1. Active Directory

|  |  |
| --- | --- |
| Computers used in  this Lab | SRV0001 |
| More information | Schema extensions for System Center Configuration Manager  <https://docs.microsoft.com/en-us/sccm/core/plan-design/network/schema-extensions> |
| Description | In this chapter, we will extend the active directory schema for SCCM. The Extension adds a new container and new attributes to the AD schema, allowing the SCCM environment to publish information to the AD and domain-joined machines to query these information. Extending the schema is not required task, however, it can simplify the deployment, configuration and management of a SCCM environment. |

* 1. Extending Active Directory Schema

|  |
| --- |
| Perform this task on the srv0001 virtual machine logged on as administrator |
| 01. Open Windows Explorer |
| 02. Navigate to C:\trainingfiles\Source\SCCMCB\Extract\SMSSETUP\BIN\X64 |
| 03. Execute extadsch.exe (run as administrator) |
| 03. Review the extending of the schema by examining the content of the C:\extadsch.log file  Note: If the schema has already been extended, the C:\extadsch.log will print lines with already exists information. |

This can also be achieved via PowerShell using the commands below:

#Extend Schema

Start-Process -Filepath ('C:\trainingfiles\Source\SCCMCB\Extract\SMSSETUP\BIN\X64\extadsch.exe') -wait

Start-Sleep 30

#Confirm Schema Extension

$schema = [DirectoryServices.ActiveDirectory.ActiveDirectorySchema]::GetCurrentSchema()

start-sleep 15

$schema.RefreshSchema()

$schema.FindClass("mSSMSSite")

* 1. Creating the System Management Container

|  |
| --- |
| Perform this task on the srv0001 virtual machine logged on as administrator |
| 01. Open Administrative Tools and then ADSI Edit. |
| 02. Right Click ADSI Edit and click Connect to… |
| 03. On Connection Settings, click Ok |
| 04. Expand Default naming context [SRV0001.classroom.intranet] -> DC=classroom,DC=intranet and then select CN=System |
| 05. right click CN=System and choose New -> Object |
| 06. Choose object class as Container, click Next |
| 07. In Value, type System Management and click Next |
| 08. Click Finish |
| 09. Back on the ADSI Edit screen, right click CN=System Management and choose Properties  Note: A refresh of the list of objects may be necessary |
| 10. Select the Security tab |
| 11.Click on the Advanced button |
| 12. On Advanced Security Settings for System Management, Click Add |
| 13. On Permission Entry for System Management, click Select a Principal |
| 14. On Select Users, Computers, Service Account, or Group, type SCCM Servers and click Check Names. Click OK |
| 15. On Permission Entry for System Management, select Allow Full Control under permissions, and This object and all descendant objects under Apply to.  Click Ok three (3) times. |

This can also be achieved via PowerShell using the commands below:

Import-Module ActiveDirectory

$root = (Get-ADRootDSE).defaultNamingContext

if (!([adsi]::Exists("LDAP://CN=System Management,CN=System,$root"))) {

$smcontainer = New-ADObject -Type Container -name "System Management" -Path "CN=System,$root" -Passthru

}

$acl = get-acl "ad:CN=System Management,CN=System,$root"

$objGroup = Get-ADGroup -filter {Name -eq "SCCM Servers"}

$All = [System.DirectoryServices.ActiveDirectorySecurityInheritance]::SelfAndChildren

$ace = new-object System.DirectoryServices.ActiveDirectoryAccessRule $objGroup.SID, "GenericAll", "Allow", $All

$acl.AddAccessRule($ace)

Set-acl -aclobject $acl "ad:CN=System Management,CN=System,$root"