Lesson 5: Configuring Advanced File Solutions

MOAC 70-412: Configuring Advanced Windows Server 2012 Services

Microsoft Official Academic Course

WILEY

Overview

- Objective 2.1: Configure advanced file services.
  - Configure NFS data store
  - Configure BranchCache
  - Configure File Classification Infrastructure (FCI) using File Server Resource Manager (FSRM)
  - Configure file access auditing

Configuring NFS Data Store

Lesson 5: Configuring Advanced File Solutions

Network File System (NFS)

- ***Network File System (NFS)*** is a distributed file system protocol used to access files over a network, similar to accessing a file using a shared folder in Windows, which uses Server Message Block (SMB).
- It is used with UNIX and Linux file server clients and VMware.
- Therefore, to support these clients, Windows Server 2012 supports NFS.

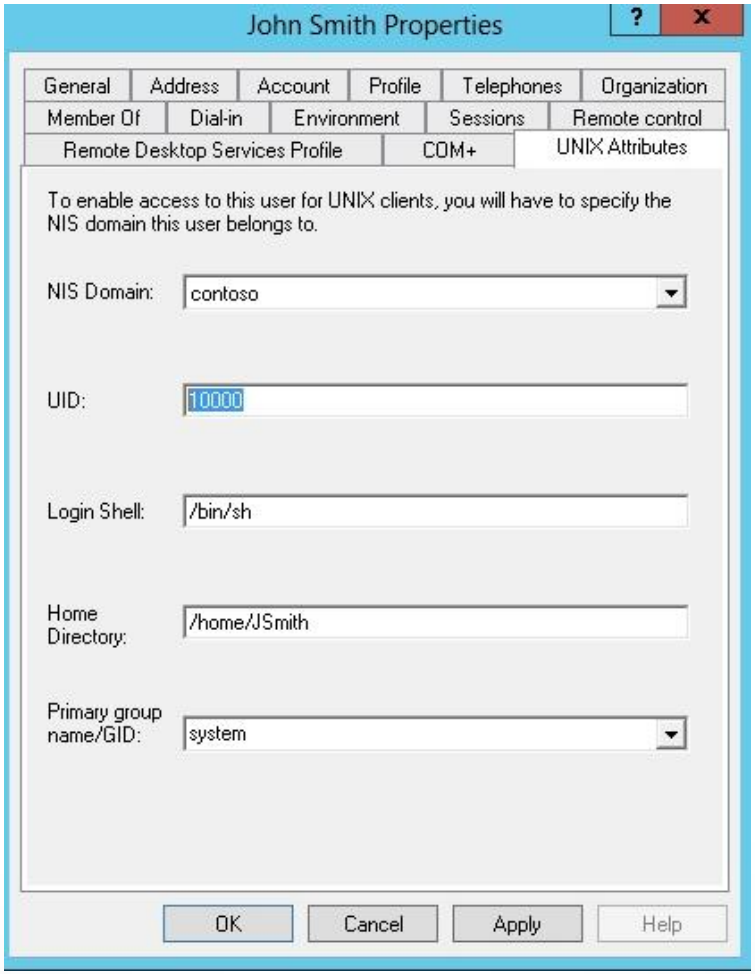
Network File System (NFS)

- By installing the Network File System role service, you can provide NFS Server and NFS Client capabilities.
- Unlike using a Universal Naming Convention (UNC), which uses a \\servername\sharename, or mounting a UNC to a drive letter, NFS takes part of a remote file system and mounts it or connects it to a local file system. The client can then access the server's files as if they were a local resource.

Network File System (NFS)

- Similar to Windows, with UNIX and Linux, you log in and authenticate with an account name and password.
- The user is identified with a ***user identifier (UID)*** value and a ***group identifier (GID)***.
- Whenever a file is accessed using NFS, the UID and GID are sent to the NFS server to see whether the user has the proper permissions for access.

Network File System (NFS)



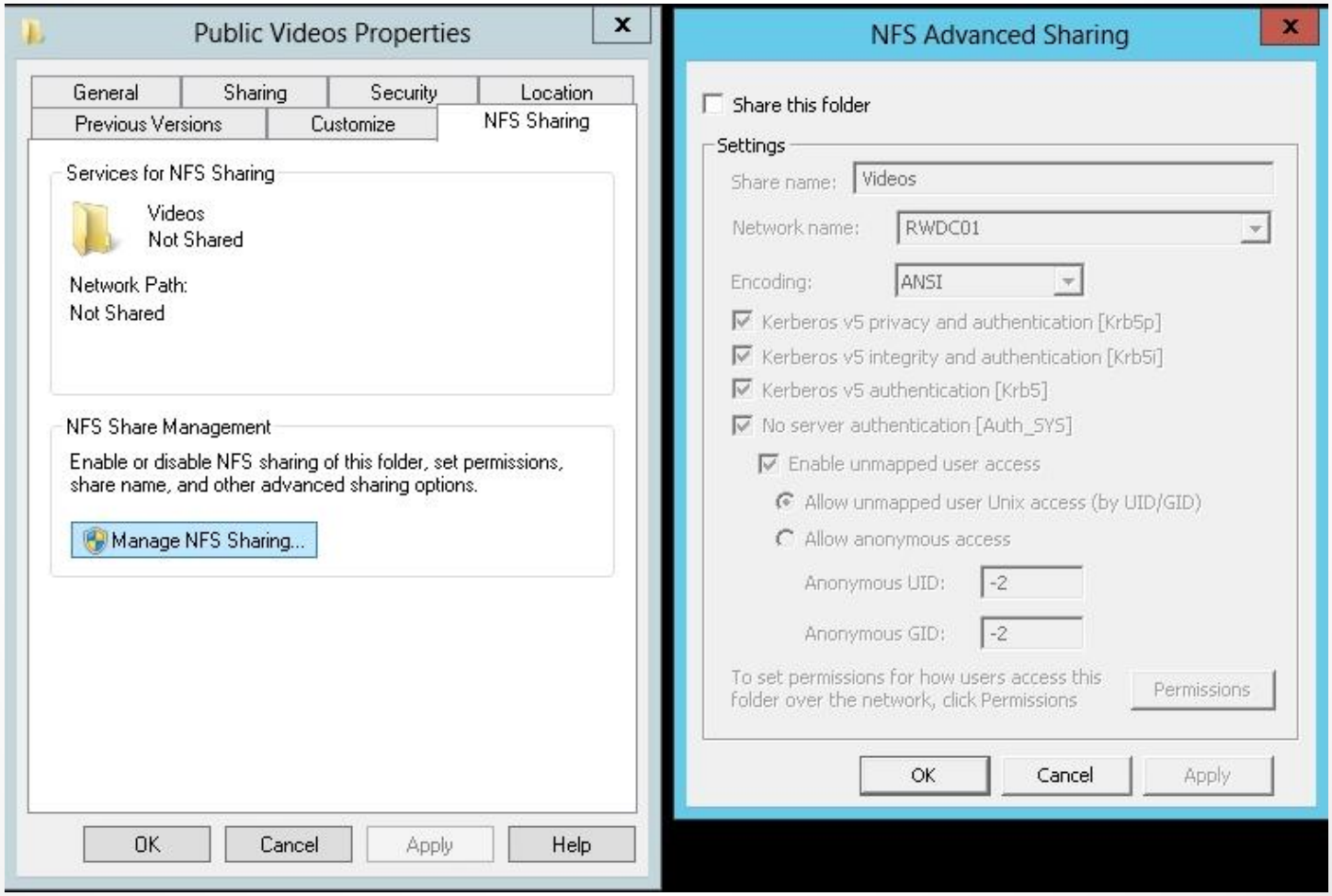
Network File System (NFS)

- For the Windows Server 2012 NFS server to grant the UNIX user access to the requested file, it must associate the UID and GID with a Windows or Active Directory account and use that account to authenticate the client.
- NFS uses Active Directory lookup and User Name Mappings to obtain user and group information when accessing NFS shared files.

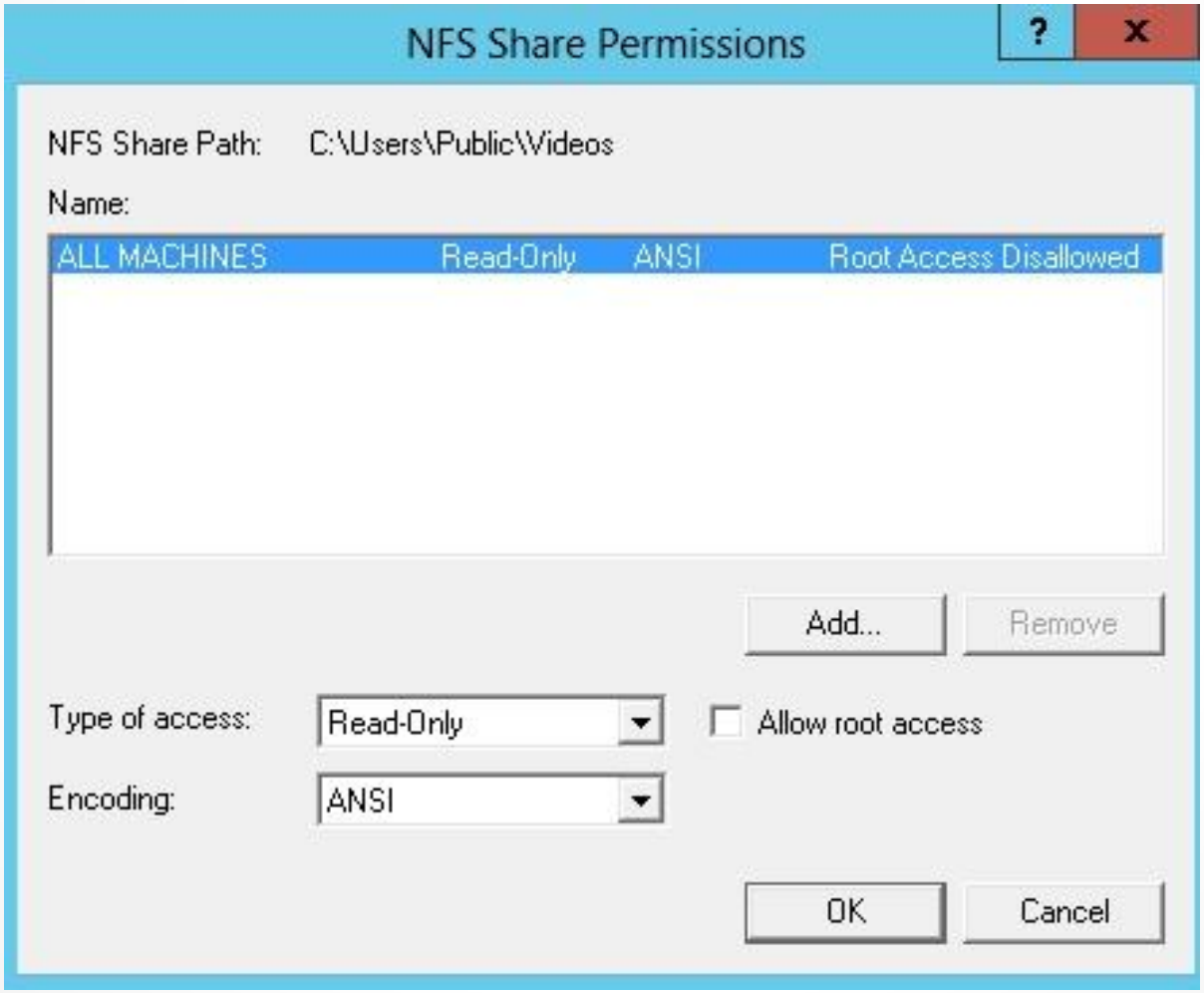
Identity Management for UNIX

- ***Identity Management for UNIX*** enables you to
  - Integrate Windows users into an existing UNIX or Linux environment
  - Manage user accounts and passwords on Windows and UNIX systems using Network Information Service (NIS)
  - Automatically synchronize passwords between Windows and UNIX operating systems.
- Install Identity Management for UNIX using the Deployment Image Servicing and management command-line tool, Dism.exe.

NFS Share



NFS Share



NFS Data Store

- Starting with Windows Server 2012, Server for NFS can now be used with failover clustering so that you can deploy NFS while providing fault tolerance.
- The shared folder within a cluster is known as an ***NFS Data Store***.

NFS Data Store

- To create an NFS shared folder on a cluster, install the following on each cluster node:
  - The File Services role
  - The Services for Network File System (NFS) role service
  - The Failover Clustering feature
- After installing these and creating a cluster, you can configure the cluster to provide high availability for NFS and create an NFS share.

Configuring BranchCache

Lesson 5: Configuring Advanced File Solutions

BranchCache

- Branch offices typically have slow connectivity to the central office and limited infrastructure for security servers.
- When users access files over the slower WAN links, there might be a delay when opening files and when opening large files or many files at the same time, which can cause other programs to be slow or delayed.
- When using ***BranchCache***, you are essentially creating a WAN accelerator where information is cached on branch computers or local servers.
- If the document is cached, it is accessed from the local branch office rather than going across a slower WAN link.

BranchCache

- BranchCache supports the following protocols:
  - HTTP or HTTPS
  - SMB, including signed SMB traffic
  - Background Intelligent Transfer Service (BITS)
- BranchCache supports IPv4, IPv6, and end-to-end encryption methods such as SSL and IPsec.

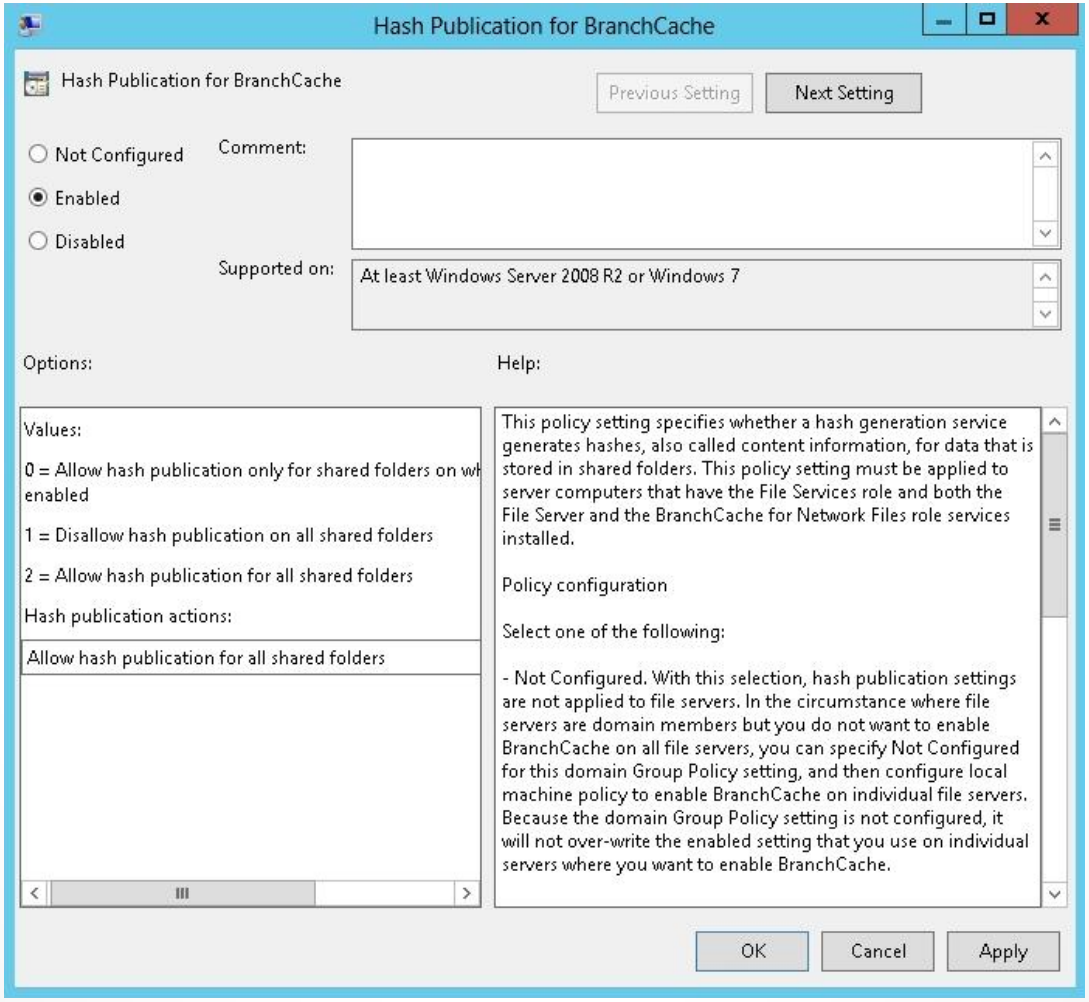
BranchCache Modes

- BranchCache can operate in one of two modes:
  - Hosted cache mode
  - Distributed cache mode
- Starting with Windows 8 and Windows Server 2012, Windows 8 Clients can be configured through Group Policy as distributed cache mode clients by default.
- The clients will search for a hosted cache server, and if one is found, it will automatically configure itself into hosted cache mode clients so that it can use the local server.

BranchCache

- To use BranchCache:
  - Install the BranchCache feature for each web server that you want to cache.
  - Install BranchCache for Network Files role service on each file server that is hosting the data.
  - Configure a hash publication for BranchCache and create BranchCache-enabled file shares.
  - Configure the clients using Group Policy or the netsh command so that the clients can use BranchCache.
  - When using the hosted cache mode, just add the BranchCache feature to the computer running Windows Server 2012 that will be holding the hosted cache.

Hash Publication for BranchCache



BranchCache

- BranchCache is disabled by default on client computers. To enable and configure BranchCache:
  1. Enable BranchCache.
  2. Enable the *Distributed Cache* mode or *Hosted Cache* mode.
  3. Configure the client firewall to allow BranchCache protocols.

Configuring File Classification Infrastructure

Lesson 5: Configuring Advanced File Solutions

File Server Resource Manager (FSRM)

- ***File Server Resource Manager (FSRM***) is a suite of tools that enables you to control and manage the quantity and type of data stored on a file server. You can
  - Define how much data a person can store.
  - Define what type of files a user can store on a file server.
  - Generate reports about the file server being used.
- You can classify files based on defined properties and apply policies based on the classification.
- You can restrict access to files, encrypt files, and have files expire.

File Classification

- ***File classification*** allows you to configure automatic procedures for defining a desired property on a file, based on the conditions specified in classification rules.
- For example, if the content contains "sales figure," you can automatically set the *Confidentiality* property to *High*.
- By using file classification, you can automate file and folder maintenance tasks, such as deleting old data or protecting sensitive information.

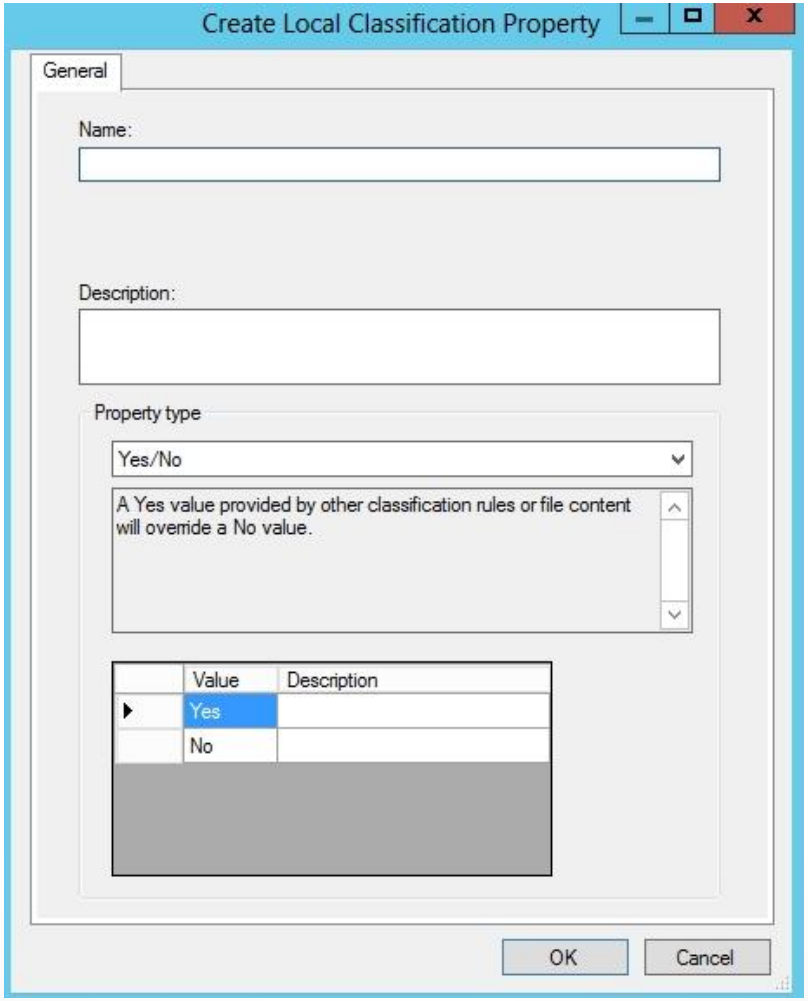
File Classification

- To use file classification:
  1. Define classification properties and values, which you can assign to files by running classification rules.
  2. Create, update, and run classification rules, which assign a single predefined property and value to files within a specified directory based on installed classification plug-ins.
  3. When running a classification rule, reevaluate files that are already classified. You can choose to overwrite existing classification values, or add the value to properties that support multiple values. You can also use classification rules to declassify files that are not in the classification criterion anymore.

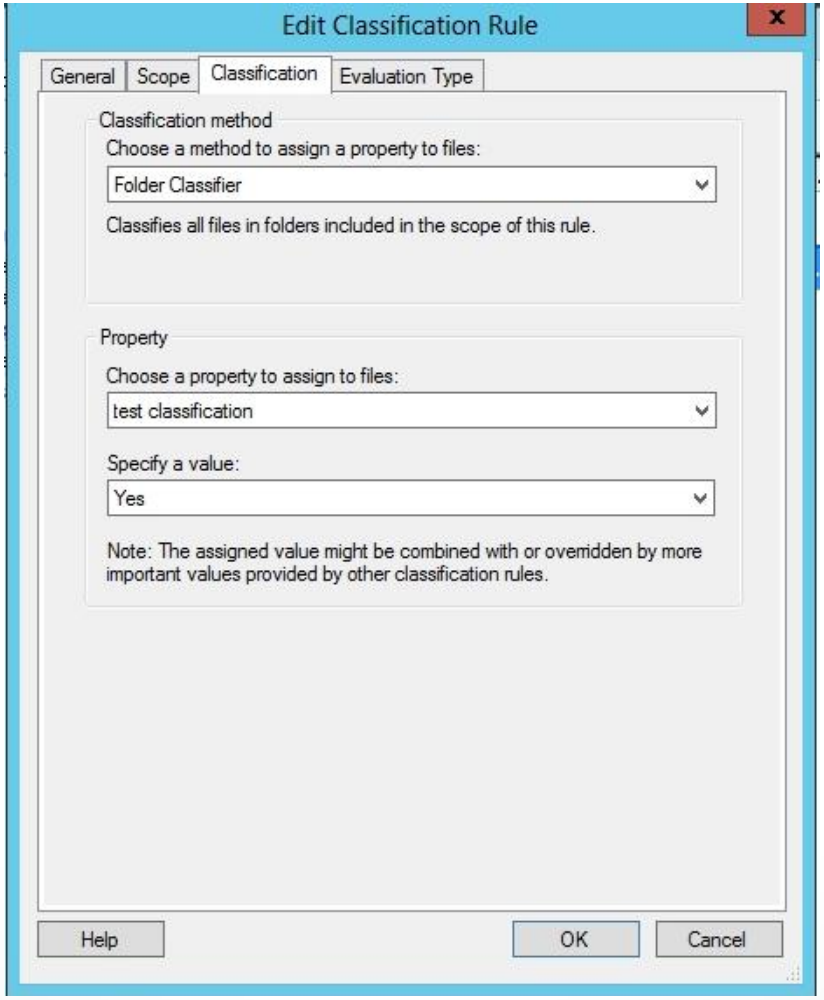
File Classifications

- To configure file classifications, you use the File Server Resource Manager console to create classification rules that scan files for a standard text string, or a string that matches a pattern.
- When a match is found, the file is classified as specified in the classification rule.

Classification Property



Editing Classification Rule



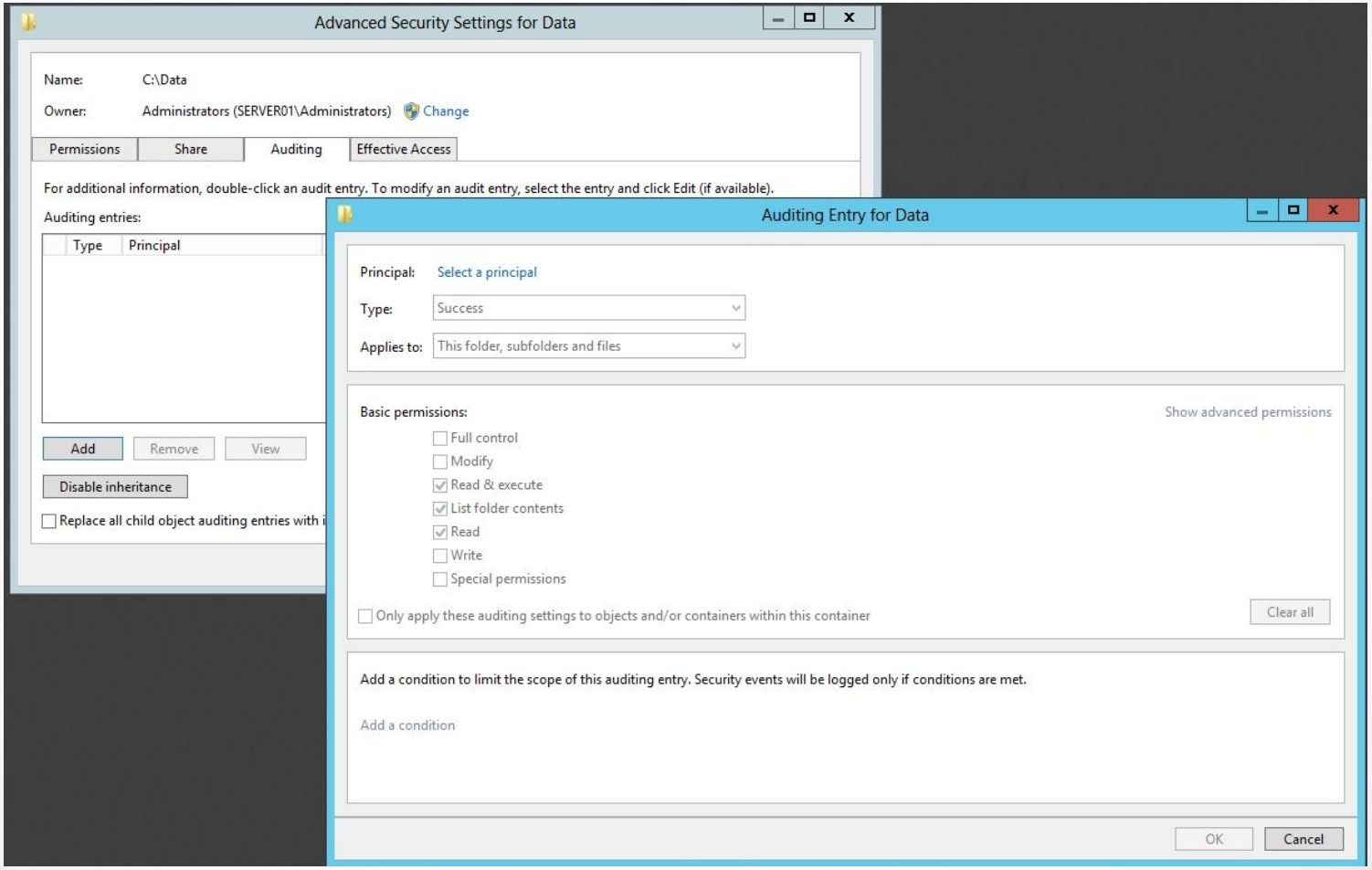
Configuring File Access Auditing

Lesson 5: Configuring Advanced File Solutions

Authentication, Authorization, and Auditing

- Security can be divided into three areas:
  - ***Authentication***: Used to prove the identity of a user.
  - ***Authorization***: Gives access to the user who was authenticated.
  - ***Auditing***: Gives you a record of the users who have logged in, what those users accessed or tried to access, and what action those users performed (e.g., rebooting, shutting down a computer, or accessing a file).
- When you want to audit files, you must first enable object access auditing. Then you must specify what files you want to audit.

File Auditing



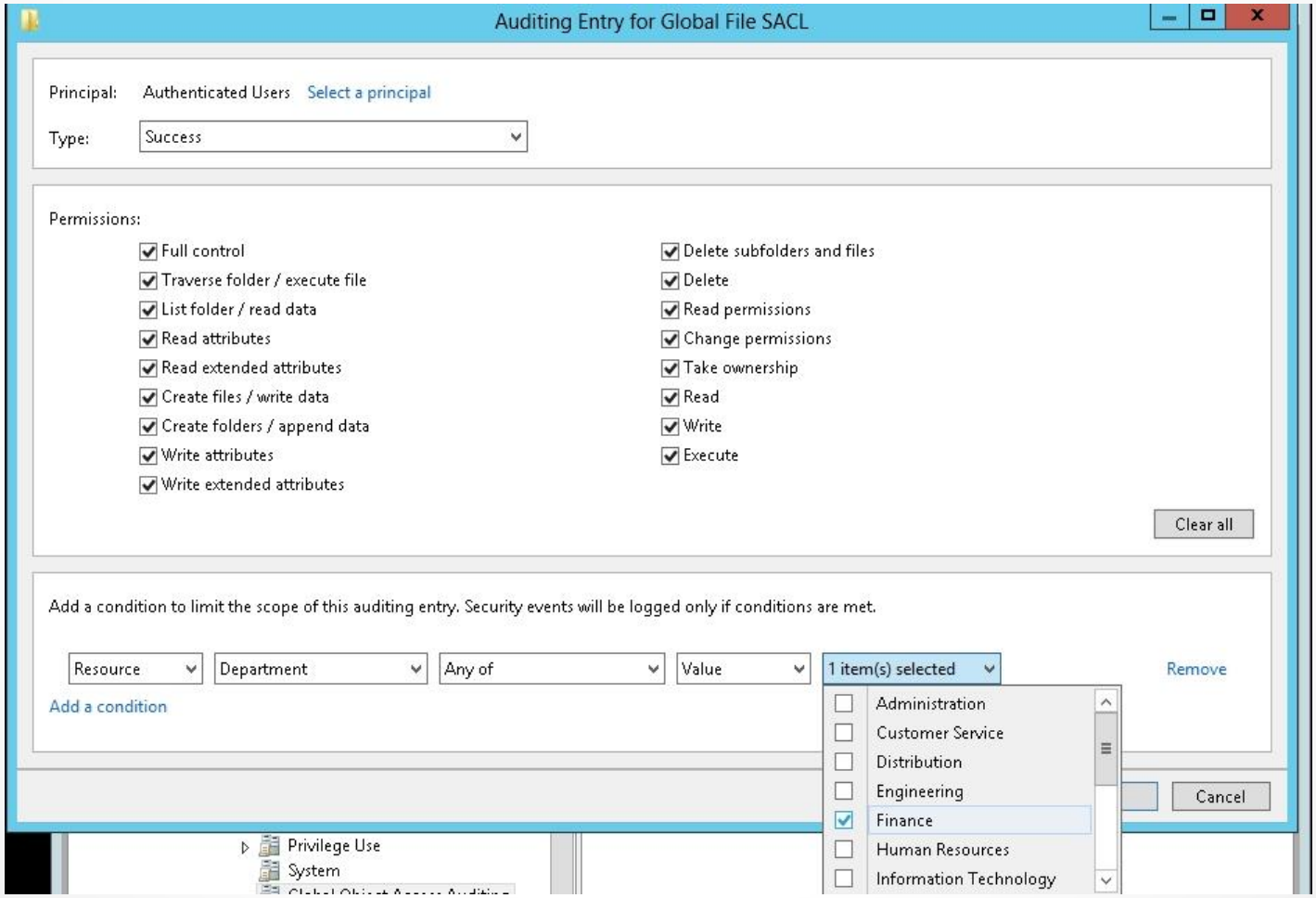
Global Object Access Auditing

- Starting with Windows 7 and Windows Server 2008 R2, you can enable Global Object Access Auditing so that you can
  - Configure object access auditing for every file and folder in a computer's file system.
  - Centrally manage and configure Windows to monitor files without going to each computer to configure the auditing of each computer or folder.

Global Object Access Auditing

- To use global object access to audit files, you must enable two settings:
  - Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy\Audit Policies\Object Access\Audit File System
  - Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy\Audit Policy\Global Object Access Auditing\File System (see Figure 5-15).
- Additionally, you must configure the System Access Control List (SACL), where you define the principal that you want to monitor, the type of event (success, failure, or all), the permission that you want to monitor, and a condition.

Global Object Access Auditing



Lesson Summary

- Network File System (NFS) is a distributed file system protocol used to access files over a network, similar to accessing a file using a shared folder in Windows, which uses Server Message Block (SMB).
- Install the Network File System role service to provide NFS Server and NFS Client capabilities.
- Similar to Windows, with UNIX and Linux, you log in and authenticate with an account name and password. The user is identified with a user identifier (UID) value and a group identifier (GID).

Lesson Summary

- Identity Management for UNIX allows you to integrate Windows users into an existing UNIX/Linux environment, manage user accounts and passwords on Windows and UNIX systems using Network Information Service (NIS), and automatically synchronize passwords between Windows and UNIX operating systems.
- When you install the Services for NFS role service, an NFS Sharing tab is added to the properties of every volume and folder on the computer's drives.
- Starting with Windows Server 2012, Server for NFS can now be used with failover clustering so that you can deploy NFS while providing fault tolerance. The shared folder within a cluster is known as an *NFS Data Store*.

Lesson Summary

- BranchCache improves the performance of applications by reducing the network use on the WAN connection between branch offices and the central office by locally caching frequently used files on computers in the branch office.
- BrancheCache can operate in one of two modes: hosted cache mode and distributed cache mode.
- The hosted cache mode uses a dedicated server to host the cache. If the content is not available in the hosted cache, the content will be retrieved over the WAN link and added to the hosted cache so that clients requesting the same content in the future will benefit.
- Instead of having a centralized cache, distributed cache mode has the cache distributed among the local Windows 7 or 8 clients at the local site.

Lesson Summary

- File Server Resource Manager (FSRM) is a suite of tools that enables you to control and manage the quantity and type of data stored on a file server.
- File classification allows you to configure automatic procedures for defining a desired property on a file, based on the conditions specified in classification rules.

Lesson Summary

- Auditing allows you to create a record of the users who have logged in, what the users accessed or tried to access, and what action the users performed (e.g., rebooting, shutting down a computer, or accessing a file).
- To audit files, you must first enable object access auditing. Then you must specify what files you want to audit.
- Starting with Windows 7 and Windows Server 2008 R2, you can enable Global Object Access Auditing, so that you can configure object access auditing for every file and folder in a computer's file system.