Microsoft® Jump Start

M10: Implementing Dynamic Access Control

Rick Claus | Technical Evangelist | Microsoft
Ed Liberman | Technical Trainer | Train Signal

Microsoft

Jump Start Target Agenda | Day One

Day 1	Day 2
Module 1: Installing and Configuring Servers Based on Windows Server 2012	Module 7: Implementing Failover Clustering
Module 2: Monitoring and Maintaining Windows Server 2012	Module 8: Implementing Hyper-V
Module 3: Managing Windows Server 2012 by Using PowerShell 3.0	Module 9: Implementing Failover Clustering with Hyper-V
- MEAL BREAK -	- MEAL BREAK -
Module 4: Managing Storage for Windows Server 2012	Module 10: Implementing Dynamic Access Control
Module 5: Implementing Network Services	Module 11: Implementing Active Directory Domain Services
Module 6: Implementing Direct Access	Module 12: Implementing Active Directory Federation Services

Module Overview

- Overview of Dynamic Access Control
- Planning for a Dynamic Access Control Implementation
- Implementing And Configuring Dynamic Access Control

What Is Dynamic Access Control?

- Helps provide secure file server-based resources over all file server based resources
- Dynamic Access Control provides:
  - Data Identification
  - Access Control to files
  - Auditing of access to files
  - Optional RMS protection integration

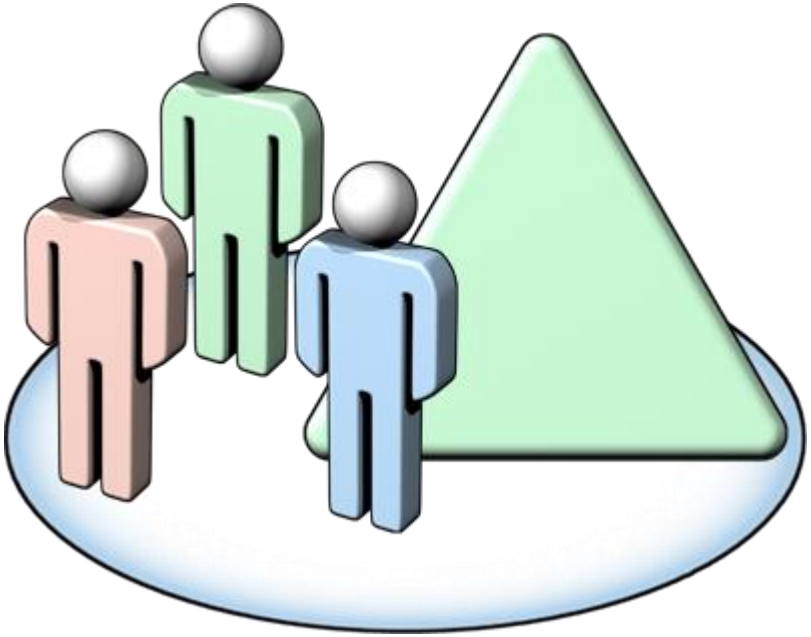
Foundation Technologies for Dynamic Access Control

- Network protocols
- DNS
- AD DS
- Kerberos
- Windows Security
- File Classifications
- Auditing

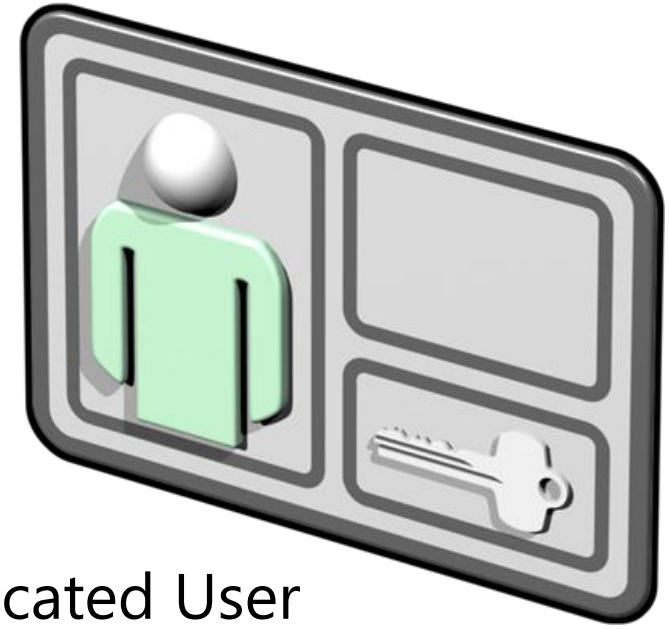
Dynamic Access Control Versus Alternative Technologies

- NTFS permissions and ACLs provide access control based on user's SID or group membership SID
- AD RMS provides deeper protection for documents by controlling how applications can use them
- Dynamic Access control provides access control based on claims – values of specific attributes

What Is an Identity?



Domain Group



Authenticated User

What Is a Claim?

- Claims are statements made by AD DS about specific user of computer object in AD DS
- AD DS in Windows Server 2012 supports:
  - User claims
  - Device claims

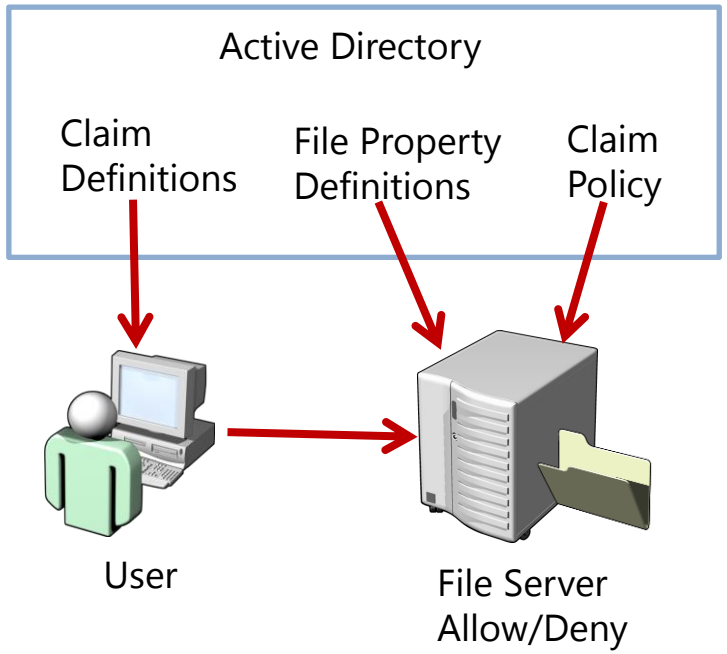
What is a Central Access Policy?

Central Access Policies consist of one or more central access rules.

Rules define conditions.

```
Allow Read|Write
User.MemberOf(IPSecurityGroup)
AND
(User.Department ANY_OF File.Department)
AND
Device.Managed = True
```

1. In AD DS, create claim and file property definitions, rules and create the central access policy
2. In Group Policy, send central access policies to the file servers
3. On file server, apply policies to the shared folder and identify information
4. On user computer, attempt access



Reasons for Implementing Dynamic Access Control

- Most common reasons for implementing Dynamic Access Control:
  - Inability to achieve desired results with NTFS
  - Requirement for access control based on attributes

Planning for Central Access Policy

- Identify business case
- Identify resources to be protected
- Understand business requirements
- Translate business requirements to conditional expressions
- Define claim types, resource properties, and rules

Planning File Classifications

- Identify classifications
- Determine method for classification
- Determine schedule
- Perform review

Planning File Access Auditing

- Track changes to user and machine attributes
- Get more information from user logon events
- Provide more information from object access auditing
- Track changes to Central Access Policies, Central Access Rules and Claims
- Track changes to file attributes

Planning Access Denied Assistance

- Message that users see
- Text of email that users use to request access
- Recipients for request access emails
- Target operating systems

Planning Policy Changes

- Dynamic Access Control enables you to stage changes
- Staging is implemented with Proposed Permissions
- Permissions are compared to current permissions
- Every attempt to access resource is logged in Security log of file server

Prerequisites for Implementing Dynamic Access Control

Dynamic Access Control is a technology specific to Windows Server 2012

To deploy Dynamic Access Control, you must have these technologies:

- Domain controller running on Windows Server 2012
- File server running Windows Server 2012
- Windows 8 desktop (for device claims)

Enabling Support in AD DS for Dynamic Access Control

- Dynamic Access Control support in AD DS is enabled by using Group Policy
- GPO that contain Dynamic Access Control Settings must be linked to the OU of the domain controller
- Dynamic Access Control setting is available in Computer Configuration\Policies\Administrative Templates\System\KDC node in GPO Object Editor
- Settings Support Dynamic Access Control can be configured as:
  - Do not support Dynamic Access Control and Kerberos armoring
  - Support Dynamic Access Control and Kerberos armoring
  - Always provide claims and FAST RFC behavior
  - Also fail unarmored authentication requests

Implementing Claims and Resource Property Objects

- Claims:
  - Created for users and computers
  - Have attributes as source
  - Created in AD AC or Windows PowerShell
- Resource Property Objects:
  - Created for resources
  - Have properties as a source
  - Create in AD AC or Windows PowerShell
- Both Claims and RPOs are used in conditional expressions

Implementing Central Access Rules and Policy

Central Access enables you manage and deploy consistent authorization throughout the enterprise

Central Access Policy main component is Central Access Rule

Central Access Rule specify:

- Targeted resource
- Permissions
- Conditions

Implementing File Access Auditing

- Global Object Access Auditing centrally manages and configures Windows to monitor every file and folder on the server
- Can be integrated with Dynamic Access Control
- New Audit policy categories in Group Policy

Implementing Access Denied Assistance

On File Server:

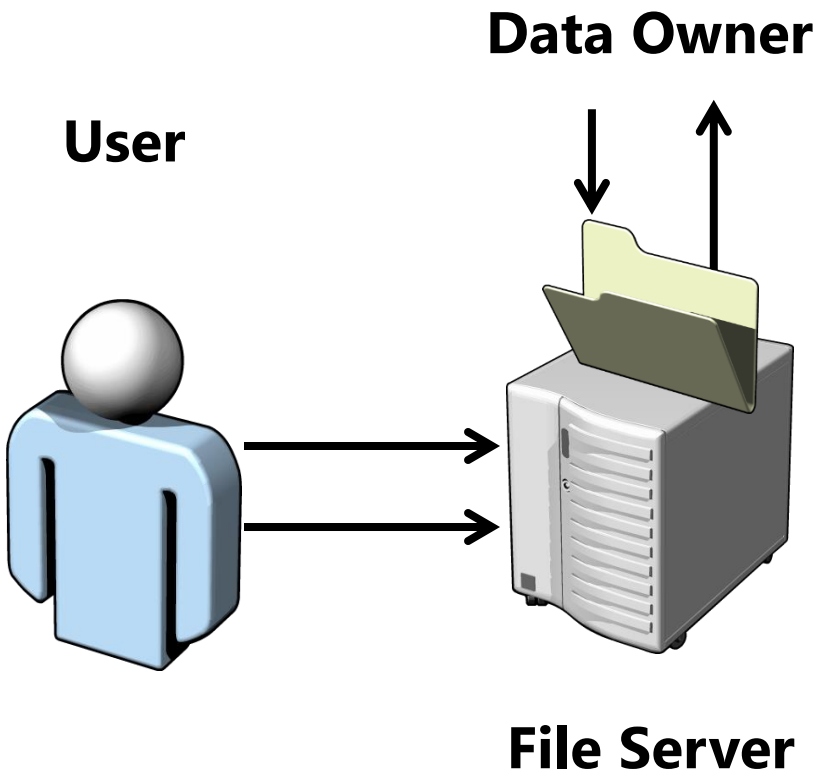
- Specify troubleshooting text for access denied
- Specify business owners email for Share/Folder

Access Time:

- User is denied access, sees troubleshooting text, and optionally device state troubleshooting
- User can request access via email

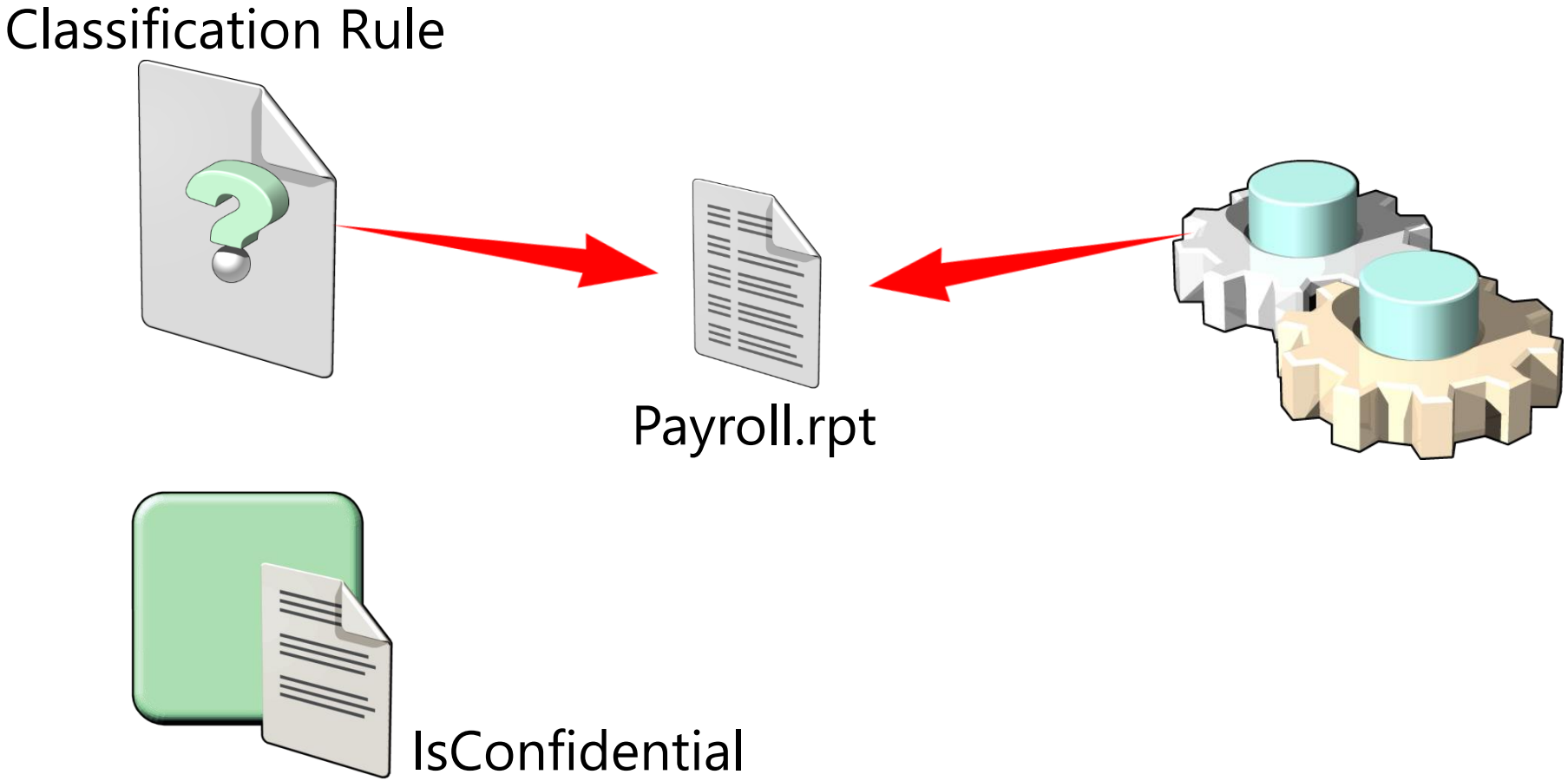
Data Owner/Helpdesk:

- Owner receives user's request
- User effective permissions UI to decide appropriate actions
- Can forward request to IT admin



Implementing File Classifications

Classification Management allows you create and assign classification properties to files using an automated mechanism



DEMO: Implementing Central Access Rules & Policies

In this demonstration, you will see how to create Central Access Rules and Policies.

Microsoft