Lesson 4: Configuring File and Share Access

MOAC 70-410: Installing and Configuring Windows Server 2012

Microsoft Official Academic Course

WILEY

Overview

- Exam Objective 2.1: Configure File and Share Access
- Designing a File Sharing Strategy
- Creating Folder Shares
- Assigning Permissions
- Configuring Volume Shadow Copies
- Configuring NTFS Quotas

Designing a File Sharing Strategy

Lesson 4: Configuring File and Share Access

Designing a File-Sharing Strategy

Why store user files on shared server drives?

- To enable users to collaborate on projects by sharing files
- To back up document files more easily
- To protect company information by controlling access to documents
- To reduce the number of shares needed on the network
- To prevent the need to share access to workstations
- To monitor users' storage habits and regulate their disk space consumption
- To insulate users from the sharing and permission assignment processes

Arranging Shares

- A well-designed sharing strategy provides each user with three resources:
  - A private storage space, such as a home folder, to which the user has exclusive access.
  - A public storage space, where each user can store files that he or she wants colleagues to be able to access.
  - Access to a shared work space for communal and collaborative documents.

Controlling Access

- The principle of "least privileges" states that users should have only the privileges they need to perform their required tasks and no more.
- Users should have complete access and control of their own files and no privileges to others' private files.
- Users should have complete control of their own Public folder, but limited access to others'.
- In the shared work space, users should have privileges based on their individual needs.
- Administrators should have privileges to have full control over users' private and public folders.

Controlling Access

- Always assign permissions to security groups, not to individuals.
- Utilize domain local groups and global or universal groups to simplify administration of permissions.
- In special cases, use the Deny Access NTFS permission to override assigned permissions.

Mapping Drives

- Folder Redirection settings in Group Policy can be used to map each user's Documents folder to his or her home folder on the network share.
- This practice enables users to work with their files without ever knowing they are stored on a network drive.
- Login scripts can be used to map each user's directory to a drive letter on that user's computer.
- Users know they must save their files to their F: drive, for example, not knowing it is pointing to a network share.

Creating Folder Shares

Lesson 4: Configuring File and Share Access

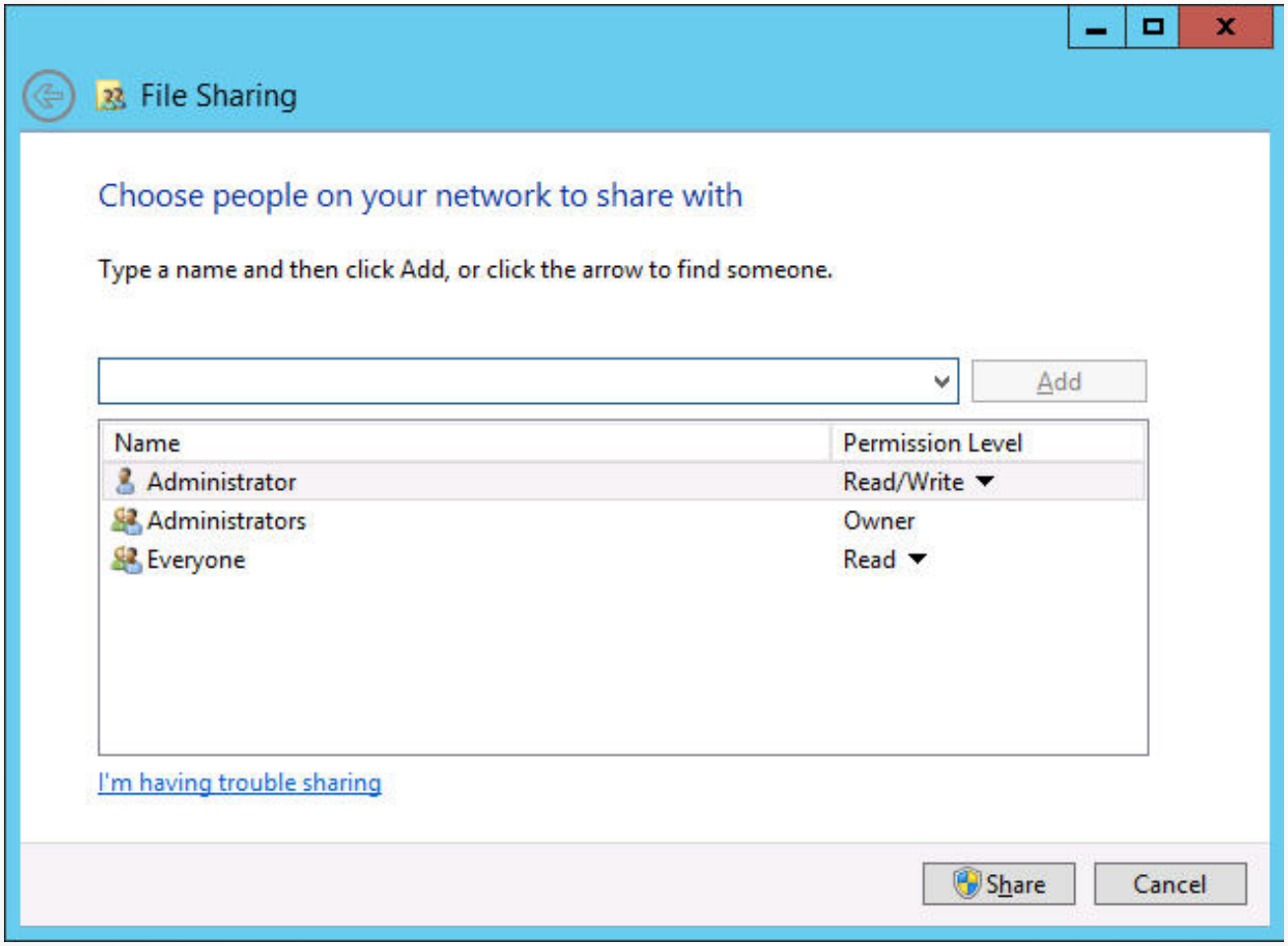
Creating Folder Shares

- Shares must be created in order for network users to be able to access the disks on the servers. You must determine:
  - What folders you will share
  - What names you will assign to the shares
  - What permissions you will grant users to the shares
  - What Offline Files settings you will use for the shares

Creator/Owner

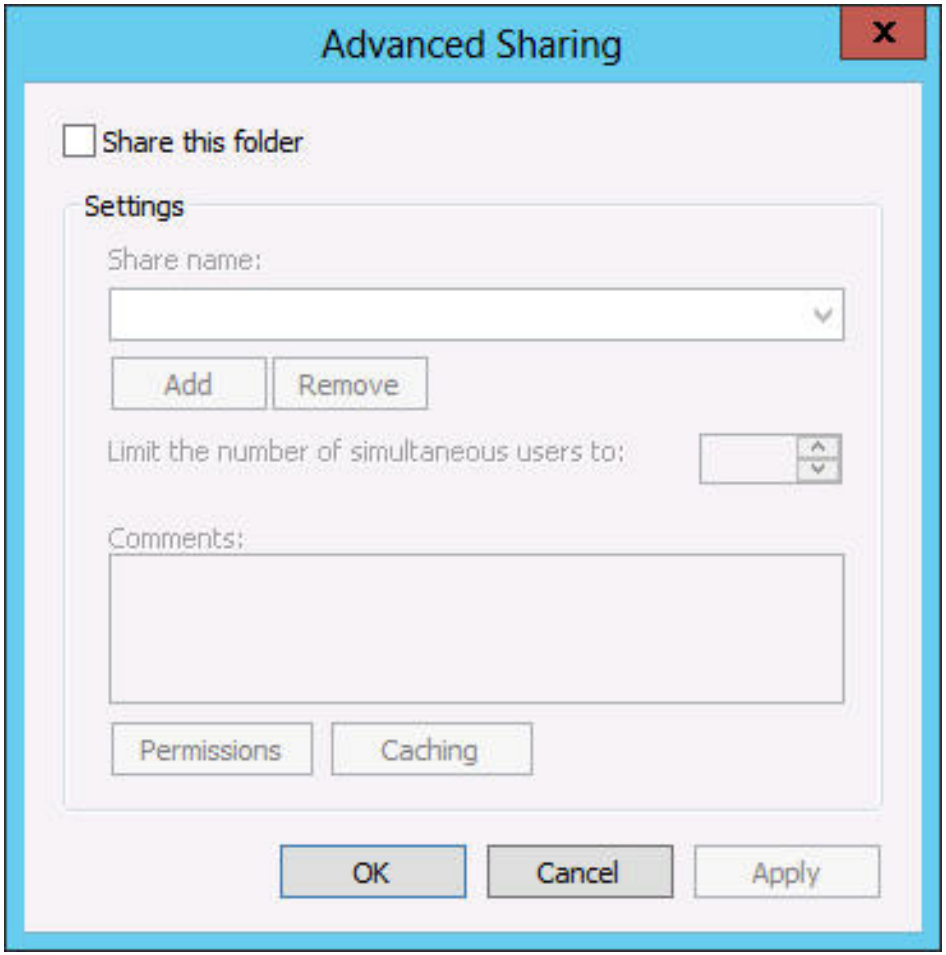
- You can share your own folders.
- Right-click and select **Share with > Specific People** to access a simplified interface.
- Use **Sharing** tab of the folder's Properties sheet for greater control.

Creating Folder Shares



The File Sharing dialog box

Creating Folder Shares

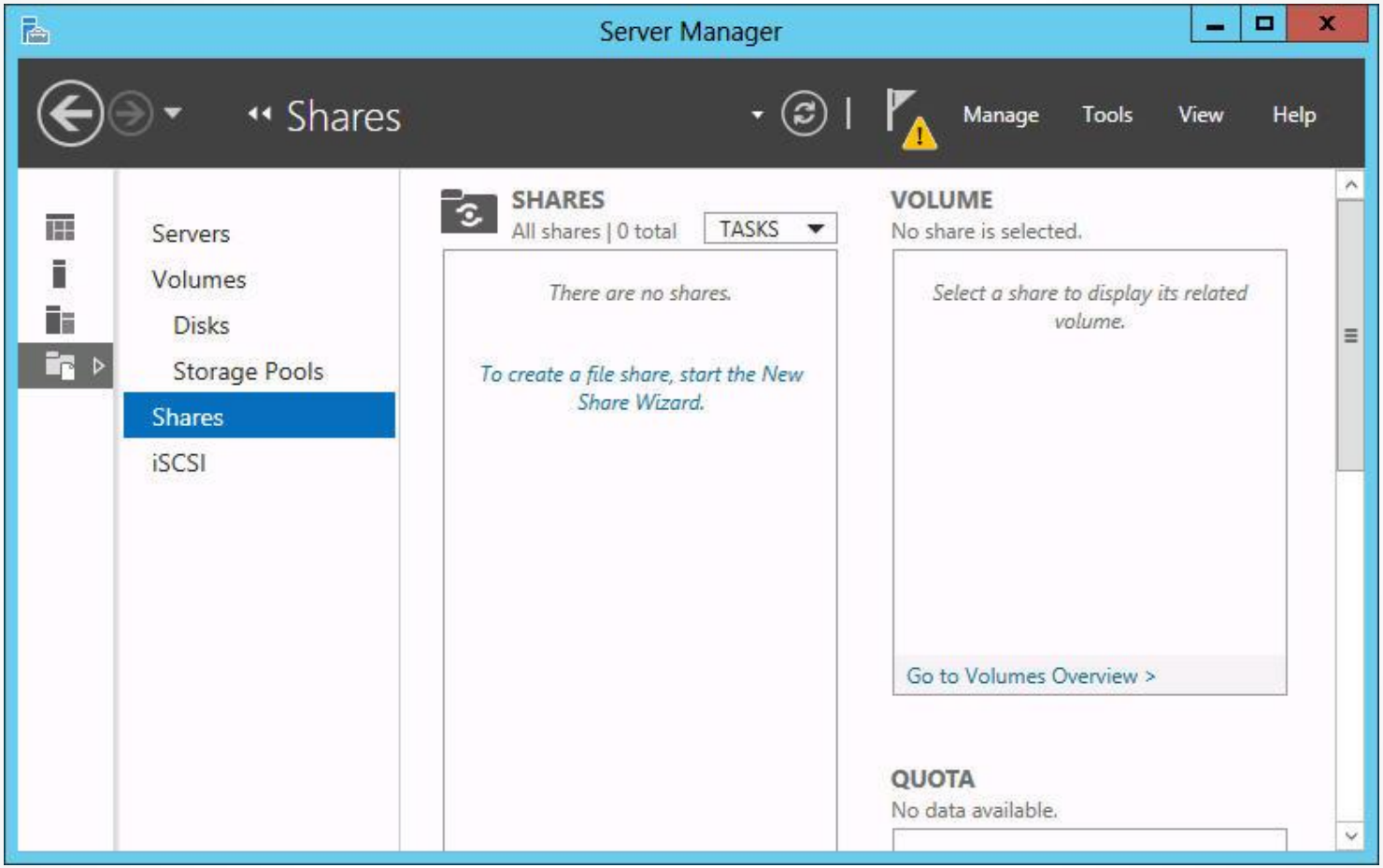


The Advanced Sharing dialog box

Types of Folder Shares

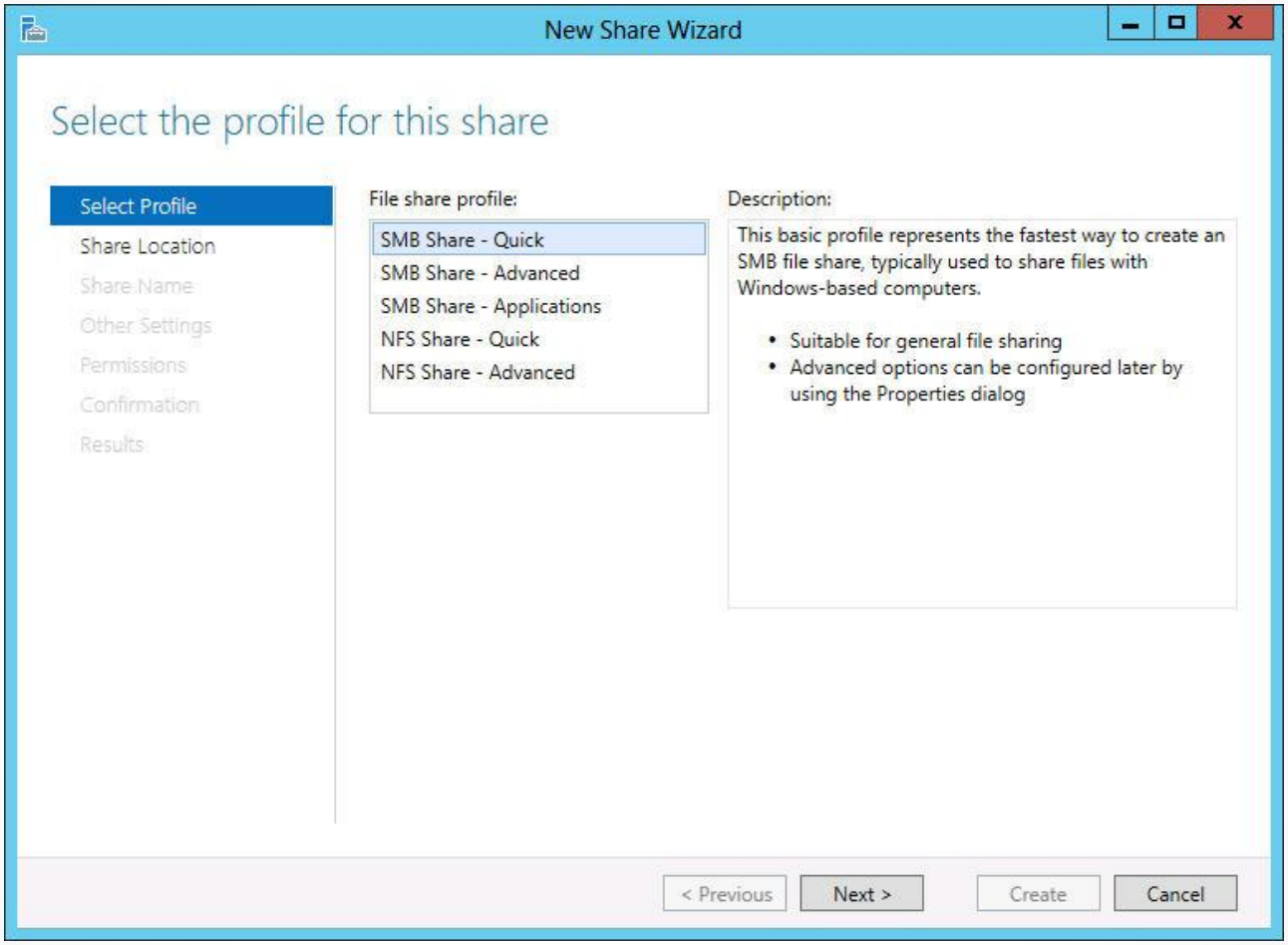
- **Server Message Blocks (SMB)**
  - The standard file-sharing protocol used by all versions of Windows.
  - Requires the File Server role service.
- **Network File System (NFS)**
  - The standard file sharing protocol used by most UNIX and Linux distributions.
  - Requires the Server for NFS role service.

Create a Folder Share



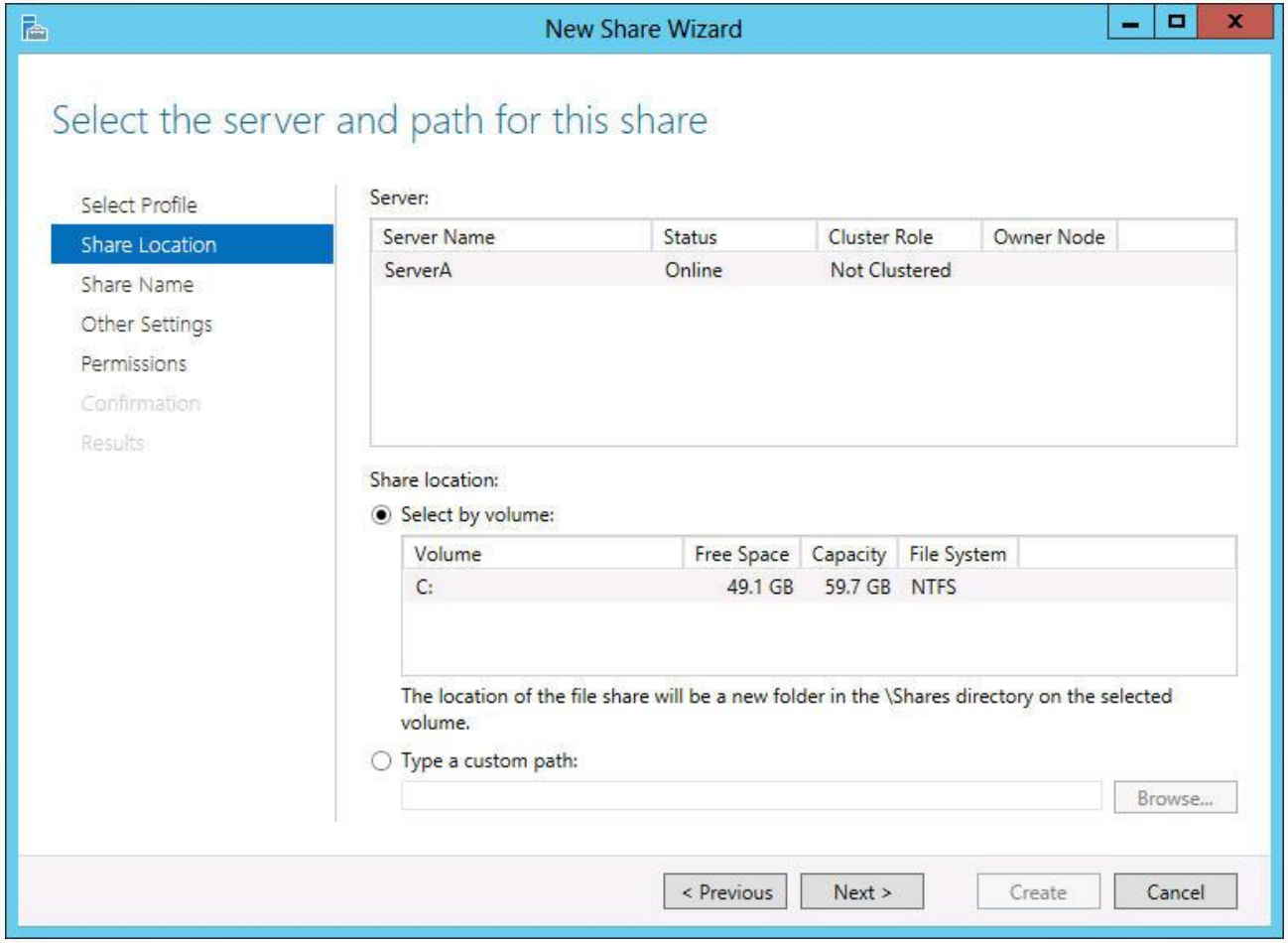
The Shares homepage

Create a Folder Share



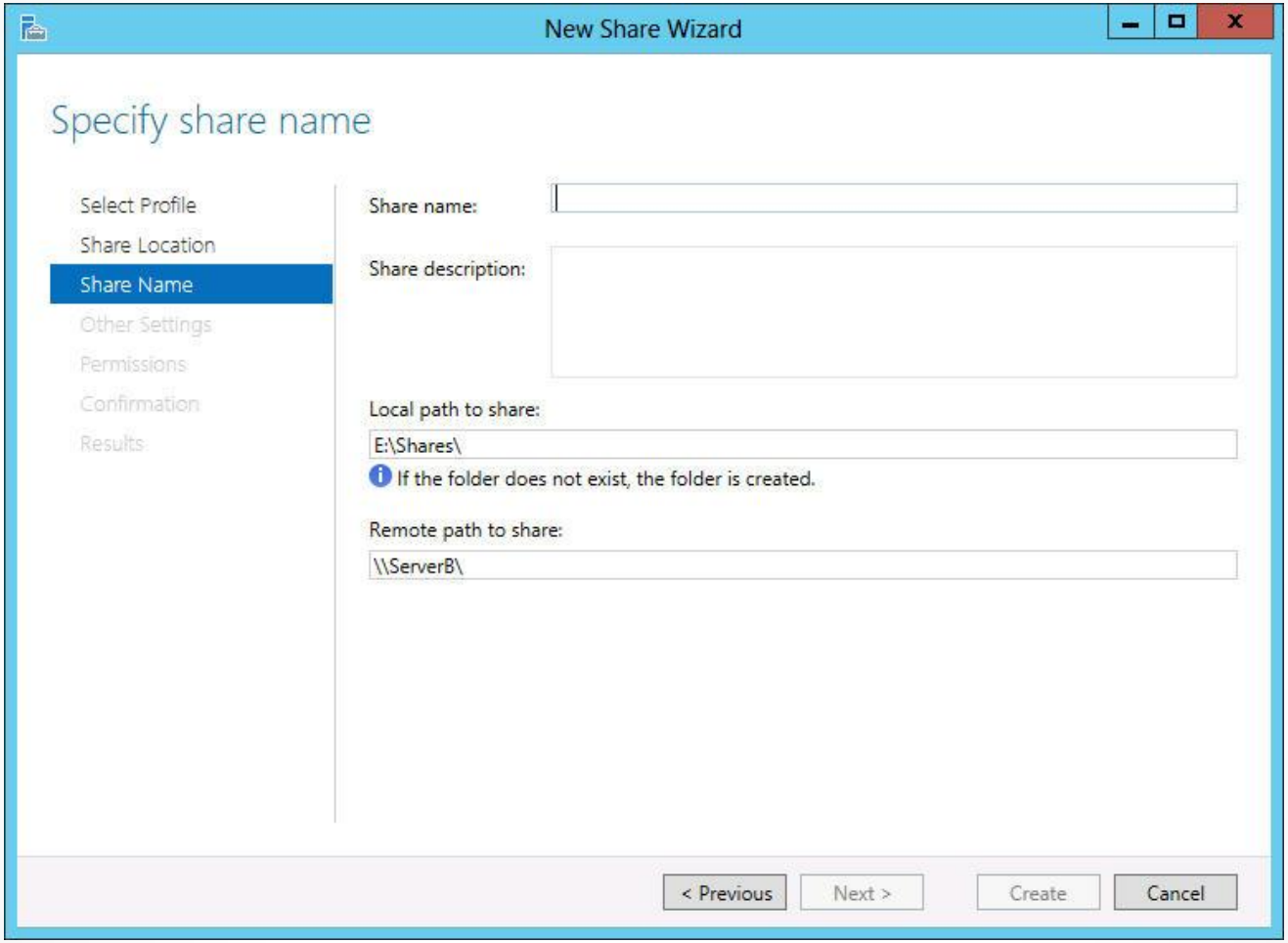
The Select the profile for this share page in the New Share Wizard

Create a Folder Share



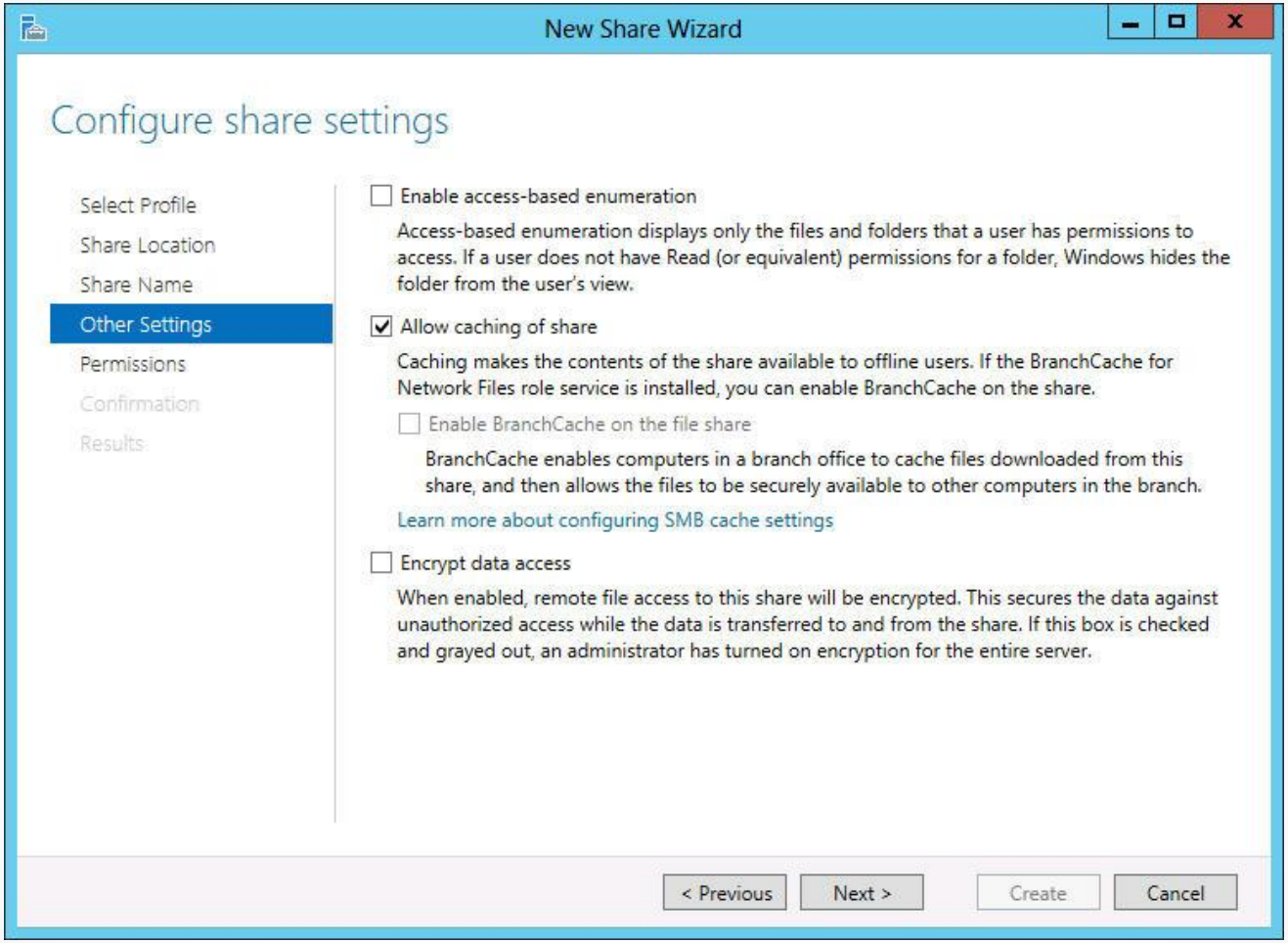
The Select the server and path for this share page of the New Share Wizard

Create a Folder Share



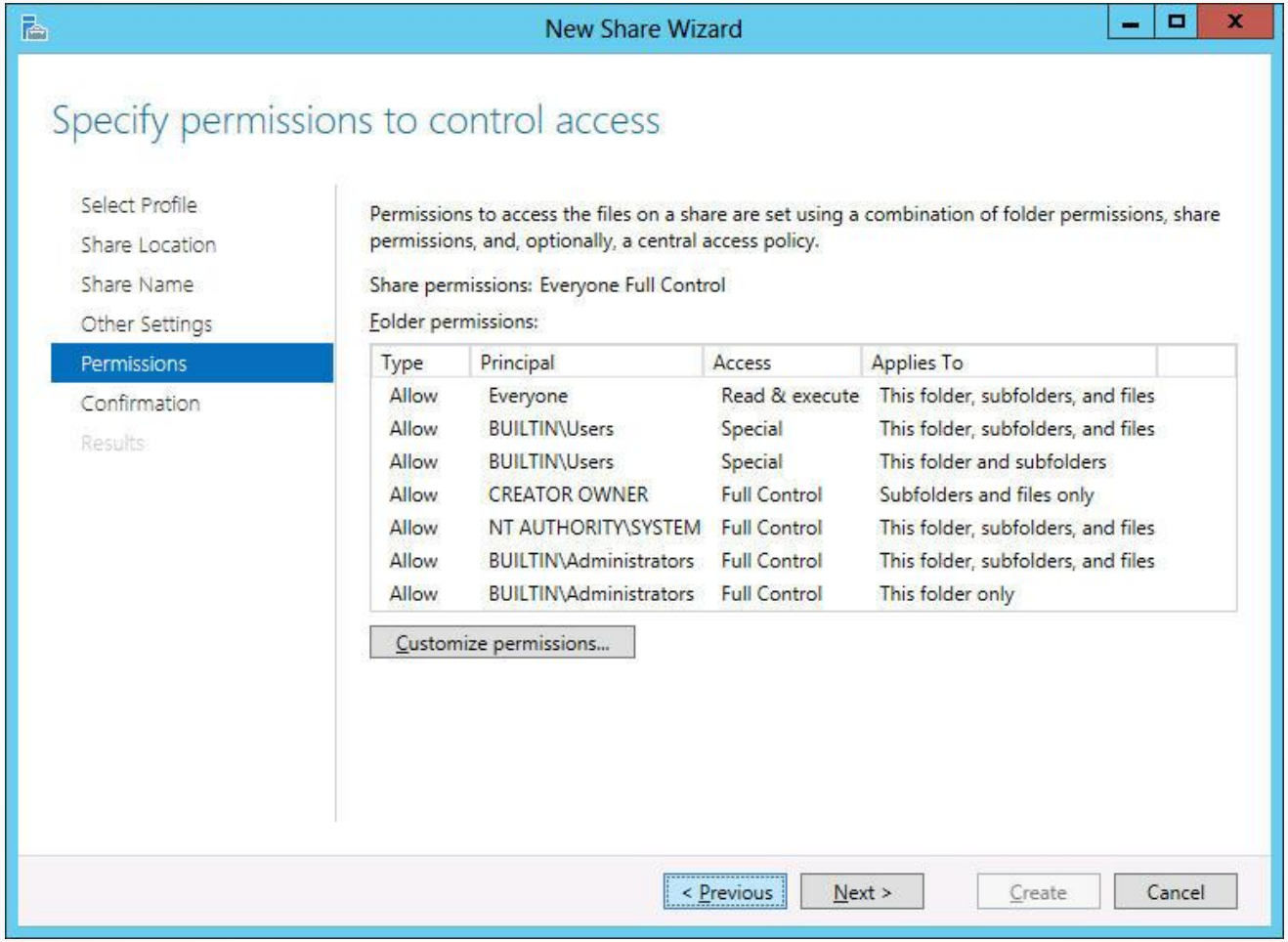
The Specify share name page of the New Share Wizard

Create a Folder Share



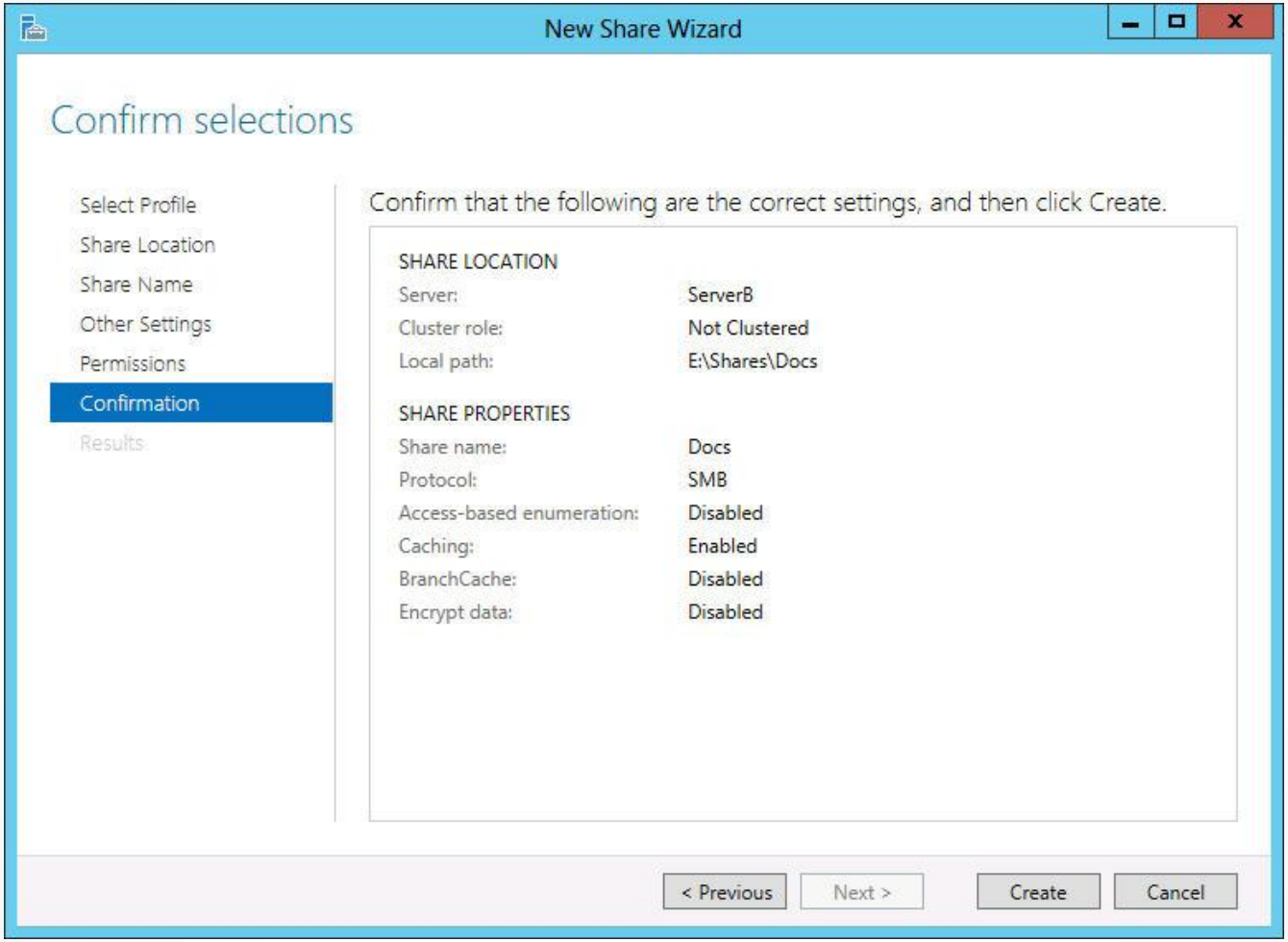
The Configure share settings page of the New Share Wizard

Create a Folder Share



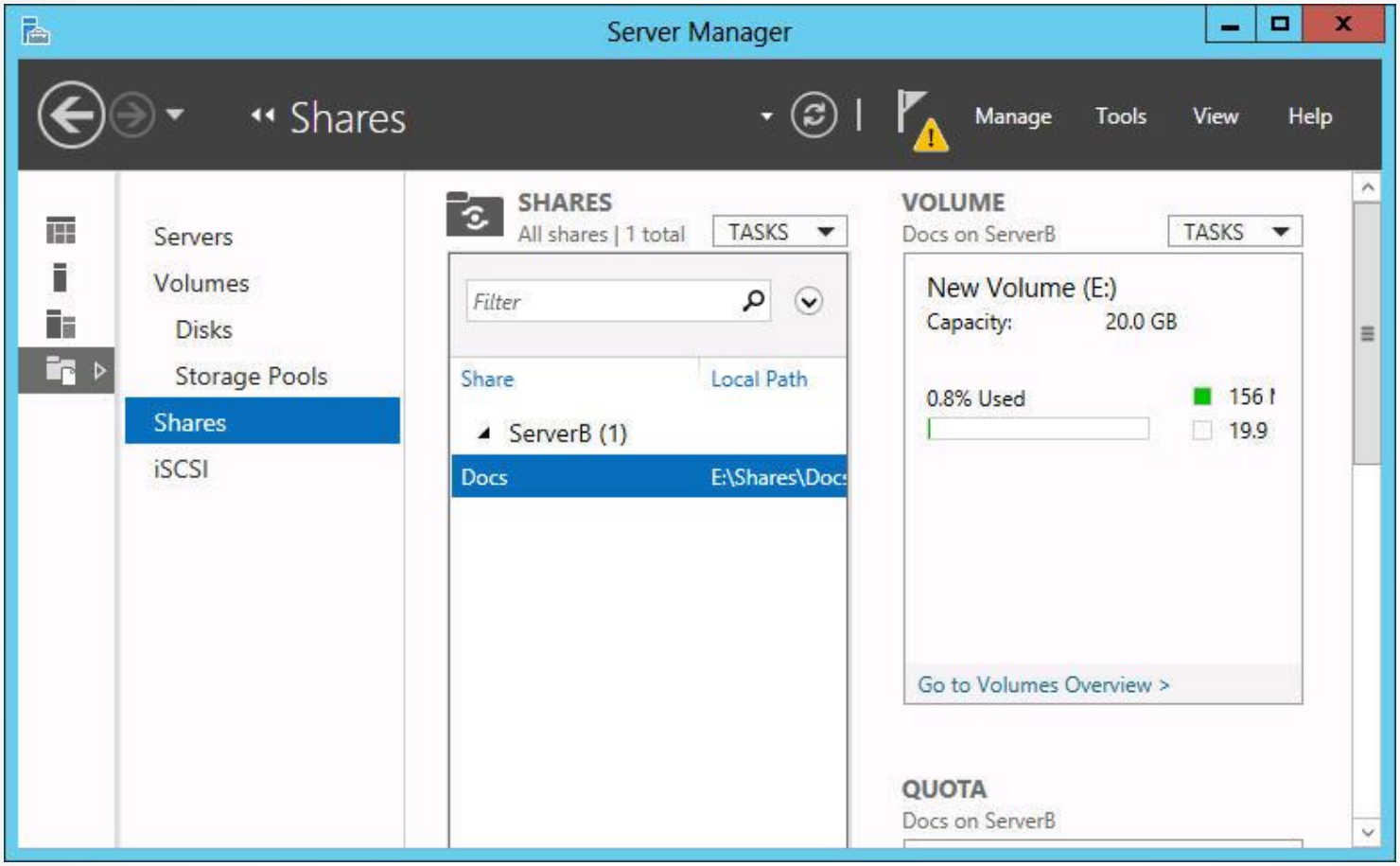
The Specify permissions to control access page of the New Share Wizard

Create a Folder Share



The Confirm selections page of the New Share Wizard

Create a Folder Share



The new share on the Shares homepage in Server Manager

Assigning Permissions

Lesson 4: Configuring File and Share Access

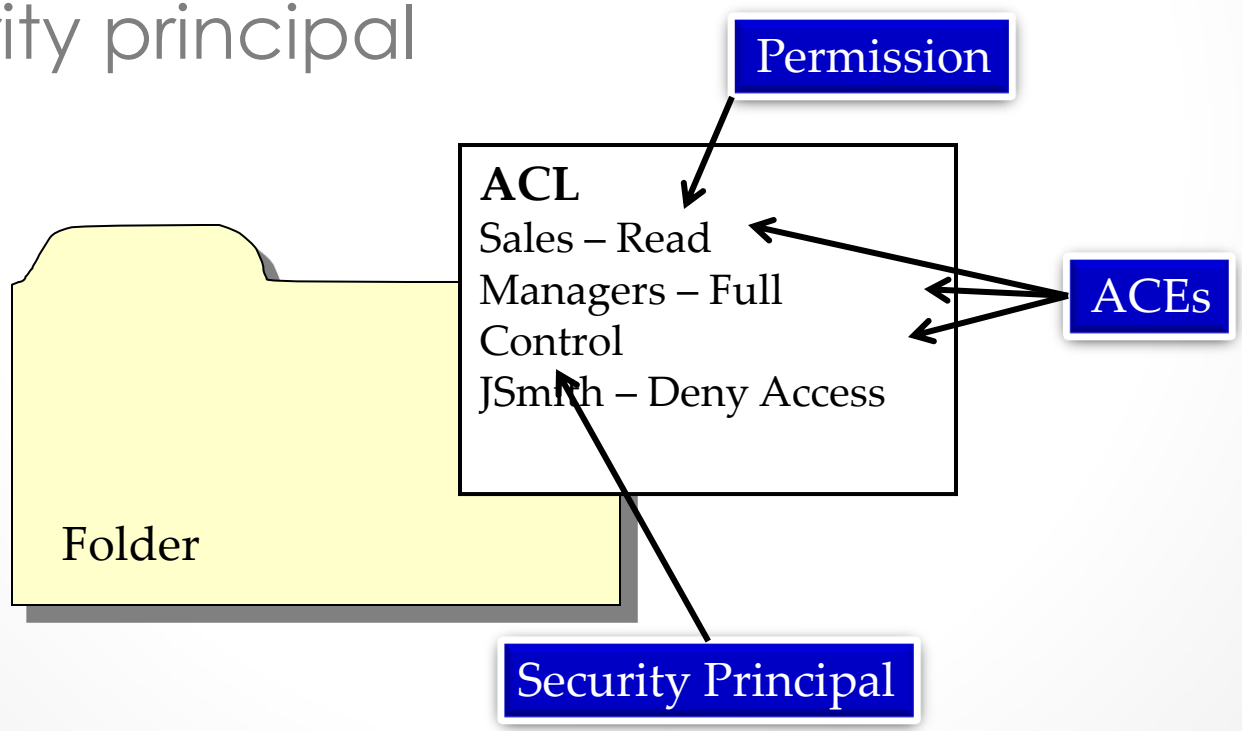
Assigning Permissions

The four permissions systems:

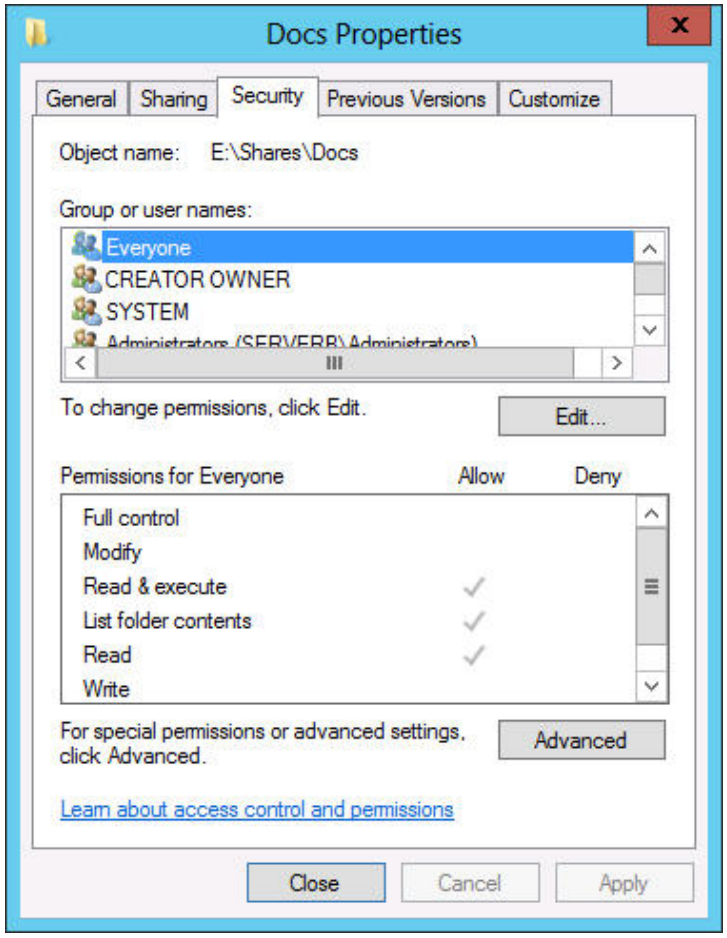
- **Share permissions:** Control access to folders over a network.
- **NTFS permissions:** Control access to the files and folders stored on disk volumes formatted with the NTFS file system.
- **Registry permissions:** Control access to specific parts of the Windows registry.
- **Active Directory permissions:** Control access to specific parts of an Active Directory Domain Services (AD DS) hierarchy.

Windows Permissions Architecture

- Access Control List (ACL)
- Access Control Entries (ACEs)
- Security principal



Windows Permissions



The Security tab of a Properties sheet

Basic and Advanced Permissions

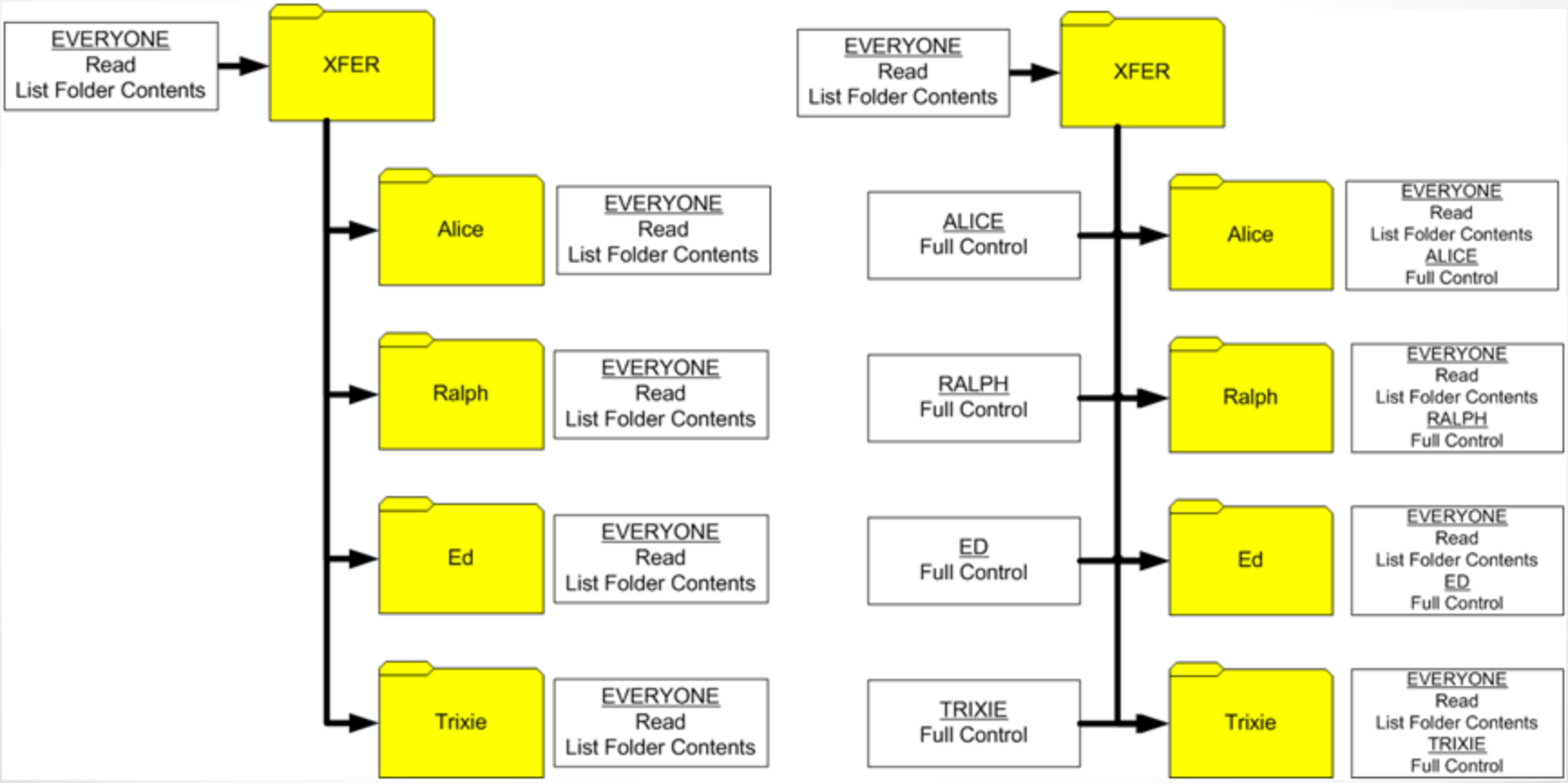
- Permissions allow you to grant specific degrees of access to security principals.
- Preconfigured permission combinations are called **Basic Permissions.**
- **Advanced Permissions** are more granular and can be applied individually, but are rarely used.

Allowing and Denying Permissions

- **Additive**
  - Start with no permissions and then grant Allow permissions (preferred method).
- **Subtractive**
  - Start by granting Allow permissions and then grant Deny permissions.

Inheriting Permissions

Permissions run downward through a hierarchy

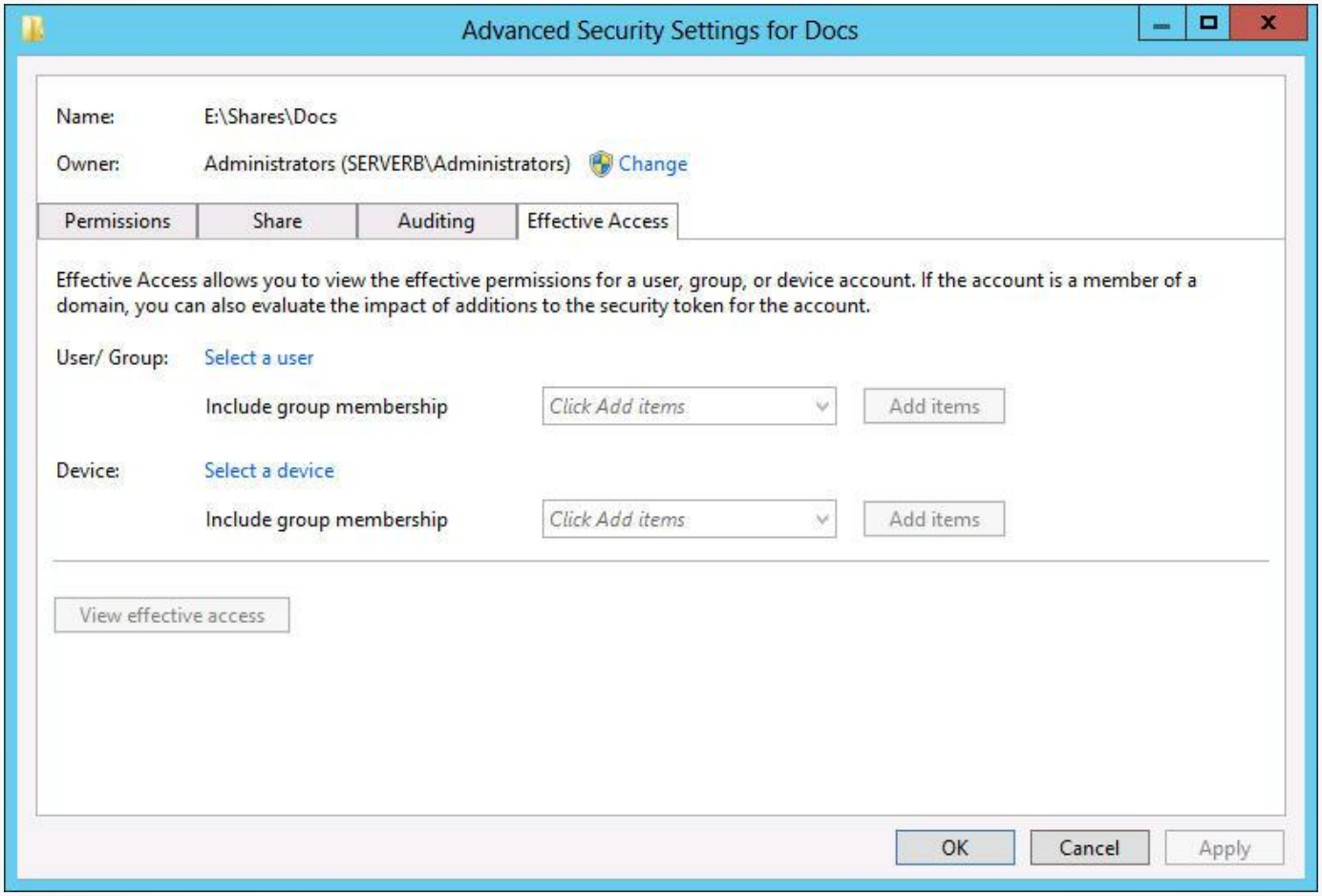


Effective Access

The combination of Allow permissions and Deny permissions that a security principal receives for a system element:

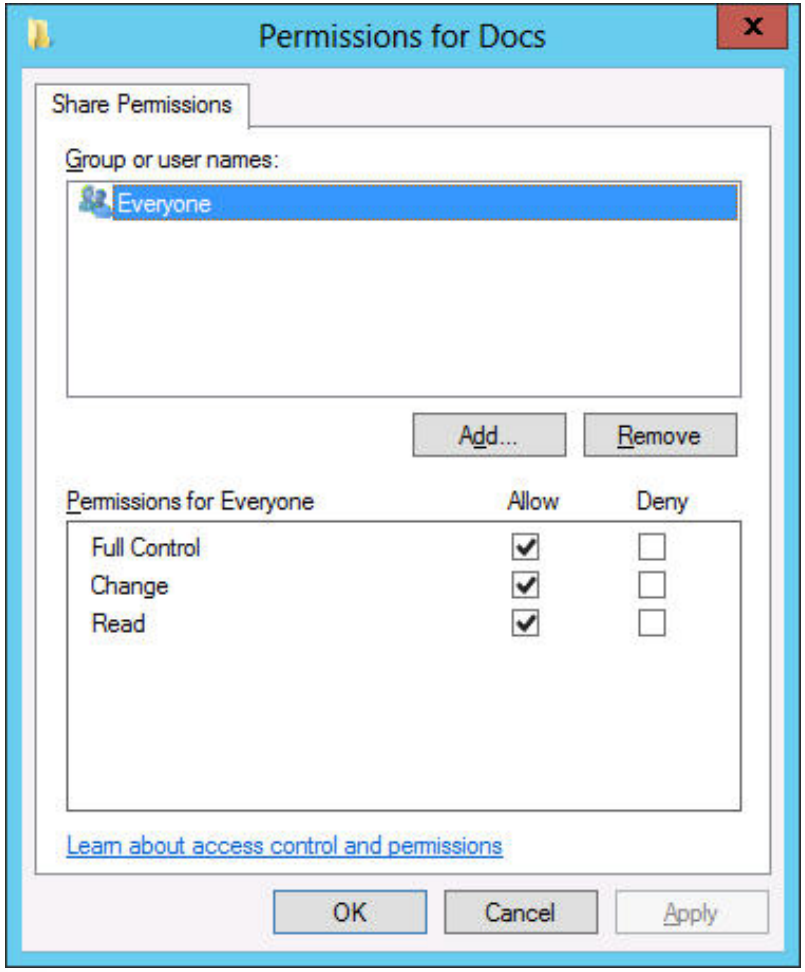
- Allow permissions are cumulative.
- Deny permissions override Allow permissions.
- Explicit permissions take precedence over inherited permissions.

Effective Access



The Effective Access tab of the Advanced Security Settings dialog box

Setting Share Permissions

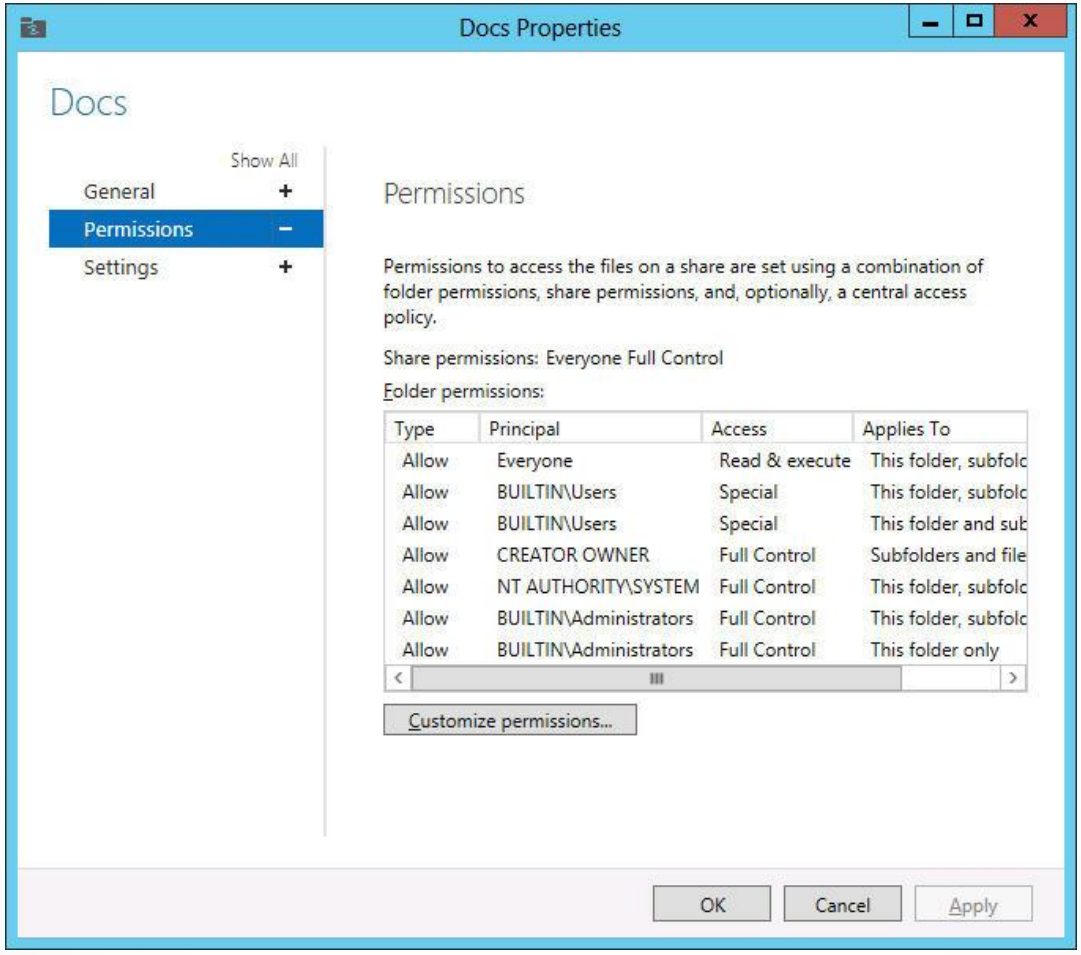


The Share Permissions tab for a shared folder

Share Permissions

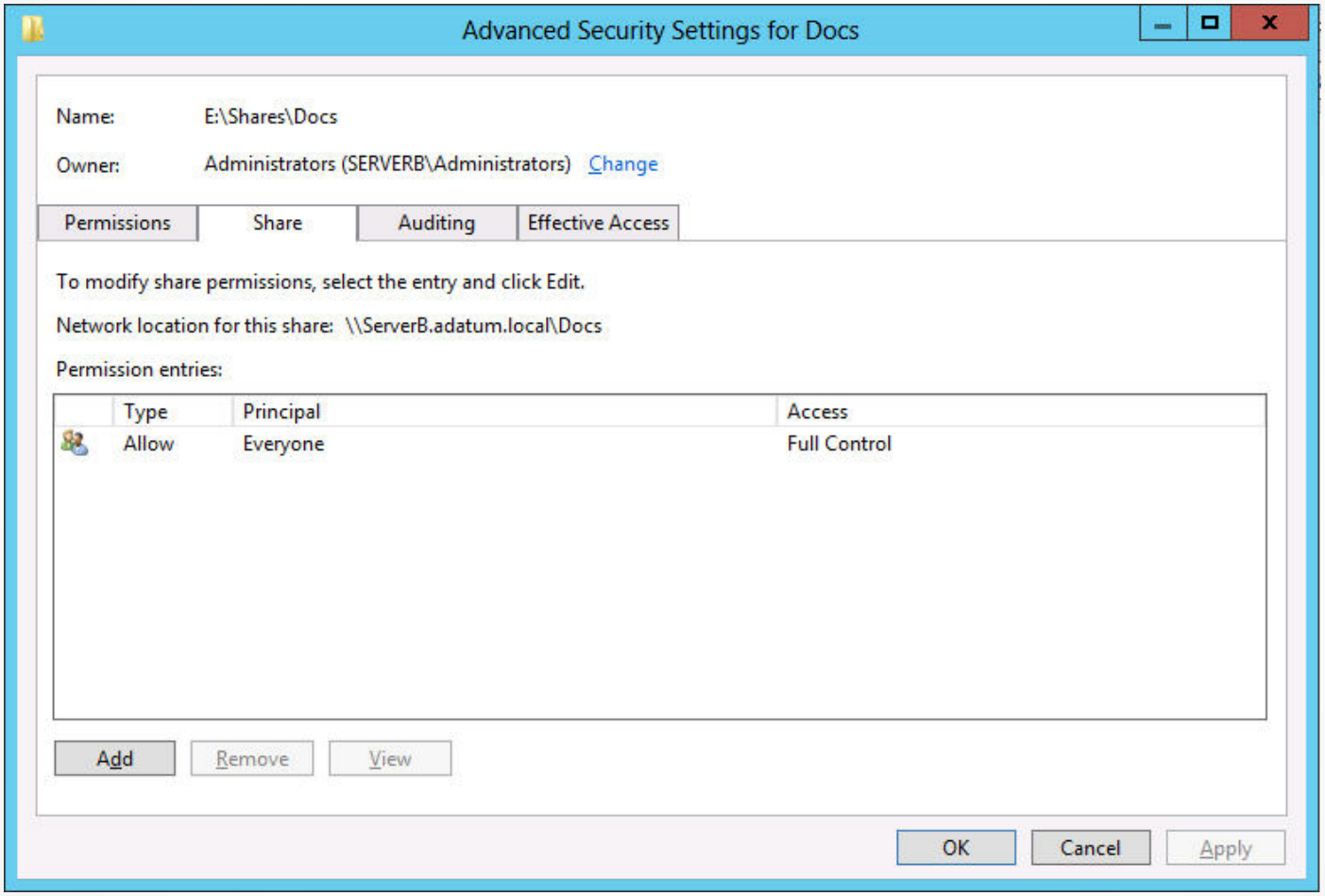
Share permission	***Allows or denies security principals the ability to:***
Full Control	Change file permissions. Take ownership of files. Perform all tasks allowed by the Change permission.
Change	Create folders. Add files to folders. Change data in files. Append data to files. Change file attributes. Delete folders and files. Perform all actions permitted by the Read permission.
Read	Display folder names, filenames, file data, and attributes. Execute program files. Access other folders within the shared folder.

Set Share Permissions



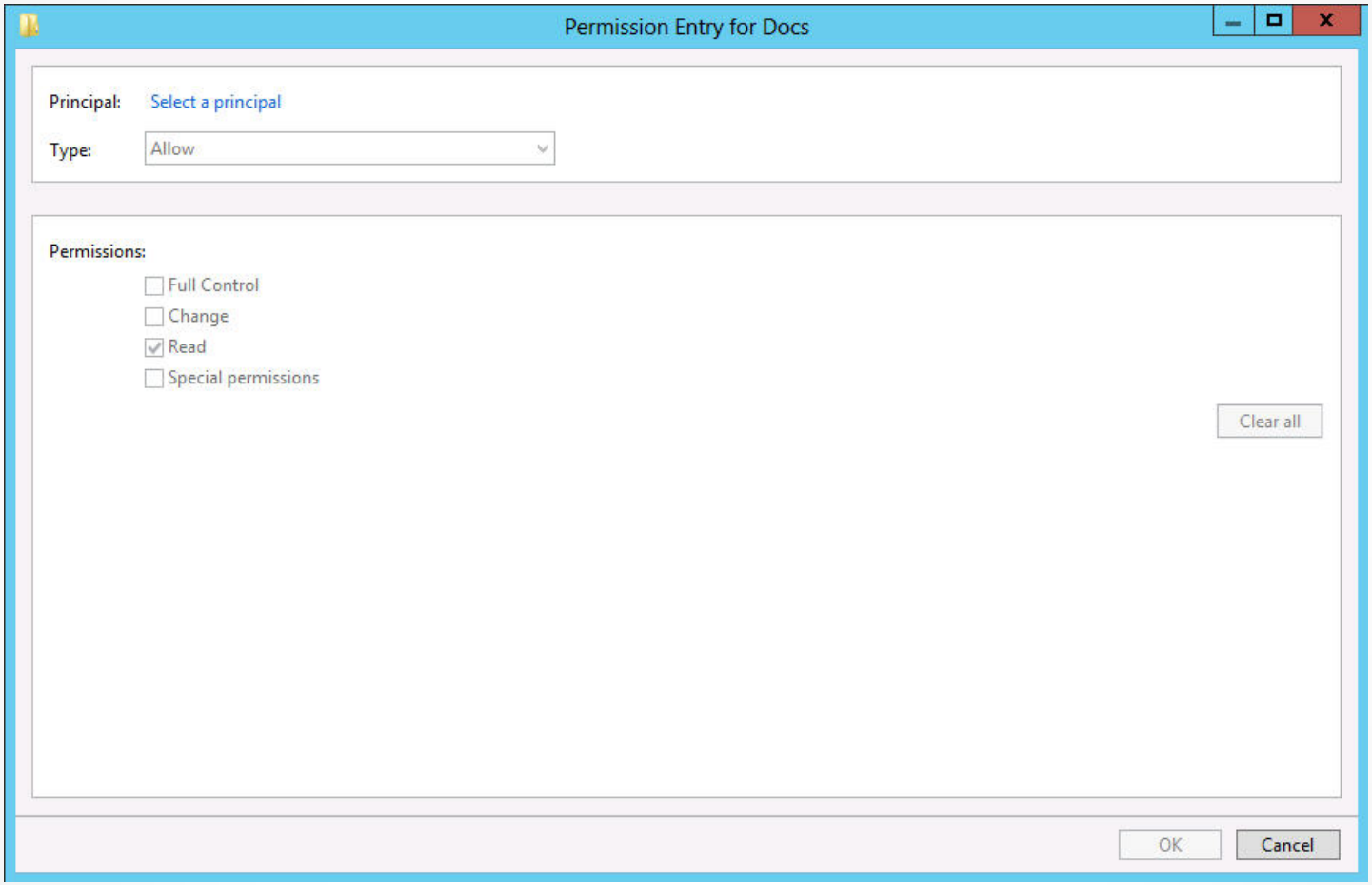
The Permissions page of a share's Properties sheet in Server Manager

Set Share Permissions



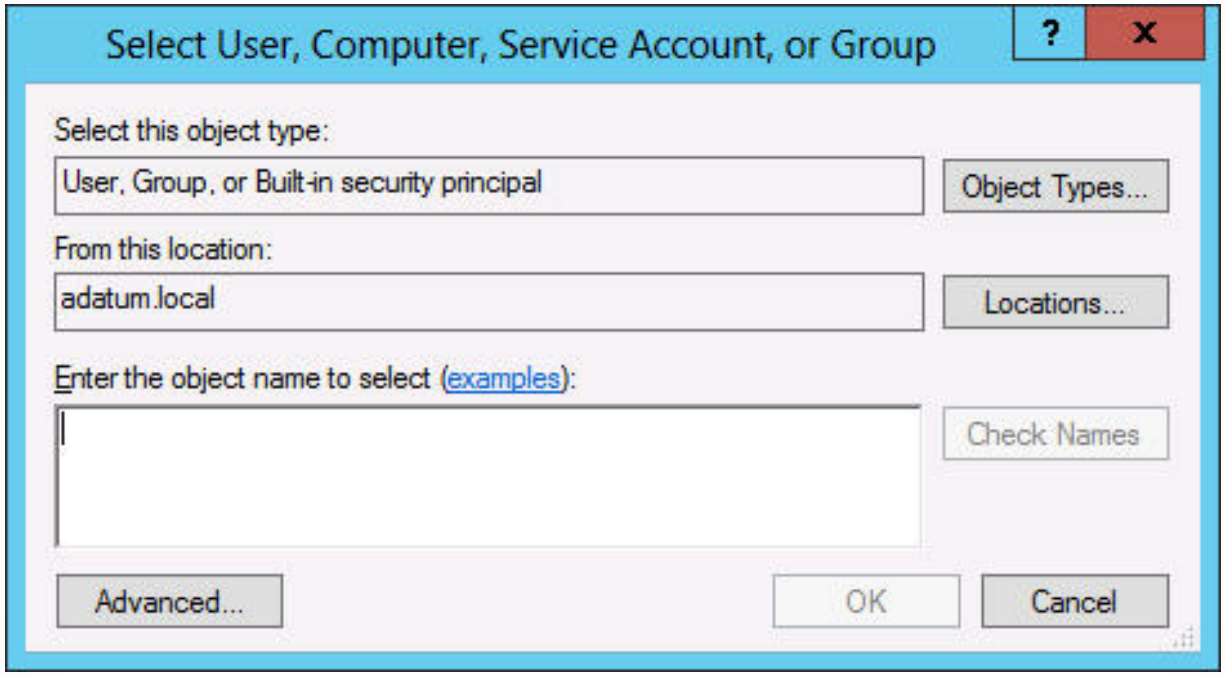
The Share tab of the Advanced Security Settings dialog box for a share in Server Manager

Set Share Permissions



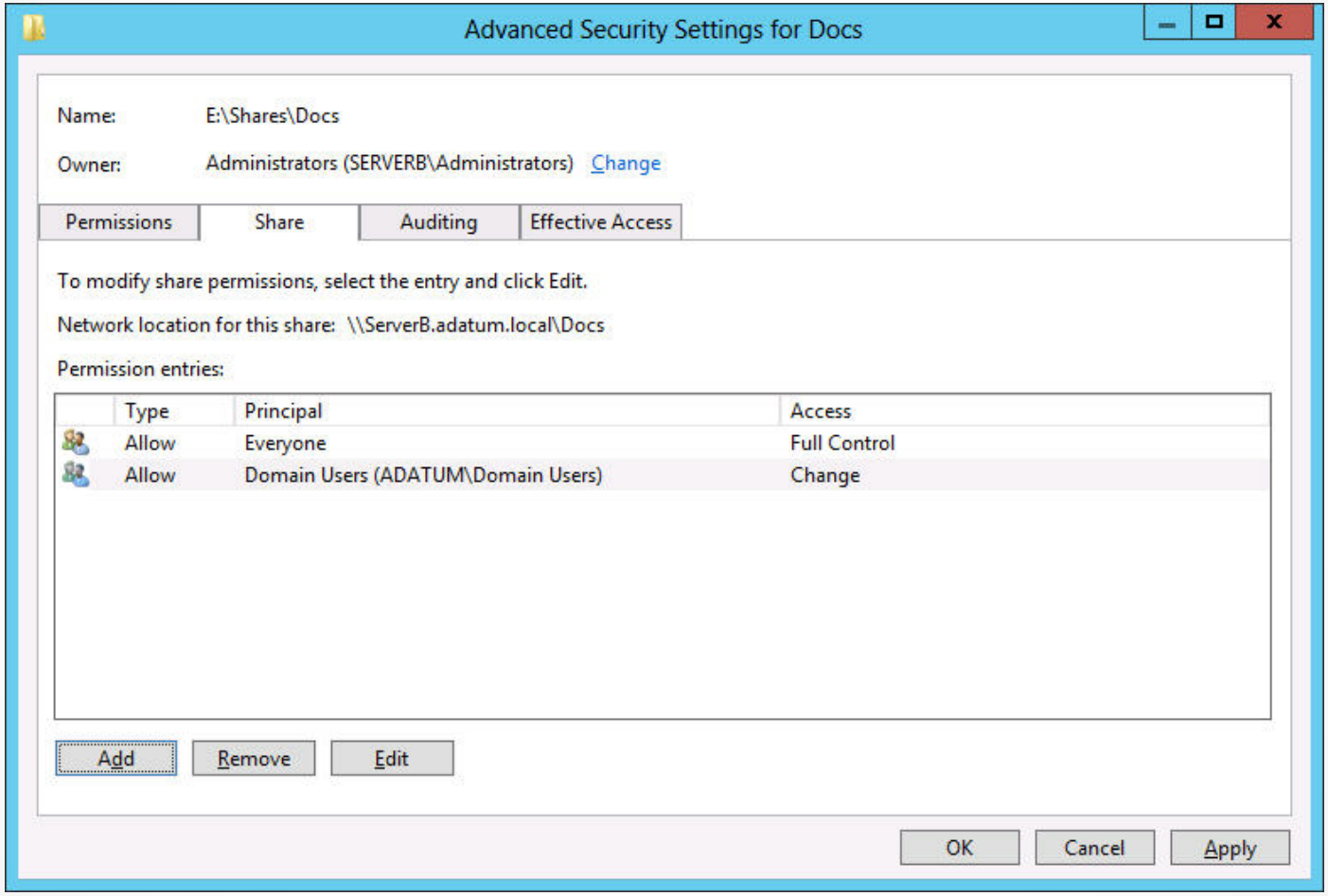
A Permission Entry dialog box for a share in Server Manager

Set Share Permissions



The Select User, Computer, Service Account, or Group dialog box

Set Share Permission



A new share permission entry in a share's access control list

NTFS Authorization

- NTFS and ReFS support permissions.
- Every file and folder on an NTFS or ReFS drive has an ACL with ACEs, each of which contains a security principal and their permissions.
- Security Principals are users and groups identified by Windows using **security identifiers (SIDs).**
- During **authorization**, when a user accesses a file/folder, the system compares the user's SIDs to those stored in the element's ACEs to determine that user's access.

NTFS Basic Permissions—Full Control

Folder

- Modify the folder permissions.
- Take ownership of the folder.
- Delete subfolders and files contained in the folder.
- Perform all actions associated with all other NTFS folder permissions.

File

- Modify the file permissions.
- Take ownership of the file.
- Perform all actions associated with all other NTFS file permissions.

NTFS Basic Permissions—Modify

Folder

- Delete the folder.
- Perform all actions associated with the Write and the Read & Execute permissions.

File

- Modify the file.
- Delete the file.
- Perform all actions associated with the Write and the Read & Execute permissions.

NTFS Basic Permissions—Read & Execute

Folder

- Navigate through restricted folders to reach other files and folders.
- Perform all actions associated with the Read and List Folder Contents permissions.

File

- Perform all actions associated with the Read permission.
- Run applications.

NTFS Basic Permissions—List Folder Contents

Folder	File
• View the names of the files and subfolders contained in the folder.	• Not applicable

NTFS Basic Permissions—Read

Folder

- See the files and subfolders contained in the folder.
- View the ownership, permissions, and attributes of the folder.

File

- Read the contents of the file.
- View the ownership, permissions, and attributes of the file.

NTFS Basic Permissions—Write

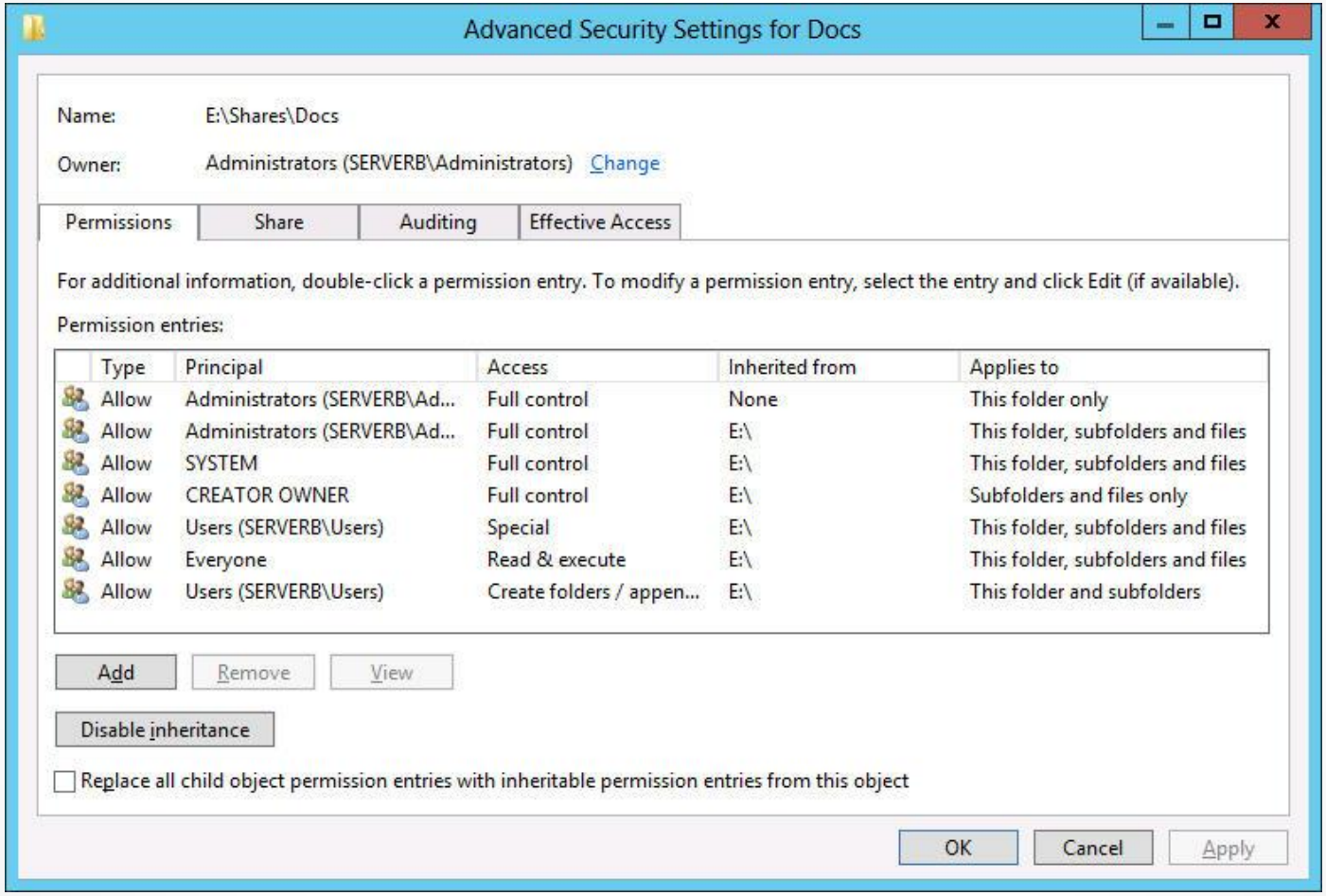
Folder

- Create new files and subfolders inside the folder.
- Modify the folder attributes.
- View the ownership and permissions of the folder.

File

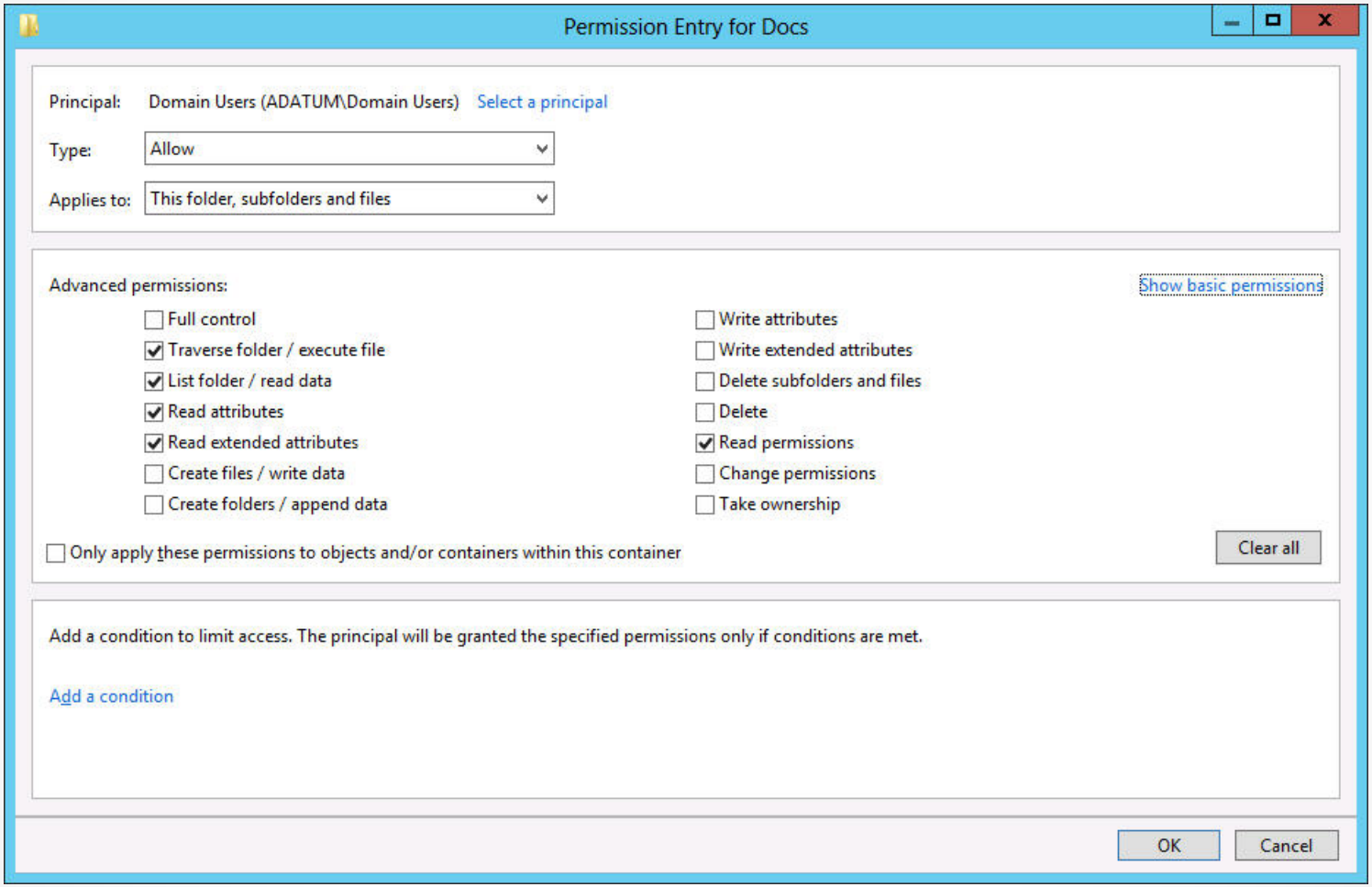
- Overwrite the file.
- Modify the file attributes.
- View the ownership and permissions of the file.

Assign Basic NTFS Permissions



The Advanced Security Settings dialog box for a share in Server Manager

Assigning Advanced NTFS Permissions

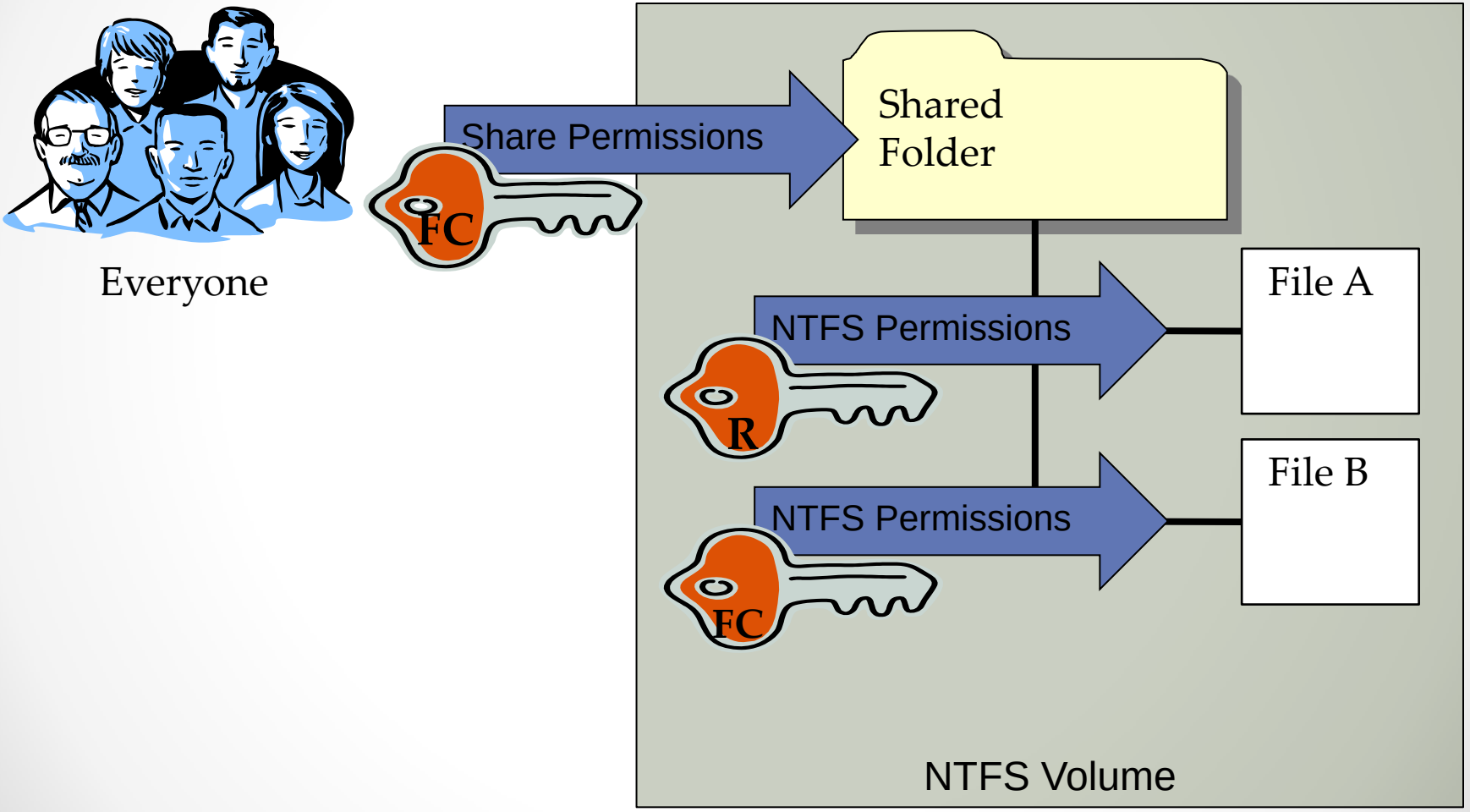


The Permission Entry dialog box displaying Advanced Permissions

Resource Ownership

- Every file and folder on an NTFS drive has an owner.
- The owner always has the ability to modify the permissions, even if current permissions settings deny them access.
- The owner is the person who created the file or folder.
- Others with the Take Ownership permission can become the owner.

Combining Share and NTFS Permissions



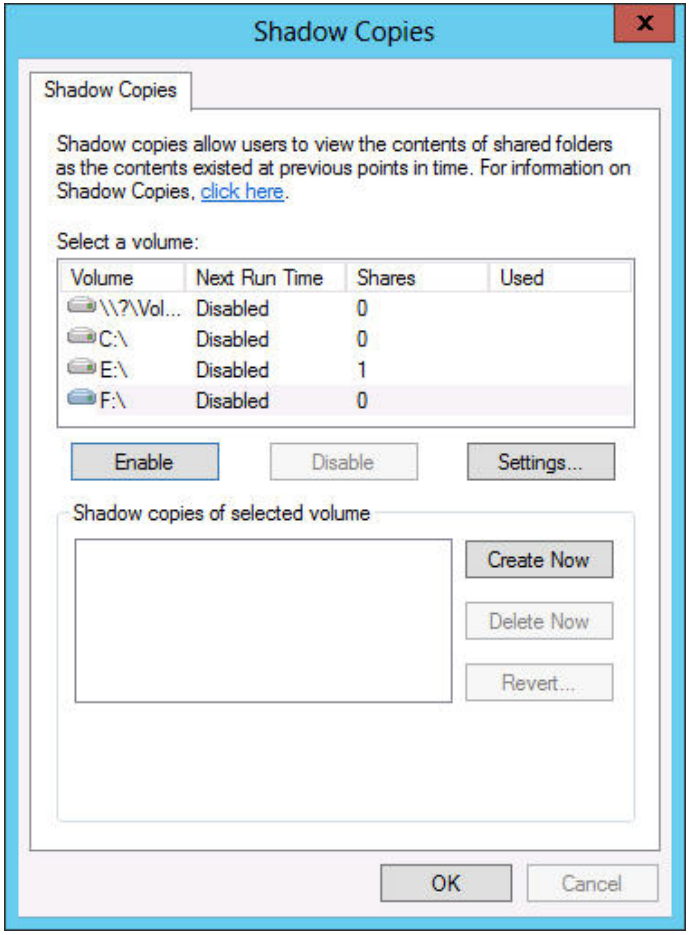
Configuring Volume Shadow Copies

Lesson 4: Configuring File and Share Access

Volume Shadow Copies

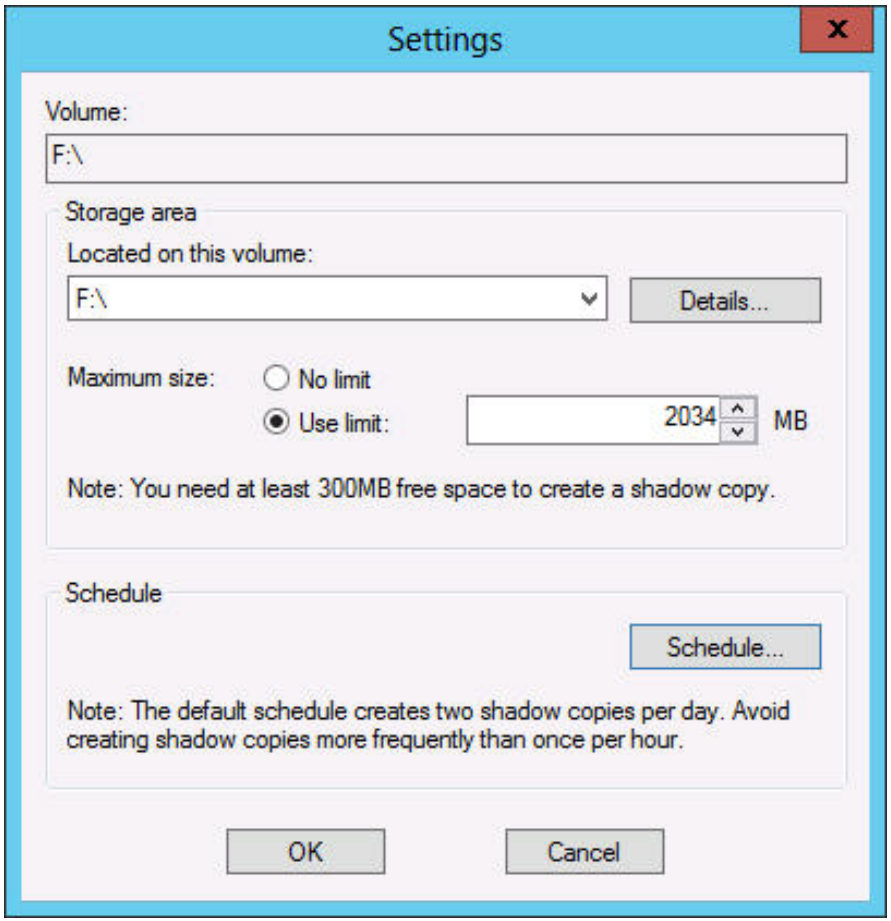
- Allow you to maintain previous versions of files on a server.
- A copy of a file can be accessed even if a file has been accidentally deleted or overwritten.
- Can be implemented for entire volumes only.

Configure Shadow Copies



The Shadow Copies dialog box

Configure Shadow Copies



The Settings dialog box

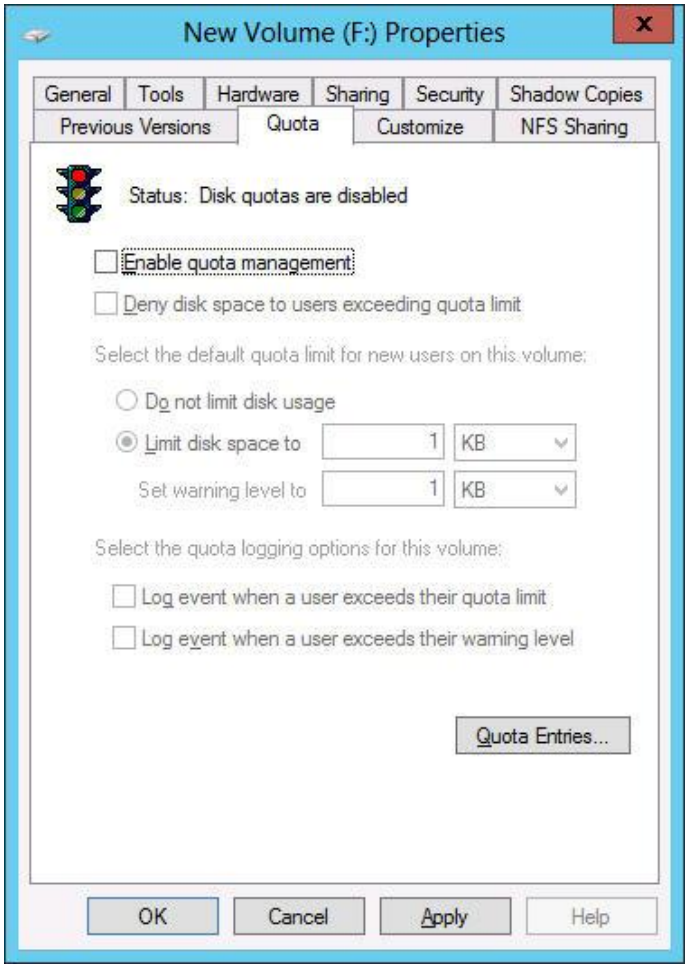
Configuring NTFS Quotas

Lesson 4: Configuring File and Share Access

NTFS Quotas

- Enable administrators to set a storage limit for users of a particular volume.
- Users exceeding the limit can be denied access or just receive a warning.
- Space consumed by users is measured by the size of the files they own or create.

Configure NTFS Quotas



The Quota tab of a volume's Properties sheet

Lesson Summary

- Creating folder shares makes the data stored on a file server's disks accessible to network users.
- Windows Server 2012 has several sets of permissions that operate independently of each other, including NTFS permissions, share permissions, registry permissions, and Active Directory permissions.
- NTFS permissions enable you to control access to files and folders by specifying the tasks individual users can perform on them. Share permissions provide rudimentary access control for all of the files on a network share. Network users must have the proper share and NTFS permissions to access file server shares.
- Access-based enumeration (ABE) applies filters to shared folders based on individual user's permissions to the files and subfolders in the share. Users who cannot access a particular shared resource are unable to see that resource on the network.

Lesson Summary

- Offline Files is a Windows feature that enables client systems to maintain local copies of files they access from server shares.
- Volume Shadow Copies is a Windows Server 2012 feature that enables you to maintain previous versions of files on a server, so that if users accidentally delete or overwrite a file, they can access a copy. You can only implement Shadow Copies for an entire volume; you cannot select specific shares, folders, or files.
- NTFS quotas enable administrators to set a storage limit for users of a particular volume. Depending on how you configure the quota, users exceeding the limit can be denied disk space, or just receive a warning.