Lesson 6: Implementing Dynamic Access Control

MOAC 70-412: Configuring Advanced Windows Server 2012 Services

Microsoft Official Academic Course

WILEY

Overview

- Objective 2.2 – Implement Dynamic Access Control (DAC).
  - Configure user and device claim types
  - Implement policy changes and staging
  - Perform access-denied remediation
  - Configure file classification

Using Dynamic Access Control

Lesson 6: Implementing Dynamic Access Control

Windows Deployment Services (WDS)

- ***Dynamic Access Control (DAC)***, originally called *claims-based access control*, was introduced with Windows Server 2012 and is used for access management.
- It provides an automatic mechanism to secure and control access to resources.

Claims-Based Access Control

- ***Claims-based access control*** uses a trusted identity provider to provide authentication.
- The ***trusted identity provider*** issues a token to the user, which the user then presents to the application or service as proof of identity.
- Identity is based on a set of information. Each piece of information is referred to as a ***claim*** (e.g., who the user or computer claims to be) and is stored as a token, which is a digital key.
- The ***token*** is digital identification for the user or computer that is accessing a network resource.
- As users or computers need access to a resource, the user or computer presents the token to get access to the resource.

Security Token Service (STS)

- In Windows Server 2012, the identity provider is the ***Security Token Service (STS)*** and the claims are the Active Directory attributes assigned to a user or device (e.g., a computer).
- The claims, the user's security identifier (SID), and group membership are stored inside the Kerberos ticket.
- The ticket is then used to access protected resources.
- Claims authorization relies on the Kerberos Key Distribution Center (KDC).

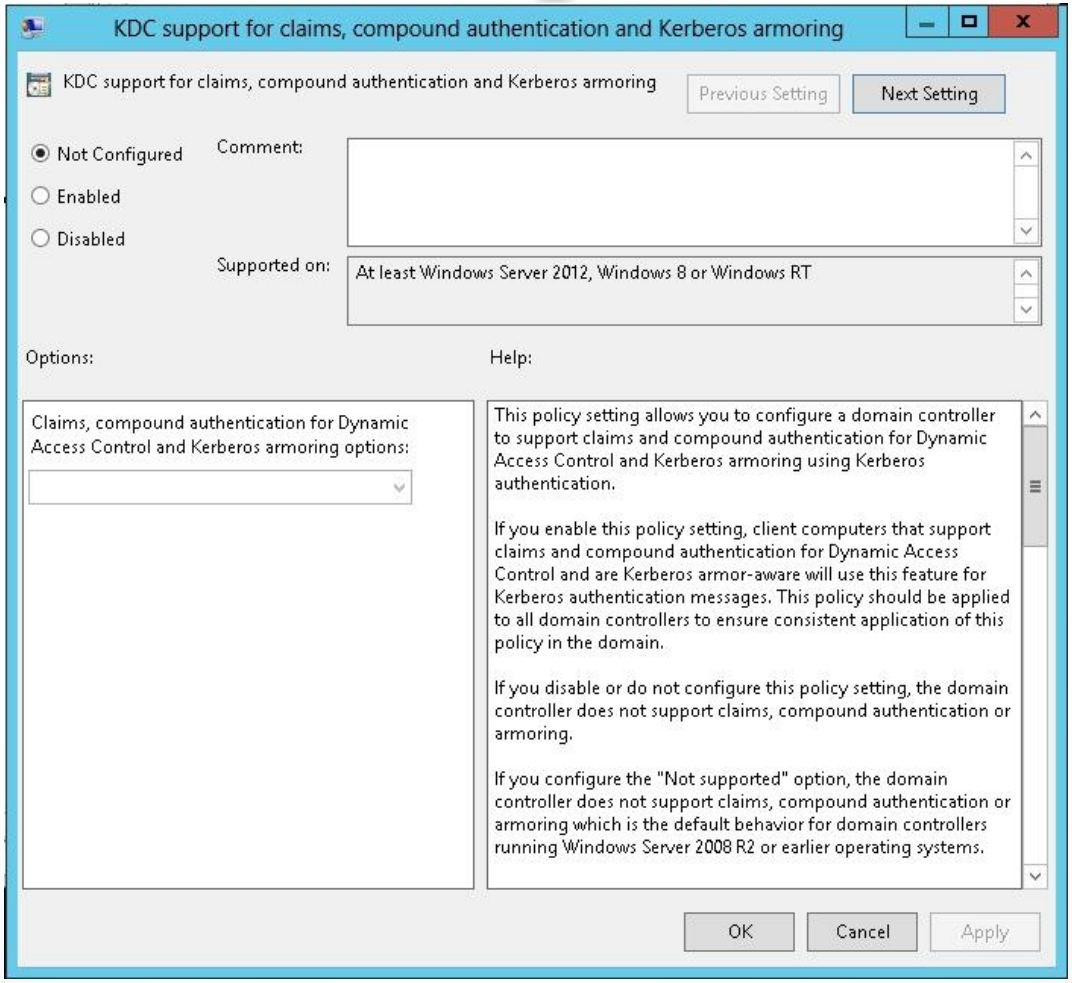
Dynamic Access Control

- In Windows Server 2012, DAC allows you to
  - Identify data by using automatic and manual classification or tagging files in an organization.
  - Control access to files by applying automatic policies that are controlled by Central Access Policies.
  - Audit access by using a Central Audit Policy to ensure compliance and to be used in forensic analysis.
  - Use Active Directory Rights Management Service (RMS) to encrypt sensitive documents. Active Directory Management Services is discussed in Lesson 21, "Installing and Configuring Active Directory Rights Management Services."
  - Offer Access-Denied Assistance, which provides a method for users to request access from the owner of data when he or she is denied access.

Dynamic Access Control

- Requirements to use claims-based authorization include:
  - Windows Server 2012 must be installed on the file server that hosts the resources that DAC protects.
  - At least one Windows Server 2012 domain controller must be accessible by the requesting client.
  - If you use claims across a forest, you must have a Windows Server 2012 domain controller in each domain.
  - If you use device claims, clients must run Windows 8.

KDC Options



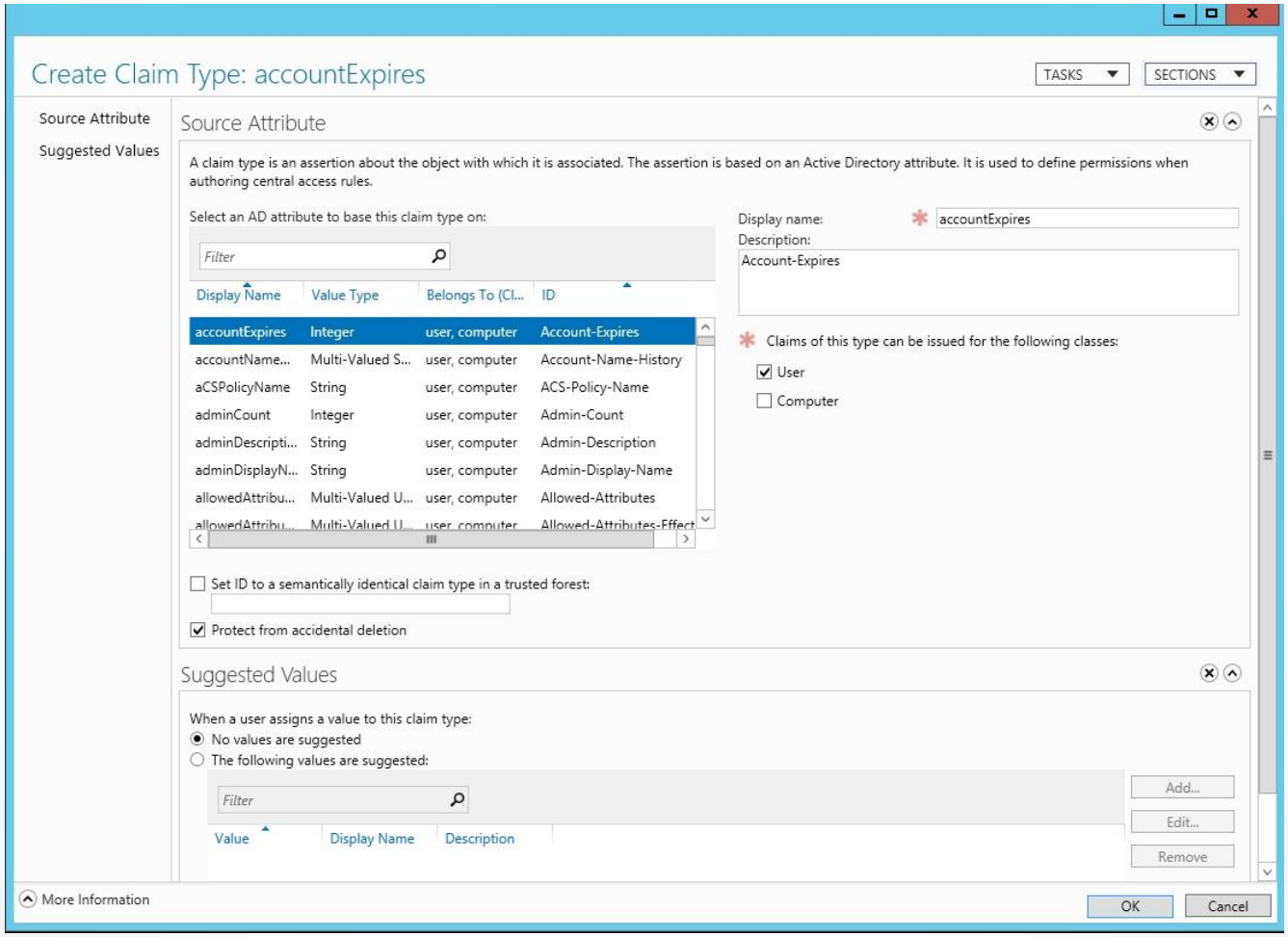
Attribute-Based Claims

- Attribute-based claims are
  - The most common types of claims
  - Usually configured with Active Directory Administrative Center, specifically using the Dynamic Access Control node.
- All claims are stored in the configuration partition in AD DS, which is a forest-wide partition. As a result, all domains in the forest share the claim dictionary.

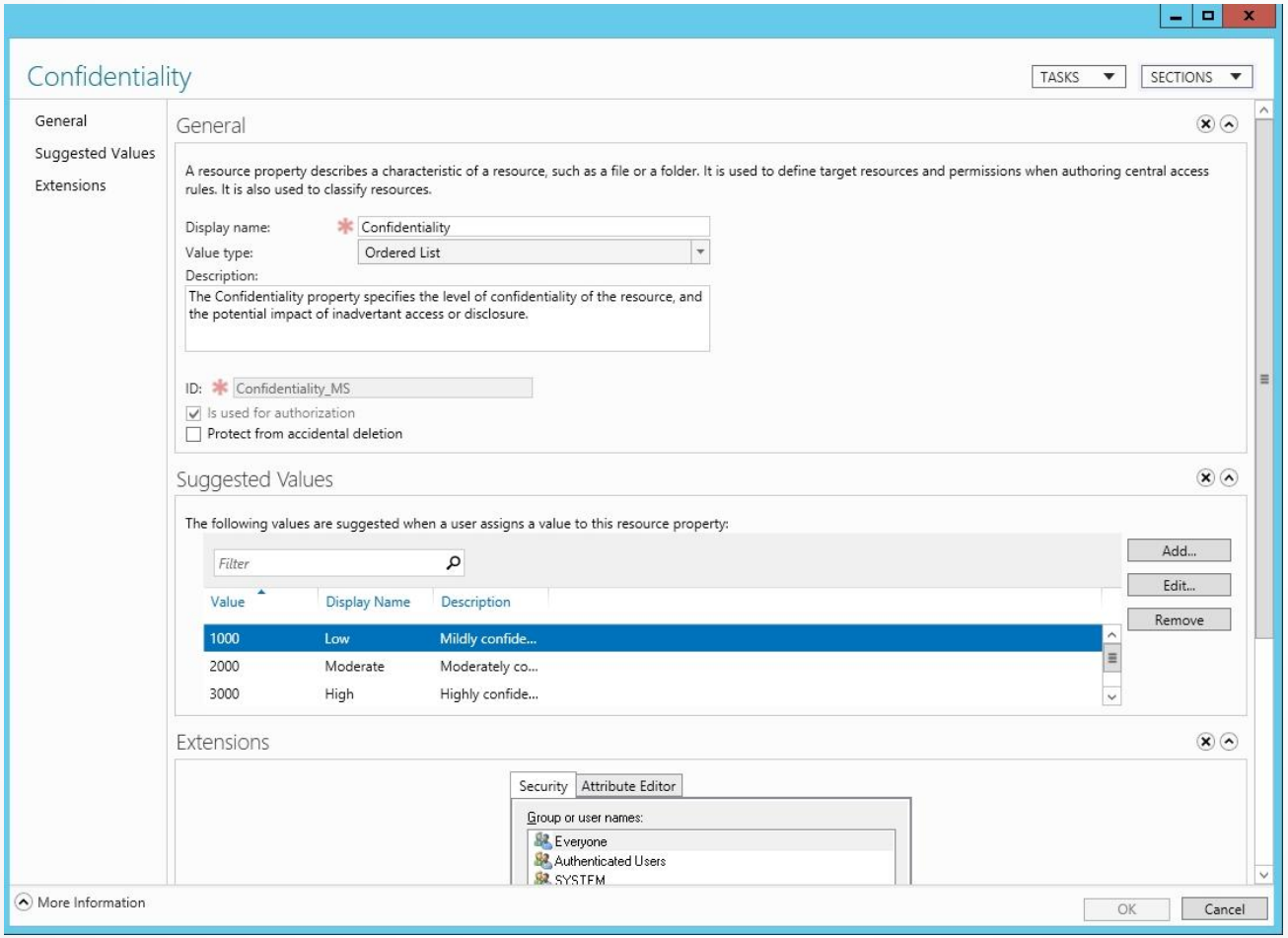
Attribute-Based Claims

- To create a ***claim type*** specify a specific attribute from Active Directory.
- For DAC to be effective, Active Directory must contain accurate information.
- By default, the claim name is the name of the selected attribute name.
- You can modify this to give the claim a more meaningful name.
- You also have the option to provide suggested values for the claim.

Creating Claim Type



Confidentiality Resource Property



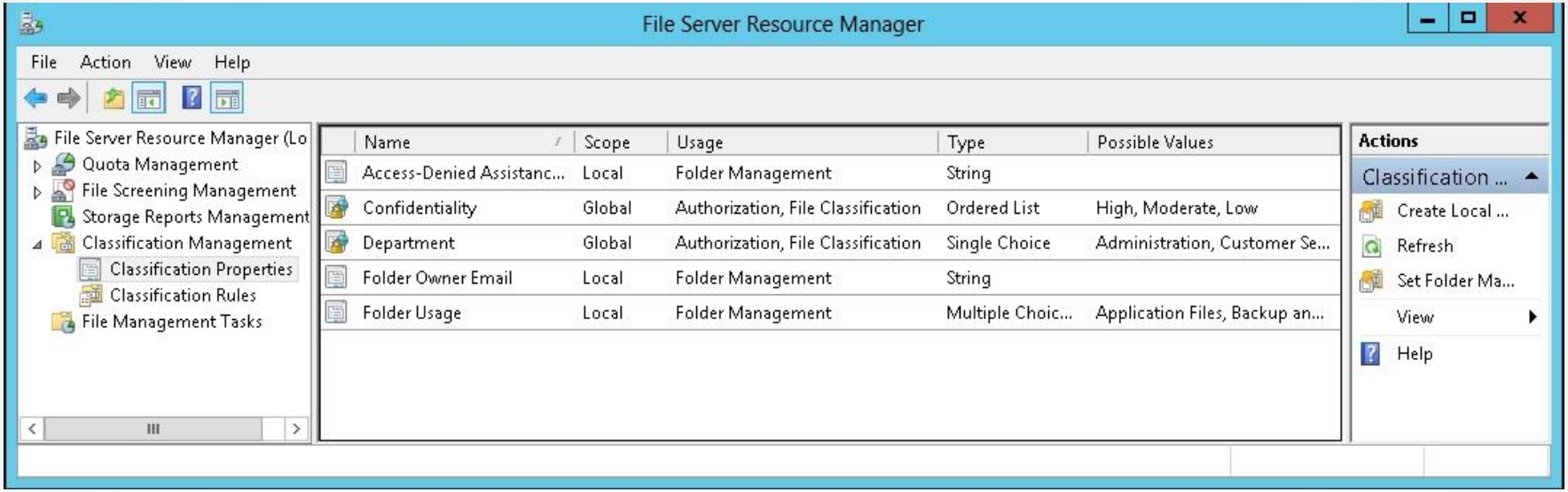
Configuring File Classification

- Classification management and file management tasks enable administrators to manage groups of files based on various file and folder attributes.
- After folders and files are classified, you can automate file and folder maintenance tasks (e.g., cleaning up stale data or protecting sensitive information).
- Although classification management can be done manually, you can automate this process with the File Server Resource Manager console.

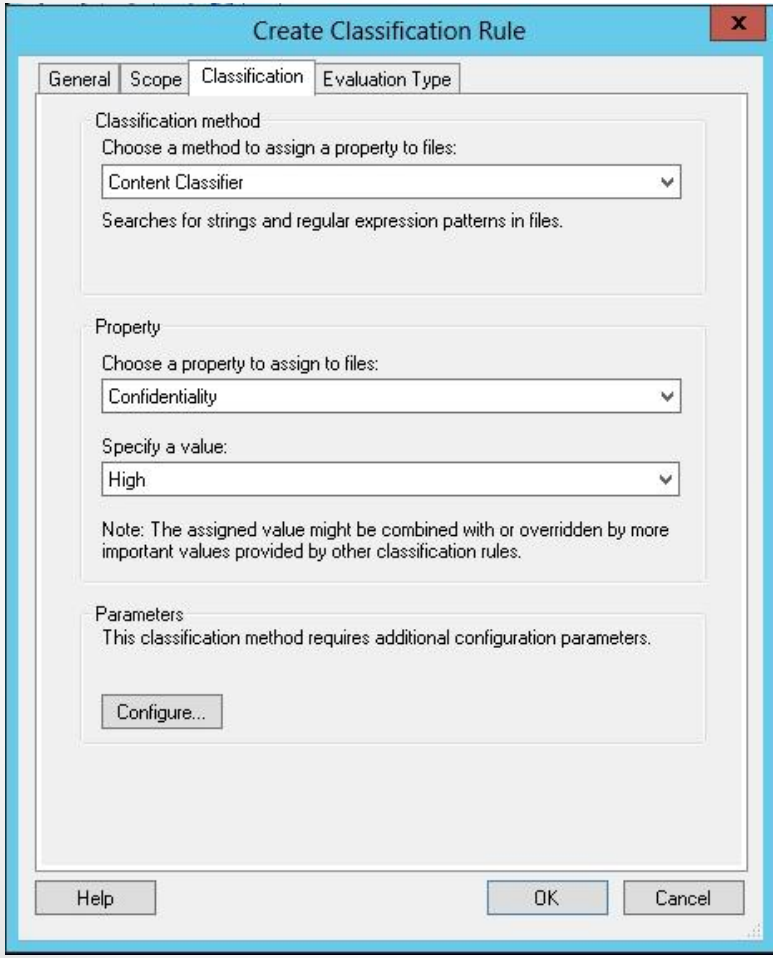
Classification Rules

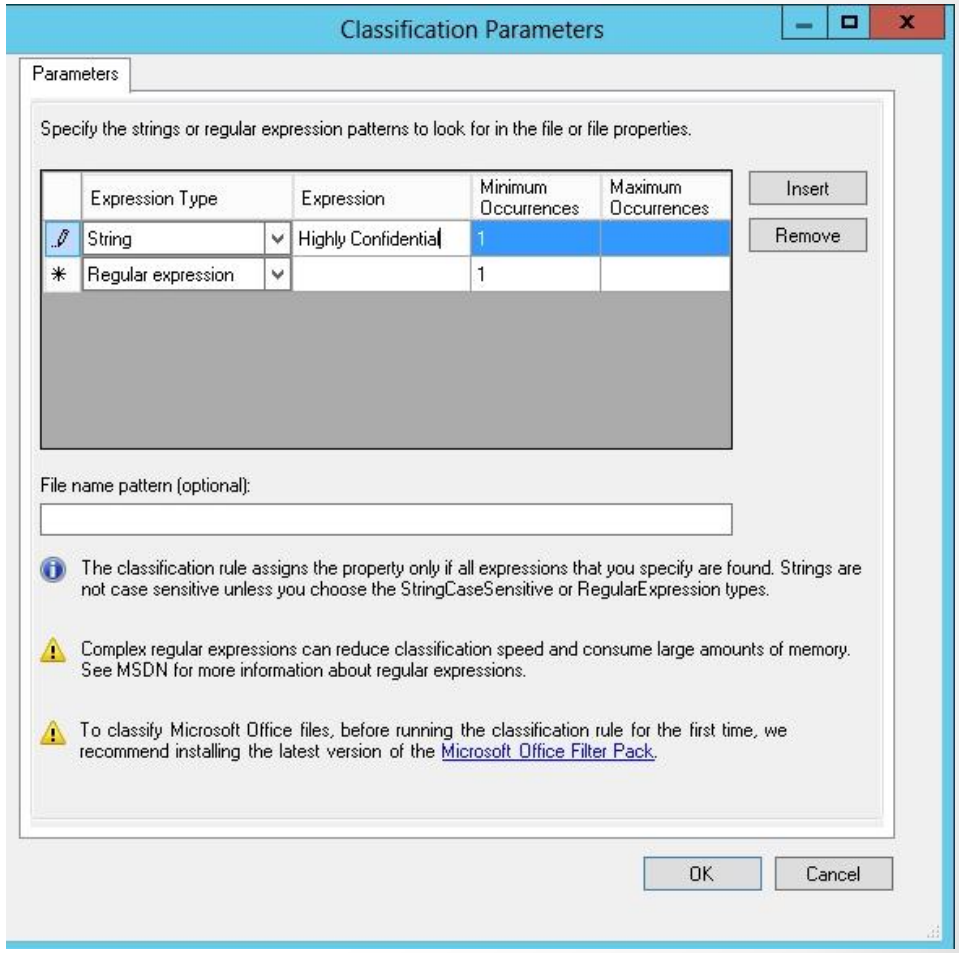
- ***Classification rules*** can be created and then scheduled to be applied on a regular basis so that files are automatically scanned and classified based on the content of the file.
- When performing file classification:
  - Identify classifications that you want to apply to documents.
  - Choose the method that you will use to identify documents for classification.
  - Set up the schedule for automatic classifications.
- Establish periodic reviews to determine the success of the classification.

Viewing Created Classification Properties



Creating Classification Rules





Viewing Document File Classification

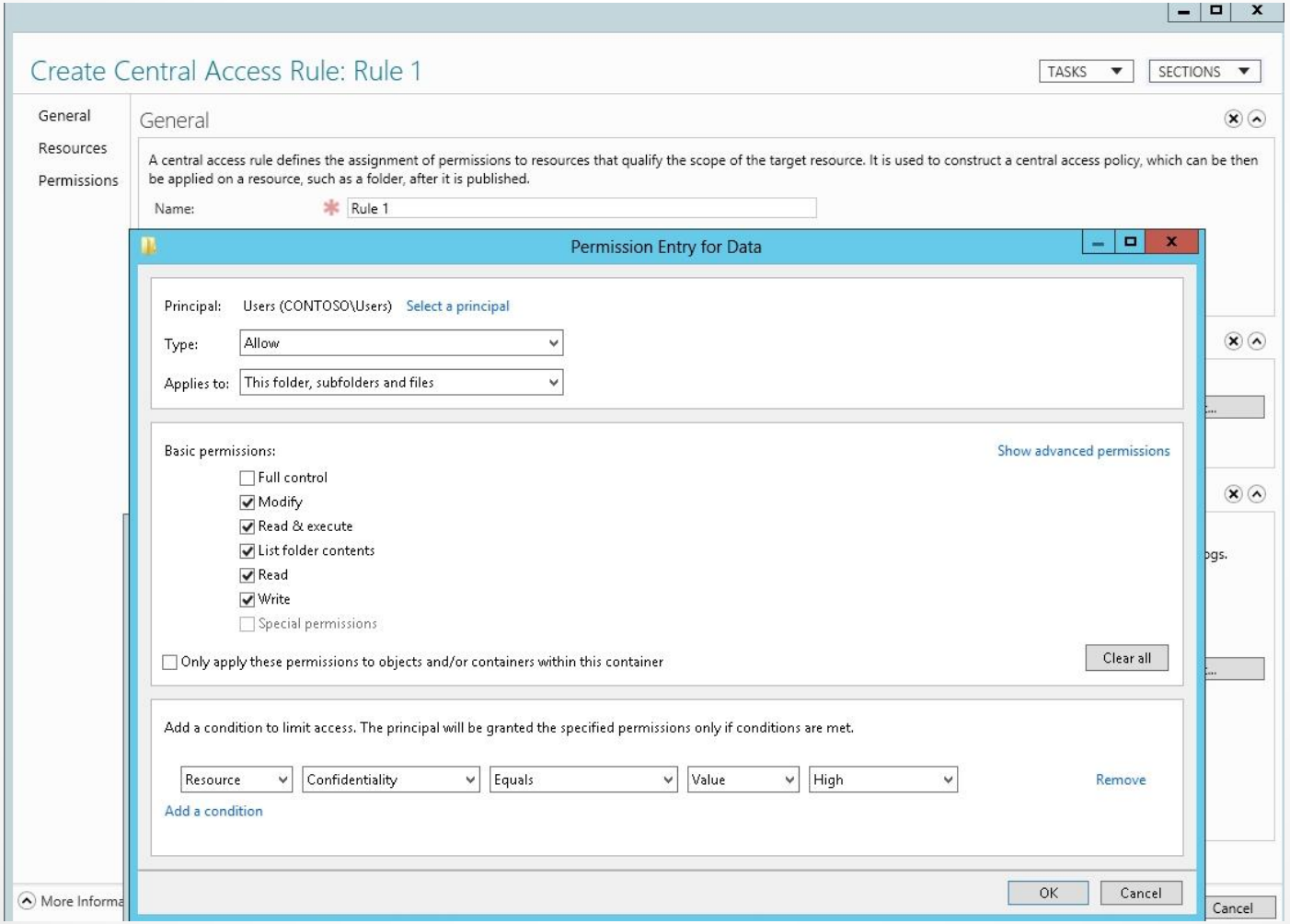
Central Access Policy

- A ***Central Access Policy*** contains ***Central Access Rules*** that grant permissions to objects for a defined group of resources.
- By default the rules apply to all resources, but you can limit the resources to which the rule will apply.
- Once the rule is defined, you can choose to apply it live or you can choose to use a "staging" mode.

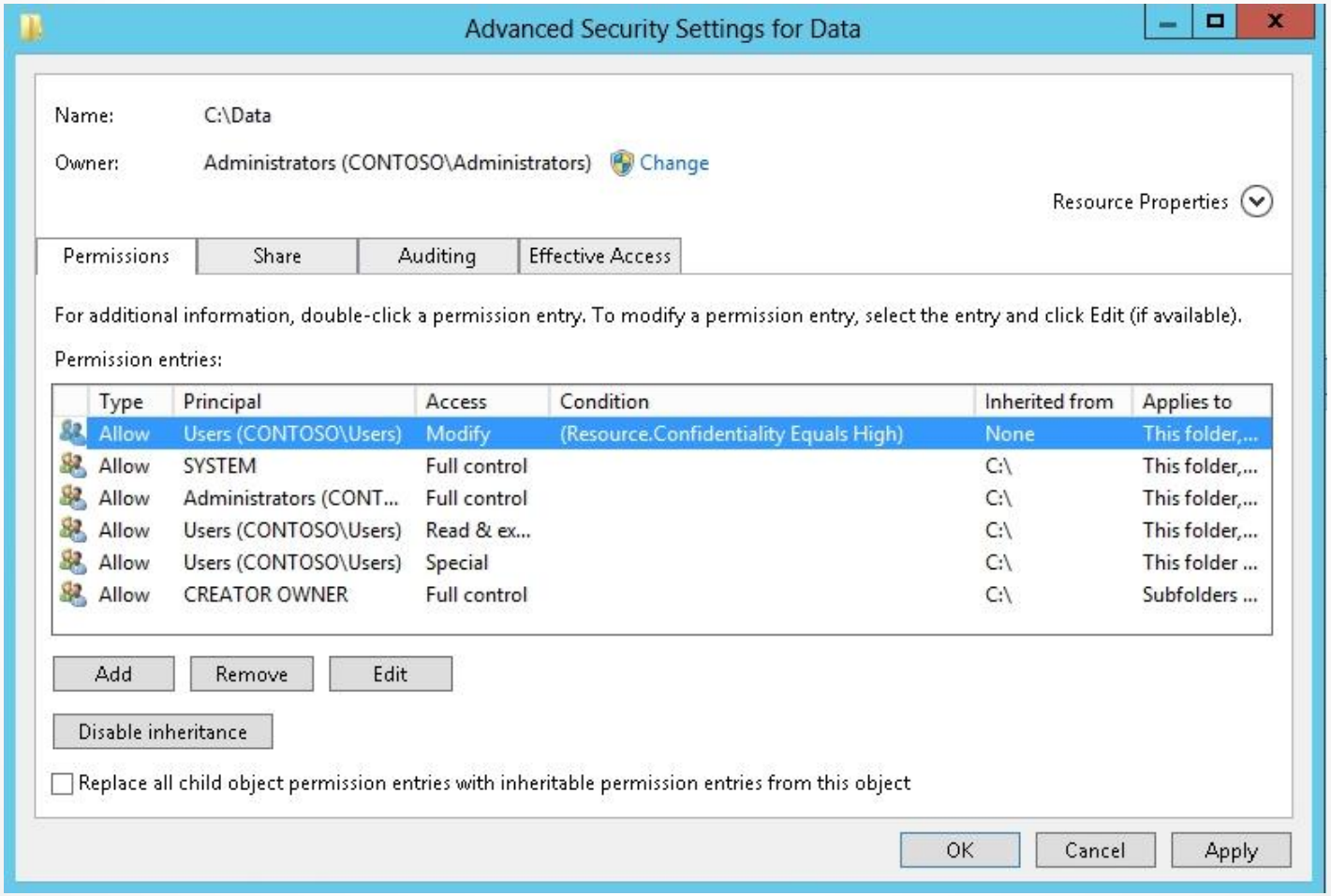
Central Access Policy

- Before you implement a Central Access Policy, you should:
  1. Identify the resources that you want to protect.
  2. Define the authorization policies.
  3. Translate the authorization policies into expressions.
  4. Break down the expressions that you have created and determine what claim types, resource properties, and device claims you must create to deploy the policies.

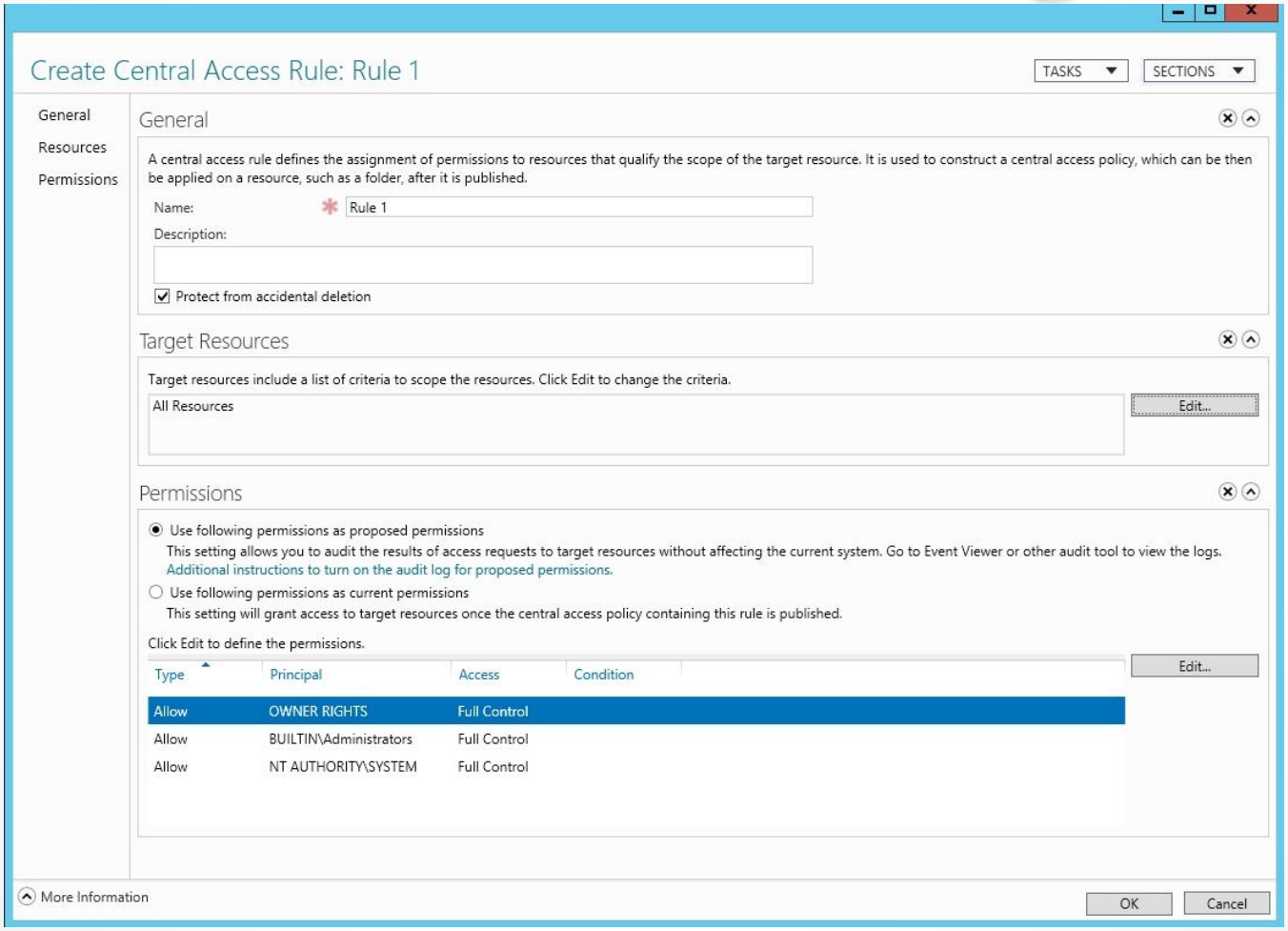
Configuring a Condition for an ACL



Viewing the Condition



Using the Create Central Access Rule Dialog Box



Policy Changes and Staging

- To test implementing DAC or making changes, Windows Server 2012 allows you to perform staging, which lets you verify the proposed policy updates before enforcing them.
- To use staging, deploy the proposed polices along with the enforced policies, but do not actually grant or deny permissions.
- Next, open the Event Viewer on the file server and search for Audit Event 4818 in the security logs.
  - Audit Event 4818 shows the difference between the access check that is using the staged policy and the access check that is using the enforced policy.
- Before staging appears, you need to first enable *Audit Central Access Policy Staging* using *Group Policies*.

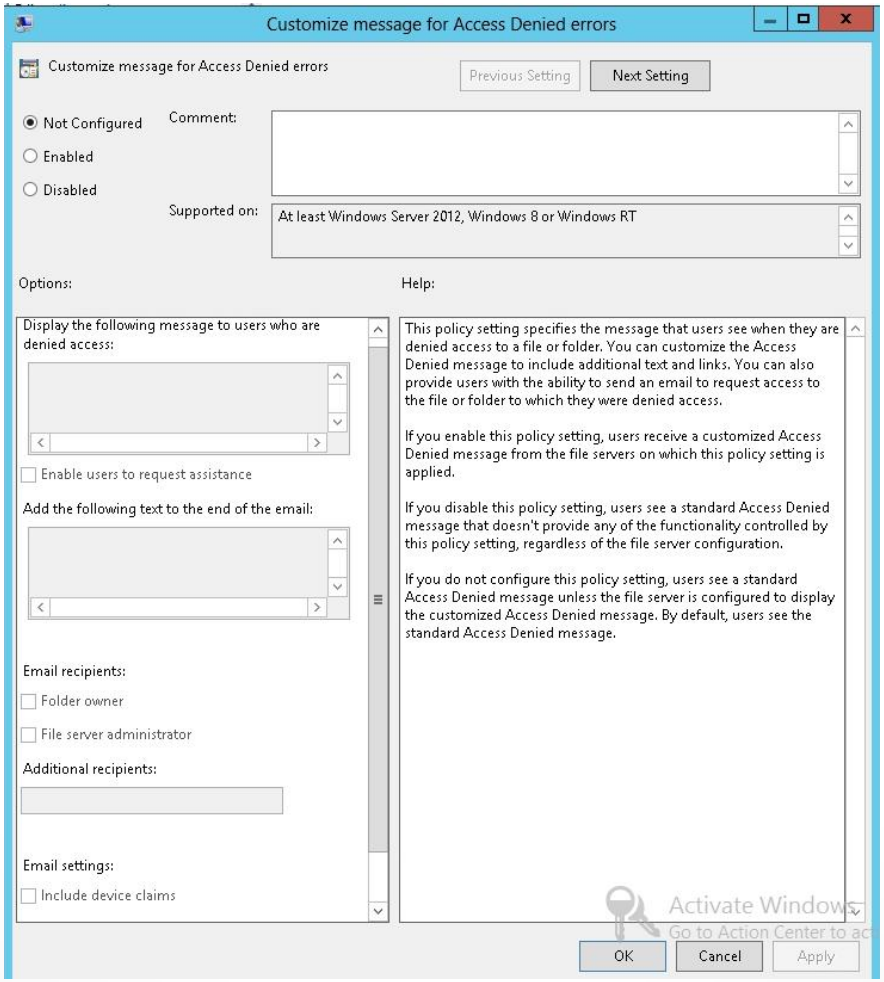
Expression-Based Audit Policies

- Windows Server 2012 has new advanced audit policies that implement more detailed and precise auditing on the file system, including the configuration of global-based audit policies and expression-based auditing.
- Expression-based audit policies let you specify what to audit based on defined properties or document attributes (e.g., a department or country).
- With ***Global Object Access Auditing*** you define computer-wide system access control lists (ACLs) for either the file system or registry instead of manually altering and maintaining System Access Control Lists (SACLs) on large sets of shared files or registry entry.
- In addition, the auditing is implicitly specified, which does not actually modify the files.

Access-Denied Remediation

- When users are denied access to a shared folder or file, Windows Server 2012 provides ***Access-Denied Assistance***, which helps users determine why they cannot access the folder or file and directs users to resolve the issue without calling the help desk.
- At this time, Access-Denied Remediation works only with Windows 8 and Windows Server 2012.

Access-Denied Remediation



Lesson Summary

- Dynamic Access Control (DAC), originally called *claim-based access control*, was introduced with Windows Server 2012. It is used for access management and provides an automatic mechanism to secure and control access to resources.
- Claims-based access control uses a trusted identity provider to provide authentication.
- The trusted identity provider issues a token to the user, which the user then presents to the application or service as proof of identity.

Lesson Summary

- After you enable support for DAC in Active Directory Domain Services (AD DS), you must next create and configure claims and resource property objects. To create and configure claims, you primarily use the Active Directory Administrative Center.
- When planning a DAC implementation, you should include file classification. Although file classification is not mandatory for DAC, it can enhance the automation of access control because it can be used to identify documents that you need to protect and classify them appropriately.

Lesson Summary

- Classification rules can be created and then scheduled to run on a regular basis so that files are automatically scanned and classified based on the content of the file.
- A Central Access Policy contains Central Access Rules that grant permissions to those objects for a defined group of resources.
- If you do not properly plan out DAC, when you first implement DAC or when you make changes, you can either grant more access than desired, or you can restrict access to the file too much, resulting in an increase of help desk calls.

Lesson Summary

- Global Object Access Auditing lets you define computer-wide system access control lists (ACLs) for either the file system or registry instead of manually altering and maintaining SACLs on large sets of shared files or registry entry. In addition, the auditing is implicitly specified, which does not actually modify the files.
- When a user is denied access to a shared file or folder, Windows Server 2012 provides Access-Denied Assistance, which helps users determine why they cannot access a file or folder and directs users to resolve the issue without calling the help desk.