

Lesson 6: Implementing Dynamic Access Control

MOAC 70-412: Configuring Advanced
Windows Server 2012 Services

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

The screenshot shows a Windows Group Policy Editor window titled "KDC support for claims, compound authentication and Kerberos armoring". The window has a standard Windows title bar with minimize, maximize, and close buttons. Below the title bar, there is a breadcrumb trail showing the current policy setting, and two buttons: "Previous Setting" and "Next Setting".

The main content area is divided into several sections:

- Configuration:** Three radio buttons are present: "Not Configured" (selected), "Enabled", and "Disabled". To the right of these buttons is a "Comment:" text box with a vertical scrollbar.
- Supported on:** A text box containing the text "At least Windows Server 2012, Windows 8 or Windows RT" with a vertical scrollbar.
- Options:** A section with a label "Options:" and a dropdown menu. The dropdown menu is currently empty.
- Help:** A section with a label "Help:" and a large text area containing detailed information about the policy setting.

The "Help:" section contains the following text:

This policy setting allows you to configure a domain controller to support claims and compound authentication for Dynamic Access Control and Kerberos armoring using Kerberos authentication.

If you enable this policy setting, client computers that support claims and compound authentication for Dynamic Access Control and are Kerberos armor-aware will use this feature for Kerberos authentication messages. This policy should be applied to all domain controllers to ensure consistent application of this policy in the domain.

If you disable or do not configure this policy setting, the domain controller does not support claims, compound authentication or armoring.

If you configure the "Not supported" option, the domain controller does not support claims, compound authentication or armoring which is the default behavior for domain controllers running Windows Server 2008 R2 or earlier operating systems.

At the bottom of the window, there are three buttons: "OK", "Cancel", and "Apply".

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

The screenshot shows the 'Create Claim Type' wizard for 'accountExpires'. The window title is 'Create Claim Type: accountExpires'. It features a 'TASKS' dropdown and a 'SECTIONS' dropdown. The main content is divided into two sections: 'Source Attribute' and 'Suggested Values'.

Source Attribute

A claim type is an assertion about the object with which it is associated. The assertion is based on an Active Directory attribute. It is used to define permissions when authoring central access rules.

Select an AD attribute to base this claim type on:

Filter

Display Name	Value Type	Belongs To (Cl...	ID
accountExpires	Integer	user, computer	Account-Expires
accountName...	Multi-Valued S...	user, computer	Account-Name-History
aCSPolicyName	String	user, computer	ACS-Policy-Name
adminCount	Integer	user, computer	Admin-Count
adminDescripti...	String	user, computer	Admin-Description
adminDisplayN...	String	user, computer	Admin-Display-Name
allowedAttribu...	Multi-Valued U...	user, computer	Allowed-Attributes
allowedAttribu...	Multi-Valued U...	user, computer	Allowed-Attributes-Effect...

Display name: * accountExpires
Description: Account-Expires

* Claims of this type can be issued for the following classes:
 User
 Computer

Set ID to a semantically identical claim type in a trusted forest:

Protect from accidental deletion

Suggested Values

When a user assigns a value to this claim type:

No values are suggested
 The following values are suggested:

Filter

Value	Display Name	Description
-------	--------------	-------------

Buttons: Add..., Edit..., Remove...

More Information, OK, Cancel

Confidentiality Resource Property

Confidentiality

TASKS SECTIONS

General

Suggested Values

Extensions

General

A resource property describes a characteristic of a resource, such as a file or a folder. It is used to define target resources and permissions when authoring central access rules. It is also used to classify resources.

Display name: * Confidentiality

Value type: Ordered List

Description:

The Confidentiality property specifies the level of confidentiality of the resource, and the potential impact of inadvertent access or disclosure.

ID: * Confidentiality_MS

Is used for authorization

Protect from accidental deletion

Suggested Values

The following values are suggested when a user assigns a value to this resource property:

Filter

Value	Display Name	Description
1000	Low	Mildly confide...
2000	Moderate	Moderately co...
3000	High	Highly confide...

Buttons: Add... Edit... Remove

Extensions

Security Attribute Editor

Group or user names:

- Everyone
- Authenticated Users
- SYSTEM

More Information

OK Cancel

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

The screenshot displays the File Server Resource Manager (FSRM) console. The left-hand navigation pane shows a tree view with 'Classification Management' expanded to 'Classification Properties'. The main pane shows a table of classification properties. The right-hand pane shows the 'Actions' menu for the selected 'Classification Properties' node, with options like 'Create Local...', 'Refresh', and 'Set Folder Ma...'. The table below contains the following data:

Name	Scope	Usage	Type	Possible Values
Access-Denied Assistanc...	Local	Folder Management	String	
Confidentiality	Global	Authorization, File Classification	Ordered List	High, Moderate, Low
Department	Global	Authorization, File Classification	Single Choice	Administration, Customer Se...
Folder Owner Email	Local	Folder Management	String	
Folder Usage	Local	Folder Management	Multiple Choic...	Application Files, Backup an...

Creating Classification Rules

Create Classification Rule

General | Scope | Classification | Evaluation Type

Classification method
Choose a method to assign a property to files:
Content Classifier
Searches for strings and regular expression patterns in files.

Property
Choose a property to assign to files:
Confidentiality
Specify a value:
High
Note: The assigned value might be combined with or overridden by more important values provided by other classification rules.

Parameters
This classification method requires additional configuration parameters.
Configure...

Help OK Cancel

Classification Parameters

Parameters

Specify the strings or regular expression patterns to look for in the file or file properties.

	Expression Type	Expression	Minimum Occurrences	Maximum Occurrences
	String	Highly Confidential	1	
*	Regular expression		1	

Insert
Remove

File name pattern (optional):

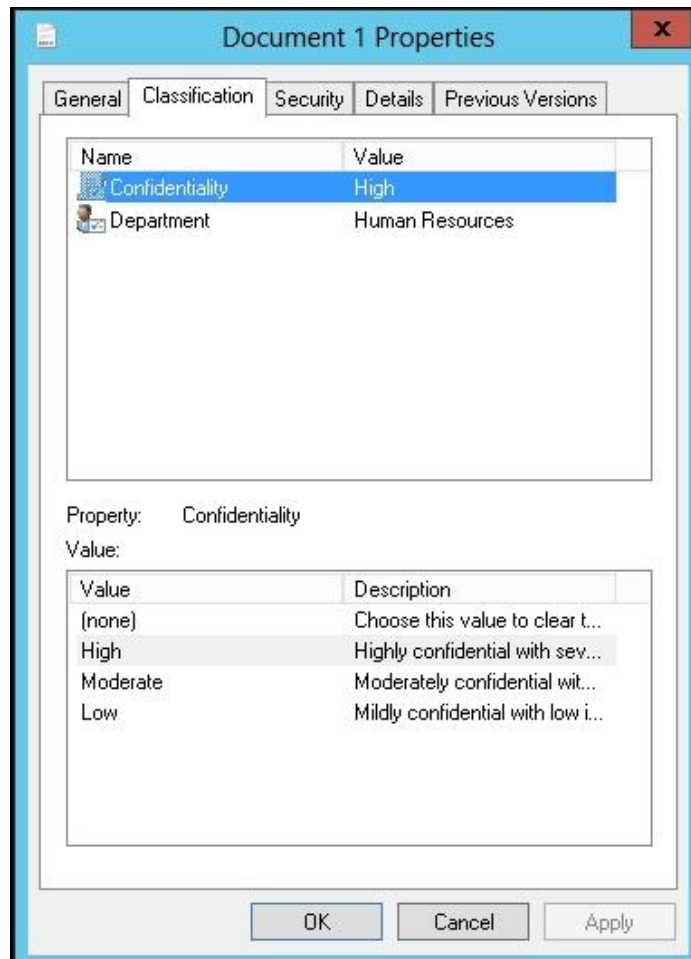
The classification rule assigns the property only if all expressions that you specify are found. Strings are not case sensitive unless you choose the StringCaseSensitive or RegularExpression types.

Complex regular expressions can reduce classification speed and consume large amounts of memory. See MSDN for more information about regular expressions.

To classify Microsoft Office files, before running the classification rule for the first time, we recommend installing the latest version of the [Microsoft Office Filter Pack](#).

OK Cancel

Viewing Document File Classification



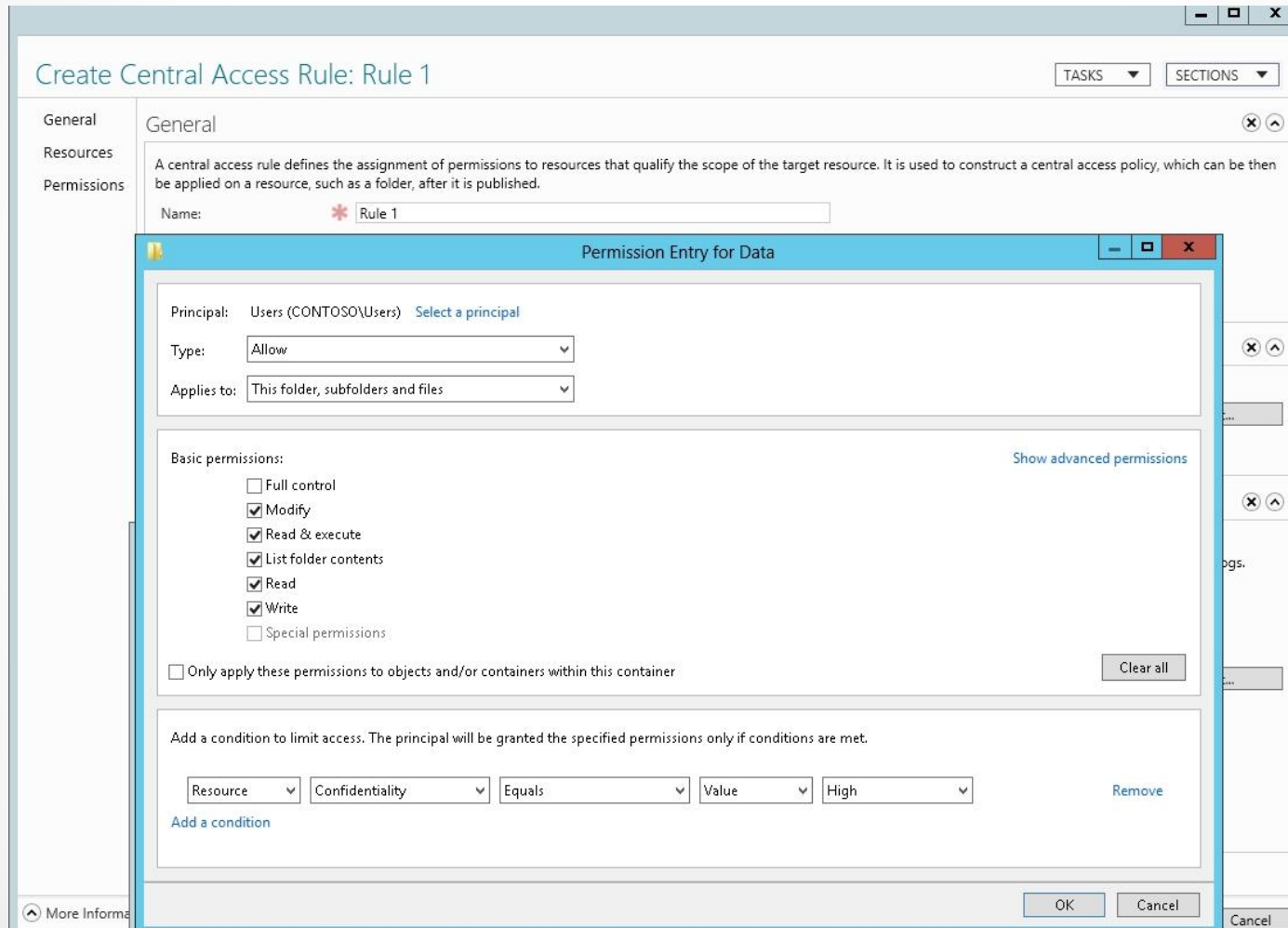
Central Access Policy

- 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

Advanced Security Settings for Data

Name: C:\Data

Owner: Administrators (CONTOSO\Administrators) Change

Resource Properties

Permissions | Share | Auditing | Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Condition	Inherited from	Applies to
Allow	Users (CONTOSO\Users)	Modify	(Resource.Confidentiality Equals High)	None	This folder,...
Allow	SYSTEM	Full control		C:\	This folder,...
Allow	Administrators (CONT...	Full control		C:\	This folder,...
Allow	Users (CONTOSO\Users)	Read & ex...		C:\	This folder,...
Allow	Users (CONTOSO\Users)	Special		C:\	This folder ...
Allow	CREATOR OWNER	Full control		C:\	Subfolders ...

Replace all child object permission entries with inheritable permission entries from this object

Using the Create Central Access Rule Dialog Box

Create Central Access Rule: Rule 1 [TASKS] [SECTIONS]

General

Resources
A central access rule defines the assignment of permissions to resources that qualify the scope of the target resource. It is used to construct a central access policy, which can be then be applied on a resource, such as a folder, after it is published.

Name: * Rule 1
Description:
 Protect from accidental deletion

Target Resources
Target resources include a list of criteria to scope the resources. Click Edit to change the criteria.
All Resources [Edit...]

Permissions

Use following permissions as proposed permissions
This setting allows you to audit the results of access requests to target resources without affecting the current system. Go to Event Viewer or other audit tool to view the logs.
[Additional instructions to turn on the audit log for proposed permissions.](#)

Use following permissions as current permissions
This setting will grant access to target resources once the central access policy containing this rule is published.

Click Edit to define the permissions.

Type	Principal	Access	Condition
Allow	OWNER RIGHTS	Full Control	
Allow	BUILTIN\Administrators	Full Control	
Allow	NT AUTHORITY\SYSTEM	Full Control	

[More Information] [OK] [Cancel]

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 policies 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

Customize message for Access Denied errors

Previous Setting Next Setting

Not Configured Comment:

Enabled

Disabled

Supported on: At least Windows Server 2012, Windows 8 or Windows RT

Options: Help:

Display the following message to users who are denied access:

Enable users to request assistance

Add the following text to the end of the email:

Email recipients:

Folder owner

File server administrator

Additional recipients:

Email settings:

Include device claims

This policy setting specifies the message that users see when they are denied access to a file or folder. You can customize the Access Denied message to include additional text and links. You can also provide users with the ability to send an email to request access to the file or folder to which they were denied access.

If you enable this policy setting, users receive a customized Access Denied message from the file servers on which this policy setting is applied.

If you disable this policy setting, users see a standard Access Denied message that doesn't provide any of the functionality controlled by this policy setting, regardless of the file server configuration.

If you do not configure this policy setting, users see a standard Access Denied message unless the file server is configured to display the customized Access Denied message. By default, users see the standard Access Denied message.

Activate Windows
Go to Action Center to activate Windows.

OK Cancel Apply

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.

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make backup copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.