling or disabling this option determines how file security on files and folders with UNIX security is presented to SMB clients. If enabled, ONTAP presents files and folders in volumes with UNIX security to SMB clients as having NTFS file security with NTFS ACLs. If disabled, ONTAP presents volumes with UNIX security as FAT volumes, with no file security. By default, volumes are presented as having NTFS file security with NTFS ACLs.

- **Enabling or disabling the SMB fake open functionality**

  Enabling this functionality improves SMB 2.x and SMB 3.0 performance by optimizing how ONTAP makes open and close requests when querying for attribute information on files and directories. By default, the SMB fake open functionality is enabled. This option is useful only for connections that are made with SMB 2.x or later.

- **Enabling or disabling the UNIX extensions**

  Enabling this option enables UNIX extensions on a SMB server. UNIX extensions allow POSIX/UNIX style security to be displayed through the SMB protocol. By default this option is disabled.

  If you have UNIX-based SMB clients, such as Mac OSX clients, in your environment, you should enable UNIX extensions. Enabling UNIX extensions allows the SMB server to transmit POSIX/UNIX security information over SMB to the UNIX-based client, which then translates the security information into POSIX/UNIX security.

- **Enabling or disabling support for short name searches**

  Enabling this option allows the SMB server to perform searches on short names. A search query with this option enabled tries to match 8.3 file names along with long file names. The default value for this parameter is `false`.

- **Enabling or disabling support for automatic advertisement of DFS capabilities**

  Enabling or disabling this option determines whether SMB servers automatically advertise DFS capabilities to SMB 2.x and SMB 3.0 clients that connect to shares. ONTAP uses DFS referrals in the implementation of symbolic links for SMB access. If enabled, the SMB server always advertises DFS capabilities regardless of whether symbolic link access is enabled. If disabled, the SMB server advertises DFS capabilities only when the clients connect to shares where symbolic link access is enabled.

- **Configuring the maximum number of SMB credits**

Beginning with ONTAP 9.4, configuring the `-max-credits` option allows you to limit the number of credits to be granted on an SMB connection when clients and server are running SMB version 2 or later. The default value is 128.

- **Enabling or disabling support for SMB Multichannel**

  Enabling the `-is-multichannel-enabled` option in ONTAP 9.4 and later releases allows the SMB server to establish multiple connections for a single SMB session when appropriate NICs are deployed on the cluster and its clients. Doing so improves throughput and fault tolerance. The default value for this parameter is `false`.

  When SMB Multichannel is enabled, you can also specify the following parameters:

  - The maximum number of connections allowed per Multichannel session. The default value for this parameter is 32.
  - The maximum number of network interfaces advertised per Multichannel session. The default value for this parameter is 256.

Configuring SMB server options

You can configure SMB server options at any time after you have created a SMB server on a storage virtual machine (SVM).

Step

1. Perform the desired action:

If you want to configure SMB server options…	Enter the command…
At admin-privilege level	`vserver cifs options modify -vserver` *`vserver_name options`*
At advanced-privilege level	a. `set -privilege advanced` b. `vserver cifs options modify -vserver` *`vserver_name options`* c. `set -privilege admin`

For more information about configuring SMB server options, see the man page for the `vserver cifs options modify` command.

Configure the grant UNIX group permission to SMB users

You can configure this option to grant group permissions to access files or directories even if the incoming SMB user is not the owner of the file.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`

2. Configure the grant UNIX group permission as appropriate:

If you want to	Enter the command
Enable the access to the files or directories to get group permissions even if the user is not the owner of the file	`vserver cifs options modify -grant-unix-group-perms-to-others true`
Disable the access to the files or directories to get group permissions even if the user is not the owner of the file	`vserver cifs options modify -grant-unix-group-perms-to-others false`

3. Verify that the option is set to the desired value: `vserver cifs options show -fields grant-unix-group-perms-to-others`

4. Return to the admin privilege level: `set -privilege admin`

Configure access restrictions for anonymous users

By default, an anonymous, unauthenticated user (also known as the *null user*) can access certain information on the network. You can use a SMB server option to configure access restrictions for the anonymous user.

About this task

The `-restrict-anonymous` SMB server option corresponds to the `RestrictAnonymous` registry entry in Windows.

Anonymous users can list or enumerate certain types of system information from Windows hosts on the network, including user names and details, account policies, and share names. You can control access for the anonymous user by specifying one of three access restriction settings:

Value	Description
`no-restriction` (default)	Specifies no access restrictions for anonymous users.
`no-enumeration`	Specifies that only enumeration is restricted for anonymous users.
`no-access`	Specifies that access is restricted for anonymous users.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`

2. Configure the restrict anonymous setting: `vserver cifs options modify -vserver vserver_name -restrict-anonymous {no-restriction|no-enumeration|no-access}`

3. Verify that the option is set to the desired value: `vserver cifs options show -vserver vserver_name`

4. Return to the admin privilege level: `set -privilege admin`

Related information

Manage how file security is presented to SMB clients for UNIX security-style data

Manage how file security is presented to SMB clients for UNIX security-style data overview

You can choose how you want to present file security to SMB clients for UNIX security-style data by enabling or disabling the presentation of NTFS ACLs to SMB clients. There are advantages with each setting, which you should understand to choose the setting best suited for your business requirements.

By default, ONTAP presents UNIX permissions on UNIX security-style volumes to SMB clients as NTFS ACLs. There are scenarios where this is desirable, including the following:

- You want to view and edit UNIX permissions by using the **Security** tab in the Windows Properties box.

  You cannot modify permissions from a Windows client if the operation is not permitted by the UNIX system. For example, you cannot change the ownership of a file you do not own, because the UNIX system does not permit this operation. This restriction prevents SMB clients from bypassing UNIX permissions set on the files and folders.

- Users are editing and saving files on the UNIX security-style volume by using certain Windows applications, for example Microsoft Office, where ONTAP must preserve UNIX permissions during save operations.

- There are certain Windows applications in your environment that expect to read NTFS ACLs on files they use.

Under certain circumstances, you might want to disable the presentation of UNIX permissions as NTFS ACLs. If this functionality is disabled, ONTAP presents UNIX security-style volumes as FAT volumes to SMB clients. There are specific reasons why you might want to present UNIX security-style volumes as FAT volumes to SMB clients:

- You only change UNIX permissions by using mounts on UNIX clients.

  The Security tab is not available when a UNIX security-style volume is mapped on an SMB client. The mapped drive appears to be formatted with the FAT file system, which has no file permissions.

- You are using applications over SMB that set NTFS ACLs on accessed files and folders, which can fail if the data resides on UNIX security-style volumes.

  If ONTAP reports the volume as FAT, the application does not try to change an ACL.

Related information

Configuring security styles on FlexVol volumes

Configuring security styles on qtrees

Enable or disable the presentation of NTFS ACLs for UNIX security-style data

You can enable or disable the presentation of NTFS ACLs to SMB clients for UNIX security-style data (UNIX security-style volumes and mixed security-style volumes with UNIX effective security).

About this task

If you enable this option, ONTAP presents files and folders on volumes with effective UNIX security style to SMB clients as having NTFS ACLs. If you disable this option, the volumes are presented as FAT volumes to SMB clients. The default is to present NTFS ACLs to SMB clients.

Steps

1. Set the privilege level to advanced: `set -privilege advanced`

2. Configure the UNIX NTFS ACL option setting: `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`

3. Verify that the option is set to the desired value: `vserver cifs options show -vserver vserver_name`

4. Return to the admin privilege level: `set -privilege admin`

How ONTAP preserves UNIX permissions

When files in a FlexVol volume that currently have UNIX permissions are edited and saved by Windows applications, ONTAP can preserve the UNIX permissions.

When applications on Windows clients edit and save files, they read the security properties of the file, create a new temporary file, apply those properties to the temporary file, and then give the temporary file the original file name.

When Windows clients perform a query for the security properties, they receive a constructed ACL that exactly represents the UNIX permissions. The sole purpose of this constructed ACL is to preserve the file's UNIX permissions as files are updated by Windows applications to ensure that the resulting files have the same UNIX permissions. ONTAP does not set any NTFS ACLs using the constructed ACL.

Manage UNIX permissions using the Windows Security tab

If you want to manipulate UNIX permissions of files or folders in mixed security-style volumes or qtrees on SVMs, you can use the Security tab on Windows clients. Alternatively, you can use applications that can query and set Windows ACLs.

- Modifying UNIX permissions

  You can use the Windows Security tab to view and change UNIX permissions for a mixed security-style volume or qtree. If you use the main Windows Security tab to change UNIX permissions, you must first remove the existing ACE you want to edit (this sets the mode bits to 0) before you make your changes. Alternatively, you can use the Advanced editor to change permissions.

  If mode permissions are used, you can directly change the mode permissions for the listed UID, GID, and others (everyone else with an account on the computer). For example, if the displayed UID has r-x permissions, you can change the UID permissions to rwx.

- Changing UNIX permissions to NTFS permissions

  You can use the Windows Security tab to replace UNIX security objects with Windows security objects on a mixed security-style volume or qtree where the files and folders have a UNIX effective security style.

  You must first remove all listed UNIX permission entries before you can replace them with the desired Windows User and Group objects. You can then configure NTFS-based ACLs on the Windows User and Group objects. By removing all UNIX security objects and adding only Windows Users and Groups to a file or folder in a mixed security-style volume or qtree, you change the effective security style on the file or folder from UNIX to NTFS.

  When changing permissions on a folder, the default Windows behavior is to propagate these changes to all subfolders and files. Therefore, you must change the propagation choice to the desired setting if you do not want to propagate a change in security style to all child folders, subfolders, and files.