**NE247 – Windows Server – Lab4**

If you see the Domain name **WIDGETS.PRI** anywhere, including images, think **AVERY.PRI**

**Points will be deducted if All Answers Are Not In:**

**Ariel, 14pt, Bold, Red!**

In this lab, you will investigate NTFS permissions, Share permissions and the result of both Share and NTF permissions in combination

Required Materials:

**SRV16** and **WIN10** images prepared in previous lab exercises

Permissions

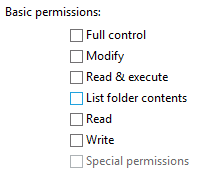
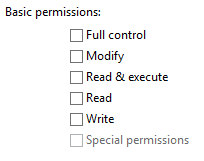
Controlling access to resources such as files and folders is called **Authorization.** We use Permissions to protect these resources from both access at the local computer and access from across the network. There are two kinds of permissions we can assign.

**NTFS permissions** are settings applied to a file or folder using the file system on the storage medium such as a hard disk drive. For NTFS permissions to be used, the drive must be formatted with the NTFS file system. Because NTFS permissions are applied at the file system level, they are always in effect. This applies to any access to the file or folder whether the user is accessing the resource from the local keyboard or from another computer in the network.

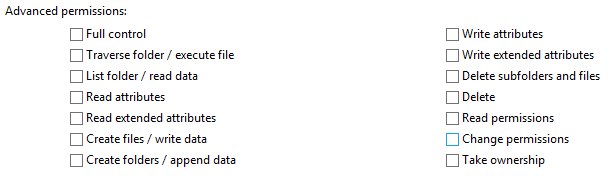
There are 6 standard folder permissions and 5 standard file permissions. Each standard permission is in turn made up of more granular permissions called Special or Advanced permissions.

Standard or Basic Permissions

For Folders For Files



Special or Advanced Permissions for Folders



**Share permissions** control access to folders that are accessed from other computers in the network. They have no effect on a user who is using the local computer that contains the shared folder.

There are only three standard or basic Share permissions which are shown by different names depending on whether you are doing basic or advanced sharing. It is strongly recommended that you only use advanced sharing because basic sharing also modifies the underlying NTFS permissions can easily lead to errors and security holes.

Basic Sharing Advanced Sharing



What leads to confusion with basic sharing is that if you give a user or group either the Owner or Read/Write basic share permission, the NTFS permission for that user or group is set to Full Control for that folder. Any files or sub folders will inherit the Full Control permission for that security principle. If you give a security principle the Read basic share permission, the NTFS permission for that principle is given the Read and Execute NTFS permissions.

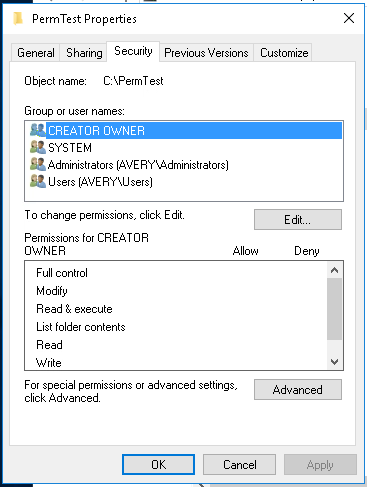
**Combined permissions**: When a user connects to a shared folder and then accesses files or subfolders though that share, both the share permissions and any NTFS permissions are used to determine the users effective level of access. In such a case, whichever permission (share or NTFS) is the most restrictive is the permission that sets the maximum level of access. For example if a user has the Full Control permission at the Share, but only Read permission set on the NTFS file system, the user is only have the Read permission. Neither NTFS nor Share permissions take precedence over the other. Whichever is set to the most restrictive level of access is the maximum permission the user is allowed.

It is common practice to set Share permissions (using Advanced Sharing permissions) very open and use NTFS permissions as the primary means of securing folders and files since the NTFS permissions are always in effect wither the resource is access locally or from across the network. Typically this would involve giving the Everyone system group the Full Control share permissions.

Part 1: NTFS Permissions

***In the next steps you will examine the default NTFS permissions and the permissions interface and permission inheritance from parent to child object.***

* Start **SRV16** if it isn’t already running and log on with your personal administrative account.
* Open File Explorer and **create a new folder** under your C: drive called **PermTest**.
* After creating the folder, **right click on it and select Properties**. You will see several tabs including the Sharing tab for configuring sharing and the Security tab for NTFS settings.
* Click on the **Security tab** to view the Discretionary Access Control List.



* Under Group or user name you will see all the groups or users that currently have permissions defined for them. These entries are called the Access Control Entries or ACEs.
* When you click on one of the ACEs you will see the standard permissions below with check marks for the current permissions. You may see some that only have a checkmark for Special Permissions which just means you have to dig deeper to find out exactly what permissions they have.
* Fill in the following for the ACEs and their standard permissions (you will probably not need all the lines provided).

User or Group Name Standard Permissions

**Administrators Full Control**

**Users Read and Execute**

**William Bain Special Permissions**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

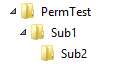
**\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

* Click on the Advanced button and you will see more information. Note that some entries may be listed more than once. If so, look under that Applies to column and you will see differences.
* On the Advanced Security Settings window you will see an entry for the Owner of this resource (folder).

Who is the owner? **William Bain**

* Click Cancel twice to close the Properties windows.
* Create a folder under the **PermTest** folder call **Sub1** and a folder under **Sub1** called **Sub2**.

Ensure that the hierarchy looks like **PermTest > Sub1 > Sub2** as shown below.



* Check the NTFS permissions on **Sub1** and **Sub2**. You should find that they have inherited the NTFS permissions from their parent folders (Sub1 from PermTest and Sub2 permissions from Sub1).
* Do you see any differences between the Standard NTFS permission in the child folders and the permissions of the **PermTest** folder? [**Y / N] N** (you shouldn’t).
* Create a New Text Document in **Sub2** called **Test1.txt** This file will inherit NTFS permissions from its parent folder.
* Right click on Test1.txt and select Properties.
* You will notice that while there are several tabs on a file, there is no Sharing tab. That is because you can only share folders, not files. Files are accessed from within the shared folders when you connect to the share. Click on the Security tab.
* List the ACEs and Standard permissions.   
  User or Group Name Standard Permissions

**SYSTEM Full Control**

**William Bain Full Control**

**Admins Full Control**

**Users Read and Execute**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

* What is different in the Groups and User name ACEs in the file from its parent folder?

**Administrators is in the list**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

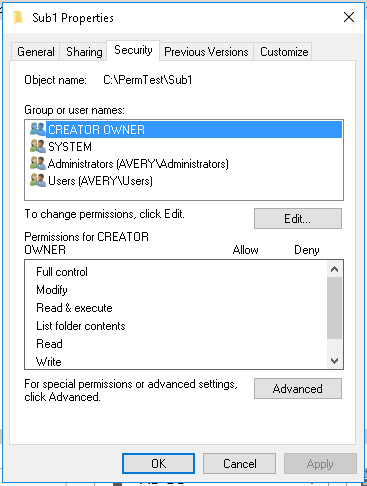
* What is different in the list of Standard Permissions in the file form its parent folder?

**Users have read and execute**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

***In the next steps you will stop inheritance and examine the effects on object permissions.***

* Open the NTFS permissions access control list for Sub1 (security tab in properties)
* .Click the Edit button and then click on the ACE for the Administrators group



* Try to uncheck one of the permissions check marks.

Why can’t you change it?

**The folder is inheriting the permissions from permtest**

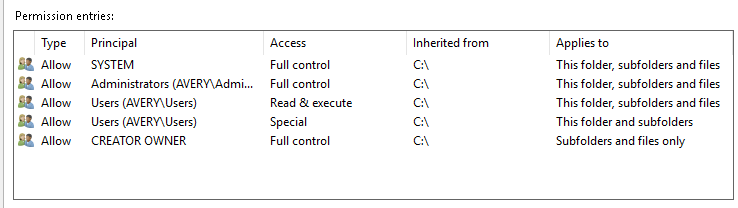
* Click cancel to get back to the Security tab and then click the Advanced button.
* Click on the button for Disable inheritance.

What are your choices?

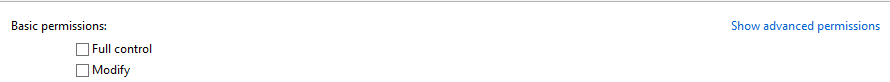
**Explicit vs remove all**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

* Select to convert to explicit permissions, then click OK to return to the Security tab in the properties window.
* Click Edit and then select the Users group.
* Uncheck the Read & Execute permission then click to check it again. Now that there are all explicit permissions, you can change them any way you want.
* You should see that you still can’t change the Special permissions check box. To examine the special permissions you will need to click Cancel to return to the Properties window then click the Advanced button
* Highlight the row that contains Special under the Access column, then click the Edit button.



* Locate the link on the right side of the widows that says Show advanced permissions and then click on the link.



What are the Advanced Permissions that the user group has in addition to its standard permissions?

**Traverse, execute file, list folder, read data, read attributes, create files, write data, create folders, append data, read permissions**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

* Return to the main Security tab window in Properties and click Edit.
* Remove the Administrator group from the list and click OK, then continue to click OK until the widows have closed.
* Locate Check the NTFS permissions on the Sub2 folder.

Does the Administrators group have any permissions set for Sub2?  **[Y / N] N**

* Check the NTFS permissions on the Test1 file.

Does the Administrator group have any permissions set for Test1? **[Y / N] N**

* Close any properties windows.
* Open the Test1 file, type your name in it and save the changes.
* Log off **SRV16**

***In the next steps you will see how and Administrator can use membership on other groups to access resources***

* Log on as the built in **Administrator** account.
* What security groups is the built in Administrator a member of? [Hint: check ADUC]

**administrators**

**domain admins**

**domain users**

**enterprise admins**

**group policy creator owners**

**schema admins**

* What security groups is the Domain Users a member of?

**Users**

Keep in mind that any an account not only gets permissions from the groups it is a direct member of, but of any groups those groups are member of. So even though the Administrator isn’t a member of the Users group, the Administrator gets User group permissions from membership in the Domain Users group.

* Still logged in as the Administrator, open the Test1 file, add the date and try to save the file. Are you able to save the change without creating a new file? **[Y / N] N**

(if you can, you did something wrong!)

* Open the Test1.txt Properties and click on Security, then Edit.
* Can you change the permissions? **[Y / N] Y**

**In the next section you will see how an administrator can gain access to a resource even without any permission initially.**

* Log off **SRV16** and log back on as your personal administrate account..
* User File Explorer to navigate to Sub1 and remove the Users group from the NTFS access control list.
* **Log off and log on as the built in Administrator account**
* Use File Explorer to navigate to the Sub1 folder.

What message do you get when you try to open Sub1?

**“You don’t currently have permission to access this folder”**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

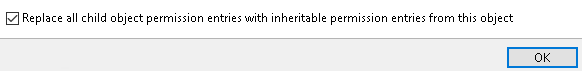
* Go to the Properties of Sub1 and click on Security, then click the Advanced button.

What does it say for Owner of Sub1?

**“Unable to display current owner”**

* Click on Change next to the Owner message
* Type in Administrators and click on Check Name to make sure you spelled it correctly, then click OK.
* If you want this to apply to child objects (and you do) **you will need to check the box to Replace owner on sub containers and objects** then click OK. (Remember that the Owner of an object can always change the permissions on the object.)





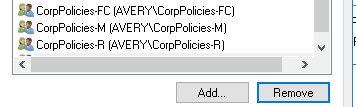
* Close the Security tab and reopen it
* Click Edit to add your personal account to the list and give your account Full Control.
* Click on the Advanced button and check the box to Replace all child object permissions …. And then click OK
* Still logged in as Administrator, open the Test1 file add the date and try to save the changes.

Can you save the changes now? **[Y / N ] Y**

* Log off as Administrator and log back on with our personal administrative account.
* Can you access the Test1 folder and save changes to it? **[Y / N ] Y** (don’t continue until you can)

**SOME OF THIS MAY ALREADY BE DONE, READ THOUROUGHLY!!**  In Lab 3 you created a folder structure for some of the Widget departments. You also designed several Domain Local groups for assigning permissions to those folders. Now it is time to set the permissions.

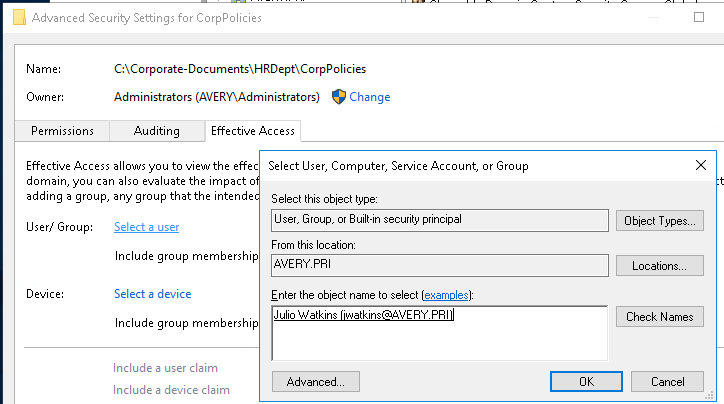
* Use File Explorer to navigate to the **HRDept** folder then down to the CorpPolicies folder, and open the NTFS permissions access control list.
* Remove all groups from the access control list [Hint: stop inheritance]
* Add the three domain local groups you created in Lab 3 for this folder.
* Set each group to the permission indicated in the name of the DL group



* Now, configure permissions for the other DL groups for the appropriate folders in the Corporate Documents structure. *Be sure to remove any unnecessary groups from the Access Control Lis*t. Leave the Administrators group in the ACL so the administrator (you) will always have control.

***You will now determine the effective permissions (or effective access) for a user or group. Effective access is a good way to check to see if your permissions will have the effect you want.***

* At this point you have finished setting permissions for the CorpPolicies folder. In the Security tab of the CorpPolicies Properties, click on Advanced and then click on the **Effective Access** tab



* Click on Select a User and [Check Names] for **Julio Watkins**
* Click the **View effective access** to see what permissions Julio Watkins on this folder based on group memberships and the permissions you set for those groups. You’ll see a red X at every permission that’s not available to the user and a green check mark for every permission that the user has.

What are Julio Watkins permissions for the CorpPolicies folder?

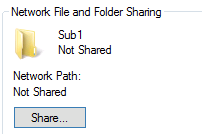
**Traverse, list, read, read attributes, create files/folders, read permissions**

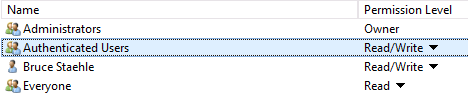
* Using the process what permissions does **Ivan Grant** have for the **CorpPolicies** folder?

**Traverse, list, read, read attributes, create files/folders, read permissions**

* Examine the effective access for several different users for different folders to see if your permissions are set correctly.
* Close all tabs for the CorpPolicies folder.

Part 2: Share Permissions

* In the next few steps you will see how to use the basic sharing button and you will also see why it can lead to unexpected results because it not only sets sharing permissions, but also sets NTFS permissions.
* Using File Explorer navigate to the **\PermTest\Sub1** folder.
* Open the **Sub1** Properties and click on the Security tab.
* Remove any users or groups except for your personal administrative account which should have the Full Control NTFS permission.
* Click the Share button
* In the blank input box type in **Everyone** and click Add
* Next, add the **Authenticated Users** group
* In the Permissions level, set the **Everyone group to Read** and **the Authenticated Users group to Read/Write,** then click the Share button at the bottom of the File Sharing window.



* You should then get a screen saying that the folder is shared.
* Click Done
* Now open the Security tab for **Sub1** and examine the NTFS permissions.

What is the highest permission for the Everyone group?

**Read and execute**

What is the highest permission for the Authenticated Users group?

**Full control**

You should now see that using this basic sharing mode causes and opening of NTFS permissions which could lead to errors or even security lapses. The advantage of this method is that an inexperienced user can share a folder without having to add groups and permissions at the NTFS level. While simple, it has potential problems.

***In the next steps you will see how to stop sharing a folder.***

* Return to the Sharing tab of **Sub1** and click on the Advanced Sharing button.
* Uncheck the box for Share this folder to remove the share, then click OK.
* Now go to the Security tab to examine the NTFS permissions.
* When you stopped sharing, did the NTFS permissions to back to where they were before you used the basic sharing option? [Y / N] **N**

***In the next steps you will use the Advanced Sharing option.***

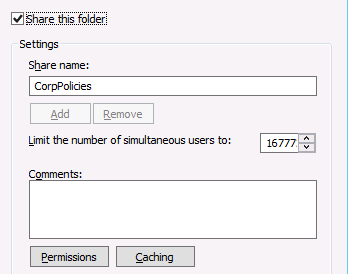
* Close any windows that might still be open for the Sub1 folder.
* Navigate to the **CorpPolicies** folder and open the Properties windows.
* Just as a reminder, examine the Security tab to confirm the groups that have permissions set. List the group names below.

**CorpPolicies-FC**

**CorpPolicies-M**

**CorpPolicies-R**

* Now open the Sharing tab and click on Advanced Sharing.
* Click to check the box to Share this folder then click the Permissions button



* What is the default group and what permission does this group have?

Group **Everyone**  Permission **Read**

* Add the Authenticated Users group and give this group the Full Control permission.
* Remove the Everyone group so that the only share permission is for the Authenticated Users group then click OK twice to finish setting up the share.
* Close the Properties window.
* Start **WIN10** and log on with the **Woodrow Webb** account.
* Go to the Desktop and open File Explorer as **Woodrow Webb** on **WIN10**
* Expand the Network tab in the left pane and then expand the **SRV16** icon.

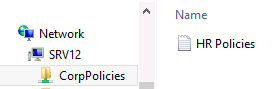
What shared do you see on the domain controller, **SRV16**?

**CorpPolicies**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

* **Click on the CorpPolicies share and in the right pane create a new text document called HR Policies**. Open the text file, put in the date and save the changes.



* Log off **WIN10** and log on as **Julio Watkins** who is an HR staff member.
* Navigate to the HR Polices text document on **SRV16** and open the file.
* Add some content to the file and try to change save the changes.

Why can’t **Julio Watkins** save changes to the file?

**Julio Watkins is only HR Staff, so they only have read permissions**

* Log off and log on with the **Lavern Keller** account which is not a member of the HR department.

What happens when **Lavern Keller** tries to open the CorpPolices shared folder?

**User does not have permission to access the folder**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

* Log off and log on to **WIN10** with your personal administrative account.
* Navigate to the **HR Polices** file**, enter your name and date to the file and save the changes**.

Part 3: Accessing Hidden Shares

Every drive on a computer is automatically given a hidden share at the root of the drive. This share can only be accessed by users who have administrative privileges to the drive. You can also hide any regular share by adding a $ to the end of the share name. This allows an administrator access to a computer remotely with administrative control even if there are no other shares that allow such access.

* Close File Explorer and open the Run dialog box (go to the Start screen and type in \\.)
* Type in \\**SRV16**\c$ and press enter *(NOTE: Use the actual name of your server in place of* ***SRV16*** *in this example*)



* You should get a window presenting the directory structure of the root of the C: drive on **SRV16**.
* Log off **WIN10** and log back on as **Woodrow Web**. (Note how much quicker this logon is.)
* Open the Run dialog box, type in \\**SRV16**\c$ (using your computer’s name) as you did before.

Describe what happens when you try to access the administrative share using this account.

**Access denied, credentials required**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

* .Shutdown your images -END