**Dynamic Access Control**

Minimum OS: Windows Server 2012/Windows 8

Tested: Windows Server 2012 R2 File Server + 2016 Forest Level + Windows 10 1803

Components:

**Central Access Rule:** can contains user claims, device claims, user groups and recource properties. Multiple rules for a Central Access Policy

**Central Access Policy**

**Claims** are info about users, computers and resources published by a domain controller which are used in rules and policies to grant or restrict access to a resource dynamically.

**Expressions**

**Proposed permissions** help administrators see the impact of changes to access control before applying them

**Task related to Dynamic Access Control**

**In AD:**

Create claim definitions

Create file property definitions

Create central access policy

**In Group Policy:**

Set central access policies on file servers

**On file servers:**

Apply access policies to shared folders

Identify information

**Deploy a central access policy:**

We want to permit only O level users access to the O folder on FS01. We will use the title field for this.

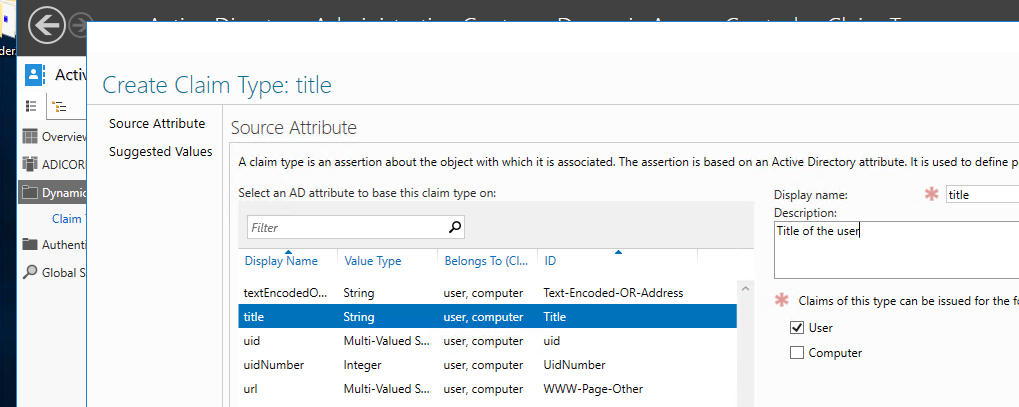
Steps:

**Enable Dynamic Access Control in domain:**

Create a GPO linked to Domain Controllers. Go to Computer Settings\Policies\Admin Templates\System\KDC and Enable KDC support for claims…; Set it to supported.

**Create a claim type for title:**

In AD Admin Center go to Dynamic Access Control and add a new claim type. Select title as the AD property to base the claim on and click OK.



**Create a resource property for the folder**

In AD Admin Center in Dynamic Access Control go to Resource Properties. Make a new Resource Property called Title as a Multi-valued text

**Create a central access rule:**

In AD Admin Center go to Central Access Rules and create a new Central Access Rule, give it a name like access to the O folder for upper management and edit the target resources. Add a condition that specifies this: (Resource.Title Any of {"Upper Management"}). Set the permissions desired to the group and add a condition that the user title has to be one of: CEO,CIO,CFO etc. Set also full control for admins

**Add rule to a central access policy:**

Create a Central Access Policy from AD Admin Center. Give it a name and add the access rule previously created.

**Use group policy to apply central policy to file servers:**

Create a GPO and link it to where the file server is located. Navigate to Computer\Policies\Windows Settings\Security Settings\File System\Central Access Policies. Add the desired policy.

Now go to Advanced Audit Policy… \Audit Policy. Select Object Access and enable the check boxes for File System and Central Access Policy Staging.

**Configure File Server**

Install file server resource manager. Run this command: Update-FSRMClassificationpropertyDefinition

On the O folder add Upper Management to Title in the Classification tab. Go to Security and Central Policy and add the configured policy

**Configure a user’s title property with CEO and test access**