Module 10

Implementing File and Print Services

Module Overview

Accessing files and printers on the network is one of the most common activities in the Windows Server® environment. Reliable, secure access to files and folders and print resources is often the first requirement of a Windows Server 2012-based network. To provide access to file and print resources on your network, you must understand how to configure these resources within Windows Server 2012 server, and how to configure appropriate access to the resources for users in your environment.

This module discusses how to provide these important file and print resources with Windows Server 2012. It describes how to secure files and folders, how to protect previous versions of files and folders by using shadow copies, and how to give workers remote access to corporate files by implementing the new Work Folders role service. It also describes new network printing features that help manage the network printing environment.

Securing Files and Folders

The files and folders that your servers store typically contain your organization's business and functional data. Providing appropriate access to these files and folders, usually over the network, is an important part of managing file and print services in Windows Server 2012.

This lesson gives you information necessary to secure files and folders on your Windows Server 2012 servers, so that your organization's data is available yet protected.

What Are NTFS Permissions?

NTFS permissions are assigned to files or folders on a storage volume that is formatted with NTFS. The permissions that you assign to NTFS files and folders govern user access to these files and folders.

The following points describe the key aspects of NTFS permissions:

- NTFS permissions control access for files and folders on NTFS-formatted storage volumes
- NTFS Permissions:
  - Are configured for files or folders
  - Can be granted or denied
  - Are inherited from parent folders
- Permissions conflict precedence:
  1. Explicitly assigned Deny
  2. Explicitly assigned Allow
  3. Inherited Deny
  4. Inherited Allow

- NTFS permissions can be configured for an individual file or folder, or sets of files or folders.
- NTFS permissions can be assigned individually to objects that include users, groups, and computers.
- NTFS permissions are controlled by granting or denying specific types of NTFS file and folder access, such as Read or Write.
- NTFS permissions can be inherited from parent folders. By default, the NTFS permissions that are assigned to a folder are also assigned to newly created folders or files within that parent folder.

NTFS Permission Types

There are two assignable NTFS permissions types: standard, and advanced.

Standard Permissions

Standard permissions provide the most commonly used permission settings for files and folders. You assign standard permissions in the Permissions for *folder name* dialog box.

The following table details the standard permissions options for NTFS files and folders.

File permissions	Description
Full Control	Grants the user complete control of the file or folder, including control of permissions.
Modify	Grants the user permission to read, write, or delete a file or folder, including creating a file or folder. It also grants permission to execute files.
Read and Execute	Grants the user permission to read a file and start apps.
Read	Grants the user permission to view file or folder content.
Write	Grants the user permission to write to a file.
List folder contents (folders only)	Grants the user permission to view a list of the folder's contents.

Note: Granting users Full Control permissions on a file or a folder gives them the ability to perform any file system operation on the object, and the ability to change permissions on the object. They can also remove permissions on the resource for any or all users, including you.

Advanced Permissions

Advanced permissions can provide a much greater level of control over NTFS files and folders. Advanced permissions are accessible by clicking the **Advanced** button from the **Security** tab of a file or folder's **Properties** dialog box.

The following table details the Advanced permissions for NTFS files and folders.

File permissions	Description
Traverse Folder/Execute File	The Traverse Folder permission applies only to folders. This permission grants or denies users the right to browse through folders to reach other files or folders, even if the user has no permissions for the traversed folders. The Traverse Folder permission takes effect only when the group or user is not granted the Bypass Traverse Checking user right. By default, the Everyone group is given the Bypass Traverse Checking user right. The Execute File permission grants or denies access to run program files. If you set the Traverse Folder permission on a folder, the Execute File permission is not automatically set on all files in that folder.
List Folder/Read Data	The List Folder permission grants the user permission to view file names and subfolder names. This permission applies only to folders and affects only the contents of that folder—it does not affect whether the folder itself is listed. In addition, this setting has no effect on viewing the file structure from a command-line interface. The Read Data permission grants or denies the user permission to view data in files. The Read Data permission applies only to files.

Read Attributes	The Read Attributes permission grants the user permission to view the basic attributes of a file or a folder such as Read-only and Hidden attributes. Attributes are defined by NTFS.

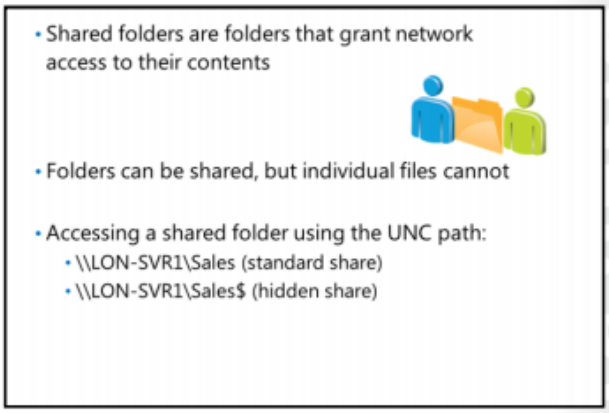
File permissions	Description
Read Extended Attributes	The Read Extended Attributes permission grants the user permission to view the extended attributes of a file or folder. Extended attributes are defined by apps, and can vary by app.
Create Files/Write Data	The Create Files permission applies only to folders, and grants the user permission to create files in the folder. The Write Data permission grants the user permission to make changes to the file and overwrite existing content by NTFS. The Write Data permission applies only to files.
Create Folders /Append Data	The Create Folders permission grants the user permission to create folders within the folder. The Create Folders permission applies only to folders. The Append Data permission grants the user permission to make changes to the end of the file, but not to delete or overwrite existing data. The Append Data permission applies only to files.
Write Attributes	The Write Attributes permission grants the user permission to change the basic attributes of a file or folder, such as Read-only or Hidden. Attributes are defined by NTFS. The Write Attributes permission does not imply that you can create or delete files or folders; it includes only the permission to make changes to the attributes of a file or folder. To grant Create or Delete permissions, see the Create Files/Write Data, Create Folders/Append Data, Delete Subfolders and Files, and Delete entries in this table.

Write Extended Attributes	The Write Extended Attributes permission grants the user permission to change the extended attributes of a file or folder. Extended attributes are defined by programs and apps, and can vary by each one. The Write Extended Attributes permission does not imply that the user can create or delete files or folders; it includes only the permission to make changes to the attributes of a file or folder. To grant Create or Delete permissions, see the Create Files/Write Data, Create Folders/Append Data, Delete Subfolders and Files, and Delete entries in this table.
Delete Subfolders and Files	The Delete Subfolders and Files permission grants the user permission to delete subfolders and files, even if the Delete permission is not granted on the subfolder or file. The Delete Subfolders and Files permission applies only to folders.
Delete	The Delete permission grants the user permission to delete the file or folder. If you have not been assigned Delete permission on a file or folder, you can still delete the file or folder if you are granted Delete Subfolders and Files permissions on the parent folder.
Read Permissions	Read Permissions grants the user permission to read permissions about the file or folder, such as Full Control, Read, and Write.
Change Permissions	Change Permissions grants the user permission to change permissions on the file or folder, such as Full Control, Read, and Write.

File permissions	Description
Take Ownership	The Take Ownership permission grants the user permission to take ownership of the file or folder. The owner of a file or folder can change permissions on it, regardless of any existing permissions that protect the file or folder.
Synchronize	The Synchronize permission assigns different threads to wait on the handle for the file or folder, and then synchronize with another thread that may signal it. This permission applies only to multiple-threaded, multiple-process programs and apps.

What Are Shared Folders?

Shared folders are a key component to granting access to files on your server from the network. When you share a folder, the folder and all of its contents are made available to multiple users simultaneously over the network. Shared folders maintain a separate set of permissions from the NTFS permissions, which apply to the folder's contents. These permissions provide an extra level of security for files and folders that are made available on the network.



Most organizations deploy dedicated file servers to host shared folders. You can store files in shared folders according to categories or functions. For example, you can put shared files for the Sales department in one shared folder, and shared files for the Marketing department in another.

Note: The sharing process applies only to the folder level. You cannot share an individual file or a group of files.

Administrative Shares

If you have shared folders that need to be available from the network, but should be hidden from users browsing the network, you can create administrative (or hidden) shared folders. You can access an administrative shared folder by typing in its UNC path, but the folder will not be visible if you browse the server by using File Explorer. Administrative shared folders also typically have a more restrictive set of permissions to reflect the administrative nature of the folder's contents.

To hide a shared folder, append the dollar symbol ($) to the folder's name. For example, a shared folder on LON-SVR1 named Sales can be made into a hidden shared folder by naming it Sales$. The shared folder is accessible over the network by using the UNC path \\LON-SVR1\Sales$.

Note: Shared folder permissions apply only to users who access the folder over the network. They do not affect users who access the folder locally on the computer where the folder is stored.

Shared Folder Permissions

Just like NTFS permissions, you can assign shared folder permissions to users, groups, or computers. However, unlike NTFS permissions, shared folder permissions are not configurable for individual files or folders within the shared folder. Shared folder permissions are set once for the shared folder itself, and apply universally to the entire contents of the shared folder for users who access the folder over the network.

When you create a shared folder, the default assigned shared permission for the Everyone group is set to Read.

The following table lists the permissions that you can grant to a shared folder.

Shared folder permission	Description
Read	Users can view folder and file names, view file data and attributes, run program files and scripts, and navigate the folder structure within the shared folder.
Change	Users can create folders, add files to folders, change data in files, append data to files, change file attributes, delete folders and files, and perform all tasks permitted by the Read permission.
Full Control	Users can change file permissions, take ownership of files, and perform all tasks permitted by the Change permission.

Note: When you assign Full Control permissions on a shared folder to a user, that user can modify permissions on the shared folder, which includes removing all users (including administrators), from the shared folder's permissions list. In most cases, you should grant Change Permission instead of Full Control permission.

Permissions Inheritance

By default, NTFS and shared folders use inheritance to propagate permissions throughout a folder structure. When you create a file or a folder, it is automatically assigned the permissions that are set on any folders that exist above it (parent folders) in the hierarchy of the folder structure.

- Inheritance is used to manage access to resources without assigning explicit permissions to each object
- By default, permissions are inherited in a parent/child relationship
- Blocking inheritance:
  - You can block permission inheritance
  - You can apply blocking at the file or folder level
  - You can set blocking on a folder to propagate the new permissions to child objects

How Inheritance Is Applied

Consider the following example. Adam Carter is a member of the Marketing group and the New York Editors group. The following table is a summary of the permissions for this example:

Folder or File	Assigned Permissions	Adam's Permissions
Marketing (folder)	Read – Marketing	Read
Marketing Pictures (folder)	None set	Read (inherited)
New York (folder)	Write – New York Editors	Read(i) + Write
Fall_Composite.jpg (file)	None set	Read(i) + Write(i)

In this example, Adam is a member of two groups that are assigned permissions for files or folders within the folder structure. They are as follows:

- The top-level folder, Marketing, has an assigned permission for the Marketing Group giving them Read access.
- In the next level, the Marketing Pictures folder has no explicit permissions set, but because of permissions inheritance Adam has Read access to this folder and its contents from the permissions that are set on the Marketing folder.
- In the third level, the New York folder has Write permissions assigned to one of Adam's groups—New York Editors. In addition to this explicitly assigned Write permission, the New York folder also inherits the Read permission from the Marketing folder. These permissions pass down to file and folder objects, cumulating with any explicit Read and Write permissions set on those files.
- The fourth and last level is the Fall_Composite.jpg file. Even though no explicit permissions have been set for this file, Adam has both Read and Write access to the file due to the inherited permissions from both the Marketing folder and the New York folder.

Permission Conflicts

Sometimes, explicitly set permissions on a file or folder conflict with permissions inherited from a parent folder. In these cases, the explicitly assigned permissions always override the inherited permissions. In the given example, if Adam Carter was denied Write access to the parent Marketing folder, but then explicitly granted Write access to the New York folder, the granted Write access permissions take precedence over the inherited deny Write access permission.

Blocking Inheritance

You can also disable the inheritance behavior for a file or a folder (and its contents) on an NTFS drive. You do this when you want to explicitly define permissions for a set of objects without including any of the inherited permissions from any parent folders. Windows Server 2012 provides an option for blocking inheritance on a file or a folder. To block inheritance on a file or folder, complete the following steps:

1. Right-click the file or folder where you want to block inheritance, and then click **Properties**.
2. In the **Properties** dialog box, click the **Security** tab, and then click **Advanced**.
3. In the **Advanced Security Settings** dialog box, click **Change Permissions**.
4. In the next **Advanced Security Settings** dialog box, click **Disable inheritance**.
5. At this point, you are prompted to either convert the inherited permissions into explicit permissions or remove all inherited permissions from the object to start with a blank permissions slate.

Resetting Default Inheritance Behavior

After you block inheritance, changes made to permissions on the parent folder structure no longer have an effect on the permissions for the child object (and its contents) that has blocked inheritance, unless you reset that behavior from one of the parent folders by selecting the Replace All Child Objects With Inheritable Permissions From This Object option. When you select this option, the existing set of permissions on the current folder are propagated down to all child objects in the tree structure, and override all explicitly assigned permissions for those files and folders. This check box is located directly under the Include Inheritable Permissions From This Object's Parent check box.

Effective Permissions

Access to a file or folder in Windows Server 2012 is granted based on a combination of permissions. When a user attempts to access a file or folder, the permission that applies is dependent on various factors, including:

- Explicitly defined and inherited permissions that apply to the user
- Explicitly defined and inherited permissions that apply to the groups to which the user belongs
- How the user is accessing the file or folders: locally, or over the network

- When combining shared folder and NTFS permissions, the most restrictive permission is applied
  - Example: If a user or group is given the shared folder permission of Read and the NTFS permission of Write, the user or group will only be able to read the file because it is the more restrictive permission
- Both the share and the NTFS file and folder permissions must have the correct permissions, otherwise the user or group will be denied access to the resource

Effective NTFS permissions are the cumulative permissions that are assigned to a user for a file of folder based on the factors listed above. The following principles determine effective NTFS permissions:

- Cumulative permissions are the combination of the highest NTFS permissions granted to the user and to all the groups of which the user is a member. For example, if a user is a member of a group that has Read permission and is a member of a group that has Modify permission, the user is assigned cumulative Modify permissions.

- Deny permissions override equivalent Allow permissions. However, an explicit Allow permission can override an inherited Deny permission. For example, if a user is denied Write access to a folder via an inherited Deny permission, but is explicitly granted Write access to a subfolder or a particular file, the explicit Allow overrides the inherited Deny for the particular subfolder or file.
- You can apply permissions to a user or to a group. Assigning permissions to groups is preferred because they are more efficient than managing permissions that are set for many individuals.

- NTFS file permissions take priority over folder permissions. For example, if a user has Read permission to a folder, but has been granted Modify permission to certain files in that folder, the effective permission for those files will be set to Modify.
- Every object in an NTFS drive or in Active Directory® Domain Services (AD DS) is owned. The owner controls how permissions are set on the object and to whom permissions are granted. For example, a user who creates a file in a folder where they have Modify permissions can change the permissions on the file to Full Control.

Effective Access Tool

Windows Server 2012 provides an Effective Access tool that shows the effective NTFS permissions on a file or folder for a user, based on permissions assigned to the user account and groups to which the user account belongs. You can access Effective Access tool by the following steps:

1. Right-click the file or folder for which you want to analyze permissions, and then click **Properties**.
2. In the **Properties** dialog box, click the **Advanced** button.
3. In the **Advanced Security Settings** dialog box, click the **Effective Access** tab.
4. Choose a user or group to evaluate by using **Select a user**.

Combining NTFS Permissions and Shared Folder Permissions

NTFS permissions and shared folder permissions work together to control access to file and folder resources that are accessed from a network. When you configure access to network resources on an NTFS drive, use the most restrictive NTFS permissions to control access to folders and files, and combine them with the most restrictive shared folder permissions to control access to the network.

How Combining NTFS and Shared Folder Permissions Works

When you apply both NTFS and shared folder permissions, remember that the more restrictive of the two permissions dictates the access that a user will have to a file or folder. The following two examples explain this further:

- If you set the NTFS permissions on a folder to Full Control, but you set the shared folder permissions to Read, then that user has only Read permission when accessing the folder over the network. Access is restricted at the shared folder level, and any greater access at the NTFS permissions level does not apply.
- Likewise, if you set the shared folder permission to Full Control, and you set the NTFS permissions to Write, then the user will have no restrictions at the shared folder level, but the NTFS permissions on the folder grants only Write permissions to that folder.

The user must have appropriate permissions on both the NTFS file or folder and the shared folder. If no permissions exist for the user (either as an individual or as the member of a group) on either resource, access is denied.

Considerations for Combined NTFS and Shared Folder Permissions

The following are several considerations that make administering permissions more manageable:

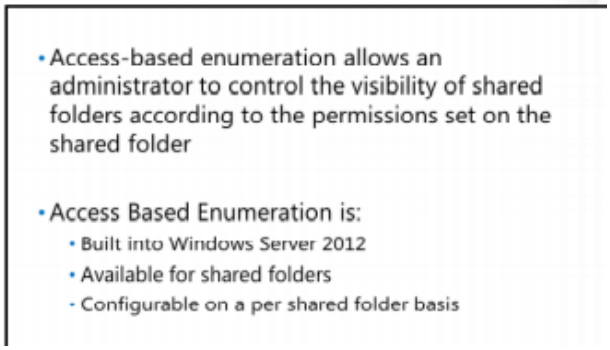
- Grant permissions to groups instead of users. Groups can always have individuals added or deleted, while permissions on a case-by-case basis are difficult to track and cumbersome to manage.
- Use Deny permissions only when necessary. Because Deny permissions are inherited, assigning deny permissions to a folder can result in users not being able to access files further down in the folder structure tree. You should assign Deny permissions only in the following situations:
    - To exclude a subset of a group that has Allow permissions

- To exclude one specific permission when you have granted Full Control permissions to a user or a group

- Never deny the Everyone group access to an object. If you deny the Everyone group access to an object, you deny Administrators access—including yourself. Instead, remove the Everyone group from the permissions list, as long as you grant permissions for the object to other users, groups, or computers.
- Grant permissions to an object that is as high in the folder structure as possible, so that the security settings are propagated throughout the tree. For example, instead of bringing groups representing all departments of the company together into a Read folder, assign Domain Users (which is a default group for all user accounts on the domain) to the share. In this manner, you eliminate the need to update department groups before new users receive the shared folder.
- Use NTFS permissions instead of shared permissions for fine-grained access. Configuring both NTFS and shared folder permissions can be difficult. Consider assigning the most restrictive permissions for a group that contains many users at the shared folder level, and then use NTFS permissions to assign permissions that are more specific.

What Is Access-Based Enumeration?

With access-based enumeration, users see only the files and folders which they have permission to access. Access-based enumeration provides a better user experience because it displays a less complex view of the contents of a shared folder, making it easier for users to find the files that they need. Windows Server 2012 allows access-based enumeration of folders that a server shares over the network.



Enabling Access-Based Enumeration

To enable access-based enumeration for a shared folder:

1. Open Server Manager.
2. In the navigation pane, click **File and Storage Services**.
3. In the navigation pane, click **Shares**.
4. In the Shares pane, right-click the shared folder for which you want to enable access-based enumeration, and then click **Properties**.
5. In the **Properties** dialog box, click **Settings**, and then select **Enable access-based enumeration**.

When **Enable access-based enumeration** is selected, access-based enumeration is enabled on the shared folder. This setting is unique to each shared folder on the server.

Note: The File and Storage Services console is the only place in the Windows Server 2012 interface where you can configure access-based enumeration for a shared folder. Access-based enumeration is not available in any of the properties dialog boxes that are accessible by right-clicking the shared folder in File Explorer.

What Are Offline Files?

An *offline file* is a copy of a network file that is stored on a client computer. By using offline files, users can access network-based files when their client computer is disconnected from the network.

If offline files and folders have been edited or modified by the client, then the changes are synchronized with the network copy of the files the next time the client reconnects to the network. The synchronization schedule and behavior of offline files is controlled by the Windows client operating system.

Offline file settings allow a client computer to cache network files locally for offline use when they are disconnected from the network

Offline settings window

Module 10

Lab: Implementing File and Print Services

Exercise 1: Creating and Configuring a File Share

▶ Task 1: Create the folder structure for the new share

1. On LON-SVR1, on the taskbar, click the **File Explorer** icon.
2. In File Explorer, in the navigation pane, expand **This PC**, and then click **Allfiles (E:)**.
3. On the menu toolbar, click **Home**, click **New folder**, type **Data**, and then press Enter.
4. Double-click the **Data** folder.
5. On the menu toolbar, click **Home**, click **New folder**, type **Development**, and then press Enter.
6. Repeat step 5 for the following new folder names:
   - **Marketing**
   - **Research**
   - **Sales**

▶ Task 2: Configure NTFS permissions on the folder structure

1. In File Explorer, navigate to drive E, right-click the **Data** folder, and then click **Properties**.
2. In the **Data Properties** dialog box, click **Security**, and then click **Advanced**.
3. In the **Advanced Security Settings for Data** dialog box, click **Disable Inheritance**.
4. In the **Block Inheritance** dialog box, click **Convert inherited permissions into explicit permissions on this object**.
5. Click **OK** to close the **Advanced Security Settings for Data** dialog box.
6. Click **OK** to close the **Data Properties** dialog box.
7. In File Explorer, double-click the **Data** folder.
8. Right-click the **Development** folder, and then click **Properties**.
9. In the **Development Properties** dialog box, click **Security**, and then click **Advanced**.
10. In the **Advanced Security Settings for Development** dialog box, click **Disable Inheritance**.
11. In the **Block Inheritance** dialog box, click **Convert inherited permissions into explicit permissions on this object**.
12. Remove the two permissions entries for Users (LON-SVR1\Users), and then click **OK**.

13. On the **Security** tab, click **Edit**.
14. In the **Permissions for Development** dialog box, click **Add**.
15. Type **Development**, click **Check names**, and then click **OK**.
16. In the **Permissions for Development** dialog box, under **Allow**, select **Modify** permission.
17. Click **OK** to close the **Permissions for Development** dialog box.
18. Click **OK** to close the **Development Properties** dialog box.
19. Repeat steps 8 through 18 for the **Marketing**, **Research**, and **Sales** folders, assigning Modify permissions to the **Marketing**, **Research**, and **Sales** groups for their respective folders.

▶ Task 3: Create the shared folder

1. In File Explorer, navigate to drive E, right-click the **Data** folder, and then click **Properties**.
2. In the **Data Properties** dialog box, click the **Sharing** tab, and then click **Advanced Sharing**.
3. In the **Advanced Sharing** dialog box, select **Share this folder**, and then click **Permissions**.
4. In the **Permissions for Data** dialog box, click **Add**.
5. Type **Authenticated Users**, click **Check names**, and then click **OK**.
6. In the **Permissions for Data** dialog box, click **Authenticated Users**, and then under **Allow**, select **Change** permission.
7. Click **OK** to close the **Permissions for Data** dialog box.
8. Click **OK** to close the **Advanced Sharing** dialog box.
9. Click **Close** to close the **Data Properties** dialog box.

▶ Task 4: Test access to the shared folder

1. Sign in to LON-CL1 as **Adatum\Bernard** with the password **Pa$$w0rd**.

Note: Bernard is a member of the Development group.

2. On the Start screen, click **Desktop**.
3. On the taskbar, click the **File Explorer** icon.
4. In File Explorer, in the address bar, type **\\LON-SVR1\Data**, and then press Enter.
5. Double-click the **Development** folder.

Note: Bernard should have access to the Development folder.

6. Attempt to access the **Marketing**, **Research**, and **Sales** folders.

   NTFS permissions on these folders prevents you from doing this.

Note: Bernard can still see the other folders, even though he does not have access to their contents.

7. Sign out of LON-CL1.

▶ Task 5: Enable access-based enumeration

1. Switch to LON-SVR1.
2. On the taskbar, click the **Server Manager** icon.
3. In Server Manager, in the navigation pane, click **File and Storage Services**.
4. In the File and Storage Services window, in the navigation pane, click **Shares**.
5. In the **Shares** pane, right-click **Data**, and then click **Properties**.
6. In the **Data Properties** dialog box, click **Settings**, and then select **Enable access-based enumeration**.

7. Click **OK** to close the **Data Properties** dialog box.
8. Close Server Manager.

▶ Task 6: Test access to the share

1. Sign in to LON-CL1 as **Adatum\Bernard** with the password **Pa$$w0rd**.
2. Click the **Desktop** tile.
3. On the taskbar, click the **File Explorer** icon.
4. In File Explorer, in the address bar, type **\\LON-SVR1\Data**, and then press Enter.

Note: Bernard can now view only the Development folder, the folder for which he has been assigned permissions.

5. Double-click the **Development** folder.

Note: Bernard should have access to the Development folder.

6. Sign out of LON-CL1.

▶ Task 7: Disable Offline Files for the share

1. Switch to LON-SVR1.
2. On the taskbar, click the **File Explorer** icon.
3. In File Explorer, navigate to drive E, right-click the **Data** folder, and then click **Properties**.
4. In the **Data Properties** dialog box, click the **Sharing** tab, click **Advanced Sharing**, and then click **Caching**.
5. In the **Offline Settings** dialog box, click **No files or programs from the shared folder are available offline**, and then click **OK**.
6. Click **OK** to close the **Advanced Sharing** dialog box.
7. Click **Close** to close the **Data Properties** dialog box.

Results: After completing this exercise, you will have created a new shared folder for use by multiple departments.

Shadow Copy (also known as Volume Snapshot Service, Volume **Shadow Copy** Service or **VSS**) is a technology included in **Microsoft Windows** that can create backup **copies** or snapshots of computer files or volumes, even when they are in use.

Exercise 2: Configuring Shadow Copies

▶ Task 1: Configure shadow copies for the file share

1. On LON-SVR1.
2. Open File Explorer.
3. Navigate to drive E, right-click **Allfiles (E:)**, and then click **Configure Shadow Copies**.
4. In the **Shadow Copies** dialog box, click drive **E**, and then click **Enable**.
5. In the **Enable Shadow Copies** dialog box, click **Yes**.
6. In the drive **Shadow Copies** dialog box, click **Settings**.

7. In the **Settings** dialog box, click **Schedule**.

   This opens the drive **E:** dialog box.
8. In drive **E:** dialog box, change Schedule Task to **Daily**, change Start time to **12:00 AM** and then click **Advanced**.
9. In the **Advanced Schedule Options** dialog box, select **Repeat task**, and then set the frequency to **every 1 hours**.
10. Select **Time**, and change the time value to **11:59 PM**.
11. Click **OK** twice.
12. Click **OK** to close the **Settings** dialog box.
13. Leave the drive **Shadow Copies** dialog box open.

▶ Task 2: Create multiple shadow copies of a file

1. On LON-SVR1, open File Explorer.
2. Navigate to **E:\Data\Development**.
3. On the menu toolbar, click **Home**, click **New item**, and then click **Text Document**.
4. Type **Report**, and then press Enter.
5. Switch back to the **Shadow Copies** dialog box; it should still be opened on the **Shadow Copies** tab.
6. Click **Create Now**.

▶ Task 3: Recover a deleted file from a shadow copy

1. On LON-SVR1, switch back to File Explorer.
2. Right-click **Report.txt**, and then click **Delete**.
3. In File Explorer, right-click the **Development** folder, and then click **Properties**.
4. In the **Development Properties** dialog box, click the **Previous Versions** tab.
5. Click the most recent folder version for **Development**, and then click **Open**.
6. Confirm that Report.txt is in the folder, right-click **Report.txt**, and then click **Copy**.
7. Close the File Explorer window that just opened.
8. In the other File Explorer window, right-click the **Development** folder, and then click **Paste**.
9. Close File Explorer.
10. Click **OK** and close all open windows.

Results: After completing this exercise, you will have enabled shadow copies on the file server.

Work Folders is a feature in **Windows** that enables you to access your **work** files from your personal computer or device. With **Work Folders**, you can keep copies of your **work** files on your personal devices and have them automatically synchronized to your company's datacenter.

Exercise 3: Enabling and Configuring Work Folders

▶ Task 1: Install the Work Folders role service

1. On LON-SVR1, on the taskbar, click the **Windows PowerShell®** icon.
2. At the command prompt type the following command and press Enter:

   Add-WindowsFeature FS-SyncShareService

   Note that the name of the feature is case-sensitive.

▶ Task 2: Create a Sync Share on the File Server

1. On LON-SVR1, in the Windows PowerShell command window type the following command and press Enter:

   New-SyncShare Corp –path C:\CorpData –User "Adatum\Domain Users"

2. If required, on the taskbar, click the **Server Manager** icon to open Server Manager.
3. Click **File and Storage Services**.
4. Click **Work Folders** and ensure the Corp sync share exists.

▶ Task 3: Automate settings for users via Group Policy

1. On LON-DC1, in Server Manager, click **Tools** and click **Group Policy Management**.
2. In the **Group Policy Management Console**, go to **Forest:Adatum.com\Domains\Adatum.com**.
3. Right-click **Adatum.com** and click **Create a GPO in this domain, and Link it here**.
4. In the **New GPO** dialog box, in **Name**, type **Work Folders**, and then click **OK**.
5. Right-click the **Work Folders** GPO and then click **Edit**.
6. In the Group Policy Management Editor window, go to **User Configuration\Policies \Administrative Templates\Windows Components\Work Folders**.
7. In the details pane, double-click **Specify Work Folders settings**.
8. Click **Enabled** and, in **Work Folders URL**, type **http://lon-svr1.Adatum.com**.
9. Select **Force automatic setup** and click **OK**.
10. Close all open windows.

▶ Task 4: Test synchronization

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
2. On the Start screen, click **Desktop**.
3. On the taskbar, click the **File Explorer** icon.
4. Navigate to **C:\Labfiles\Mod10** and double-click **WorkFolders.bat**.

   This adds a registry entry to allow unsecured connections to the work folders.
5. In the lower-left corner of the screen, click the **Start** button.
6. Sign out of LON-CL1.
7. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa$$w0rd**.
8. Click the **Desktop** tile and click **File Explorer**.
9. Double-click the **Work Folders** folder.
10. In the Work Folders folder, right-click an empty space, point to **New**, and then click **Text Document**.
11. Name the new text document **TestFile2**, and then press Enter.
12. Switch to LON-SVR1 and click **File Explorer**.
13. Navigate to **C:\CorpData\Administrator**. Ensure the new text file named TestFile2 exists.
14. Close all open Windows.

Results: After completing this exercise, you will have installed the Work Folders role service, created a sync share, and created a Group Policy Object to deliver the settings to the users automatically. You will have also tested the settings.

Exercise 4: Creating and Configuring a Printer Pool

▶ Task 1: Install the Print and Document Services server role

1. On LON-SVR1, on the taskbar, click the **Server Manager** icon.
2. In Server Manager, on the menu toolbar, click **Manage**.
3. Click **Add Roles and Features**, click **Next**.
4. Click **Role-based or feature-based Installation**, click **Next**.
5. On the **Select destination server** page, click the server on which you want to install the Print and Document Services, and then click **Next**.

   The default server is the local server.
6. On the **Select Server Roles** page, select **Print and Document Services**.
7. In the Add Roles and Features Wizard, click **Add Features**.
8. On the **Select server roles** page, click **Next**.
9. On the **Select Features** page, click **Next**.
10. On the **Print and Document Services** page, review the Notes for the administrator, and then click **Next**.
11. On the **Select Role Services** page, click **Next** until the **Confirm Installation Selections** page displays.
12. Click **Install** to install the required role services.
13. Click **Close**.

▶ Task 2: Install a printer

1. On LON-SVR1, in the Server Manager, click **Tools**, and then click **Print Management**.
2. Expand **Printer Servers**, expand **LON-SVR1**, right-click **Printers**, and then click **Add Printer**.

   The Network Printer Installation Wizard starts.
3. On the **Network Printer Installation Wizard** page, click **Add a TCP/IP or Web Services Printer by IP address or hostname**, and then click **Next**.
4. Change the Type of Device to **TCP/IP Device**.
5. In **Host name or IP address**, type **172.16.0.200**, clear **Auto detect the printer driver to use**, and then click **Next**.
6. Under Device Type, click **Generic Network Card**, and then click **Next**.
7. Click **Install a new driver**, and then click **Next**.
8. Click **Microsoft** as the Manufacturer, under Printers, click **Microsoft XPS Class Driver**, and then click **Next**.

9. Change the Printer Name to **Branch Office Printer**, and then click **Next**.
10. Click **Next** two times to accept the default printer name and share name, and to install the printer.
11. Click **Finish** to close the Network Printer Installation Wizard.
12. In the Print Management console, right-click the **Branch Office Printer**, and then click **Enable Branch Office Direct Printing**.
13. In the Print Management console, right-click the **Branch Office Printer**, and then select **Properties**.
14. Click the **Sharing** tab, select **List in the directory**, and then click **OK**.

▶ Task 3: Configure printer pooling

1. In the Print Management console, under **LON-SVR1**, right-click **Ports**, and then click **Add Port**.
2. In the **Printer Ports** dialog box, click **Standard TCP/IP Port**, and then click **New Port**.
3. In the Add Standard TCP/IP Printer Port Wizard, click **Next**.
4. In **Printer Name or IP Address**, type **172.16.0.201**, and then click **Next**.
5. In the **Additional port information required** dialog box, click **Next**.
6. Click **Finish** to close the Add Standard TCP/IP Printer Port Wizard.
7. Click **Close** to close the **Printer Ports** dialog box.
8. In the Print Management console, click **Printers**, right-click **Branch Office Printer**, and then click **Properties**.
9. In the **Branch Office Printer Properties** dialog page, click the **Ports** tab, select **Enable printer pooling**, and then click the **172.16.0.201** port to select it as the second port.
10. Click **OK** to close the **Branch Office Printer Properties** dialog box.
11. Close the Print Management Console.

▶ Task 4: Install a printer on a client computer

1. On LON-CL1, in the lower-left corner of the screen, right-click the **Start** button, and click **Control Panel**.
2. In Control Panel, under **Hardware and Sound**, click **Add a device**.
3. In the **Add a device** dialog box, click **Branch Office Printer on LON-SVR1**, and then click **Next**. The device installs automatically.

Results: After completing this exercise, you will have installed the Print and Document Services server role and installed a printer with printer pooling.

▶ Prepare for the next module

After you finish the lab, revert the virtual machines back to their initial state.

To do this, complete the following steps.

1. On the host computer, start Hyper-V® Manager.
2. In the **Virtual Machines** list, right-click **20410C-LON-SVR1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410C-LON-CL1** and **20410C-LON-DC1**.