



# Server Configuration

## Lab04

### Configure File and Share Access

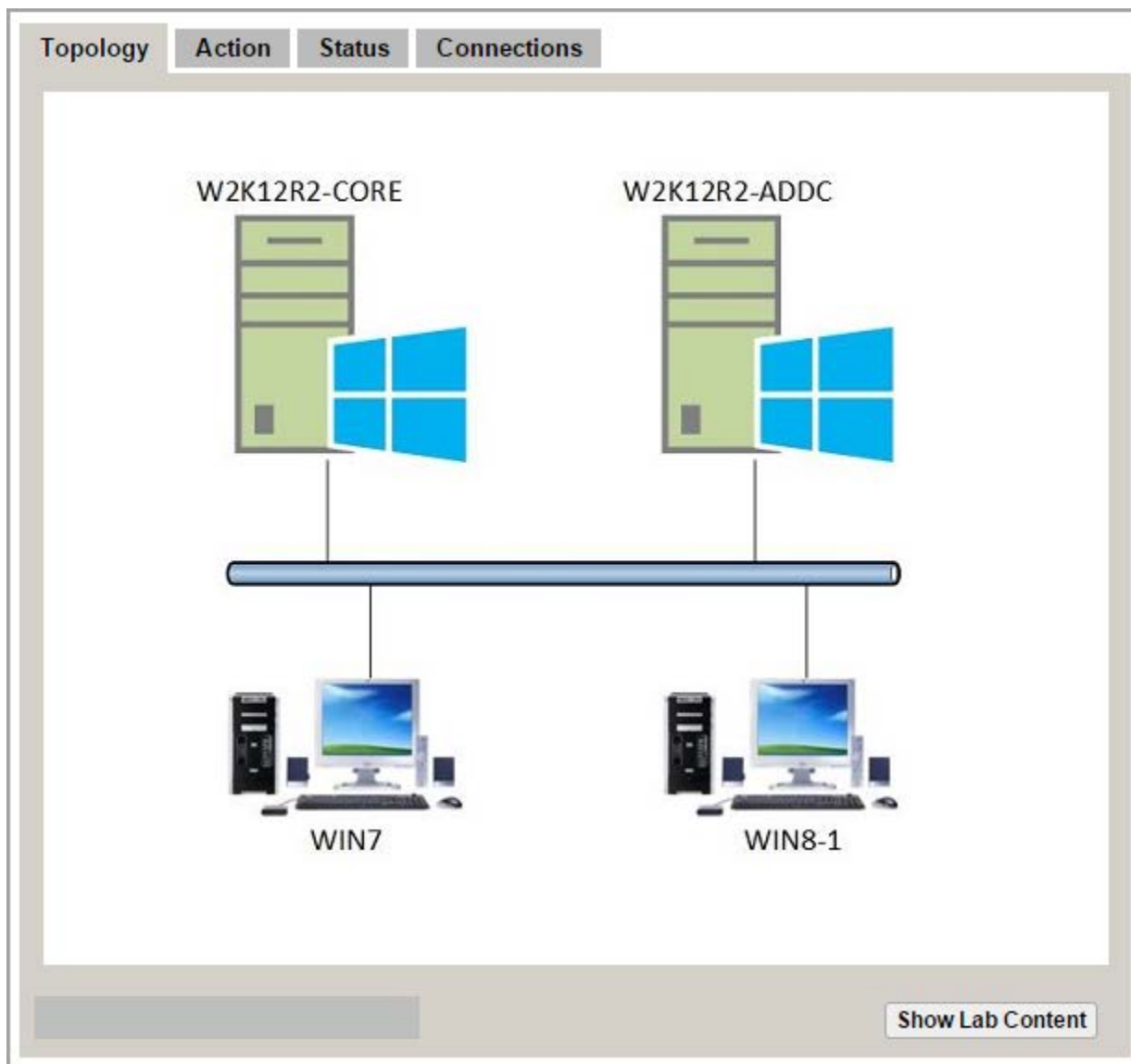


## Contents

Topology .....	3
1 Shares.....	4
1.1 Creating Shares .....	4
1.2 NTFS Quotas.....	21
2 Volume Shadow Copy Services (VSS).....	24
2.1 Enable VSS.....	24
3 Work Folders.....	32
3.1 Install Work Folders Role .....	32
4 Research Topics (Optional) .....	49
References .....	49



## Topology

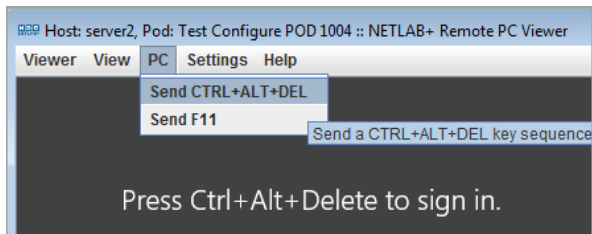


## 1 Shares

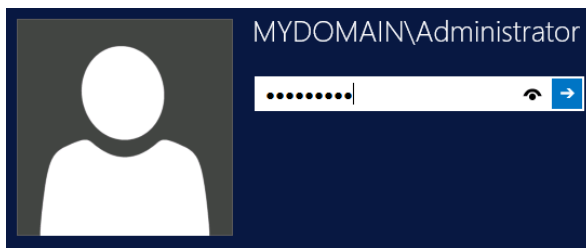
Shares provide centralized management as well as higher data security and protection.

### 1.1 Creating Shares

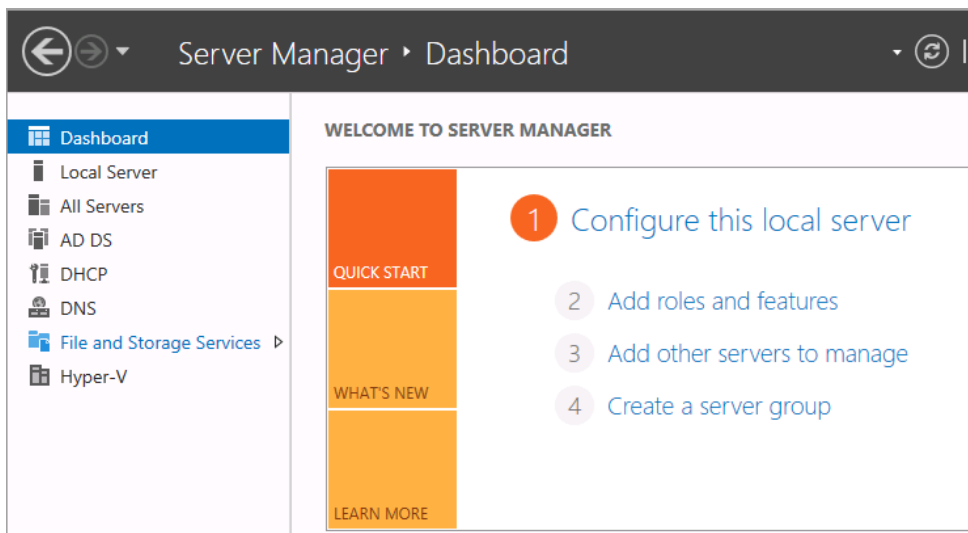
1. Open the Windows W2K12R2-ADDC server by clicking the icon in the topology. Click “PC > Send CTRL+ALT+DEL”.



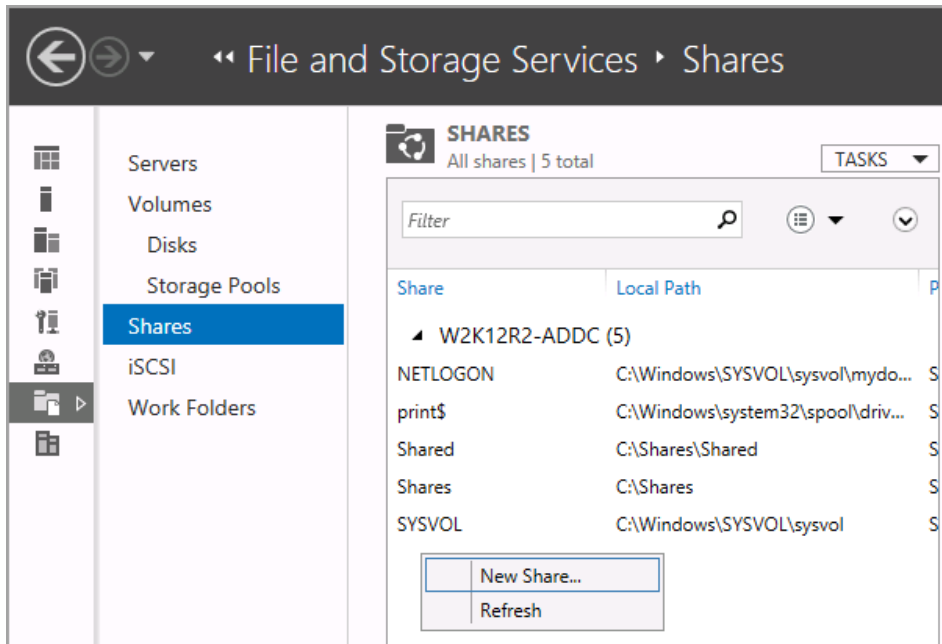
2. Type **P@ssw0rd1** as the administrator password and hit “Enter”.



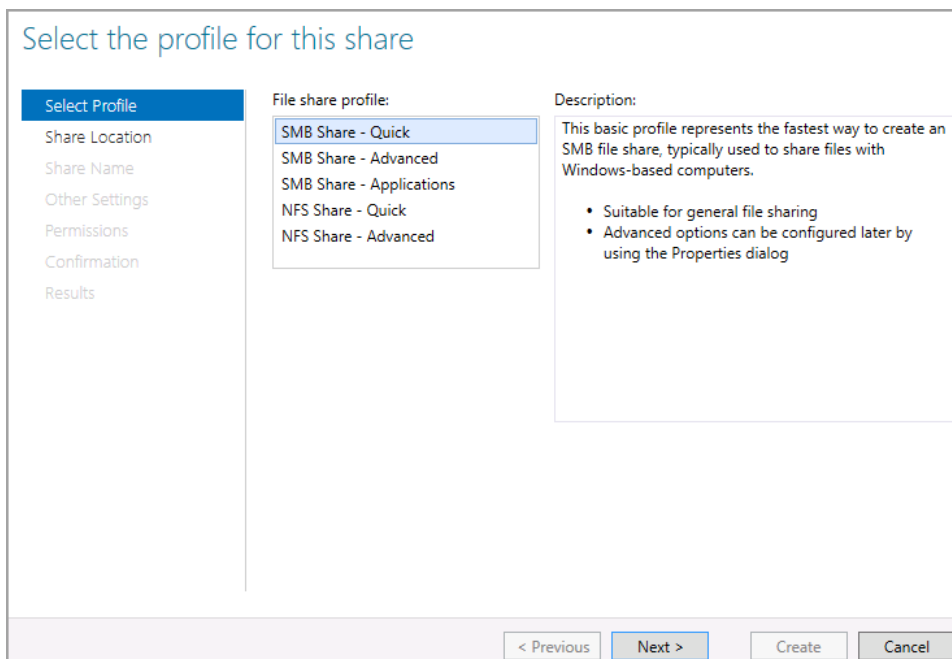
3. From the “Server Manager – Dashboard”, click “File and Storage Services”.



4. Click on “Shares”, right click the open white space under SYSVOL and select “New Share”.



5. Click through each of the share profiles and read the descriptions. Select “SMB Share – Quick” and click “Next”.



6. On the “Share Location” window, select the “H:” drive and click “Next”.

### Select the server and path for this share

Select Profile  
**Share Location**  
Share Name  
Other Settings  
Permissions  
Confirmation  
Results

Server:

Server Name	Status	Cluster Role	Owner Node
W2K12R2-ADDC	Online	Not Clustered	

Share location:

☒ Select by volume:

Volume	Free Space	Capacity	File System
C:	10.5 GB	19.7 GB	NTFS
<b>H:</b>	982 MB	1,024 MB	NTFS
T:	982 MB	1,024 MB	NTFS

The location of the file share will be a new folder in the \Shares directory on the selected volume.

☐ Type a custom path:

7. On the “Share Name” window, type **Human Resources** and click “Next”.

### Specify share name

Select Profile  
Share Location  
**Share Name**  
Other Settings  
Permissions  
Confirmation  
Results

Share name:

Share description:

Local path to share:

**i** If the folder does not exist, the folder is created.

Remote path to share:

8. On the “Other Settings” page, click “Next”.

### Configure share settings

Select Profile

Share Location

Share Name

**Other Settings**

Permissions

Confirmation

Results

☐ Enable access-based enumeration

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

☒ Allow caching of share

Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

☐ Enable BranchCache on the file share

BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

☐ Encrypt data access

When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

9. On the “Permissions” window, select “Customize permissions”.

### Specify permissions to control access

Select Profile

Share Location

Share Name

Other Settings

**Permissions**

Confirmation

Results

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Full Control

Folder permissions:

Type	Principal	Access	Applies To
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execute	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder only

Customize permissions...

10. Click the “Share” tab, click “Everyone” and click “Remove”.

Name: H:\Shares\Human Resources  
Owner: Administrators (MYDOMAIN\Administrators) [Change](#)

Permissions Share Auditing Effective Access

To modify share permissions, select the entry and click Edit.

Network location for this share: \\W2K12R2-ADDC.mydomain.local\Human Resources

Permission entries:

Type	Principal	Access
Allow	Everyone	Full Control

[Add](#) [Remove](#) [Edit](#)

11. Stay on the page and click “Add”.

Name: H:\Shares\Human Resources  
Owner: Administrators (MYDOMAIN\Administrators) [Change](#)

Permissions Share Auditing Effective Access

To modify share permissions, select the entry and click Edit.

Network location for this share: \\W2K12R2-ADDC.mydomain.local\Human Resources

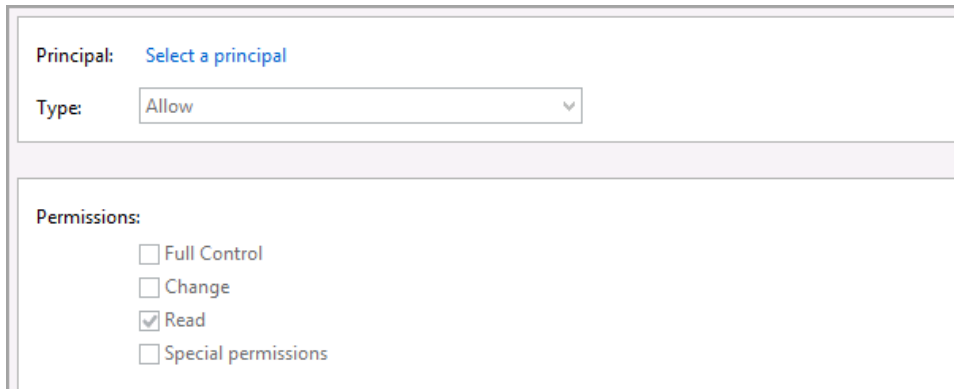
Permission entries:

No groups or users have permission to access this object. However, the owner of this object can assign permissions.

[Add](#) [Remove](#) [Edit](#)



12. Click “Select a principal”.



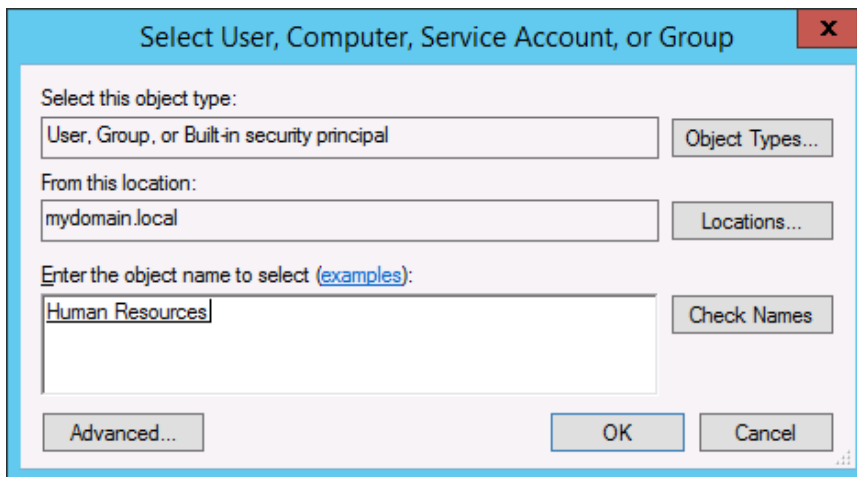
Principal: [Select a principal](#)

Type: Allow

Permissions:

- ☐ Full Control
- ☐ Change
- ☒ Read
- ☐ Special permissions

13. Type “Human Resources” and click “Check Names”. Click “OK”.



Select User, Computer, Service Account, or Group

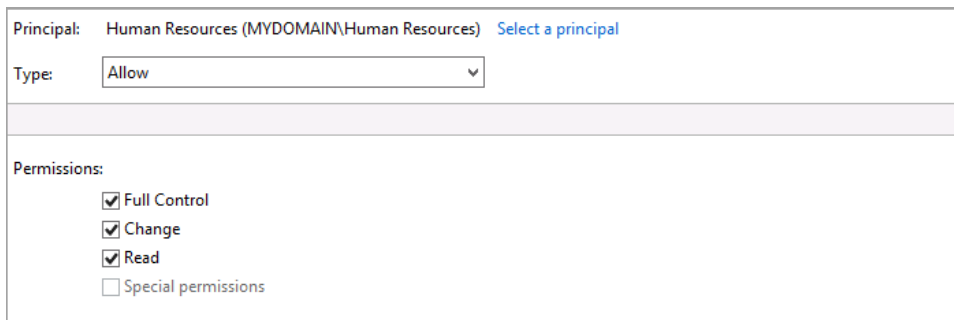
Select this object type:  
User, Group, or Built-in security principal Object Types...

From this location:  
mydomain.local Locations...

Enter the object name to select (examples):  
Human Resources Check Names

Advanced... OK Cancel

14. Place a check mark by “Full Control” and click “OK”. Click “OK”.



Principal: Human Resources (MYDOMAIN\Human Resources) [Select a principal](#)

Type: Allow

Permissions:

- ☒ Full Control
- ☒ Change
- ☒ Read
- ☐ Special permissions

15. On the “Permissions” page, click “Next”.

### Specify permissions to control access

Select Profile  
Share Location  
Share Name  
Other Settings  
**Permissions**  
Confirmation  
Results

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Custom

Folder permissions:

Type	Principal	Access	Applies To
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execute	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder only

Customize permissions...

16. Click “Create” and click “Close”.

### Confirm selections

Select Profile  
Share Location  
Share Name  
Other Settings  
Permissions  
**Confirmation**  
Results

Confirm that the following are the correct settings, and then click Create.

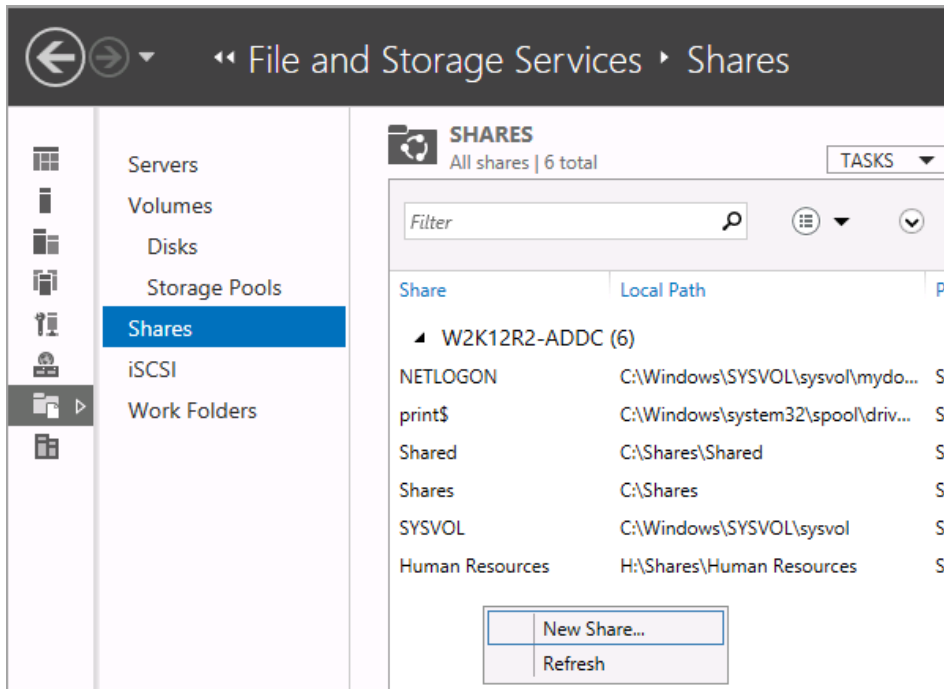
**SHARE LOCATION**

Server: W2K12R2-ADDC  
Cluster role: Not Clustered  
Local path: H:\Shares\Human Resources

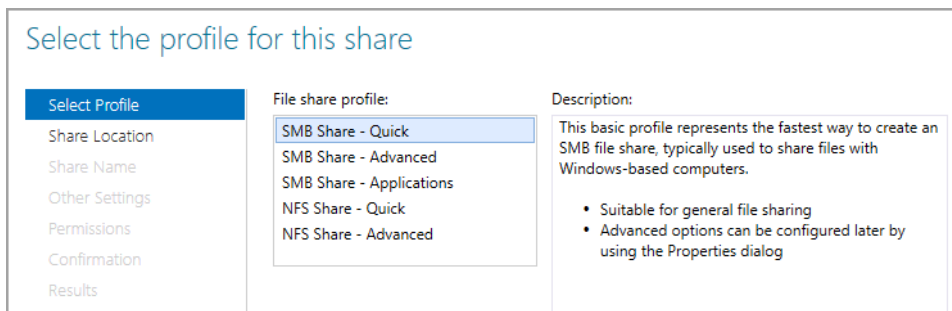
**SHARE PROPERTIES**

Share name: Human Resources  
Protocol: SMB  
Access-based enumeration: Disabled  
Caching: Enabled  
BranchCache: Disabled  
Encrypt data: Disabled

17. Right click the white space under Human Resources and select “New Share”.



18. On the “Select Profile” page, select “SMB Share – Quick” and click “Next”.



19. On the “Share Location” page, select the “T:” volume and click “Next”.

Select the server and path for this share

Select Profile  
**Share Location**  
Share Name  
Other Settings  
Permissions  
Confirmation  
Results

Server:

Server Name	Status	Cluster Role	Owner Node
W2K12R2-ADDC	Online	Not Clustered	

Share location:

☒ Select by volume:

Volume	Free Space	Capacity	File System
H:	982 MB	1,024 MB	NTFS
<b>T:</b>	<b>982 MB</b>	<b>1,024 MB</b>	<b>NTFS</b>
X:	3.94 GB	3.99 GB	NTFS

The location of the file share will be a new folder in the \Shares directory on the selected volume.

20. On the “Share Name” page, type IT for the name and click “Next”.

Specify share name

Select Profile  
Share Location  
**Share Name**  
Other Settings  
Permissions  
Confirmation  
Results

Share name:

Share description:

Local path to share:

If the folder does not exist, the folder is created.

Remote path to share:

21. On the “Other Settings” page, click “Next”.

### Configure share settings

Select Profile

Share Location

Share Name

**Other Settings**

Permissions

Confirmation

Results

☐ Enable access-based enumeration

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

☒ Allow caching of share

Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

☐ Enable BranchCache on the file share

BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

☐ Encrypt data access

When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

22. On the “Permissions” page, click “Customize permissions”.

### Specify permissions to control access

Select Profile

Share Location

Share Name

Other Settings

**Permissions**

Confirmation

Results

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Full Control

Folder permissions:

Type	Principal	Access	Applies To
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execute	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder only

Customize permissions...

23. Click the Share Tab, click on “Everyone” and click “Remove”.

Name: T:\Shares\IT  
Owner: Administrators (MYDOMAIN\Administrators) [Change](#)

Permissions Share Auditing Effective Access

To modify share permissions, select the entry and click Edit.

Network location for this share: \\W2K12R2-ADDC.mydomain.local\IT

Permission entries:

Type	Principal	Access
Allow	Everyone	Full Control

Add Remove Edit

24. Click on “Add”.

Name: T:\Shares\IT  
Owner: Administrators (MYDOMAIN\Administrators) [Change](#)

Permissions Share Auditing Effective Access

To modify share permissions, select the entry and click Edit.

Network location for this share: \\W2K12R2-ADDC.mydomain.local\IT

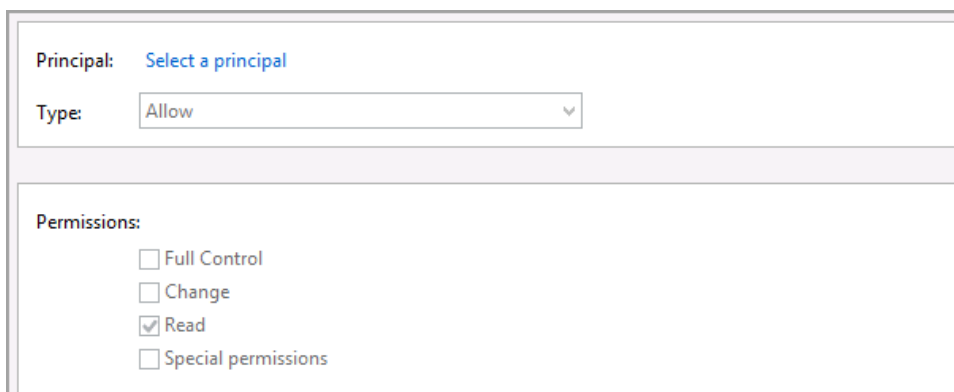
Permission entries:

No groups or users have permission to access this object. However, the owner of this object can assign permissions.

Add Remove Edit



25. Click “Select a principal”



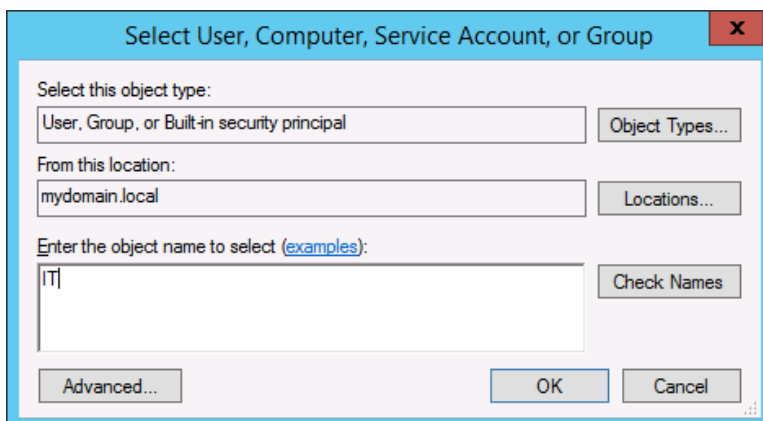
Principal: [Select a principal](#)

Type: Allow

Permissions:

- ☐ Full Control
- ☐ Change
- ☒ Read
- ☐ Special permissions

26. Type “IT” and click “Check Names” and click “OK”.



Select User, Computer, Service Account, or Group

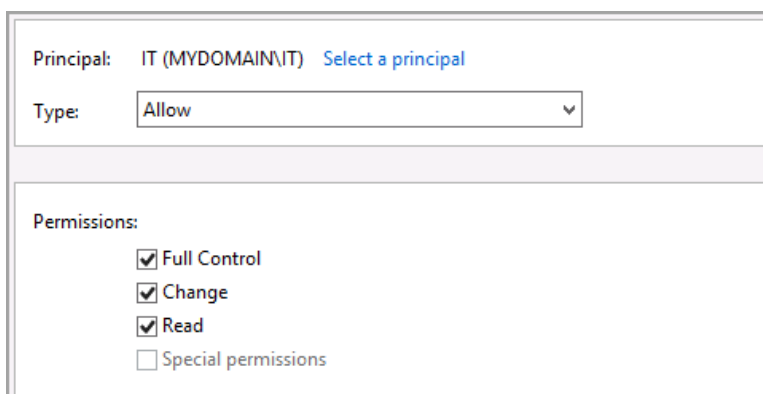
Select this object type:  
User, Group, or Built-in security principal Object Types...

From this location:  
mydomain.local Locations...

Enter the object name to select ([examples](#)):  
IT Check Names

Advanced... OK Cancel

27. Place a check by “Full Control” and click “OK”.



Principal: IT (MYDOMAIN\IT) [Select a principal](#)

Type: Allow

Permissions:

- ☒ Full Control
- ☒ Change
- ☒ Read
- ☐ Special permissions

28. On the “Permissions” page, click “Next”. Click “Create”.

**Specify permissions to control access**

Select Profile  
Share Location  
Share Name  
Other Settings  
**Permissions**  
Confirmation  
Results

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Custom

Folder permissions:

Type	Principal	Access	Applies To
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execute	This folder, subfolders, and files
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder only

[Customize permissions...](#)

29. On the “Results” page, click “Close”.

**View results**

Select Profile  
Share Location  
Share Name  
Other Settings  
Permissions  
Confirmation  
**Results**

The share was successfully created.

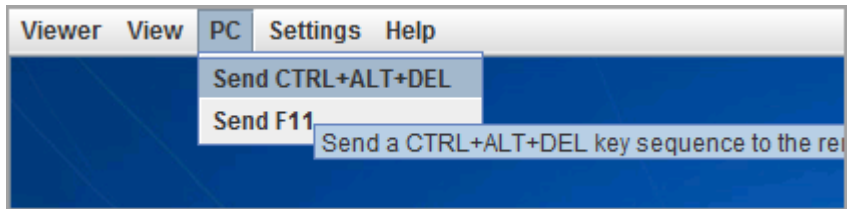
Task	Progress	Status
Create SMB share	<div style="width: 100%;"></div>	Completed
Set SMB permissions	<div style="width: 100%;"></div>	Completed

30. Open a console to the WIN7 machine by clicking the icon in the topology.

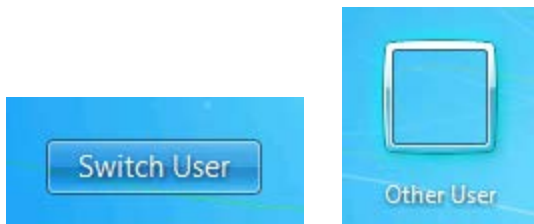




31. Click “PC > Send CTRL+ALT+DEL”.



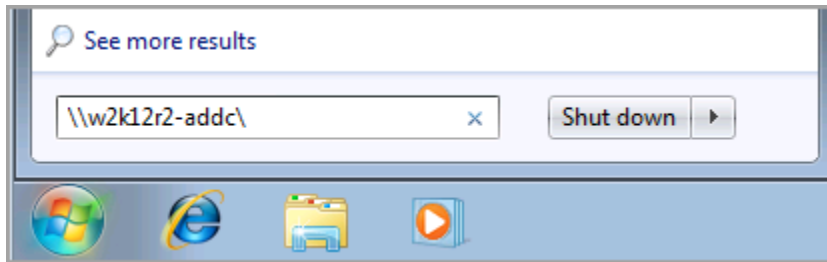
32. Click on “Switch User” and select “Other User”.



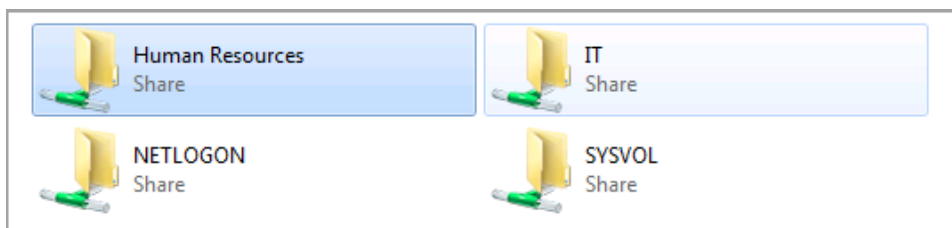
33. Type **mydomain\sallyhr** as the username and **Password1** as the password. Hit “Enter”.



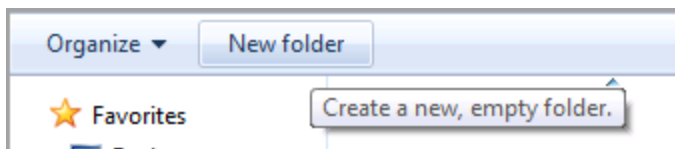
34. Left click the Start Button and type [\\w2k12r2-addc\](#) and hit “Enter”.



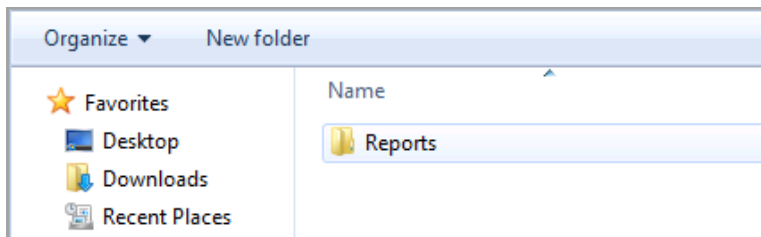
35. Double click on the Human Resources folder.



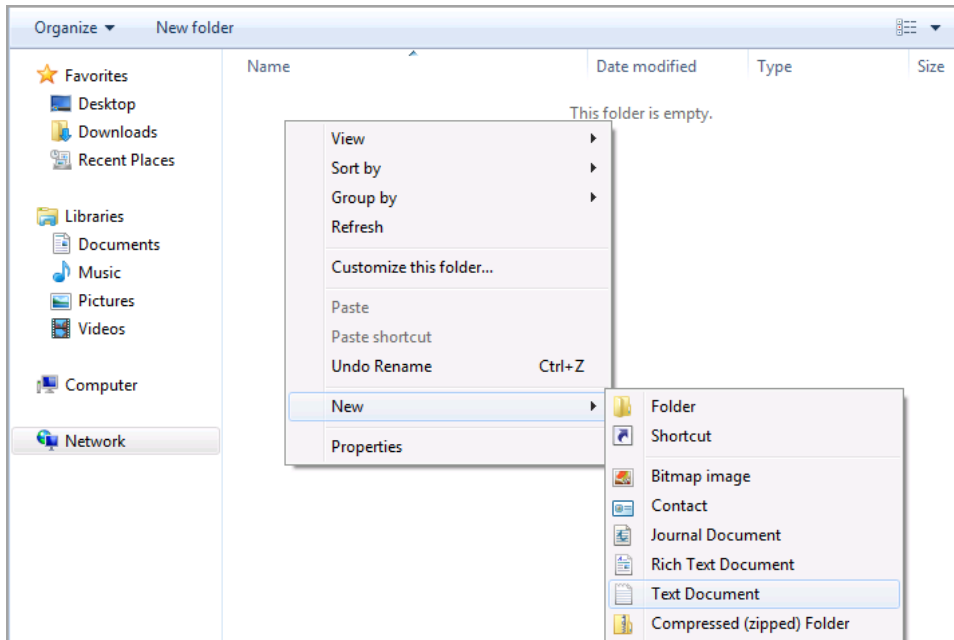
36. Click once on “New Folder” in the navigation bar and type **Reports** as the folder name. Hit “Enter”.



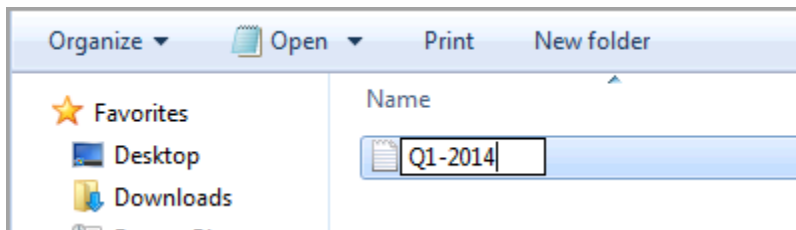
37. Double click the “Reports” folder to open.



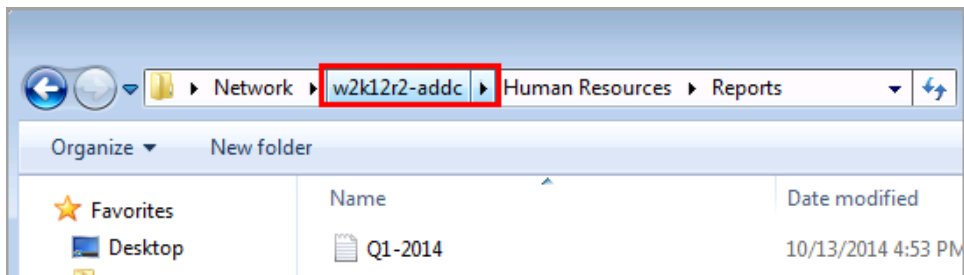
38. Right click any open white area and select “New > Text Document”.



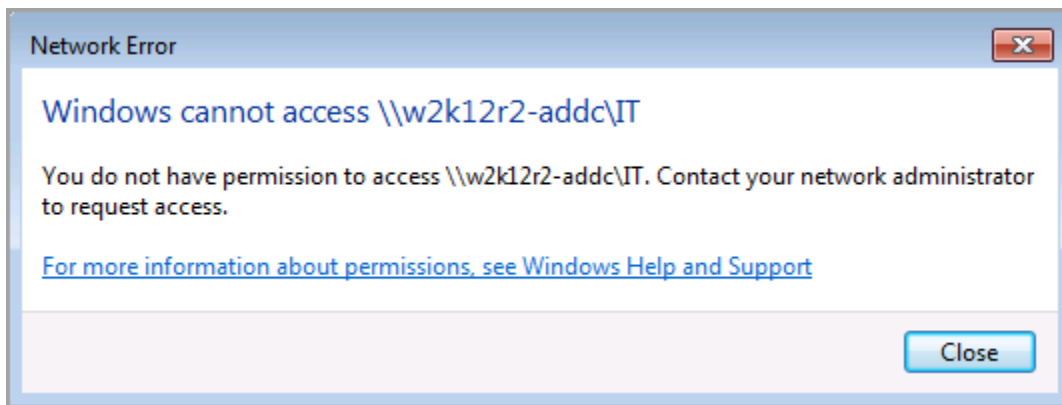
39. Name the document “Q1-2014” and hit “Enter”.



40. Click on w2k12r2-addc in the navigation bar to return to the root share.

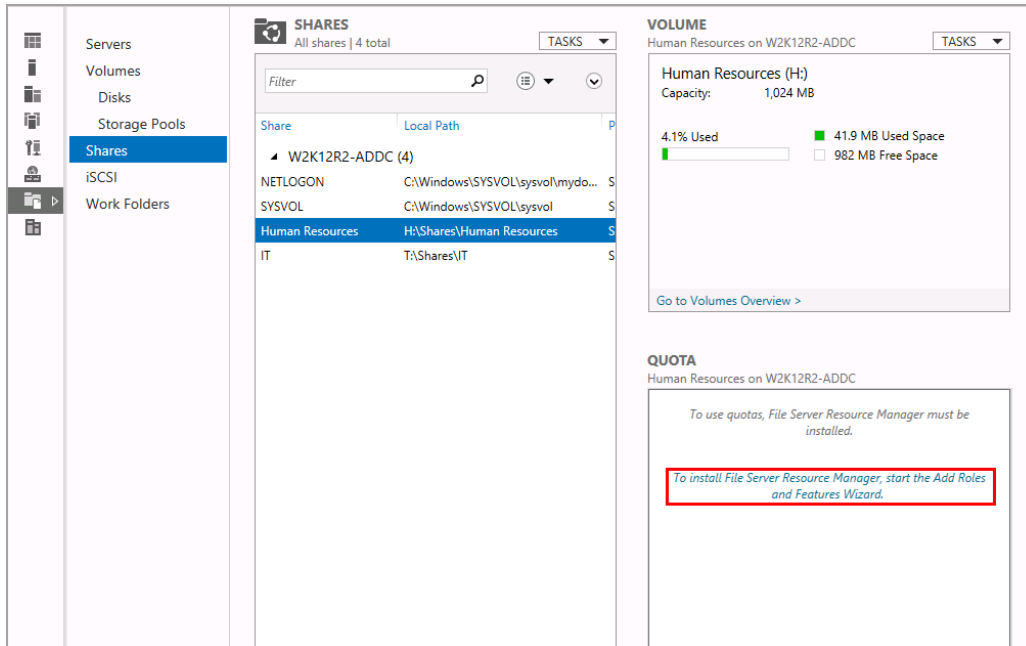


41. Double click on “IT” to see the access error. Click “Close”.

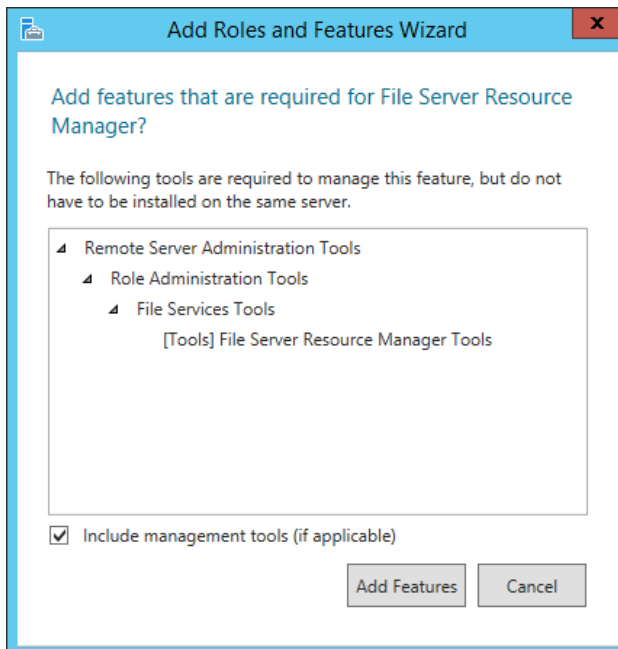


## 1.2 NTFS Quotas

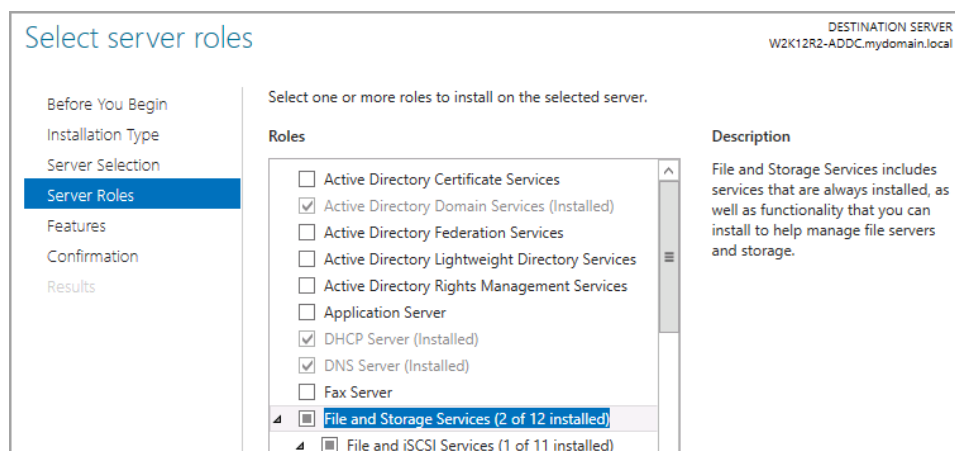
1. Return to the W2K12R2-ADDC machine. On the “Shares – Dashboard”, make sure Human Resources is highlighted and click the link to install the “File Resource Manager”.



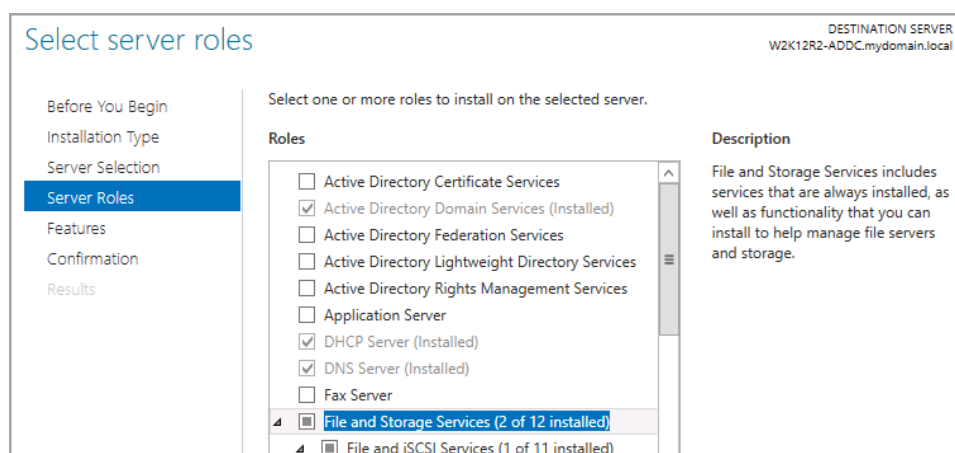
2. Click “Add Features” to install the required features.



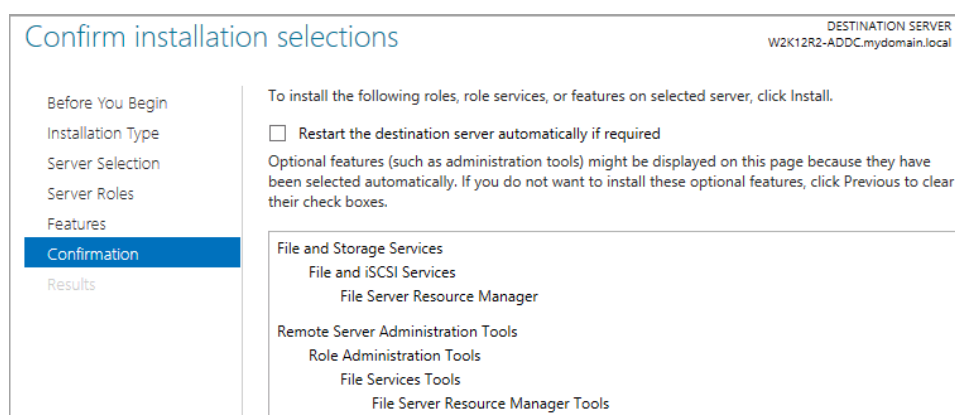
3. On the “Server Roles” page, click “Next”.



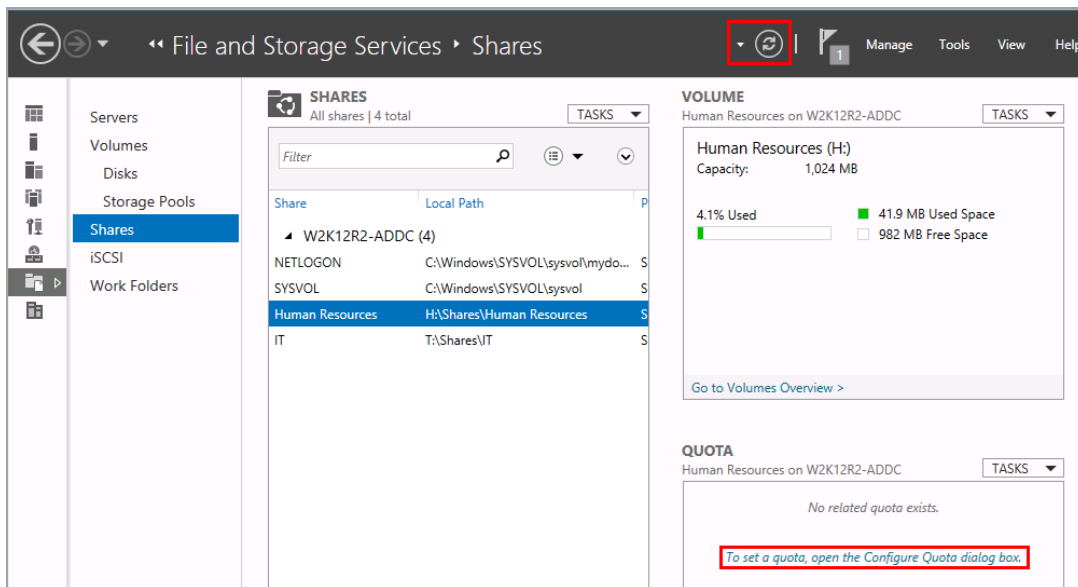
4. On the “Features” page, click “Next”.



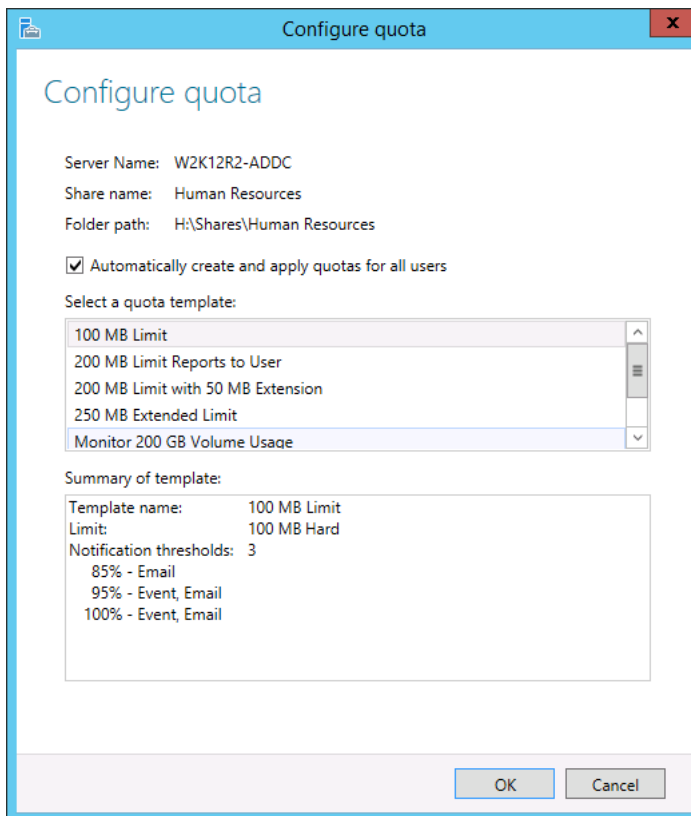
5. On the “Confirmation” page, click “Install”. Click “Close”.



6. Wait a few seconds and click refresh button on the “Shares – Dashboard”. Make sure the “Human Resources” share is highlighted in the middle pane. When the link below changes, click the link to open the “Configuration Quota dialog box”.



7. Place a check by “Automatically create and apply quotas for all users” click “OK”.

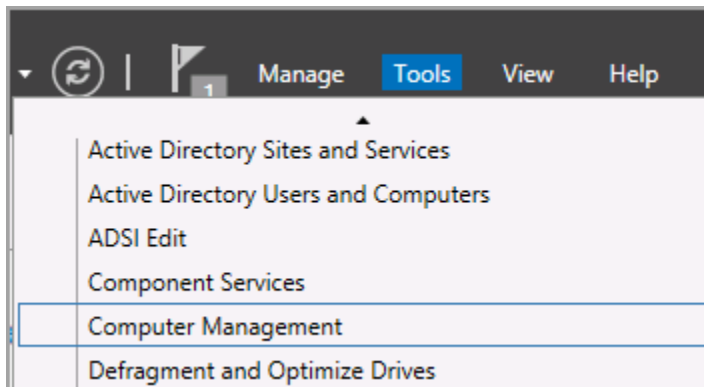


## 2 Volume Shadow Copy Services (VSS)

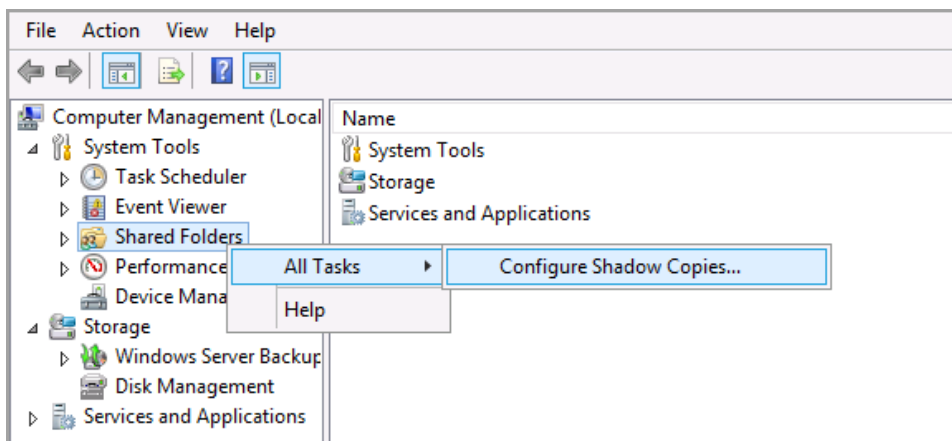
Volume Shadow Copy Services is a technology that allows point-in-time backups of entire volumes.

### 2.1 Enable VSS

1. On the “Server Manager – Dashboard” navigate to “Tools > Computer Management”.

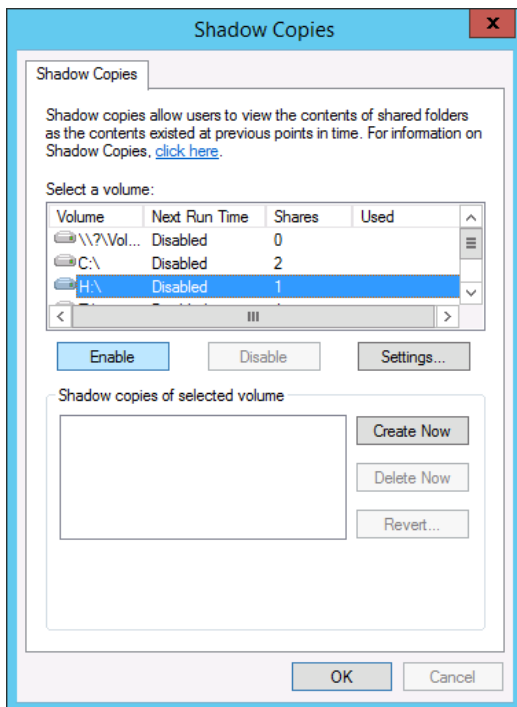


2. Right click “Shared Folders” and click “All Tasks > Configure Shadow Copies”.

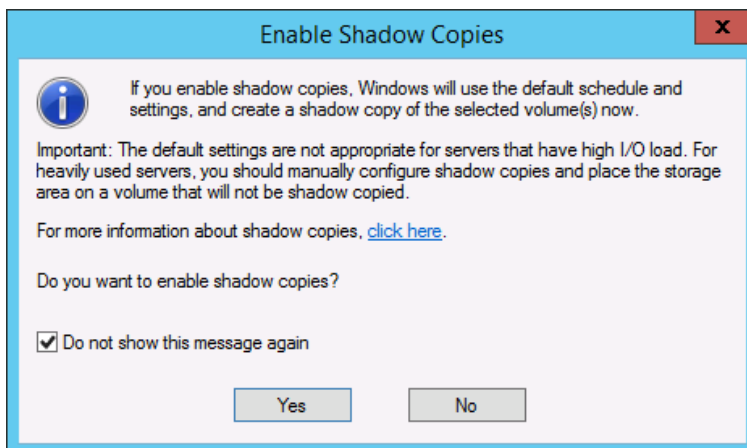




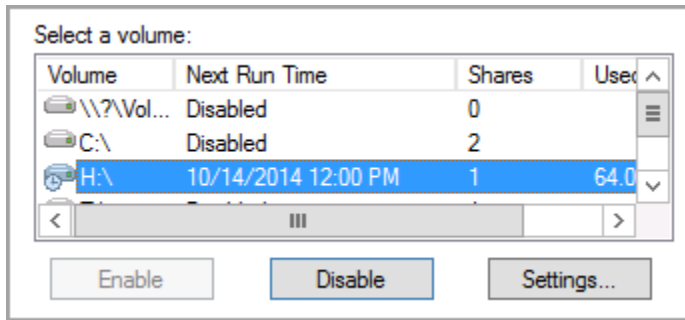
3. In the “Shadow Copies” window, highlight “H:\” and click “Enable”.



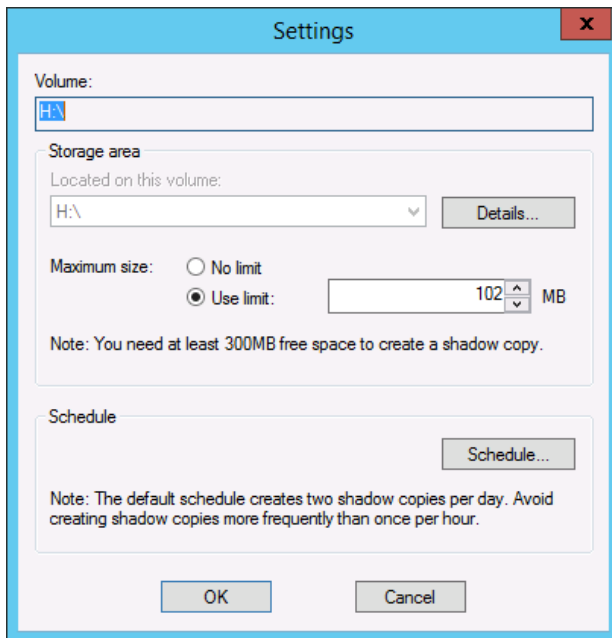
4. Read the information about high volume I/O and click “Yes”.



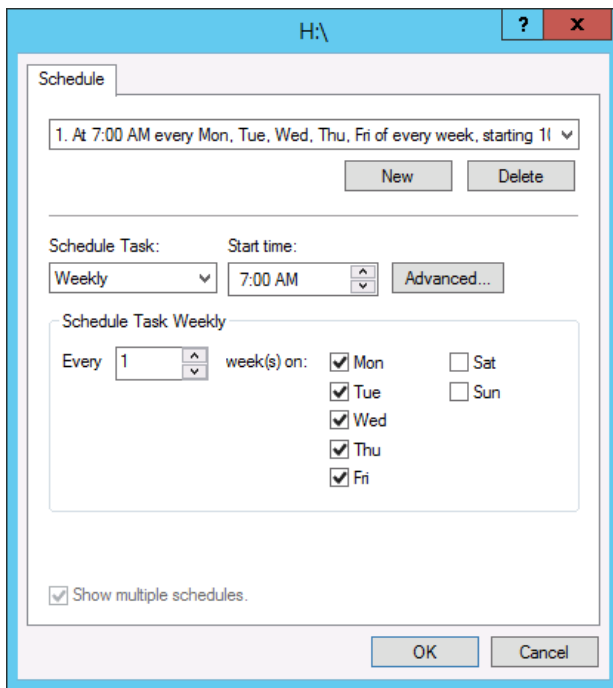
5. Highlight “H:\” and click “Settings”.



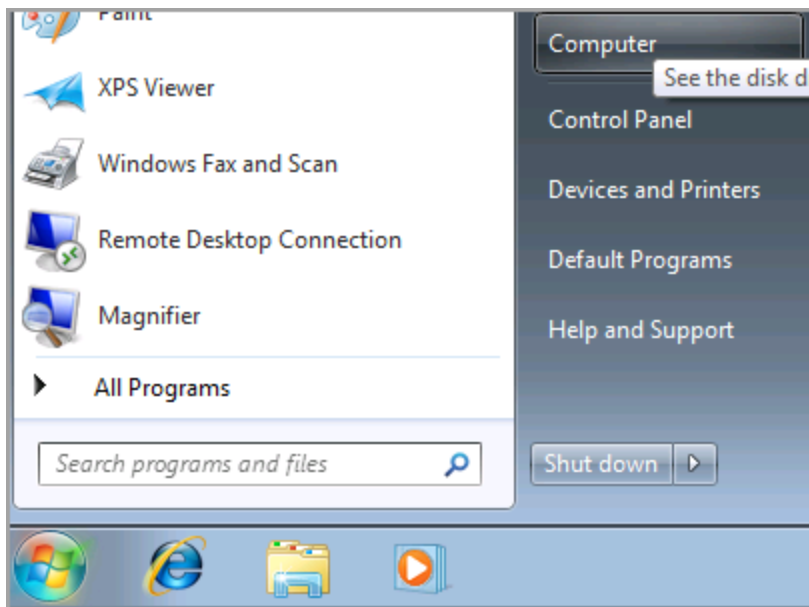
6. This is where you input manual settings for the VSS.



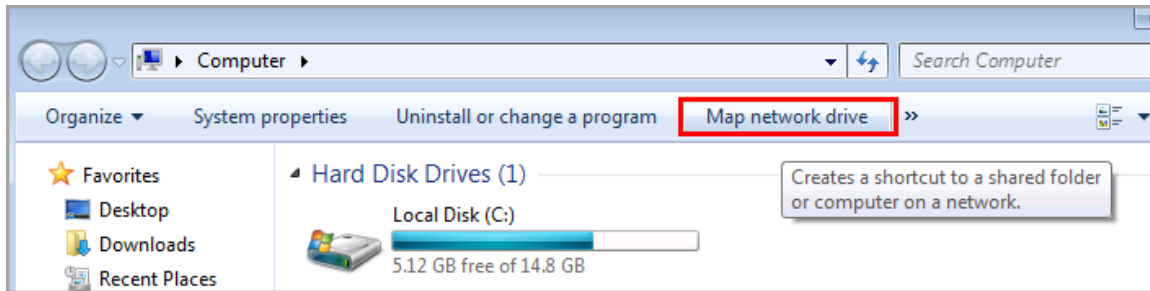
7. Click “Schedule” to view the current schedule. Click “Cancel” twice.



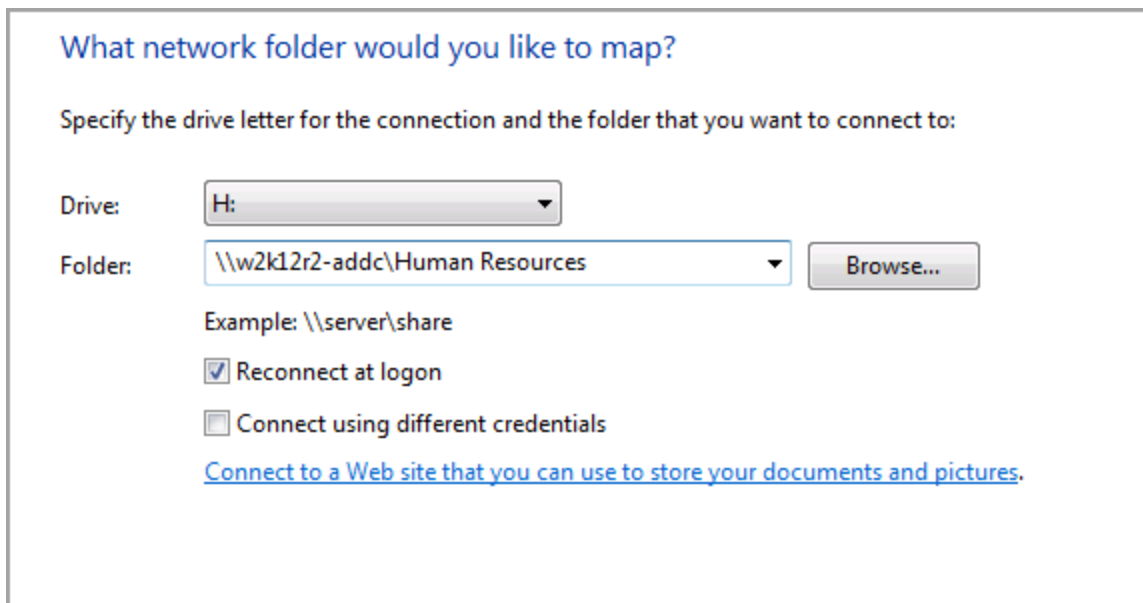
8. Open a console to the WIN7 machine, left click the Start Button and left click “Computer”.



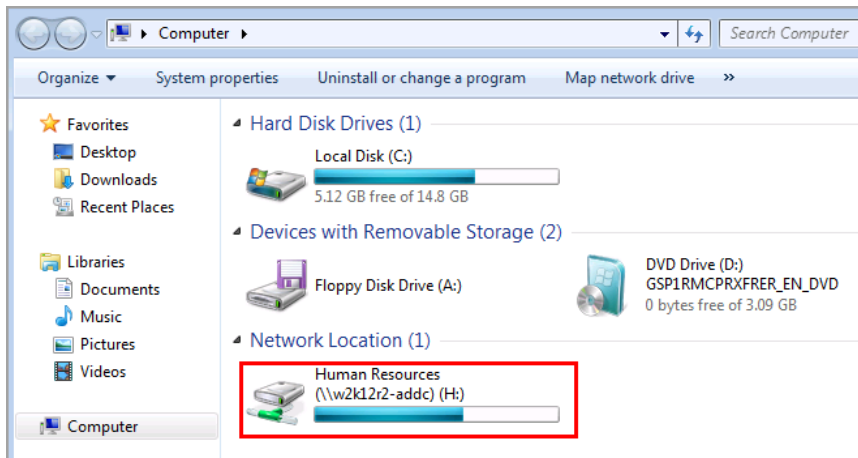
9. Select “Map network drive” from the navigation bar.



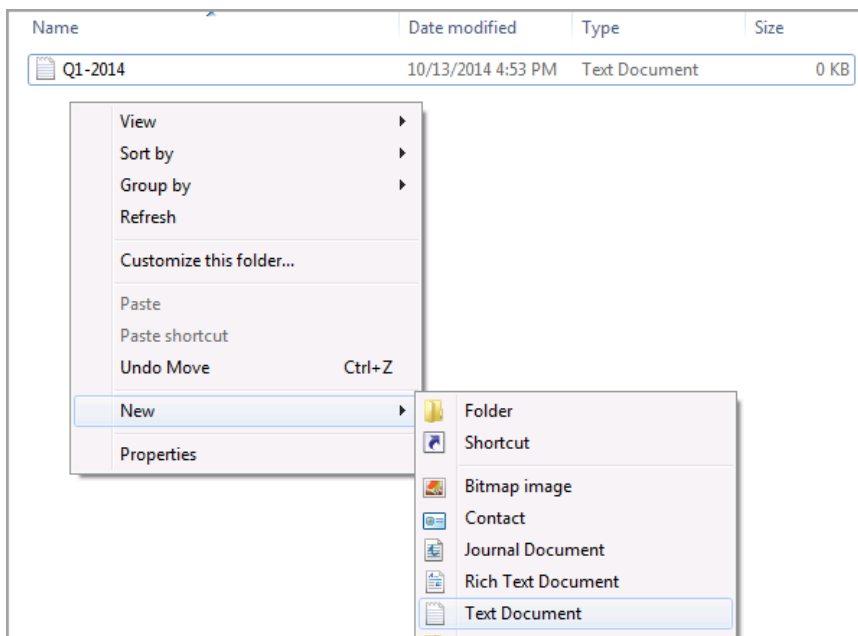
10. Use the drop down to change the drive letter to H:\ and type \\w2k12r2-addc\Human Resources into the Folder box. Click “Finish”.



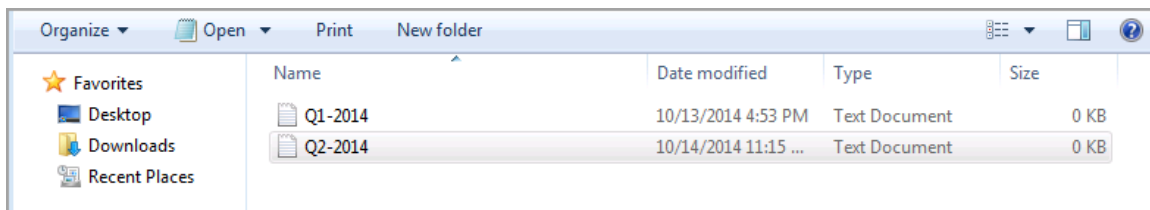
11. The Human Resources folder will automatically open. Close the folder and notice the new network location.



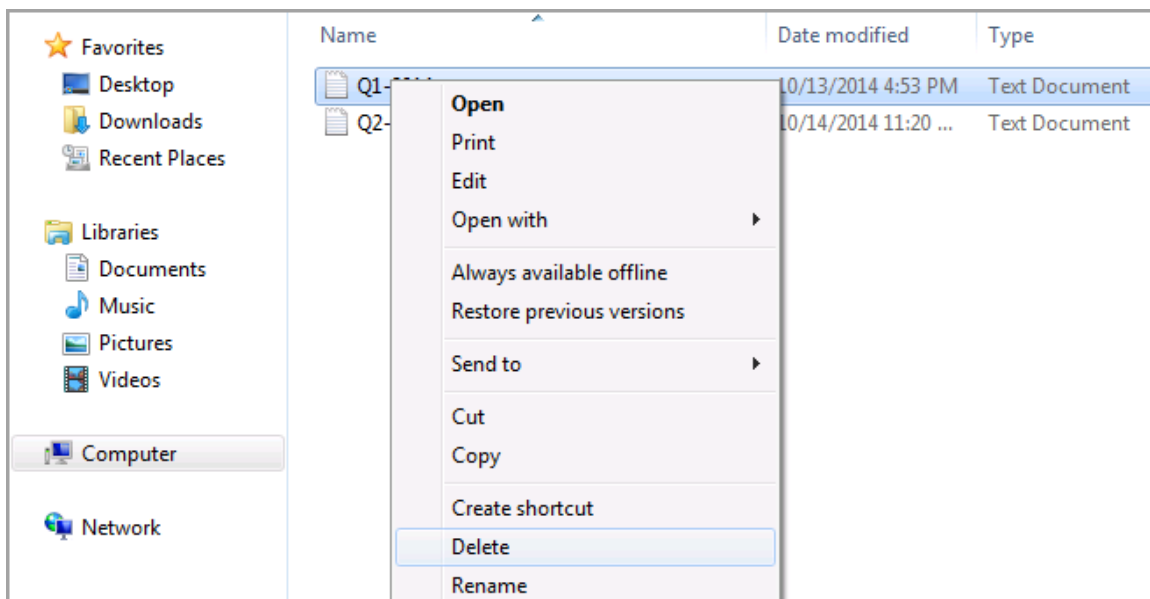
12. Double click on the “Human Resources” network location. Double click on the “Reports” folder. Right click under “Q1-2014” and select “New > Text document”.



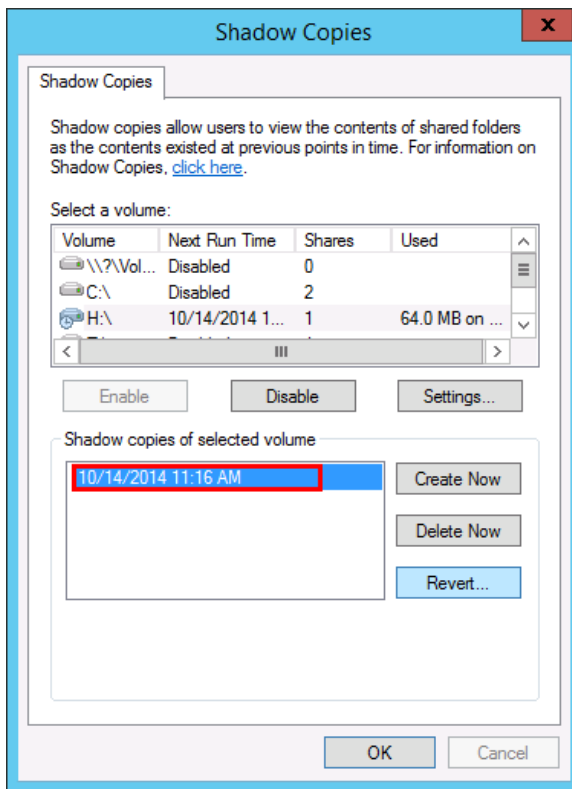
13. Type **Q2-2014** as the file name and hit “Enter”.



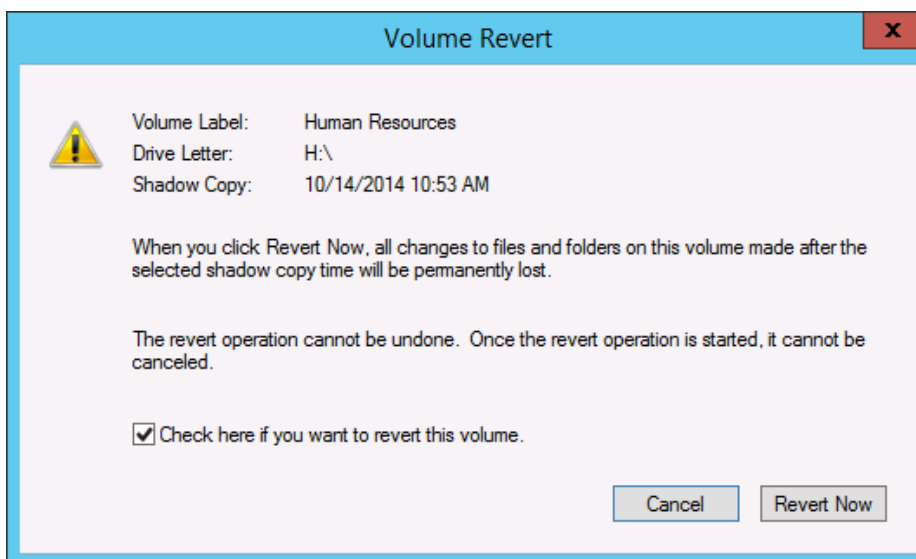
14. Right click on “Q1-2014” and select “Delete”. Click “Yes” to confirm the deletion.



15. Return to the W2K12R2-ADDC server and click on the Shadow Copy that was created. Click “Revert”.

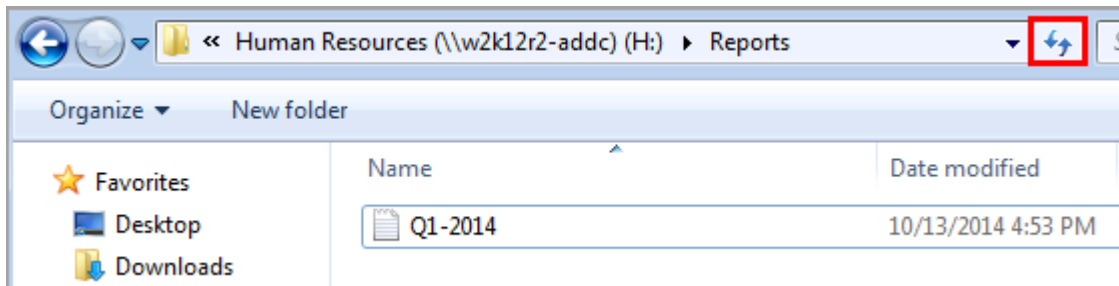


16. Read the information about reverting a Shadow Copy, place a check next to “Check here if you want to revert this volume” and click “Revert Now”. Click “Ok” and close the “Computer Management” window.



17. Return to the WIN7 machine and refresh the Reports folder.

(Note: Only Q1-2014 returns. Q2-2014 was not part of the original Volume Shadow Copy.)

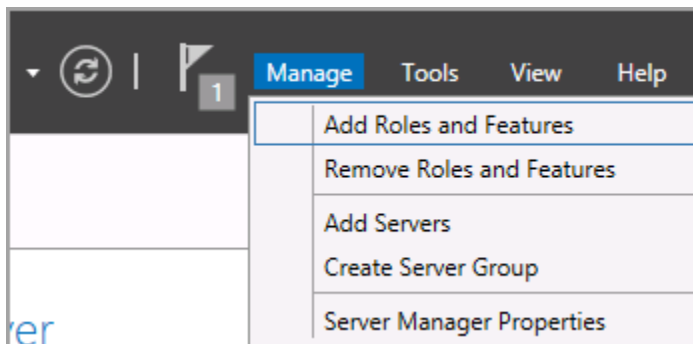


### 3 Work Folders

Work Folders is a network file sync role. Users are able to work from almost any device in the office or from home and have access to the required documents to perform their job.

#### 3.1 Install Work Folders Role

1. Return to the W2K12R2-ADDC server. On the “Server Manager – Dashboard”, click “Manage > Add Roles and Features”.





2. On the “Before you begin” page, select “Next”.

## Before you begin

DESTINATION SERVER  
W2K12R2-ADDC.mydomain.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:  
[Start the Remove Roles and Features Wizard](#)

Before you continue, verify that the following tasks have been completed:

- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

3. On the “Installation Type” page, leave the defaults and select “Next”.

## Select installation type

DESTINATION SERVER  
W2K12R2-ADDC.mydomain.local

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Confirmation

Results

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

☒ **Role-based or feature-based installation**  
Configure a single server by adding roles, role services, and features.

☐ **Remote Desktop Services installation**  
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

4. On the “Server Selection” page, select “Next”.

**Select destination server** DESTINATION SERVER  
W2K12R2-ADDC.mydomain.local

Before You Begin  
Installation Type  
**Server Selection**  
Server Roles  
Features  
Confirmation  
Results

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool  
☐ Select a virtual hard disk

**Server Pool**

Filter:

Name	IP Address	Operating System
W2K12R2-ADDC.mydom...	192.168.1.100	Microsoft Windows Server 2012 R2 Datacenter

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

5. On the “Server Roles” page, expand “File and Storage Services (3 of 12 installed)”. Expand “File and iSCSI Services (2 of 11 installed)”. Place a check next to “Work Folders”.

**Select server roles** DESTINATION SERVER  
W2K12R2-ADDC.mydomain.local

Before You Begin  
Installation Type  
Server Selection  
**Server Roles**  
Features  
Confirmation  
Results

Select one or more roles to install on the selected server.

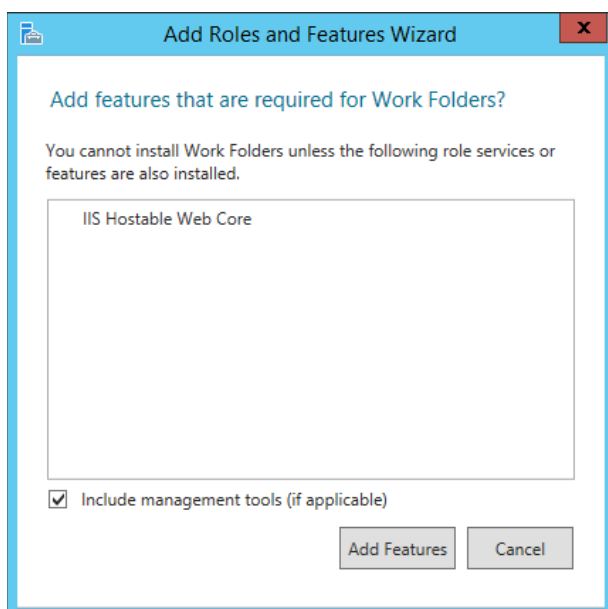
**Roles**

- ☐ Fax Server
- ☒ **File and Storage Services (3 of 12 installed)**
  - ☒ **File and iSCSI Services (2 of 11 installed)**
    - ☒ File Server (Installed)
    - ☐ BranchCache for Network Files
    - ☐ Data Deduplication
    - ☐ DFS Namespaces
    - ☐ DFS Replication
    - ☒ File Server Resource Manager (Installed)
    - ☐ File Server VSS Agent Service
    - ☐ iSCSI Target Server
    - ☐ iSCSI Target Storage Provider (VDS and VSS)
    - ☐ Server for NFS
    - ☐ **Work Folders**
  - ☒ Storage Services (Installed)

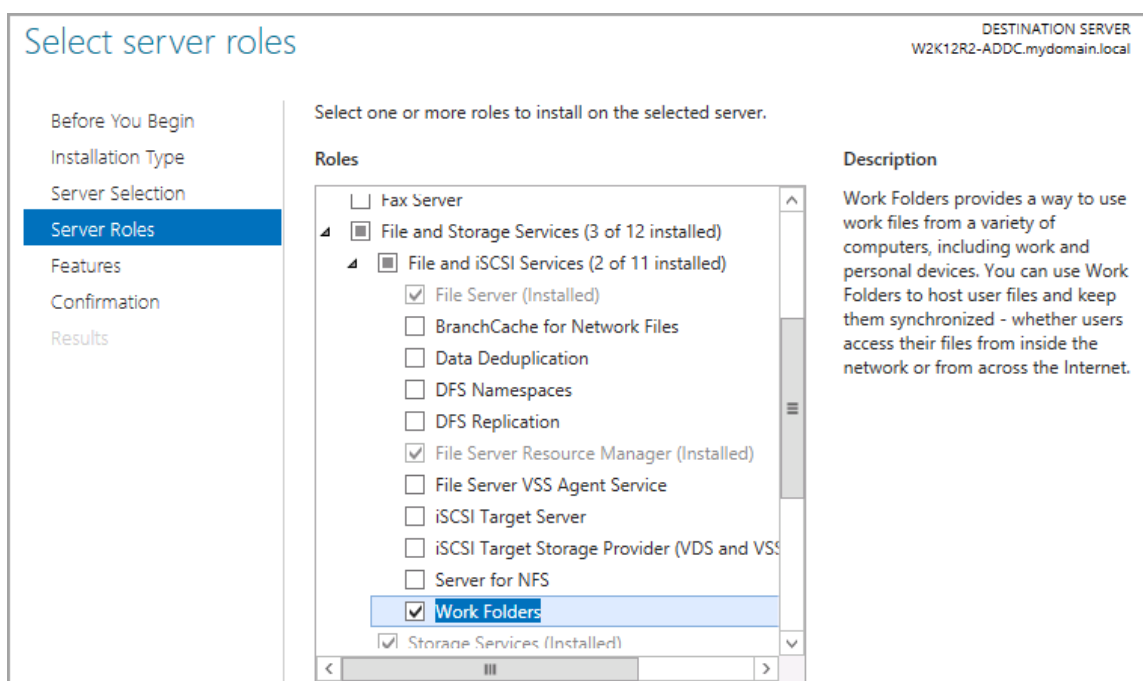
**Description**

Work Folders provides a way to use work files from a variety of computers, including work and personal devices. You can use Work Folders to host user files and keep them synchronized - whether users access their files from inside the network or from across the Internet.

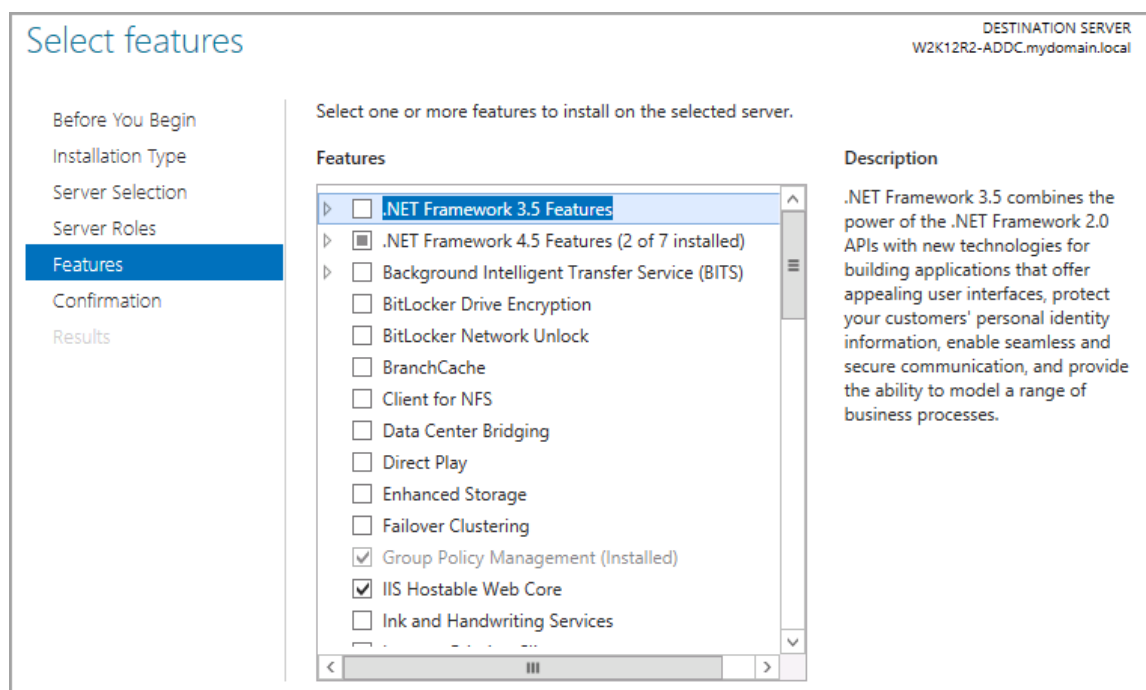
6. A Features window will appear listing dependency roles and features that must be installed. Click “Add Features”.



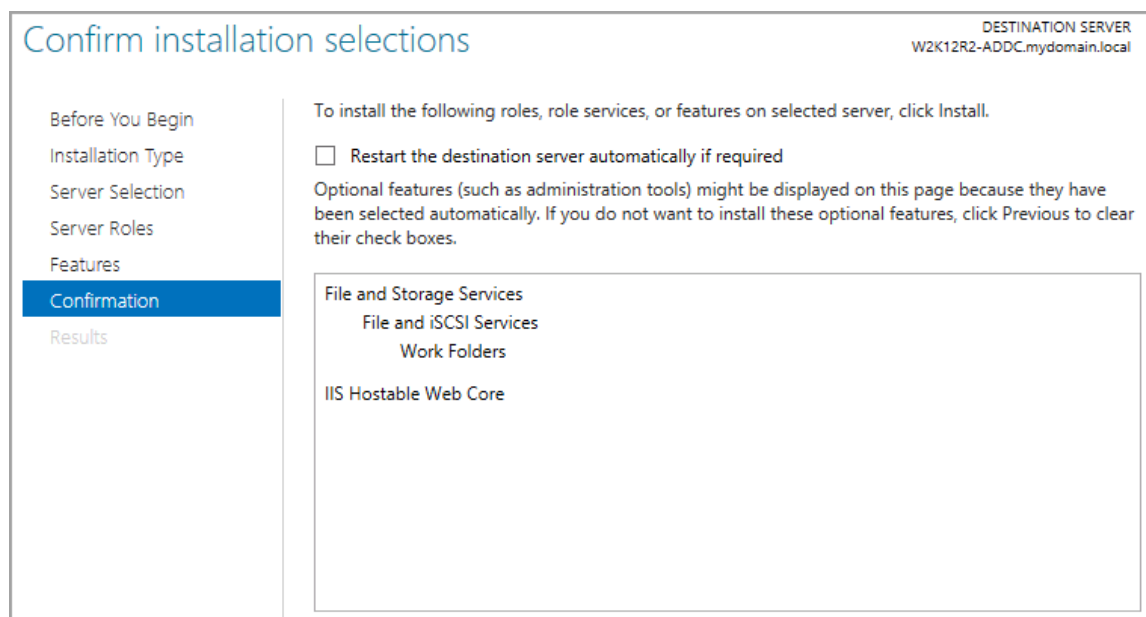
7. On the “Server Roles” page, click “Next”.



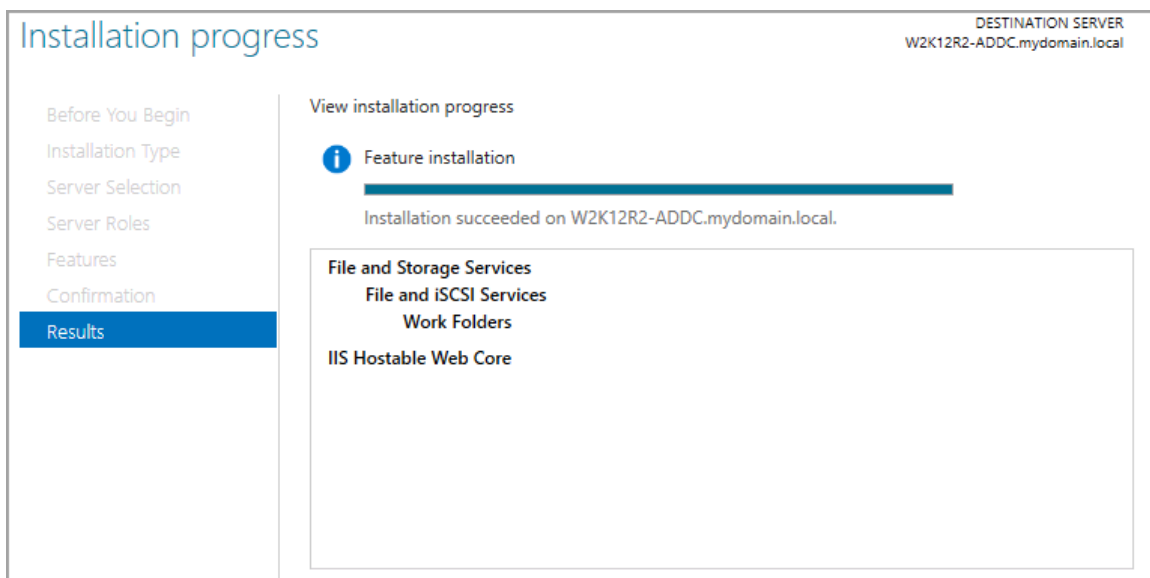
8. On the “Features” page, click “Next”.



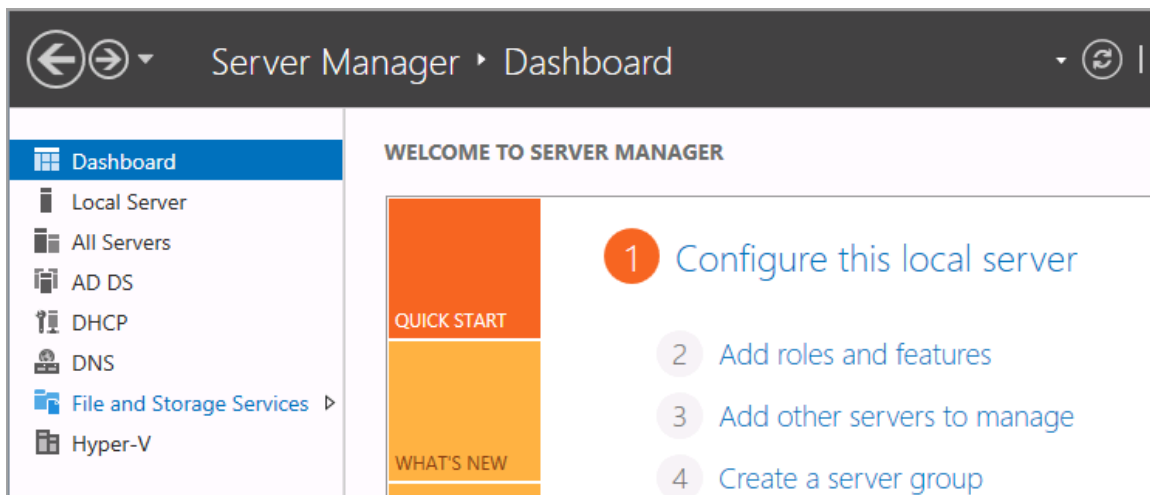
9. On the “Confirmation” page, click “Install”.



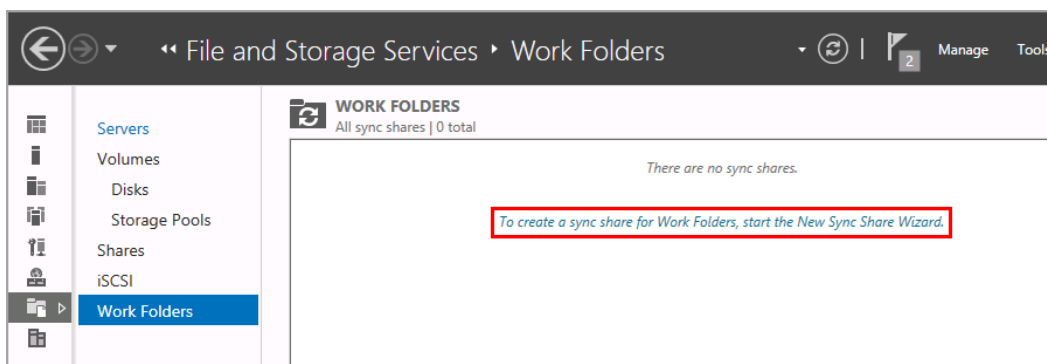
10. On the “Results” page, click “Close”.



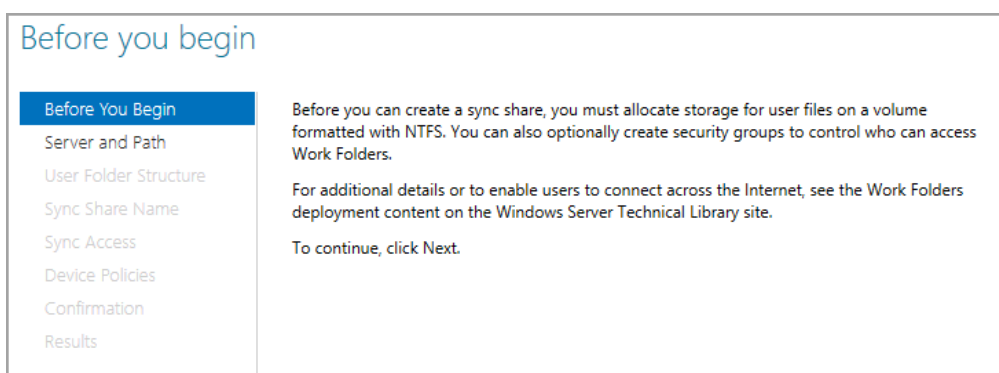
11. On the “Server Manager – Dashboard” select “File and Storage Services”.



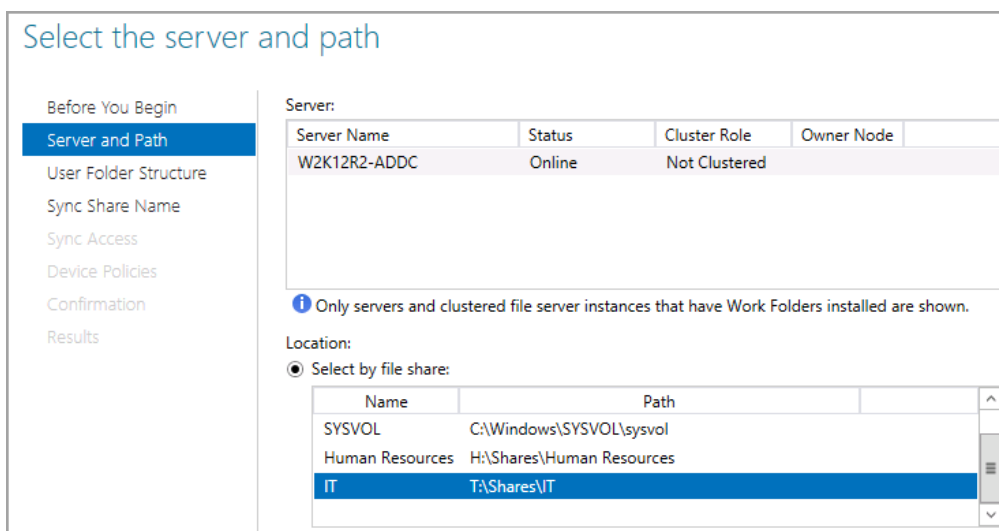
12. Select “Work Folders” and select the link to “create a sync share for Work Folders”.  
(Note: You may need to click the refresh button to get the link to appear.)



13. On the “Before you begin” page, click “Next”.



14. On the “Server and Path” page, scroll down and highlight “T:\Shares\IT”. Click “Next”.



15. On the “User Folder Structure” page, leave the defaults and click “Next”.

### Specify the structure for user folders

Before You Begin

Server and Path

**User Folder Structure**

Sync Share Name

Sync Access

Device Policies

Confirmation

Results

Choose a folder-naming format based on whether you have to maintain user folder compatibility or want to support identical aliases across domains.

☒ **User alias**  
 Maintains compatibility with existing user folders that use aliases for their names

☐ **User alias@domain**  
 Eliminates conflicts between identical user aliases in different domains

Syncing a subfolder can be useful if you currently redirect multiple folders for users and want to use this sync share with only one of these, such as the Documents folder.

☐ Sync only the following subfolder:

If the subfolder doesn't exist, it will be created for every user assigned to this Work Folders instance.

16. On the “Sync Share Name” page, leave the defaults and click “Next”.

### Enter the sync share name

Before You Begin

Server and Path

User Folder Structure

**Sync Share Name**

Sync Access

Device Policies

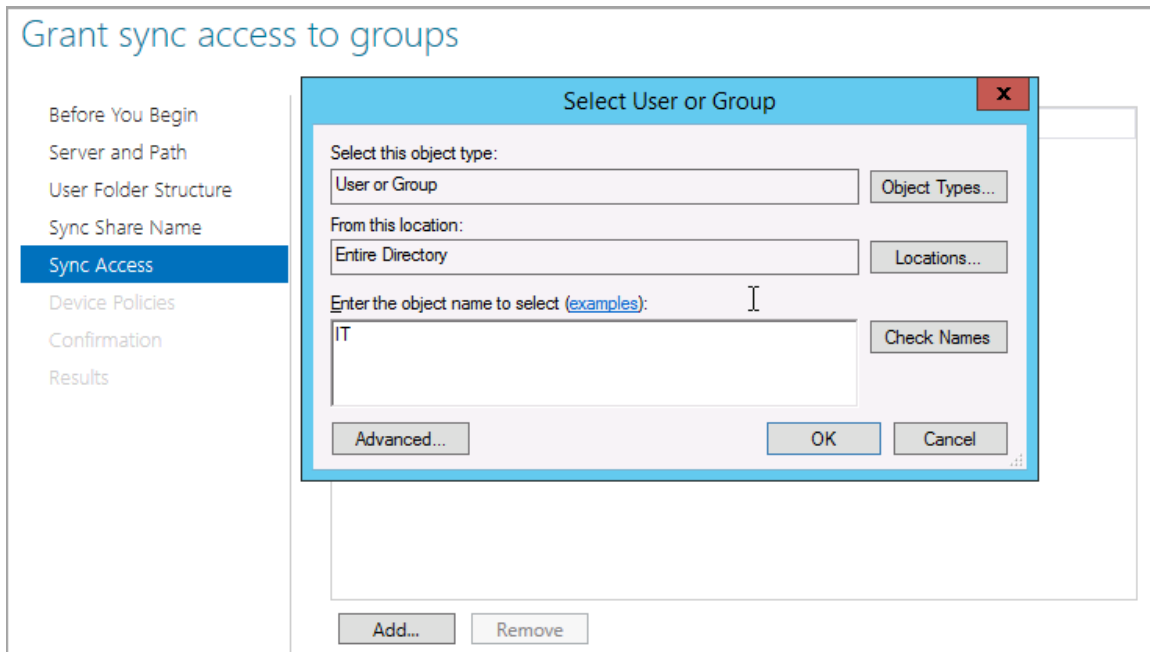
Confirmation

Results

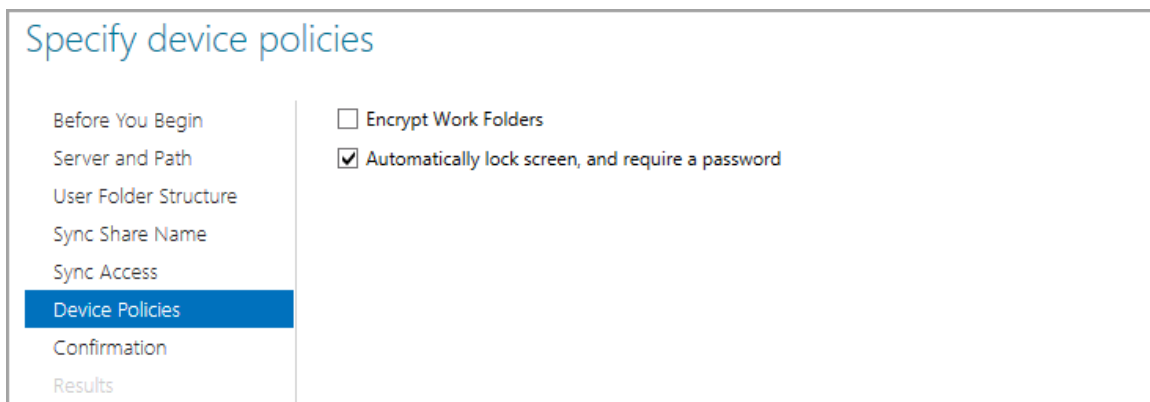
Name:

Description:

17. On the “Sync Access” page, select “Add”. Type IT in the name field and click “Check Names”. Click “OK”. Click “Next”.



18. On the “Device Policies” page, click “Next”.





19. On the “Confirmation” page, click “Create”. On the “Results” page, click “Close”.

### Confirm selections

Before You Begin

Server and Path

User Folder Structure

Sync Share Name

Sync Access

Device Policies

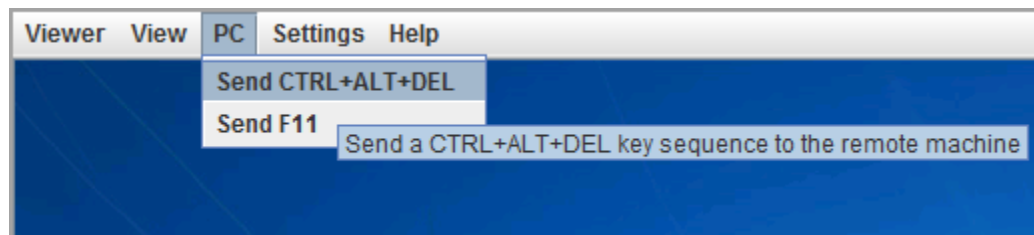
**Confirmation**

Results

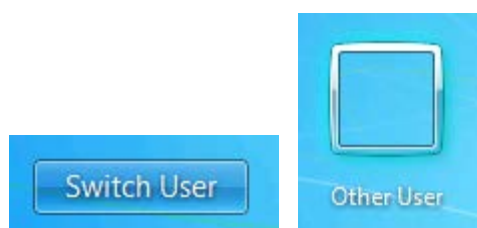
Confirm that the following are the correct settings, and then click Create.

<b>SYNC SHARE LOCATION</b>	
Server name:	W2K12R2-ADDC.mydomain.local
Cluster role:	Not Clustered
Path:	T:\Shares\IT
File share name:	IT
<b>SYNC SHARE PROPERTIES</b>	
Name:	IT
Description:	
Sync access:	MYDOMAIN\IT
Grant users exclusive access:	Yes
User folder structure:	User alias
Sync only this subfolder:	
<b>DEVICE POLICIES</b>	
Encrypt Work Folders:	No
Automatically lock screen, and require a password:	Yes

20. Open a console to the WIN7 machine. Click “PC > Send CTRL+ALT+DEL”.



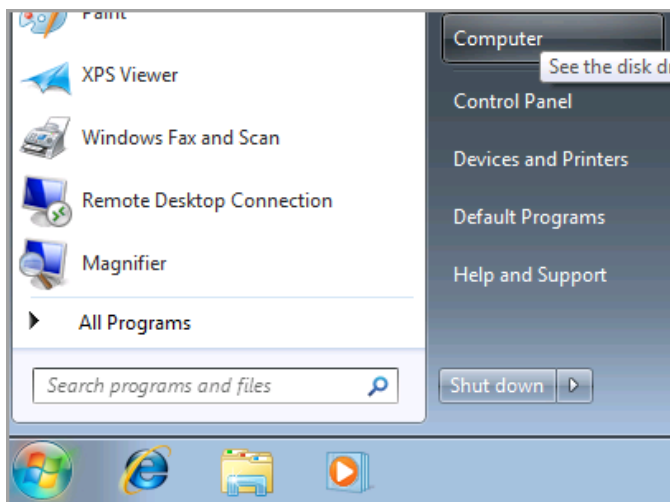
21. Click “Switch User” and “Other User”.



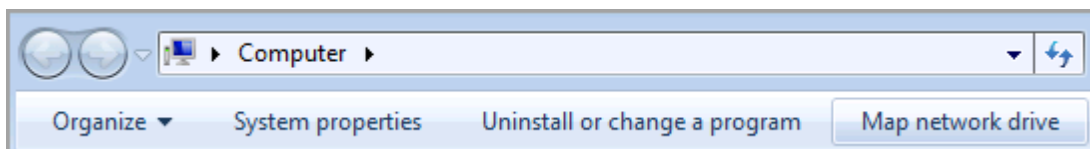
22. Type **mydomain\joeit** as the username and **Password1** as the password. Hit “Enter”.



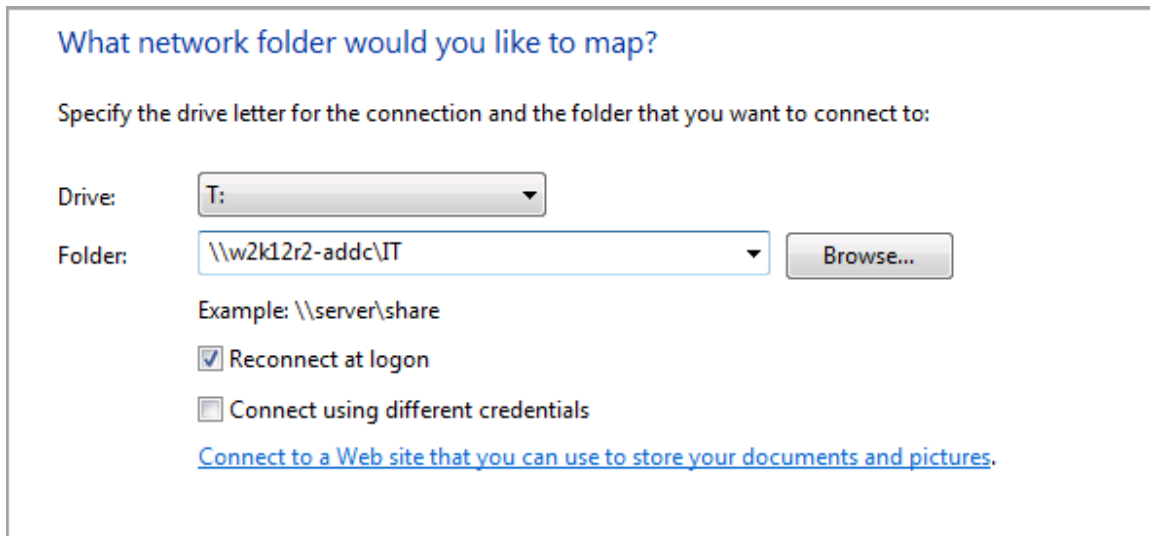
23. Left click the start button and select “Computer”.



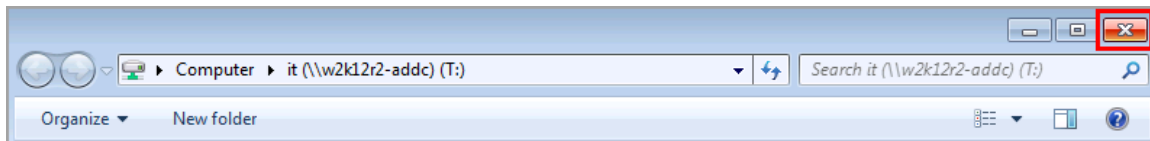
24. Select “Map network drive” from the navigation bar.



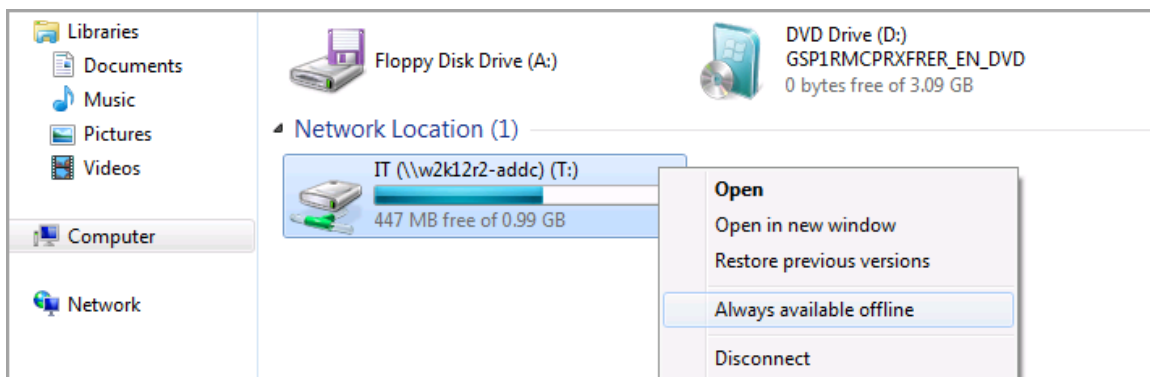
25. Change the drop down drive letter to T: and add the folder path [\\w2k12r2-addc\IT](#) and click “Finish”.



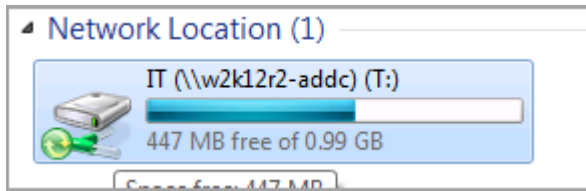
26. The shared location will automatically open. Close the share location window.



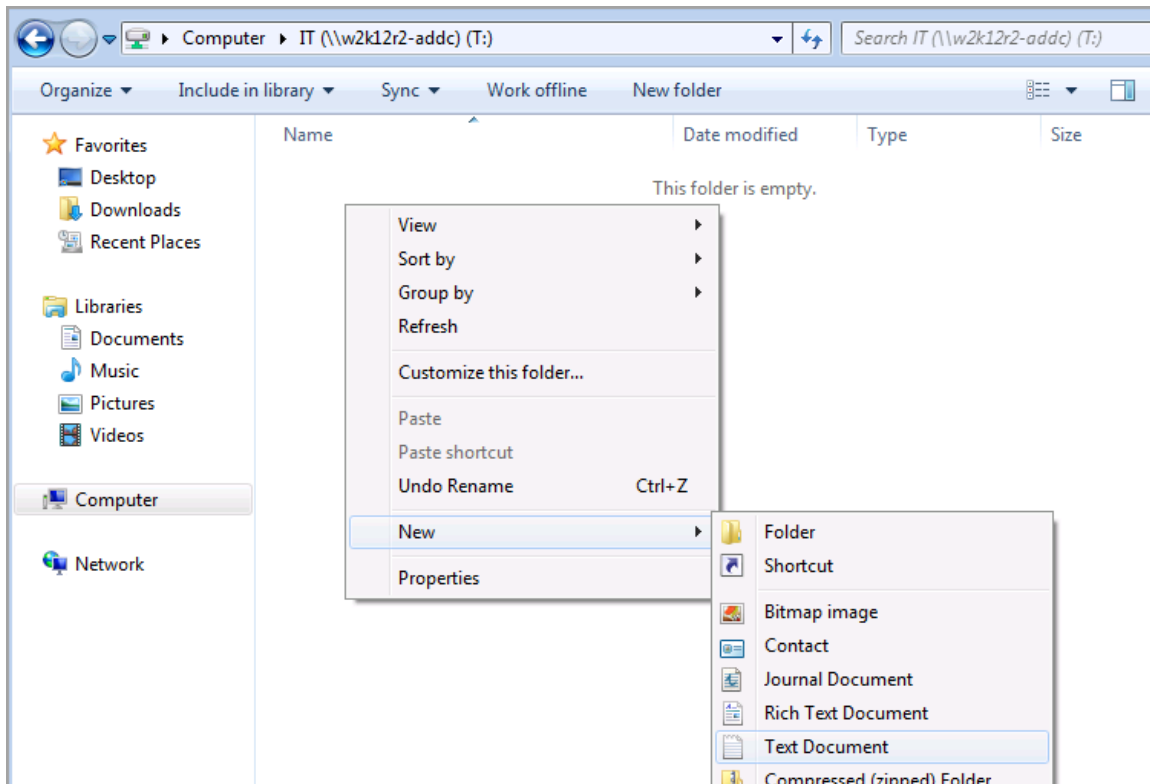
27. Right click on the new Network Location and select “Always available offline”



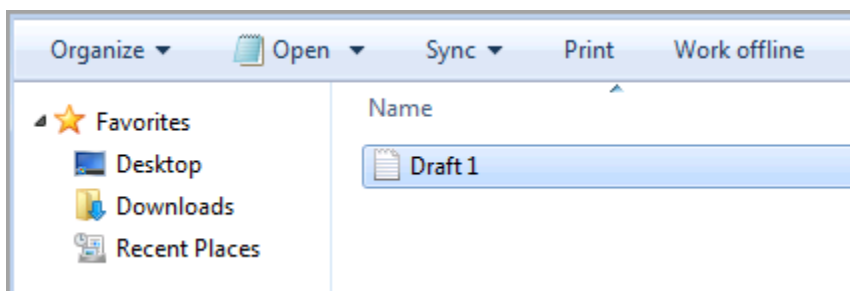
28. Double click on the shared location.



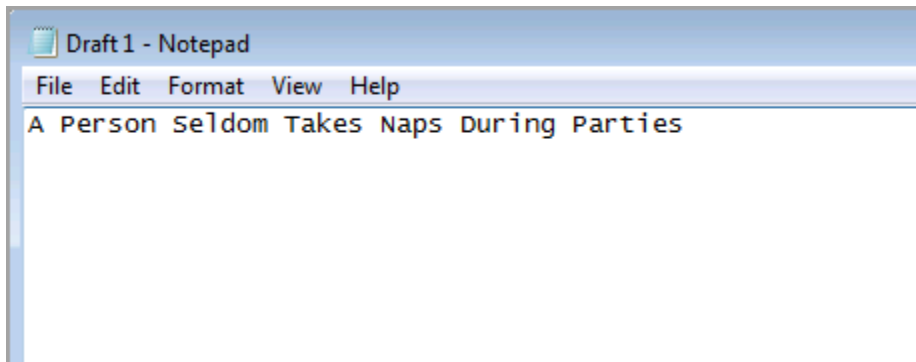
29. Right click in the open white space and select “New > Text Document”.



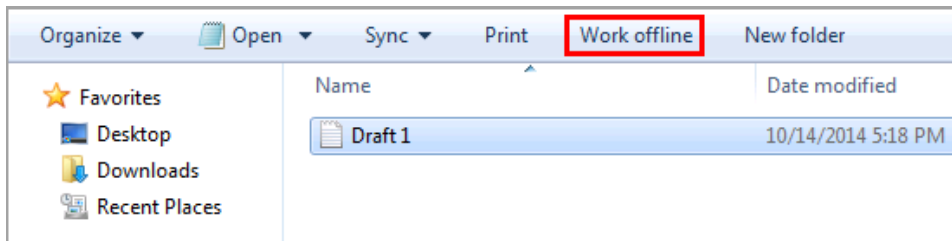
30. Name the document **Draft 1** and hit “Enter”.



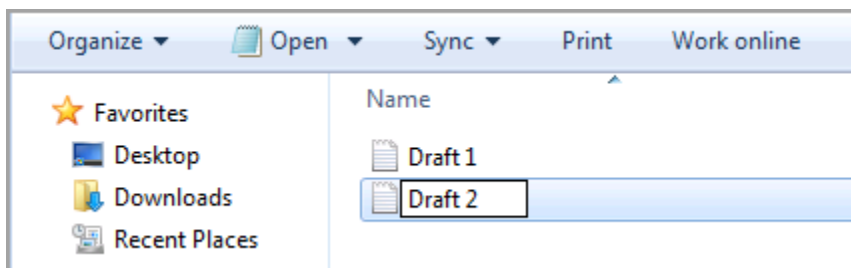
31. Double click “Draft 1” to open the document and type **A Person Seldom Takes Naps During Parties**. Click “File > Save”. Close “Draft 1 – Notepad”.



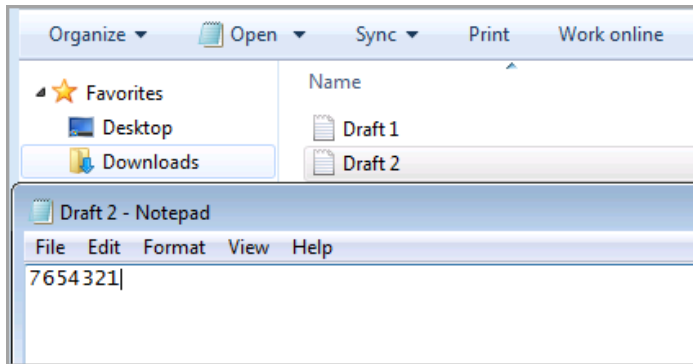
32. Click “Work offline” in the navigation bar.



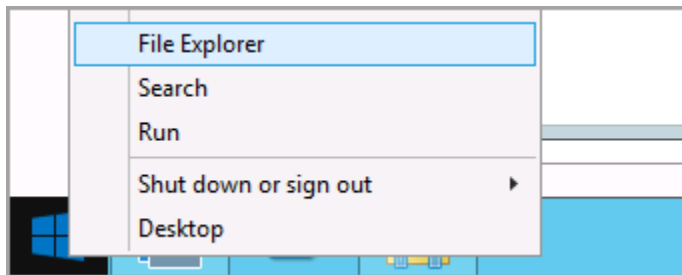
33. Right click under “Draft 1” and create a new text document called “Draft 2”.



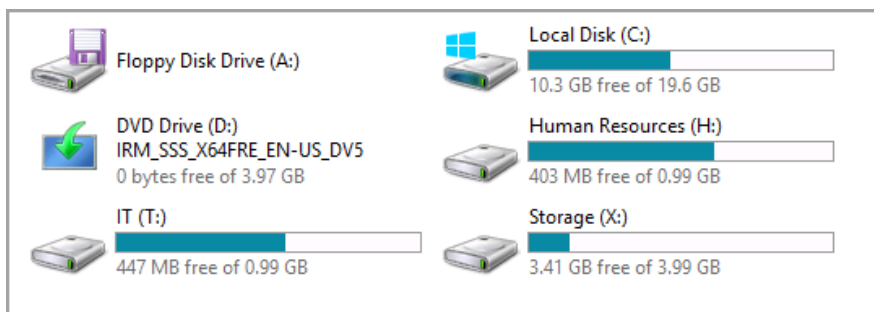
34. Double click “Draft 2” and type **7654321**. Click “File > Save”. Close “Draft 2 – Notepad”.



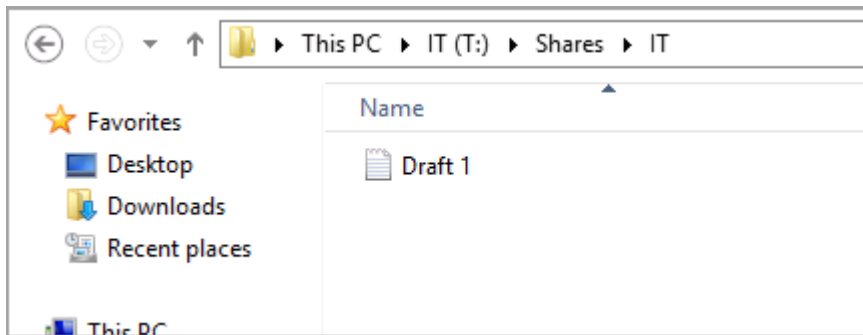
35. Open a console to W2K12R2-ADDC. Right click the Start Button and click “File Explorer”.



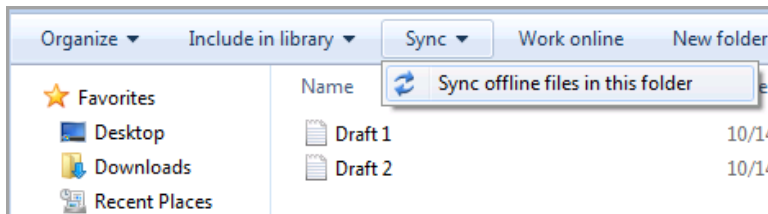
36. Double click the “IT (T:)” volume to open.



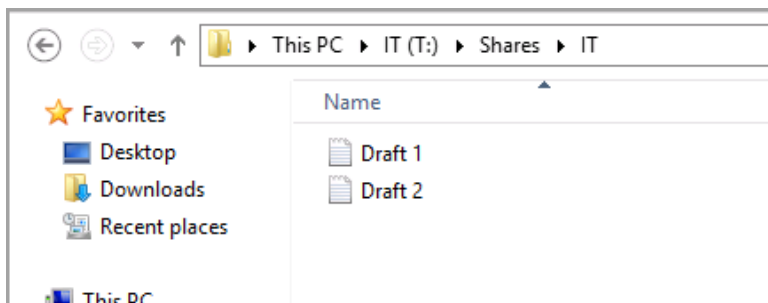
37. Double click on the “Shares” folder then double click on the “IT” folder. Notice that only Draft 1 has updated.



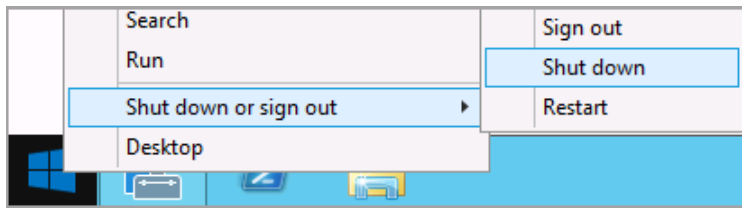
38. Return to the WIN7 machine and select “Sync > Sync offline files in this folder” from the navigation bar.



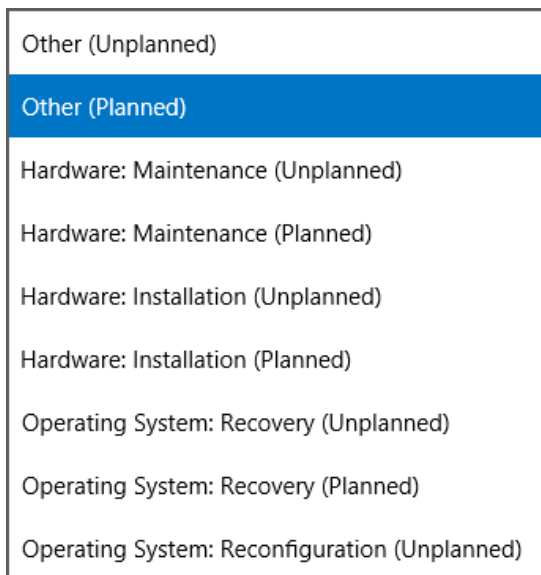
39. Return to the W2K12R2-ADDC machine to see the newly updated file.



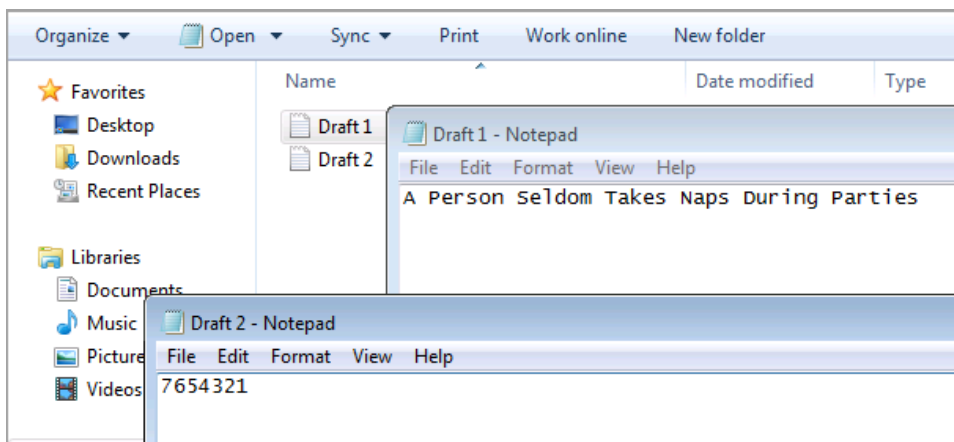
40. On the W2K12r2-ADDC machine, right click the start button and select “Shut down or sign out > Shut down”.



41. From the drop down, select “Other (Planned)”. Click “Continue”.

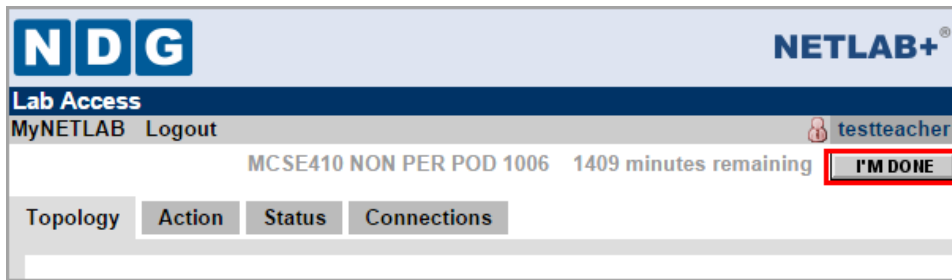


42. Return to the WIN7 machine and notice that both files are still available in offline mode.





Take any screenshots and notes required by your instructor and click “I’M DONE” at the top of the topology page. You may complete this lab as many times as you wish by making a new reservation.



## 4 Research Topics (Optional)

1. OneDrive
2. Share Point
3. Active Directory Federation Services

## References

1. Share and NTFS Permissions on a File Server  
<http://technet.microsoft.com/en-us/library/cc754178.aspx>
2. Work Folders  
<http://technet.microsoft.com/en-us/library/dn528861.aspx>

