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

ONTAP 9

NetApp
August 15, 2023

Table of Contents

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.

Copyright information

Trademark information