# **Module 5**

**Configuring Resource Access**

|  |
| --- |
| **At a Glance** |

#### Instructor’s Manual Table of Contents

* Overview
* Objectives
* Teaching Tips
* Quick Quizzes
* Class Discussion Topics
* Additional Projects
* Additional Resources
* Key Terms

|  |
| --- |
| Lecture Notes |

# **Overview**

You begin this chapter by teaching your students how to use attributes and permissions to manage who accesses folders and files. They will learn how to use the Encrypting File System to guard important resources and how to customize access through advanced permissions and ownership. They will also learn how to create an audit trail from historical data about who has accessed information. Your students will explore the steps for configuring information to be shared over the network using UNIX, Linux, macOS, and Windows computers, and they will learn how to publish shared folders in Active Directory. Your students will additionally find out how to install and set up the Distributed File System for coordinating and backing up a system of shared information. Finally, they will examine how to avoid overloaded disks by setting up disk quotas.

# **Module Objectives**

* Describe the use and configuration of folder and file attributes
* Identify the permissions available for NTFS and ReFS folders and files
* Configure file ownership, permissions, and auditing
* Share folders using SMB and NFS
* Publish shared folders to Active Directory
* Implement DFS namespaces to simplify shared folder access
* Configure DFS replication to synchronize folder contents
* Restrict content using user quotas, folder quotas, and file screens

# **Teaching Tips**

**Configuring Folder and File Attributes**

1. Define the term *attributes* as the features of a folder or file that are used by a filesystem.
2. Define the term *metadata* as a component that stores information about a folder or file.
3. Explain what folder and file characteristics are stored in the metadata component.

**Working with Basic Attributes**

1. Review the two main filesystems supported by Windows Server 2019: NTFS and ReFS.
2. Discuss the two additional filesystems supported by Windows Server 2019: FAT32 and exFAT.
3. Emphasize that each of these filesystems contains two basic attributes that are compatible with the original FAT filesystem: read-only and hidden.
4. Refer to Figure 5-1 and explain how to view and set these attributes, by right-clicking a folder or file within a File Explorer window and clicking Properties. Point out that both attributes are listed at the bottom of the General tab.
5. Explain what happens when an administrator enables the read-only attribute for a file.
6. Explain what happens when an administrator enables the read-only attribute for a folder.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Most Windows Server 2019 administrators ignore the read-only attribute box and set the equivalent protection using permissions instead, because permissions apply to the folder and can be inherited by its files. |

1. Mention why folders and files are assigned the hidden attribute.
2. Refer to Figure 5-2 and review the ways to view hidden folders and files.

* Add an option to a command to view the folder or file
* Configure File Explorer to view hidden folders and files by clicking the View menu and enabling the Hidden items checkbox

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | If an administrator modifies an attribute on a folder, he or she will be prompted about whether to apply that change to only the folder or to the files and subfolders within that folder as well. |

**Working with Advanced Attributes**

1. Introduce the four advanced attributes NTFS offers for folders and files: archive, index, compress, and encrypt.
2. Refer to Figure 5-3 and explain how to open the Advanced Attributes window to access these attributes by clicking the Advanced button on the General tab for a folder or file.
3. Describe characteristics of the archive attribute.
4. Describe characteristics of the index attribute.
5. Describe characteristics of the compress attribute.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Because compression and decompression result in additional processor calculations, the compress attribute is not enabled by default and is typically enabled only on files that are accessed infrequently, such as accounting documents from a previous fiscal year. If an administrator sets the compress attribute on a large number of frequently accessed files, the server performance may degrade significantly. |

1. Describe characteristics of the encrypt attribute.
2. Explain that the encrypt attribute indicates an encryption algorithm should be used to protect data before it is written to the filesystem.
3. Define an encryption algorithm as a series of mathematical steps used in sequence to scramble data. Explain how a key is used in the encryption process.
4. Distinguish between symmetric and asymmetric encryption. Discuss how public and private keys are used in the encryption process.
5. Explain why an administrator cannot enable the encrypt and compress attributes on the same file.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Because sensitive documents are often stored within the same folder, when an administrator encrypts a file, he or she is prompted about whether to encrypt the file or the parent folder. |

1. Explain how the Encrypting File System (EFS) filesystem feature works within a workgroup or Active Directory domain environment.
2. Discuss how keys are stored in both environments.
3. Mention that to prevent data from being lost in an Active Directory environment in the event of a password reset, each time an administrator encrypts a file using a domain user account, a second copy of the symmetric key is added to the file’s metadata and encrypted with a recovery agent public key.
4. Point out that the default recovery agent is the Domain Admins group in the domain, and describe activities members of the Domain Admins group can do and what others can do in terms of encrypting files.
5. Refer to Figure 5-4 and explain how to open the User Access window, where an administrator can add additional users, remove existing users, or even back up EFS keys.
6. Explain what happens to a file’s encryption settings when an administrator copies or moves the encrypted file to another folder within an NTFS, FAT32, or exFAT filesystem on the same computer or removable media.
7. Explain what happens to a file’s encryption settings when an administrator copies or moves 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.
8. Emphasize that if an administrator copies or moves a file to a filesystem that does not support EFS (such as ReFS, or FAT32 on a Windows 7 system), the file is automatically decrypted.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | For more information regarding EFS, please see the following Web site: <https://en.wikipedia.org/wiki/Encrypting_File_System> |

**Managing Folder and File Security**

1. Introduce the topic by reminding students that creating user and group accounts are the initial steps for sharing resources, such as folders, files, and printers.
2. Explain that the next steps are to modify the access control lists (ACLs) on each resource and then to set them up for sharing.
3. Introduce the two types of ACLs Windows Server 2019 uses: discretionary and system.
4. Define a discretionary access control list (DACL) as the record of permissions given to user and group accounts, which is used to grant or deny access to the resource.
5. Define a system access control list (SACL) as the entity that contains information used to audit the access to the resource.
6. Discuss how ownership of a resource is defined when the resource is created. Discuss the rights a resource owner has for a that resource.
7. Note that folders and files on an NTFS or ReFS filesystem support both DACLs and SACLs.

**Configuring Folder and File Permissions**

1. Explain how to view and configure the DACL for a folder or file on an NTFS or ReFS filesystem using the File Explorer window.
2. Refer to Figure 5-5 to illustrate the file Properties window in the File Explorer window. Note that the Security tab is highlighted.
3. Refer to Table 5-1 and review the folder and file permissions supported by NTFS and ReFS.
4. Refer to Figure 5-5 again and explain that the built-in SYSTEM group (which represents operating system components) is allowed Full control permission to a file, which includes all other permissions on the file. Point out that these permissions are grey, which indicates that they were not set on the file directly but instead were inherited from the parent folder that contains the file.
5. Refer to Figure 5-6 to illustrate the Permissions window that appears when an administrator clicks Edit in Figure 5-5. Explain that the Permissions window allows an administrator to add or remove existing users or groups, as well as set their basic permissions.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | When an administrator sets permissions on a folder, those permissions are inherited by default by files and subfolders. |

1. Refer to Table 5-2 an review advanced permissions supported by NTFS and ReFS that provide a specific type of access. Note that these advanced permissions can be used if the basic permissions do not suit an administrator’s needs.
2. Refer to Figure 5-7 to illustrate the Advanced Security Settings window that appears when an administrator clicks Advanced in Figure 5-5.
3. Refer to Figure 5-8 to illustrate the Permission Entry window that results from clicking Add in the Advanced Security Settings window in Figure 5-7, where an administrator can select a security principal and indicate whether to allow or deny permissions to the security principal, as well as the associated permissions.
4. Mention that an administrator can click Disable inheritance in Figure 5-7 to prevent parent folder permissions from being inherited by the selected file. When an administrator clicks this button, he or she will be prompted to either remove the inherited permissions or convert any previously inherited permissions to explicit permissions on the file that the administrator can modify afterwards.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Stress that administrators should 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**

1. Explain that each folder and file on a system must have an owner, which, by default, is the user that created the file.
2. Mention that an owner of a folder or file is able to transfer the ownership to another user.
3. Explain that if a user is granted the Take ownership advanced permission or Full control permission to a folder or file, the user can change the owner of it to himself or herself.
4. Explain how to modify the owner of a folder or file.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | If an administrator creates a folder or file as the Administrator user, the Administrators group automatically becomes the owner of it. |

**Troubleshooting Folder and File Permissions**

1. Introduce this topic by explaining that sometimes an administrator configures folder or file access for a user but finds that the user does not actually have the type of access the administrator set up.
2. Present an example where a user within an organization requires the ability to maintain all files within the C:\Blueprints folder. As a result, the administrator grants 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.
3. Explain that one way to troubleshoot a problem with a folder is for the administrator to review the permissions that have been assigned on the folder to the user, as well as all groups to which the user belongs, taking permission inheritance into consideration.
4. Refer to Figure 5-9 and explain another way to troubleshoot the problem by using the Advanced Security Settings window for the folder and highlighting the Effective Access tab. Next, the administrator can click Select a user to choose the appropriate user account, and then click View effective access to list the effective permissions.
5. Discuss the permission-related problems can occur after a file or folder is copied or moved.
6. List the ways file and folder permissions are affected when a file or folder is created, copied, or moved.

**Configuring Folder and File Auditing**

1. Introduce this topic by explaining that folder and file auditing allows an administrator to track activity on a folder or file, such as read or write activity.
2. Discuss different scenarios where organizations might choose to implement auditing on folders and files.
3. Mention that Windows Server 2019 allows an administrator to audit successful and failed attempts to access folders and files using a combination of any or all of the basic or advanced permissions.
4. Emphasize that the audit configuration is stored within the SACL on the folder or file.
5. Refer to Figure 5-10 to illustrate the Auditing Entry window that results from accessing the Advanced Security Settings window for a folder, highlighting the Auditing tab, and clicking Add. Point out that at this Auditing Entry window an administrator can make auditing selections.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Audited events are recorded in the Windows Server 2019 Security log. An administrator can access the Security log using the Get-EventLog Security command within Windows PowerShell, or by using the Event Viewer tool. To open Event Viewer, right-click Start and click Event Viewer. |

1. Explain why auditing is not enabled on Windows Server 2019 by default.
2. Mention that to enable auditing functionality, a user must edit the audit policy within a Group Policy object that applies to their computer.
3. Explain that within an Active Directory environment, an administrator can edit the settings of the Default Domain Policy object to enable auditing functionality on every computer within the domain. Explain how to accomplish this by sing the Group Policy Management tool and the Group Policy Management Editor tool.
4. Refer to Figure 5-11 to illustrate the Group Policy Management Editor tool with the *Audit object access* policy setting that enables the auditing functionality for both success and failure events.

**Configuring Shared Folders**

1. Introduce this topic by explaining that to allow users to access the files within a folder on a Windows Server 2019 system from across a network, an administrator must share the folder.
2. Introduce and define the two different protocols that can be used to share folders on Windows Server 2019 systems: Server Message Block (SMB) and Network File System (NFS).

**Sharing Folders Using SMB**

1. Inform your students that after they install Windows Server 2019, SMB sharing is enabled by default.
2. Mention that a Windows Server 2019 system is visible to other computers on the network if an administrator clicks Yes when the Networks desktop notification screen prompts the administrator to allow their PC to be discoverable by other PCs.
3. Review how to enable or disable SMB sharing for a current network profile by opening Control Panel in category view and navigating to Network and Internet, Network and Sharing Center.
4. Refer to Figure 5-12 to illustrate how an administrator can use the Network and Sharing Center and click *Change advanced sharing settings* to modify the SMB sharing settings. Review the options on the screen.
5. Mention that if SMB sharing is enabled on a system, an administrator can easily share a folder by accessing the properties of the folder or by using Server Manager.
6. Introduce the topic of sharing a folder using folder properties by mentioning that an administrator can right-click the folder, click Properties, and highlight the Sharing tab.

1. As an example, refer to Figure 5-13 to illustrate the Sharing tab for the C:\CompanyForms folder on SERVERX.
2. Refer to Figure 5-14 to illustrate the Network access window that displays when an administrator clicks the Share button in Figure 5-13. Point out that an administrator can 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.
3. Refer to Figure 5-14 again and review the permissions that SMB requires for a shared folder in order to connect to a shared folder.

* Read
* Read/Write
* Owner

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Note that a user will receive the shared folder permissions that are assigned to their user account as well as any group accounts that they belong to. Moreover, permissions that are denied to their user or group accounts override permissions that are allowed. |

1. Refer back to Figure 5-13 and mention that an administrator can also click the Advanced Sharing button to display the Advanced Sharing window illustrated in Figure 5-15. Then an administrator can select the Share this folder option.
2. Refer to Figure 5-15 to illustrate how an administrator can 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.
3. Point out that an administrator can also click the Permissions button to configure advanced shared folder permissions for groups and users. Review the three advanced shared folder permissions as illustrated in Figure 5-16.

* Read
* Change
* Full Control

1. Refer back to Figure 5-15 and mention that the Caching button allows an administrator to configure the offline file caching feature of SMB.
2. Refer to Figure 5-17 to illustrate the window that allows the offline file caching feature of SMB to be configured. Review the possible options.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | BranchCache is an optional performance enhancement to offline file caching for Windows 7 and later clients that is not installed or configured by default. More information on BranchCache can be found at: <https://docs.microsoft.com/en-us/windows-server/networking/branchcache/branchcache>. |

1. Introduce the topic of sharing a folder using Server Manager.
2. Refer to Figure 5-18 and explain how to share a folder using Server Manager by clicking File and Storage Services within the navigation pane of Server Manager, and then highlighting Shares.
3. Explain that to share a folder, an administrator can select the Tasks drop-down box in the Shares section of Figure 5-18 and click New Share. Note that this will start the New Share Wizard.
4. Refer to Figure 5-19 to illustrate the New Share Wizard. Mention that the first step is to select the desired SMB file share profile option.
5. Explain that an administrator will 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.
6. Refer to Figure 5-20 and explain that if an administrator *selects SMB Share – Quick* and clicks Next in Figure 5-19, he or she will be prompted to select the server and the volume that should contain the shared folder. Note that this will create a \Shares parent folder on the volume (if one does not already exist) that will include a subfolder for a new shared folder. Alternatively, an administrator can select Type a custom path and specify the path to an existing shared folder that he or she wishes to share.
7. Refer to Figure 5-21 to illustrate where an administrator is prompted to supply the share name and optional share description.
8. Refer to Figure 5-22 to illustrate where an administrator is prompted to configure the optional share features. Review the features.

* Enable access-based enumeration
* Allow caching of share
* Encrypt data access

1. Explain that 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.
2. Refer to Figure 5-23 to illustrate where an administrator is prompted to modify the NTFS/ReFS permissions on the folder to match the desired level of access for groups and users.
3. Note that after this configuration, an administrator can click Next and then Create to create the new shared folder.

**Sharing Folders Using NFS**

1. Inform students that in order to share folders using NFS, they will need to install the Server for NFS server role on a new windows Server 2019 system.
2. Refer to Figure 5-24 and explain how to select this role within the Add Roles and Features Wizard in Server Manager by first expanding File and Storage Services, and then expanding File and iSCSI Services.
3. Point out that as with SMB, an administrator can share a folder using NFS by accessing the properties of the folder or by using Server Manager.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Note that to connect to NFS shared directories from a Windows Server 2019 system, the administrator must also install the Client for NFS feature. |

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Note that Windows Server 2019 requires that any NFS shared folders reside on an NTFS or ReFS filesystem. |

1. Explain that one way to share a folder is to use the folder properties.
2. Describe how to access a folder’s NFS properties by right-clicking the folder, clicking Properties, highlighting the NFS Sharing tab, and clicking Manage NFS Sharing.
3. Refer to Figure 5-25 to illustrate the NFS Advanced Sharing window where an administrator can enable NFS file sharing, specify the share name, and configure the appropriate NFS options.
4. Explain that 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.
5. Emphasize that because Active Directory provides centralized user authentication using Kerberos, NFS works well within an Active Directory environment for sharing files among UNIX, Linux, macOS, and Windows systems.
6. Refer to Figure 5-25 again and discuss the three Kerberos v5 options that allow all forms of Kerberos authentication for UNIX, Linux, macOS, and Windows users within the Active Directory domain.
7. In Figure 5-25 review the other options that 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. Note that in this case, the user accounts within Active Directory for each UNIX, Linux, and macOS user must contain the same UID and GID that are stored within the UNIX user database on that user’s system.
8. In Figure 5-25, review the option to force UNIX, Linux, and macOS users that are not configured to use Kerberos to connect as the Guest account.
9. Mention that as with SMB shared folders, shared folder permissions are required to connect to an NFS shared folder.
10. Explain that NFS shared folder permissions are granted to computers instead of users.
11. Refer to Figure 5-26 to illustrate how an administrator can add entries for computers (by DNS name) that are granted access to the NFS shared folder. Review the two levels of access that an administrator 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.

1. Mention that the default permission assigns Read-Only NFS share permission to all computers.
2. Emphasize that selecting the Allow root access option will also allow the root user (the equivalent of Administrator on a UNIX, Linux, or macOS system) to access the NFS share.
3. Explain how UNIX, Linux, macOS, and Windows users can access a shared folder.
4. Introduce the topic of sharing a folder using Server Manager by explaining that the Shares section of Server Manager can also be used to create and manage NFS shared folders, using the same general process as for SMB shared folders.
5. Describe the ways the New Share Wizard can be used to create a shared folder.

* *NFS Share – Quick* to share a folder with NFS
* *NFS Share – Advanced* to additionally configure file classifications and folder quotas if the File Server Resource Manager is installed

1. Refer to Figures 5-27 through 5-29 and explain the processes of selecting *NFS Share – Quick* and progressing through the New Share Wizard prompts.
2. Mention that after an administrator clicks Next, the administrator will be able to modify the NTFS/ReFS permissions on the folder to match the desired level of access for groups and users. Mention that following this, the administrator can click Next and then Create to create the new shared folder.

**Publishing a Shared Folder in Active Directory**

1. Explain what is meant by publishing a resource to Active Directory.
2. Mention that if an administrator publishes a shared folder to Active Directory, users will be able to locate that shared folder quickly using the LDAP component of Active Directory.
3. Review the necessary steps to publish a shared folder to the Active Directory database.
4. Refer to Figure 5-30 to illustrate the New Object – Shared Folder window where an administrator can supply the name and UNC path to the SMB or NFS shared folder.
5. Mention that when an administrator clicks OK, a shared folder object is created within the associated OU.
6. Explain that 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.
7. Explain how to locate published shared folders within File Explorer.
8. Refer to Figure 5-31 to illustrate a Find window where an administrator can select Shared Folders and click Find Now to search the entire Active Directory for shared folders.
9. Describe how to narrow the search results by specifying additional criteria.

**Quick Quiz 1**

1. Which term refers to features of a folder or file that are used by a filesystem?
2. indexing
3. cache
4. attributes
5. metadata

Answer: c. attributes

1. Which term refers to a user or group that is listed within a DACL or SACL?
   1. client for NFS
   2. target
   3. recovery agent
   4. security principal

Answer: d. security principal

1. The \_\_\_\_\_\_\_\_\_\_ 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.
   1. Windows Indexing
   2. access-based enumeration
   3. passive screening
   4. system access control list

Answer: b. access-based enumeration

1. Which term refers to the processes of creating objects that represent network resources in Active Directory?
   1. replicating
   2. active screening
   3. publishing
   4. targeting

Answer: c. publishing

**Implementing Distributed File System**

1. Open this topic by mentioning that 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.
2. Introduce and define the two separate server roles that comprise DFS: DFS Namespaces and DFS Replication.
3. Mention that each of these roles works independently of the other but can be managed using the same DFS Management tool.
4. Describe how to install the DFS Namespaces and DFS Replication roles.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | For more information on DFS server roles, see the following Web site: <https://www.pdq.com/blog/setting-up-dfs-in-your-environment/> |

**Configuring DFS Namespaces**

1. Mention that by installing DFS namespaces on a Windows Server 2019 system, an administrator can create a DFS namespace shared folder that users can access.
2. Explain that after accessing the DFS namespace folder, users will see subfolders (called targets) that represent the shared folders on the file servers within the organization.
3. Mention that the DFS namespace folder provides a visual representation of multiple shared folders on the network. Point out that when users navigate to a target, they are automatically forwarded to the associated shared folder on the network.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Your students can think of a DFS namespace as a home page for some or all of the shared folders within an organization. Just as users can navigate to a home page within their Web browser and click hyperlinks that take them to different websites on the Internet, they can access a DFS namespace within File Explorer and double-click targets that connect them to different shared folders on the network. |

1. Refer to Figure 5-32. Mention that to configure a DFS namespace, an administrator can select DFS Management from the tools menu of Server Manager. Within the DFS Management window, an administrator will click New Namespace within the Actions pane to start the New Namespace Wizard.
2. Refer to Figure 5-33 to illustrate the start of the New Namespace Wizard and the prompt to specify the name of the server that will host the DFS namespace. Mention that an administrator will click Next after specifying the name of the server.
3. Refer to Figure 5-34 to illustrate New Namespace Wizard prompt for the shared folder name for the DFS namespace. Review the common naming convention most organizations use. Explain that an administrator can click Edit Settings to modify the path and share permissions to suit his or her needs. Mention that an administrator will click Next after entering this information.
4. Refer to Figure 5-35 to illustrate the New Namespace Wizard prompt to specify the namespace type. Review the possible options available.
5. Mention that after an administrator clicks Next in Figure 5-35, he or she can click Create to create the DFS namespace.
6. Mention that the next step is to add targets to the DFS namespace that represent the shared folders within the organization.
7. Refer back to Figure 5-32 if necessary. Explain how to add a target to a DFS namespace within the DFS Management tool. Mention that an administrator can highlight their DFS namespace and click New Folder in the Actions pane. Mention that a New Folder window will appear.
8. Refer to Figure 5-36 to illustrate the New Folder window where an administrator can specify a target name and the UNC of one or more shared folders on the network that contain the associated content. Discuss the example provided in Figure 5-36.

**Configuring DFS Replication**

1. Introduce this topic by mentioning that to configure folders on two or more file servers to synchronize contents, an administrator must first create a DFS replication group.
2. Refer back to Figure 5-32. Mention that to create a DFS replication group, an administrator can select DFS Management from the tools menu of Server Manager. Within the DFS Management window, an administrator can click New Replication within the Actions pane to start the New Replication Group Wizard.
3. However, note that when creating a namespace, if an administrator adds a target that contains more than one UNC to a DFS namespace, the DFS Management tool will give the administrator the option to automatically create a replication group that keeps the content within each shared folder synchronized using DFS replication. Mention that in this case, if an administrator clicks OK in the window that appears in Figure 5-36 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 the administrator for the remaining configuration. The replication group and folder name shown in Figure 5-37 are provided by default, but an administrator has the option to change their values.
4. After Next is clicked in Figure 5-37, the Replicate Folder Wizard will list the selected folders from each server.
5. Refer to Figure 5-38 to illustrate an example of the Replicate Folder Wizard listing the replicated folders on each server.
6. Emphasize that 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.
7. Mention that when an administrator clicks Next in Figure 5-38, the Replicate Folder Wizard will display a prompt to select the server whose file contents should overwrite other copies during the initial DFS replication.
8. Refer to Figure 5-39 to illustrate the Replicate Folder Wizard window containing the prompt for the primary server name whose file contents will overwrite other copies during the initial DFS replication.
9. Mention that an administrator clicks Next in Figure 5-39, and the Replication Folder Wizard prompts the administrator to select the DFS replication topology.
10. Refer to Figure 5-40 to illustrate the Replicate Folder Wizard window displaying the DFS replication topology prompt.
11. Mention that an administrator clicks Next in Figure 5-40. Then the Replicate Folder Wizard provides a window where an administrator can optionally restrict the days and times that the DFS replication service is allowed to run, and the network bandwidth it can use.
12. Refer to Figure 5-41 to illustrate the Replicate Folder Wizard window displaying the prompts to restrict the days and times that the DFS replication service is allowed to run, and the network bandwidth it can use.
13. Explain that after an administrator clicks Next in Figure 5-41, the administrator can click Create to create the replication group.

**Implementing Quotas and File Screens**

1. Introduce this section by mentioning that when an administrator shares folders on an NTFS filesystem that provide permissions for users to add files and subfolders, the administrator may need to configure additional restrictions on the size and type of files that users can add.
2. Mention that these restrictions can prevent users from consuming too much space on the file server, or block users from adding the wrong type of files to shared folders.
3. List the three features NTFS provides that that allow an administrator 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.

1. Explain that an administrator must first install the File Server Resource Manager server role on his or her file server before configuring folder quotas and file screens.
2. Explain how to install this server role. Mention that an administrator uses the Add Roles and Features Wizard in Server Manager.

**Configuring User Quotas**

1. Emphasize that NTFS user quotas are not enabled on each filesystem by default.
2. Review the steps to enable NTFS quotas for a filesystem. Explain that an administrator 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.
3. Refer to Figure 5-42 to illustrate the Quota tab. Review quota characteristics for the folder associated with the tab. Point out that the quotas prevent users from storing more than 2 GB on the C:\ filesystem. Furthermore, note that users receive a warning when they reach 1.5 GB of storage, and an event will be logged to the Windows Server 2019 System log.
4. Explain that an administrator can also click the Quota Entries button to provide specific quota options for individual users and groups that override the default options shown in the Quota tab in Figure 5-42.
5. Emphasize that by default, members of the Administrators group receive no limits.

|  |  |
| --- | --- |
| ***Teaching***  ***Tip*** | Because user quotas are based on file ownership, they are not always accurate. For example, a user can change the ownership of files they own to another user in order to bypass user quota restrictions and consume more space on the filesystem. |

**Configuring Folder Quotas**

1. Introduce this topic by mentioning that folder quotas can be configured to prevent users from storing files after a limit has been reached (hard quota) or allow the limit to be surpassed (soft quota).
2. Point out that 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.
3. Refer to Figure 5-43 and explain that an administrator can select File Server Resource Manager from the Tools menu within Server Manager to start the File Server Resource Manager tool.
4. Explain that the Quota Management section within the navigation pane of the File Server Resource Manager tool contains two subfolders: Quotas and Quota Templates. Review the contents of each of the subfolders.
5. Refer to Figure 5-44 and review the necessary steps to create a new folder quota using the File Server Resource Manager tool. Mention that to create a new folder quota, an administrator highlights the Quotas folder. Then, an administrator clicks Create Quota within the Actions pane, and specifies the appropriate folder path and settings.
6. Explain how to modify quota settings within the Create Quota window. Explain that an administrator clicks the Custom Properties button and selects the appropriate options.
7. Refer to Figure 5-44 and emphasize that if an administrator selects *Derive properties from this quota template (recommended)*, an administrator can select a pre-configured template from the drop-down box to copy the quota settings from that template. Additionally, mention that an administrator can select *Auto apply template and create quotas on existing and new subfolders* to create folder quotas on existing and new subfolders of a folder based on the template chosen.
8. Refer to Figure 5-45 to illustrate how an administrator can optionally save the quota settings in a new quota template for future use when he or she clicks Create.

**Configuring File Screens**

1. Introduce and describe the two type of file screening: active screening and passive screening.
2. Define a group as a specific category of files consisting of one or more filename extensions.
3. Mention that an administrator configures file screens within the File Server Resource Manager tool.
4. Refer back to Figure 5-43 and explain that the File Screening Management section within the navigation pane of the File Server Resource Manager tool contains three subfolders: File Screens, File Screen Templates, and File Groups. Review the contents of each of the subfolders.
5. Refer to Figure 5-46 and review the necessary steps to create a new file screen by using the File Server Resource Manager tool. Mention that to create a new file screen, an administrator can highlight the File Screens folder. Then, an administrator clicks Create File Screen within the Actions pane, and specifies the appropriate folder path and settings.
6. Explain how to modify file screen settings within the Create File Screen window. Explain that an administrator clicks the Custom Properties button and selects the appropriate options.
7. Refer to Figure 5-46 and emphasize that if an administrator selects *Derive properties from this file screen template (recommended)*, an administrator can select a pre-configured template from the drop-down box to copy the file screen settings from that template.

**Quick Quiz 2**

1. Which DFS server role provides a central location from which users can access the different shared folders within their organization?
   1. DFS Namespaces
   2. DFS Replication
   3. DFS Registry
   4. DFS Authenticator

Answer: a. DFS Namespaces

1. Which NTFS feature can be configured to prevent certain types of files from being stored within a folder on the filesystem?
   1. user quotas
   2. folder quotas
   3. file screens
   4. recovery agent

Answer: c. file screens

1. When configuring user quotas, which Windows Server 2019 group’s members receive no limits?
   1. Administrators
   2. Users
   3. Guest
   4. Managers

Answer: a. Administrators

1. When configuring DFS Replication topology, which topology allows each server within the replication group to replicate directly to all other members, consuming additional network bandwidth as a result?
   1. hub and spoke
   2. full mesh
   3. ring
   4. elliptic star

Answer: b. full mesh

# **Class Discussion Topics**

1. What are the benefits of folder and file auditing?
2. What are the advantages and disadvantages of using Microsoft Encrypting File System to protect files and folders?
3. Discuss why it is important to implement quotas.

# **Additional Projects**

1. Encrypting File System (EFS) enables a user to encrypt the contents of a folder or a file so that it can only be accessed via private key code by the user who encrypted it. Ask your students to read more about EFS and write a report explaining how it works. Use the following link as starting point:

<http://technet.microsoft.com/en-us/library/cc700811.aspx>.

1. Ask your students to read the following article and write a report summarizing its most important points.   
   “Overview of DFS Namespaces”

<https://technet.microsoft.com/en-us/library/cc730736(v=ws.11).aspx>

1. BranchCache is an optional performance enhancement to offline file caching for Windows 7 and later clients that is not installed or configured by default. Have your students research BranchCache and write a report summarizing the advantages it provides and/or why it is useful. Students can start their research here:

<https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-r2-and-2008/dd759172(v=ws.11)>.

# **Additional Resources**

1. Disk quota

<http://en.wikipedia.org/wiki/Disk_quota>

1. The Encrypting File System

<https://technet.microsoft.com/en-us/library/cc700811.aspx>

1. Distributed File System

<https://en.wikipedia.org/wiki/Distributed_File_System_(Microsoft)>

1. Server Message Block Overview

<https://technet.microsoft.com/en-us/library/hh831795(v=ws.11).aspx>

1. Working with the Universal Naming Convention (UNC Path)

<http://compnetworking.about.com/od/windowsnetworking/g/unc-name.htm>

1. DFS Namespaces Overview

<https://docs.microsoft.com/en-us/windows-server/storage/dfs-namespaces/dfs-overview>

**Key Terms**

* **access-based enumeration** A feature that 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.
* **active screening** A file screen that is used to prevent users from storing files of a certain category within folders on an NTFS volume.
* **asymmetric encryption** Encryption that uses a pair of keys that are uniquely generated for a system or user account: a public key and a private key.
* **attribute** A feature of a folder or file that is used by a filesystem.
* **audit policy** When enabled, folders and files will log events to the Security log according to the audit entries configured within the SACL.
* **BranchCache** An optional performance enhancement to offline file caching for Windows 7 and later clients that is not installed or configured by default.
* **Client for NFS** A feature that allows a Windows-based computer running Windows Server to access files stored on a non-Windows NFS server.
* **Common Internet File System (CIFS)** A file-sharing protocol that provides an open and cross-platform mechanism for requesting network server files and services. CIFS is based on the enhanced version of Microsoft's Server Message Block (SMB) protocol for Internet and intranet file sharing.
* **DFS Management** A management tool used to manage the DFS Namespaces and DFS Replication server roles that comprise DFS.
* **DFS namespace** A shared folder that users can access.
* **DFS Namespaces** A role service in Windows Server that enables you to group shared folders located on different servers into one or more logically structured namespaces. 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** A role service in Windows Server that enables you to efficiently replicate folders (including those referred to by a DFS namespace path) across multiple servers and sites. DFS Replication can synchronize folder contents between different servers. It must be installed on every server that synchronizes folder contents.
* **DFS replication group** A group used to configure folders on two or more file servers to synchronize their contents.
* **DFS staging folder** A temporary folder used by the DFS replication service to store files that need to replicate to other systems.
* **discretionary access control list (DACL)** An ACL that lists the permissions given to user and group accounts and is used to grant or deny access to the resource.
* **Encrypting File System (EFS)** A filesystem feature that works within a workgroup or Active Directory domain environment. EFS provides filesystem-level encryption. The technology enables files to be transparently encrypted to protect confidential data from attackers with physical access to the computer.
* **encryption algorithm** A series of mathematical steps executed in sequence to scramble data.
* **Event Viewer** A component of Microsoft's Windows operating system that lets administrators and users view the event logs on a local or remote machine.
* **File Explorer** A file manager application that provides a graphical user interface for accessing Windows file systems.
* **file group** A category of files grouped by file extension.
* **file screens** Used to prevent certain types of files (such as audio and video files) from being stored within a folder on the filesystem.
* **File Server Resource Manager** A tool that is used to set storage quotas and to control the types of files that can be saved to a file server.
* **folder quota** Used to limit the space consumed by a folder on the filesystem.
* **group ID (GID)** A number assigned to each UNIX user in a UNIX user database stored on a system.
* **Group Policy Management** The process of configuring password requirements and startup programs, and defining what applications or settings other users can change on their own.
* **Group Policy Management Editor** A Windows administration tool that allows users to configure many important settings on their computers or networks. Administrators can configure password requirements and startup programs, and define what applications or settings other users can change on their own.
* **hard quota** A folder quota that prevents users from storing files after a limit has been reached.
* **index** A pre-created list used in searching.
* **key** A random component of an encryption algorithm used to modify the steps within the algorithm.
* **metadata** A component that stores information about a folder or file.
* **Network File System (NFS)** A UNIX file sharing protocol that was introduced by Sun Microsystems and can be installed on Windows Server 2003 and later systems.
* **offline file caching** A feature of SMB. The feature caches network files and folders on a PC hard disk so that a user can access them when their PC is not connected to the network.
* **passive screening** A file screen that logs an event when active screening occurs.
* **private key** A key required to decrypt data.
* **public key** A key used to encrypt data.
* **publishing** A process in Active Directory that allows you to create objects that represent network resources, such as shared folders.
* **recovery agent** A Microsoft Windows user who has been granted the right to decrypt data that was encrypted by other users. The assignment of DRA rights to an approved individual provides an IT department with a way to unlock encrypted data in case of an emergency.
* **remote differential compression (RDC)** A feature of the DFS replication service when it replicates folder contents and it only replicates the changes made to each file by default.
* **Security log** A log that contains records of login/logout activity or other security-related events specified by the system's audit policy. Auditing allows administrators to configure Windows to record operating system activity in the Security Log. The Security Log is one of three logs viewable under Event Viewer.
* **security principal** A user or group that is listed within a DACL or SACL.
* **Server for NFS** A server role required to share folders using NFS on Windows Server 2019.
* **Server Message Block (SMB)** The default file sharing protocol used by Windows systems.
* **shared folder permission** Share permissions manage access to folders shared over a network; they do not apply to users who log on locally. Share permissions apply to all files and folders in the share; you cannot granularly control access to subfolders or objects on a share.
* **soft quota** A folder quota that allows files to be stored after the limit has been reached.
* **symmetric encryption** Reversible encryption algorithms where data can be decrypted by reversing the algorithm using the same key that was used to encrypt it.
* **system access control list (SACL)** An ACL that contains information used to audit the access to the resource.
* **System log** The system log file contains events that are logged by the operating system components.
* **target** Subfolders in the DFS Namespace folder that represent the shared folders on the file servers within the organization.
* **Universal Naming Convention (UNC)** The standard for naming and accessing a network resource such as a network drive, printer, or server.
* **user ID (UID)** A number assigned to each UNIX user in a UNIX user database stored on a system.
* **user quota** Used to limit the space that users can consume within the filesystem.
* **Windows Explorer** The original name for File Explorer. See File Explorer.
* **Windows Indexing Service** The legacy service used to obtain a list of files whose name or content matches your search based on a pre-created list called an index. See Windows Search Service.
* **Windows Search Service** The current service used to obtain a list of files whose name or content matches your search based on a pre-created list called an index.