1. Basic Site Configuration

|  |  |
| --- | --- |
| Computers used in  this Lab | ROUTER01  SRV0001  SRV0002 |
| More information | Prepare Windows Servers to support System Center Configuration Manager  <https://docs.microsoft.com/en-us/sccm/core/plan-design/network/prepare-windows-servers>  Deploy and manage content management infrastructure for System Center Configuration Manager  <https://docs.microsoft.com/en-us/sccm/core/servers/deploy/configure/deploy-and-manage-content>  Define site boundaries and boundary groups for System Center Configuration Manager  <https://docs.microsoft.com/en-us/sccm/core/servers/deploy/configure/define-site-boundaries-and-boundary-groups>  Run discovery for System Center Configuration Manager  <https://docs.microsoft.com/en-us/sccm/core/servers/deploy/configure/run-discovery>  Manage accounts to access content in System Center Configuration Manager  <https://docs.microsoft.com/en-us/sccm/core/plan-design/hierarchy/manage-accounts-to-access-content> |
| Firewall Rules | Many firewall rules are being created in this lab for the same set of TCP Ports (80 and 443). They are only being created multiple times to show what ports are required per Site Role. In a production environment, when co-hosting site roles, there is no need to create multiple rules for the same set of TCP Ports |
| Description | In this chapter, we will be performing the basic configuration of the SCCM. Installation and Configuration of the basic infrastructure for the SCCM to work, including Distribution Point, Management Point, FallBack Status Point, SQL Reporting Services Point, Boundaries, Boundary Group, Distribution Point Group, Network Access Account and Discovery.  **Note:** Distribution Point and Management Point can be installed during the SCCM Installation. It has not been done in this lab because we wanted to show you how to perform the installation at later stage, allowing you to be prepared to perform the same steps when installing in a remove server.  **Note:** With SCCM 1806 and usage of Enhanced HTTP site system (feature that is still in pre-release) Network Access Account for OS Deployment is not a requirement anymore. For more information refer to <https://docs.microsoft.com/en-us/sccm/core/plan-design/changes/whats-new-in-version-1806#network-access-account-not-required-for-some-scenarios> |

* 1. Installation of basic Roles (DP, MP, FSP, SRS)
     1. Distribution Point
        1. Creating Firewall Rules

|  |
| --- |
| 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 80 under specify local ports and click Next |
| 05. On Action, click Next |
| 06. On Profile, click Next |
| 07. On Name, type IIS Distribution Point (TCP 80) Inbound and click Finish |
| 08. Click New Rule |
| 09. On New Inbound Rule Wizard, select Port and click Next |
| 10. On Protocol and Ports select TCP and type 443 under specify local ports and click Next |
| 11. On Action, click Next |
| 12. On Profile, click Next |
| 13. On Name, type IIS Distribution Point (TCP 443) Inbound and click Finish |

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

New-NetFirewallRule -DisplayName "IIS Distribution Point (TCP 80) Inbound" -Action Allow -Direction Inbound -LocalPort 80 -Protocol TCP

New-NetFirewallRule -DisplayName "IIS Distribution Point (TCP 443) Inbound" -Action Allow -Direction Inbound -LocalPort 443 -Protocol TCP

* + - 1. Install Requirements

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Open Server Manager |
| 02. Click Manage and Add Roles and Features |
| 03. Before you begin, click Next |
| 04. Select Role-based or feature-based installation and click Next |
| 05. Select select a server from the server pool and select the server “SRV0002.classroom.intranet” and click Next |
| 06. Under select server roles, select Web Server (IIS) |
| 07. On Add Roles and Features Wizard, click Add Features and click Next |
| 08. Under Select Features, select Remote Differential Compression and click Next |
| 09. Under Web Server Role (IIS), click Next |
| 10. On Select role service, select:   * Security->Windows Authentication * Application Deployment->ISAP Extensions * Management Tools->IIS 6 Management Compatibility->IIS 6 Metabase Compatibility * Management Tools->IIS 6 Management Compatibility->IIS 6 WMI Compatibility * Management Tools->IIS Management Scripts and Tools   Click Next |
| 11. Under Confirm installation selections, click Install |
| 12. Once the installation is succeeded. Click Close |

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

@("RDC", "Web-Server", "Web-ISAPI-Ext", "Web-Metabase", "Web-Windows-Auth") | Get-WindowsFeature | Install-WindowsFeature

* + - 1. Installing Site System Role

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Configuration Manager Console and Click Administration. |
| 02. Expand Site Configuration and click Servers and Site System Roles |
| 03. Right click \\SRV0002.classroom.intranet and click Add Site System Roles |
| 04. On Add Site System Roles Wizard, General, click Next |
| 05. Under proxy, click Next |
| 06. Under Specify roles for this server, select Distribution Point and click Next |
| 07. Under Specify distribution point settings select “Install and configure IIS if required by Configuration Manager”. Leave the other default options and click Next |
| 08. Under Specify drive settings for this distribution point click Next |
| 09. Under Specify settings to install operating systems by using PXE boot click Next |
| 10. Under specify multicast settings for operating system deployment click Next |
| 11. Under specify the content validation settings, click Next |
| 12. Under specify the boundary groups associate with this site system click Next |
| 13. Under confirm the settings, click Next |
| 14. Under You have successfully completed the Add Site System Roles wizard with the following settings click close |
| 15. Click Monitoring |
| 16. Expand System Status and click Component Status |
| 17. Search for SMS\_DISTRIBUTION\_MANAGER |
| 18. Right Click SMS\_DISTRIBUTION\_MANAGER, Show Messages and click All |
| 19. Under Status Messages: Set Viewing Period, click OK |
| 20. Verify the existence of Message ID 2302  Note: When installing a new Distribution Point, it is normal see this message for the default SCCM Client packages (<SITECODE>00002, <SITECODE>00003 and <SITECODE>00007) and SCCM will retry the package again every 30 minutes. Once SCCM successfully distribute the package, you will see the Message ID 2301 |
| 21. Double click any 2302 messages to see its details. Once done, click Ok |
| 22. Verify the existence of Message ID 2399 |
| 23. Double click this message to see its details. Once done, click Ok |
| 24. Verify the existence of Message ID 2362  Note: This message will appear if the Install and Configure IIS checkbox was selected |
| 25. Double click this message to see its details. Once done, click Ok |
| 26. Verify the existence of Message ID 9501  Note: This message will appear if the PXE options was not selected |
| 27. Double click this message to see its details. Once done, click Ok |
| 28. Verify the existence of Message ID 9503  Note: This message will appear if the Multicast option was not selected |
| 29. Double click this message to see its details. Once done, click Ok |
| 30. You can also review the following logs:   * C:\ConfigMgr\Logs\DistMgr.log   Note: As the Install and Configure IIS checkbox was selected, the DISM command line will run |

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

$SiteCode = "001"

$servername = "SRV0002.classroom.intranet"

if ((Get-CMSiteSystemServer -SiteSystemServerName "$servername") -eq $null) { New-CMSiteSystemServer -SiteCode $SiteCode -UseSiteServerAccount -ServerName $servername }

Add-CMDistributionPoint -CertificateExpirationTimeUtc "$((Get-Date).AddYears(20).ToString())" -SiteSystemServerName $servername -SiteCode $siteCode -ClientConnectionType Intranet -InstallInternetServer

start-sleep 90

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_DISTRIBUTION\_MANAGER' and stmsg.MessageID = 2302 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "ERROR: Found SMS\_DISTRIBUTION\_MANAGER 2302 id's" -ForegroundColor Red

}

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_DISTRIBUTION\_MANAGER' and stmsg.MessageID = 2391 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "ERROR: Found SMS\_DISTRIBUTION\_MANAGER 2391 id's" -ForegroundColor Red

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_DISTRIBUTION\_MANAGER' and stmsg.MessageID = 2362 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_DISTRIBUTION\_MANAGER 2362 id's"

break

} else { Start-Sleep 10 }

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_DISTRIBUTION\_MANAGER' and stmsg.MessageID = 2399 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_DISTRIBUTION\_MANAGER 2399 id's"

break

} else { Start-Sleep 10 }

}

* + 1. Management Point
       1. Creating Firewall Rules

|  |
| --- |
| 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 80 under specify local ports and click Next |
| 05. On Action, click Next |
| 06. On Profile, click Next |
| 07. On Name, type IIS Management Point (TCP 80) Inbound and click Finish |
| 08. Click New Rule |
| 09. On New Inbound Rule Wizard, select Port and click Next |
| 10. On Protocol and Ports select TCP and type 443 under specify local ports and click Next |
| 11. On Action, click Next |
| 12. On Profile, click Next |
| 13. On Name, type IIS Management Point (TCP 443) Inbound and click Finish |
| 14. Click New Rule |
| 15. On New Inbound Rule Wizard, select Port and click Next |
| 16. On Protocol and Ports select TCP and type 10123 under specify local ports and click Next |
| 17. On Action, click Next |
| 18. On Profile, click Next |
| 19. On Name, type IIS Client Notification (TCP 10123) Inbound and click Finish |

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

New-NetFirewallRule -DisplayName "IIS Management Point (TCP 80) Inbound" -Action Allow -Direction Inbound -LocalPort 80 -Protocol TCP

New-NetFirewallRule -DisplayName "IIS Management Point (TCP 443) Inbound" -Action Allow -Direction Inbound -LocalPort 443 -Protocol TCP

New-NetFirewallRule -DisplayName "IIS Client Notification (TCP 10123) Inbound" -Action Allow -Direction Inbound -LocalPort 10123 -Protocol TCP

* + - 1. Install Requirements

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Open Server Manager |
| 02. Click Manage and Add Roles and Features |
| 03. Before you begin, click Next |
| 04. Select Role-based or feature-based installation and click Next |
| 05. Select select a server from the server pool and select the server “SRV0002.classroom.intranet” and click Next |
| 06. Under select server roles, select Web Server (IIS) |
| 07. On Add Roles and Features Wizard, click Add Features and click Next |
| 08. Under Select Features, select Background Intelligent Transfer Service (BITS)->IIS Server Extension |
| 09. On Add Roles and Features Wizard, click Add Features and click Next |
| 10. Under Web Server Role (IIS), click Next |
| 11. On Select role service, select:   * Security->Windows Authentication * Application Deployment->ISAP Extensions * Management Tools->IIS 6 Management Compatibility->IIS 6 Metabase Compatibility * Management Tools->IIS 6 Management Compatibility->IIS 6 WMI Compatibility * Management Tools->IIS Management Scripts and Tools.   Click Next |
| 12. Under Confirm installation selections, click Install |
| 13. Once the installation is succeeded. Click Close |

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

@("Web-Server", "Web-ISAPI-Ext", "Web-Metabase", "Web-Windows-Auth", "BITS-IIS-Ext") | Get-WindowsFeature | Install-WindowsFeature

* + - 1. Installing Site System Role

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Configuration Manager Console and Click Administration. |
| 02. Expand Site Configuration and click Servers and Site System Roles |
| 03. Right click \\SRV0002.classroom.intranet and click Add Site System Roles |
| 04. On Add Site System Roles Wizard, General, click Next |
| 05. Under proxy, click Next |
| 06. Under Specify roles for this server, select Management Point and click Next |
| 07. Under Specify management point settings, click Next |
| 08. Under specify management point database settings click Next |
| 09. Under confirm the settings, click Next |
| 10. Under You have successfully completed the Add Site System Roles Wizard with the following settings click Close |
| 11. Click Monitoring |
| 12. Expand System Status and click Component Status |
| 13. Search for SMS\_MP\_CONTROL\_MANAGER |
| 14. Right Click SMS\_MP\_CONTROL\_MANAGER, Show Messages and click All |
| 15. Under Status Messages: Set Viewing Period, click OK |
| 16. Verify the existence of Message ID 1013, 1014 and 1015 |
| 17. Double click any of the 1013, 1014 and 1015 messages to see its details. Once done, click Ok |
| 18. Verify the existence of Message ID 500 |
| 19. Double click on the messages to see its details. Once done, click Ok |
| 20. Verify the existence of Message ID 5460. |
| 21. Double click on the message to see its details. Once done, click Ok |
| 22. Open Internet Explorer and navigate to http://SRV0002.classroom.intranet/sms\_mp/.sms\_aut?mplist |
| 23. Navigate to http://SRV0002.classroom.intranet/sms\_mp/.sms\_aut?mpcert |
| 24. You can also review the following logs:   * C:\ConfigMgr\Logs\MPSetup.log: Records the installation wrapper process. * C:\ConfigMgr\Logs\mpMSI.log: Records details of installation. * C:\ConfigMgr\Logs\mpcontrol.log: Records the registration of the management point with WINS. Records the availability of the management point every 10 minutes. * C:\ConfigMgr\Logs\mpfdm.log: Records the actions of the management point component that moves client files to the corresponding INBOXES folder on the site server. |

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

$SiteCode = "001"

$servername = "SRV0002.classroom.intranet"

if ((Get-CMSiteSystemServer -SiteSystemServerName "$servername") -eq $null) { New-CMSiteSystemServer -SiteCode $SiteCode -UseSiteServerAccount -ServerName $servername }

Add-CMManagementPoint -SiteSystemServerName $servername -SiteCode $siteCode

start-sleep 90

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_MP\_CONTROL\_MANAGER' and stmsg.MessageID = 1013 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_MP\_CONTROL\_MANAGER 1013 id's"

break

} else { Start-Sleep 10 }

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsg.\* from SMS\_StatMsg stmsg where stmsg.Component = 'SMS\_MP\_CONTROL\_MANAGER' and stmsg.MessageID = 1014 and stmsg.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_MP\_CONTROL\_MANAGER 1014 id's"

break

} else { Start-Sleep 10 }

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsg.\* from SMS\_StatMsg stmsg where stmsg.Component = 'SMS\_MP\_CONTROL\_MANAGER' and stmsg.MessageID = 1015 and stmsg.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_MP\_CONTROL\_MANAGER 1015 id's"

break

} else { Start-Sleep 10 }

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsg.\* from SMS\_StatMsg stmsg where stmsg.Component = 'SMS\_MP\_CONTROL\_MANAGER' and stmsg.MessageID = 500 and stmsg.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_MP\_CONTROL\_MANAGER 500 id's"

break

} else { Start-Sleep 10 }

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsg.\* from SMS\_StatMsg stmsg where stmsg.Component = 'SMS\_MP\_CONTROL\_MANAGER' and stmsg.MessageID = 5460 and stmsg.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_MP\_CONTROL\_MANAGER 5460 id's"

break

} else { Start-Sleep 10 }

}

$web = New-Object -ComObject msxml2.xmlhttp

$url = "http://$($servername):80/sms\_mp/.sms\_aut?mplist"

try {

$web.open('GET', $url, $false)

$web.send()

Write-host "MPList HTTP Return $($web.status)"

} catch {

Write-host "MPList ERROR: $($\_)" -ForegroundColor Red

}

$web = New-Object -ComObject msxml2.xmlhttp

$url = "http://$($servername):80/sms\_mp/.sms\_aut?mpcert"

try {

$web.open('GET', $url, $false)

$web.send()

Write-host "MPCert HTTP Return $($web.status)"

} catch {

Write-host "MPCert ERROR: $($\_)" -ForegroundColor Red

}

* + 1. Fallback Status Point
       1. Creating Firewall Rules

|  |
| --- |
| 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 80 under specify local ports and click Next |
| 05. On Action, click Next |
| 06. On Profile, click Next |
| 07. On Name, type IIS Fallback Status Point (TCP 80) Inbound and click Finish |

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

New-NetFirewallRule -DisplayName "IIS Fallback Status Point (TCP 80) Inbound" -Action Allow -Direction Inbound -LocalPort 80 -Protocol TCP

* + - 1. Install Fallback Requirements

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Open Server Manager |
| 02. Click Manage and Add Roles and Features |
| 03. Before you begin, click Next |
| 04. Select Role-based or feature-based installation and click Next |
| 05. Select select a server from the server pool and select the server “SRV0002.classroom.intranet” and click Next |
| 06. Under select server roles, select Web Server (IIS) |
| 07. On Add Roles and Features Wizard, click Add Features |
| 08. Under Select Features, click Next |
| 09. On Add Roles and Features Wizard, click Add Features and click Next |
| 10. Under Web Server Role (IIS), click Next |
| 11. On Select role service, select:   * Management Tools->IIS 6 Management Compatibility->IIS 6 Metabase Compatibility * Management Tools->IIS 6 Management Compatibility->IIS 6 WMI Compatibility * Management Tools->IIS Management Scripts and Tools.   Click Next |
| 12. Under Confirm installation selections, click Install |
| 13. Once the installation is succeeded. Click Close |

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

@("Web-Server", "Web-Metabase") | Get-WindowsFeature | Install-WindowsFeature

* + - 1. Installing Site System Role

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Configuration Manager Console and Click Administration. |
| 02. Expand Site Configuration and click Servers and Site System Roles |
| 03. Right click \\SRV0002.classroom.intranet and click Add Site System Roles |
| 04. On Add Site System Roles Wizard, General, click Next |
| 05. Under proxy, click Next |
| 06. Under Specify roles for this server, select Fallback Status Point and click Next |
| 07. Under Specify Fallback Status Point settings leave the default settings and click Next |
| 08. Under confirm the settings, click Next |
| 09. Under You have successfully completed the Add Site System Roles wizard with the following settings click close |
| 10. Click Monitoring |
| 11. Expand System Status and click Component Status |
| 12. Search for SMS\_FALLBACK\_STATUS\_POINT |
| 13. Right Click SMS\_FALLBACK\_STATUS\_POINT, Show Messages and click All |
| 14. Under Status Messages: Set Viewing Period, click OK |
| 15. Verify the existence of Message ID 1013, 1014 and 1015 |
| 16. Double click any of the 1013, 1014 and 1015 messages to see its details. Once done, click Ok |
| 17. Verify the existence of Message ID 500 |
| 18. Double click on the messages to see its details. Once done, click Ok |
| 19. You can also review the following logs:   * C:\ConfigMgr\Logs\fspMSI.log: Records messages generated by the installation. * C:\ConfigMgr\Logs\SMSFSPSetup.log: Records messages generated by the installation. * C:\ConfigMgr\Logs\FspIsapi.log: Records details about communications to the fallback status point from mobile device legacy clients and client computers. |

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

$SiteCode = "001"

$servername = "SRV0002.classroom.intranet"

if ((Get-CMSiteSystemServer -SiteSystemServerName "$servername") -eq $null) { New-CMSiteSystemServer -SiteCode $SiteCode -UseSiteServerAccount -ServerName $servername }

Add-CMFallbackStatusPoint -SiteSystemServerName $servername -SiteCode $siteCode

start-sleep 90

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_FALLBACK\_STATUS\_POINT' and stmsg.MessageID = 1013 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_FALLBACK\_STATUS\_POINT 1013 id's"

break

} else { Start-Sleep 10 }

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsg.\* from SMS\_StatMsg stmsg where stmsg.Component = 'SMS\_FALLBACK\_STATUS\_POINT' and stmsg.MessageID = 1014 and stmsg.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_FALLBACK\_STATUS\_POINT 1014 id's"

break

} else { Start-Sleep 10 }

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsg.\* from SMS\_StatMsg stmsg where stmsg.Component = 'SMS\_FALLBACK\_STATUS\_POINT' and stmsg.MessageID = 1015 and stmsg.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_FALLBACK\_STATUS\_POINT 1015 id's"

break

} else { Start-Sleep 10 }

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsg.\* from SMS\_StatMsg stmsg where stmsg.Component = 'SMS\_FALLBACK\_STATUS\_POINT' and stmsg.MessageID = 500 and stmsg.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_FALLBACK\_STATUS\_POINT 500 id's"

break

} else { Start-Sleep 10 }

}

* + 1. Reporting Services Point
       1. Creating Firewall Rules

|  |
| --- |
| 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 80 under specify local ports and click Next |
| 05. On Action, click Next |
| 06. On Profile, click Next |
| 07. On Name, type SQL Server Reporting Services (TCP 80) Inbound and click Finish |

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

New-NetFirewallRule -DisplayName "SQL Server Reporting Services (TCP 80) Inbound" -Action Allow -Direction Inbound -LocalPort 80 -Protocol TCP

* + - 1. Installing Site System Role

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Configuration Manager Console and Click Administration. |
| 02. Expand Site Configuration and click Servers and Site System Roles |
| 03. Right click \\SRV0002.classroom.intranet and click Add Site System Roles |
| 04. On Add Site System Roles Wizard, General, click Next |
| 05. Under proxy, click Next |
| 06. Under Specify roles for this server, select Reporting Services Point and click Next |
| 07. Under Specify Reporting Services Point settings, click Verify and under User name click Set New Account |
| 08. Under Windows User Account, type the following;   * User name: CLASSROOM\svc\_ssrsea * Password: Pa$$w0rd * Confirm password: Pa$$w0rd   Click Ok |
| 09. Once back to the Add Site System Roles Wizard, click Next |
| 10. Under confirm the settings, click Next |
| 11. Under You have successfully completed the Add Site System Roles wizard with the following settings click close |
| 12. Click Monitoring |
| 13. Expand System Status and click Component Status |
| 14. Search for SMS\_SRS\_REPORTING\_POINT |
| 15. Right Click SMS\_SRS\_REPORTING\_POINT, Show Messages and click All |
| 16. Under Status Messages: Set Viewing Period, click OK |
| 17. Verify the existence of Message ID 1013, 1014 and 1015 |
| 18. Double click any of the 1013, 1014 and 1015 messages to see its details. Once done, click Ok |
| 19. Verify the existence of Message ID 500 |
| 20. Double click on the messages to see its details. Once done, click Ok |
| 21. Monitor C:\ConfigMgr\Logs\srsrp.log for the status of the reports importation.  Note: Once the Reporting Services Point is installed, SCCM will import reports into the SQL Server Reporting Service. As there are few hundred reports, this process can take some time. |
| 22. Return to Configuration Manager console, monitoring workspace, expand Reporting and click Reports  Note: You should see all reports being populated. Once the process of importing the reports are done, there should be over 450 reports. |
| 23. You can also review the following logs:   * C:\ConfigMgr\Logs\srsrpsetup.log: Records messages generated by the installation. * C:\ConfigMgr\Logs\srsrpMSI.log: Records messages generated by the installation. * C:\ConfigMgr\Logs\srsrp.log: Records information about the activity and status of the reporting services point. |

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

$SiteCode = "001"

$servername = "SRV0002.classroom.intranet"

$sqlServerInstance = 'SSRS'

$Secure = 'Pa$$w0rd'| ConvertTo-SecureString -AsPlainText -Force

$account = "CLASSROOM\svc\_ssrsea"

New-CMAccount -Name "$account" -Password $Secure -SiteCode "$SiteCode"

if ((Get-CMSiteSystemServer -SiteSystemServerName "$servername") -eq $null) { New-CMSiteSystemServer -SiteCode $SiteCode -UseSiteServerAccount -ServerName $servername }

Add-CMReportingServicePoint -ReportServerInstance $sqlServerInstance -SiteSystemServerName "$servername" -UserName "$account" -DatabaseName "CM\_$SiteCode" -DatabaseServerName "$servername" -FolderName "ConfigMgr\_$SiteCode" -SiteCode "$SiteCode"

start-sleep 90

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsgin.InsStrValue from SMS\_StatMsg stmsg inner join SMS\_StatMsgInsStrings stmsgin on stmsg.RecordID = stmsgin.RecordID where stmsg.Component = 'SMS\_SRS\_REPORTING\_POINT' and stmsg.MessageID = 1013 and stmsgin.InsStrIndex = 0 and stmsgin.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_SRS\_REPORTING\_POINT 1013 id's"

break

} else { Start-Sleep 10 }

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsg.\* from SMS\_StatMsg stmsg where stmsg.Component = 'SMS\_SRS\_REPORTING\_POINT' and stmsg.MessageID = 1014 and stmsg.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_SRS\_REPORTING\_POINT 1014 id's"

break

} else { Start-Sleep 10 }

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsg.\* from SMS\_StatMsg stmsg where stmsg.Component = 'SMS\_SRS\_REPORTING\_POINT' and stmsg.MessageID = 1015 and stmsg.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_SRS\_REPORTING\_POINT 1015 id's"

break

} else { Start-Sleep 10 }

}

while ($true) {

$component = gwmi -Namespace ("root\sms\site\_$SiteCode") -query "select stmsg.\* from SMS\_StatMsg stmsg where stmsg.Component = 'SMS\_SRS\_REPORTING\_POINT' and stmsg.MessageID = 500 and stmsg.SiteCode = '$SiteCode'"

if ($component -ne $null) {

Write-Host "Found SMS\_SRS\_REPORTING\_POINT 500 id's"

break

} else { Start-Sleep 10 }

}

$web = New-Object -ComObject msxml2.xmlhttp

$url = "http://localhost:80/reportserver/ConfigMgr\_$SiteCode"

while ($true) {

try {

$web.open('GET', $url, $false)

$web.send()

if ($web.status -eq "404") { start-sleep 10 }

if ($web.status -eq "200") {

Write-Host "Found ConfigMgr\_$SiteCode reporting site"

break

}

} catch {

#

}

}

* 1. Boundaries

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Configuration Manager Console and Click Administration. |
| 02. Expand Hierarchy Configuration and click Boundaries |
| 03. Click Create Boundary |
| 04. On General select:   * Type: IP Address Range * Starting IP Address: 192.168.3.1 * Ending IP Address: 192.168.3.254   Click Ok |

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

New-CMBoundary -DisplayName "Training Lab Boundary" -BoundaryType IPRange -Value "192.168.3.1-192.168.3.254"

* 1. Boundary Group

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Configuration Manager Console and Click Administration. |
| 02. Expand Hierarchy Configuration and click Boundary Group |
| 03. Click Create Boundary Group |
| 04. On General:   * Name: Training Lab * Boundaries: 192.168.3.1-192.168.3.254   Change to the References Tab |
| 05. On References:   * Select Use this boundary group for site assignment * Site Systems Servers: \\SRV0002.rflsytems.intranet   Click OK |
| 06. Right Click Training Lab and click Show Members |
| 07. The 192.168.3.1-192.168.3.254 boundary was added to the boundary group Training Lab |

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

$SiteCode = "001"

$servername = "SRV0002.classroom.intranet"

New-CMBoundaryGroup -Name "Training Lab" -AddSiteSystemServerName @($servername) -DefaultSiteCode $SiteCode

Add-CMBoundaryToGroup -BoundaryGroupName "Training Lab" -BoundaryName "Training Lab Boundary"

* 1. Distribution Point Group

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Configuration Manager Console and Click Administration |
| 02. Click Distribution Point Group |
| 03. Click Create Group |
| 04. On General, type Training Lab under Name and then Click Add |
| 05. On Add Distribution Points, select SRV0002.CLASSROOM.INTRANET and click OK twice |
| 06. Right Click Training Lab and click Show Members |
| 07. The SRV0002.CLASSROOM.INTRANET boundary was added to the distribution point group Training Lab |

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

$servername = "SRV0002.classroom.intranet"

New-CMDistributionPointGroup -Name "Training Lab"

Add-CMDistributionPointToGroup -DistributionPointGroupName "Training Lab" -DistributionPointName "$servername"

* 1. Network Access Account

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Configuration Manager Console and Click Administration. |
| 02. Expand Site Configuration and click Sites |
| 03. Select 001 – Training Lab site and click Configuration Site Components -> Software Distribution |
| 04. On Software Distribution Component Properties, change to the Network Access Account tab |
| 05. Under Network Access Account tab select Specify the account that accesses network locations and click Set -> New Account |
| 06. Under Windows User account type:   * User Name: CLASSROOM\svc\_sccmna * Password: Pa$$w0rd * Confirm Password: Pa$$w0rd   Click Verify |
| 07. Under verify type \\SRV0002\sms\_site for Network Share and click Test Connection |
| 08. Once the connection was successfully verified, click Ok three times |

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

$SiteCode = "001"

$Secure = 'Pa$$w0rd'| ConvertTo-SecureString -AsPlainText -Force

$account = "CLASSROOM\svc\_sccmna"

New-CMAccount -Name "$account" -Password $Secure -SiteCode $SiteCode

Set-CMSoftwareDistributionComponent -SiteCode $SiteCode -NetworkAccessAccountNames $account

* 1. Discovery
     1. Active Directory Forest Discovery

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Configuration Manager Console and Click Administration. |
| 02. Expand Hierarchy Configuration and click Discovery Methods |
| 03. Select Active Directory Forest Discovery and click Properties |
| 04. Under General, select Enabled Active Directory Forest Discovery and select Automatically create IP address range boundaries for IP subnets when they are discovered and Automatically create Active Directory site boundaries when they are discovered. Leave the schedule to run every 1 weeks and click OK |
| 05. When asked if you want to run full discovery as soon as possible, click Yes |
| 06. Select Boundaries and confirm that 3 new boundaries have been populated there |
| 07. Select Active Directory Forests and confirm that the Classroom.intranet is populated there. |
| 08. You can also review the following logs:   * C:\ConfigMgr\Logs\ADForestDisc.Log: Records Active Directory Forest Discovery actions. |

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

$SiteCode = "001"

Set-CMDiscoveryMethod -ActiveDirectoryForestDiscovery -EnableActiveDirectorySiteBoundaryCreation $True -Enabled $True -EnableSubnetBoundaryCreation $True -SiteCode $SiteCode

Invoke-CMForestDiscovery -SiteCode $SiteCode

* + 1. Active Directory System Discovery

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Configuration Manager Console and Click Administration. |
| 02. Expand Hierarchy Configuration and click Discovery Methods |
| 03. Select Active Directory System Discovery and click Properties |
| 04. Under General, select Enabled Active Directory System Discovery and add the active directory containers you want to search (using the yellow button)  Note: In this exercise we will use the classroom.intranet domain |
| 05. Click Polling Schedule to change the default schedule |
| 06. Click Active Directory Attributes to add more attributes to be discovered  Note: In this exercise, we will add pwdLastSet attribute |
| 07. Click options to add a filter to the discovered machines  Note: This option requires an active directory functional level of Windows Server 2003 or later  Note: In this exercise, we will select both options with default value of 90 days |
| 08. Click Ok and When asked if you want to run full discovery as soon as possible, click Yes |
| 09. Click Assets and Compliance and select Devices.  Note: There are a few more machines discovered now.  Note: Disabled Computers Accounts in Active Directory and Computers that do not have an IP Address are not going to be discovered |
| 10. Select WKS0001 and click Properties |
| 11. Once the WKS0001 Properties open, note the discovery method used under Agent Name. |
| 12. note the pwdLastSet property was also added to the list. Click Ok |
| 13. You can also review the following logs:   * C:\ConfigMgr\Logs\adsysdis.log: Records Active Directory System Discovery actions.   Note: Look for a line that starts: INFO: Search filter. This line shows the actual search query that was send to AD. There are two types of queries: Full synchronization and Incremental synchronization. |

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

$SiteCode = "001"

$domainName = "LDAP://DC=$($env:USERDNSDOMAIN.Split(".") -join ",DC=")"

Set-CMDiscoveryMethod -ActiveDirectorySystemDiscovery -AddActiveDirectoryContainer "$($domainName)" -Enabled $True -EnableDeltaDiscovery $True -EnableFilteringExpiredLogon $True -EnableFilteringExpiredPassword $True -SiteCode $SiteCode -TimeSinceLastLogonDays 90 -TimeSinceLastPasswordUpdateDays 90 -AddAdditionalAttribute @("pwdLastSet") -Recursive

Invoke-CMSystemDiscovery -SiteCode $SiteCode

* + 1. Active Directory User Discovery

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Configuration Manager Console and Click Administration. |
| 02. Expand Hierarchy Configuration and click Discovery Methods |
| 03. Select Active Directory User Discovery and click Properties |
| 04. Under General, select Enabled Active Directory User Discovery and add the active directory containers you want to search (using the yellow button)  Note: In this exercise we will use the classroom.intranet domain |
| 05. Click Polling Schedule to change the default schedule |
| 06. Click Active Directory Attributes to add more attributes to be discovered  Note: In this exercise, we will add physicalDeliveryOfficeName and department attribute |
| 07. Click Ok and When asked if you want to run full discovery as soon as possible, click Yes |
| 08. Click Assets and Compliance and select Users. |
| 09. Select CLASSROOM\User01 (User01) and click Properties |
| 10. Once the CLASSROOM\User01 (User01) Properties open, note the discovery method used under Agent Name. |
| 11. Note the physicalDeliveryOfficeName and department property was also added to the list. Click Ok |
| 09. You can also review the following logs:   * C:\ConfigMgr\Logs\adusrdis.log: Records Active Directory User Discovery actions.   Note: Look for a line that starts: INFO: Search filter. This line shows the actual search query that was send to AD. There are two types of queries: Full synchronization and Incremental synchronization. |

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

$SiteCode = "001"

$domainName = "LDAP://DC=$($env:USERDNSDOMAIN.Split(".") -join ",DC=")"

Set-CMDiscoveryMethod -ActiveDirectoryUserDiscovery -AddActiveDirectoryContainer "$($domainname)" -DeltaDiscoveryIntervalMinutes 30 -Enabled $True -EnableDeltaDiscovery $True -SiteCode $SiteCode -AddAdditionalAttribute @("physicalDeliveryOfficeName") -recursive

Invoke-CMUserDiscovery -SiteCode $SiteCode

* + 1. Active Directory Group Discovery

|  |
| --- |
| Perform this task on the SRV0002 virtual machine logged on as sccmadmin |
| 01. Start Configuration Manager Console and Click Administration. |
| 02. Expand Hierarchy Configuration and click Discovery Methods |
| 03. Select Active Directory Group Discovery and click Properties |
| 04. Under General, select Enabled Active Directory Group Discovery and click Add -> Location |
| 05. Under Add Active Directory Location add active directory containers you want to search and click Ok  Note: In this exercise, we will use the classroom.intranet domain |
| 06. One Back to the Active Directory Group Discovery Properties, click Next |
| 07. Click Polling Schedule to change the default schedule |
| 08. Click options to add a filter to the discovered machines  Note: This option required active directory functional level of Windows Server 2003 or later  Note: In this exercise, we will leave the default unchecked option |
| 09. Click Ok and When asked if you want to run full discovery as soon as possible, click Yes |
| 10. Click Assets and Compliance and select Users. |
| 11. Select CLASSROOM\Allowed RODC Password Replication Group and click Properties |
| 12. Once the CLASSROOM\Allowed RODC Password Replication Group Properties open, note the discovery method used under Agent Name. |
| 13. You can also review the following logs:   * C:\ConfigMgr\Logs\adsgdis.log: Records Active Directory Group Discovery actions.   Note: Look for a line that starts: INFO: Search filter. This line shows the actual search query that was send to AD. There are two types of queries: Full synchronization and Incremental synchronization. |

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

$SiteCode = "001"

$domainName = "LDAP://DC=$($env:USERDNSDOMAIN.Split(".") -join ",DC=")"

$discovery = New-CMADGroupDiscoveryScope -LdapLocation "$($domainName)" -Name "$($domainName)" -SiteCode $SiteCode -RecursiveSearch $true

Set-CMDiscoveryMethod -ActiveDirectoryGroupDiscovery -AddGroupDiscoveryScope ($discovery) -Enabled $True -SiteCode $SiteCode -EnableDeltaDiscovery $true

Invoke-CMGroupDiscovery -SiteCode $SiteCode