**CIFS structure**

**Security Style**

7MODE:

The root volume is always created as unix security-style.

CIFS-only data volumes are created as ntfs with ntfs qtrees.

Multiprotocol (CIFS/NFS) data volumes are created as unix with unix qtrees.

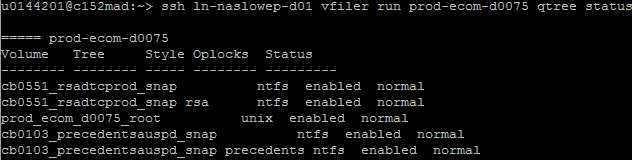
Non-standard, unix volume with ntfs qtree is considered CIFS-only qtree.

CDOT:

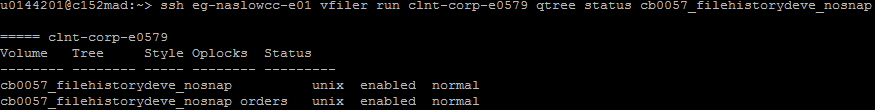
All volumes in a CIFS-only vserver are created as ntfs with ntfs qtrees, root included. Setting the root volume to ntfs is a new standard and new vservers will be created this way while pre-existing vservers will have a unix root volume.

Multiprotocol (CIFS/NFS) data volumes are created as unix with unix qtrees.

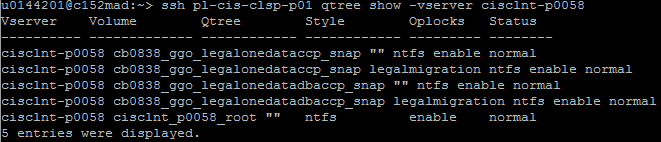
Example CIFS-only setup on 7mode



Example Multiprotocol setup on CDOT



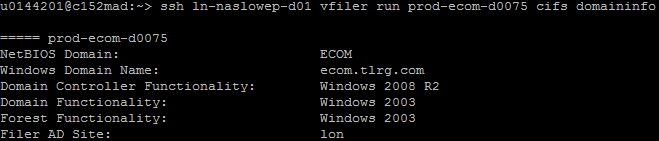
Example CIFS-only setup on CDOT



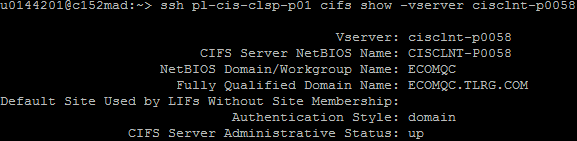
**Initial CIFS setup**

Running “cifs setup” on a 7Mode vfiler or running “cifs create” on a CDOT vserver will create and start the CIFS server on that vfiler or vserver tied to the provided Active Directory domain. This can take place before or after the volumes are created.

Example domain for 7Mode CIFS server



Example domain for CDOT CIFS server

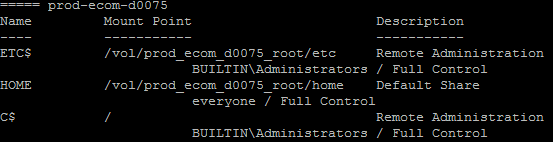


When the CIFS server is created, a few default shares are created off the root volume. In 7Mode, the default shares are ETC$, HOME, and C$. Per new standard, the HOME share should be deleted. In CDOT, the shares are admin$, c$, and ipc$.

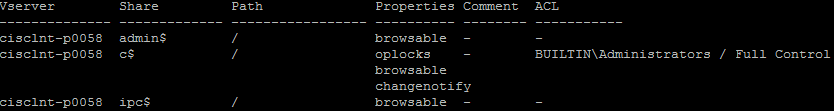
We do not use the default shares. This KB lists what the CDOT default shares could be used for.

<https://library.netapp.com/ecmdocs/ECMP1610207/html/GUID-5B56B12D-219C-4E23-B3F8-1CB1C4F619CE.html>

Example default shares on 7Mode



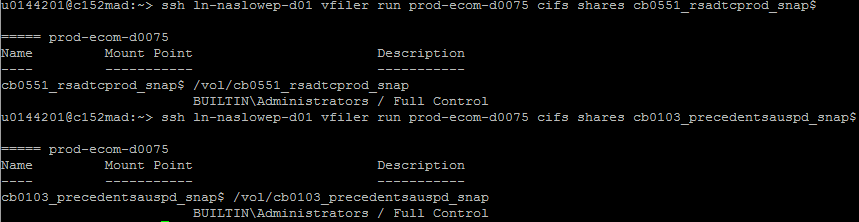
Example default shares on CDOT



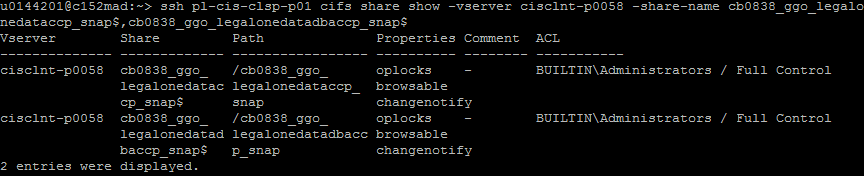
**Volume-level shares**

Storage team creates a volume-level share for each CIFS volume. This allows the CIFS support team to create and manage the data shares and permissions. The share-name is <volume>$ and points to the volume path, /vol/<volume> on 7Mode or /<volume> on CDOT.

Example volume-level shares on 7Mode



Example volume-level shares on CDOT



**Data Shares**

If new storage is required for a new share, at minimum storage creates a new qtree with quotas on pre-existing storage, while at maximum storage creates a new vserver, cifs server, volume, volume-level share, and qtree with quotas.

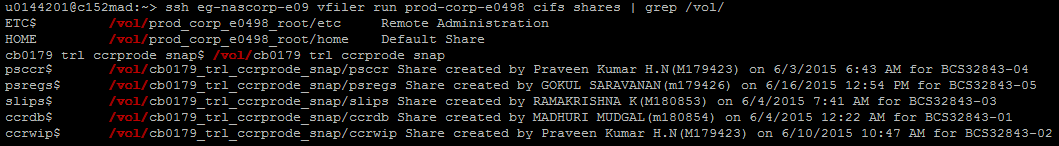
Example data shares

The volume-level shares are named after the volume and point to the volume path.

The data shares are named after the qtree+subfolder and point to the volume\qtree\subfolder path.



The multiprotocol shares are named after the qtree and point to the volume\qtree path.



**CIFS Access**

There are three levels of CIFS access which cross both Storage and Windows standards.

**Domains and trusts**

The CIFS server is created in an Active Directory domain, TEN, MGMT, ECOM, ECOMQC, TLR, TLRQA, LHTRP, CLRRS, ERF, TFPROD, and TFCORP to name a few.

Most domains are trusted to the primary domains MGMT and TEN. Due to this trust, for any CIFS servers created in a domain trusted to MGMT (MGMT, ECOM, ECOMQC, LHTRP, CLRRS, TFPROD) should use MGMT groups and any CIFS servers created in a domain trusted to TEN (TEN, TLR, TLRQA, ERF, TFCORP) should use TEN groups.

**AD Group Definition**

|  |  |
| --- | --- |
| **Group or Account** | **Definition** |
| BUILTIN\Administrators | Default local group on the vserver |
| Everyone | Open access to all, insecure |
| NT AUTHORITY\Authenticated Users | Group covering all valid domain accounts, more secure than Everyone |
| <domain>\<vserver>.<sharename>.m | CIFS-only structure 1 **MODIFY** group\* |
| <domain>\<vserver>.<sharename>.r | CIFS-only structure 1 **READONLY** group\* |
| <domain>\<vserver>.<sharename>.<subfolder>.m | CIFS-only structure 2 **MODIFY** group\* |
| <domain>\<vserver>.<sharename>.<subfolder>.r | CIFS-only structure 2 **READONLY** group\* |
| <domain>\<vserver>.<sharename>.c | Multiprotocol **CHANGE** group\* |
| <domain>\<vserver>.<sharename>.f | BU is granted FULL CONTROL access\* |
| MGMT\M-EaganServerAdmins | Windows AD group for MGMT trust domains |
| TEN\M-EaganServerAdmins | Windows AD group for TEN trust domains |
| MGMT\REST-STORAGE-SUPPORT-ServerAdmins | Storage AD group for MGMT trust domains |
| TEN\-DG-APP-REST-STORAGE-SUPPORT-ServerAdmins | Storage AD group for TEN trust domains |
| <domain>\M-Storage-Admins.G | Old storage AD group for various domains, should be replaced with appropriate new group |

\*TEN domain follows its own set of unique naming standards. TEN domain groups will be prefixed with “-DL-FIL” and end in “modify”, “read”, “change”, or “full” instead of just m, r, c, or f.

Example TEN groups on a Structure 2.



1. **LAG: Local Administrators Group**

When the CIFS server is created, a default local group is created called BUILTIN\Administrators, commonly referred to as the LAG. The team which will be supporting the CIFS share creation and permissions needs to be added to the LAG. In most cases this is Windows-Support, but Remote Office teams manage some shares in the infrastructure.

Storage-Support is not required in the LAG since we do not manage CIFS creation and permissions, but we can grant ourselves this access to view the shares to assist in troubleshooting issues – Look, but do not touch!

BU groups or accounts should NEVER be added to LAG.

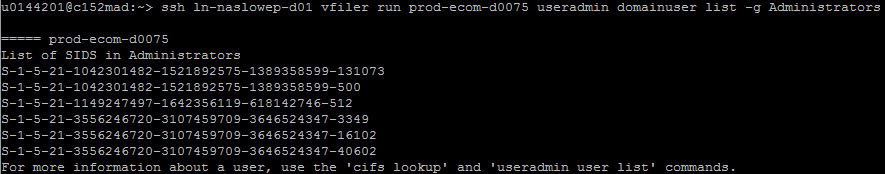
For Windows-Support, the MGMT\M-EaganServerAdmins group should be used for all MGMT domains and trusts while the TEN\M-EaganServerAdmins group should be used for all TEN domains and trusts.

For Storage-Support, the MGMT\REST-STORAGE-SUPPORT-ServerAdmins should be used for all MGMT domains and trusts while the TEN\-DG-APP-REST-STORAGE-SUPPORT-ServerAdmins group should be used for all TEN domains and trusts.

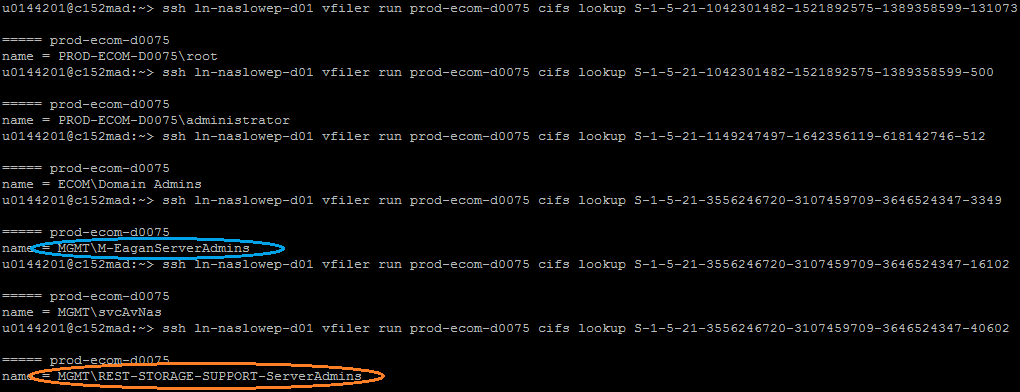
Remote office groups are dependent on the build. (Examples TBD)

To view the LAG in 7Mode, first list the members of the local Administrators group. This will output a list of SIDS which will then need to be resolved into their human-readable names using cifs lookup. Viewing the LAG in CDOT will already list the human-readable names.

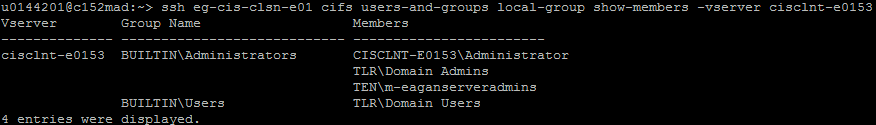
Example in 7Mode, first list the SIDS



Example in 7Mode, second perform cifs lookup



Example in CDOT



1. **Share-level Access / Share Permissions**

The share-level access is the permissions depicted in the “cifs shares” 7Mode or “cifs share show” CDOT output. In CDOT, this is referred to as the ACL access control list.

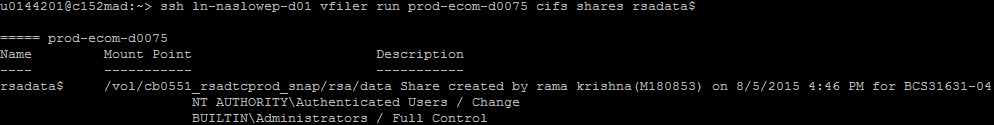
The Volume-level shares should only list “BUILTIN\Administrators” with Full Control access. The “Everyone” group should always be removed and replaced with the LAG. This is done by Storage because it is the volume-level share.

CIFS-only data shares should only list “BUILTIN\Administrators” with Full Control access and “NT AUTHORITY\Authenticated Users” with Change access. “Everyone” group should always be removed.

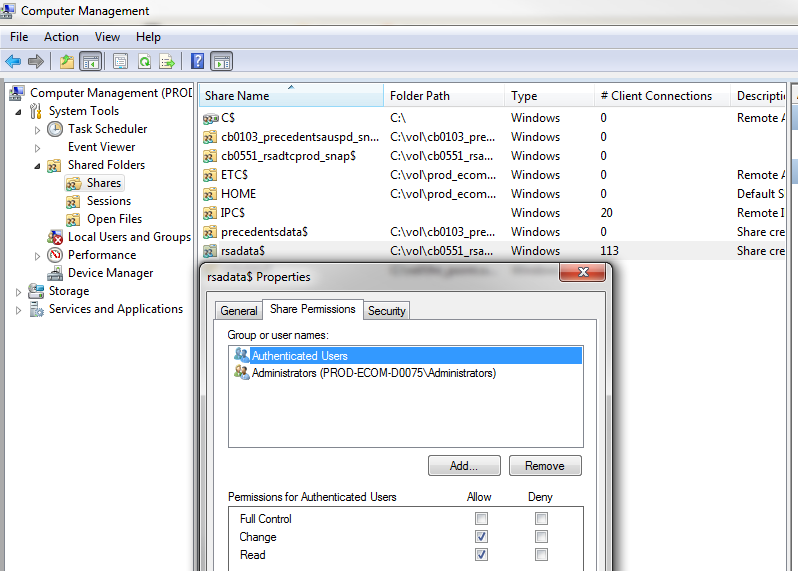
Multiprotocol CIFS/NFS data shares have unix permissions set open to 777. The share-level permissions are then locked down with “BUILTIN\Administrators” with Full Control access and a CHANGE group (<domain>\<vserver>.<sharename>.c) with Change access. Any BU groups or users requiring access are added to the CHANGE group.

The CIFS support team has access to modify the share-level permissions which is why Storage does not modify these permissions on data shares. Other than the permissions listed in the above descriptions, no other groups should be added. Remember, CIFS support team is in the LAG, so the LAG needs to be added to the share-level permissions and NOT the CIFS support team directly.

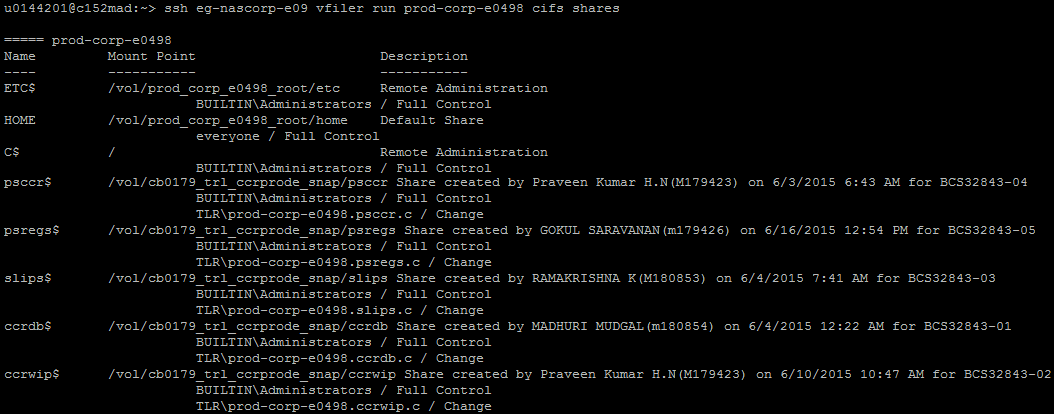
Example of CIFS-only data share on 7Mode, as seen by Storage



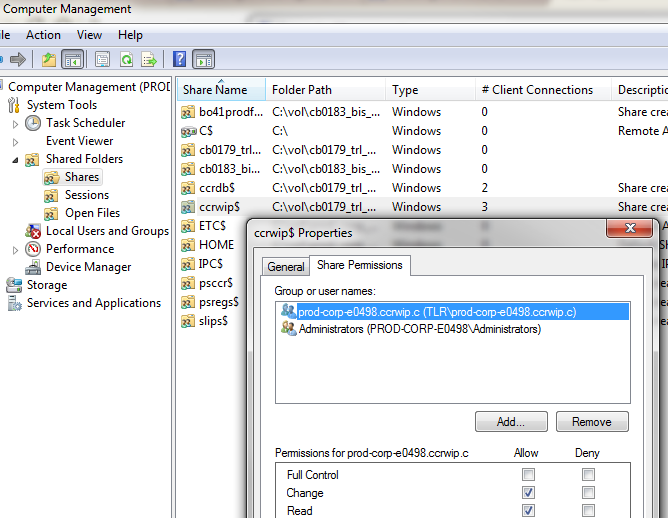
Example of CIFS-only data share on 7Mode, as seen by Windows



Example of Multiprotocol data share on 7Mode, as seen by Storage



Example of Multiprotocol data share on 7Mode, as seen by Windows; note there is no Security tab in the Properties window.



1. **NTFS File Permissions / Security**

NTFS permissions are set on CIFS-only builds. Multiprotocol builds only use the CHANGE group applied to the share-level permissions. This is because multiprotocol volumes and qtrees are set to unix security-style while NTFS permissions require ntfs security-style.

The CIFS support team manages the file-level permissions. Storage should NEVER modify these permissions. The NTFS permissions can be viewed in Computer Management under the Security tab of the share Properties or with “fsecurity” command on 7Mode or “vserver security file-directory show” command on CDOT.

There are two CIFS structure standards set by Windows D&E. Structure 1 is most common.

**Structure 1**

Volume

Qtree

Subfolder1 (share$) 🡨 Unique permissions set here

The share points to volume\qtree\subfolder1 and the permissions are restricted on subfolder1.

Permissions are set to “NT AUTHORITY\SYSTEM” account and “BUILTIN\Administrators” group with Full Control access. “NT AUTHORITY \Authenticated Users” group is removed. MODIFY (“<domain>\<vserver>.<sharename>.m”) and READONLY (“<domain>\<vserver>.<sharename>.r”) groups are added. Any BU users or groups needing access to the share will be added to the MODIFY or READONLY group depending on the access requested.

**Structure 2**

Volume

Qtree (share$)

Subfolder1a 🡨 Unique permissions set here

Subfolder1b 🡨 Other unique permissions set here

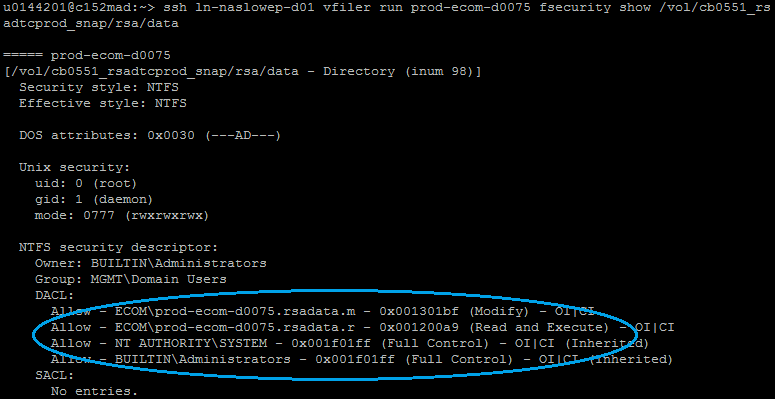
Subfolder1c 🡨 Additional unique permissions set here

The share points to volume\qtree, but permissions are restricted on each subfolder1. Each subfolder1 will have unique permissions from each other.

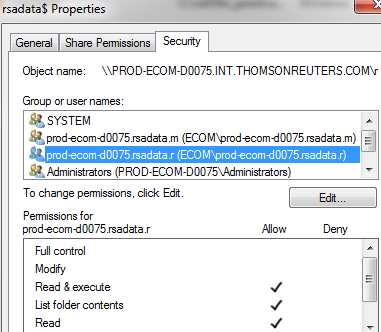
The share/qtree will have “NT AUTHORITY\Authenticated Users” group with Readonly access, “BUILTIN\Administrators” group with Full Control access, and “NT AUTHORITY\SYSTEM” account with Full Control access.

Each subfolder1 has permissions set to “NT AUTHORITY\SYSTEM” account and “BUILTIN\Administrators” group with Full Control access. “NT AUTHORITY \Authenticated Users” group is removed. MODIFY (“<domain>\<vserver>.<sharename>.<subfolder>.m”) and READONLY (“<domain>\<vserver>.<sharename>.<subfolder>.r”) groups are added. Any BU users or groups needing access to the share will be added to the MODIFY or READONLY group depending on the access requested.

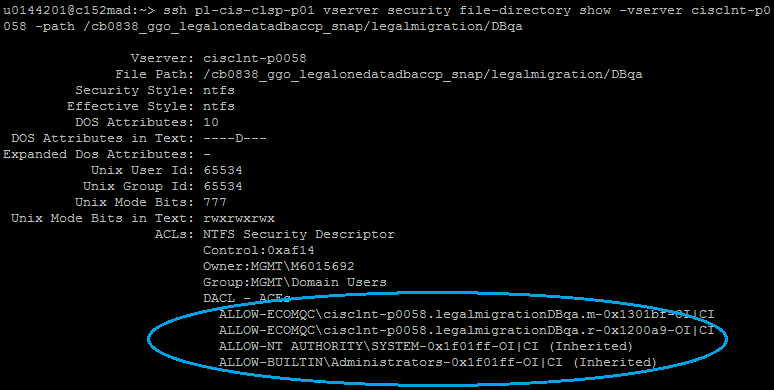
Example Structure 1 NTFS permissions on 7Mode, as seen by Storage



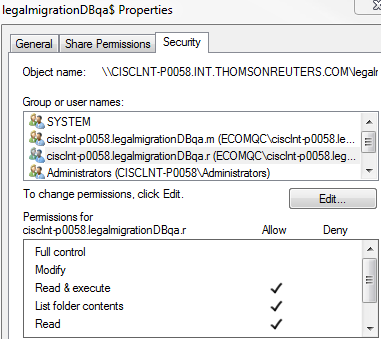
Example Structure 1 NTFS permissions on 7Mode, as seen by Windows



Example Structure 1 NTFS permissions on CDOT, as seen by Storage

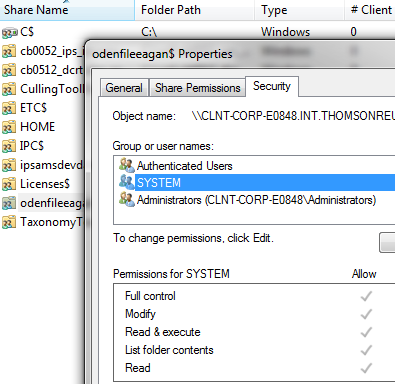


Example Structure 1 NTFS permissions on CDOT, as seen by Windows

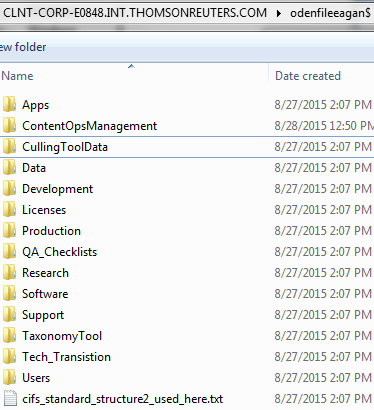


Example Structure 2 NTFS permissions on 7Mode, as seen by Windows

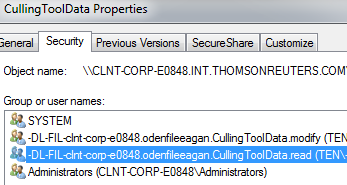
In Computer Management, the base permissions are listed, but there are no MODIFY or READONLY groups specified. Need to open the share and view the subfolder permissions.

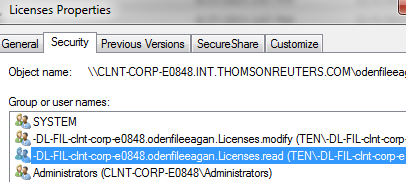


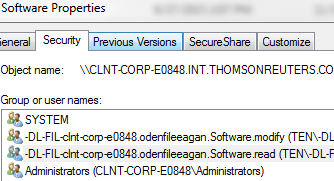
Opening the share shows the subfolders that have unique permissions. There is also a text document stating this is a Structure 2 build.

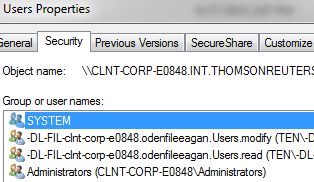


Each subfolder has unique permission groups created and applied. The unique groups are named for the subfolder.









Windows standards document

<https://theshare.thomsonreuters.com/sites/windows/Operational%20Documents/Standard%20-%20Folder-Share-Standards.docx>