1. Installation of SCCM Primary Site

|  |  |
| --- | --- |
| Computers used in  this Lab | ROUTER01  SRV0001  SRV0002 |
| More information | Supported configurations for System Center Configuration Manager  <https://docs.microsoft.com/en-us/sccm/core/plan-design/configs/supported-configurations>  List of Prerequisite Checks for System Center Configuration Manager  <https://docs.microsoft.com/en-us/sccm/core/servers/deploy/install/list-of-prerequisite-checks>  Install System Center Configuration Manager sites  <https://docs.microsoft.com/en-us/sccm/core/servers/deploy/install/installing-sites> |
| Description | In this chapter, we will install SCCM as well as validate if the installation has occurred correctly. We will also be installing the Configuration Manager Toolkit, a set of extra tools to help administration of the SCCM environment. |

* 1. Downloading SCCM Setup Files

|  |
| --- |
| Perform this task on the SRV0001 virtual machine logged on as administrator |
| 01. Execute setupdl.exe from C:\Trainingfiles\Source\SCCMCB\Extract\SMSSETUP\BIN\X64  Note: This step was already executed on section 4.4 and can be safely ignored |
| 02. Once the Configuration Manager Setup download is loaded, type C:\Trainingfiles\Source\SCCMCB\Redist and click download |
| 03. Once the download is completed, examine the \\srv0001\Trainingfiles\Source\SCCMCB\Redist folder |

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

Start-Process -Filepath ("\\srv0001\Trainingfiles\Source\SCCMCB\Extract\SMSSETUP\BIN\X64\SETUPDL.exe") -ArgumentList ("\\srv0001\Trainingfiles\Source\SCCMCB\Redist") -wait

* 1. Pre-requirements Check

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Open Command Prompt as administrator |
| 02. type \\srv0001\Trainingfiles\Source\SCCMCB\Extract\SMSSETUP\BIN\X64\prereqchk.exe /pri /sql SRV0002.classroom.intranet /sdk SRV0002.classroom.intranet and press enter |
| 03. Once the Installation prerequisite check completed, confirm that there are no errors. Click OK  Note: You should see the following warnings:   * WSUS on site Server * Verify site server permission to publish to active directory * SQL Server process memory allocation |
| 04. You can also review the errors and warnings by examining the content of the C:\ConfigMgrPrereq.log file |

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

Start-Process -Filepath ("\\srv0001\Trainingfiles\Source\SCCMCB\Extract\SMSSETUP\BIN\X64\prereqchk.exe") -ArgumentList ("/pri /sql SRV0002.classroom.intranet /sdk SRV0002.classroom.intranet") -wait

* 1. Creating Firewall Rules for SCCM Site Server Console Communication

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Open Windows Firewall with Advanced Security and click Inbound Rules |
| 02. Click New Rule |
| 03. On New Inbound Rule Wizard, select Port and click Next |
| 04. On Protocol and Ports select TCP and type 135 under specify local ports and click Next |
| 05. On Action, click Next |
| 06. On Profile, click Next |
| 07. On Name, type SCCM Console (TCP 135) Inbound and click Finish |

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

New-NetFirewallRule -DisplayName "SCCM Console (TCP 135) Inbound" -Action Allow -Direction Inbound -LocalPort 135 -Protocol TCP

* 1. Site Server Installation

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Execute splash.hta from \\srv0001\Trainingfiles\Source\SCCMCB\Extract |
| 02. Under Microsoft System Center Configuration Manager, click Install |
| 03. On Before You Begin, click Next |
| 04. On Available Setup Options, click Install a Configuration Manager Primary Site and click Next |
| 05. Select Install the evaluation edition of this product and click Next |
| 06. Under Product License Terms, select I accept for all products and click Next |
| 07. Under Prerequisite Downloads, select Use previously downloaded files and in path type \\srv0001\Trainingfiles\Source\SCCMCB\Redist and click Next |
| 08. Under server language selection, leave the default selection and click Next |
| 09. Under Client Language selection leave the default selection and click Next |
| 10. Under Site and Installation Settings, use the following information:   * Site Code: 001 * Site Name: Training Lab * Installation Folder: C:\ConfigMgr * Install the Configuration Manager Console: Checked   Click Next  Note: In production, SCCM should not be installed on the System Drive. It is only being installed here on the System Drive because it is a lab environment.  Note: A file called NO\_SMS\_ON\_DRIVE.SMS should be used to exclude SCCM from using a specific drive. Fore more information, refer to <https://technet.microsoft.com/en-us/library/bb632890.aspx>  Note: Site Code, Site Name and Installation Folder cannot be changed after the installation. |
| 12. Under Primary Site Installation select Install the primary site as a stand-alone site and click Next |
| 13. On the Configuration Manager question window, click Yes |
| 14. Under Database Information leave the default and click Next |
| 15. Under Database Information (Path to the SQL files) leave the default and click Next |
| 16. Under SMS Provider Settings, leave the default and click Next |
| 17. Under Client Computer Communication Settings select Configure the communication method on each site system role and click Next |
| 18. Under Site System Roles uncheck Install a management point and Install a distribution Point and click Next  Note: These site system roles are going to be installed later |
| 19. Under Diagnostic and Usage Data, click Next |
| 20. Under Service Connection Point Setup, leave the default and click Next |
| 21. Under Settings summary, review the settings and click Next |
| 22. The prerequisite check will validate the system. Once it is done, click Begin Install |
| 23. Once the installation is completed, click Close.  Note: Installation takes about half an hour. During the installation process, you can press the View Log button multiple times and examine the progress of the installation by reviewing the log file status. |
| 24. At the root of C-partition, multiple log files are created that tell the status of the installation:   * ConfigMgrAdminUISetup.log: SCCM console installation log * ConfigMgrPrereq.log: Prerequisites review log * ConfigMgrSetup.log: site server installation log * ConfigMgrSetupWizard.log: installation wizard log * smstsvc.log: installation program log (the errors in it can be ignored) |

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

$inifile = @"

[Identification]

Action=InstallPrimarySite

[Options]

ProductID=EVAL

SiteCode=001

SiteName=Training Lab

SMSInstallDir=c:\ConfigMgr

SDKServer=SRV0002.classroom.intranet

RoleCommunicationProtocol=HTTPorHTTPS

ClientsUsePKICertificate=0

PrerequisiteComp=1

PrerequisitePath=\\srv0001\Trainingfiles\Source\SCCMCB\Redist

MobileDeviceLanguage=0

AdminConsole=1

JoinCEIP=0

[SQLConfigOptions]

SQLServerName=SRV0002.classroom.intranet

SQLServerPort=1433

DatabaseName=CM\_001

SQLSSBPort=4022

SQLDataFilePath=C:\SQLServer\MSSQL14.MSSQLSERVER\MSSQL\DATA\

SQLLogFilePath=C:\SQLServer\MSSQL14.MSSQLSERVER\MSSQL\DATA\

[CloudConnectorOptions]

CloudConnector=1

CloudConnectorServer=SRV0002.classroom.intranet

UseProxy=0

ProxyName=

ProxyPort=

[SystemCenterOptions]

SysCenterId=Lzyga7QBe84u7mZvvIcFmoh9fWeQymoIYs0Cvqz4yhU=

[HierarchyExpansionOption]

"@

$inifile -replace "`n", "`r`n"| Out-File -FilePath "\\srv0001\TempFiles\installcmcb.ini"

Start-Process -Filepath ("\\srv0001\TrainingFiles\Source\SCCMCB\Extract\SMSSETUP\BIN\X64\setup.exe") -ArgumentList ('/script "\\srv0001\TempFiles\installcmcb.ini"') -wait

* 1. Installation Status

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Services console |
| 02. Services for SCCM are still named with SMS-prefix.  Note the existence of:   * SMS\_EXECUTIE * SMS\_SITE\_BACKUP * SMS\_SITE\_COMPONENT\_MANAGER * SMS\_SITE\_SQL\_BACKUP * SMS\_SITE\_VSS\_WRITER   Note: All services should be with Status running and the startup type as Automatic. The only exception is the SMS\_SITE\_BACKUP, that will set to Manual and will be started only when needed by SCCM |
| 03. Open Windows Explorer and navigate to C:\ConfigMgr. |
| 04. Open Local Users and groups and navigate to groups |
| 05. Multiple groups exist for SCCM, and they have a prefix of ConfigMgr or SMS.  Note: The following groups should be created:   * ConfigMgr\_CollectedFilesAccess * ConfigMgr\_DViewAccess * SMS Admins * SMS\_SiteSystemToSiteServerConnection\_MP\_<SITECODE> * SMS\_SiteSystemToSiteServerConnection\_SMSProv\_<SITECODE> * SMS\_SiteSystemToSiteServerConnection\_Stat\_<SITECODE> * SMS\_SiteToSiteConnection\_<SITECODE> |
| 06. On SRV0001 (Domain Controller), open ADSI Edit |
| 07. Expand Default naming context, DC=CLASSROOM,DC=intranet, CN=System, CN=System Management  Note: Existence of CN=SMS-Site-001 record from mSSMSSite class |

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

Get-CimInstance win32\_service | where-object {$\_.Name -in ("SMS\_EXECUTIVE","SMS\_SITE\_BACKUP","SMS\_SITE\_COMPONENT\_MANAGER","SMS\_SITE\_SQL\_BACKUP","SMS\_SITE\_VSS\_WRITER")} | select Name,StartMode,State,Status

$dn = New-Object System.DirectoryServices.DirectoryEntry

$dsLookFor = new-object System.DirectoryServices.DirectorySearcher($dn)

$dsLookFor.Filter = ("CN=SMS-SITE-001")

$dsLookFor.SearchScope = "subtree";

$dsLookFor.findOne()

Get-ChildItem -Path C:\ConfigMgr

$Groups = Gwmi win32\_group | where { $\_.Name -in ("ConfigMgr\_CollectedFilesAccess", "ConfigMgr\_DViewAccess", "SMS Admins", "SMS\_SiteSystemToSiteServerConnection\_MP\_001", "SMS\_SiteSystemToSiteServerConnection\_SMSProv\_001", "SMS\_SiteSystemToSiteServerConnection\_Stat\_001", "SMS\_SiteToSiteConnection\_001") } | select Name

if ($Groups.Count -ne 7) { Write-Host "Should be 7 Groups" } else { "Groups OK" }

* 1. Console Overview

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Configuration Manager Console. As the Management Console starts, it is good to notice that the new console is not MMC-based. |
| 02. Let’s look at few main points:   * Console uses new Ribbon-user interface (Originally introduced in Office 2007). * Bottom left corner has a list of main views:   + Assets and Compliance: here is information on machines and users as well as their settings   + Software Library: includes application management, software updates and operating systems deployment related tasks   + Monitoring: information on the status of SCCM and reporting related settings   + Administration: SCCM environment and configuration related settings |
| 03. Click Assets and Compliance. Here are the settings for:   * Users: Manage users and user groups for the hierarchy * Devices: Manage devices for the hierarchy * User Collections: Manage user collection for the hierarchy * Device Collections: Manage device collection for the hierarchy * User State Migration: Manage user state migration for when you deploy operating system * Asset Intelligence: Manage the Asset Intelligence catalog, import license files, and synchronize with System Center Online to reconcile software licenses. * Software Metering: Configure rules to monitor software application usage. * Compliance Settings: Manage configuration items and configuration baselines to assess and remediate the compliance of settings on devices. * Endpoint Protection: Manage Antimalware and Firewall policies. * All Corporate-owned Devices: Manage Corporate-owned Devices and Device Enrollment Profiles |
| 04. Click Devices. Note that ribbon bar functions update to relevant tasks. This view shows all devices know to SCCM. Right-click Devices and look at the available options. From the right side of the window pane, right-click SRV0002 and notice the options. Ribbon displays options from both left side selection e.g. Devices and right-side selection SRV0002. |
| 05. Click Software Library. There are 4 main levels:   * Application Management: Manage application deployments for users and devices, and configure global conditions for all applications in the hierarchy. * Software Updates: Manage software updates, software update groups, deployment packages for software updates, and automatic deployment rules * Operating Systems: Manage drivers, operating system images, upgrade packages, boot images, and task sequences to deploy operating systems and virtual hard disks. * Windows 10 Servicing: Manage Servicing for Windows 10 * Office 365 Client Management: Monitor amd Manage Office 365 clients (available in SCCM 1610 and later) |
| 06. Expand Application Management. There are 9 sublevels:   * Applications: Manage and deploy applications to users and devices, and configure rules to install and uninstall applications. * License Information for Store Apps: Manage Licensed Store Applications from Windows Store for Business and Apple’s VPP. * Packages: Manage packages that contain the files and instructions to deploy programs to users and devices. * Approval Requests: Manage application requests from users for Software Center applications that require approval. * Global Conditions: Manage global conditions for all applications in the site hierarchy. * App-V Virtual Environments: Virtual Environment * Windows Sideloading Key: Windows Sideloading Keys * Application Management Policies: Configure application management policies for the hierarchy. * App Configuration Policies: Manage app configuration policies. |
| 07. Expand Software Update. There are 4 sublevels:   * All Software Updates: Synchronize, configure, download, and deploy software updates. * Software Update Groups: Manage software updates as a group * Deployment Packages: Manage software update deployment packages * Automatic Deployment Rules: Manage rules that automatically identify, download, add to a software update group, and optionally deploy software updates that meet specific criteria. |
| 08. Expand Operating Systems. There are 7 sublevels:   * Drivers: Manage device drivers and device driver catalogs to deploy operating systems * Driver Packages: Manage device driver packages. * Operating System Images: Manage Windows image files for operating system deployment * Operating System Upgrade Packages: Manage operating system upgrade packages * Boot Images: Manage boot images for operating system deployment. * Task Sequences: Manage task sequences that automate steps or tasks on client computers. * Virtual Hard Disks: Manage Virtual Hard Disks. |
| 09. Expand Windows 10 Servicing. There are 2 sublevels:   * All Windows 10 Updates: Manage Updates for Windows 10. * Servicing Plans: Manage servicing plans for Windows 10. |
| 10. Click Monitoring. There are 13 levels here:   * Alerts: View and manage alerts. * Queries: View and manage Configuration Manager queries. * Reporting: View and manage reports and report subscriptions, and configure report options. * Site Hierarchy: View and manage the status of all sites in the hierarchy by using a hierarchy diagram or a geographical view. The geographical view of the hierarchy requires a web browser and access to the Internet. * System Status: View and manage site status, component status, conflicting records, and status message queries. * Deployments: View information about the status of deployed software. * Client Operations: View client operation details. * Client Status: View and configure options for client status. * Database Replication: View site-to-site link status. * Distribution Status: View content status, distribution point status, and distribution point configuration status. * Software Update Point Synchronization Status: View software update point synchronization status across the hierarchy. * Site Servicing Status: View the status of Configuration Manager updates you’ve installed in your hierarchy. * Security: View Endpoint Protection and Health Attestation details. (available in SCCM 1610 and later) * Upgrade Analytics: Analyze device compatibility with Windows 10 to facilitate upgrades. (available in SCCM 1610 and later) * Compliance Settings: View Compliance Settings details. (available in SCCM 1610 and later) * Endpoint Protection Status: View Endpoint Protection status details. It has been moved under security in SCCM 1610 and later.   Note: In my opinion, Reporting should have a separate workspace like in other System Center products. |
| 11. Click Administration. There are 8 main levels:   * Hierarchy Configuration: Manage boundaries, site-to-site communication, discovery methods, Active Directory forest and Exchange Server connection settings. * Cloud Services: Manage subscriptions to cloud services in your hierarchy. * Site Configuration: Manage servers and site system roles, components, site maintenance, and status configuration * Client Settings: Configure default and custom client settings. * Security: Manage administrative users, security roles, security scopes, certificates, and accounts that you configure in the Configuration Manager console. * Distribution Points: Manage individual distribution points and configuration properties, and view disk space capacity. * Distribution Point Groups: Manage distribution points as a group * Migration: Manage migration of data from sites in a Configuration Manager hierarchy to sites in this Configuration Manager hierarchy.   Note: Only the user that performed the installation will have permissions in SCCM by default. You need to remember to give other users permissions. |
| 12. Click on File->Connect via PowerShell |
| 13. On Do you want to run Software from this untrusted publisher? Type A and enter |
| 14. Type Get-Module -Name ConfigurationManager | select Version and confirm the version is 5.1802.1082.1800 |

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

#Step 12, 13 and 14 only

$ModulePath = $env:SMS\_ADMIN\_UI\_PATH

if ($ModulePath -eq $null) {

$ModulePath = (Get-ItemProperty -Path "Registry::HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment").SMS\_ADMIN\_UI\_PATH

}

$ModulePath = $ModulePath.Replace("bin\i386","bin\ConfigurationManager.psd1")

$Certificate = Get-AuthenticodeSignature -FilePath "$ModulePath" -ErrorAction SilentlyContinue

$CertStore = New-Object System.Security.Cryptography.X509Certificates.X509Store("TrustedPublisher")

$CertStore.Open([System.Security.Cryptography.X509Certificates.OpenFlags]::MaxAllowed)

$Certexist = ($CertStore.Certificates | where {$\_.thumbprint -eq $Certificate.SignerCertificate.Thumbprint}) -ne $null

if ($Certexist -eq $false) {

$CertStore.Add($Certificate.SignerCertificate)

}

$CertStore.Close()

import-module $ModulePath -force

Get-Module -Name ConfigurationManager | select Version

Remove-Module ConfigurationManager -Force

* 1. Validating Installation

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Configuration Manager Console and Click Monitoring. |
| 02. Under monitoring, expand System Status and click Component Status |
| 03. Search for SMS\_DATABASE\_NOTIFICATION\_MONITOR |
| 04. Right Click SMS\_DATABASE\_NOTIFICATION\_MONITOR, Show Messages and click All |
| 05. Under Status Messages: Set Viewing Period, click OK |
| 06. Verify the existence of Message ID 2420  Note: During the installation, these messages are normal, however, it should not occur after the installation |
| 07. Double click any 2420 messages to see its details. Once done, click Ok |
| 08. Search for SMS\_SITE\_SQL\_BACKUP |
| 09. Right Click SMS\_SITE\_SQL\_BACKUP, Show Messages and click All |
| 10. Under Status Messages: Set Viewing Period, click OK |
| 11. Verify the existence of Message ID 4959  Note: If this Message ID exist, there is a problem with the SQL Server Account SPN. Refer to <https://docs.microsoft.com/en-us/sccm/core/servers/manage/modify-your-infrastructure#bkmk_SPN> for more information |
| 12. Search for SMS\_SITE\_COMPONENT\_MANAGER |
| 13. Right Click SMS\_SITE\_COMPONENT\_MANAGER, Show Messages and click All |
| 14. Under Status Messages: Set Viewing Period, click OK |
| 15. Verify the existence of Message ID 1027 |
| 16. Double click the message to see its details. Once done, click Ok |
| 17. Search for SMS\_HIERARCHY\_MANAGER |
| 18. Right Click SMS\_HIERARCHY\_MANAGER, Show Messages and click All |
| 19. Under Status Messages: Set Viewing Period, click OK |
| 20. Verify the existence of Message ID 3306 |
| 21. Double click any of the messages to see its details. Once done, click Ok |
| 22. Verify the existence of Message ID 3323  Note: If this Message ID exist, the SCCM Server will accept HTTP or HTTPS connections. |
| 23. Double click any of the messages to see its details. Once done, click Ok |
| 24. Verify the existence of Message ID 3351  Note: If this Message ID exist, SCCM found there is an enabled firewall rule for TCP ports for SQL Server (TCP 1433) & SQL Server Service Broker (TCP 4022). |
| 25. Double click any of the messages to see its details. Once done, click Ok |
| 26. Verify the existence of Message ID 3353  Note: If this Message ID exist, confirm there is an enabled firewall rule for TCP ports for SQL Server (TCP 1433) & SQL Server Service Broker (TCP 4022). |
| 27. Double click any of the messages to see its details. Once done, click Ok |
| 28. Verify the existence of Message ID 4909  Note: If this Message ID exist, the container System Management does not exist. |
| 29. Double click any of the messages to see its details. Once done, click Ok |
| 30. Verify the existence of Message ID 4911  Note: If this Message ID exist, the container System Management have the correct permissions. |
| 31. Double click any of the messages to see its details. Once done, click Ok |
| 32. Verify the existence of Message ID 4912  Note: If this Message ID exist, there is already an object inside the container System Management the SCCM cannot update. |
| 33. Double click any of the messages to see its details. Once done, click Ok |
| 34. Verify the existence of Message ID 4913  Note: If this Message ID exist, there is a problem with the security of the System Management container. |
| 35. Double click any of the messages to see its details. Once done, click Ok |
| 36. Search for SMS\_REPLICATION\_CONFIGURATION\_MONITOR |
| 37. Right Click SMS\_REPLICATION\_CONFIGURATION\_MONITOR, Show Messages and click All |
| 38. Under Status Messages: Set Viewing Period, click OK |
| 39. Verify the existence of Message ID 4629 |
| 40. Double click any of the messages to see its details. Once done, click Ok |
| 41. Verify the existence of Message ID 620  Note: If found, check the performance of your SQL Server. |
| 42. Search for SMS\_DMP\_DOWNLOADER |
| 43. Right Click SMS\_DMP\_DOWNLOADER, Show Messages and click All |
| 44. Under Status Messages: Set Viewing Period, click OK |
| 45. Verify the existence of Message ID 4629 |
| 46. Double click any of the messages to see its details. Once done, click Ok |
| 47. Verify the existence of Message ID 9700  Note: If found check the network and/or internet. Also, this message is also normal to be seen during the installation. |
| 48. Verify the existence of Message ID 1104  Note: During the installation, this message is normal, however, it should not occur after the installation |
| 49. Search for SMS\_WINNT\_SERVER\_DISCOVERY\_AGENT |
| 50. Right Click SMS\_WINNT\_SERVER\_DISCOVERY\_AGENT, Show Messages and click All |
| 51. Under Status Messages: Set Viewing Period, click OK |
| 52. Verify the existence of Message ID 4202 |
| 53. Double click any of the messages to see its details. Note the number of system roles found, it should be 5. Once done, click Ok |
| 54. Click Administration. |
| 55. Expand Site Configuration and click Servers and Site System Roles  Note: Confirm that the Count of Roles for all listed servers match the number at message ID 4202 |

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

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_DATABASE\_NOTIFICATION\_MONITOR' and stmsg.MessageID = 2420 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Warning: Found SMS\_DATABASE\_NOTIFICATION\_MONITOR 2420 id's" -ForegroundColor Yellow

}

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_SITE\_SQL\_BACKUP' and stmsg.MessageID = 4959 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Error: Missing SQL SPN Information - https://technet.microsoft.com/en-us/library/hh427336.aspx#BKMK\_ManageSPNforDBSrv" -ForegroundColor Red

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_SITE\_COMPONENT\_MANAGER' and stmsg.MessageID = 1027 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Found SMS\_SITE\_COMPONENT\_MANAGER 2017 id's"

break

} else { Start-Sleep 10 }

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_HIERARCHY\_MANAGER' and stmsg.MessageID = 3306 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Found SMS\_HIERARCHY\_MANAGER 3306 id's"

break

} else { Start-Sleep 10 }

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsg.RecordID from SMS\_StatMsg stmsg where stmsg.Component = 'SMS\_HIERARCHY\_MANAGER' and stmsg.MessageID = 3323 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Found SMS\_HIERARCHY\_MANAGER 3323 id's"

break

} else { Start-Sleep 10 }

}

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_HIERARCHY\_MANAGER' and stmsg.MessageID = 3351 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Found SMS\_HIERARCHY\_MANAGER 3351 id's"

break

}

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_HIERARCHY\_MANAGER' and stmsg.MessageID = 3353 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Error: Found SMS\_HIERARCHY\_MANAGER 3353 id's" -ForegroundColor Red

break

}

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_HIERARCHY\_MANAGER' and stmsg.MessageID = 4909 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Error: Found SMS\_HIERARCHY\_MANAGER 4909 id's" -ForegroundColor Red

break

}

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_HIERARCHY\_MANAGER' and stmsg.MessageID = 4911 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Found SMS\_HIERARCHY\_MANAGER 4911 id's"

} else {

Write-Host "ERROR: Not Found SMS\_HIERARCHY\_MANAGER 4911 id's" -ForegroundColor Red

}

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_HIERARCHY\_MANAGER' and stmsg.MessageID = 4012 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Error: Found SMS\_HIERARCHY\_MANAGER 4012 id's" -ForegroundColor Red

break

}

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_HIERARCHY\_MANAGER' and stmsg.MessageID = 4913 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "ERROR: Found SMS\_HIERARCHY\_MANAGER 4913 id's" -ForegroundColor Red

}

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_REPLICATION\_CONFIGURATION\_MONITOR' and stmsg.MessageID = 4629 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Found SMS\_REPLICATION\_CONFIGURATION\_MONITOR 4629 id's"

}

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_REPLICATION\_CONFIGURATION\_MONITOR' and stmsg.MessageID = 620 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Error: Found SMS\_REPLICATION\_CONFIGURATION\_MONITOR 620 id's" -ForegroundColor Red

}

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_DMP\_DOWNLOADER' and stmsg.MessageID = 4629 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Found SMS\_DMP\_DOWNLOADER 4629 id's"

}

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsg.RecordID from SMS\_StatMsg stmsg where stmsg.Component = 'SMS\_DMP\_DOWNLOADER' and stmsg.MessageID = 9700 and stmsg.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Error: Found SMS\_DMP\_DOWNLOADER 9700 id's" -ForegroundColor Red

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_001") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_WINNT\_SERVER\_DISCOVERY\_AGENT' and stmsg.MessageID = 4202 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '001'"

if ($component -ne $null) {

Write-Host "Found SMS\_WINNT\_SERVER\_DISCOVERY\_AGENT 4202 id's"

break

} else { Start-Sleep 10 }

}

if ($component -is [Array]) {

$Total = $component[0].InsStrValue

} else {

$Total = $component.InsStrValue

}

$roles = gwmi -Namespace ("root\sms\site\_001") -query "select \* from SMS\_SCI\_SysResUse where FileType=2"

if ($roles.count -ne $total) {

Write-Host "ERROR: Found $($roles.count). expected $Total" -ForegroundColor Red

} else {

Write-Host "All $Total roles have been created"

}

* 1. Configuration Manager Toolkit

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Execute ConfigMgrTools.msi from \\srv0001\Trainingfiles\Source\SCCMCB-Toolkit |
| 02. On ConfigMgr 2012 Toolkit R2 click Next |
| 03. Under Software License Terms, click I accept the license agreement and click Next |
| 04. Under Select Components, click Next |
| 05. Under Setup Complete, click Finish |

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

Start-Process -Filepath ("msiexec.exe") -ArgumentList ('/i "\\srv0001\Trainingfiles\Source\SCCMCB-Toolkit\ConfigMgrTools.msi" /qb /l\*v c:\ConfigMgrTools.msi.log') -wait