CIFS Permissions Best Practices

Nasuni Corporation – Boston, MA

Overview

You use permissions to control user access to data. There are two basic considerations when using permissions to control user access to data:

- Which users have access to the data.
- What type of access users have to the data.

You can assign permissions in Windows or using the Nasuni Filer, or both. In Windows, you apply NTFS permissions to folders and files. With the Nasuni Filer, you apply permissions to CIFS shares, which contain folders and files.

How CIFS share permissions and NTFS permissions interact

This example illustrates the relationship between NTFS and CIFS share permissions. Imagine that your data is locked inside a house. If you have the correct NTFS permissions, you can open the house to get your data. However, the house also has a fence around it. To get to the house, you must first open the gate in the fence. If you have the correct CIFS share permissions, you can open the gate to get to the house.

By default, CIFS shares authenticate all users: the gate in the fence is left open. However, by enabling any of the advanced access options, you lock the gate, which must be opened before you can open the house. Even if you leave the house door open (using NTFS permissions that allow everyone), you must still get through the gate.

For this reason, if enabling both levels of permissions, be aware that users may be locked out if their NTFS and CIFS share permissions do not align.

Nasuni recommends that the CIFS permissions allow everyone access. In this case, use the NTFS permissions to define who has access and what access they have.

The most complicated situation is when NTFS permissions restrict access to some users, but do not accurately define who has access and what access they have. In this situation, use the permissions for the CIFS share to define the subset of those users who should have access, and the access they should have.

Windows Permissions

On a Windows system, you can set permissions for folders and files. You can assign permissions to individual users or groups of users. You can allow or deny any combination of a variety of types of access, including read, write, modify, execute, create, delete, and full control.

Tip: The "Create folders / append data" permission is necessary to create files. If you want users to be able to create files in a folder, the "Create folders / append data" permission must be allowed.

Nasuni Filer Permissions

The Nasuni Filer offers CIFS share permissions using Active Directory or LDAP Directory Services security. To control who has permission to access CIFS shares that have Active Directory or LDAP Directory Services security, you can define users and groups of users, then assign specific permissions.

Setting permissions

Setting permissions in Windows

In Windows, you can set permissions using Windows Explorer. Right-click the folder or file, then select **Properties** from the drop-down list. Click the **Security** tab. Depending on the Windows version, you can click **Continue** to continue setting permissions or **Advanced** to set advanced permissions. You can create groups of users, assign users to groups, and set permissions for users and groups. Some actions require administrative privileges.

Requirement: In Windows, Nasuni requires that Authenticated Users have “Traverse folder / execute file” access to the root of the share as well as “Read attributes”, “Read permissions”, and “Read extended attributes”.
1. On the **Permissions** tab, click **Change Permissions**.
2. Select **Authenticated Users** in the list, then click **Edit**.
3. Click anywhere in the **Permissions** area, then click **Clear All** to clear all permissions.
4. Select the **Allow** check box for “Traverse folder / execute file”, “Read attributes”, “Read permissions”, and “Read extended attributes”.
5. Keep clicking **OK** to close all dialog boxes.

Tip: In Windows, Nasuni recommends that users NOT have “Full control” access to the share. On the **Advanced Permissions** pane, unselect the “Full control”, “Change permissions”, and “Take ownership” checkboxes.

Tip: In Windows, Nasuni recommends that “Full control” access to the share only be allowed for a service account specifically created for this purpose. “Full control” access to the share should not be given to ordinary groups such as Domain Admins or IT Department.

Warning: The membership of the `BUILTIN\Users` and `BUILTIN\Administrators` groups cannot be guaranteed on the Nasuni Filer. Use the Windows Explorer **Security** tab to check if any objects have the `BUILTIN\Users` or the `BUILTIN\Administrators` permission. If so, remove the `BUILTIN\Users` and `BUILTIN\Administrators` permissions, and instead add explicit permissions for the appropriate users and groups.

Setting permissions with the Nasuni Filer

On the Nasuni Filer, you can set permissions only for CIFS shares that use Active Directory or LDAP Directory Services security. These CIFS shares must be on volumes and Nasuni Filers that use Active Directory or LDAP Directory Services security. By default, folder and file security settings are set to Public. This means that any user may read, write, and execute from the default CIFS share.

If the Nasuni Filer has not yet joined an Active Directory domain, you can join the Nasuni Filer to an Active Directory domain. On the **Configuration** menu, select **General Settings**, then click **Join Domain**.

Tip: The hostname of the Nasuni Filer should not be the same as the name of the domain. This can interfere with the join process.

If necessary, create a CIFS volume that uses Active Directory or LDAP Directory Services security. It is not possible to change the authentication mode of a volume after you create the volume. Click **Volumes**, then click **Add New Volume**.

If necessary, for any CIFS volume that uses Active Directory or LDAP Directory Services security, create a new CIFS share. Each CIFS share has its own set of permissions. CIFS shares automatically use Active Directory or LDAP Directory Services security if they are on a CIFS volume that uses Active Directory or LDAP Directory Services security.
On the **Volumes** page, select the volume where you want to create a CIFS share. From the **Properties** drop down list, click **CIFS Shares**, then click **Add Share**. Click **Show Advanced Options**. The **Authentication**, **Group Access Levels**, and **User Access Levels** options appear.

- To authenticate all users, select **Authenticate all Users** (this is the default).
  Otherwise, to authenticate only specified groups and users, select "**Authenticate only specified Groups and Users**".
- Selecting "**Authenticate only specified Groups and Users**" enables the **Group Access Levels** and **User Access Levels** areas.

- To add a group, click **Add Groups**. The **Select Groups** page appears.
  - You can search for and add groups.
  - For each group, select either **Read/Write** or **Read Only** permission.
- To add a user, click **Add Users**. The **Select Users** page appears.
  - You can search for and add users.
  - For each user, select either **Read/Write** or **Read Only** permission.
- To hide files and folders that a user cannot access, leave the **Hide Unreadable Files** check box selected. This is the default.
- To enable case sensitivity for file or folder names, select the **Case-Sensitive Paths** check box. Using case-sensitive paths may improve performance but may reduce compatibility.

Tip: To ensure that users can access the CIFS share, if the "Authenticate only specified Groups and Users" option is set, make sure that the users are either in a Group (group level access) or are listed as specific Users (user level access), and have either Read/Write or Read Only permissions to the CIFS share.

Note: A CIFS share can be created from a folder already included in another CIFS share. You can create as many CIFS shares as you like to the same point or sub-points. They are not CIFS shares within CIFS shares, but just CIFS shares that are unrelated and could overlap.

You can also edit the settings of existing CIFS shares that use Active Directory or LDAP Directory Services security.

Note: When permissions change on a shared volume, any Nasuni Filers that connect to the volume see the changed permissions.

Setting up NTFS permissions from the Nasuni Filer

You can create inheritable NTFS permissions on a file or a folder tree based on CIFS share permissions. Follow these steps:

1. Create a CIFS share on the Nasuni Filer.
2. Apply Active Directory or LDAP Directory Services permissions to the CIFS share. The access permissions that are applied to the CIFS share on the Nasuni Filer only affect how the user connects to the CIFS share.
3. In Windows, map to the CIFS share from a host.
4. In Windows, create a new folder.
5. Apply the NTFS access permissions that are required to the new folder. Any subfolders and files created in the new folder inherit its permissions.

Permissions of Data Migration files

You can use the Data Migration Service to copy files from other locations to the Nasuni Filer. When you configure data migrations, you can handle the existing permissions of files in several ways:

- Apply specified NTFS-style permission sets: Allows you to define customized permission sets for data.
- (Advanced) Clone NTFS-Style permissions: Copies the permissions from the source as closely as possible.
- Copy Data Only, ignores NTFS-style permissions: Only copies data and ignores existing permissions.

Native Users and Local Authentication

Using the Nasuni Filer or Nasuni Management Console (NMC), you can grant access to specific users without using Active Directory or LDAP Directory Services. This can be useful for providing secure, authenticated access for users outside your corporate network such as customers, clients, or partners. Nasuni calls such users “native users.” Native users are explicitly defined and managed using the Nasuni Filer or NMC.

Creating external user accounts that are local to a Nasuni Filer is performed through Nasuni’s role-based access control settings. You can define specific access permissions for groups and users to perform actions within the Nasuni Filer user interface.

First, you define permission groups. You can add up to 150 permission groups to which you can assign users. For each group, you can specify exactly which actions the users in that group have permission to perform in the Nasuni Filer interface.

One of those role-based permissions is “storage access.” In order for members of a permission group to access storage without Active Directory or LDAP Directory Services authentication, the permission group must have the Storage Access permission enabled. Note that Storage Access does not grant any access to the Nasuni Filer user interface.

After you create the permission groups you need, you can add up to 150 users. For each user, you can specify which permission groups that user belongs to.

After you create a share that contains data that you’d like to make accessible to non-AD users, go to that share: on the Status menu, select CIFS Status, then select the share name. Click **Show Advanced Options**, and then enable **Web Access**. From the Authentication drop-down menu, select “**Authenticate only specified groups and Users**.” Then specify the Native Group or Native Users that can access this share.

To access data in that share, the external user then visits the web URL that IT provides. When accessing the web browser, the user enters the local authentication credentials that the Nasuni administrator created for them during the role-based access steps above.

In sum, providing Nasuni access to external network users is performed through the role-based access control settings normally reserved for setting administrative interface permissions.

Issues related to permissions

Historical SIDs

In Active Directory, a SID (Security Identifier) is a unique, immutable identifier of a user or user group. A security principal has a single SID for life (in a given domain), and all properties of the principal, including its name, are associated with the SID.

Part of the SID is unique to the domain of the SID, and the remainder of the SID is called a RID (Relative ID).

Practically, a SID consists of a string, such as:
"S-1-5-21-3623811015-3361044348-30300820-1013"

where

S indicates that the string is a SID.
1 is the revision level or the version of the SID specification.
5 is the identifier authority value.
21-3623811015-3361044348-30300820 is the domain ID.
1013 is the RID or relative ID in the domain.

In practice, the use of SIDs can lead to confused permissions, with users either having unexpected access to an item, or lacking expected access to an item. For example, if one company is merged with another, a user might get both a new SID and a so-called historical SID based on their old SID. If only the RIDs are used, under the assumption that the domains are the same, the permissions can become confused. Likewise, two SIDs that map to the same domain, and that have the same RID, become indeterminate. Similarly, if a user is deleted from Active Directory, any permissions related to that user can become orphaned.

Before adding data to a Nasuni Filer, it is a Best Practice to clean up historical and orphaned SIDs, as described in articles such as “Finding and Removing Orphaned SIDs in File Permissions” (https://helgeklein.com/blog/2012/07/finding-removing-orphaned-sids-in-file-permissions-or-busting-the-ghosts-built-into-windows-7/). This can help prevent later difficulties with permissions.

Combined permissions issues on Windows and the Nasuni Filer

If two different principals give a user different sets of permissions on an object, the Nasuni Filer handles those combined permissions differently from how Windows handles them. For example, if a user is a member of a group that has Read and Write permissions on an object, but the user themselves has only Read permissions, then:

- On Windows, the user will have Read and Write permissions.
- On the Nasuni Filer, the user will have Read permission only.

Additive permissions issues

Windows permissions are not additive on the Nasuni Filer. For example, if a user is a member of one group that has traverse permissions and that user is also a member of another group that has permissions to create folders, that user might not be able to both traverse and create folders, unless the ACL is changed so that both rights are on the same ACL. Otherwise, the Nasuni Filer selects one of the ACLs. The Nasuni Filer does not add all of the rights of all of the ACLs.

Trailing spaces in filenames

In Windows, trailing spaces in filenames can break permissions. If a file is having permissions issues, check the filename for trailing spaces.

Deny permissions issues

If an object has an inherited Deny permission and a non-inherited Allow permission, then the object's permissions cannot be guaranteed on the Nasuni Filer. For this reason, we recommend removing all Deny permissions.

Security tab not accessible for a folder

Issue:
In Windows Explorer, viewing the Security tab of a Windows file or folder (right-click, select **Properties** → **Security**) on a CIFS share on the Nasuni Filer gives a message that the user does not have permissions to see this information.

Resolution:
This is often caused by a permissions change that locked even the administrator out of the folder. The Nasuni Filer Administrative User has permissions to fix the permissions. Follow this procedure:

1. On the Nasuni Filer user interface, go to **Configuration** → **General CIFS Settings**.
2. Verify that there is an Administrative User set. If not, set an Administrative User (Active Directory user). You must enter the Active Directory username and password to connect the Nasuni Filer to Active Directory again. This disconnects all users currently accessing the Nasuni Filer.
3. Log in to the Windows server as the Nasuni Filer Administrative User. This user has the ability to view the Security tab for the problematic Nasuni Filer or folder, and change the permissions appropriately.