Prepare AD for Microsoft Configuration Manager

Extend AD Schema

Now that the domain is functional, since this setup will leverage Microsoft Configuration Manager, there is some additional set up that needs to be done to prepare for installation. First, I want to extend the AD Schema which will add additional properties to the AD database that will be useful for managing devices. Simply run the script included with the Microsoft Configuration Manager setup as an account with the Schema Admin role. This is a very quick process and only needs to be done once per forest so if upgrading from a previous version or rebuilding in an existing domain not needed.

To extend the schema:

1. Log into the domain controller, or any other domain joined server, as a Schema Admin (the account used to create the domain has this by default).
2. Navigate to your MCM install source and go to .\SMSSETUP\BIN\X64.
3. Run extadsch.exe. A command prompt window will launch and almost immediately close itself.
4. Validate everything worked by reviewing c:\ExtADSch.log. The log file shows which attributes and classes were added and will ideally say "Successfully extended the Active Directory Schema". It also warns that there are additional configurations that are needed.

Create AD Accounts and Groups

Not everything is going to be done as a Domain Admin since we should use the principle of least privilege. I create a few accounts for the SQL Admin, Network Access, MCM Admin, Client Push, etc. In order to create an AD User there are many properties that can be set, but very few are actually required. Each account needs a Name, Logon Name, and Password. Optionally creating the account through AD Users & Computers or AD Administrative Center allows you set additional properties at creation but others need to be changed after created.

> One of the first things I always do when launching AD Users and Computers (dsa.msc) on a new system is go to View > Advanced Features. This enables a few additional tabs such as Object and Attribute Editor which are very valuable when troubleshooting account issues.

As this is one of the things that gets done all of the time and manual steps add room for error, I create the accounts and groups using PowerShell with Read-Host to set the password for the account. There are many other properties that can be set if this were a production environment. These can be explored with `Get-ADUser -Properties * | Get-Member`. For example, people like to use First and Last name (GivenName and Surname). These can also be set and/or added later with `Set-ADUser`.

```
# Create New User
New-ADUser `
    -Name "AccountName"`
    -SamAccountName "LogonName" `
    -AccountPassword (Read-Host -AsSecureString "Input User Password") `
    -ChangePasswordAtLogon $False `
    -Description "AccountDescription" `
    -Enabled $True

# Create New Group
New-ADGroup `
-Name "GroupName" `
-SamAccountName "GroupName" `
-Description "GroupDescription" `
-GroupScope "Global"

# Add Member to Group
Add-ADGroupMember -Identity "GroupName" -Members "sAMAccountName"
```

> By default, new User and Computer objects get added to the default Users and Computers container. The default location can be changed using the redirusr.exe and redircmp.exe utilities. Once the new OU has been created simply run the appropriate utility and point to the Distinguished Name (DN) of the desired OU. For example - `redircmp.exe OU=Computers,OU=Company,DC=Domain,DC=local`.

Configure System Management Container

MCM leverages a System Management Container in AD to store information used by the MCM servers to store and publish information such as boundaries and certificates. As the log for extending the schema indicated, this is not done automatically so needs to be created with ADSI Edit and permissions for the site servers granted by an account with Schema Admin.

1. Launch ADSI Edit as an account with Schema Admin
2. If this is the first time launching the tool, a connection needs to be established by selecting Action > Connect To. Leave the default options and click OK.
3. Expand Default naming context > DC=domain,DC=local > CN=System.

4. Right click CN=System and create a New Object.
5. Select container from the available classes and press Next.
6. Enter 'System Management' for the value and leave the rest of the default options to finish the wizard.
7. Right click the new CN=System Management container and open the properties.
8. On the Security Tab add the computer account for the site server(s) or a group with the servers. To select the Computer Account, you need to click Object Types and add Computers.
9. Select Full Control and click Advanced.
10. Edit or Double Click each server or the group and change Applies to: from 'This object' to 'This object and all descendant objects'.
11. Apply and click Ok to close out of the properties.

Revision #3
Created 30 December 2023 01:17:38 by Matthew B.
Updated 30 December 2023 03:13:21 by Matthew B.