# Week 8 Windows Server Activities – Resource Access

Activities

[Week 8 Windows Server Activities – Resource Access 1](#_Toc170907832)

[Activity 8-1: Sharing a Folder with Simple File Sharing 1](#_Toc170907833)

[Activity 8-2: Experimenting with NTFS Permissions 3](#_Toc170907834)

[Activity 8-3: Setup and Configure Folder Permissions 5](#_Toc170907835)

[Activity 8-4: Manually Mapping a Drive 7](#_Toc170907836)

[Activity 8-5: Map Drives with Logon Scripts 8](#_Toc170907837)

[Logon Scripts by User in Active Directory 9](#_Toc170907838)

[Activity 8-6: Mapped Drive Logon Scripts by Group Policy 9](#_Toc170907839)

[Activity 8-7: Mapped Drives by Group Policy Preferences 10](#_Toc170907840)

[Assignment Submissions 12](#_Toc170907841)

**How to Create Screenshots:** Please use the Windows Snip and Sketch Tool or the Snipping Tool. Paste a screenshot of just the program you are working on. If you are snipping a virtual machine, make sure your focus is outside the virtual machine before you snip.

1. Press and hold down the **Windows key** & **Shift**, then type **S.** This brings up the on-screen snipping tool.
2. Click and Drag your mouse around whatever you want to snip.
3. Release the mouse button. This places the snip into the Windows Clipboard.
4. Go into Word or wherever you want to paste the snip. Hold down **CTRL**, then type **V** to paste the snip.

# Activity 8-1: Sharing a Folder with Simple File Sharing

Time Required: 10 minutes

Objective: Create a test folder and then share it with simple file sharing.

Required Tools and Equipment: Server1

Description: You understand that there are several ways to create shared folders. You decide to try simple file sharing to see how it sets permissions automatically. This type of file sharing is simple, but not very useful. This is rarely used in a business environment, as you want more detailed security.

1. Log on to Server1 as your administrator level account, if necessary.
2. Create a folder named **TestShare1** in the Data folder.
3. Open **TestShare1’s** Properties dialog box. Click the **Security** tab. Make a note of the permissions assigned on this folder, and then close the Properties dialog box.
4. Right-click **TestShare1** 🡪 point to **Give access to** 🡪 Click Specific people to open the File Sharing dialog box. Notice that your administrator account user and Administrators group already have access.
5. Click the list arrow next to the Add button, use **Find People** to locate **Sales2** in the list. (You can also create a new user by clicking the “Create a new user” option.)
6. Click the **Add** button. By default, the user has Read permission.
7. Click the list arrow next to **Read** and click **Read/Write**.
8. Click **Share**. You see a message indicating the folder is shared. You can e-mail links to the shared folder or copy the links to the Clipboard. You can also click the “**Show me all the network shares on this computer**” link to open the network browse window for your server. Click Done.
9. Open **TestShare1’s** **Properties** dialog box. Click the **Sharing** tab, then Click **Advanced Sharing**.
10. Click **Permissions**. Notice that the Everyone group and Administrators group are assigned Full Control to the share, which is the default setting with simple file sharing. Permissions can be restricted by using NTFS permissions.
11. **Insert a screenshot:**

Click or tap here to enter text.

1. Click Cancel twice.
2. In the **TestShare1** folder’s Properties dialog box, click the **Security** tab. Scroll through the ACEs in the DACL. Notice that Sales2 and Administrator ACEs were added to the DACL with Full control NTFS permissions. In addition, the CREATOR OWNER ACE has been removed. However, all other ACEs were maintained. In the real world, this may or may not be what you intended. Simple file sharing is just that—simple—you typically want to exert more control over file sharing.
3. Close all open windows. If you’re continuing to the next activity, stay logged on; otherwise, log off or shut down Server1.

# Activity 8-2: Experimenting with NTFS Permissions

Time Required: 10 minutes

Objective: Experiment with NTFS permissions.

Required Tools and Equipment: Server1

Description: You’re somewhat confused about NTFS permissions, so you create some files to use in a variety of permission experiments.

1. Log on to Server1 as your administrator level account, if necessary.
2. Open **File Explorer**. Navigate to the **TestShare1** folder you created earlier in the **Data** folder.
3. Create a text file called **TestBatch.bat** in the **TestShare1** folder. When asked whether you want to change the file extension, click Yes.
4. Right-click **TestBatch.bat** and click Edit. Type **@ Echo This is a test batch file** Press Enter. On the next line, type **@ Pause**. Save the file, and then exit Notepad.
5. To test your batch file, double-click it. A command prompt window opens, and you see “This is a test batch file. Press any key to continue . . .” Press the spacebar or Enter to close the command prompt window.
6. Open the **Properties** dialog box for **TestBatch.bat**, click the **Security** tab, then Click **Advanced**. Click the **Disable inheritance** button. In the message box that opens, click **Convert inherited permissions into explicit permissions on this object**. Notice that the three permissions entries now indicate “None” in the Inherited from column.
7. **Insert a screenshot:**

Click or tap here to enter text.

1. Click OK.
2. Click Edit. Click Users in the Group or user names list box. In the **Permissions for Users** list box, click to clear the **Read & execute** check box in the Allow column and leave the **Read** check box selected.
3. **Insert a screenshot:**

Click or tap here to enter text.

1. Click OK twice.
2. In Active Directory Users and Computers, make **Sales2** a member of the Administrators group. This is temporary for this lab.
3. Log off and log on the server as **Sales2**. In File Explorer, browse to the **TestShare1** folder. Double-click **TestBatch.bat** file. Read the error message.
4. **Insert a screenshot of the error message:**

Click or tap here to enter text.

1. Click OK.
2. Right-click the **TestBatch.bat** file and click **Edit**. Notice that you can still open this file because you have Read permission, but you can’t run the batch file because you no longer have Read & execute permission. Exit Notepad.
3. In File Explorer, right-click the right pane and point to **New**. Strangely, the right-click New menu and the Quick Access toolbar menu offer only Folder as an option. However, you can create a file in Notepad and save it in this folder.
4. Right-click Start, click Run, type notepad in the Open text box, and press Enter. Type your name in the file and click File, Save As from the menu. In the Save As dialog box, click This PC, scroll down, and double-click the **Data** folder and then the **TestShare1** folder. In the File name text box, type **Permfile2.txt**, and click Save. Exit Notepad.
5. Open the **Properties** dialog box for **Permfile2.txt**, Click the **Security** tab. Click **Sales2**. This user has been assigned Full control of the file because of the CREATOR OWNER Full control permission on the parent folder. Click **Advanced**. You see Sales2 next to Owner. Notice that you can change the owner if you click the Change link.
6. Disable permission inheritance and convert the existing permissions. Click OK until you get back to the Security tab of the Permfile2 file’s Properties dialog box.
7. Click Edit. Click Sales2, and then click Remove. Click the Users entry, and then click Remove. Only SYSTEM and Administrators are left in the DACL.
8. **Insert a screenshot:**

Click or tap here to enter text.

1. Click OK twice.
2. Double-click **Permfile2.txt**. You get an “Access is denied” message because you no longer have permission to open this file. Click OK and exit Notepad. Although you no longer have access to this file, you’re still the file owner and, therefore, can assign yourself permissions.
3. Open the **Properties** dialog box for **Permfile2.txt**, click the **Security** tab, then click **Edit**. Click **Add**. Type **Sales2**, click **Check Names**, and then click OK. Click **Full control** in the Allow column in the Permissions for Sales2 list box.
4. **Insert a** screenshot**:**

Click or tap here to enter text.

1. Click OK twice. Verify that you can open, change, and save Permfile2.txt.
2. In **Active Directory Users and Computers**, remove **Sales2** from the **Administrators** group.
3. Close all open windows and log off Server1.

# Activity 8-3: Setup and Configure Folder Permissions

Time Required: Approximately 15 minutes

Objective: Setup folders and configure permissions on a folder so that users can modify its contents.

Description: You will setup data storage folders on the server that will become file shares for the users, and eventually network drives for ease of access. You will configure NTFS and share permissions.

1. Logon to Server1 with your administrator account.
2. Open File Explorer (click its icon in the taskbar), if it is not already open. On the Data drive, create a Data folder. The local path will be c:\Data.
3. Right-click the new **Data** folder, click **Properties**, and then click the **Security** tab.
4. **What users and groups already have permissions to access the folder?**

Click or tap here to enter text.

1. **Insert a screenshot:**

Click or tap here to enter text.

1. Click each group and user to determine what permissions they have.
2. Click the Edit button. Click each group and user again, and notice that some boxes are checked and deactivated because they represent inherited permissions.
3. Close the window.
4. Create 5 new folders under c:\Data for each of your business units/OU’s. **Accounting**, **Administration**, **Operations**, **Research**, **Sales**.
5. Right Click on **Data**, Click **Properties**. Look at the default inherited permissions. This is fine for the root folder, we will change that for each of the other folders. Click Cancel.

You will follow these steps for each folder, with the appropriate security groups.

1. Right Click **Sales**, Click **Properties**, Click the **Security** Tab. Click **Advanced**.
2. Click **Disable inheritance**. Click **Convert inherited permissions into explicit permissions on this object**. Click OK.
3. In the **Security** Tab, Click **Edit**. Remove **Creator Owner** and **Users**. Leave **System** and **Administrators** alone.
4. Click **Add**. Type **DL\_Sales**. Click OK. Note that the default permission are Read & execute, List folder contents, and Read.
5. Set **Modify** permissions for **DL\_Sales**. Click OK to finish setting the local NTFS permissions.
6. Click the **Sharing** tab. Click **Advanced Sharing**.
7. **How can you change the name of the share?**

Click or tap here to enter text.

1. **How can you set the limit of users who can access the share at the same time?**

Click or tap here to enter text.

1. **How can you configure offline use?**

Click or tap here to enter text.

1. Select **Share this folder**. Click **Permissions**. Click **Full Control** for the **Everyone** group. Click OK. Click OK. Close the Sales Properties window.

Repeat the setup instructions for each of your business units. Only answer the questions for the first folder.

1. Right Click the Start button and Click Computer Management. Go to **Shared Folders**, then **Shares**.
2. **Insert a screenshot:**

Click or tap here to enter text.

1. Close Computer Management.
2. Client computers can now access the shared folder through the network, such as through the Network window in File Explorer.
3. Leave open File Explorer (the window with the folder containing the Utilities folder you have been working on) for the next activity, unless you need to stop working now.

# Activity 8-4: Manually Mapping a Drive

Time Required: 10 minutes

Objective: Map a drive letter to a shared folder.

Required Tools and Equipment: Server1 and Win11

Description: A user in the Sales Department accesses the Marketing share often but forgets how to use the UNC path. You decide to show this user several ways to map a drive letter to the share.

1. Start **Server1** and **Win11**. Log on to Win11 as **Sales1**.
2. Right-click Start, click Run, type **\\Server1**, and press Enter.
3. Right-click the **Sales** share and click **Map network drive** to open the Map Network Drive dialog box.
4. Click the **Drive** list arrow, and click **M:**. By default, the “Reconnect at sign-in” check box is selected, which is what you usually want in this situation. This option means the M drive always connects to this share when the user logs on. For this activity, click to clear the Reconnect at sign-in check box. You can also use a different username to access this share, if necessary.
5. Click Finish. A File Explorer window opens, showing the contents of the **Sales** share. Close this window.
6. In the File Explorer window that’s still open, click This PC. Notice that the M drive is listed under Network locations, below the “Devices and drives” section.
7. **Insert a screenshot:**

Click or tap here to enter text.

1. Right-click the M drive and click Disconnect to remove the drive mapping.
2. Sign out of Win11.
3. Log back into Win11 with **Sales 1**.
4. Open a command prompt window. Type **net use h: \\Server1\Sales** and press Enter. In File Explorer, verify that the drive has been mapped. The net use command is good to use in batch files for mapping drives.
5. **Insert a screenshot:**

Click or tap here to enter text.

1. At the command prompt, type **net use** and press Enter to see a list of mapped drives.
2. **Insert a screenshot:**

Click or tap here to enter text.

1. At the Command Prompt, type **net use h: /delete** and press Enter to disconnect the M drive again.
2. Close all open windows and log off Server1 and Win11.

# Activity 8-5: Map Drives with Logon Scripts

Time Required: 10 minutes

Objective: Map a drive letter to a shared folder with logon scripts.

Required Tools and Equipment: Server1

Description: Why map network drives one at a time, when you can automate the process for end users? A logon script is very commonly used to setup network drives for users. You can have many different logon scripts for different OU’s, filter by security groups, by users, or use Group Policy Preferences. The following lab will show three different ways to do logon scripts.

1. Logon to Server1.
2. Create a folder under **Data\Accounting** called **Payroll**.
3. Create a batch file named **logon.cmd** with the following commands.

**net use o: \\Server1\Accounting  
net use p: \\Server1\Accounting\Payroll**

### Logon Scripts by User in Active Directory

1. On Server1, go to **C:\Windows\SYSVOL\domain\scripts**. Copy **logon.cmd** to this folder.
2. In **Active Directory Users and Computers**, Right Click **Accounting1**, Click **Properties**.
3. Click the Profile tab. Under **Logon script** type: **logon.cmd**.
4. **Insert a screenshot of this tab:**

Click or tap here to enter text.

1. Click **OK**.
2. Logon to **Win11** with **Accounting1** and see if the drives get mapped. If it doesn’t work the first time, sign out and sign in again.
3. **Insert a screenshot of the drives that you mapped:**

Click or tap here to enter text.

1. Save a file to both drives named **Logon scripts per user**.
2. Remove the logon script from Accounting1’s Profile.
3. Disconnect the drives that were mapped.
4. Sign out of Win11 to make sure the drives are disconnected.

# Activity 8-6: Mapped Drive Logon Scripts by Group Policy

Time Required: 10 minutes

Group Policies disappear when they are unlinked.

1. Create a GPO called **Mapped Drives by GPO** and link it to the Accounting OU.
2. Go to **User Configuration 🡪 Policies 🡪 Windows Settings 🡪 Scripts**.
3. Double Click Logon. Click Add. Click Browse.
4. Copy and paste the **logon.cmd** file you created earlier into this dialog box.
5. Click logon.cmd and Click Open.
6. Click OK and complete editing the Group Policy.
7. **Insert a screenshot of the Group Policy Settings showing the logon script:**

Click or tap here to enter text.

1. Logon to **Win11** with Accounting1. Do a **gupdate**
2. Sign out and sign back into Win11. Your drives should be visible.
3. **Insert a screenshot of the drives that you mapped:**

Click or tap here to enter text.

1. Save a file to both drives named **Mapped Drives by GPO**.
2. Unlink the GPO.
3. **Logoff** and **logon** as Accounting1, the drives should be gone.
4. **Insert a screenshot of all the files on the server in in one of the mapped drives.**

Click or tap here to enter text.

1. Unlink **Mapped Drives by GPO** from the Accounting OU.

# Activity 8-7: Mapped Drives by Group Policy Preferences

Time Required: 10 minutes

Mapping drives by Group Policy Preferences allow you to set mapped drives for several users or groups all at once. The reason for preferences, is that some settings can’t be changed with Group Policies. Both types of policies are useful, you just need to be aware of the difference.

1. Create a GPO named **Mapped Drive Preferences** and link it to the **Accounting OU**.
2. Go to **User Configuration 🡪 Preferences 🡪 Windows Settings 🡪 Drive Maps**
3. Right Click **Drive Maps 🡪 New 🡪 Mapped Drive**.
   1. Location: **\\Server1\Accounting**
   2. Check **Reconnect**.
   3. Drive Letter **Existing 🡪 Z**
   4. Use the option on the common tab: **Remove this item when it is no longer applied**
   5. This will change the **Action** to **Replace**.
   6. Click OK.
4. Right Click **Drive Maps 🡪 New 🡪 Mapped Drive**.
   1. Location: **\\Server1\Accounting\Payroll**
   2. Check **Reconnect**.
   3. Drive Letter **Existing 🡪 Y**
   4. Use the option on the common tab: **Remove this item when it is no longer applied**
   5. This will change the **Action** to **Replace**.
   6. Click OK.
5. **Insert a screenshot of the Group Policy Settings showing the mapped drives.**

Click or tap here to enter text.

1. Logon to **Win11** with Accounting1. Do a **gupdate**
2. Sign out and sign back into Win11. Your drives should be visible.
3. Logon to **Win11** with **Accounting1** and see if the drives get mapped.
4. **Insert a screenshot of the drives that you mapped:**

Click or tap here to enter text.

1. Save a file to both drives named **Mapped Drives by GPO Preferences**.
2. Unlink Mapped Drive preferences.
3. **Logoff** and **logon** again as **Accounting1**, the drives should be gone. If they are not, do a **gpudate**
4. Unlink the GPO.

## Assignment Submissions

Attach this completed document to the assignment in Blackboard.