



Secure file access by using file permissions

ONTAP 9

NetApp
July 03, 2023

Table of Contents

- Secure file access by using file permissions 1
 - Configure advanced NTFS file permissions using the Windows Security tab 1
 - Configure NTFS file permissions using the ONTAP CLI 4
 - How UNIX file permissions provide access control when accessing files over SMB..... 4

Secure file access by using file permissions

Configure advanced NTFS file permissions using the Windows Security tab

You can configure standard NTFS file permissions on files and folders by using the **Windows Security** tab in the Windows Properties window.

Before you begin

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

About this task

Configuring NTFS file permissions is done on a Windows host by adding entries to NTFS discretionary access control lists (DACLS) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories. These tasks are automatically handled by the Windows GUI.

Steps

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

If your CIFS server name is "CIFS_SERVER" and your share is named "share1", you should type \\CIFS_SERVER\share1.



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

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

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

6. Click **Advanced**.

The Windows Properties window displays information about existing file permissions assigned to users and groups.

7. Click **Change Permissions**.

The Permissions window opens.

8. Perform the desired actions:

| If you want to... | Do the following... |
|--|---|
| Set up advanced NTFS permissions for a new user or group | <ul style="list-style-type: none">a. Click Add.b. In the Enter the object name to select box, type the name of the user or group that you want to add.c. Click OK. |
| Change advanced NTFS permissions from a user or group | <ul style="list-style-type: none">a. In the Permissions entries: box, select the user or group whose advanced permissions you want to change.b. Click Edit. |
| Remove advanced NTFS permissions for a user or group | <ul style="list-style-type: none">a. In the Permissions entries: box, select the user or group that you want to remove.b. Click Remove.c. Skip to Step 13. |

If you are adding advanced NTFS permissions on a new user or group or changing NTFS advanced permissions on an existing user or group, the Permission Entry for <Object> box opens.

9. In the **Apply to** box, select how you want to apply this NTFS file permission entry.

If you are setting up NTFS file permissions on a single file, the **Apply to** box is not active. The **Apply to** setting defaults to **This object only**.

10. In the **Permissions** box, select the **Allow** or **Deny** boxes for the advanced permissions that you want to set on this object.

- To allow the specified access, select the **Allow** box.
- To not allow the specified access, select the **Deny** box. You can set permissions on the following advanced rights:
- **Full control**

If you choose this advanced right, all other advanced rights are automatically chosen (either Allow or Deny rights).

- **Traverse folder / execute file**
- **List folder / read data**
- **Read attributes**
- **Read extended attributes**
- **Create files / write data**
- **Create folders / append data**

- **Write attributes**
- **Write extended attributes**
- **Delete subfolders and files**
- **Delete**
- **Read permissions**
- **Change permissions**
- **Take ownership**



If any of the advanced permission boxes are not selectable, it is because the permissions are inherited from the parent object.

- If you want subfolders and files of this object to inherit these permissions, select the **Apply these permissions to objects and/or containers within this container only** box.
- Click **OK**.
- After you finish adding, removing, or editing NTFS permissions, specify the inheritance setting for this object:
 - Select the **Include inheritable permissions from this object's parent** box.

This is the default.
 - Select the **Replace all child object permissions with inheritable permissions from this object** box.

This setting is not present in the Permissions box if you are setting NTFS file permissions on a single file.



Be cautious when selecting this setting. This setting removes all existing permissions on all child objects and replaces them with this object's permission settings. You could inadvertently remove permissions that you did not want removed. It is especially important when setting permissions in a mixed security-style volume or qtree. If child objects have a UNIX effective security style, propagating NTFS permissions to those child objects results in ONTAP changing these objects from UNIX security style to NTFS security style, and all UNIX permissions on those child objects are replaced with NTFS permissions.

- Select both boxes.
- Select neither box.

- Click **OK** to close the **Permissions** box.
- Click **OK** to close the **Advanced Security settings for <Object>** box.

For more information about how to set advanced NTFS permissions, see your Windows documentation.

Related information

[Configure and apply file security on NTFS files and folders using the CLI](#)

[Displaying information about file security on NTFS security-style volumes](#)

[Displaying information about file security on mixed security-style volumes](#)

Configure NTFS file permissions using the ONTAP CLI

You can configure NTFS file permissions on files and directories using the ONTAP CLI. This enables you to configure NTFS file permissions without needing to connect to the data using an SMB share on a Windows Client.

You can configure NTFS file permissions by adding entries to NTFS discretionary access control lists (DACLS) that are associated with an NTFS security descriptor. The security descriptor is then applied to NTFS files and directories.

You can only configure NTFS file permissions using the command line. You cannot configure NFSv4 ACLs by using the CLI.

Steps

1. Create an NTFS security descriptor.

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -owner owner_name -group primary_group_name  
-control-flags-raw raw_control_flags
```

2. Add DACLS to the NTFS security descriptor.

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd  
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name  
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to  
{this-folder|sub-folders|files}
```

3. Create a file/directory security policy.

```
vserver security file-directory policy create -vserver svm_name -policy-name  
policy_name
```

How UNIX file permissions provide access control when accessing files over SMB

A FlexVol volume can have one of three types of security style: NTFS, UNIX, or mixed. You can access data over SMB regardless of security style; however, appropriate UNIX file permissions are needed to access data with UNIX effective security.

When data is accessed over SMB, there are several access controls used when determining whether a user is authorized to perform a requested action:

- Export permissions

Configuring export permissions for SMB access is optional.

- Share permissions
- File permissions

The following types of file permissions might be applied to the data on which the user wants to perform an action:

- NTFS
- UNIX NFSv4 ACLs
- UNIX mode bits

For data with NFSv4 ACLs or UNIX mode bits set, UNIX style permissions are used to determine file access rights to the data. The SVM administrator needs to set the appropriate file permission to ensure that users have the rights to perform the desired action.



Data in a mixed security-style volume might have either NTFS or UNIX effective security style. If the data has UNIX effective security style, then NFSv4 permissions or UNIX mode bits are used when determining file access rights to the data.

Copyright information

Copyright © 2023 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, 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) (FEB 2014).

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.