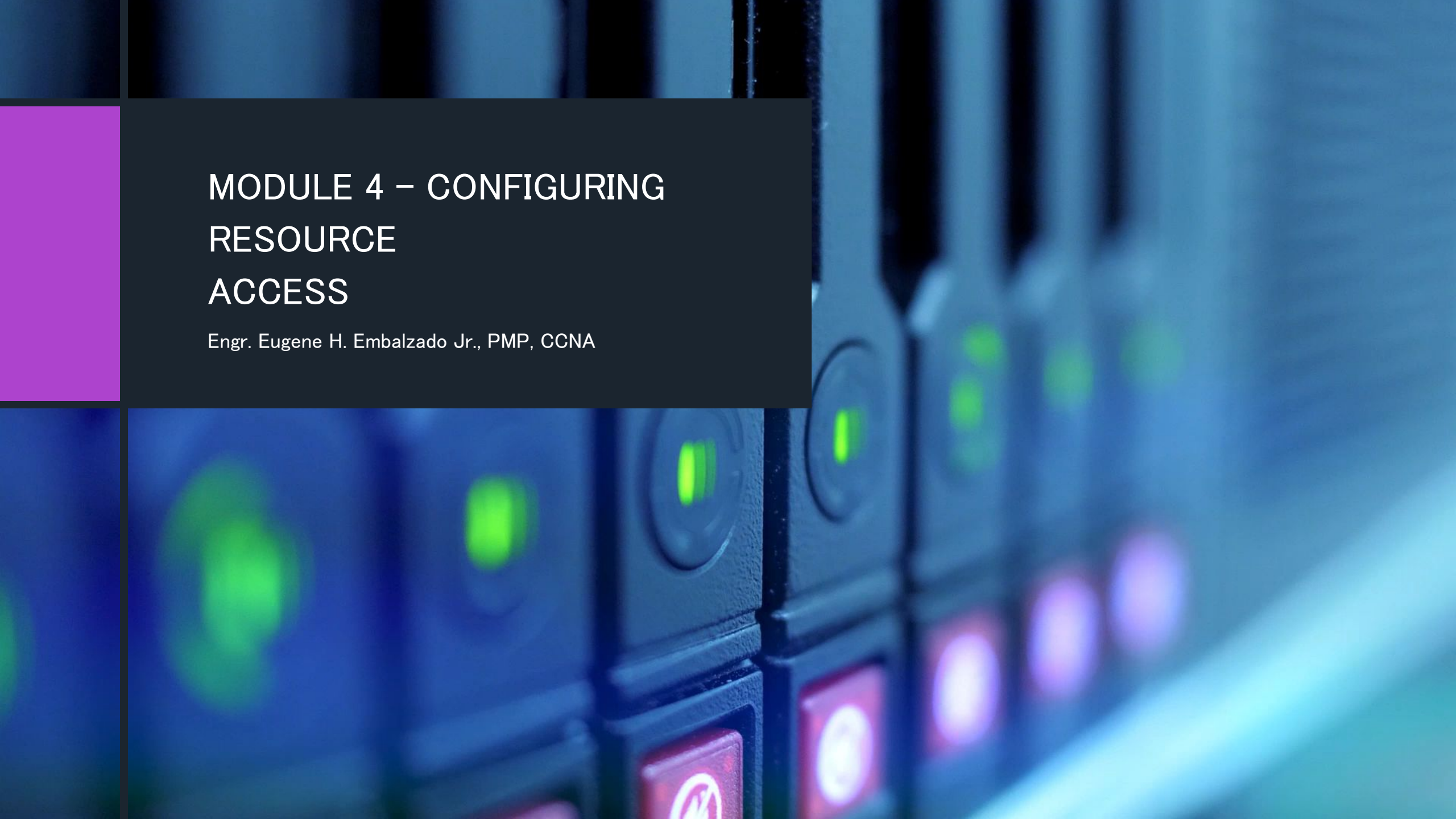
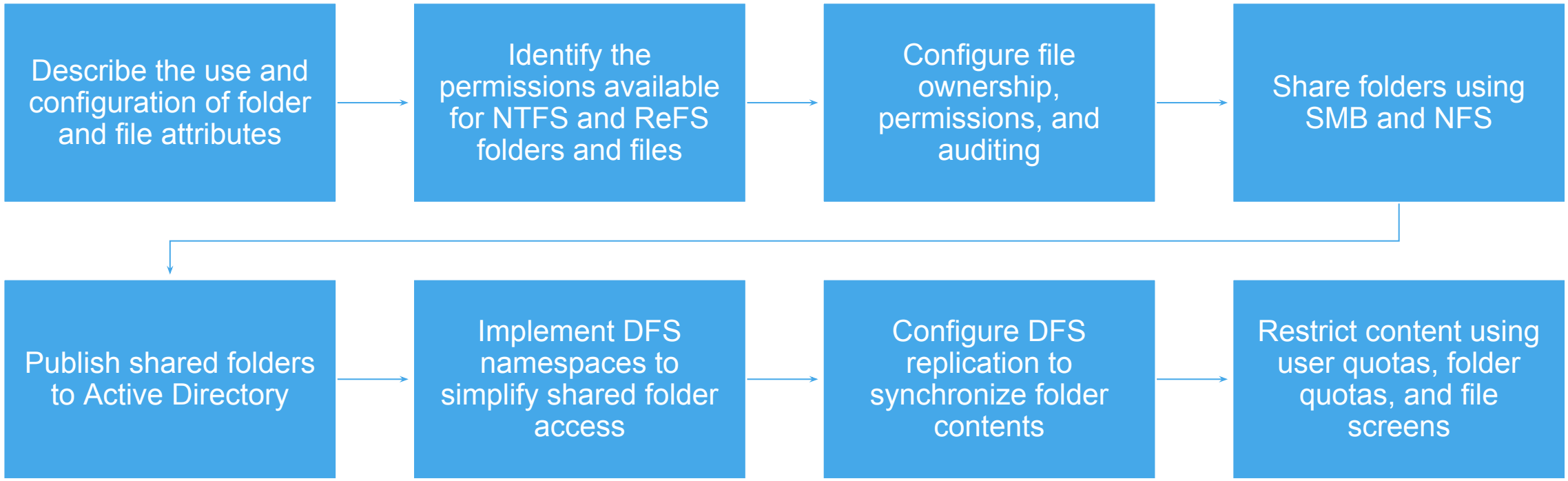


# MODULE 4 – CONFIGURING RESOURCE ACCESS

Engr. Eugene H. Embalzado Jr., PMP, CCNA

# Learning Objectives

After completing this module, you will be able to:

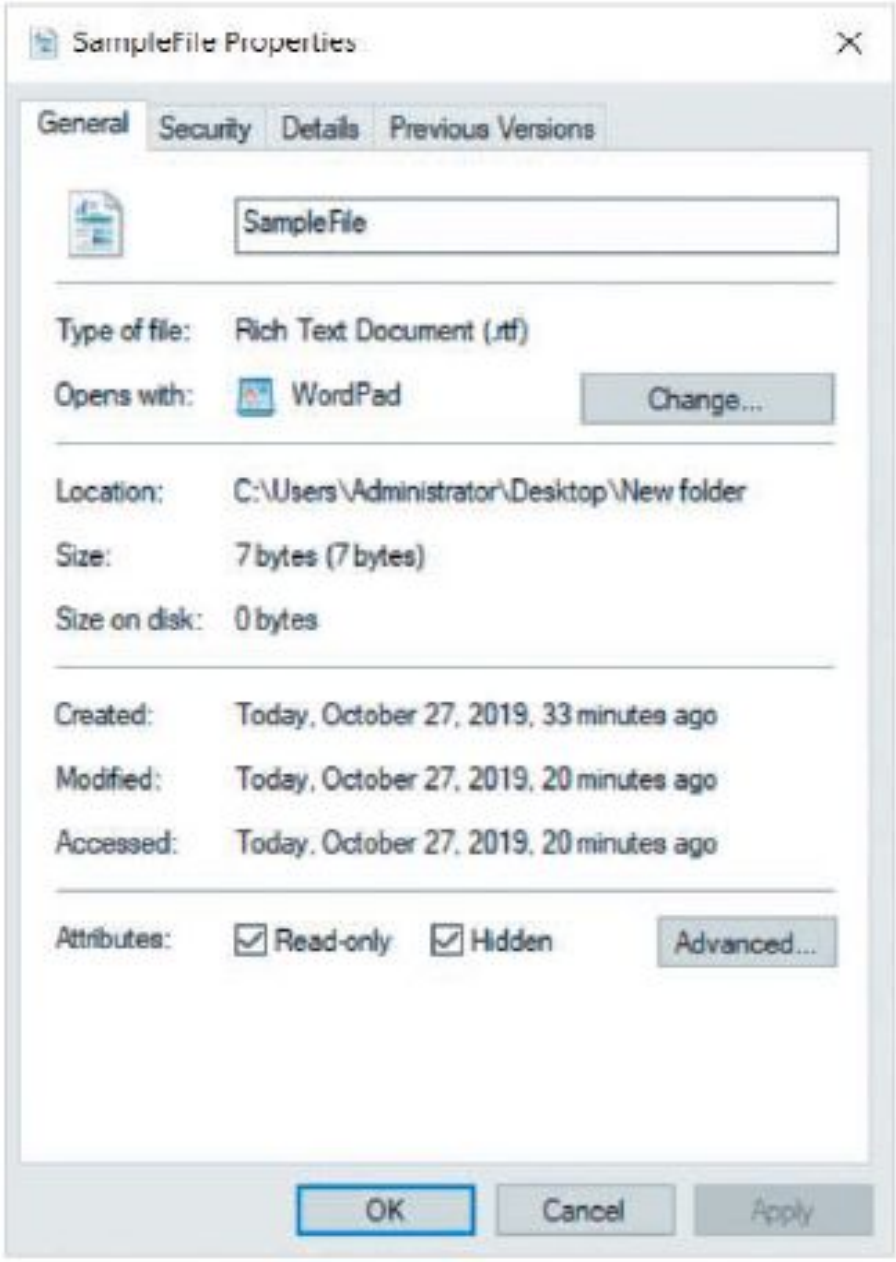


# Configuring Folder and File Attributes

- **Attributes -** features of a folder or file that are used by a filesystem.
- **Metadata-** component that stores information about the folder or file.
- **Attributes** are stored within this **metadata** component, along with other characteristics including ownership, permissions, date of creation, and time of last access.

# Working with Basic Attributes

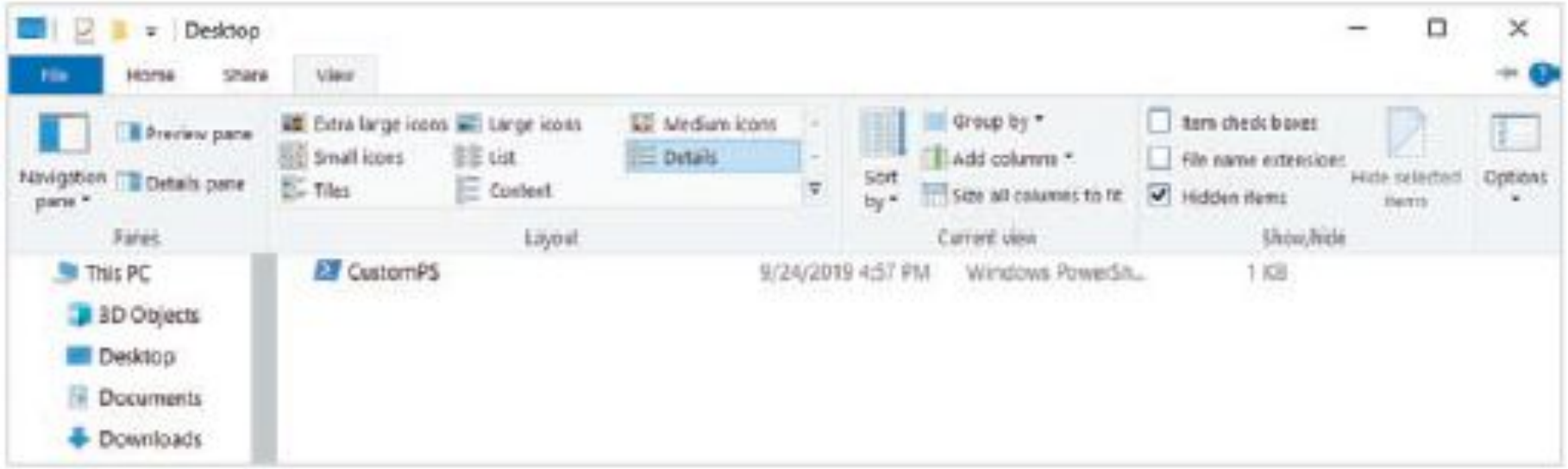
- **Main filesystems supported by Windows Server 2019**
  - NTFS **-** New Technology File System
  - ReFS **–** Resilient File System
  - FAT32 – File Allocation Table 32 (for local storage and removable media)
  - exFAT - capacity removable media.
- Two Basic Attributes: Read-only and Hidden
- Right-click a folder or file within a **File Explorer** window and click **Properties**



# Working with Basic Attributes

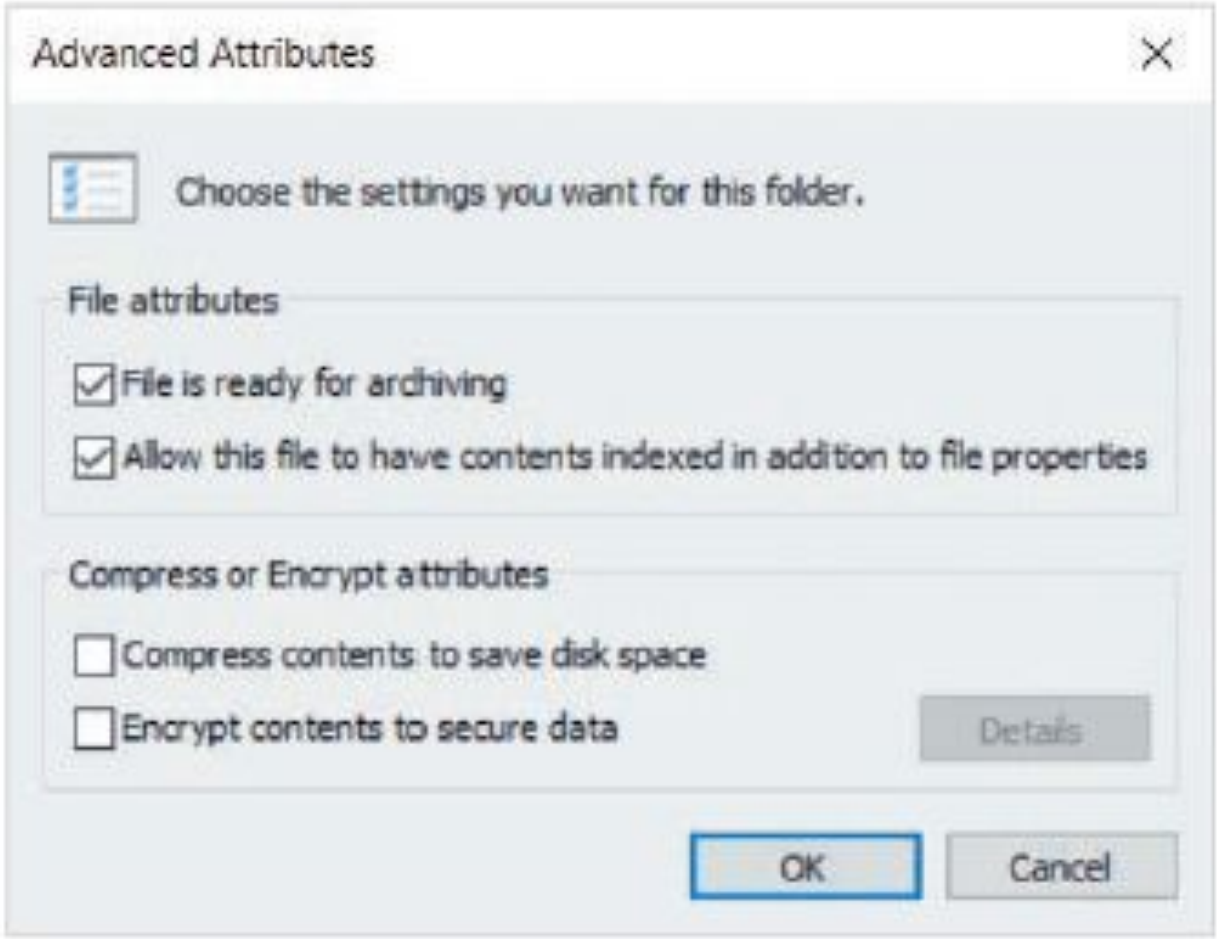
- **Read-only attribute**
- changes to its contents cannot be saved to the same file name
- cannot be deleted by using a command within a Windows PowerShell or Command Prompt but can be deleted within the File Explorer
- it applies to existing files within the folder only, and not the folder itself

- **Hidden attribute**
- Prevent users from listing their names
- Show hidden files
  - dir /ah MS-DOS command
  - Get-ChildItem –hidden Windows PowerShell command will display folders and files that have the hidden
  - clicking the View menu and enabling the Hidden items



# Working with Advanced Attributes

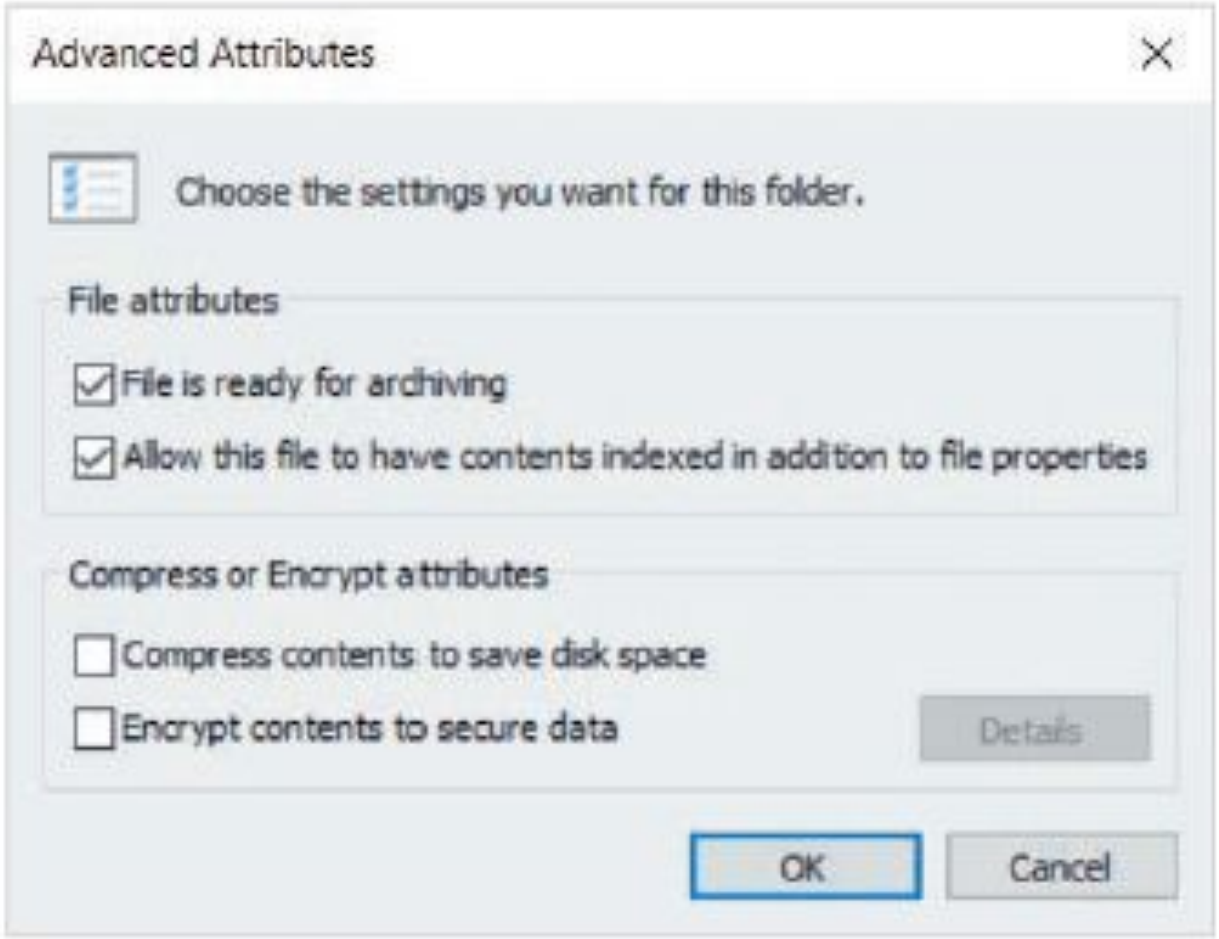
- NTFS offers four advanced attributes for folders and files: **archive, index, compress, and encrypt**.
- Click the Advanced button on the General tab for a folder or file




- **Archive Attribute**
  - (*File is ready for archiving)*
  - Folder or file needs to be backed up
  - automatically enabled on files, but not folders, when they are newly created or changed
  - You can also enable the archive attribute on the folder
  - File backup software can then be configured to detect files with the archive attribute to ensure that modified files are backed up

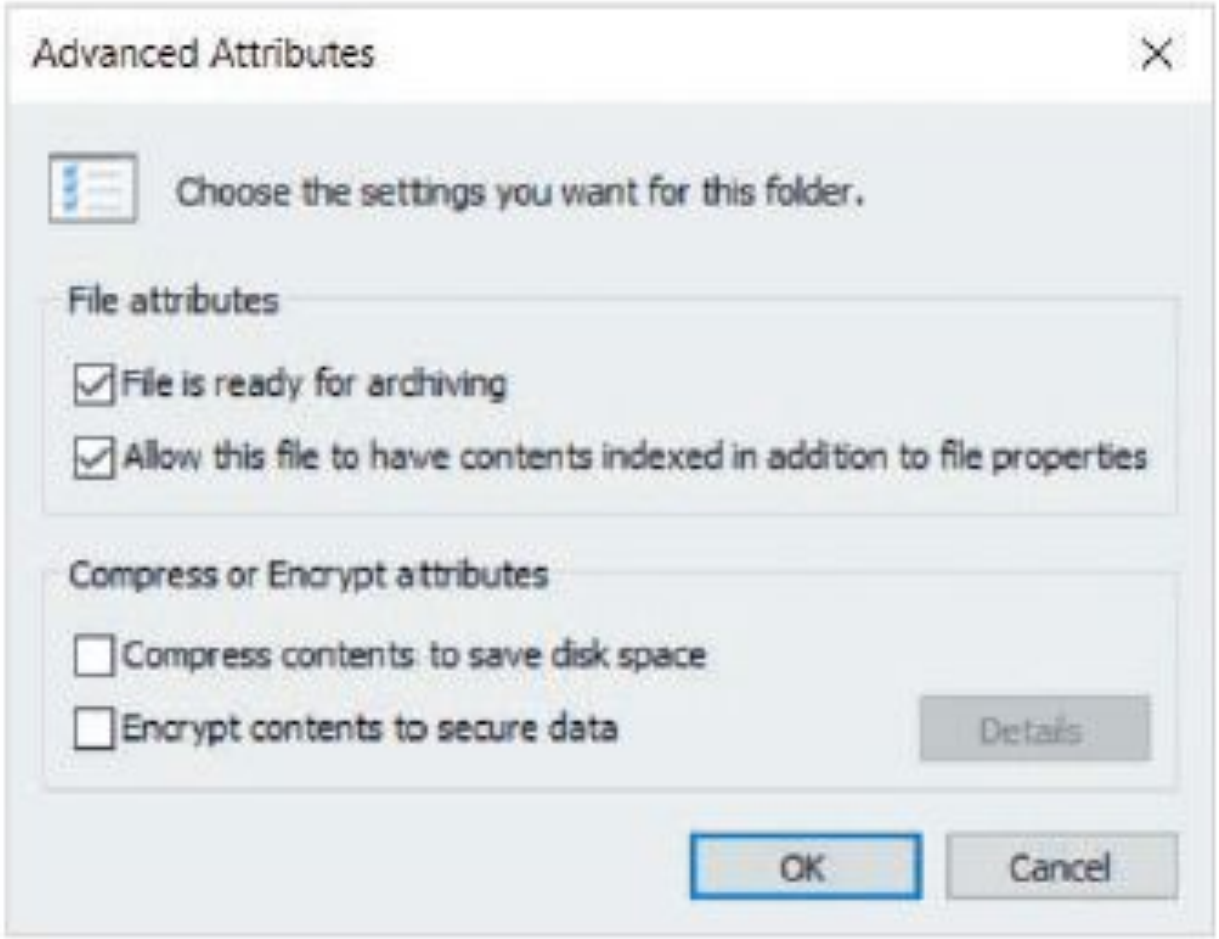
# Working with Advanced Attributes

- **Index Attribute**
  - (*Allow this file to have contents indexed in addition to file properties)*
  - When you search for files within File Explorer, the legacy Windows Indexing Service is used to obtain a list of files whose name or content matches your search based on a pre-created list called an **index**
  - **Windows Search Service -** faster replacement for the Windows Indexing Service that is available on Windows Server 2019
  - Commonly accessed user folders are indexed by default
  - System folders are excluded to help reduce the size of the index
  - Indexing Options tool within Control Panel to rebuild an index
  - All new files have the index attribute



# Working with Advanced Attributes

- **Encrypt Attribute**
  - (*Encrypt contents to secure data)*
  - **Encryption algorithm** - uses a series of mathematical steps in sequence to scramble data
  - Uses a random component called a **key** to modify the steps within the algorithm
    - Symmetric encryption - algorithms are reversible; data can be decrypted by reversing the algorithm using the same key that was used to encrypt it.
    - Asymmetric encryption - uses a pair of keys that are uniquely generated for a system or user account: a public key and a private key.
  - If you enable the encrypt attribute on a file, the system symmetrically encrypts the data within the file using a randomly-generated symmetric key that is stored in the file's metadata.
  - Next, the public key within your user account is used to asymmetrically encrypt the symmetric key stored within the file's metadata.

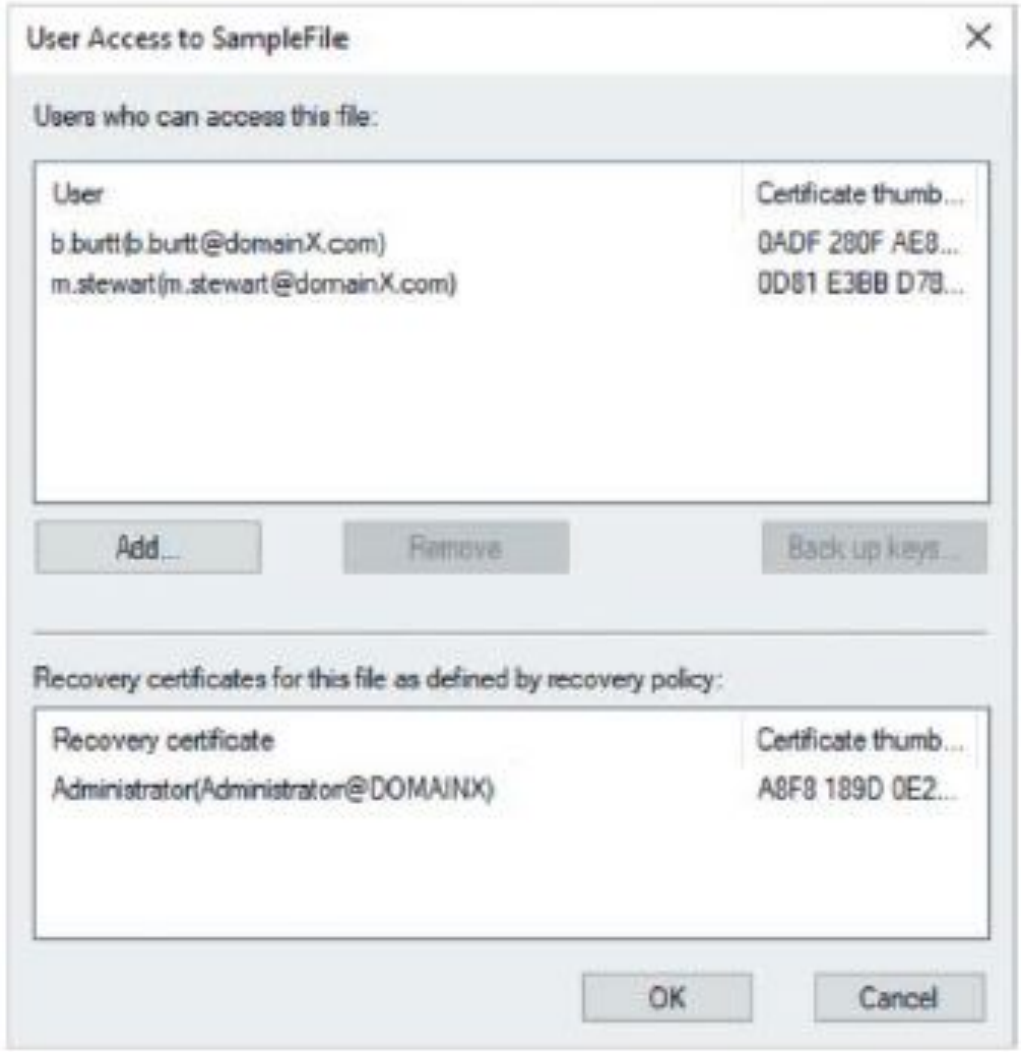


# Working with Advanced Attributes

- **Encrypt Attribute**
  - **Encrypting File System (EFS) -** filesystem feature works in workgroup or Active Directory domain environment
  - In a workgroup, your local user account stores your EFS public and private keys
  - However, within an Active Directory domain, these keys are stored within your domain user account such that you can access them from any computer within the forest.
  - The EFS private key is integrated into the password attribute of your user account
    - If a malicious user attempted to clear or reset your password using another utility, the private key is lost, and all EFS-encrypted files will not be readable.
    - This also means that if you reset a password for a local or domain user account, that user will not be able to access any of their EFS-encrypted files.
    - Recovery agent – a second copy of the symmetric key is added to the file's metadata and encrypted with a **recovery agent** public key.
    - The default recovery agent is the Domain Admins group in your domain. Any member of the Domain Admins group will be able to decrypt your EFS-encrypted files in the event that your password is reset

# Working with Advanced Attributes

- **Encrypt Attribute**
  - After encrypting a file using EFS, you can optionally allow other users to decrypt its contents.
  - Access the Advanced Attributes window, then click the Details button
  - When you copy or move an encrypted file to another folder within an NTFS, FAT32, or exFAT filesystem on the same computer or removable media, that file remains encrypted, even if you rename it.
  - The same holds true for copying or moving the file to a different NTFS, FAT32, or exFAT filesystem on another Windows 10, Windows Server 2016, or Windows Server 2019 system within the same Active Directory domain.
  - However, copying or moving files that does not support EFS will automatically decrypt file such as in Windows 7 below.

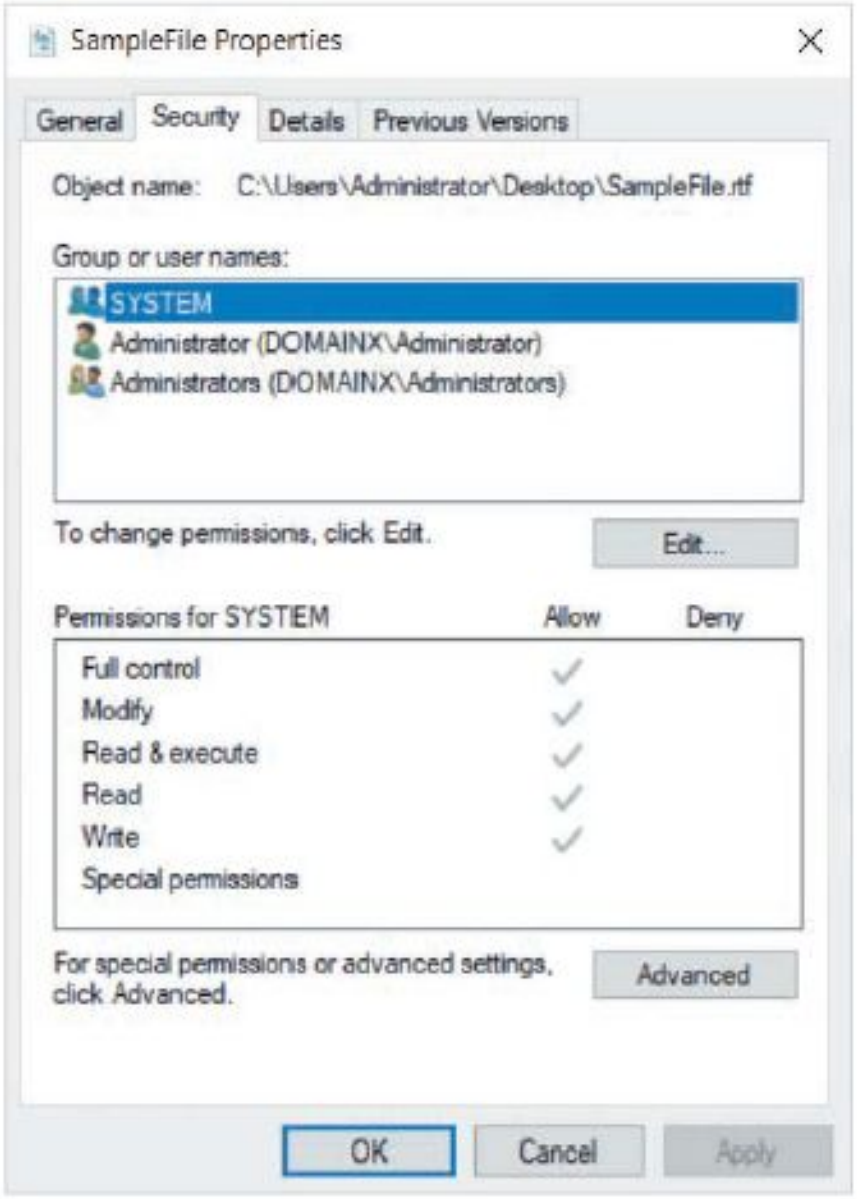


# Managing Folder and File Security

- **Two types of ACL:**
  - **Discretionary access control list (DACL)**
    - lists the permissions given to user and group accounts and is used to grant or deny access to the resource
  - **System access control list (SACL)**
    - contains information used to audit the access to the resource
    - For example, a soft drink company may decide to audit files that contain the secret recipes for their products. By configuring a SACL for each file containing a recipe, the company can monitor who has successfully viewed the file's contents and who has tried to view the contents but failed because of DACL restrictions. If no SACL is configured, auditing is disabled for the resource.
- When you create a resource, such as a file, folder, or printer, you become the owner of that resource by default.
- By default, the owner of a resource, the local Administrator user account (within a workgroup), and members of the Domain Admins group (within a domain) can change folder and file ownership as well as configure DACLs and SACLs.

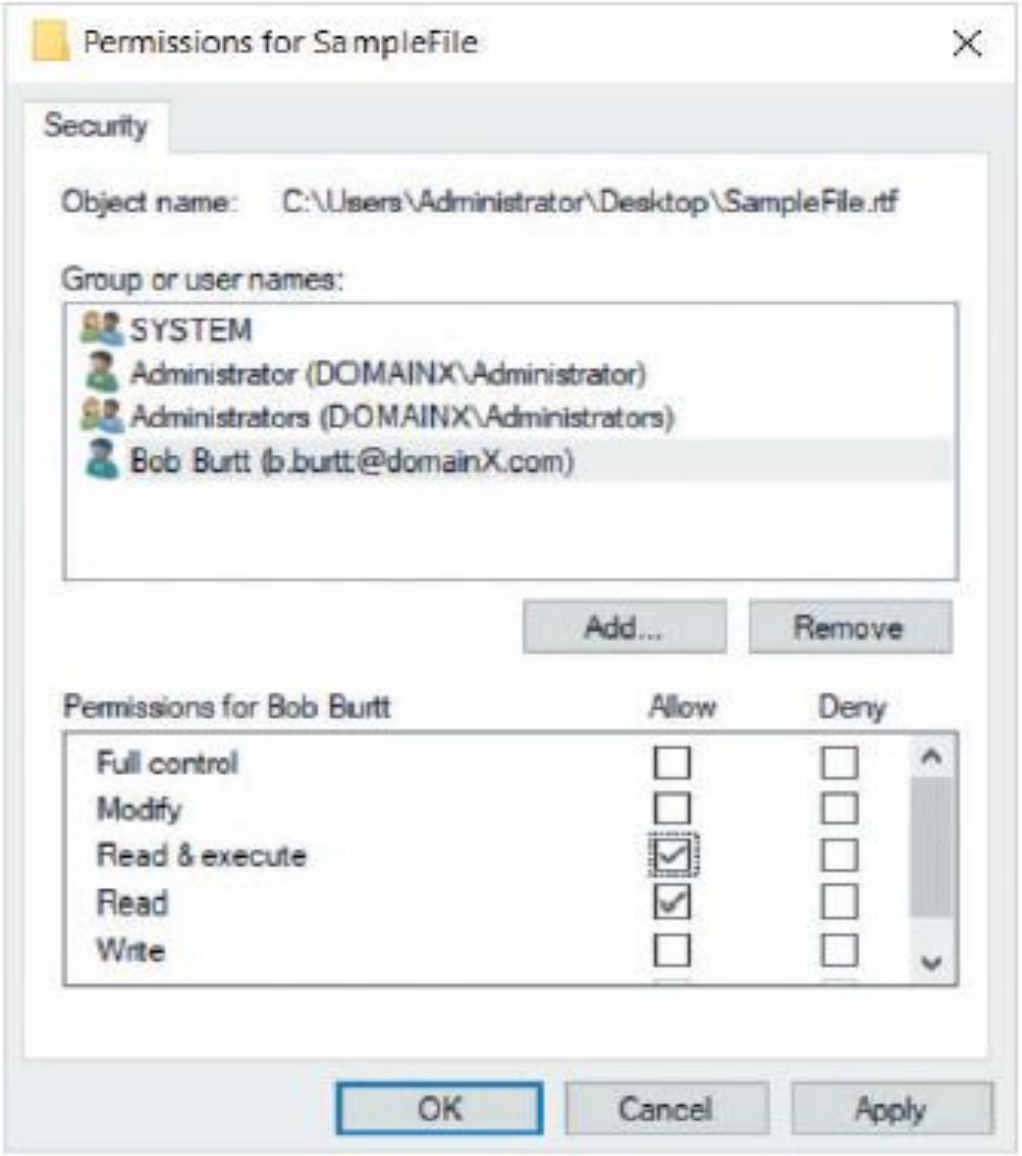
# Configuring Folder and File Permissions

- To view and configure the DACL for a folder or file on an NTFS or ReFS filesystem, you can right-click the folder or file within a File Explorer window and click Properties.
- Built-in SYSTEM group (represents operating system components)
- These permissions are grey, which indicates that they were not set on the SampleFile.rtf directly but instead were inherited from the parent folder that contains SampleFile.rtf.



# Configuring Folder and File Permissions

- To add additional permissions for users or groups, you can click Edit. This will open the Permissions window shown where you can add or remove existing users or groups as well as set their permissions.
- The Bob Burtt user shown was added to the DACL and granted Read & execute permission (which also grants Read permission).
- Notes:
  - You receive the permissions on a folder or file that are assigned to your user account as well as any group accounts that you belong to. For instance, if your user account is granted Read permission to a file and a group that your user account belongs to is granted Full control to the same file, you effectively receive Full control when accessing the file.
  - When you set permissions on a folder, those permissions are inherited by default to files and subfolders.



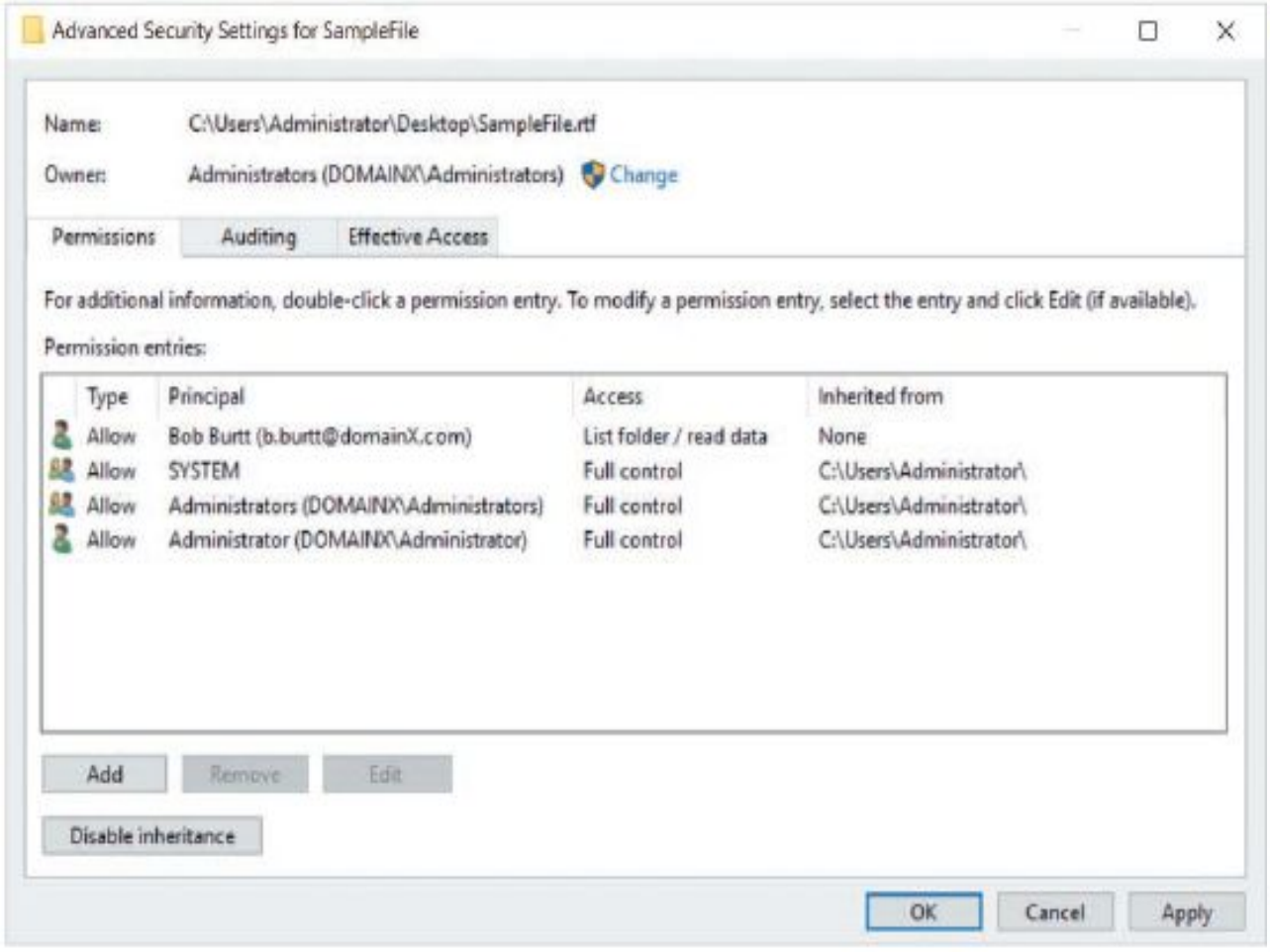
# Configuring Folder and File Permissions

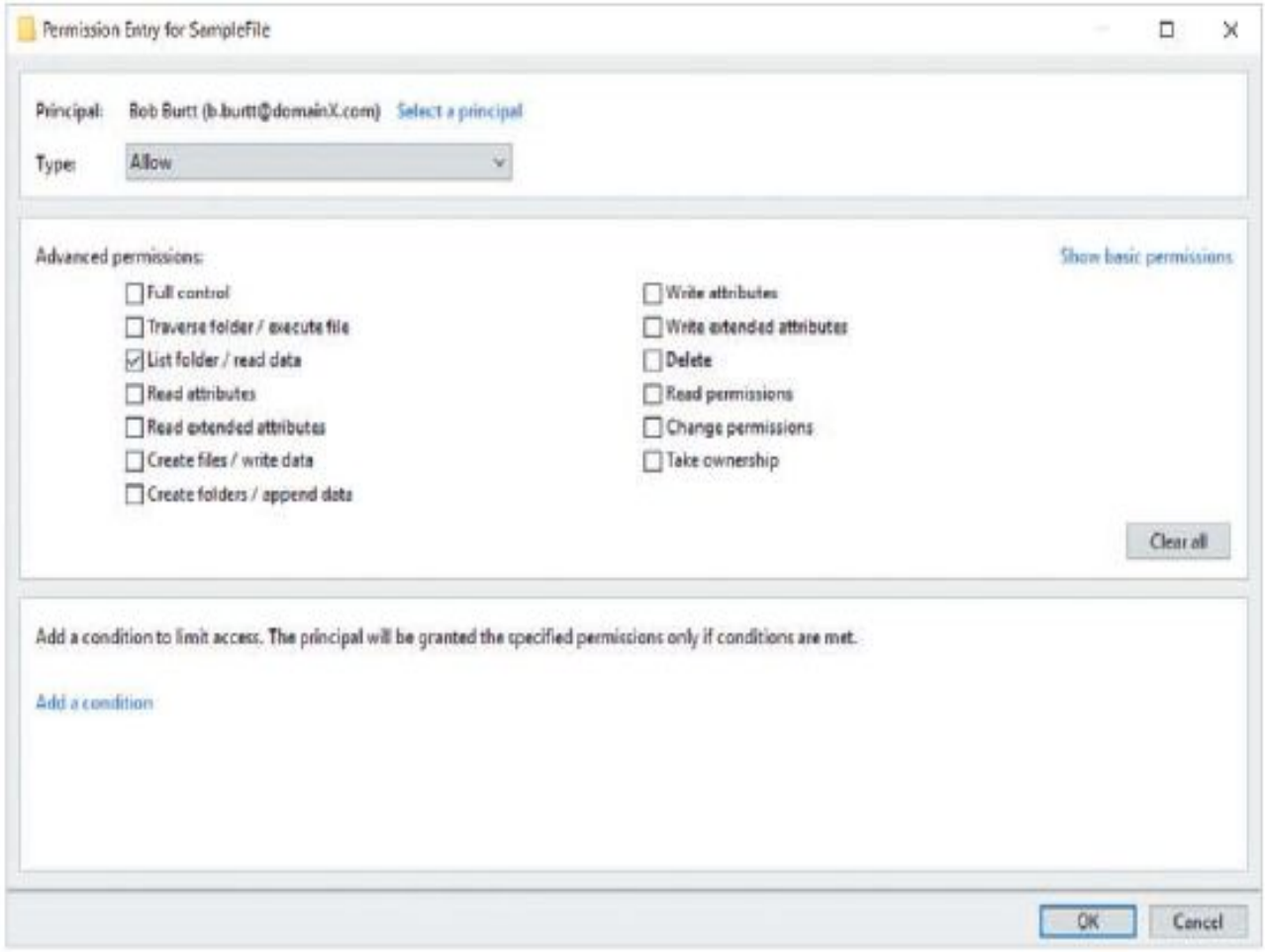
**Table 5-1** NTFS/ReFS folder and file permissions

| Permission | Description | Applies to |
|---|---|---|
| Full control | Can read, add, delete, execute, and modify files, change permissions and attributes, and take ownership | Folders and files |
| Modify | Can read, add, delete, execute, and modify files; cannot change permissions or take ownership | Folders and files |
| Read and execute | Implies the capabilities of both List folder contents and Read (traverse folders, view file contents, view attributes and permissions, and execute files) | Folders and files |
| List folder contents | Can list (traverse) files in the folder or switch to a subfolder, view folder attributes and permissions, and execute files; cannot view file contents | Folders only |
| Read | Can view file contents, as well as view file and folder attributes and permissions; cannot traverse folders or execute files | Folders and files |
| Write | Can create files, write data to files, append data to files, create folders, and modify folder and file attributes; cannot delete files | Folders and files |
| Advanced permissions | Advanced permissions apply (see Table 5-2) | Folders and files |

# Configuring Folder and File Permissions

- If the basic permissions do not suit your needs, you can modify the DACL to set advanced permissions.
- Click Advanced to open the Advanced Security Settings window shown on the left. Click Add, you will access the Permission Entry window shown on the right. At this window, you can select a security principal, whether to allow or deny permissions to the security principal, as well as the associated permissions.
- Click Disable inheritance to prevent parent folder permissions from being inherited to the file.



# Configuring Folder and File Permissions

**Table 5-2** NTFS folder and file advanced permissions

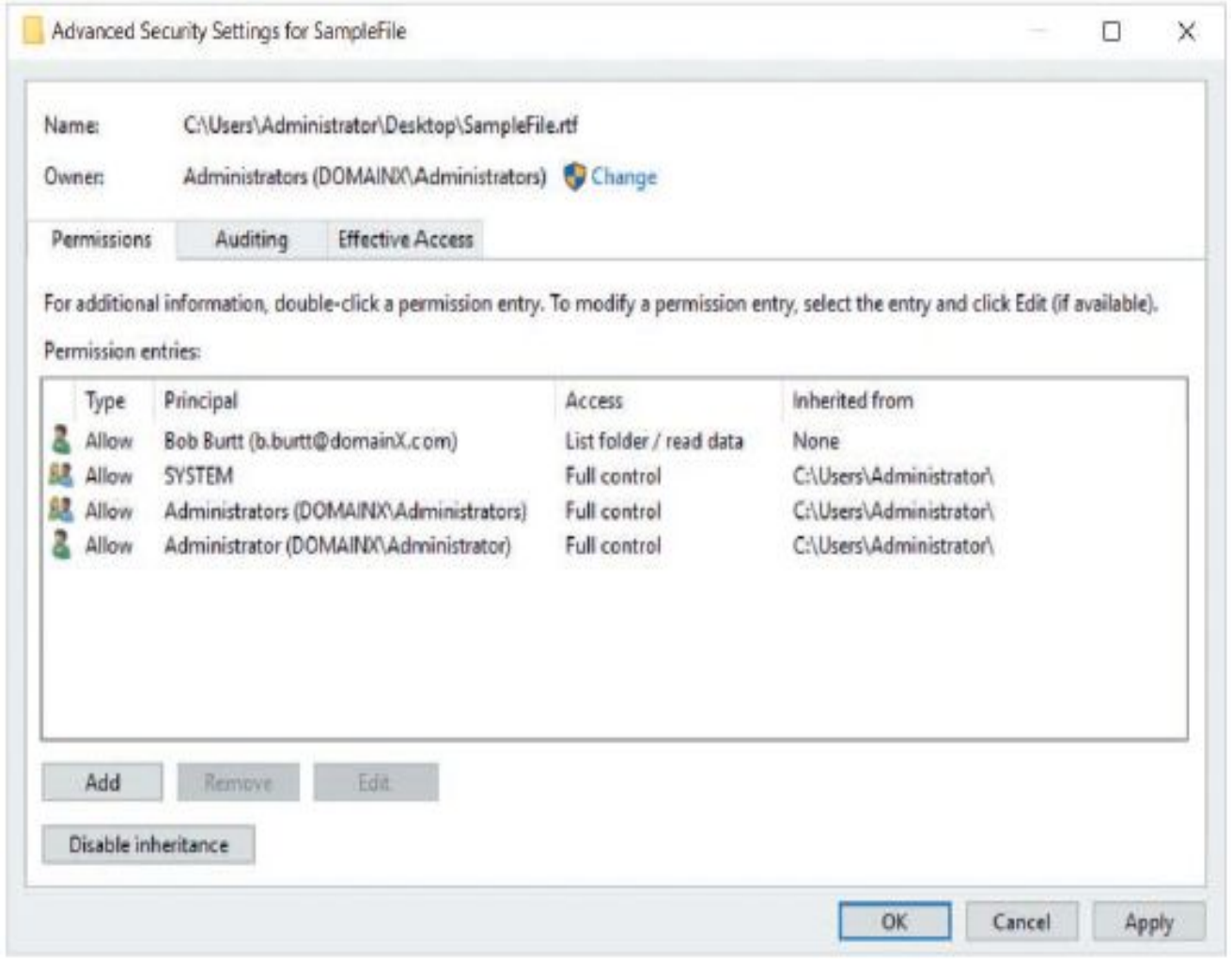
| Permission | Description | Applies to |
|---|---|---|
| Full control | Can read, add, delete, execute, and modify files, as well as change permissions and attributes, and take ownership | Folders and files |
| Traverse folder/execute file | Can list the contents of a folder and run program files in that folder | Folders and files |
| List folder/read data | Can list the contents of folders and subfolders and read the contents of files | Folders and files |
| Read attributes | Can view the read-only and hidden attributes | Folders and files |
| Read extended attributes | Can view extended attributes (archive, index, compress, and encrypt) | Folders and files |
| Create files/write data | Can add new files to a folder and modify, append to, or write over file contents | Folders and files |
| Create folders/append data | Can add new folders and add new data at the end of files, but otherwise cannot delete, write over, or modify data | Folders and files |
| Write attributes | Can add or remove the read-only and hidden attributes | Folders and files |
| Write extended attributes | Can add or remove the archive, index, compress, and encrypt attributes | Folders and files |
| Delete subfolders and files | Can delete subfolders and files (the following Delete permission is not required) | Folders and files |
| Delete | Can delete the specific subfolder or file to which this permission is attached | Folders and files |
| Read permissions | Can view the permissions (DACL) associated with a folder or file, but cannot change them | Folders and files |
| Change permissions | Can change the permissions associated with a folder or file | Folders and files |
| Take ownership | Can take ownership of the folder or file (read permissions and change permissions automatically accompany this permission) | Folders and files |

# Configuring Folder and File Permissions

- Remember:
- Always err on the side of too much security. It is easier, in terms of human relations, to give users' permissions later than it is to take away existing permissions.

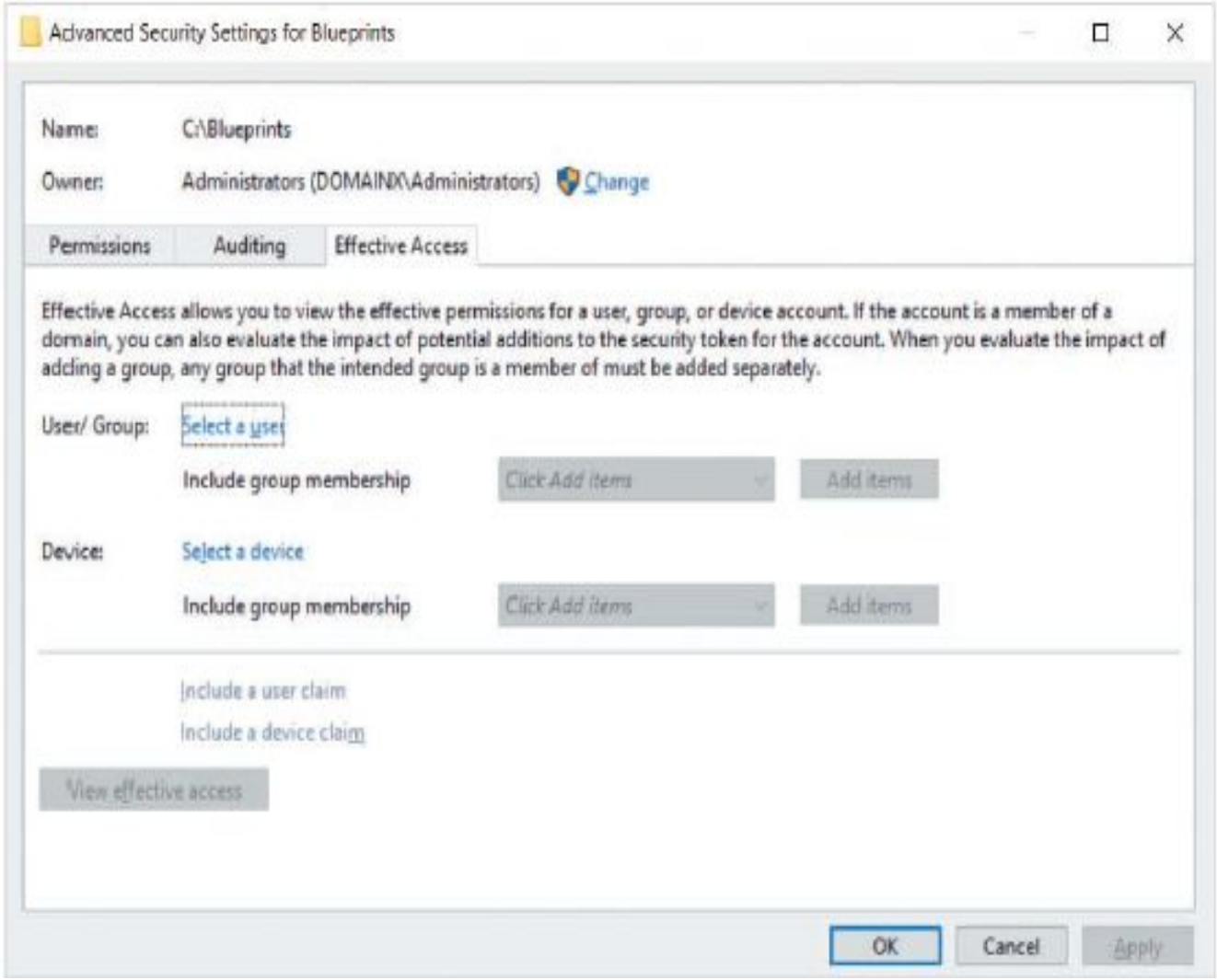
# Configuring Folder and File Ownership

- Each folder and file on a system must have an owner, which, by default, is the user that created the file.
- The owner of a folder or file can change the ownership to another user.
- If you are granted the Take ownership advanced permission or Full control permission (which includes Take ownership) to a folder or file, you can change the owner of it to yourself..
- After you are the owner of that folder or file, you have the ability to change the permissions on it.
- To modify the owner of a folder or file, you can access the Advanced Security Settings window, click Change next to the current owner, and specify the new owner.



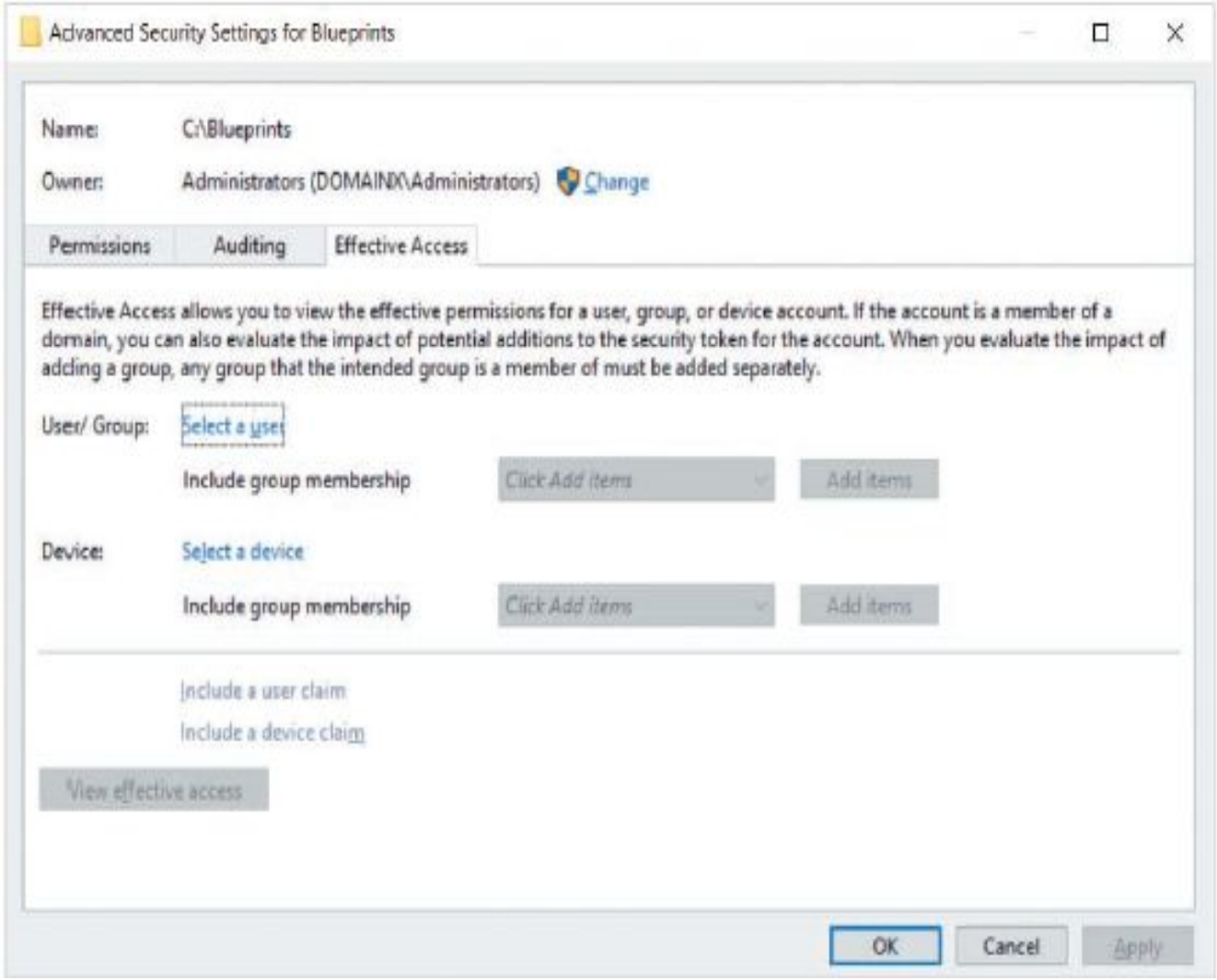
# Troubleshooting Folder and File Permissions

- Use Case:
- User within your organization requires the ability to maintain all files within the C:\Blueprints folder. As a result, you grant the user Modify permission to the folder. However, when that user attempts to access the C:\ Blueprints folder, they receive an access denied message because their user account is also a member of a group that has been denied Modify permission to the C:\Blueprints folder.



# Troubleshooting Folder and File Permissions

- To troubleshoot this problem, you should review the permissions that have been assigned on the C:\Blueprints folder to the user, as well as all groups to which the user belongs, taking permission inheritance into consideration.
- Alternatively, you can access the Advanced Security Settings window for the C:\Blueprints folder and highlight the Effective Access tab, as shown.
- You can click Select a user to choose the appropriate user account, and then click View effective access to list the effective permissions that the user has to the C:\Blueprints folder after permissions (including inherited permissions) for the user and all groups that they are a member of have been applied.



# Troubleshooting Folder and File Permissions

- When a file or folder is created, copied, or moved, the file and folder permissions are affected in the following ways:
  - A newly created file inherits the permissions configured on its folder.
  - A file that is copied from one folder to another on the same volume inherits the permissions configured on the folder to which it is copied.
  - A file or folder that is moved from one folder to another on the same volume retains its original permissions. For example, if a file assigns Read permission to the Accounting group, and it is moved to a folder that assigns Modify to the Accounting group, that file will continue to assign Read permissions to the Accounting group.
  - A file or folder that is moved or copied to a folder on a different volume inherits the permissions of the folder to which it is moved or copied.
  - A file or folder that is moved or copied from an NTFS or ReFS volume to a folder on a FAT32 or exFAT volume, all permissions are removed because FAT32 and exFAT do not support NTFS/ReFS permissions.
  - A file or folder that is moved or copied from a FAT32 or exFAT volume to a folder on an NTFS or ReFS volume inherits the permissions of the folder to which it is moved or copied.

# Configuring Folder and File Auditing

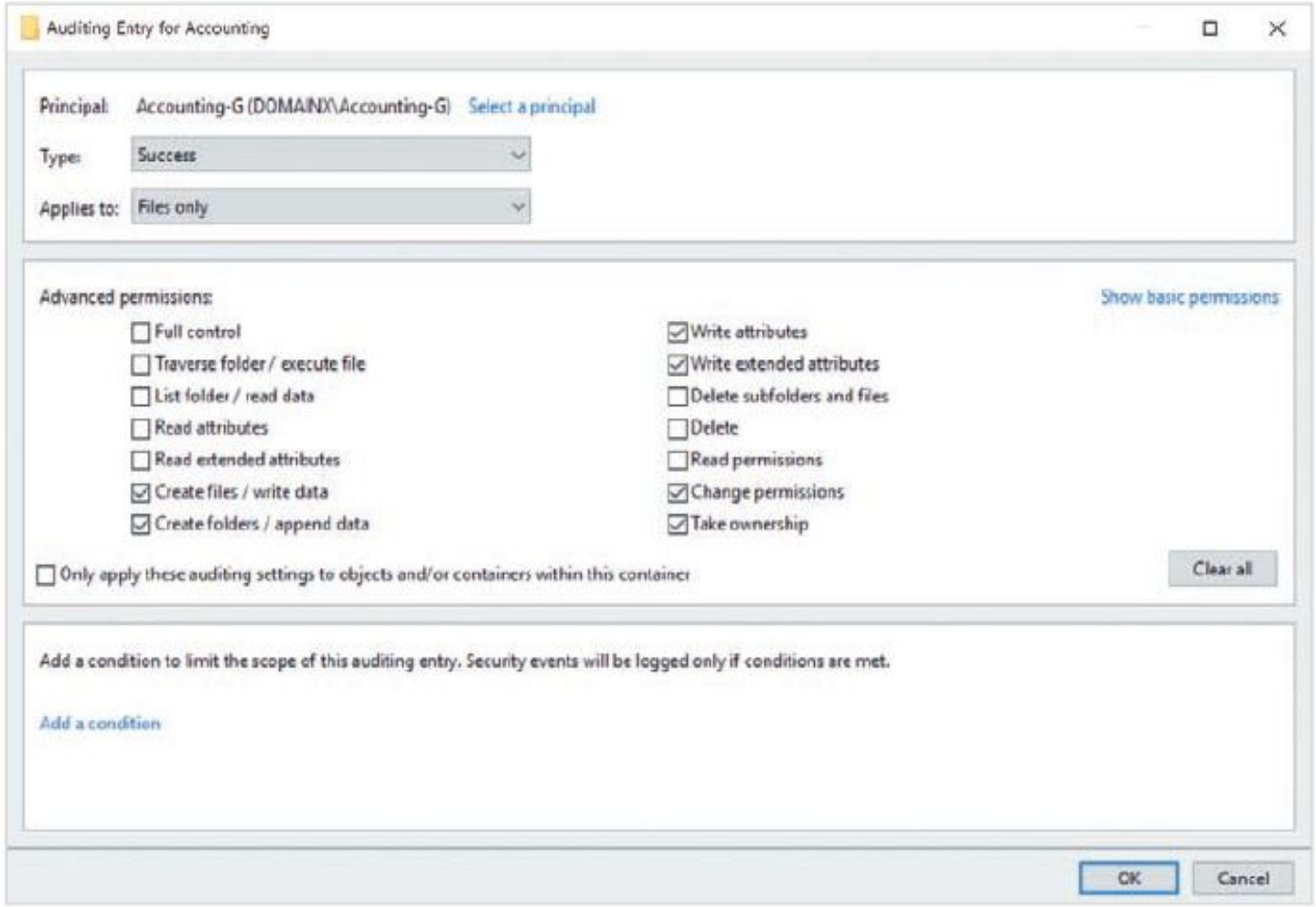
- Folder and file auditing allows you to track activity on a folder or file, such as read or write activity. Some organizations choose to implement auditing on folders and files that involve financially sensitive information, such as those involving accounting and payroll.
- Other organizations configure auditing to see which users access information, such as a folder containing files of employee guidelines and announcements, to determine if it is being used.

# Configuring Folder and File Auditing

- Consider a situation in which your organization’s financial auditors require you to record each time any files in the C:\Accounting folder are changed by a user within the Accounting-G group that has access to them.
- You could configure the folder’s security to audit each successful type of write event, including those that require the Create files / write data and Create folders / append data advanced permissions

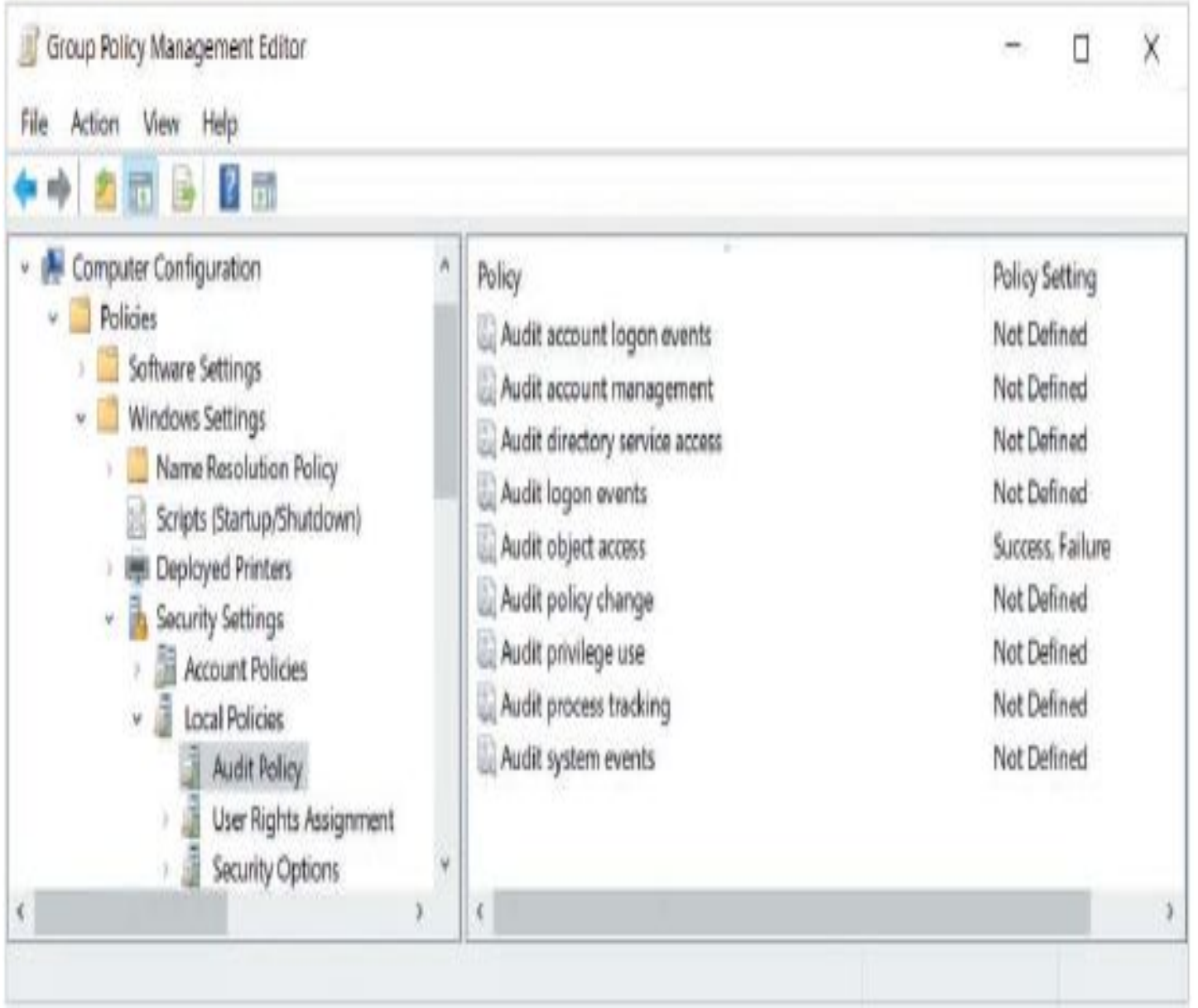
# Configuring Folder and File Auditing

- Access the Advanced Security Settings window for the C:\Accounting folder, highlight the Auditing tab, and click Add.
- This will open the Auditing Entry window, where you can make the selections shown (you must first click Show advanced permissions to select advanced permissions).



# Configuring Folder and File Auditing

- Because auditing requires additional processor calculations and storage, it is not enabled on Windows Server 2019 by default. To enable auditing functionality, you must edit the audit policy within a Group Policy object that applies to your computer.
- To do this, you can select Group Policy Management from the Tools menu within Server Manager.
- Within the Group Policy Management tool, you can navigate to, and expand, your domain object, right-click Default Domain Policy, and click Edit. This will open the Group Policy Management Editor tool, where you can navigate to the Audit Policy section shown. Finally, you can right-click the Audit object access policy setting in the right pane and click Properties to enable auditing for success or failure events, or both.
- The Audit object access policy setting shown in enables auditing functionality for both success and failure events.

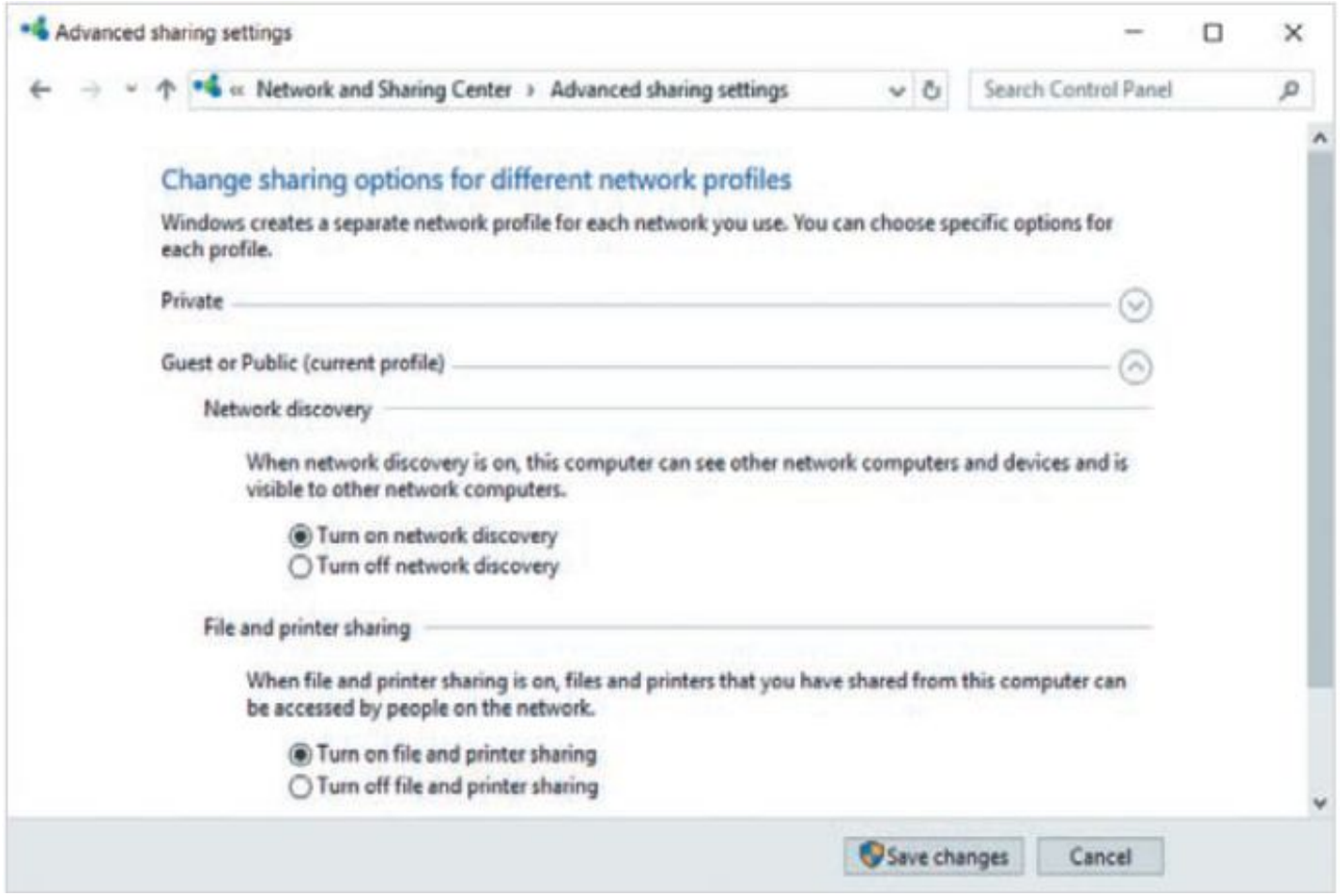


# Configuring Shared Folders

- To allow users to access the files within a folder on your Windows Server 2019 system from across a network, you must share the folder. Furthermore, there are two different protocols that can be used to share folders on Windows Server 2019 systems: **Server Message Block (SMB)** and **Network File System (NFS)**.
- Originally developed by IBM, SMB is the default file sharing protocol used by Windows systems
- NFS is a UNIX file sharing protocol that was introduced by Sun Microsystems and can be installed on Windows Server 2003 and later systems.

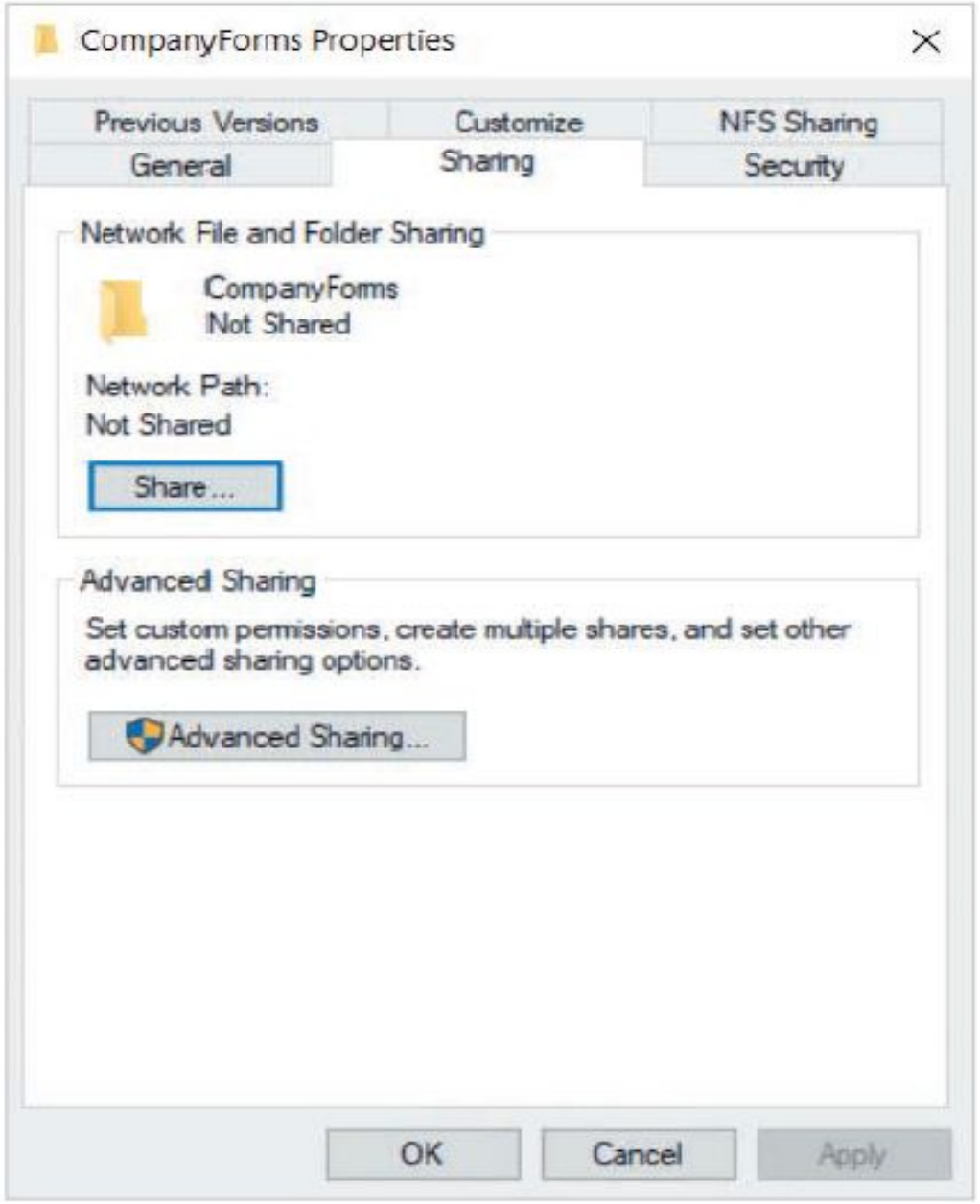
# Sharing Folders Using SMB

- After you install Windows Server 2019, SMB sharing is enabled by default.
- To enable or disable SMB sharing for your current network profile, you can open Control Panel in category view and navigate to Network and Internet, Network and Sharing Center.
- Within the Network and Sharing Center, you can then click *Change advanced sharing settings* to modify the SMB sharing settings shown.
- If SMB sharing is enabled on your system, you can easily share a folder by accessing the properties of the folder or by using Server Manager.



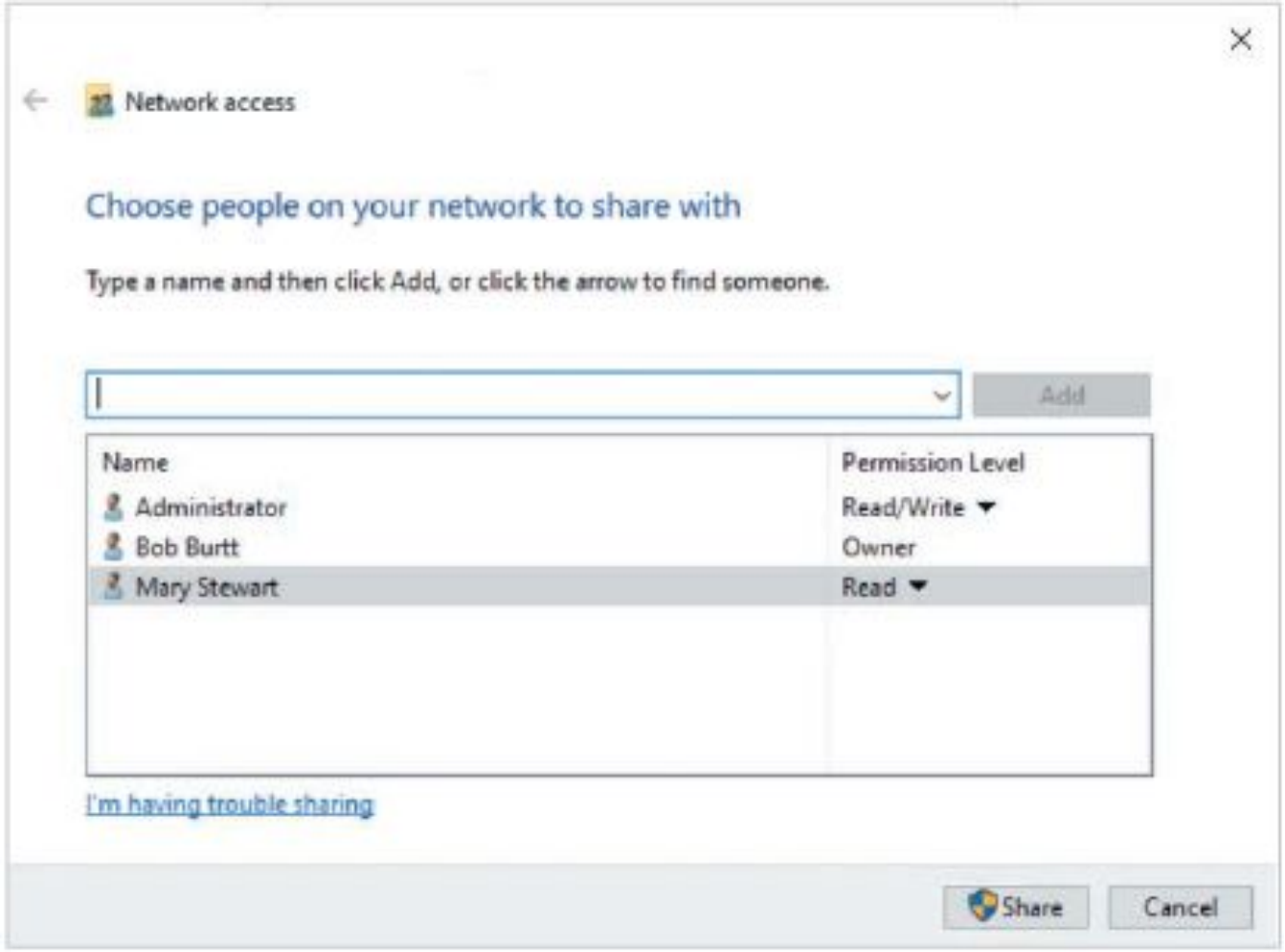
# Sharing a Folder Using Folder Properties

- **To share a folder using SMB, you can right-click the folder, click Properties, and highlight the Sharing tab.**
- **On the right shows the Sharing tab for the C:\CompanyForms folder on SERVERX.**
- If you click the Share button in Figure 5-13, you will see the Network access window shown on next slide
- You can then type a user or group name within the text dropdown box, click Add, and specify the level of permission that they have to the shared folder.



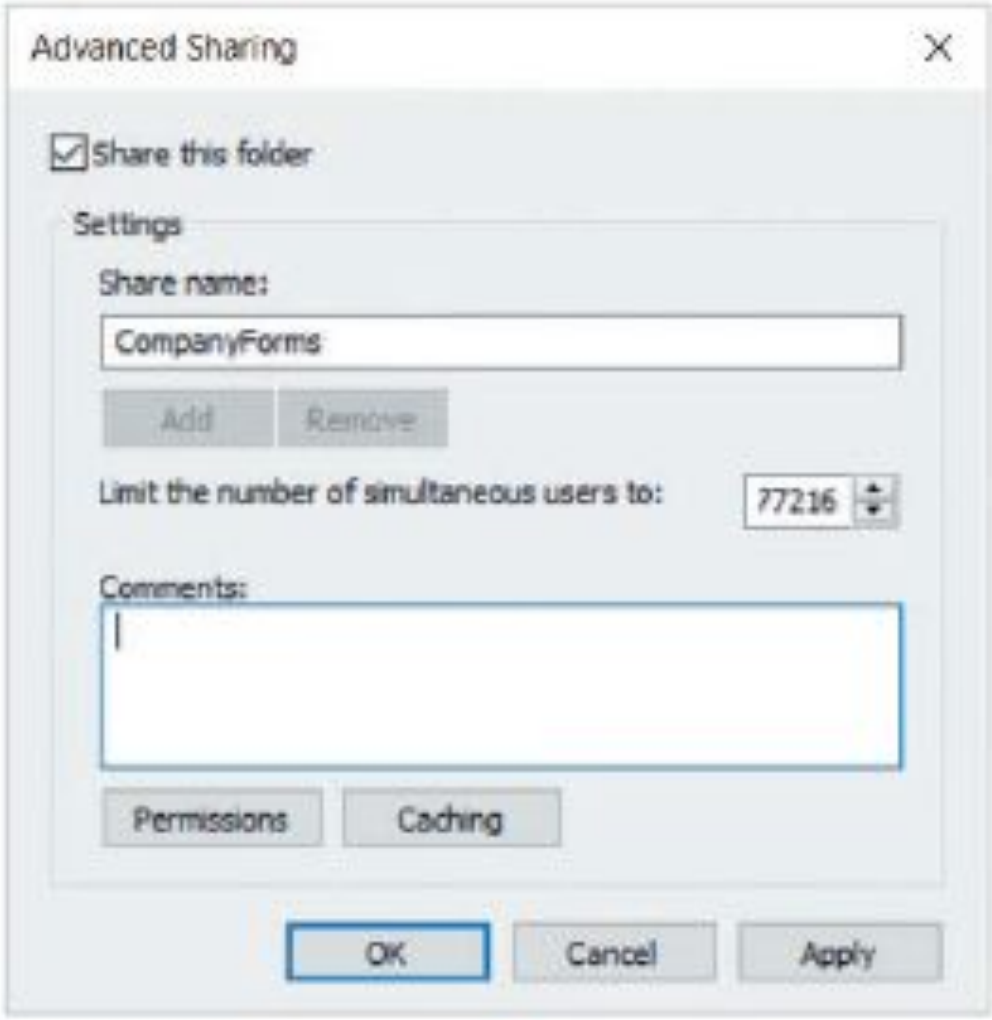
# Sharing a Folder Using Folder Properties

- SMB requires that you have a **shared folder permission** in order to connect to a shared folder. The permissions include the following:
- *Read*—Allows groups or users to read and execute files.
- *Read/Write*—Allows groups or users to read, execute, delete, and modify the contents of files, as well as add and delete subfolders.
- *Owner*—Automatically assigned to the owner of the folder, it allows the owner to read, execute, delete, and modify the contents of files, as well as add and delete subfolders and modify share permissions.



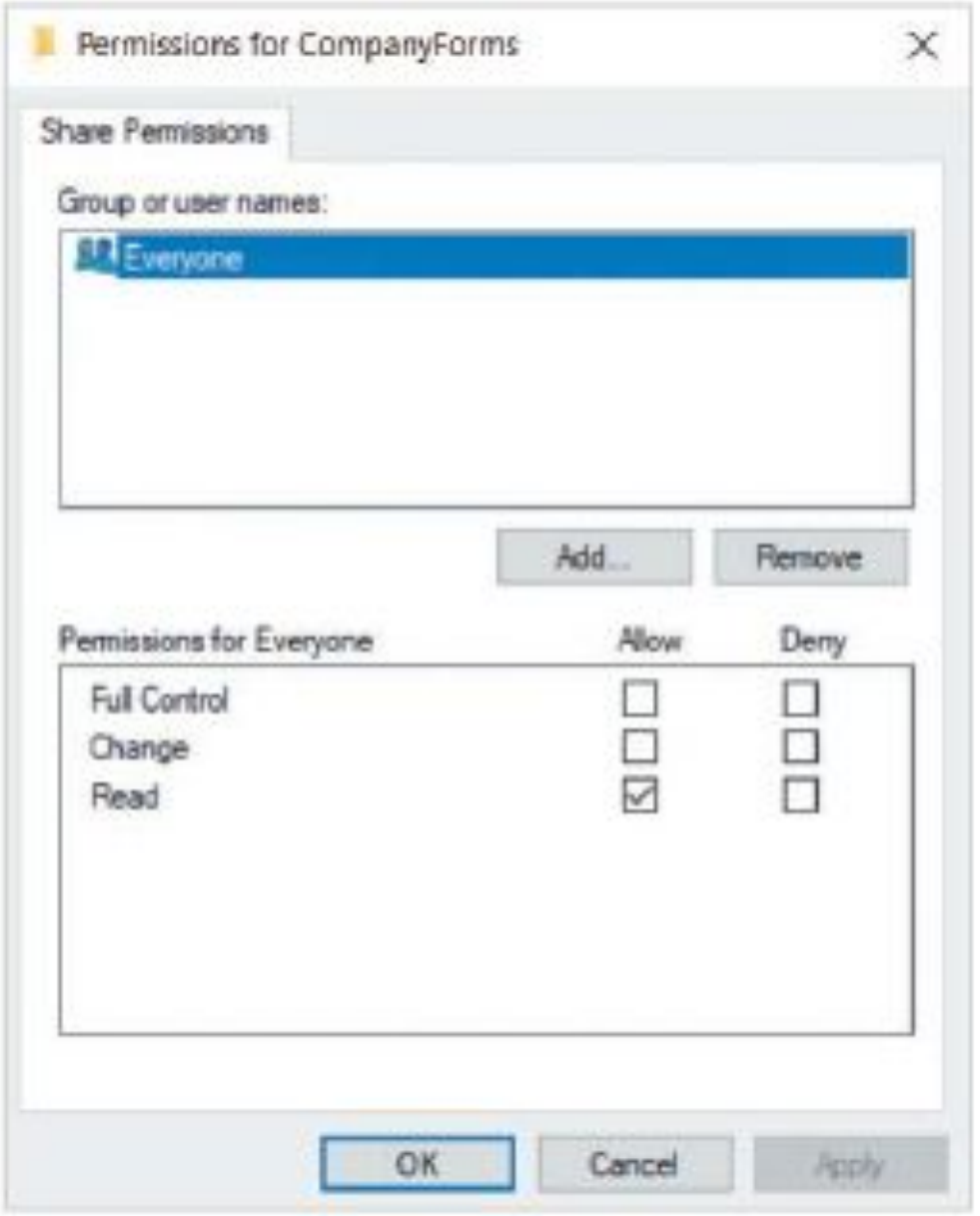
# Sharing a Folder Using Folder Properties

- **Instead of clicking the Share button in previous figure, you can instead click the Advanced Sharing button, and then select Share this folder within the Advanced Sharing window shown**
- You can then specify the share name, limit the number of simultaneous connections to the shared folder (the default value is 16777216) or supply a description within the Comments text box.



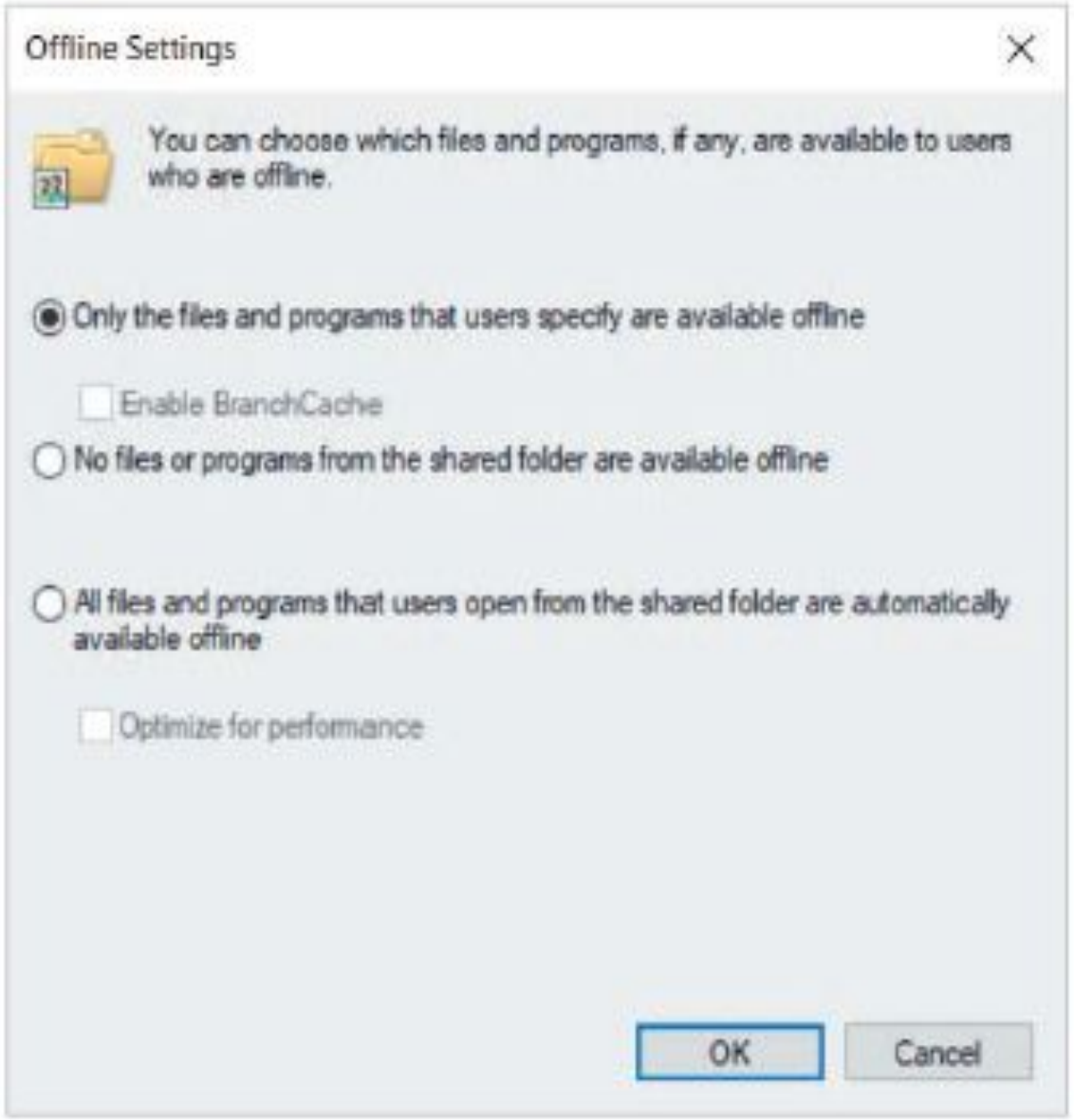
# Sharing a Folder Using Folder Properties

- If you click the Permissions button, you can configure advanced shared folder permissions for groups and users, as shown
- The three advanced shared folder permissions shown in are:
  - *Read*—Allows groups or users to read and execute files.
  - *Change*—Allows groups or users to read, execute, delete, and modify the contents of files, as well as add and delete subfolders.
  - *Full Control*—Allows groups or users to read, execute, delete, and modify the contents of files, as well as add and delete subfolders and modify share



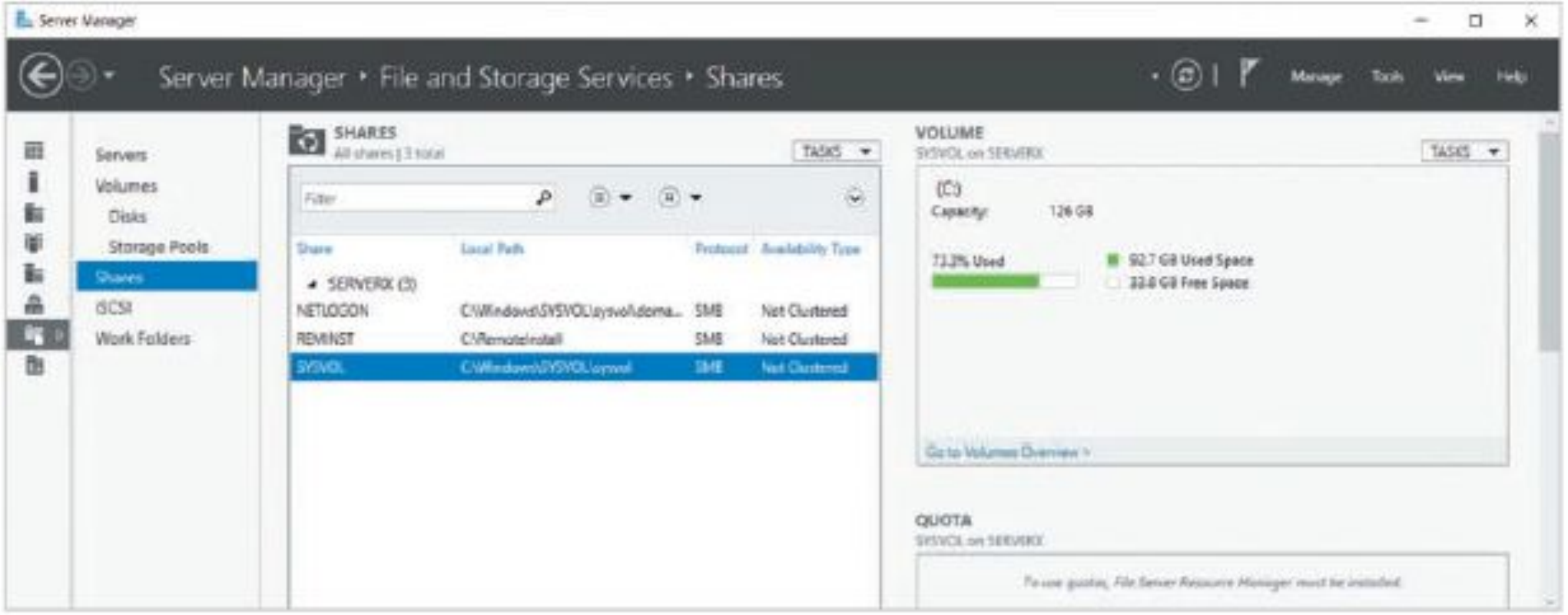
# Sharing a Folder Using Folder Properties

- The Caching button in previous slide allows you to configure the **offline file caching** feature of SMB, as shown
- The default option shown allows users to right-click files and programs within the shared folder and select *Make available offline* to ensure that a copy is downloaded to a cache folder on their local computer.
- This prevents a network disruption from impacting the editing of files or execution of a program within the shared folder.
- When the user disconnects from the shared folder, any modified files within the cache folder are then uploaded to the shared folder



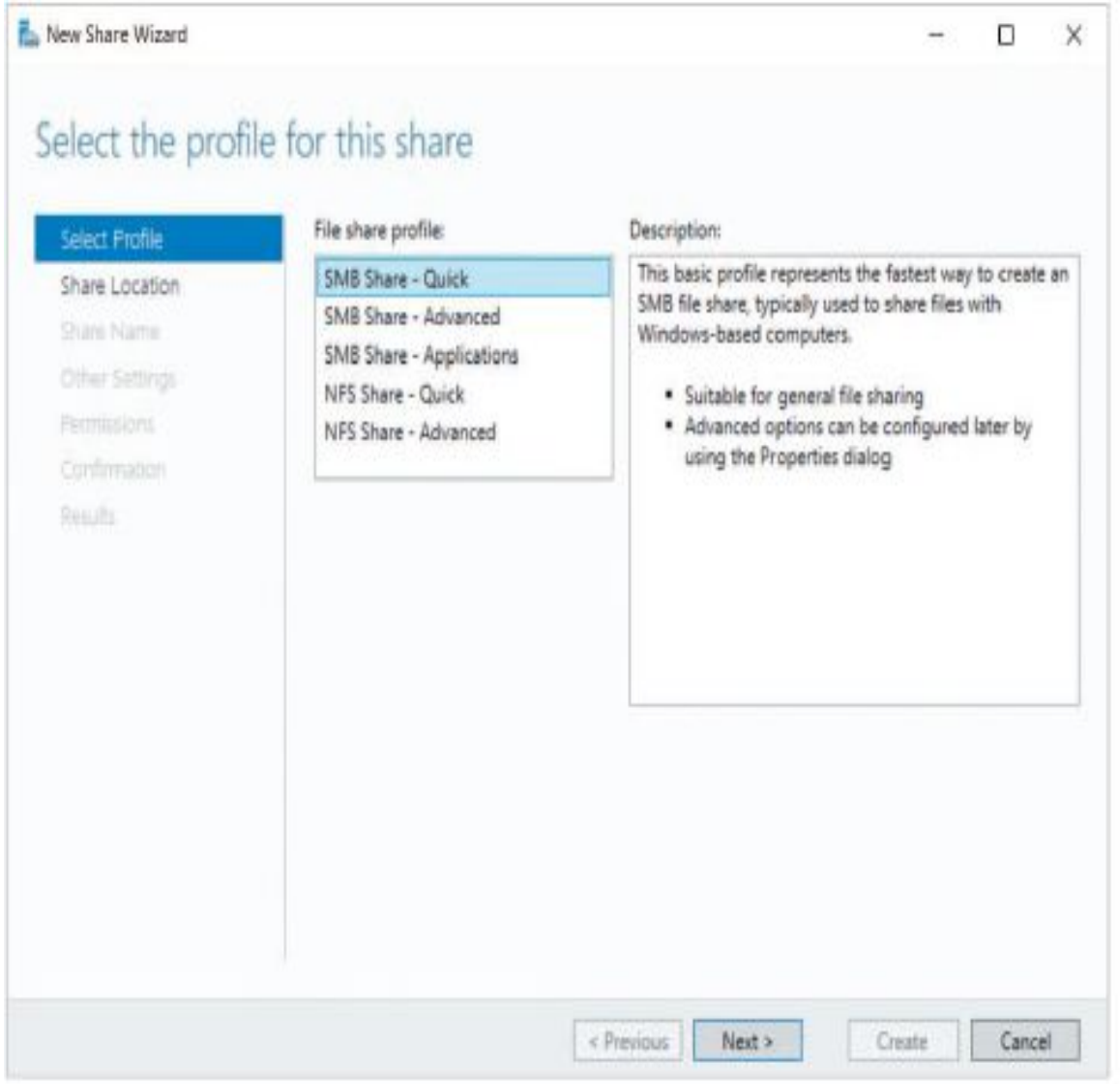
# Sharing a Folder Using Server Manager

- Click File and Storage Services within the navigation pane of Server Manager, and then highlight Shares as shown in.
- The NETLOGON and SYSVOL shares shown are automatically created during the installation of Active Directory Domain Services.



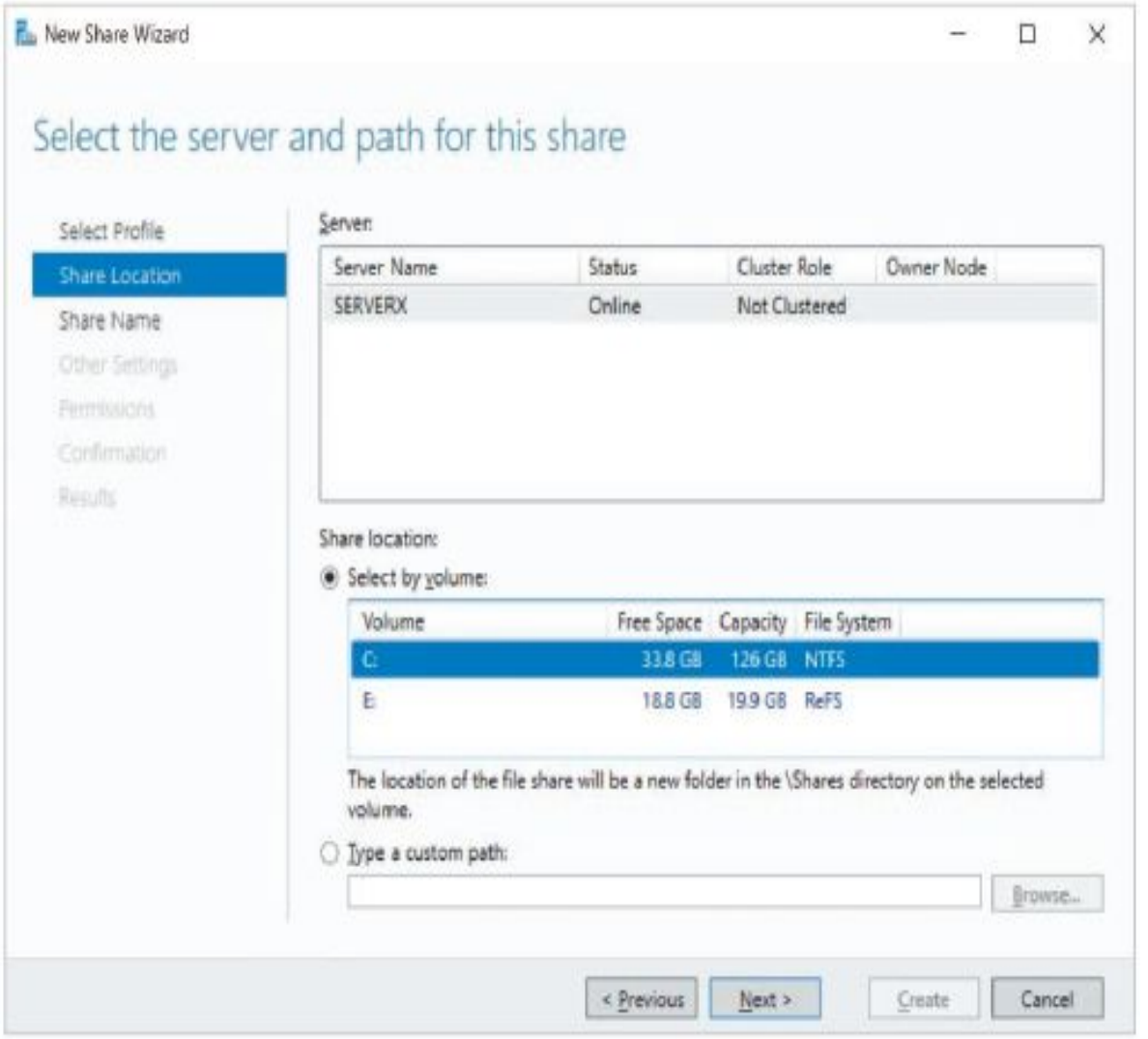
# Sharing a Folder Using Server Manager

- To share a folder, you can select the Tasks drop-down box in the Shares section and click New Share. This will start the New Share Wizard shown in Figure 5-19. Normally, you select *SMB Share – Quick*.
- You can also select *SMB Share – Advanced* to additionally configure file classifications and folder quotas if the File Server Resource Manager is installed or *SMB Share – Applications* to automatically configure NTFS/ReFS permissions on the folder that are compatible with most applications.



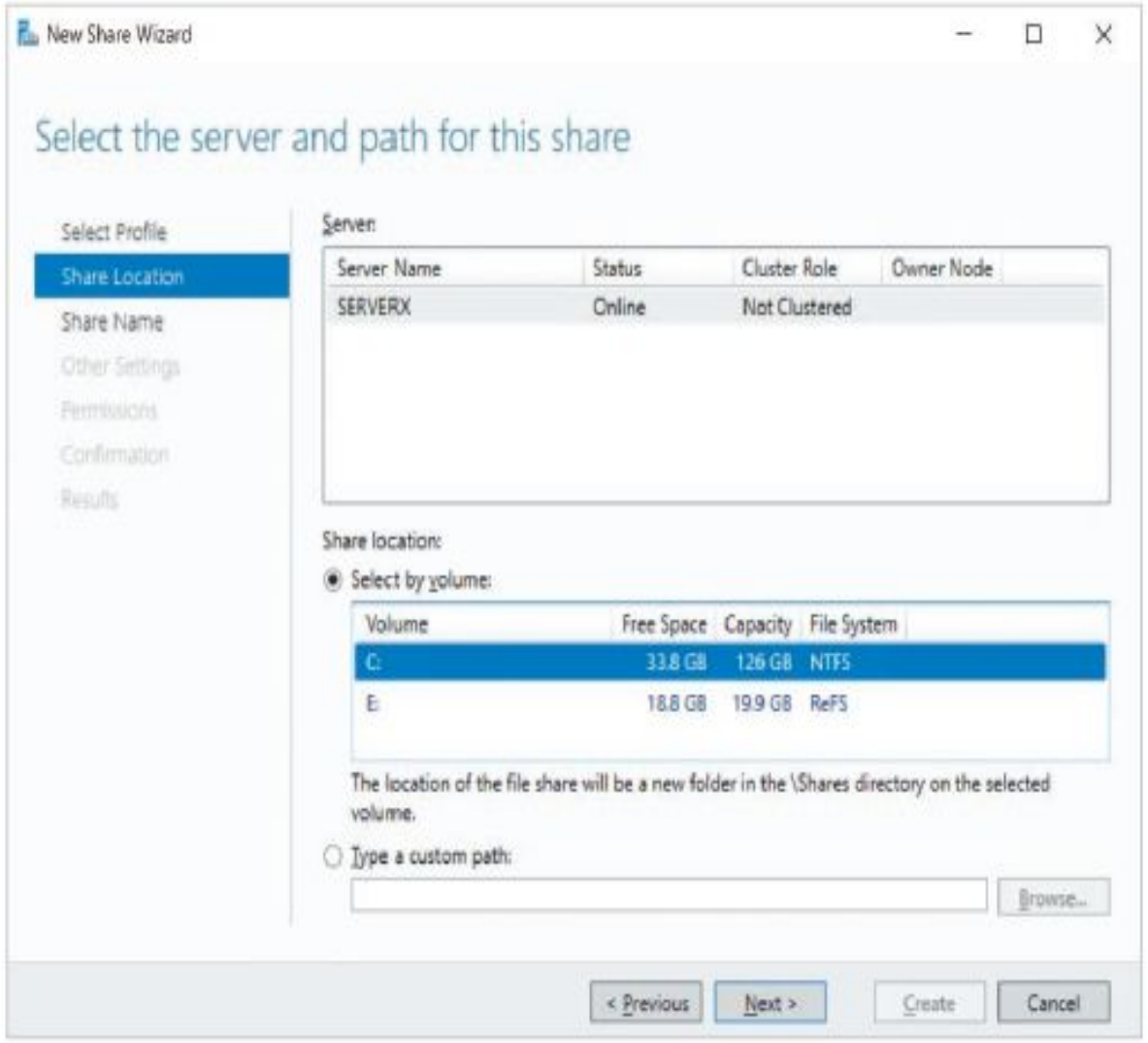
# Sharing a Folder Using Server Manager

- If you select *SMB Share – Quick* and click Next, you will be prompted to select the server, and the volume that should contain the shared folder, as shown.
- This will create a \Shares parent folder on the volume (if one does not already exist) that will include a subfolder for your new shared folder. Alternatively, you can select *Type a custom path* and specify the path to an existing shared folder that you wish to share.



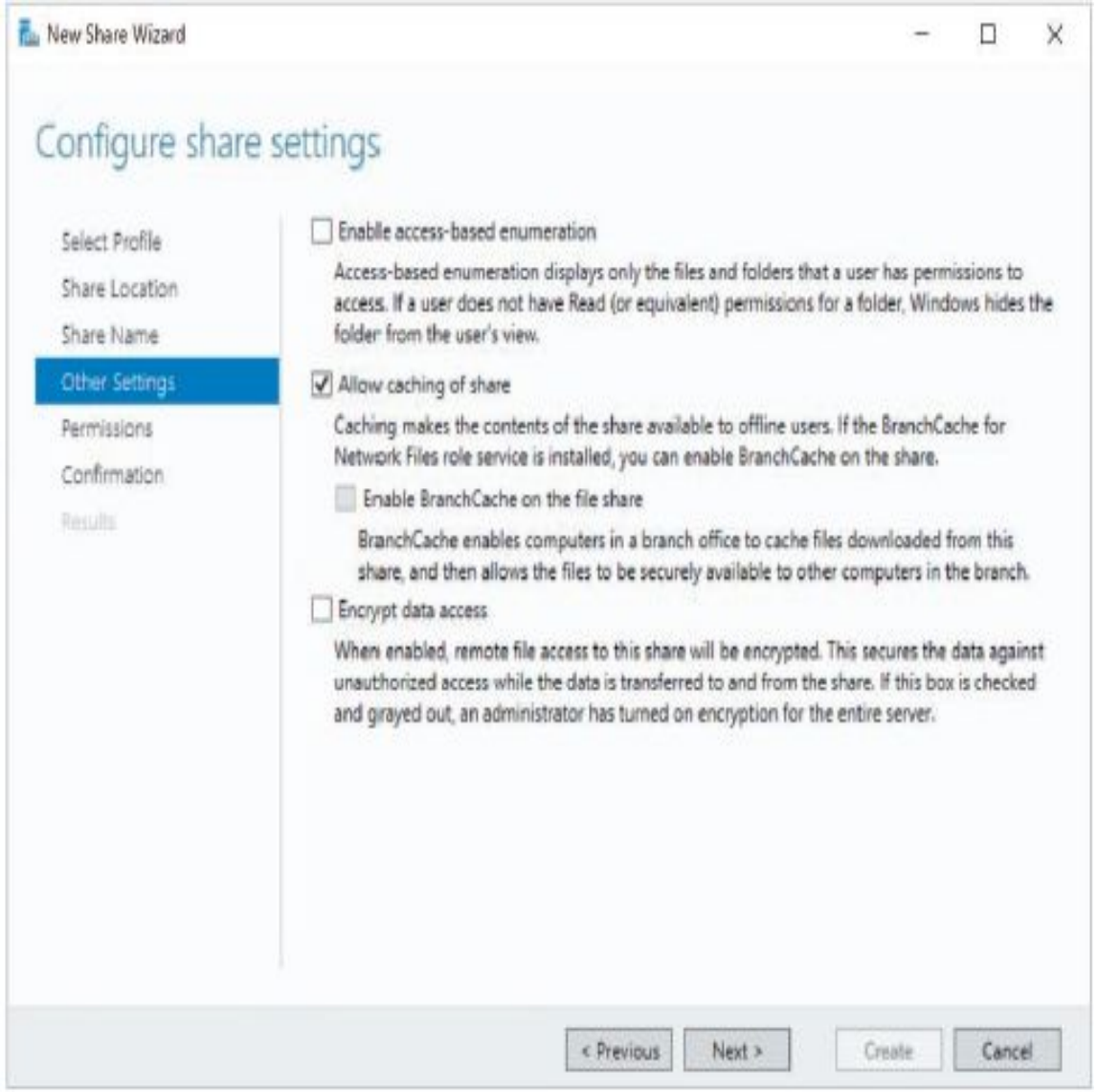
# Sharing a Folder Using Server Manager

- When you click Next, you will be prompted to supply the share name and optional share description, as shown.



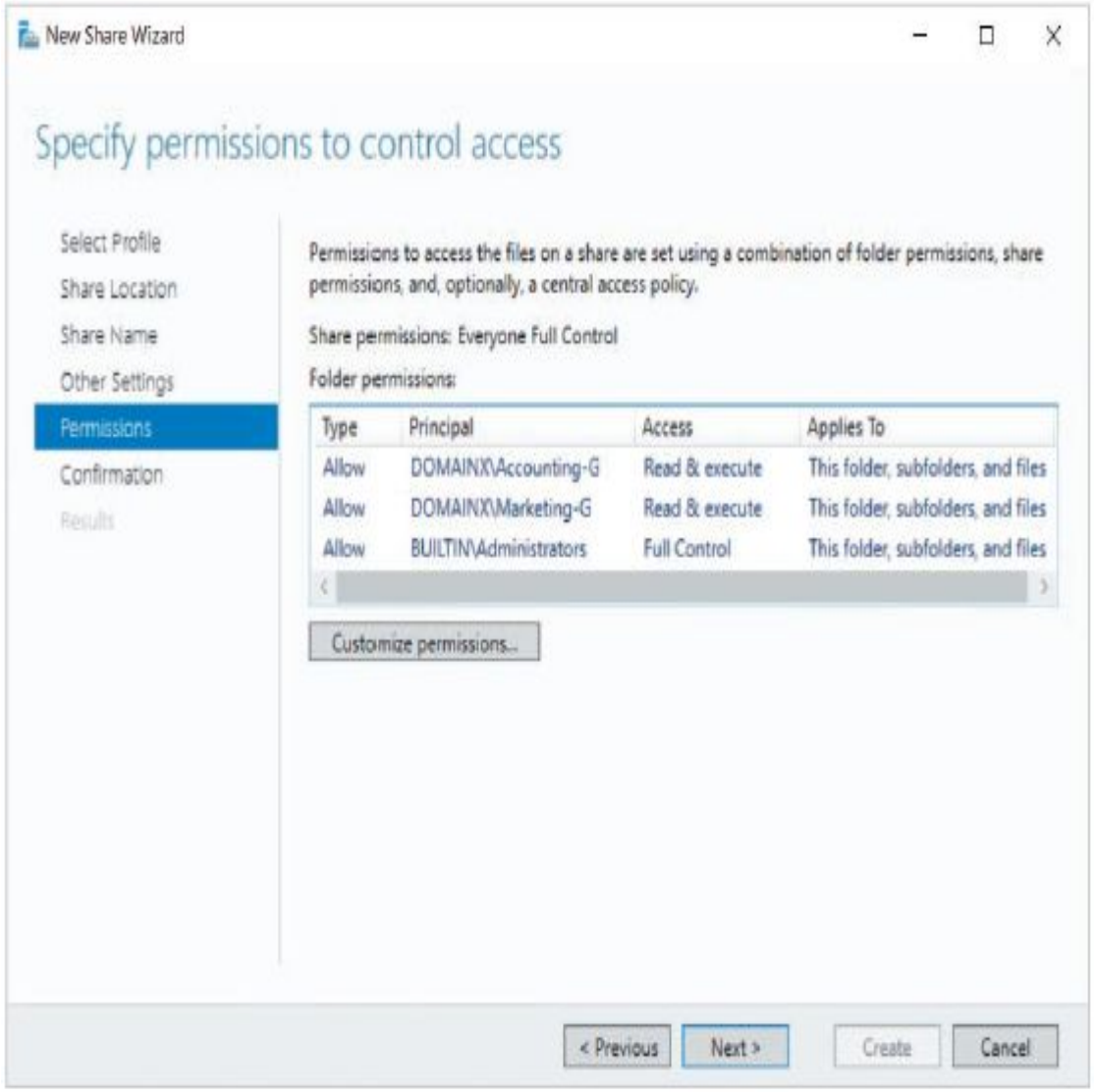
# Sharing a Folder Using Server Manager

- After clicking Next, you can configure the optional share features shown:
  - *Enable access-based enumeration* prevents users from viewing shared folders (and subfolders and files) for which they do not have at least Read share and NTFS/ ReFS permissions. The **access-based enumeration** feature prevents users from receiving an access denied error message when opening a folder or file that they can see within File Explorer but are not granted sufficient permission to access.
  - *Allow caching of share* enables offline file caching and is equivalent to the *Only the files and programs that users specify are available offline* option shown .
  - *Encrypt data access* allows Windows 8, Windows Server 2012, and later systems to encrypt SMB packets when accessing the shared folder.



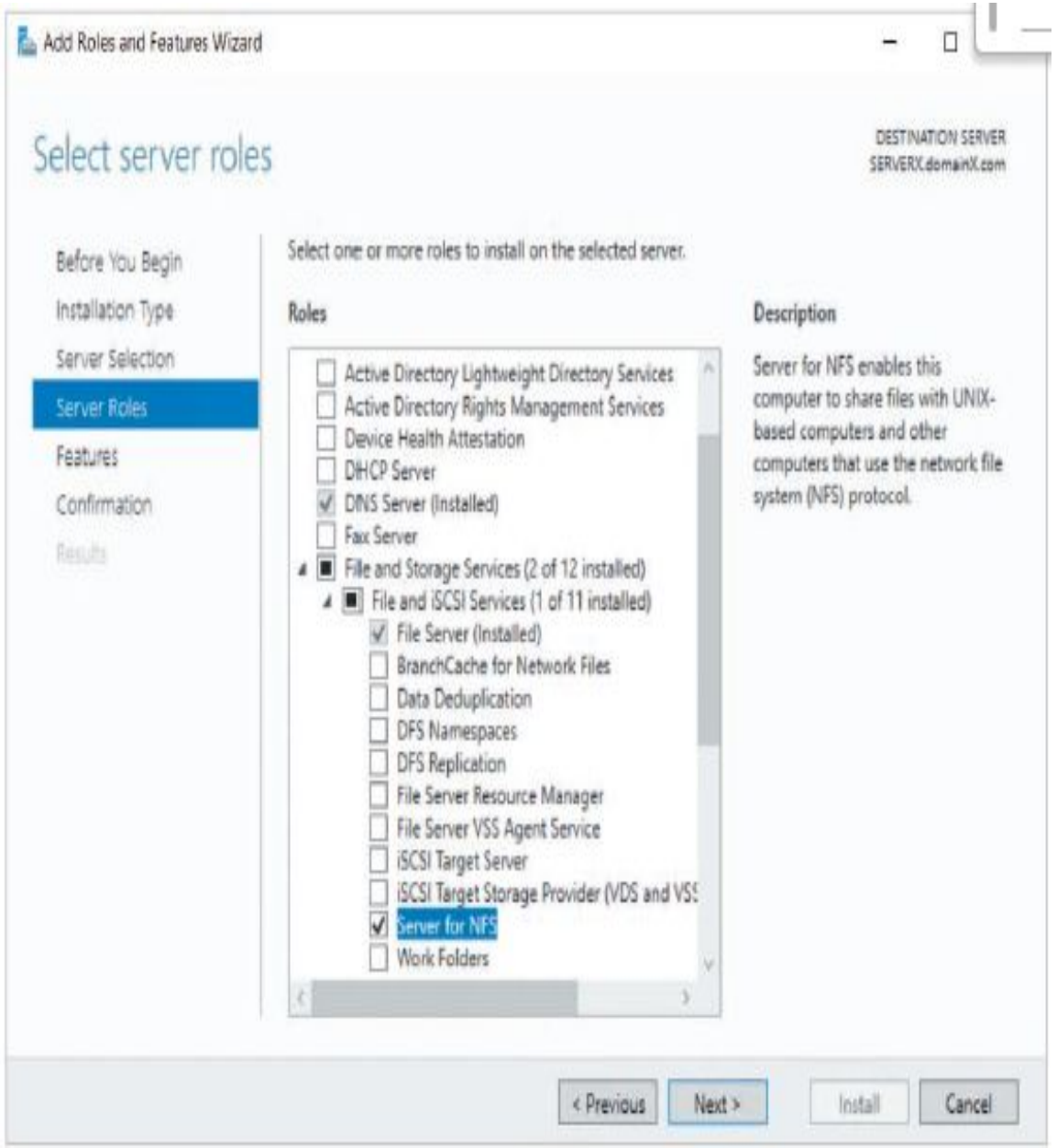
# Sharing a Folder Using Server Manager

- When you click Next, you will be able to modify the NTFS/ReFS permissions on the folder to match the desired level of access for groups and users, as shown
- To simplify the permissions associated with sharing folders on NTFS and ReFS filesystems, the New Share Wizard automatically assigns the Everyone group Full Control advanced share permission.
- Click Next and then Create to create the new shared folder.



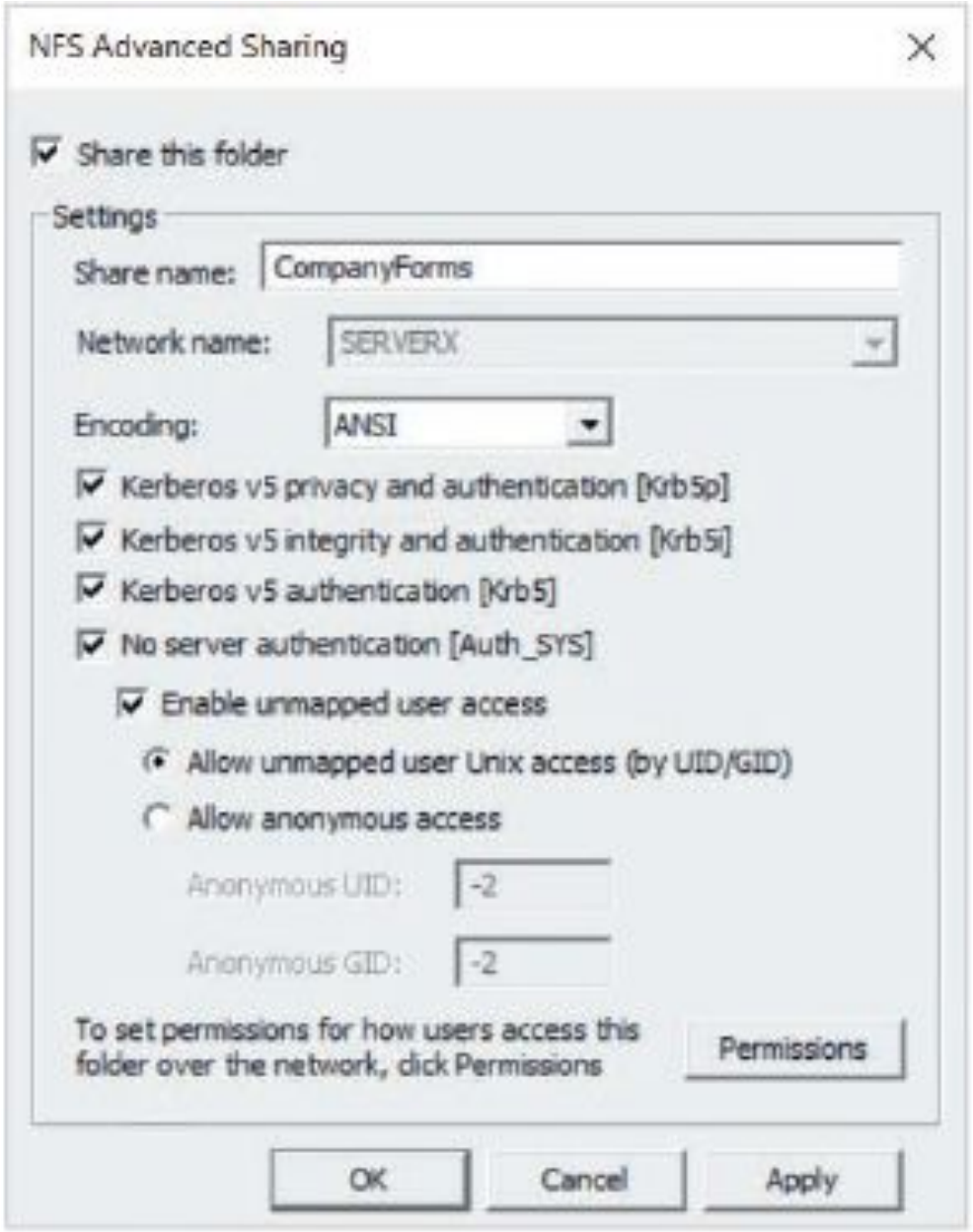
# Sharing Folders Using NFS

- To share folders using NFS on Windows Server 2019, you must first install the **Server for NFS** server role.
- To select this role within the Add Roles and Features Wizard in Server Manager, you must first expand File and Storage Services, and then expand File and iSCSI Services, as shown



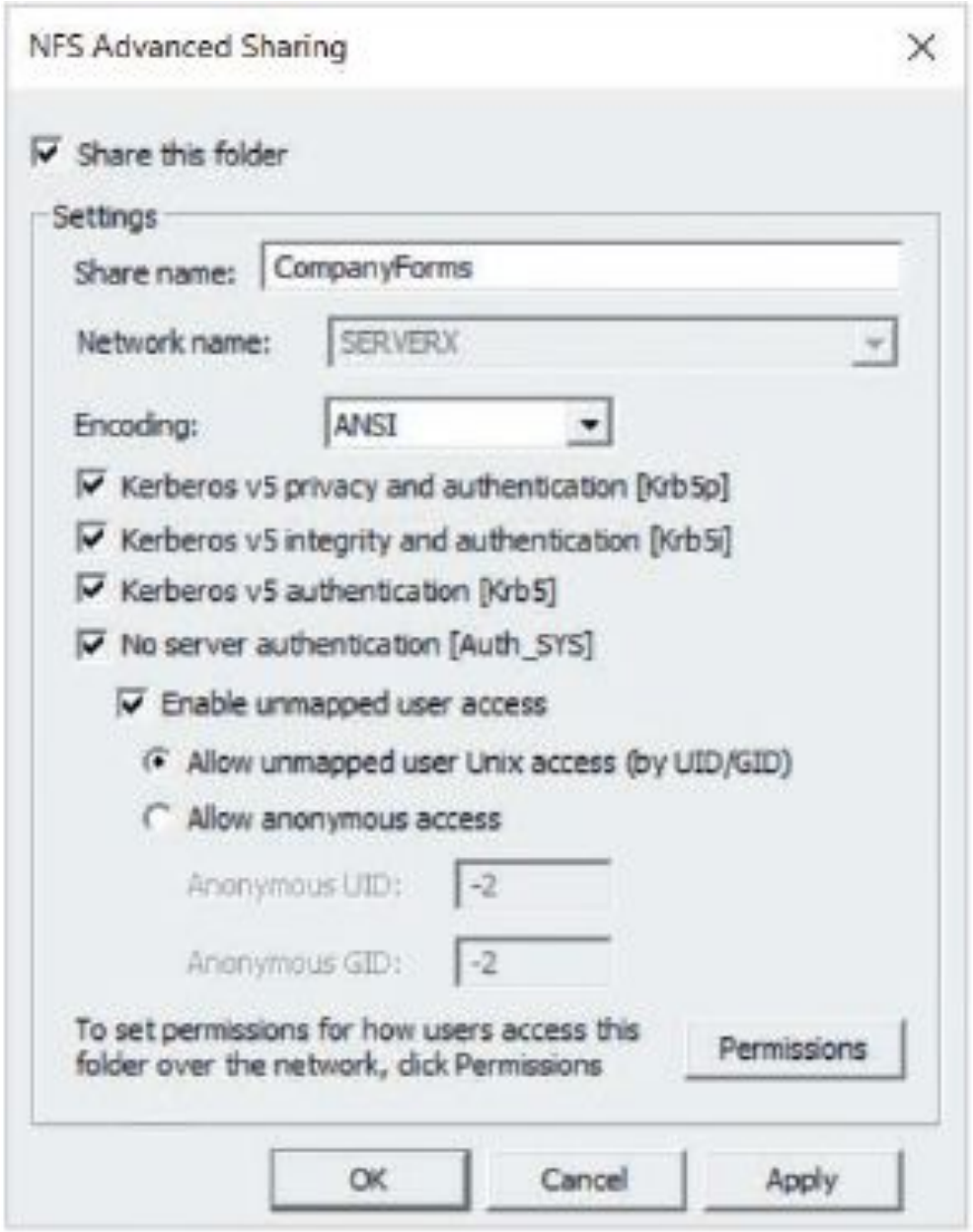
# Sharing a Folder Using Folder Properties

- To share folders using NFS on Windows Server 2019, you must first install the **Server for NFS** server role.
- This will open the NFS Advanced Sharing window shown, where you can enable NFS file sharing, specify the share name, and configure the appropriate NFS options.
- NFS was designed for UNIX systems that shared the same user database, either by coordinating the **user ID (UID)** and **group ID (GID)** numbers assigned to each UNIX user in the UNIX user database stored on each system, or by providing centralized authentication for users on the network using Kerberos.



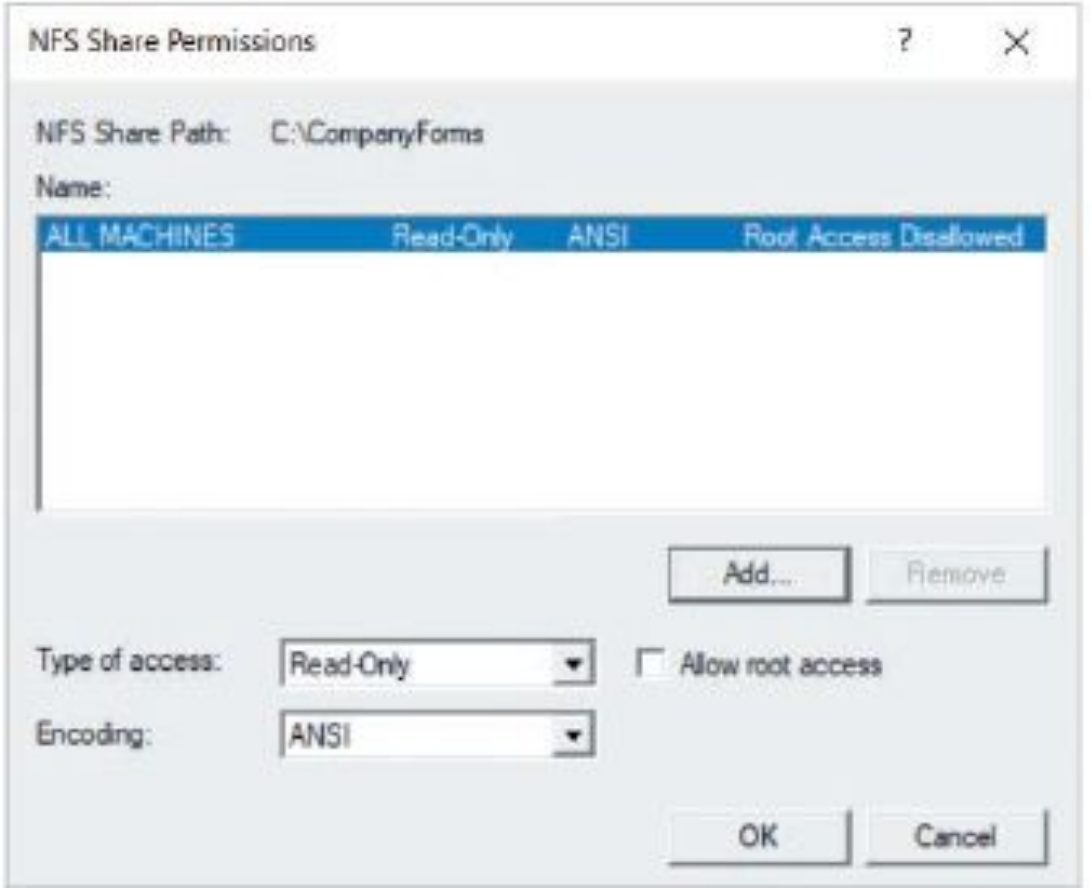
# Sharing a Folder Using Folder Properties

- The three Kerberos v5 options selected allow all forms of Kerberos authentication for UNIX, Linux, macOS, and Windows users within the Active Directory domain.
- The *No server authentication*, *Enable unmapped user access*, and *Allow unmapped user Unix access (by UID/GID)* options allow UNIX, Linux, and macOS users to access the NFS shared folder by passing their UID and GID to the server, instead of using Kerberos.
- You could select *Allow anonymous access* to force UNIX, Linux, and macOS users that are not configured to use Kerberos to connect as the Guest account



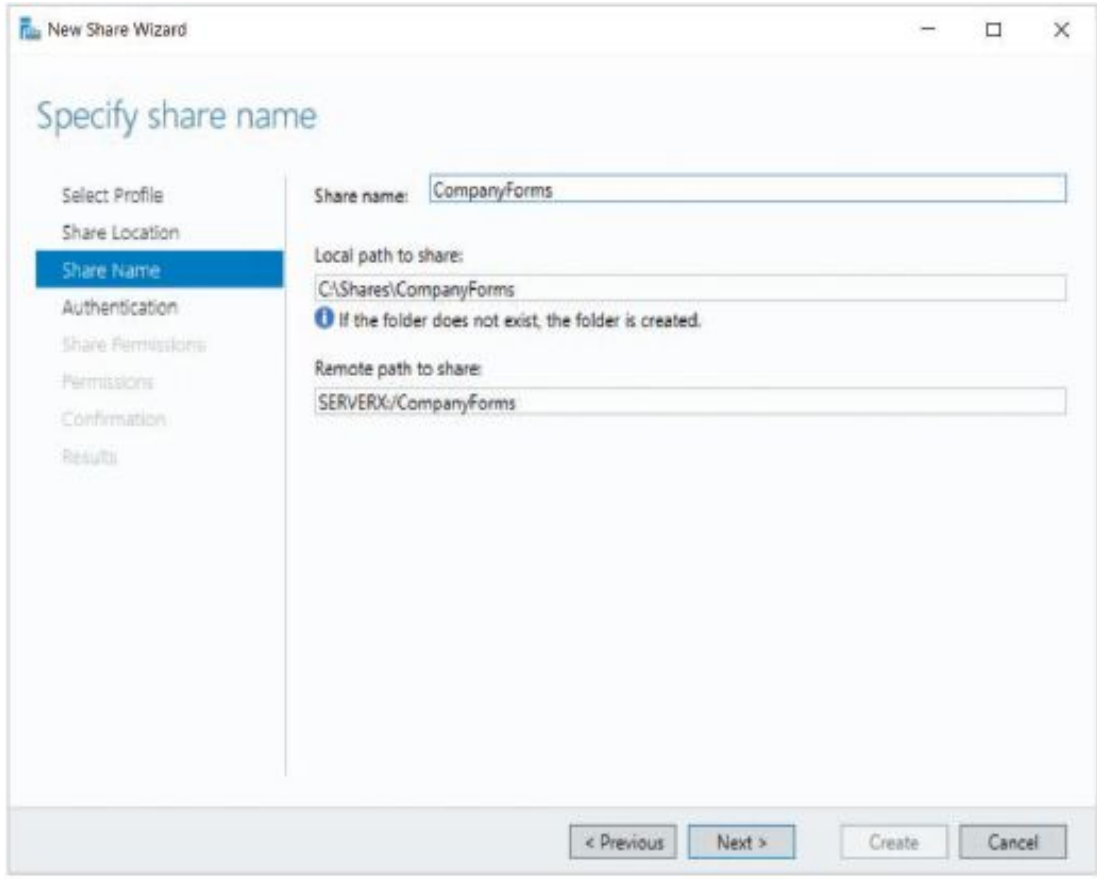
# Sharing a Folder Using Folder Properties

- As with SMB shared folders, shared folder permissions are required to connect to an NFS shared folder.
- Click the Permissions button, you can add entries for computers (by DNS name) that are granted access to the NFS shared folder, as shown.
- There are only two levels of access that you can grant to computers:
  - *Read-Only*—Allows computers to read and execute files.
  - *Read-Write*—Allows computers to read, execute, delete, and modify the contents of files, as well as add and delete subfolders.



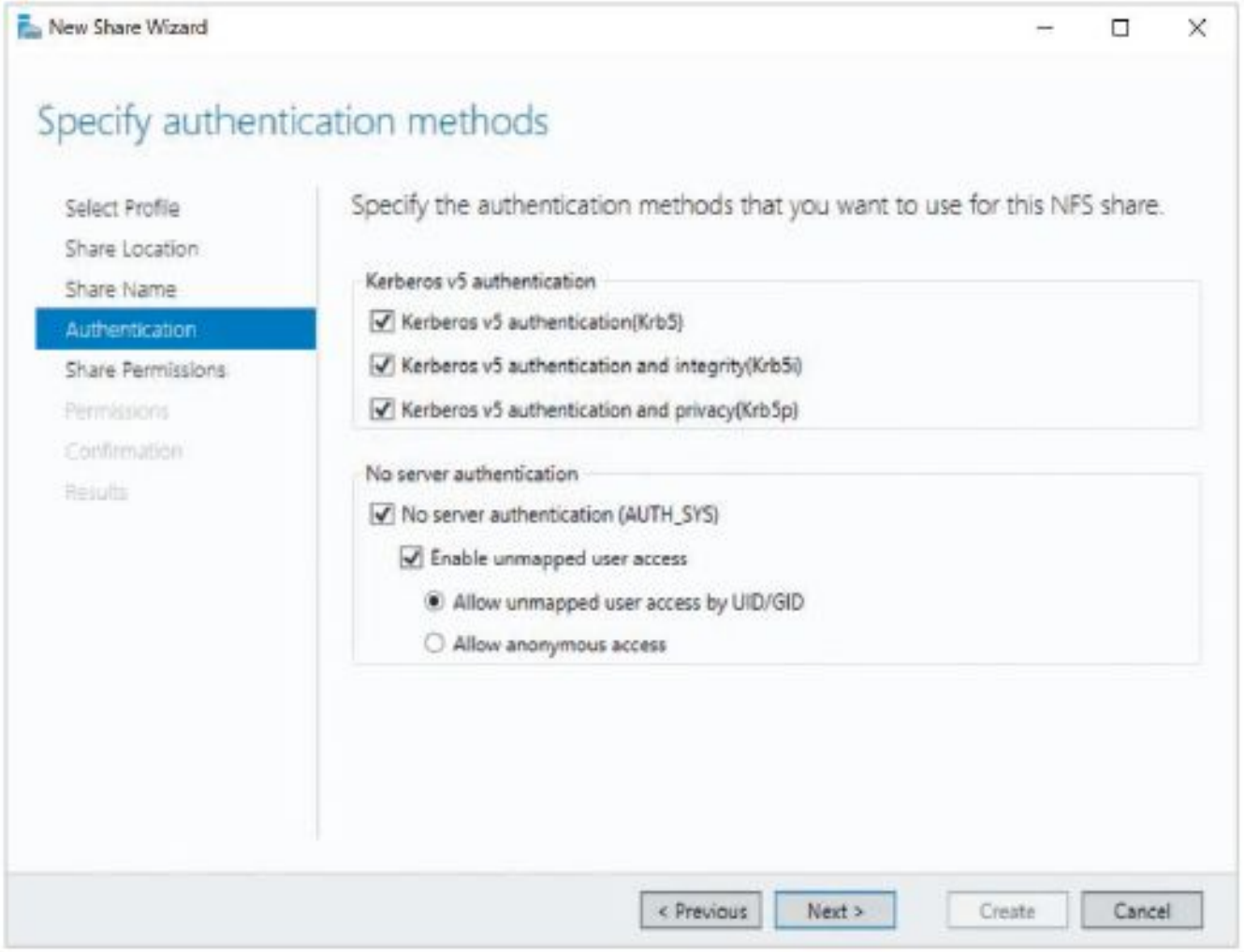
# Sharing a Folder Using Server Manager

- The Shares section of Server Manager can also be used to create and manage NFS shared folders, using the same general process as SMB shared folders.
- When you start the New Share Wizard (shown earlier in Figure 5-19), you can select *NFS Share – Quick* to share a folder with NFS, or select *NFS Share – Advanced* to additionally configure file classifications and folder quotas if the File Server Resource Manager is installed.
- Select *NFS Share – Quick* and progress through the New Share Wizard, you will be prompted to select the location of the shared folder as well as the share name.



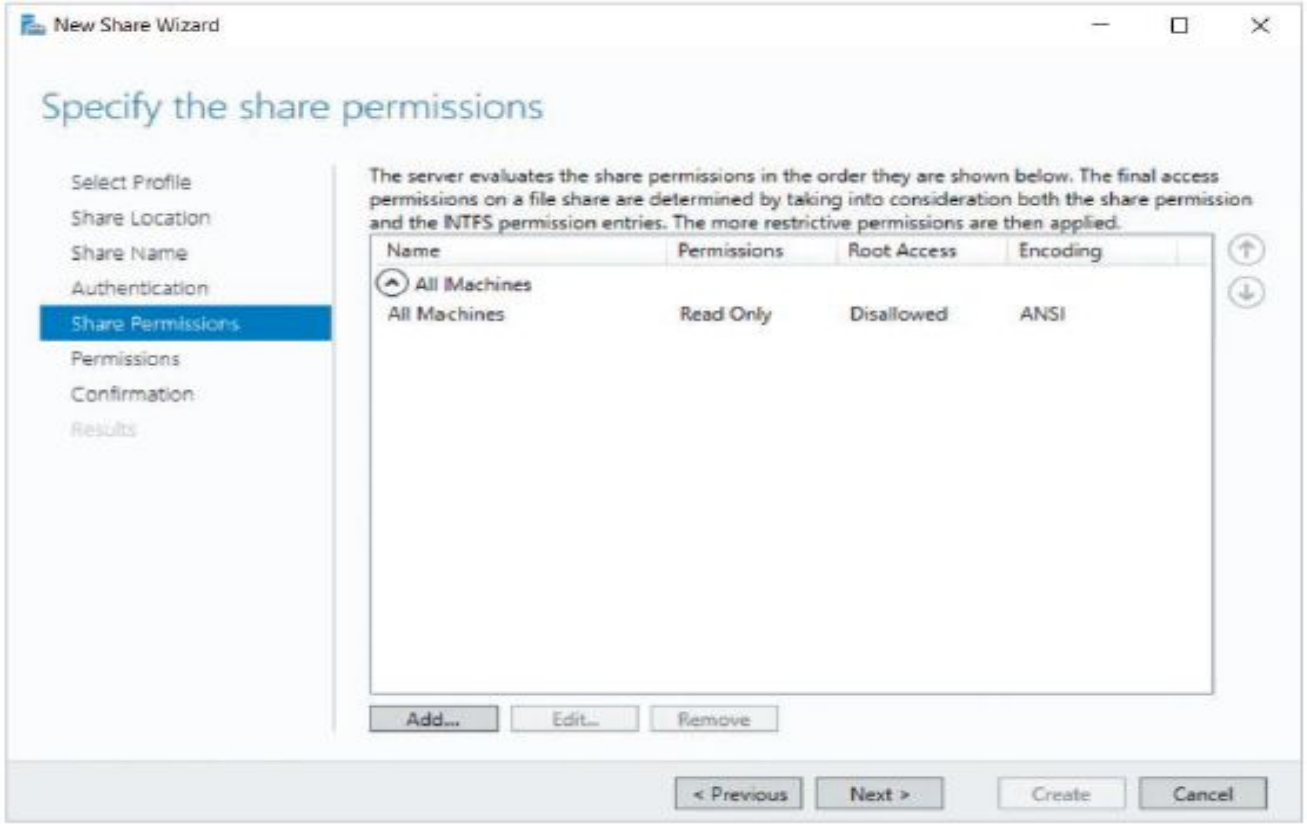
# Sharing a Folder Using Server Manager

- Click Next in previous figure, then you are prompted to select the authentication methods that clients can use when connecting to the NFS share, as shown



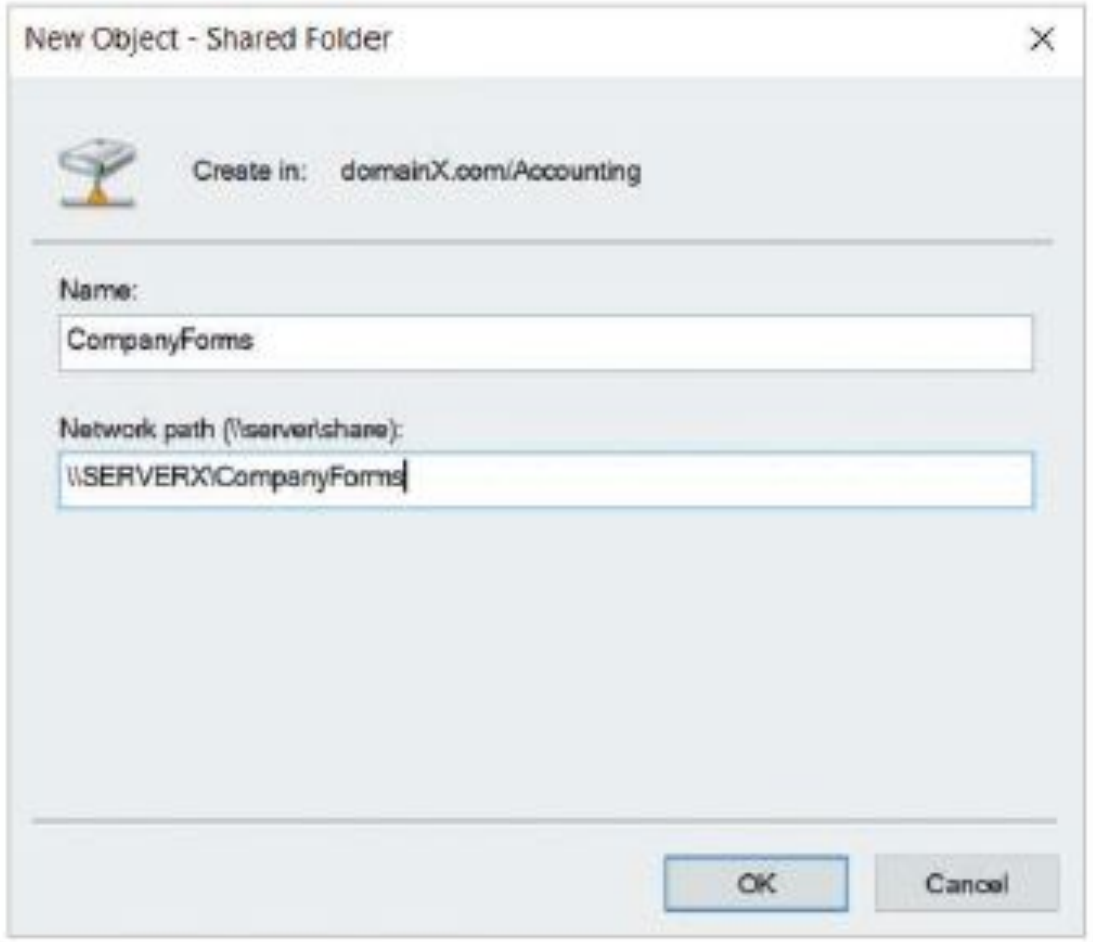
# Sharing a Folder Using Server Manager

- After clicking Next in last figure, you are prompted to add NFS shared folder permission entries for computers on the network, as shown.
- After you click Next, you will be able to modify the NTFS/ReFS permissions on the folder to match the desired level of access for groups and users, as shown. Following this, you can click Next and then Create to create the new shared folder.



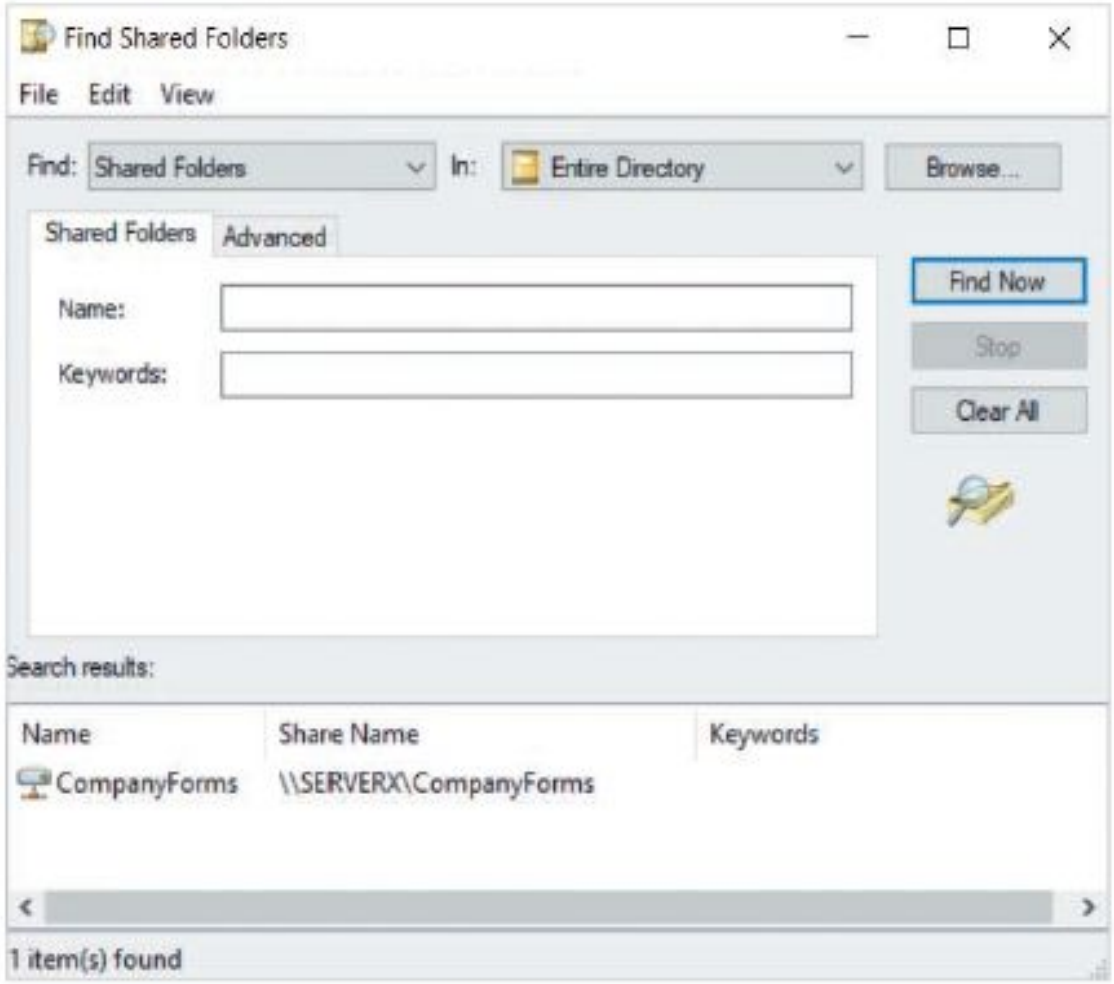
# Publishing a Shared Folder in Active Directory

- Active Directory allows you to create objects that represent network resources, such as shared folders. This process is called **publishing** a resource to Active Directory.
- To publish a shared folder to the Active Directory database, you can right-click an OU within the Active Directory Users and Computers tool, and then click New, Shared Folder. This will open the New Object – Shared Folder window shown.
- You can supply the name and UNC path to the SMB or NFS shared folder. When you click OK, a shared folder object is created within the associated OU.



# Publishing a Shared Folder in Active Directory

- After a shared folder has been published to Active Directory, domain users can search Active Directory for shared folders using File Explorer on their Windows system. To locate published shared folders within File Explorer, you can select Network within the navigation pane, highlight the Network tab, and click Search Active Directory
- In the Find window that appears, you can select Shared Folders and click Find Now to search the entire Active Directory for shared folders, as shown

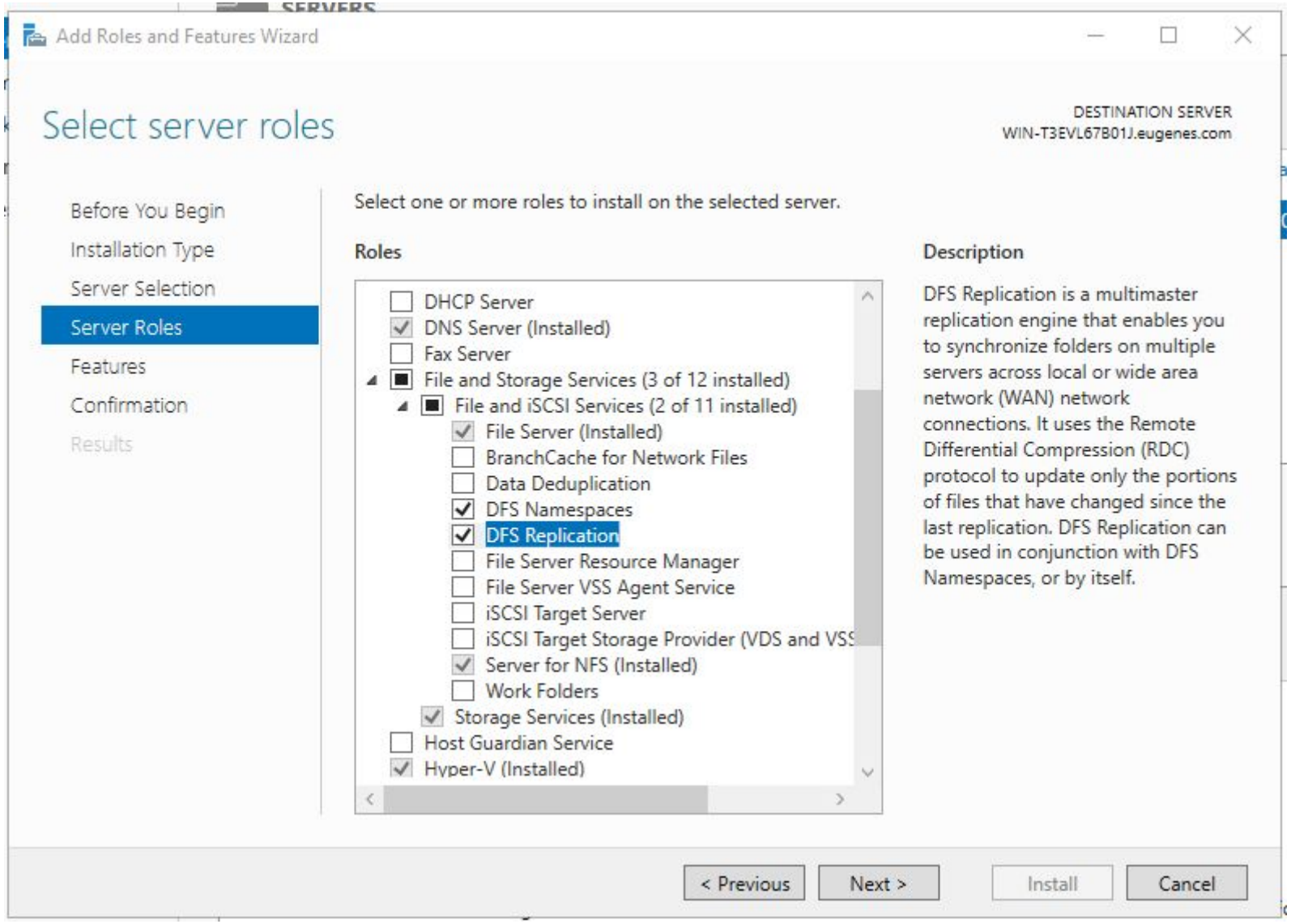


# Implementing Distributed File System

- Distributed File System (DFS) is an optional component provided by Windows Server 2019 that delivers additional functionality for accessing and managing content on file servers.
- Two separate server roles comprise DFS; each of these roles work independently of the other but can be managed using the same **DFS Management** tool:
  - **DFS Namespaces** provides a central location from which users can access the different shared folders within their organization. It can be installed on one or more file servers within your organization.
  - **DFS Replication** can synchronize folder contents between different servers. It must be installed on every server that synchronizes folder contents.

# Implementing Distributed File System

To install the DFS Namespaces and DFS Replication roles within the Add Roles and Features Wizard in Server Manager, you must first expand File and Storage Services, and then expand File and iSCSI Services, as shown



# Configuring DFS Namespaces

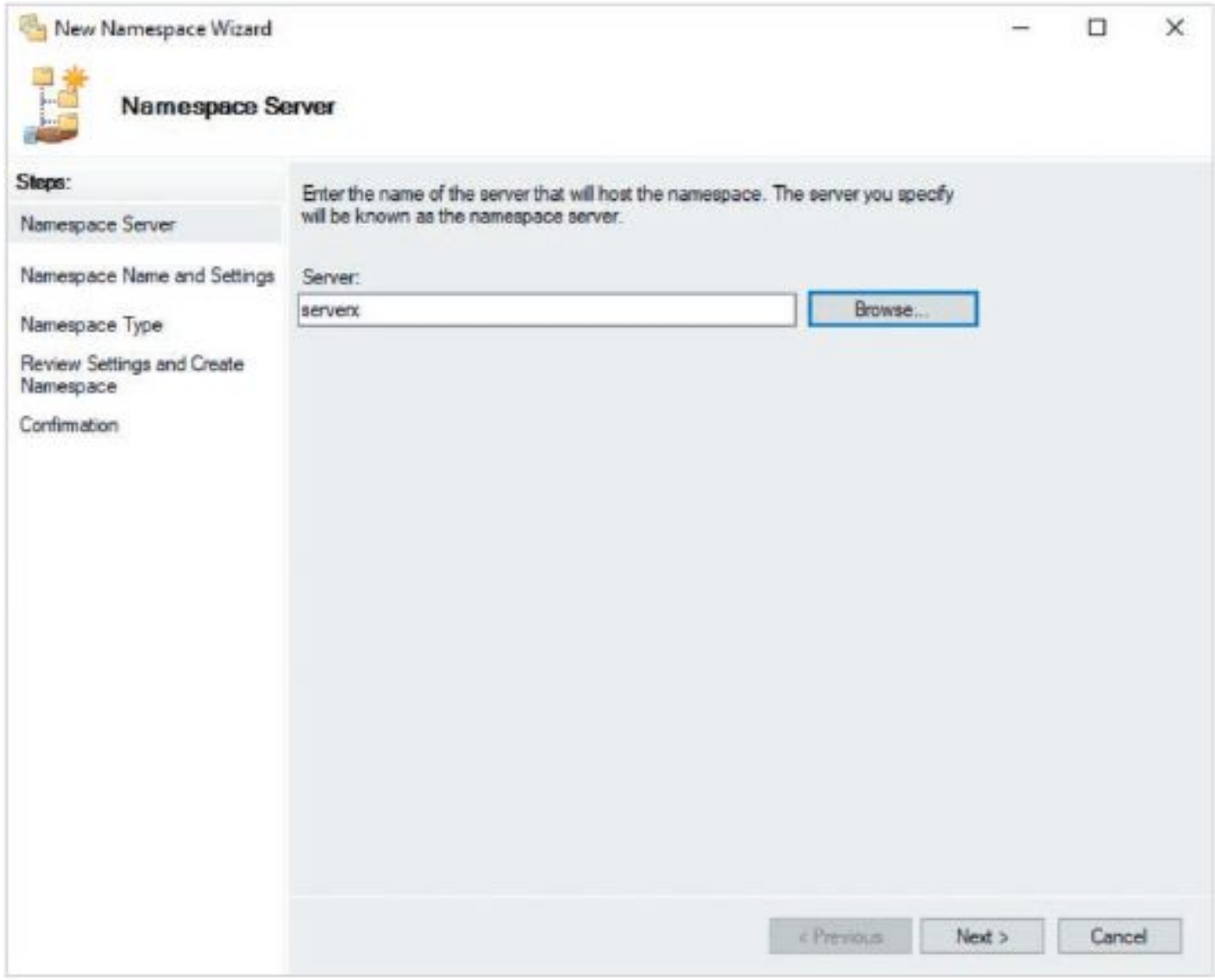
- A typical organization has many different file servers. Moreover, each file server usually hosts many different shared folders. While publishing shared folders makes it easier for users to locate a specific shared folder, it does not provide an easy way to browse the available shared folders within the organization.
- By installing DFS namespaces on a Windows Server 2019 system, you can create a **DFS namespace** shared folder that users can access. After accessing the DFS namespace folder, users will see subfolders (called **targets**) that represent the shared folders on the file servers within the organization.

# Configuring DFS Namespaces

- To configure a DFS namespace, you can select DFS Management from the tools menu of Server Manager to start the DFS Management tool shown

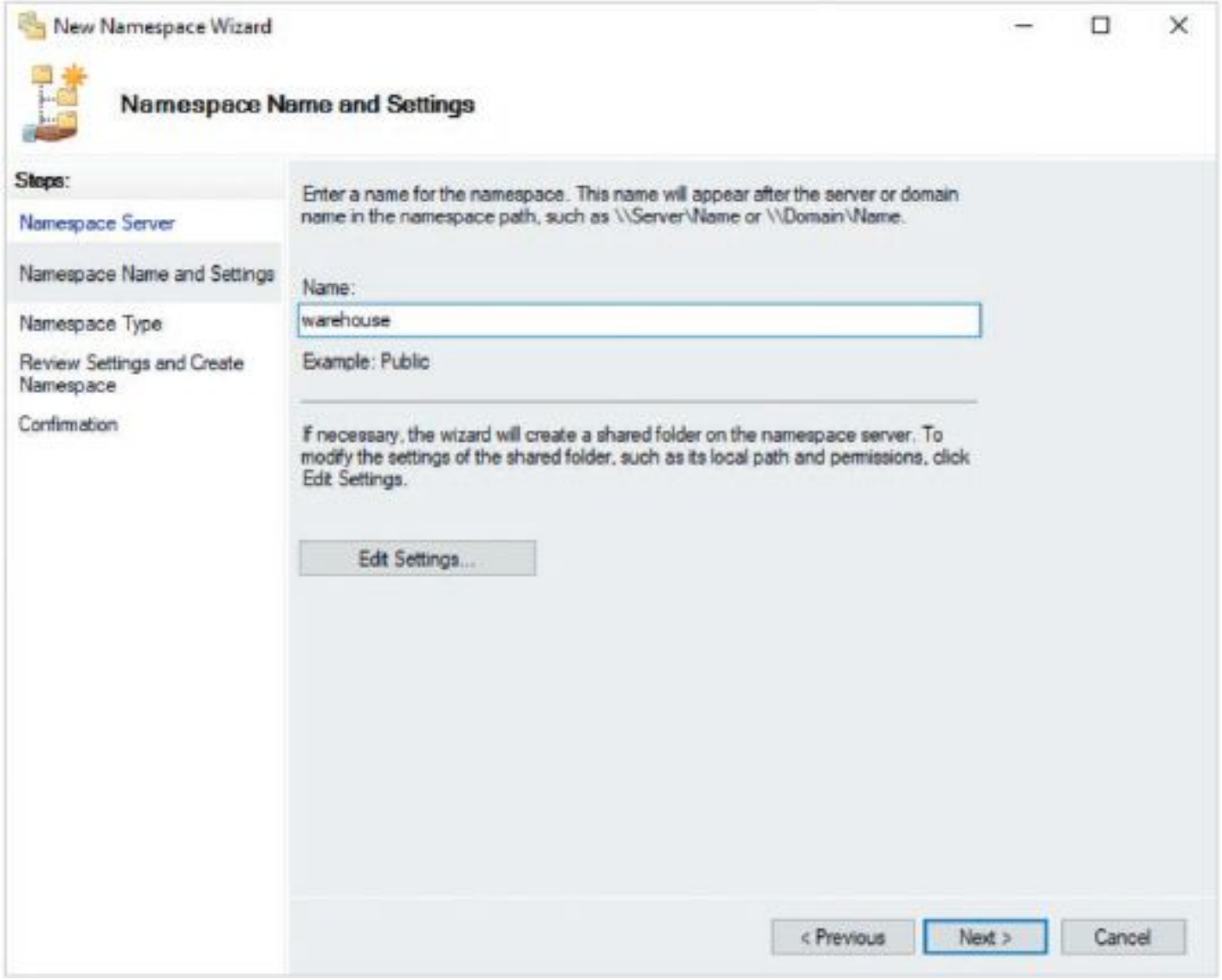
# Configuring DFS Namespaces

- Next, you can click New Namespace within the Actions pane and specify the name of the server that will host the DFS namespace within the New Namespace Wizard, as shown.



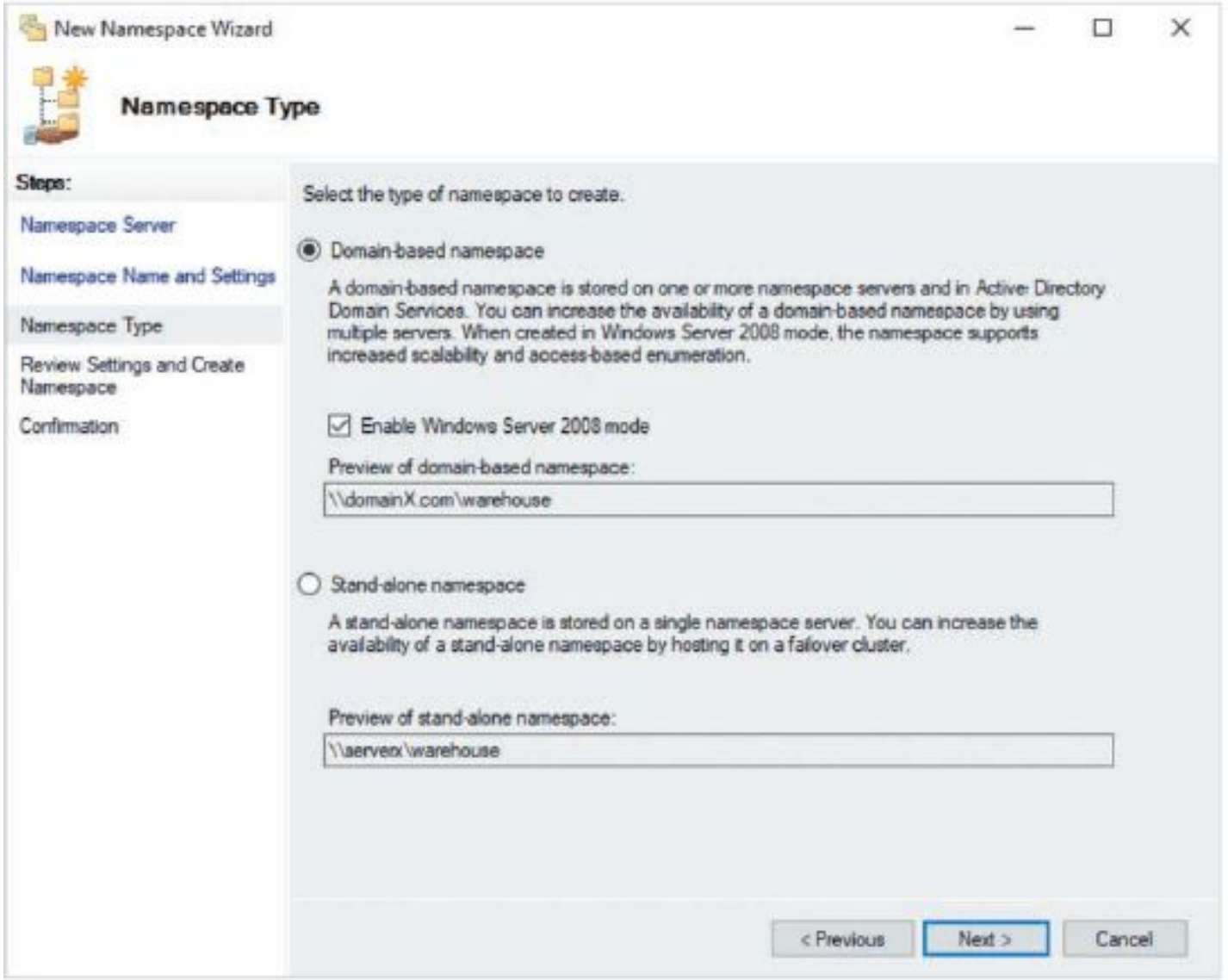
# Configuring DFS Namespaces

- When you click Next, you will be prompted for the shared folder name for the DFS namespace, as shown. Most organizations choose a name that includes their business unit name, or the word *public*, *common*, *root*, or *warehouse.*
- By default, the path for the warehouse shared folder shown is C:\DFSRoots\warehouse, and users will receive read only permission to it, such that they cannot add content directly underneath the DFS namespace.
- However, you can click Edit Settings to modify the path and share permissions to suit your needs.



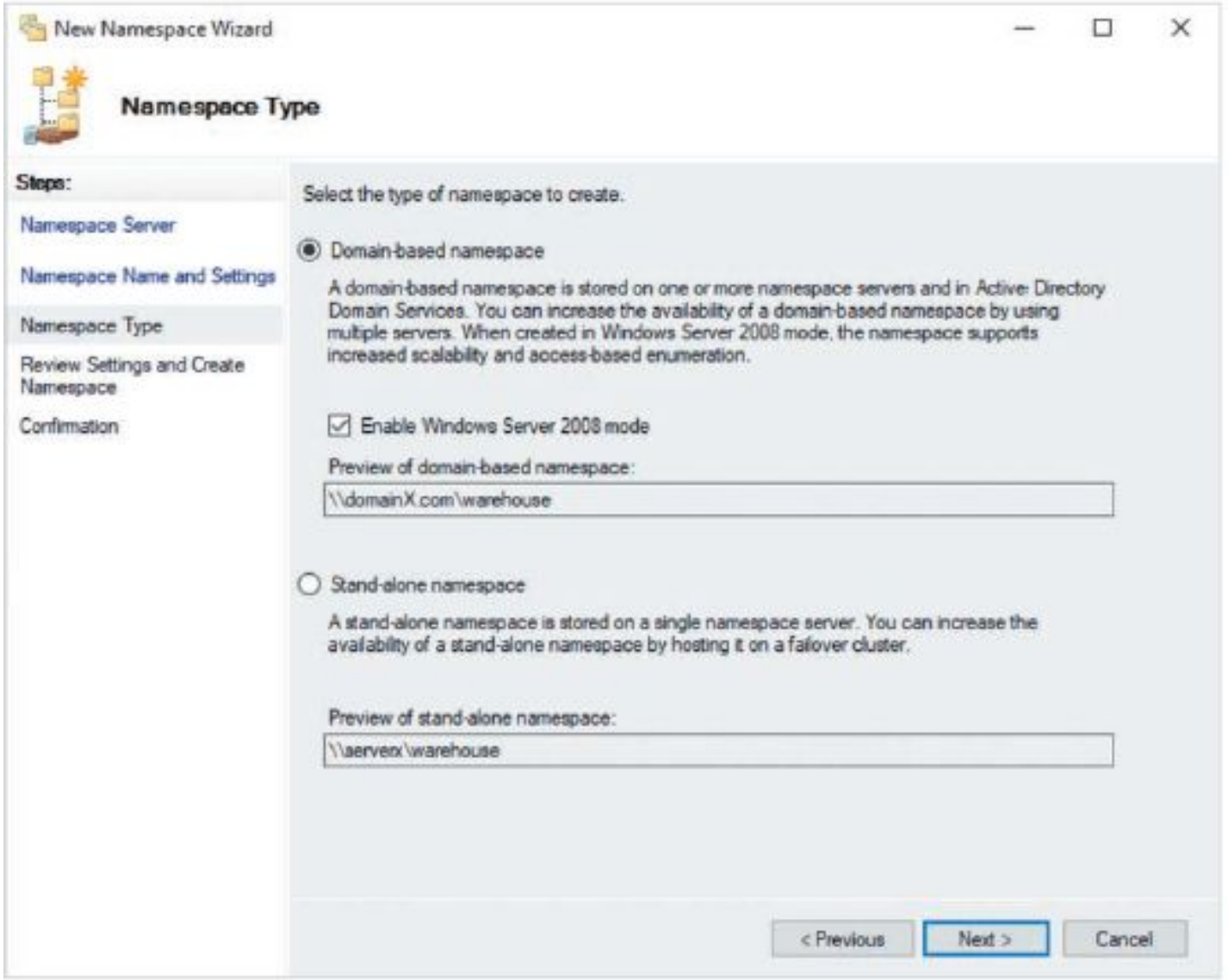
# Configuring DFS Namespaces

- After you click Next, you are prompted to specify the namespace type, as shown.
- If you install the DFS namespaces role on a domain controller, you will be able to select *Domain-based namespace.*
- Domain-Based Namespace
  - This type stores the location and configuration of the DFS namespace within Active Directory, such that it is available to all other domain controllers that have the DFS namespaces role installed.



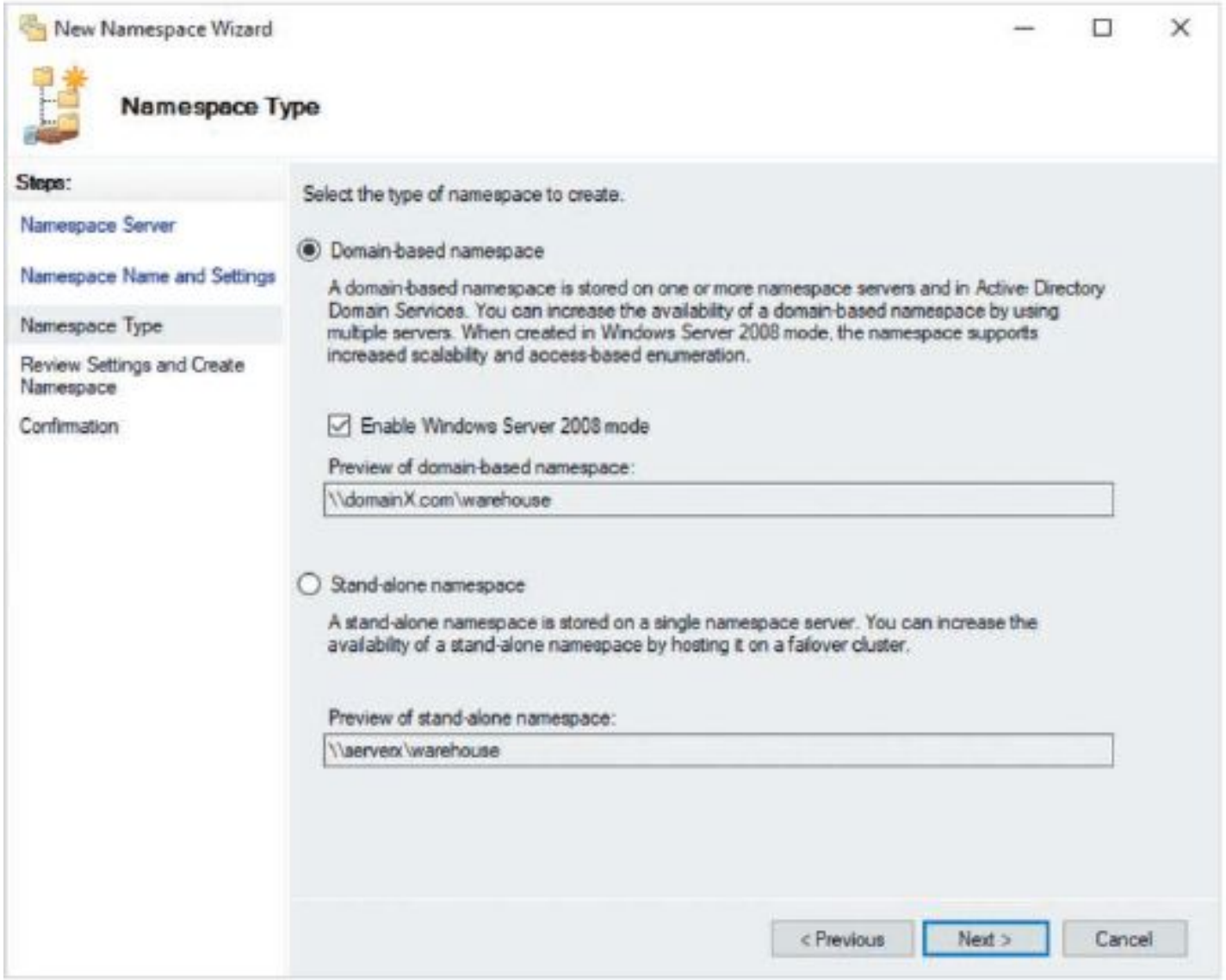
# Configuring DFS Namespaces

- Domain-Based Namespace
  - This type stores the location and configuration of the DFS namespace within Active Directory, such that it is available to all other domain controllers that have the DFS namespaces role installed.
  - If a single domain controller fails, another domain controller will provide users access to the DFS namespace.
  - Instead of remembering a DFS server name, users can connect to a domain-based namespace using their domain name.



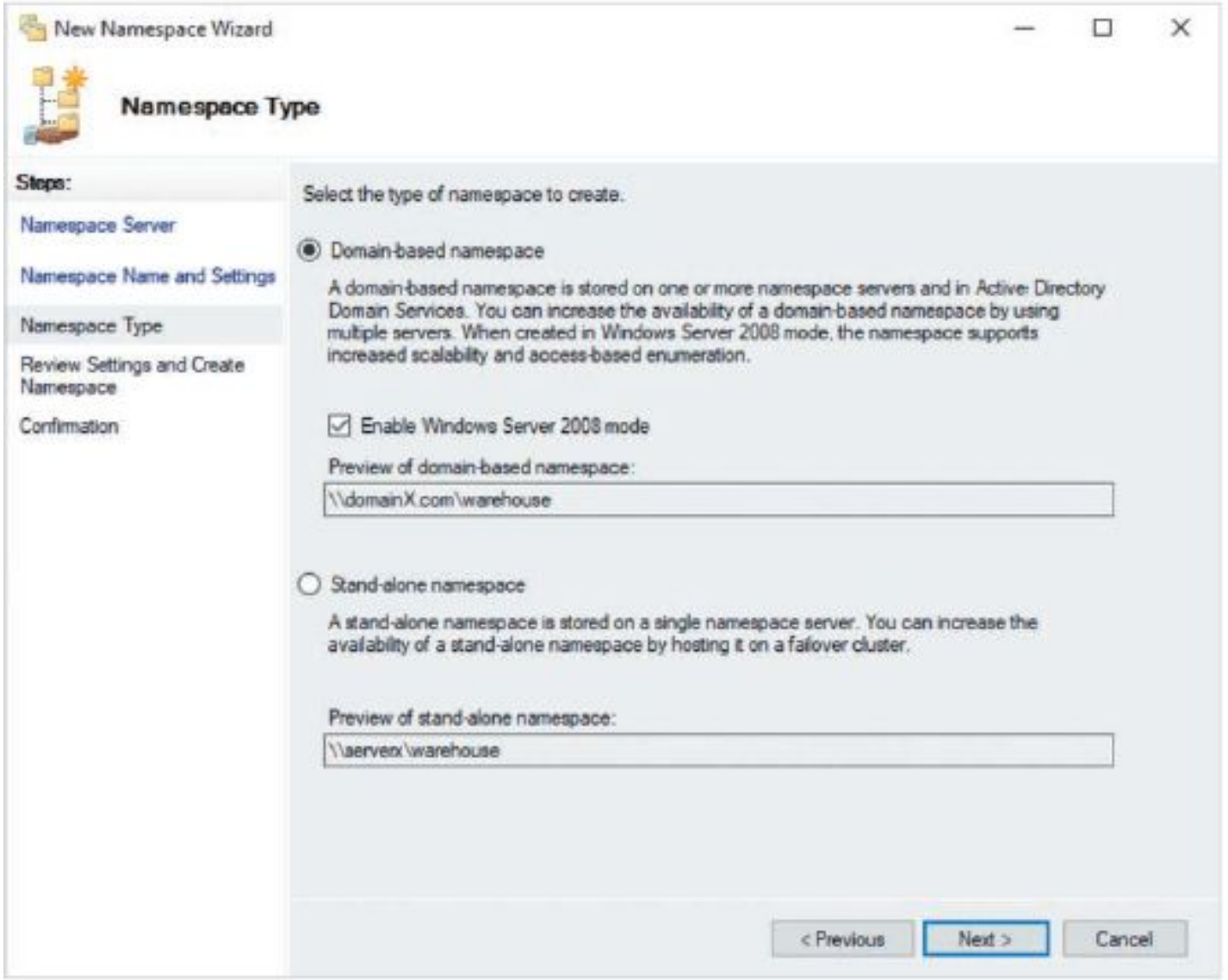
# Configuring DFS Namespaces

- Domain-Based Namespace
  - To connect to the warehouse DFS namespace, users will be able to specify the Universal Naming Convention (Ex. \\servername\sharedfoldername) syntax used when connecting to shared SMB resources, on which shown is `\\domainX.com\warehouse`.
  - If your domain functional level is Windows Server 2008 or higher, you can select *Enable Windows Server 2008 mode* to create more than 5000 targets, as well as use the access-based enumeration feature to display only targets that provide the user at least Read share and



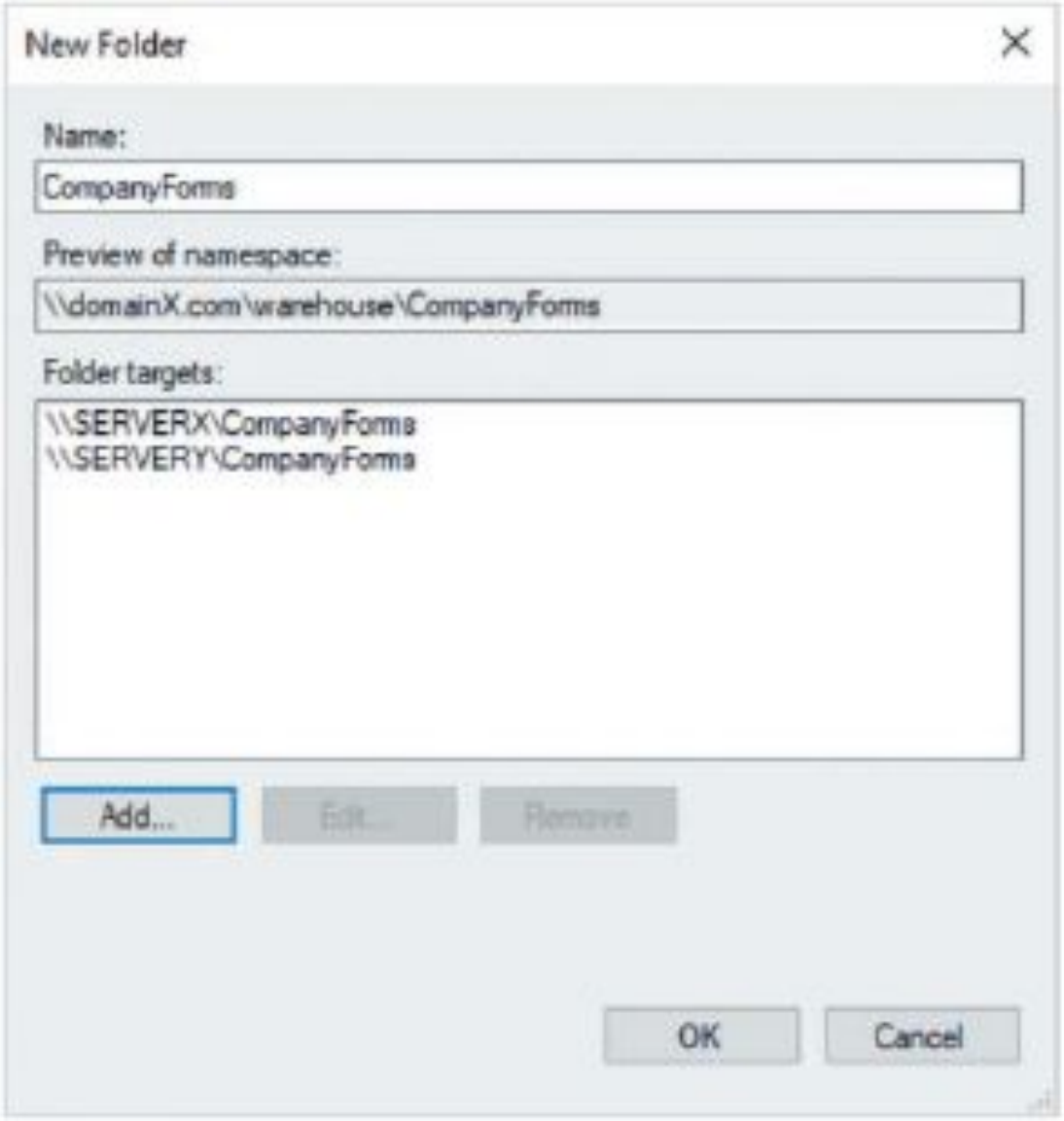
# Configuring DFS Namespaces

- Stand-alone namespace
  - stores the namespace configuration on the local file server and is the only option available if the file server is not a domain controller.
  - Users will need to specify the server name within a UNC (e.g., `\\serverx\warehouse` in order to access the DFS namespace shared folder.



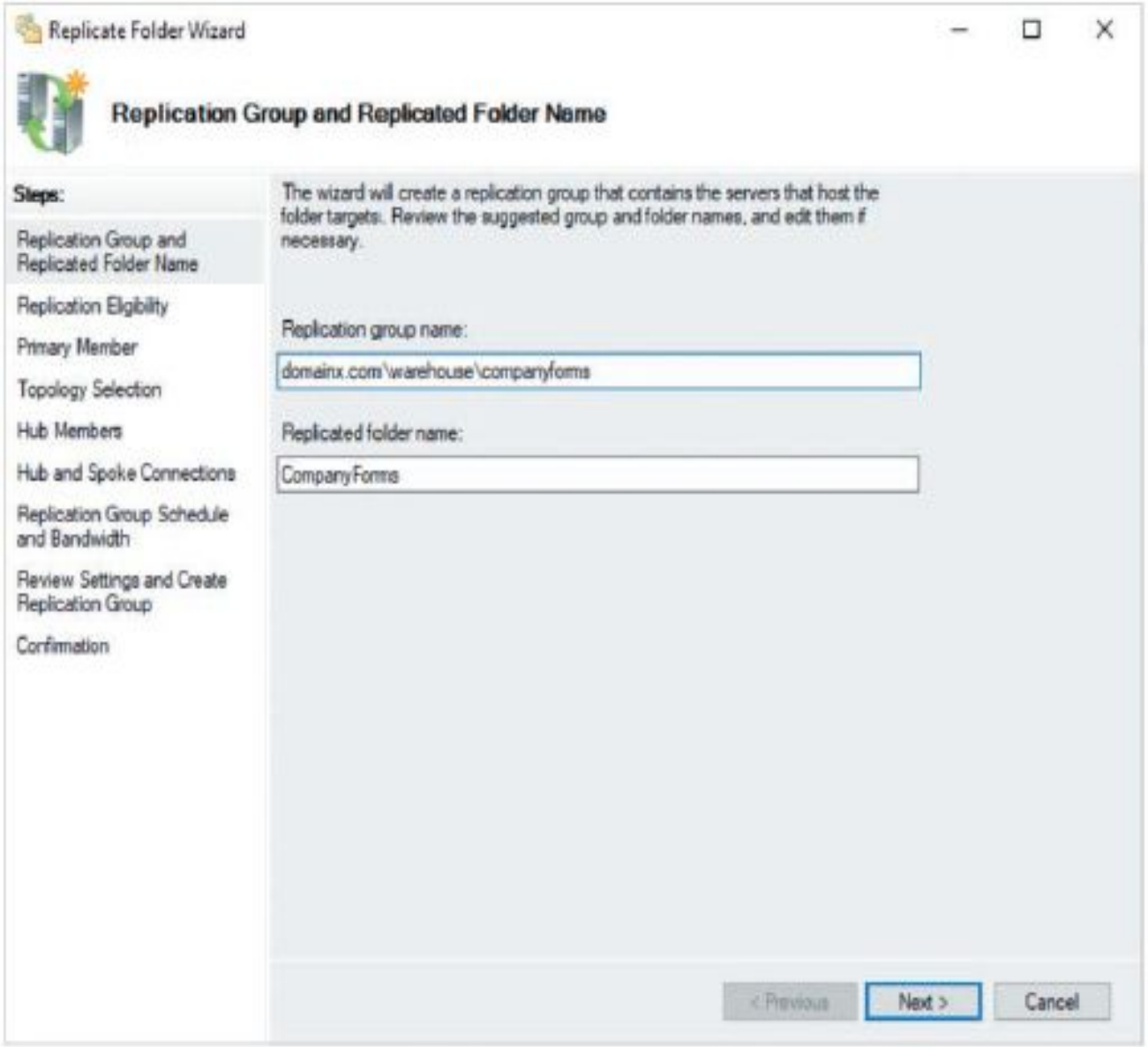
# Configuring DFS Namespaces

- Click Next, you can click Create to create the DFS namespace. Next, you can add targets to the DFS namespace that represent the shared folders within your organization.
- To add a target to your DFS namespace within the DFS Management tool, you can highlight your DFS namespace and click New Folder in the Actions pane. This will display the New Folder window shown.
- The CompanyForms target shown in figure will only appear once under the DFS namespace. However, users that select the CompanyForms target will be forwarded to the CompanyForms share on the server (either SERVERX or SERVERY) that is within their Active Directory



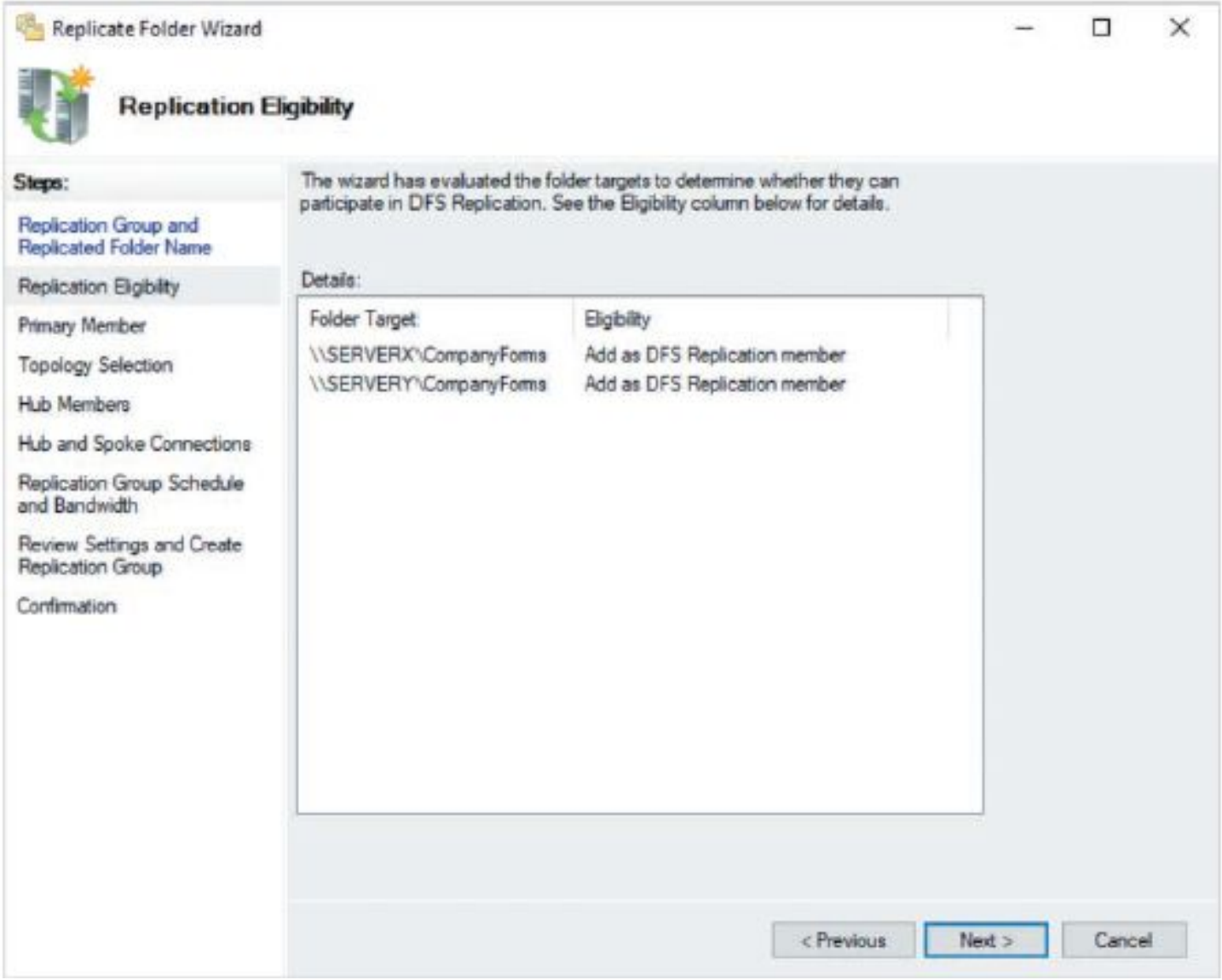
# Configuring DFS Replication

- To configure folders on two or more file servers to synchronize contents, you must first create a **DFS replication group**. To create a DFS replication group, you can click New Replication Group within the DFS Management console shown and specify the appropriate settings within the New Replication Group wizard.
- If you add a target that contains more than one UNC to a DFS namespace, the DFS Management tool will give you the option to automatically create a replication group that keeps the content within each shared folder synchronized using DFS replication.
- If you click OK in previous figure and then click Yes when prompted to create a replication group, the Replicate Folder Wizard shown in Figure 5-37 will create a replication group and prompt you for the remaining configuration



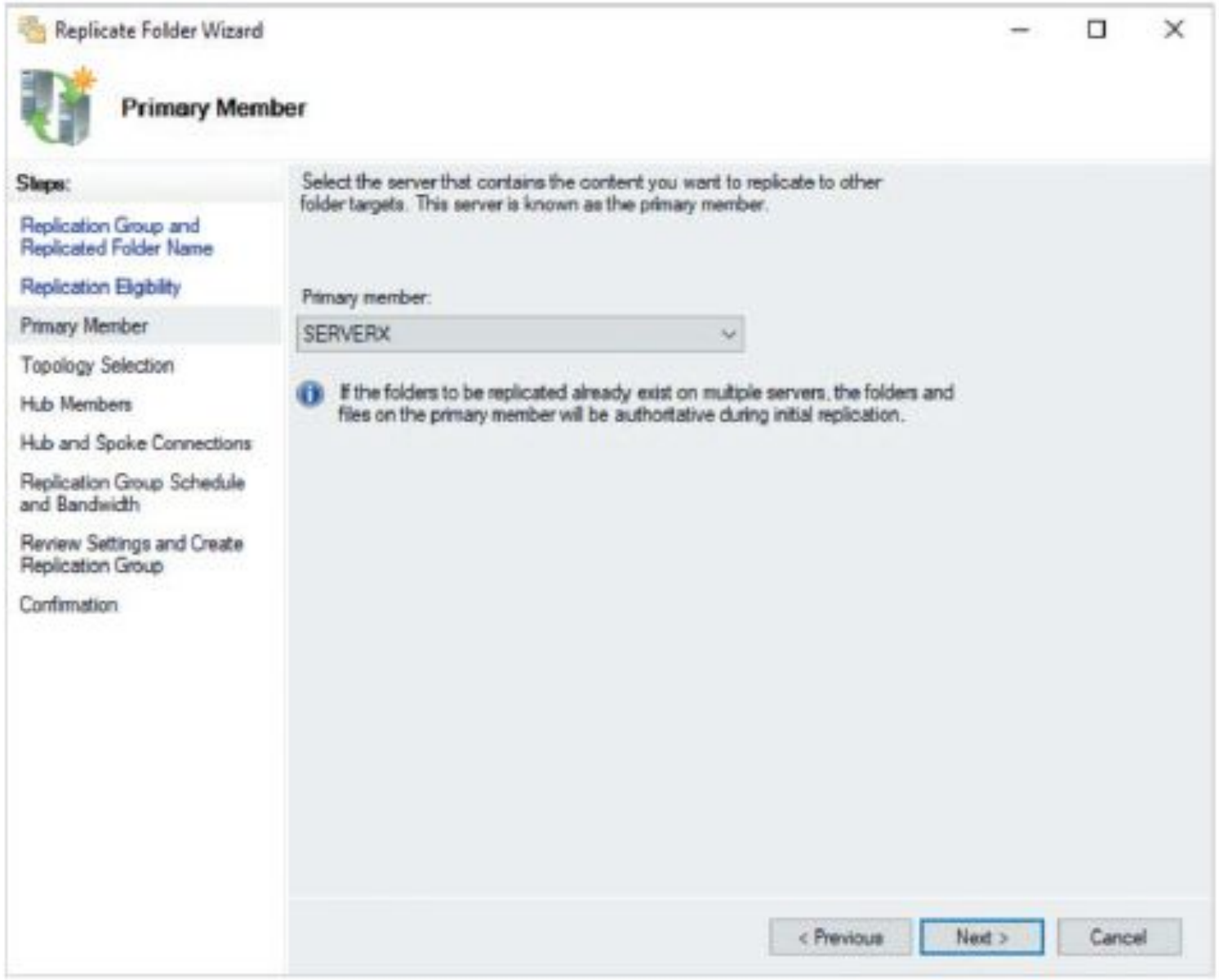
# Configuring DFS Replication

- When you click Next, the replicated folders on each server will be displayed, as shown.
- If the folders on each server contain files with identical names and different contents, the initial DFS replication will need to ensure that one copy overwrites the other.



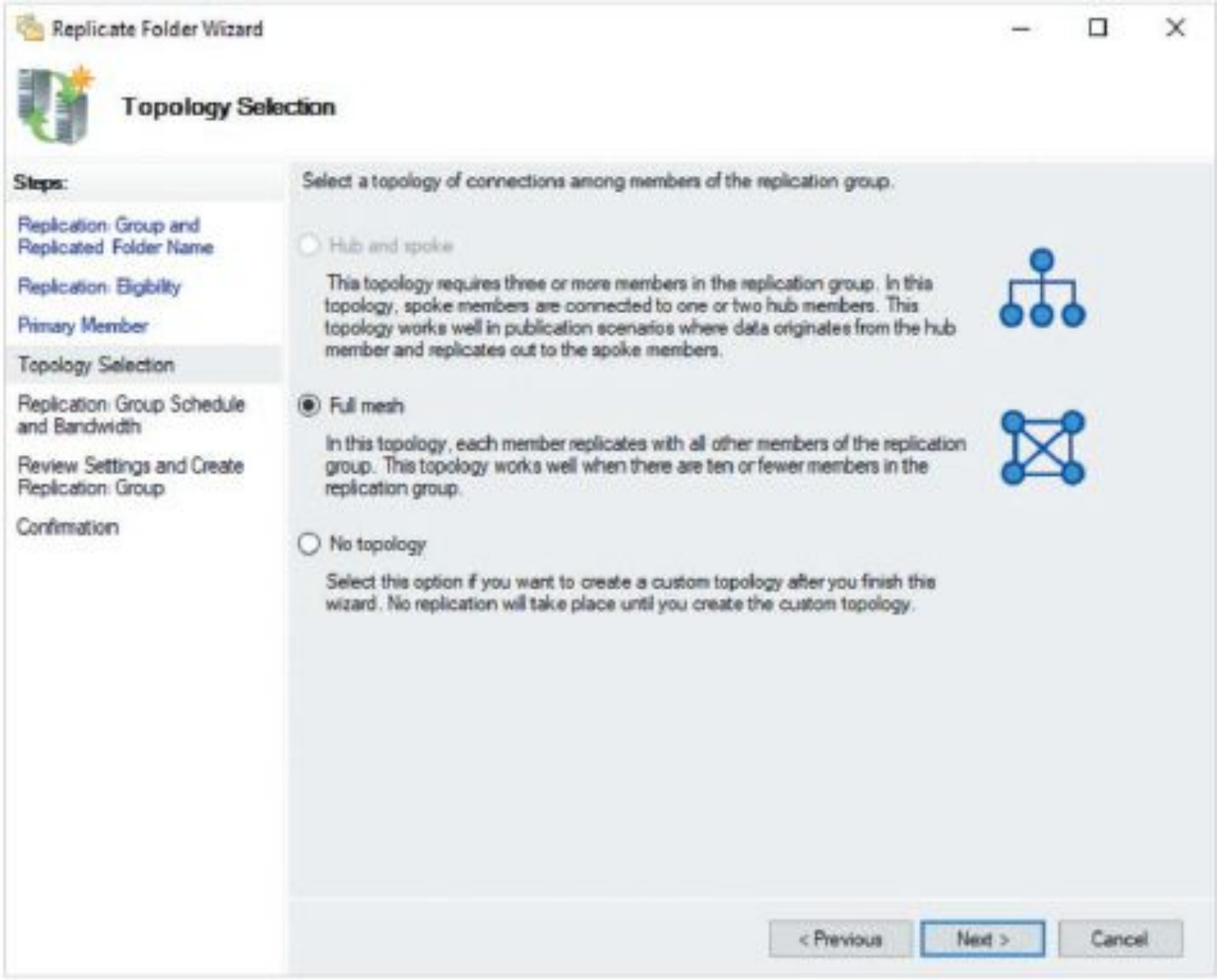
# Configuring DFS Replication

- When you click Next, you can select the server whose file contents should overwrite other copies during the initial DFS replication, as shown.



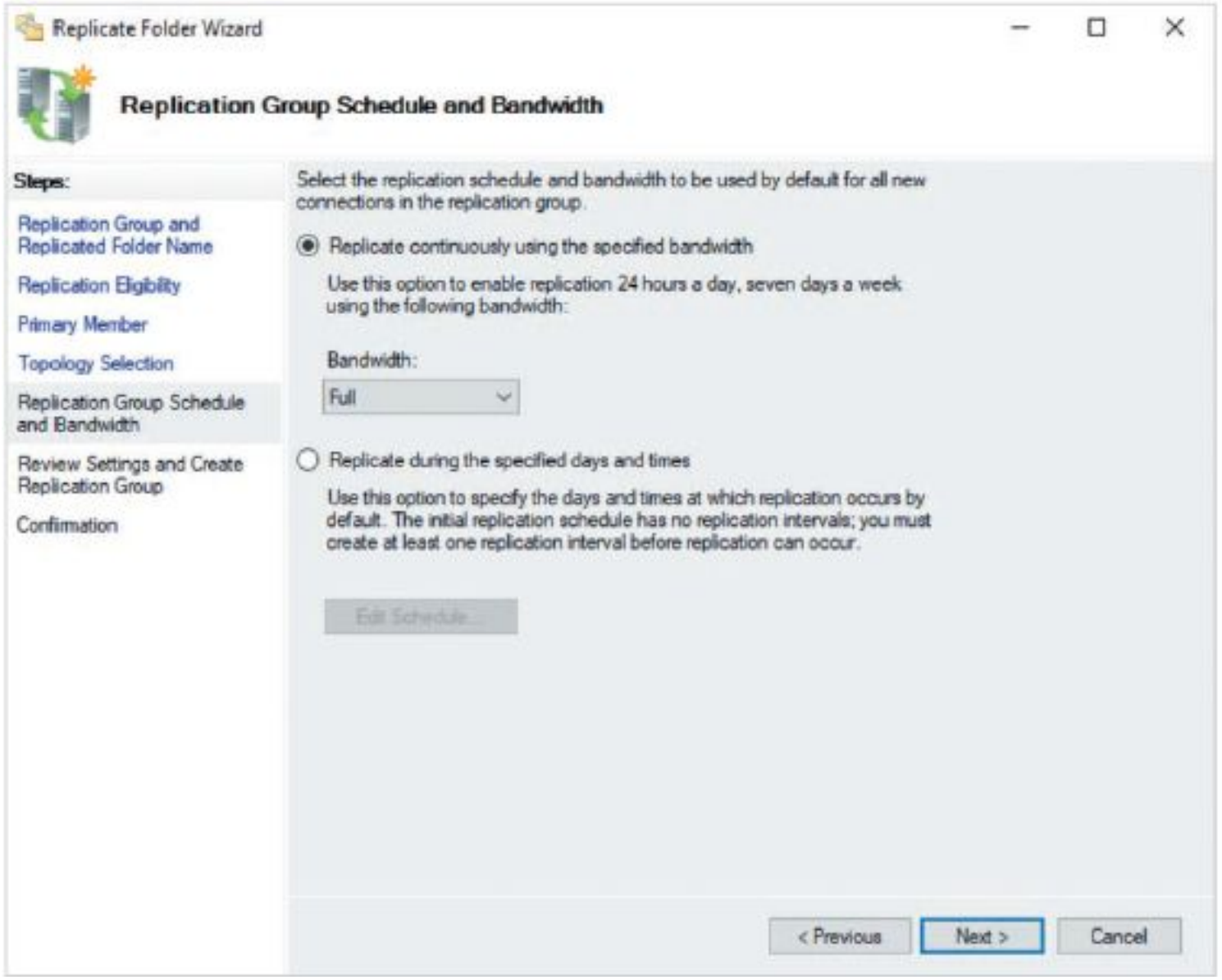
# Configuring DFS Replication

- After clicking Next, you will be prompted to select the DFS replication topology as shown.
- The *Full mesh* topology selected allows each server within the replication group to replicate directly to all other members, consuming additional network bandwidth as a result.
- If you have three or more members within the replication group, selecting *Hub and spoke* will force replication to occur via a central member to minimize network traffic.



# Configuring DFS Replication

- To ensure that replicated folder contents are updated immediately, the DFS replication service runs at all times of the day on each server within the replication group by default.
- Moreover, the DFS replication service is permitted by default to use all available network bandwidth provided by the network interface of each system.
- However, when you click Next, you can optionally restrict the days and times that the DFS replication service is allowed to run, and the network bandwidth it can use, as shown.



# Implementing Quotas and File Screens

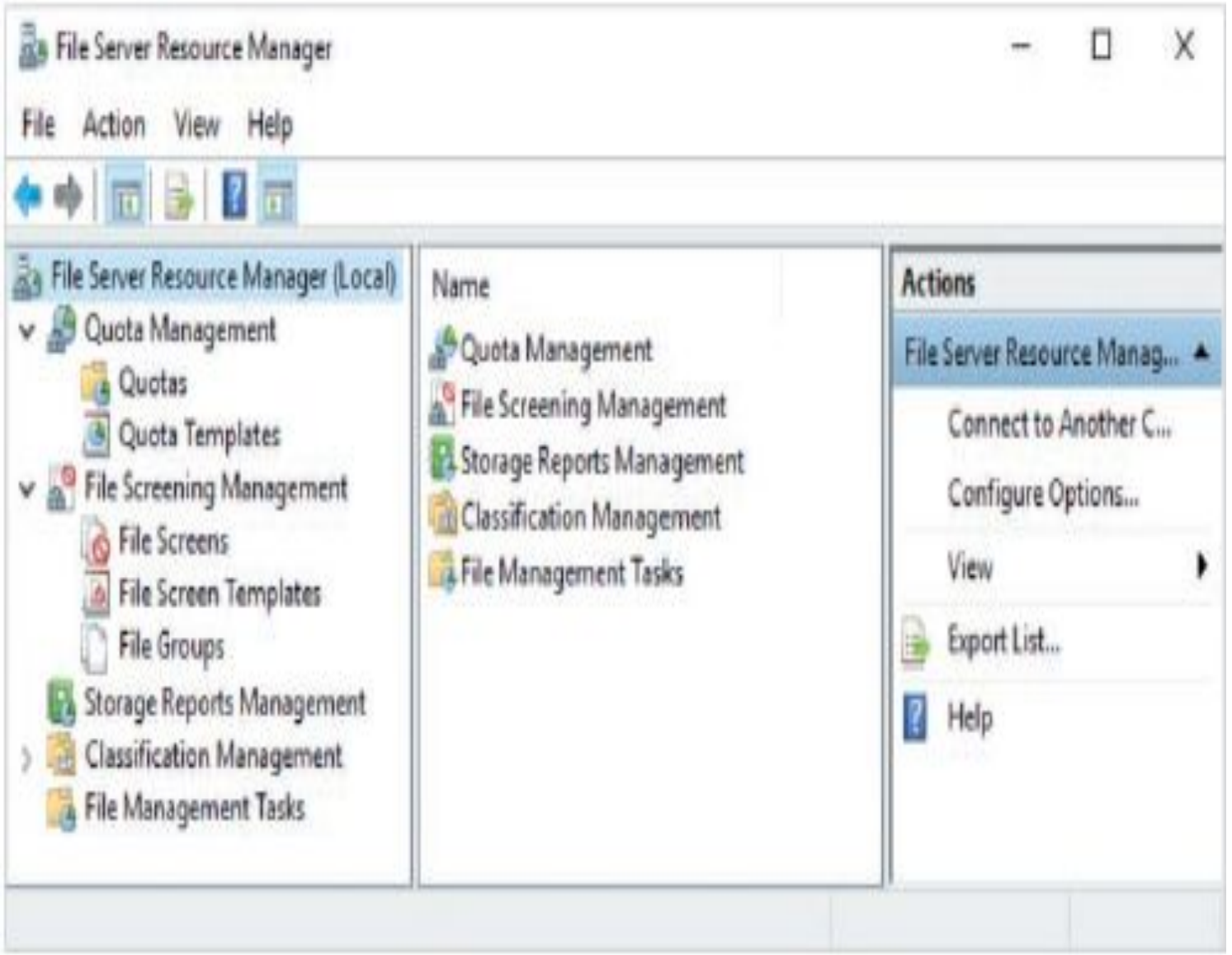
- When you share folders on an NTFS filesystem that provide permissions for users to add files and subfolders, you may need to configure additional restrictions on the size and type of files that users can add. These restrictions can prevent users from consuming too much space on your file server, or block users from adding the wrong type of files to shared folders.
- NTFS provides three features that allow you to restrict the content that users can store within folders on the filesystem:
  - **User quotas** can be configured to limit the space that users can consume within the filesystem.
  - **Folder quotas** can be configured to limit the space consumed by a folder on the filesystem.
  - **File screens** can be configured to prevent certain types of files (such as audio and video files) from being stored within a folder on the filesystem.
- Before configuring folder quotas and file screens, you must first install the File Server Resource Manager server role on your file server. To install this server role within the Add Roles and Features Wizard in Server Manager, you must first expand File and Storage Services, and then

# Configuring User Quotas

- NTFS user quotas are not enabled on each filesystem by default. To enable NTFS quotas for a filesystem, you can right-click the root folder of a filesystem (e.g., C:\) within File Explorer, click Properties, highlight the Quota tab, and select the appropriate options.
- You can also click the Quota Entries button to provide specific quota options for individual users and groups that override the default options shown.
- By default, member of the Administrators group receive no limits.

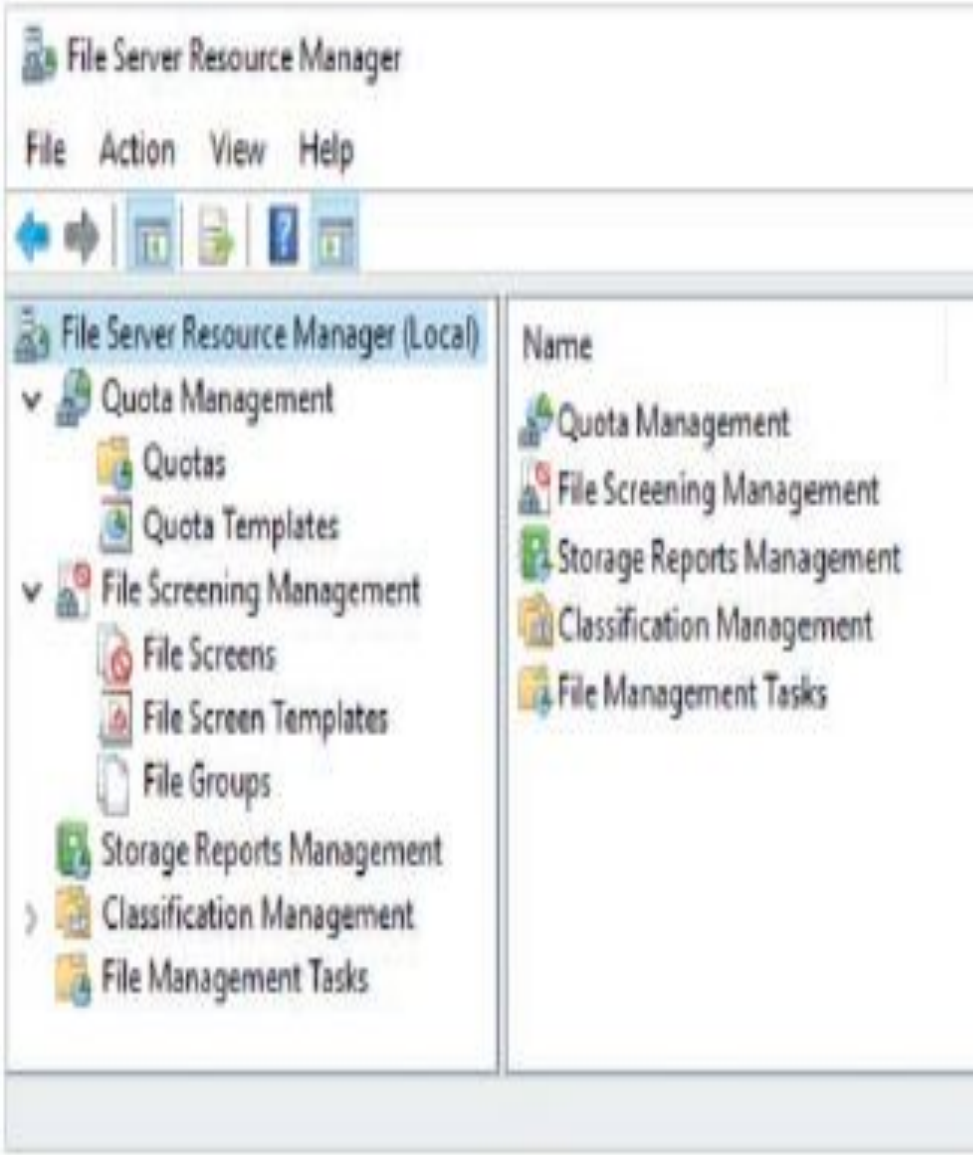
# Configuring Folder Quotas

- Folder quotas can be configured to prevent users from storing files after a limit has been reached (called a **hard quota**) or allow the limit to be surpassed (called a **soft quota**).
- Moreover, when a percentage of the limit has been reached, folder quotas can be configured to email a user, log an event to the Windows Server 2019 System log, run a command, or generate a report.
- To configure folder quotas, you can select File Server Resource Manager from the Tools menu within Server Manager to start the File Server Resource Manager tool as shown



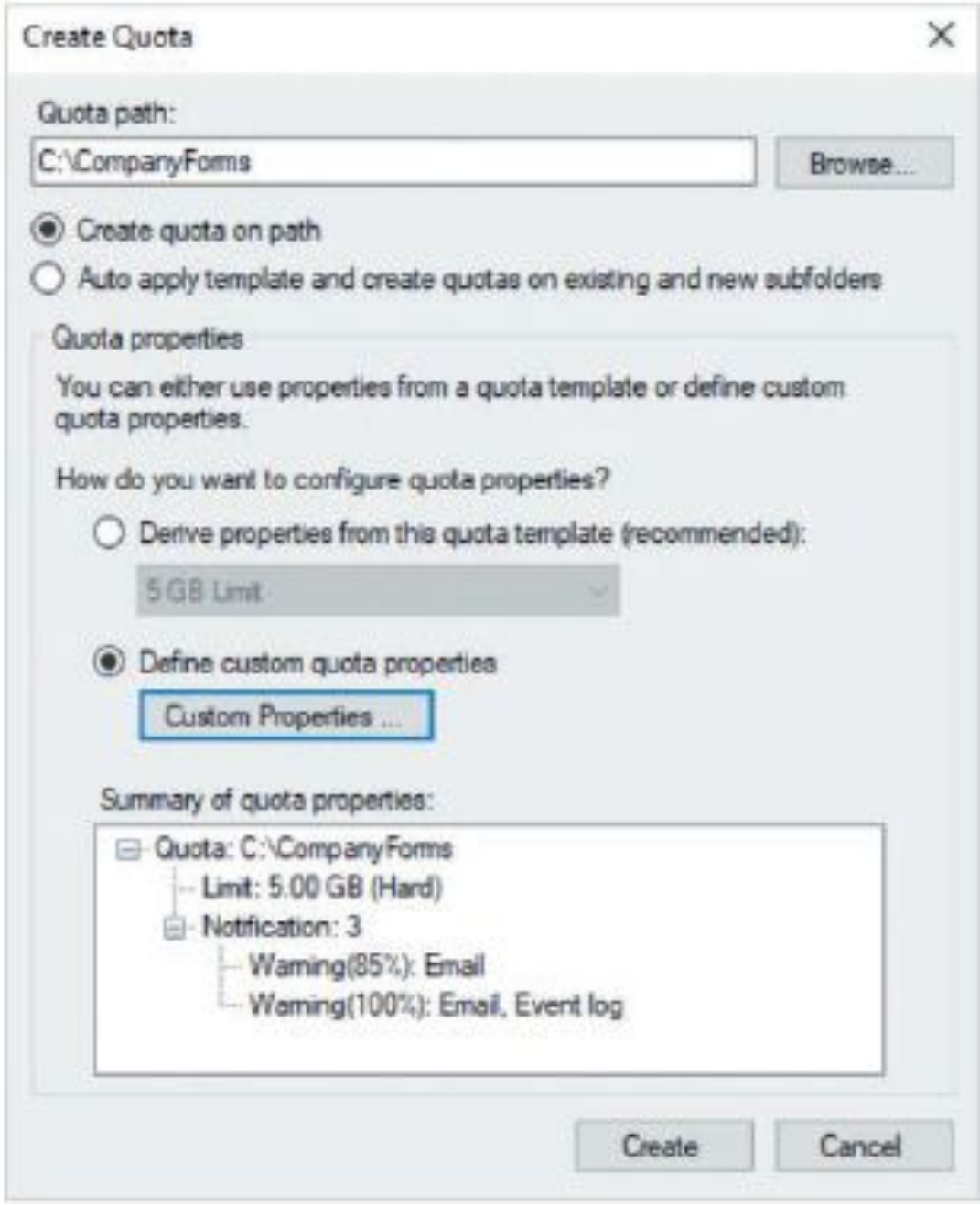
# Configuring Folder Quotas

- The Quota Management section within the navigation pane of the File Server Resource Manager tool contains two subfolders:
  - *Quotas* stores quota entries for folders on NTFS filesystems. There are no quota entries configured in this folder by default.
  - *Quota Templates* stores templates that contain quota settings that can be used to simplify the creation of new quota entries. There exist several default quota templates within this folder.



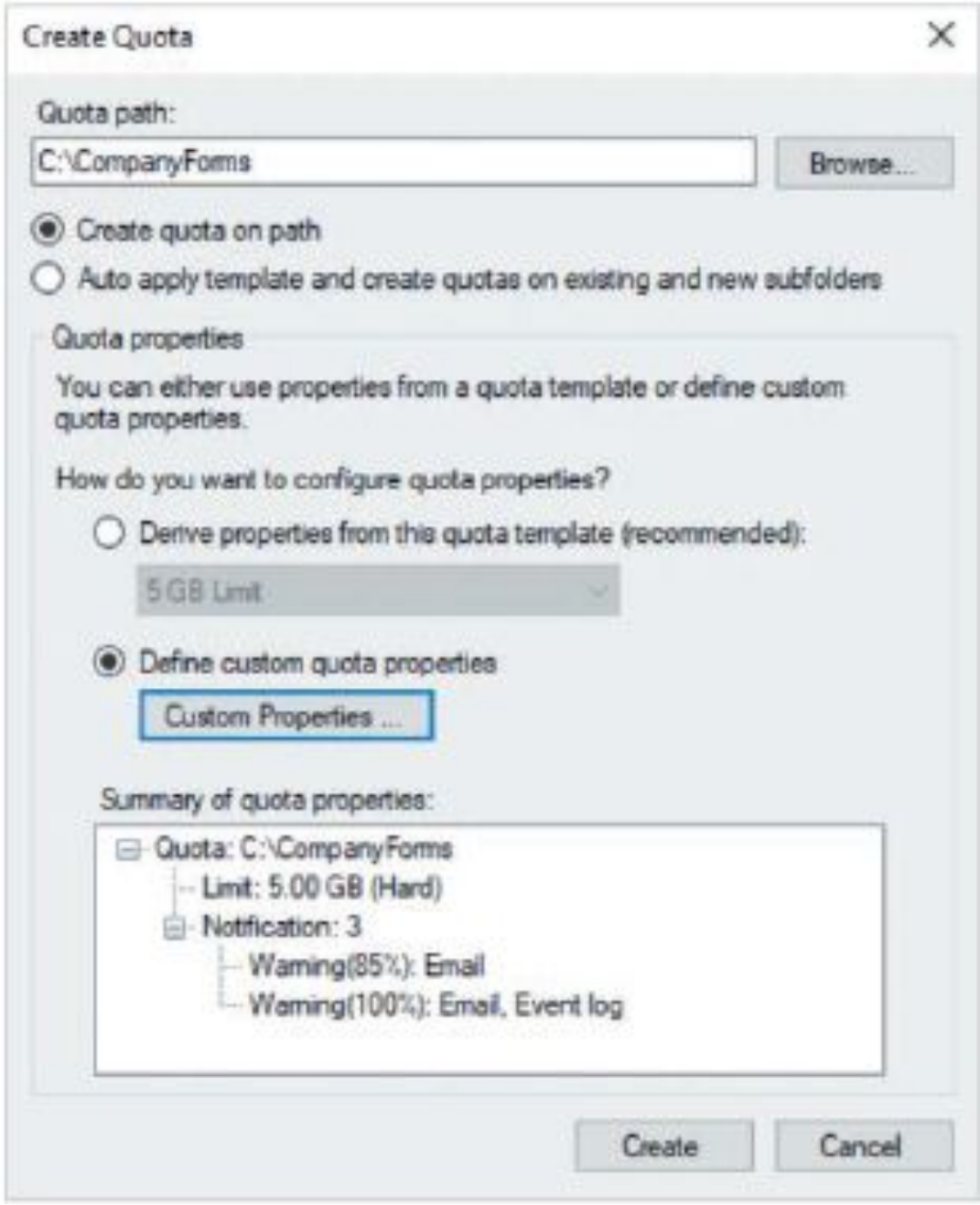
# Configuring Folder Quotas

- To create a new folder quota, you can highlight the Quotas folder with the File Server Resource Manager tool, click Create Quota within the Actions pane, and specify the appropriate folder path and settings, as shown.
- The quota for the C:\ CompanyForms folder shown prevents the folder from storing more than 5 GB of content, emails a warning to the user who reaches 85% and 100% of the 5 GB limit, as well as logs an event to the Windows Server 2019 System log when the 5 GB limit has been reached. To modify these settings, you can click the Custom Properties button and select the appropriate options.



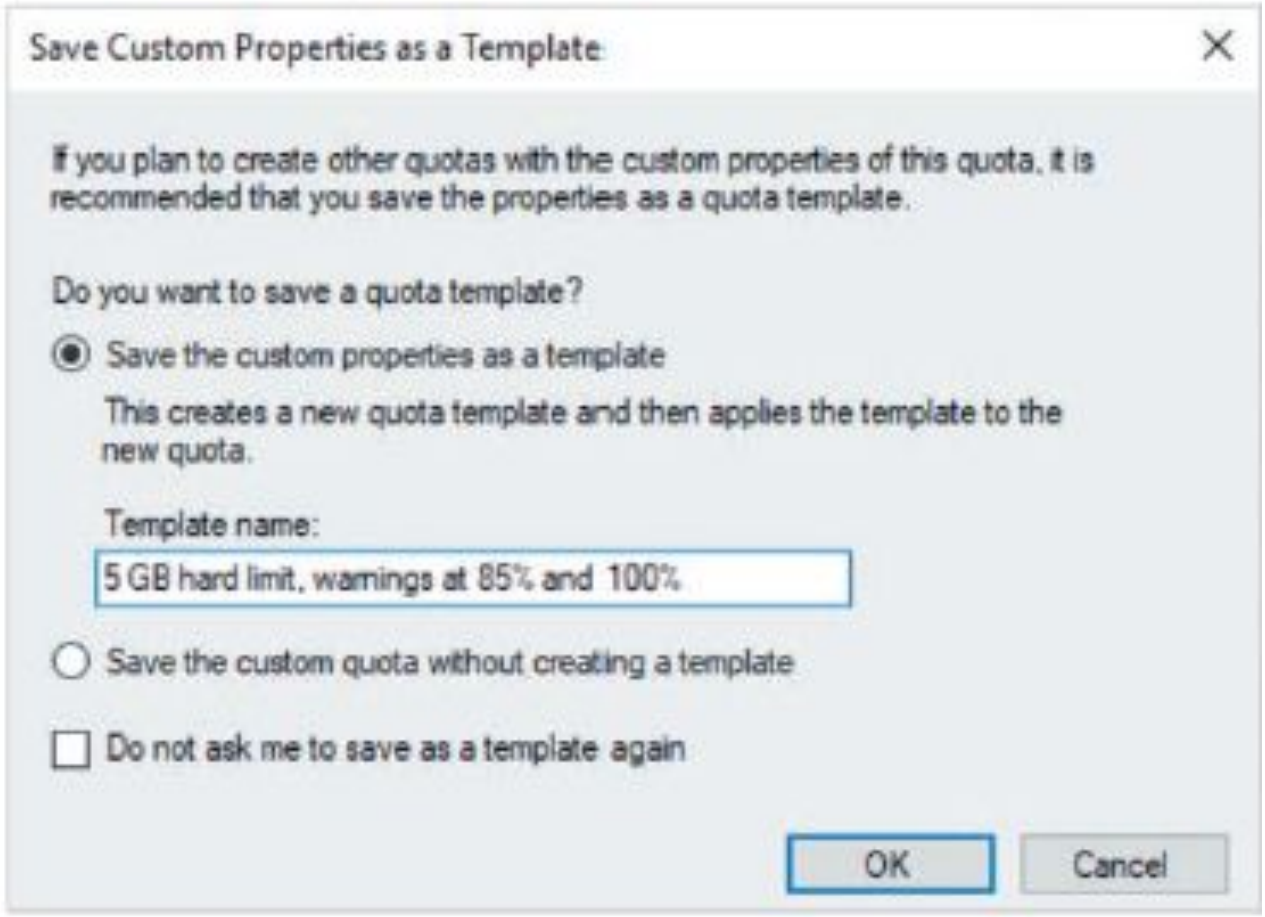
# Configuring Folder Quotas

- If you select *Derive properties from this quota template (recommended)*, you can select a pre-configured template from the drop-down box to copy the quota settings from that template.
- You can select *Auto apply template and create quotas on existing and new subfolders* to create folder quotas on existing and new subfolders of C:\CompanyForms based on the template you chose.
- Click Create, you can optionally save your quota settings in a new quota template for future use, as shown



# Configuring Folder Quotas

- Click Create on previous figure, you can optionally save your quota settings in a new quota template for future use, as shown

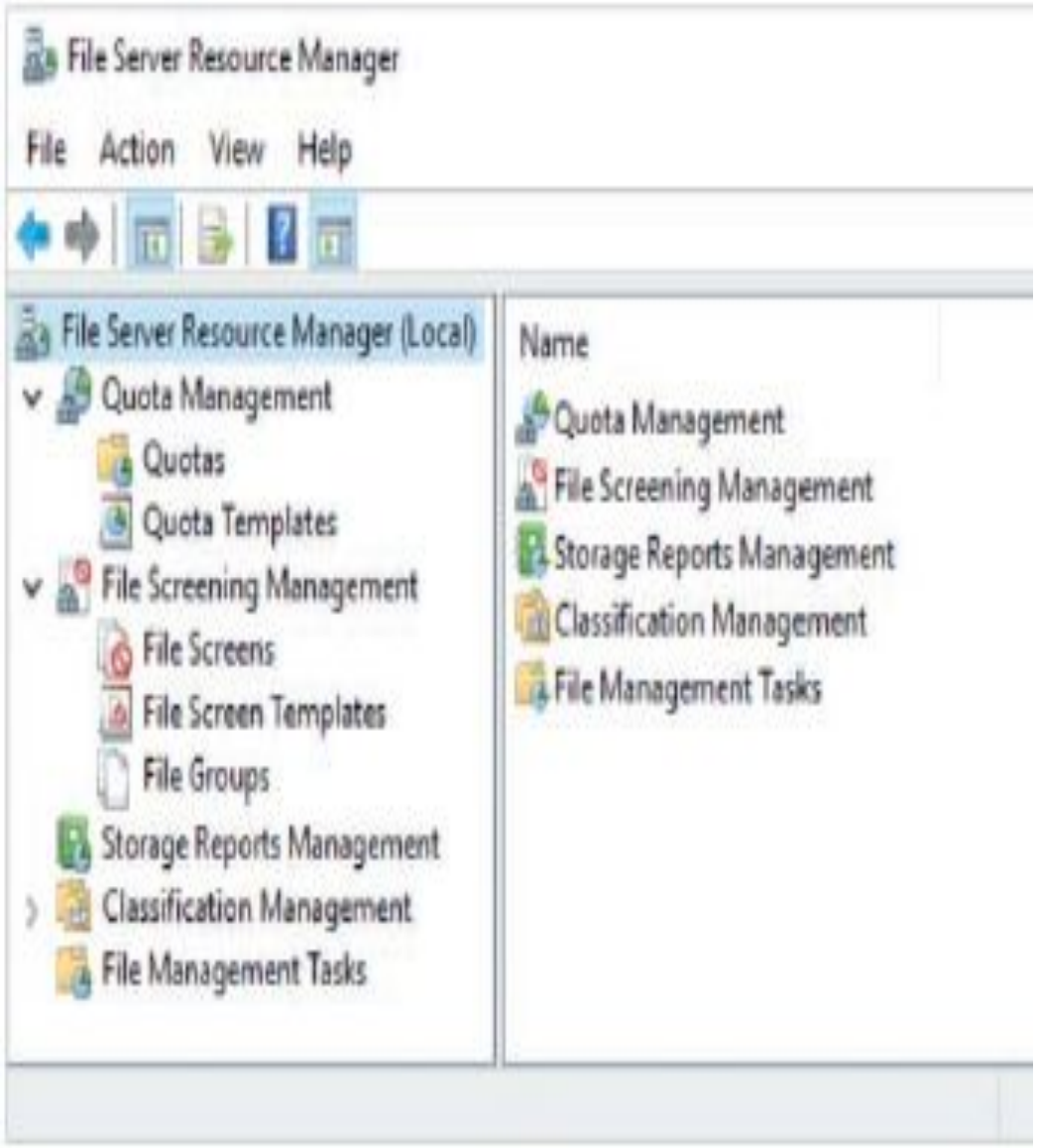


# Configuring File Screens

- File screens can be used to prevent users from storing files of a certain category within folders on an NTFS volume (called an **active screening**), or log an event when this occurs (called **passive screening**).
- Each category is called a **file group**, and consists of one or more filename extensions. For example, the default Text Files file group consists of files that end with .asc, .text, and .txt.
- Moreover, when an active or passive screening event occurs, file screens can be configured to email a user, log an event to the Windows Server 2019 System log, run a command, or generate a report.

# Configuring File Screens

- You configure file screens within the File Server Resource Manager tool. The File Screening Management section within the navigation pane of the File Server Resource Manager tool contains three subfolders:
  - *File Screens* stores file screen entries for folders on NTFS filesystems. There are no file screen entries configured by default.
  - *File Screen Templates* stores templates that contain file screen settings that can be used to simplify the creation of new file screens. There exist several default file screen templates within this folder.
  - *File Groups* stores file groups that identify file categories by filename extension. The default file groups stored within this folder include Audio and Video Files, Backup Files, Compressed Files, E-mail Files, Executable Files, Image Files, Office Files, System Files, Temporary Files, Text Files, and Web Page Files.



# Configuring File Screens

- To create a new file screen, you can highlight the File Screens folder with the File Server Resource Manager tool, click Create File Screen within the Actions pane, and specify the appropriate folder path and settings, as shown.
- The file screen for the C:\CompanyForms folder shown prevents the folder from storing audio, video, and executable files. To modify these settings, you can click the Custom Properties button and select the appropriate options.
- If you select *Derive properties from this file screen template (recommended)*, you can select a pre-configured template from the drop-down box to copy the file screen settings from that template.