Dynamics365 Finance and Operations

On-premise Installation (later 41)

Prepared by: donggyun Ha

E-Mail : donggyun.ha@sycns.co.kr

Phone :

Version: 1.0.0

Date: 2021-11-15

Version Control

Version	Date	Initials	Summary of Changes
1.0.0	2021-11-15		First Created

List

1 Dynamics365 Finance And Operations Installation (later 41)

1.1 HardWare Layout

Server Name	Service Fabric node type	Server IP
Domain		192.168.10.40
AOS1	AOSNodeType	192.168.10.41
AOS2	AOSNodeType	192.168.10.42
AOS3	AOSNodeType	192.168.10.43
ORCH1	OrchestratorType	192.168.10.44
ORCH2	OrchestratorType	192.168.10.45
ORCH3	OrchestratorType	192.168.10.46
SSRS	ReportServerType	192.168.10.48
SQL		192.168.10.47
MR	MRType	192.168.10.49
FILE		192.168.10.50

1.2 Plan your Domain Name and DNS Zones

We recommend that you use a publicly registered domain name for your production installation of AOS. In that way, the installation can be accessed outside the network, if outside access is required.

For example, if your company's domain is hdg.com, your zone for Finance + Operations might be hdg.com, and the host names might be as follows:

- ax.hdg.com for AOS machines
- sf.hdg.com for the Service Fabric cluster

1.3 Plan your users and service accounts

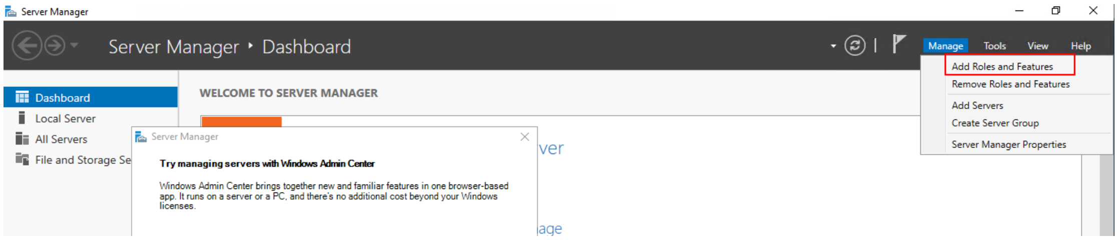
User account	Type	Purpose	User name
Financial Reporting Application Service Account	gMSA		hdg₩svc-FRAS$
Financial Reporting Process Service Account	gMSA		hdg₩svc-FRPS$
Financial Reporting Click Once Designer Service Account	gMSA		hdg₩svc-FRCO$

AOS Service Account	gMSA	You should create this user for future proofing. Microsoft plans to enable AOS to work with the gMSA in upcoming releases. By creating this user at the time of setup, you help to ensure a seamless transition to the gMSA.	hdg₩svc-AXSF$
SSRS bootstrapper Service Account	gMSA	The reporting service bootstrapper uses this account to configure the SSRS service.	hdg₩svc-ReportSvc$
AOS SQL DB Admin user	SQL User	Finance + Operations uses this user to authenticate with SQL. This user will also be replaced by the gMSA user in upcoming releases	Axdbadmin
Local Deployment Agent Service Account	gMSA	The local agent uses this account to orchestrate the deployment on various nodes.	hdg₩svc-LocalAgent$

- We don't use AxServiceUser anymore. You can find reason in purpose of AOS Service Account.

1.4 Prerequisites

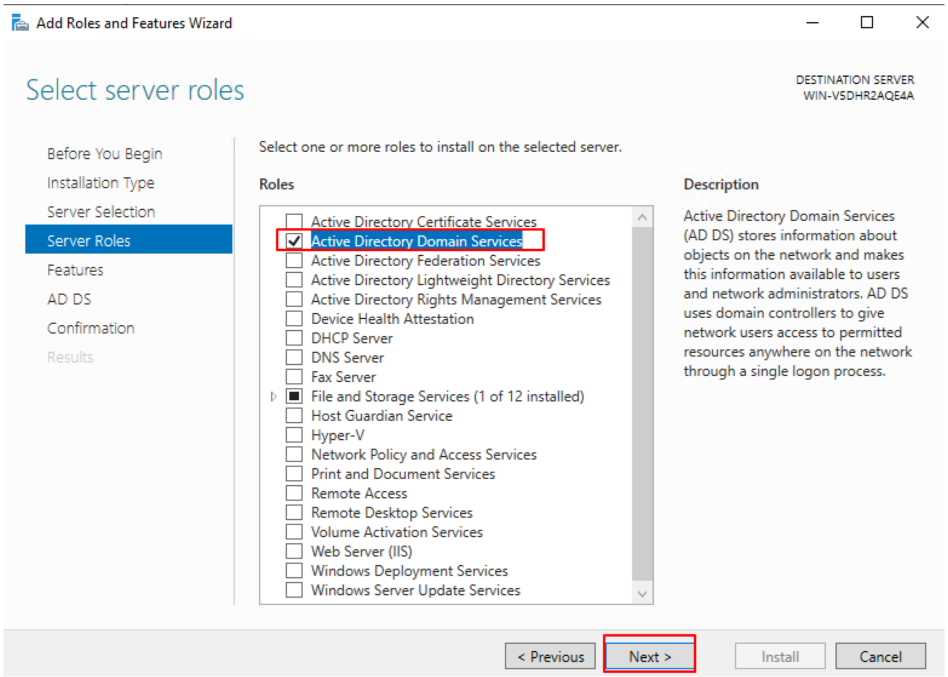
1.4.1 Acive Directory Domain Services (AD DS) must be installed and configured in your network.



Try managing servers with Windows Admin Center

Windows Admin Center brings together new and familiar features in one browser-based app. It runs on a server or a PC, and there's no additional cost beyond your Windows licenses.

1. On Server Manager in domain controller server, click **Add roles and features**.


Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-V5DHR2AQE4A

Select one or more roles to install on the selected server.

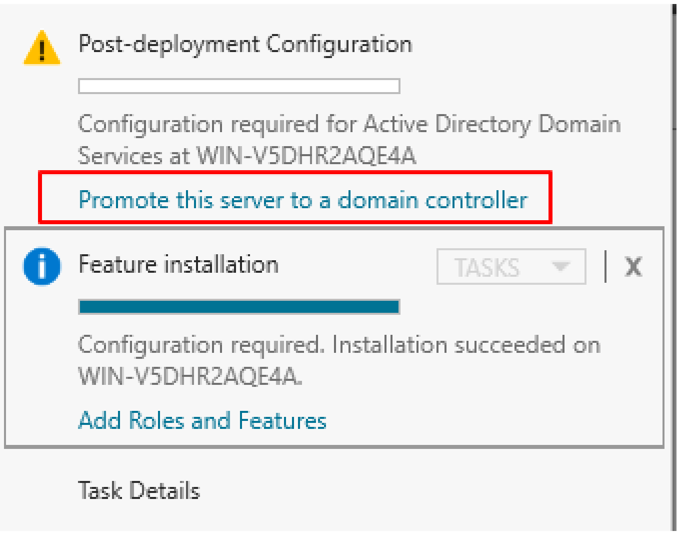
Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

2. On the Server Roles Page, select **Active Direcotry Domain Services**.


Post-deployment Configuration

Configuration required for Active Directory Domain Services at WIN-V5DHR2AQE4A

Promote this server to a domain controller

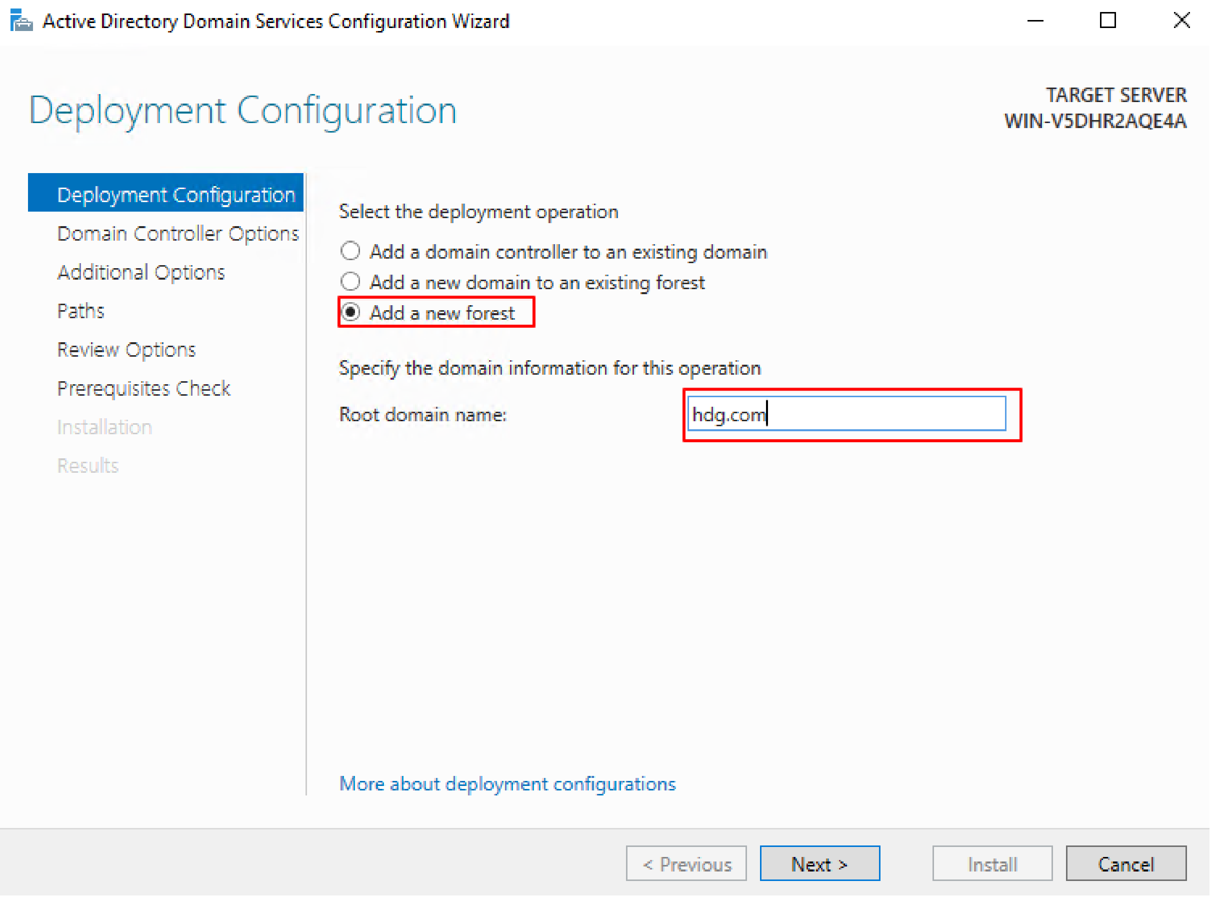
Feature installation

Configuration required. Installation succeeded on WIN-V5DHR2AQE4A.

Add Roles and Features

Task Details

3. After install, click **Promte this server to a domain controller.**



Select the deployment operation

○ Add a domain controller to an existing domain

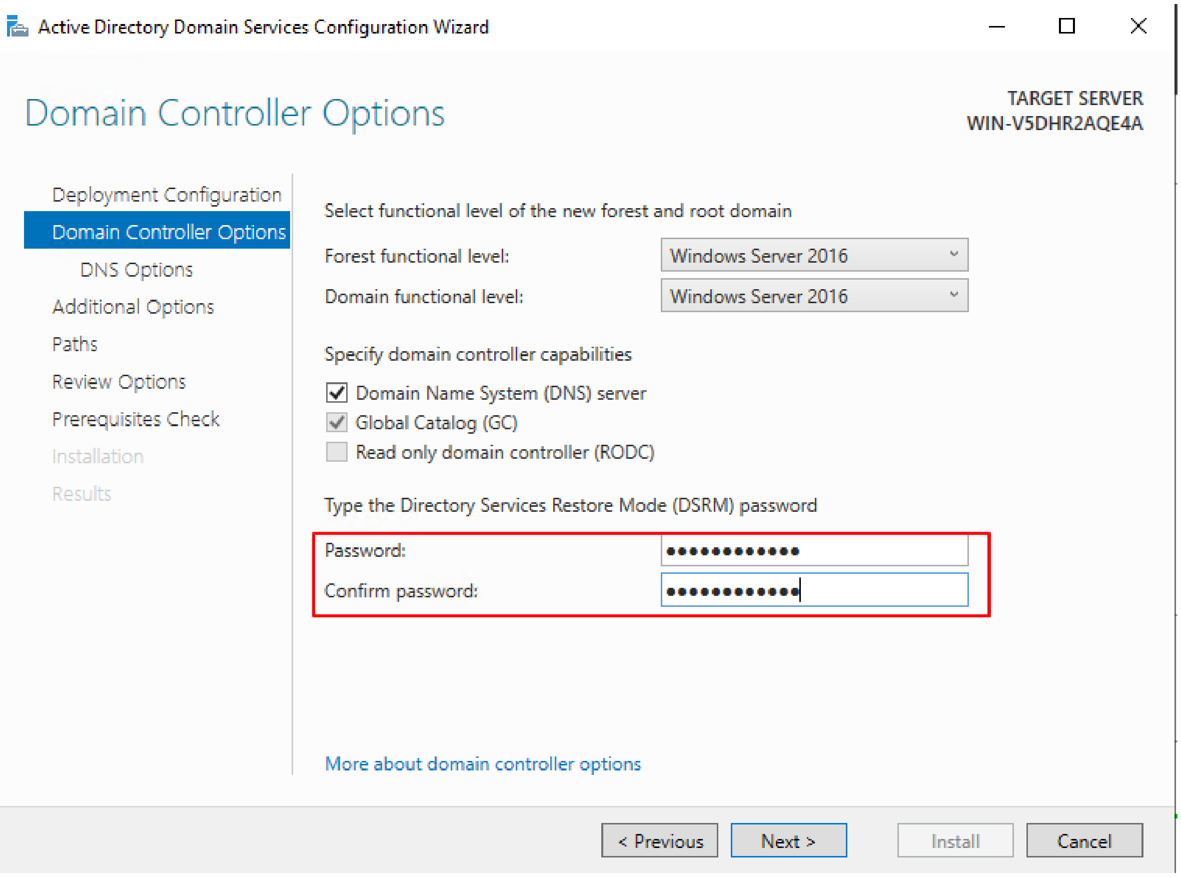
○ Add a new domain to an existing forest

● Add a new forest

Specify the domain information for this operation

Root domain name: hdg.com

4. On Deployment Configuration page, select **Add a new forest** and insert Root domain name.



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
WIN-V5DHR2AQE4A

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2016

Domain functional level: Windows Server 2016

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

□ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: ●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●

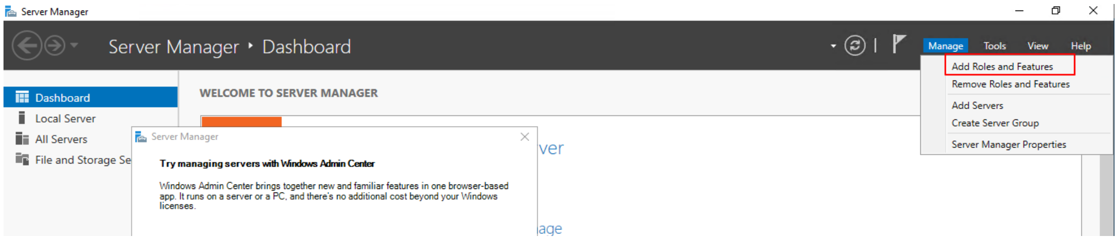
More about domain controller options

5. On Domain Controller Options page, insert password.

6. After all installaion is completed, the computer must be restarted.

1.4.2 AD CS is intalled and configured in your network

1. On Server Manager in Domain controller server, click **Add roles and features**.

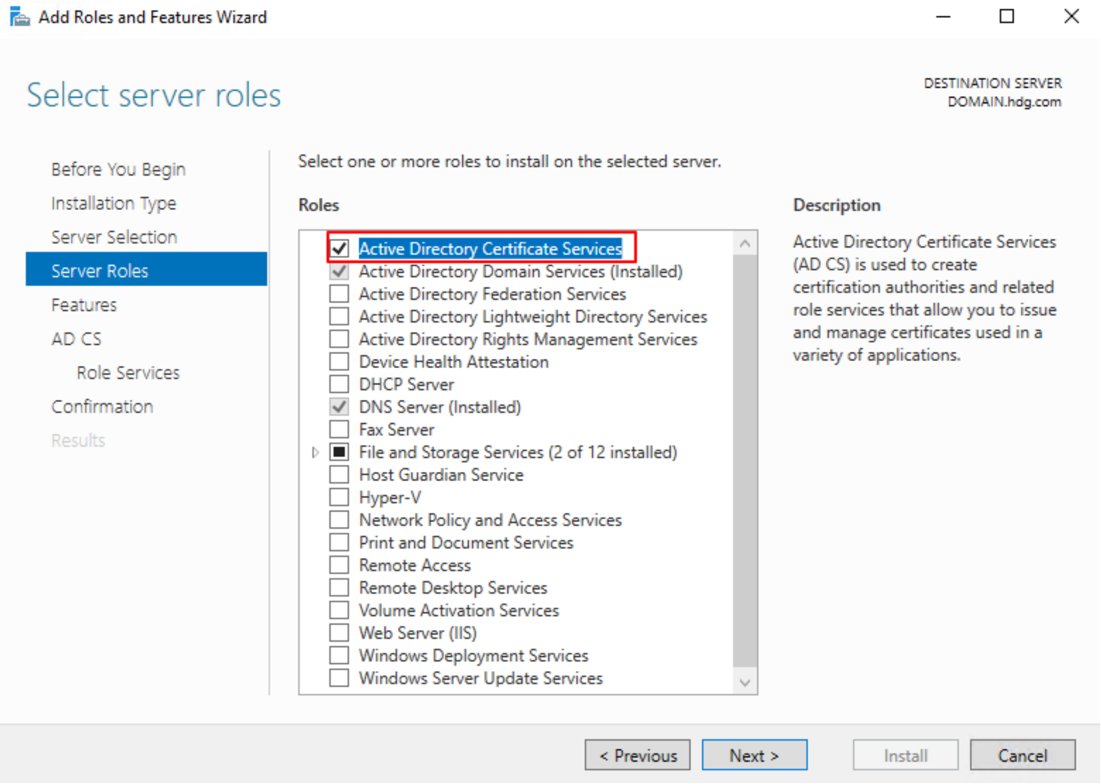


Server Manager

Try managing servers with Windows Admin Center

Windows Admin Center brings together new and familiar features in one browser-based app. It runs on a server or a PC, and there's no additional cost beyond your Windows licenses.

2. On the Server Roles Page, select **Active Direcotry Certificate Services**.



Select one or more roles to install on the selected server.

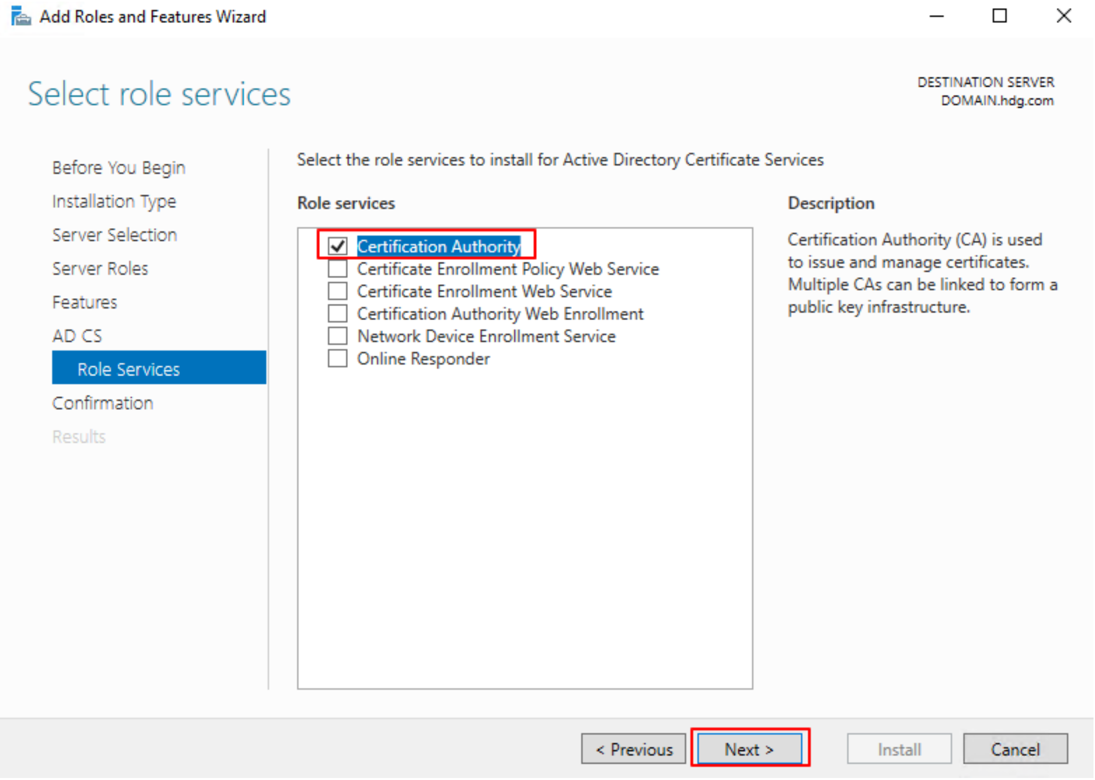
Roles

☑ Active Directory Certificate Services
☑ Active Directory Domain Services (Installed)
□ Active Directory Federation Services
□ Active Directory Lightweight Directory Services
□ Active Directory Rights Management Services
□ Device Health Attestation
□ DHCP Server
☑ DNS Server (Installed)
□ Fax Server
■ File and Storage Services (2 of 12 installed)
□ Host Guardian Service
□ Hyper-V
□ Network Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services
□ Volume Activation Services
□ Web Server (IIS)
□ Windows Deployment Services
□ Windows Server Update Services

Description

Active Directory Certificate Services (AD CS) is used to create certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.

3. On the Role Services page, select **Certification Authority.**



Select the role services to install for Active Directory Certificate Services

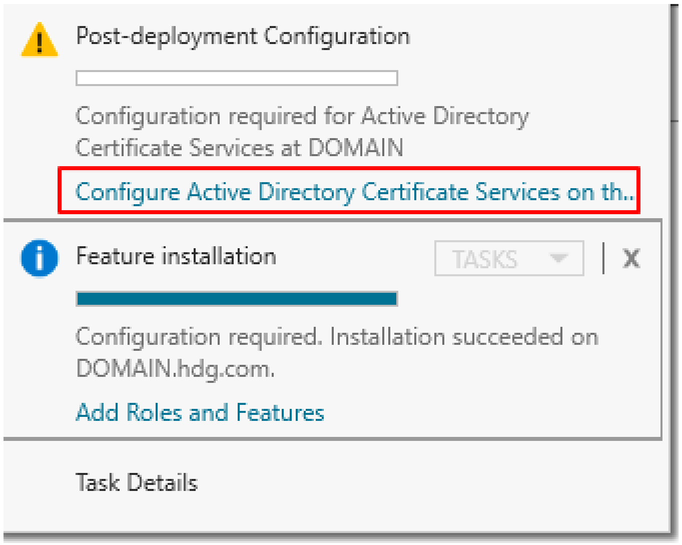
Role services

☑ Certification Authority
□ Certificate Enrollment Policy Web Service
□ Certificate Enrollment Web Service
□ Certification Authority Web Enrollment
□ Network Device Enrollment Service
□ Online Responder

Description

Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

4. After Install is finished, click **Configure Active Directory Certificate Serevices on this server.**



Post-deployment Configuration

Configuration required for Active Directory Certificate Services at DOMAIN

Configure Active Directory Certificate Services on th..

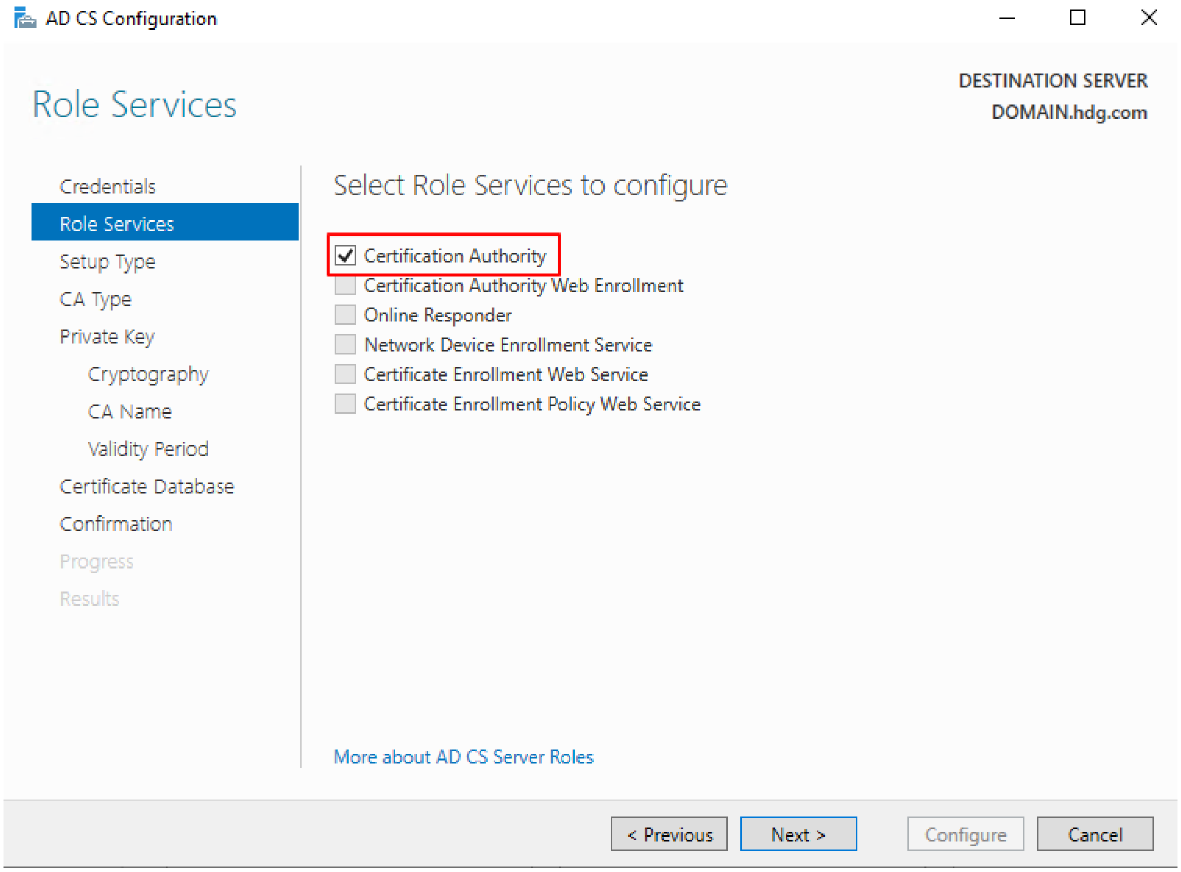
Feature installation

Configuration required. Installation succeeded on DOMAIN.hdg.com.

Add Roles and Features

Task Details

5. On the Roles Services page, click **Certification Authority**.



AD CS Configuration

Role Services

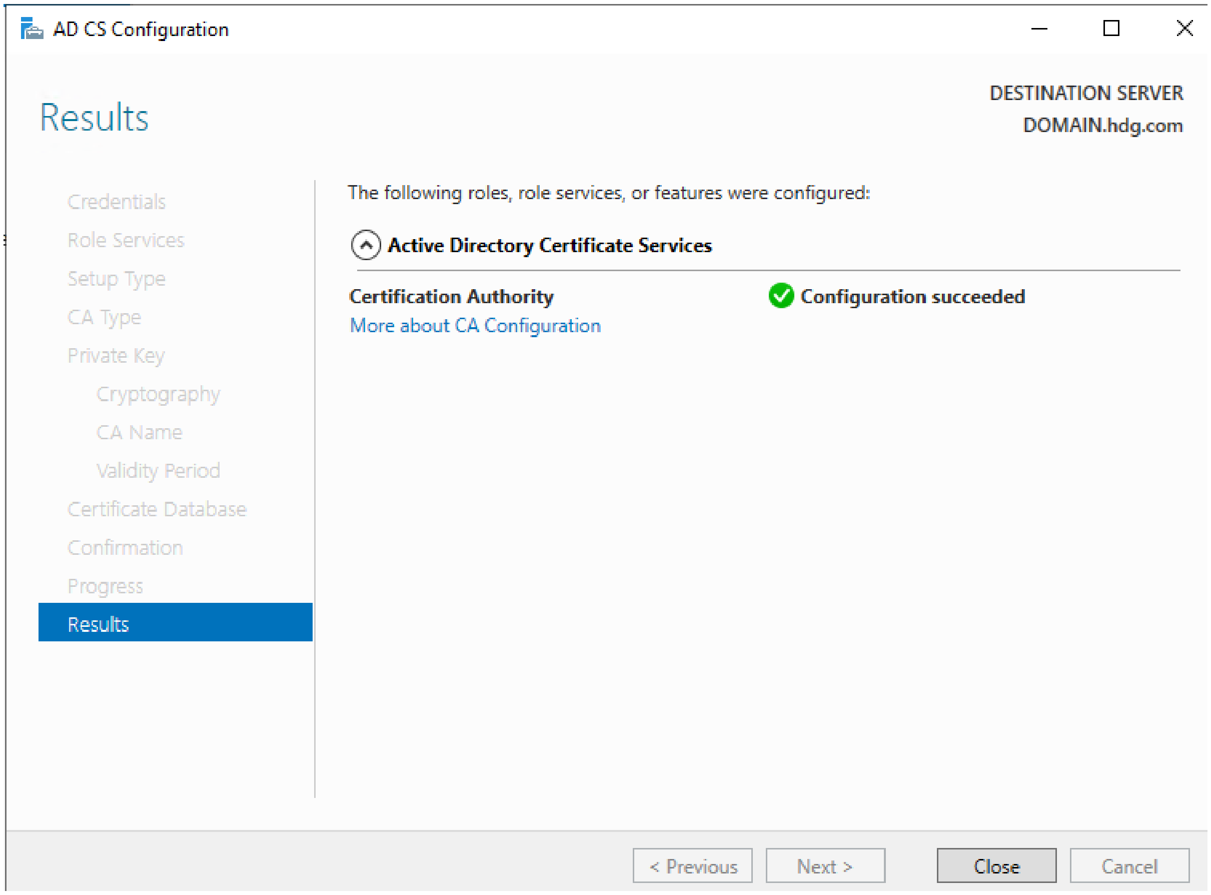
DESTINATION SERVER
DOMAIN.hdg.com

Select Role Services to configure

☑ Certification Authority
□ Certification Authority Web Enrollment
□ Online Responder
□ Network Device Enrollment Service
□ Certificate Enrollment Web Service
□ Certificate Enrollment Policy Web Service

More about AD CS Server Roles

6. Install finish.



AD CS Configuration

Results

DESTINATION SERVER
DOMAIN.hdg.com

The following roles, role services, or features were configured:

Active Directory Certificate Services

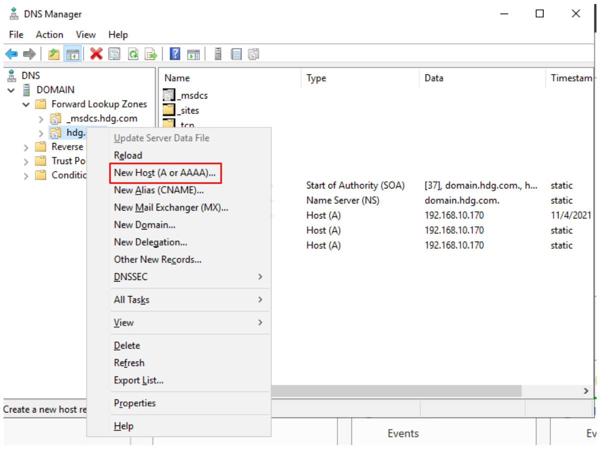
Certification Authority — ✓ Configuration succeeded

More about CA Configuration

1.5 Create A records

Sign in to the domatin controller machine, then open DNS Manager by entering dnsmgmt.msc and selecting the domain before we created at prequisites.

For each Servire Fabric culster node of the **AOSNodeType** type, create on A record that named **ax.hdg.com**. Don’t create A records for the other node types.

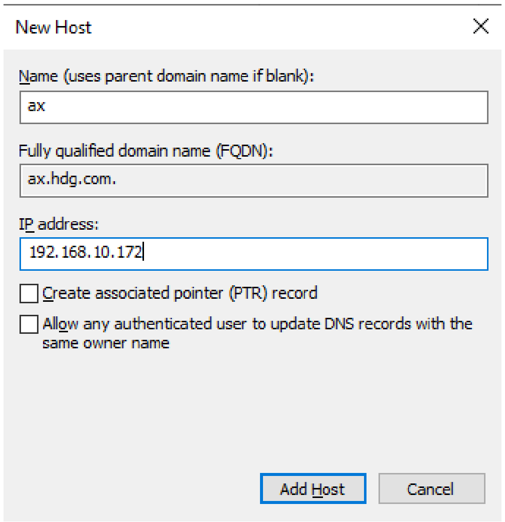


DNS Manager

```
Name        Type                       Data                          Timestam
_msdcs
_sites
_tcp
            Start of Authority (SOA)   [37], domain.hdg.com., h...   static
            Name Server (NS)           domain.hdg.com.               static
            Host (A)                   192.168.10.170                11/4/2021
            Host (A)                   192.168.10.170                static
            Host (A)                   192.168.10.170                static
```

Create a new host re

1. Right-click the zone, and then select **New Host**.



Name (uses parent domain name if blank): ax

Fully qualified domain name (FQDN): ax.hdg.com.

IP address: 192.168.10.172

☐ Create associated pointer (PTR) record

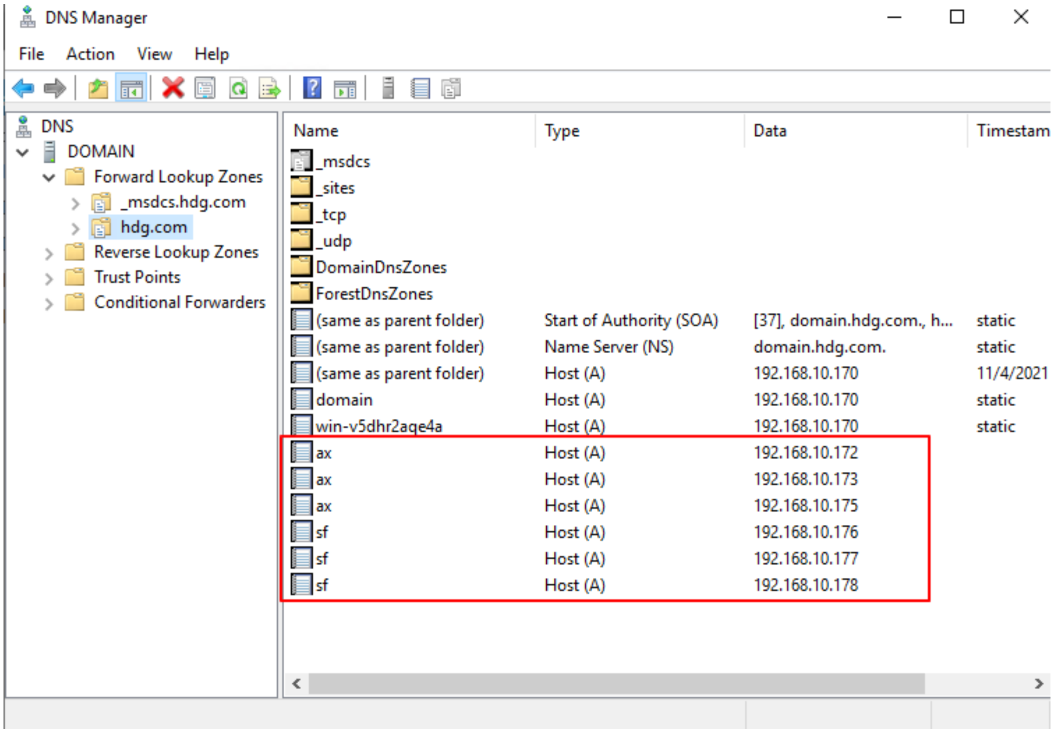
☐ Allow any authenticated user to update DNS records with the same owner name

2. Enter the name and IP address of the Service Fabric node and don’t select either check box.

3. Repeat steps 2 through 4 for each additional AOS node.

For each Servire Fabric culster node of the **OrchestratorType type**, create on A record that named **sf.hdg.com**. Don’t create A records for the other node types.

1. The same Procedure should be following for remaining sf.



Name	Type	Data	Timestam
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[37], domain.hdg.com., h...	static
(same as parent folder)	Name Server (NS)	domain.hdg.com.	static
(same as parent folder)	Host (A)	192.168.10.170	11/4/2021
domain	Host (A)	192.168.10.170	static
win-v5dhr2aqe4a	Host (A)	192.168.10.170	static
ax	Host (A)	192.168.10.172	
ax	Host (A)	192.168.10.173	
ax	Host (A)	192.168.10.175	
sf	Host (A)	192.168.10.176	
sf	Host (A)	192.168.10.177	
sf	Host (A)	192.168.10.178	

1.6 Join VMs to the domain

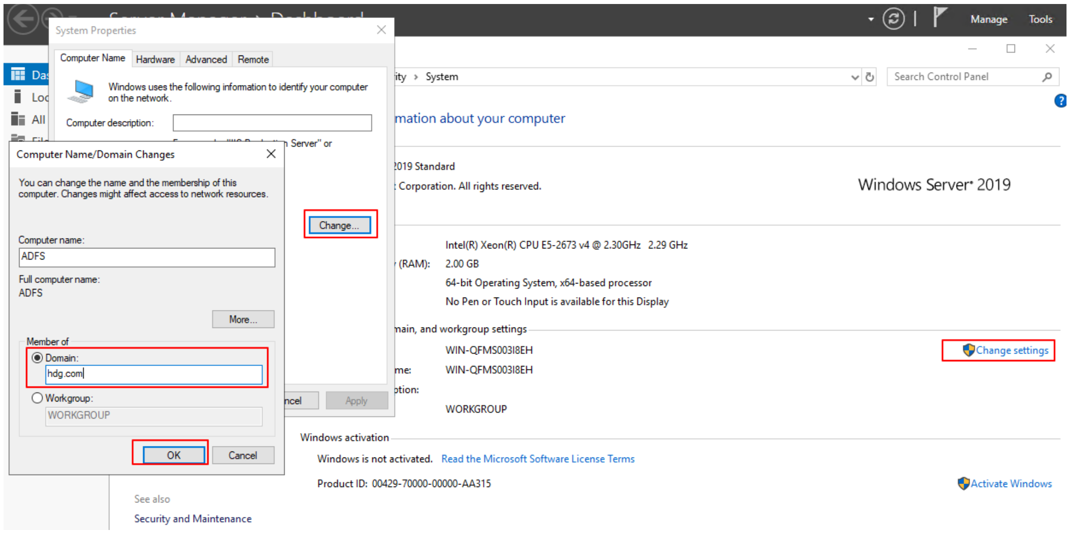
There are two ways to Join VMs.

First is using PowerShell.

```
$domainName = Read-Host -Prompt 'Specify domain name (ex: contoso.com)'

Add-Computer -DomainName $domainName -Credential (Get-Credential -Message 'Enter domain credential')
```

The second way is using Control Panel.

1. Enter **Control Panel – System and Security – System**.
2. Click **Change settings – Change – Insert Domain**
3. After login, the Server must be restarted.



System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name: ADFS

Full computer name: ADFS

Member of

● Domain: hdg.com

○ Workgroup: WORKGROUP

mation about your computer

2019 Standard

Corporation. All rights reserved.

Windows Server 2019

Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz 2.29 GHz

(RAM): 2.00 GB

64-bit Operating System, x64-based processor

No Pen or Touch Input is available for this Display

main, and workgroup settings

WIN-QFMS003I8EH

me: WIN-QFMS003I8EH

ption:

WORKGROUP

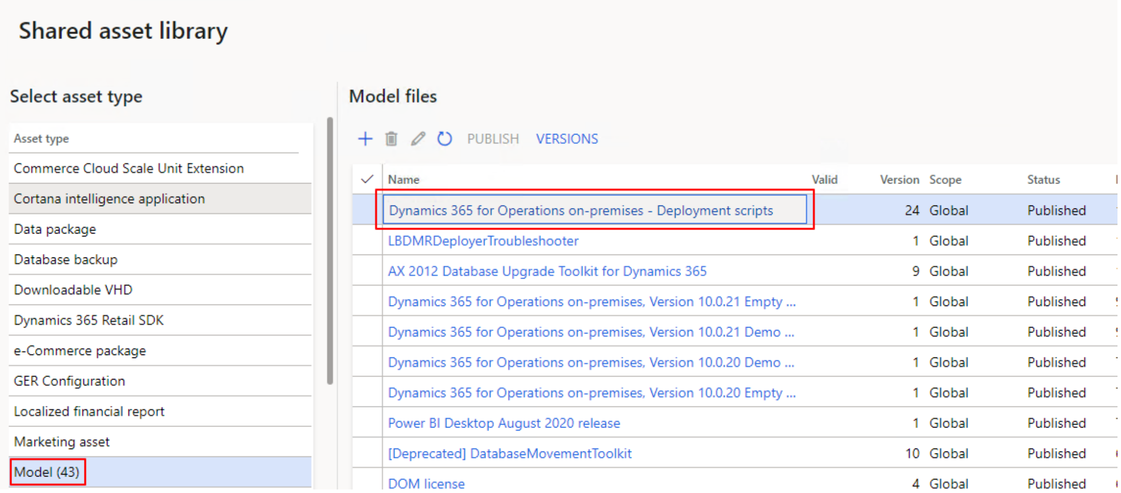
Windows activation

Windows is not activated. Read the Microsoft Software License Terms

Product ID: 00429-70000-00000-AA315

1.7 Download setup scripts from LCS

1. Sign in to LCS.
2. On the dashboard, select the **Shared asset library** tile.
3. Select Model tab, int the grid, select the row for **Dynamics 365 for Operations on-premises – Deployment scripts.**



Shared asset library

Select asset type

Asset type
Commerce Cloud Scale Unit Extension
Cortana intelligence application
Data package
Database backup
Downloadable VHD
Dynamics 365 Retail SDK
e-Commerce package
GER Configuration
Localized financial report
Marketing asset
Model (43)

Model files

Name	Valid	Version	Scope	Status
Dynamics 365 for Operations on-premises - Deployment scripts		24	Global	Published
LBDMRDeployerTroubleshooter		1	Global	Published
AX 2012 Database Upgrade Toolkit for Dynamics 365		9	Global	Published
Dynamics 365 for Operations on-premises, Version 10.0.21 Empty ...		1	Global	Published
Dynamics 365 for Operations on-premises, Version 10.0.21 Demo ...		1	Global	Published
Dynamics 365 for Operations on-premises, Version 10.0.20 Demo ...		1	Global	Published
Dynamics 365 for Operations on-premises, Version 10.0.20 Empty ...		1	Global	Published
Power BI Desktop August 2020 release		1	Global	Published
[Deprecated] DatabaseMovementToolkit		10	Global	Published
DOM license		4	Global	Published

4. Select **Versions**, and download the latest version of the zip file for the scripts.

5. After the zip file is downloaded, select and hold (or right-click) it, and then select **Properties**. In the **Properties** dialog box, select the Unblock checkbox.

6. Copy the zip file to the machine that will be used to run the scripts.

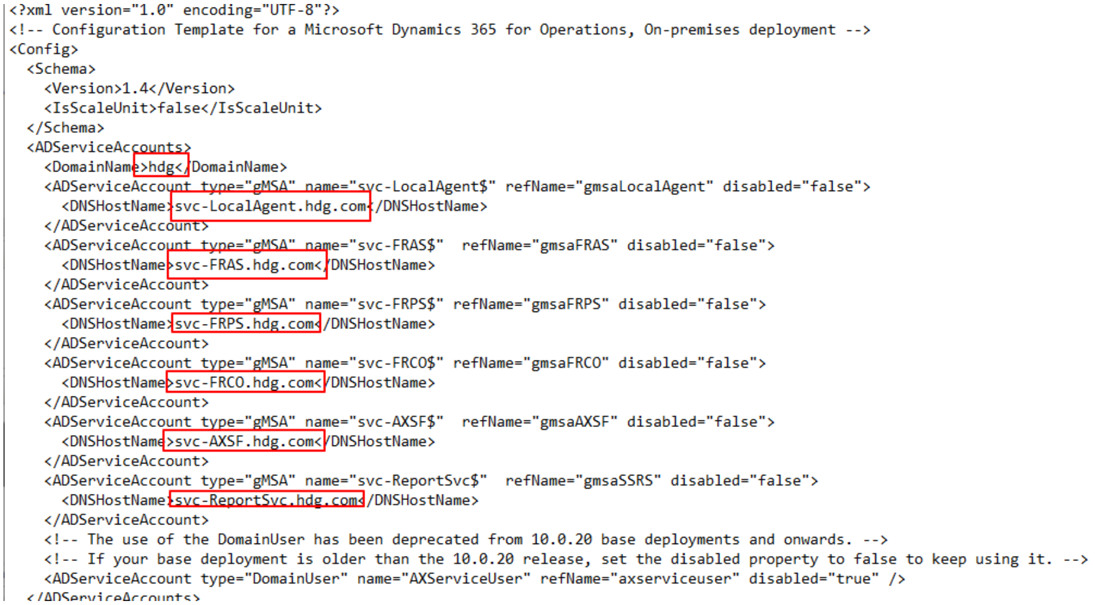
7. Unzip the files into a folder that is named **infrastructure**.

1.8 Config Template file configuration

1. Go to the machine that has the unzipped infrastructure scripts in the **infrastructure** folder.

2. Edit Configuration.xml

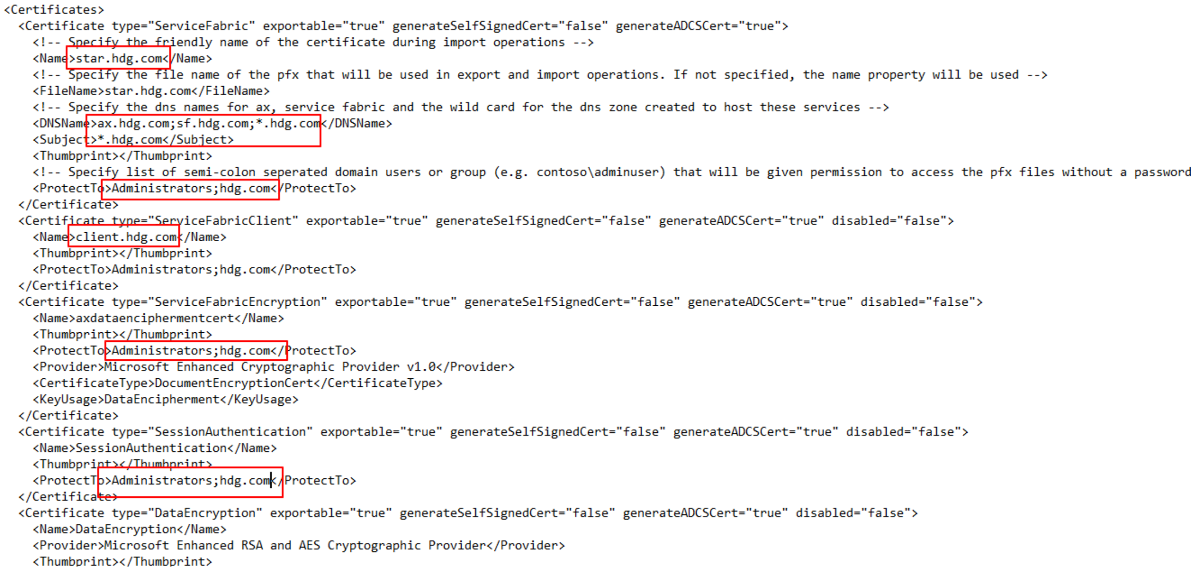
3. Update the Users for each purpose with your **domain Name**.



```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Configuration Template for a Microsoft Dynamics 365 for Operations, On-premises deployment -->
<Config>
  <Schema>
    <Version>1.4</Version>
    <IsScaleUnit>false</IsScaleUnit>
  </Schema>
  <ADServiceAccounts>
    <DomainName>hdg</DomainName>
    <ADServiceAccount type="gMSA" name="svc-LocalAgent$" refName="gmsaLocalAgent" disabled="false">
      <DNSHostName>svc-LocalAgent.hdg.com</DNSHostName>
    </ADServiceAccount>
    <ADServiceAccount type="gMSA" name="svc-FRAS$"  refName="gmsaFRAS" disabled="false">
      <DNSHostName>svc-FRAS.hdg.com</DNSHostName>
    </ADServiceAccount>
    <ADServiceAccount type="gMSA" name="svc-FRPS$" refName="gmsaFRPS" disabled="false">
      <DNSHostName>svc-FRPS.hdg.com</DNSHostName>
    </ADServiceAccount>
    <ADServiceAccount type="gMSA" name="svc-FRCO$" refName="gmsaFRCO" disabled="false">
      <DNSHostName>svc-FRCO.hdg.com</DNSHostName>
    </ADServiceAccount>
    <ADServiceAccount type="gMSA" name="svc-AXSF$"  refName="gmsaAXSF" disabled="false">
      <DNSHostName>svc-AXSF.hdg.com</DNSHostName>
    </ADServiceAccount>
    <ADServiceAccount type="gMSA" name="svc-ReportSvc$"  refName="gmsaSSRS" disabled="false">
      <DNSHostName>svc-ReportSvc.hdg.com</DNSHostName>
    </ADServiceAccount>
    <!-- The use of the DomainUser has been deprecated from 10.0.20 base deployments and onwards. -->
    <!-- If your base deployment is older than the 10.0.20 release, set the disabled property to false to keep using it. -->
    <ADServiceAccount type="DomainUser" name="AXServiceUser" refName="axserviceuser" disabled="true" />
  </ADServiceAccounts>
```

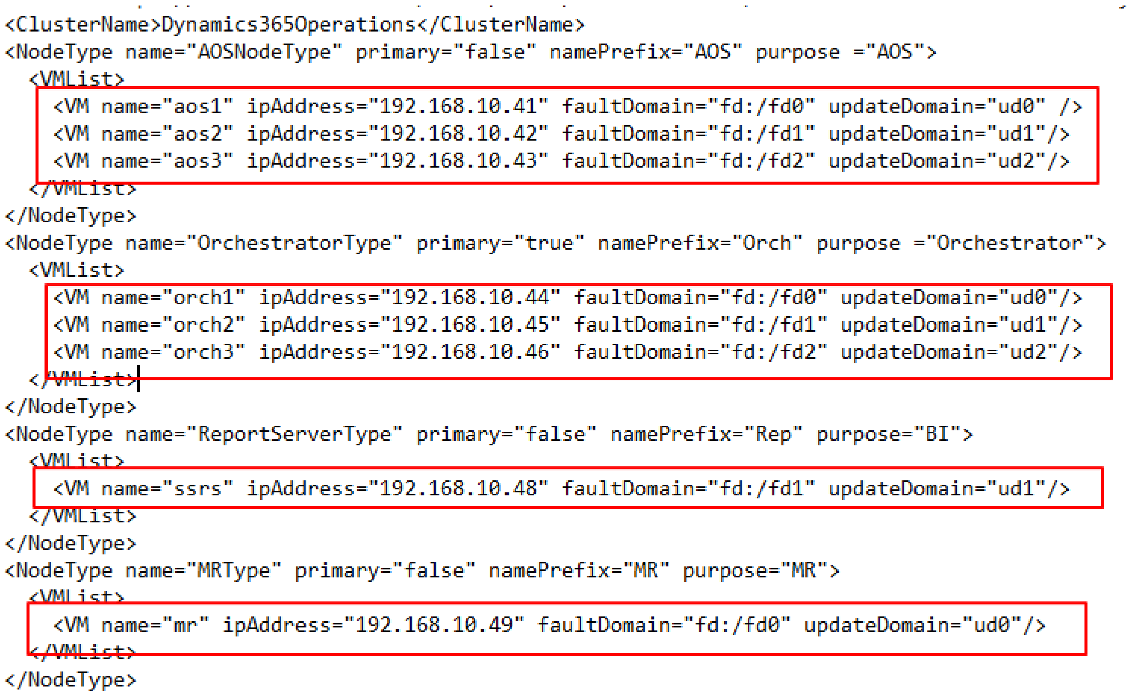
4. Update the **Cetificate Subject Name and add the administrators** group for the Domain.

5. Update the sames for all the Certificates.



```
<Certificates>
  <Certificate type="ServiceFabric" exportable="true" generateSelfSignedCert="false" generateADCSCert="true">
    <!-- Specify the friendly name of the certificate during import operations -->
    <Name>star.hdg.com</Name>
    <!-- Specify the file name of the pfx that will be used in export and import operations. If not specified, the name property will be used -->
    <FileName>star.hdg.com</FileName>
    <!-- Specify the dns names for ax, service fabric and the wild card for the dns zone created to host these services -->
    <DNSName>ax.hdg.com;sf.hdg.com;*.hdg.com</DNSName>
    <Subject>*.hdg.com</Subject>
    <Thumbprint></Thumbprint>
    <!-- Specify list of semi-colon seperated domain users or group (e.g. contoso\adminuser) that will be given permission to access the pfx files without a password
    <ProtectTo>Administrators;hdg.com</ProtectTo>
  </Certificate>
  <Certificate type="ServiceFabricClient" exportable="true" generateSelfSignedCert="false" generateADCSCert="true" disabled="false">
    <Name>client.hdg.com</Name>
    <Thumbprint></Thumbprint>
    <ProtectTo>Administrators;hdg.com</ProtectTo>
  </Certificate>
  <Certificate type="ServiceFabricEncryption" exportable="true" generateSelfSignedCert="false" generateADCSCert="true" disabled="false">
    <Name>axdataenciphermentcert</Name>
    <Thumbprint></Thumbprint>
    <ProtectTo>Administrators;hdg.com</ProtectTo>
    <Provider>Microsoft Enhanced Cryptographic Provider v1.0</Provider>
    <CertificateType>DocumentEncryptionCert</CertificateType>
    <KeyUsage>DataEncipherment</KeyUsage>
  </Certificate>
  <Certificate type="SessionAuthentication" exportable="true" generateSelfSignedCert="false" generateADCSCert="true" disabled="false">
    <Name>SessionAuthentication</Name>
    <Thumbprint></Thumbprint>
    <ProtectTo>Administrators;hdg.com</ProtectTo>
  </Certificate>
  <Certificate type="DataEncryption" exportable="true" generateSelfSignedCert="false" generateADCSCert="true" disabled="false">
    <Name>DataEncryption</Name>
    <Provider>Microsoft Enhanced RSA and AES Cryptographic Provider</Provider>
    <Thumbprint></Thumbprint>
```

6. Update the VM Name and the IP addrees of the VM.



```
<ClusterName>Dynamics365Operations</ClusterName>
<NodeType name="AOSNodeType" primary="false" namePrefix="AOS" purpose ="AOS">
  <VMList>
    <VM name="aos1" ipAddress="192.168.10.41" faultDomain="fd:/fd0" updateDomain="ud0" />
    <VM name="aos2" ipAddress="192.168.10.42" faultDomain="fd:/fd1" updateDomain="ud1"/>
    <VM name="aos3" ipAddress="192.168.10.43" faultDomain="fd:/fd2" updateDomain="ud2"/>
  </VMList>
</NodeType>
<NodeType name="OrchestratorType" primary="true" namePrefix="Orch" purpose ="Orchestrator">
  <VMList>
    <VM name="orch1" ipAddress="192.168.10.44" faultDomain="fd:/fd0" updateDomain="ud0"/>
    <VM name="orch2" ipAddress="192.168.10.45" faultDomain="fd:/fd1" updateDomain="ud1"/>
    <VM name="orch3" ipAddress="192.168.10.46" faultDomain="fd:/fd2" updateDomain="ud2"/>
  </VMList>
</NodeType>
<NodeType name="ReportServerType" primary="false" namePrefix="Rep" purpose="BI">
  <VMList>
    <VM name="ssrs" ipAddress="192.168.10.48" faultDomain="fd:/fd1" updateDomain="ud1"/>
  </VMList>
</NodeType>
<NodeType name="MRType" primary="false" namePrefix="MR" purpose="MR">
  <VMList>
    <VM name="mr" ipAddress="192.168.10.49" faultDomain="fd:/fd0" updateDomain="ud0"/>
  </VMList>
</NodeType>
```

1.9 Create gMSA and domain user accounts

1. Copy the **infrastructure** folder to the **domain controller machine**.

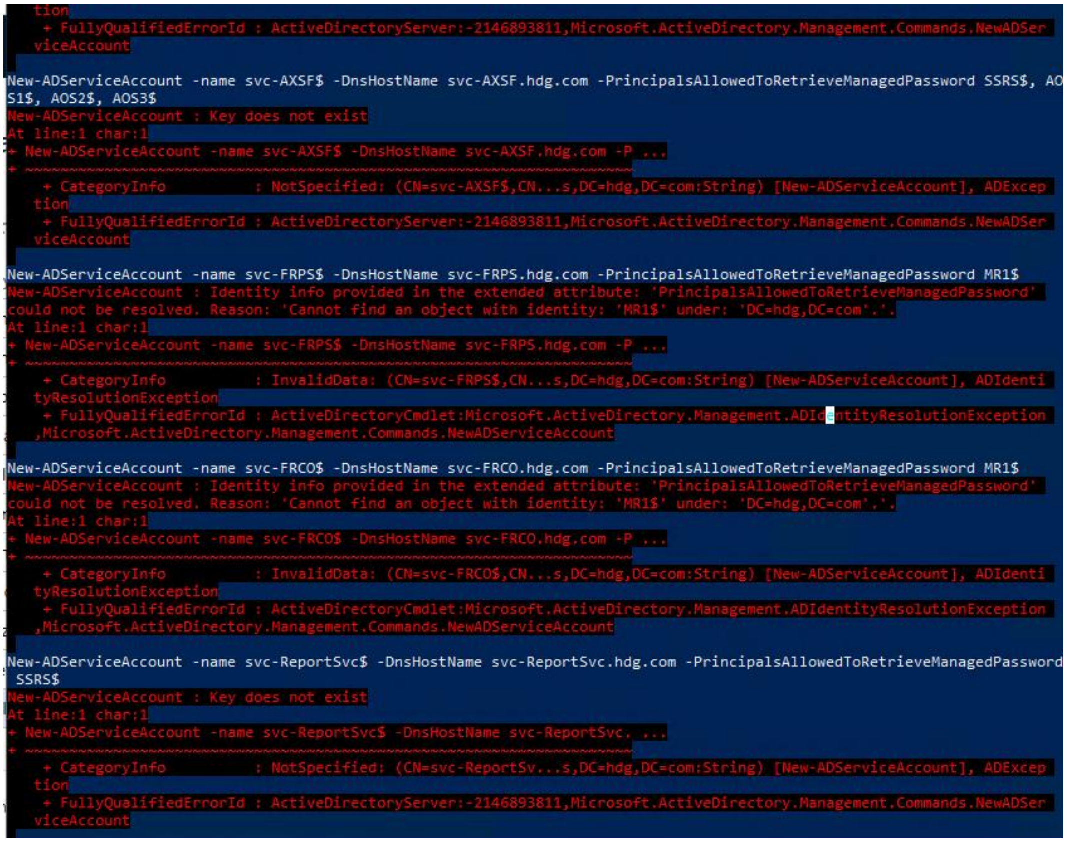
2. Open Windows PowerShell in elevated mode, change the directory to the **infrastructure** folder, and run the following commands.

Import-Module .₩D365FO-OP₩D365FO-OP.psd1

New-D365FOGMSAAccounts -ConfigurationFilePath .₩ConfigTemplate.xml

- When error ocurred like below picture, run following commands. (Ref. docs)

Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))



```
  tion
    + FullyQualifiedErrorId : ActiveDirectoryServer:-2146893811,Microsoft.ActiveDirectory.Management.Commands.NewADSer
   viceAccount

New-ADServiceAccount -name svc-AXSF$ -DnsHostName svc-AXSF.hdg.com -PrincipalsAllowedToRetrieveManagedPassword SSRS$, AO
S1$, AOS2$, AOS3$
New-ADServiceAccount : Key does not exist
At line:1 char:1
+ New-ADServiceAccount -name svc-AXSF$ -DnsHostName svc-AXSF.hdg.com -P ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (CN=svc-AXSF$,CN...s,DC=hdg,DC=com:String) [New-ADServiceAccount], ADExcep
   tion
    + FullyQualifiedErrorId : ActiveDirectoryServer:-2146893811,Microsoft.ActiveDirectory.Management.Commands.NewADSer
   viceAccount

New-ADServiceAccount -name svc-FRPS$ -DnsHostName svc-FRPS.hdg.com -PrincipalsAllowedToRetrieveManagedPassword MR1$
New-ADServiceAccount : Identity info provided in the extended attribute: 'PrincipalsAllowedToRetrieveManagedPassword'
could not be resolved. Reason: 'Cannot find an object with identity: 'MR1$' under: 'DC=hdg,DC=com'.'.
At line:1 char:1
+ New-ADServiceAccount -name svc-FRPS$ -DnsHostName svc-FRPS.hdg.com -P ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidData: (CN=svc-FRPS$,CN...s,DC=hdg,DC=com:String) [New-ADServiceAccount], ADIdenti
   tyResolutionException
    + FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityResolutionException
   ,Microsoft.ActiveDirectory.Management.Commands.NewADServiceAccount

New-ADServiceAccount -name svc-FRCO$ -DnsHostName svc-FRCO.hdg.com -PrincipalsAllowedToRetrieveManagedPassword MR1$
New-ADServiceAccount : Identity info provided in the extended attribute: 'PrincipalsAllowedToRetrieveManagedPassword'
could not be resolved. Reason: 'Cannot find an object with identity: 'MR1$' under: 'DC=hdg,DC=com'.'.
At line:1 char:1
+ New-ADServiceAccount -name svc-FRCO$ -DnsHostName svc-FRCO.hdg.com -P ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidData: (CN=svc-FRCO$,CN...s,DC=hdg,DC=com:String) [New-ADServiceAccount], ADIdenti
   tyResolutionException
    + FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityResolutionException
   ,Microsoft.ActiveDirectory.Management.Commands.NewADServiceAccount

New-ADServiceAccount -name svc-ReportSvc$ -DnsHostName svc-ReportSvc.hdg.com -PrincipalsAllowedToRetrieveManagedPassword
 SSRS$
New-ADServiceAccount : Key does not exist
At line:1 char:1
+ New-ADServiceAccount -name svc-ReportSvc$ -DnsHostName svc-ReportSvc. ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : NotSpecified: (CN=svc-ReportSv...s,DC=hdg,DC=com:String) [New-ADServiceAccount], ADExcep
   tion
    + FullyQualifiedErrorId : ActiveDirectoryServer:-2146893811,Microsoft.ActiveDirectory.Management.Commands.NewADSer
   viceAccount
```

3. If you must make changes to accounts or machines, update the **ConfigTemplate.xml** file in the original **infrastructure** folder, copy it to this machine, and then run the following command.

Update-D365FOGMSAAccounts -ConfigurationFilePath .₩ConfigTemplate.xml

1.10 Configure certificates

1. Go to the machine that you originally unzipped the infrastructure folder to.

2. If you must generate certificates, run the following commands. These commands create the certificate templates in AD CS, generate the certificates from the templates, put the certificates in

the **CurrentUser₩My** certificate store on the machine, and update the thumbprints in the XML file.

```
# If you must create self-signed certs, set the generateSelfSignedCert attribute to true.

#.₩New-SelfSignedCertificates.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml


.₩New-ADCSCertificates.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml -CreateTemplates

.₩New-ADCSCertificates.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml
```

- We must run these commands on **domain controller machine**.

3. Export the Cretificates in to .pfx files. As part of the export process, the following command will check that the correct cryptographic provider is set for your certificates.

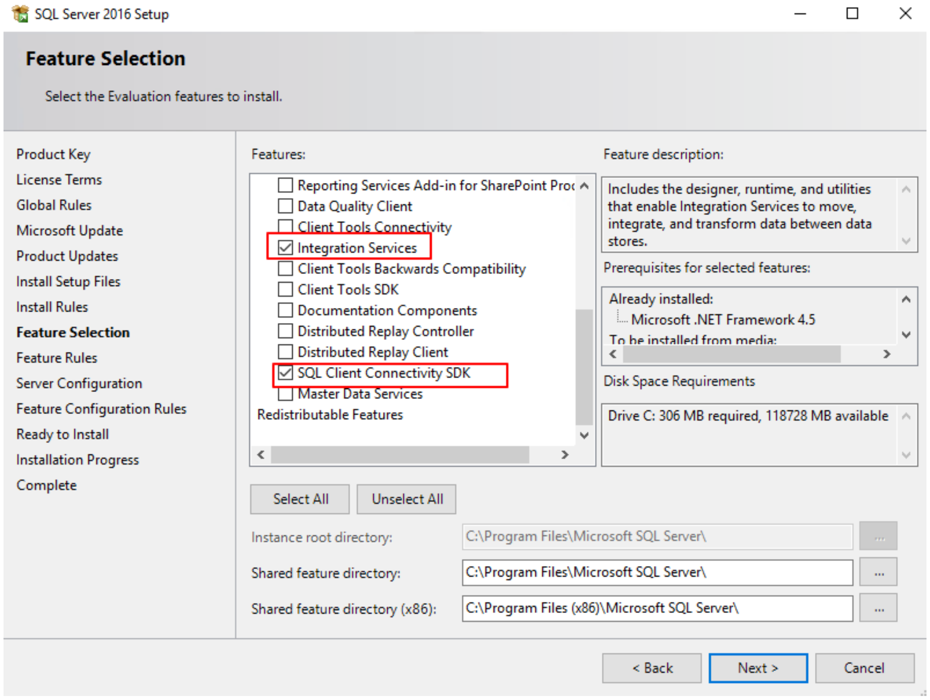
```
# Exports .pfx files into a directory VMs₩<VMName>. All the certs will be written to the infrastructure₩Certs folder.

.₩Export-PfxFiles.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml
```

1.11 Set up SSIS

To enable Data management and SSIS workloads, you must install SSIS on each AOS VM. Follow these steps on each AOS VM. (Ref. docs)

1. Verify that the machine has access to the SSIS installation, and open the **SSIS Setup** wizard.

2. On the **Feature Selection** page, in the **Features** pane, select the **Integration Services** and **SQL Client Connectivity SDK** checkboxes.



SQL Server 2016 Setup

Feature Selection

Select the Evaluation features to install.

- Product Key
- License Terms
- Global Rules
- Microsoft Update
- Product Updates
- Install Setup Files
- Install Rules
- **Feature Selection**
- Feature Rules
- Server Configuration
- Feature Configuration Rules
- Ready to Install
- Installation Progress
- Complete

Features:

☐ Reporting Services Add-in for SharePoint Proc
☐ Data Quality Client
☐ Client Tools Connectivity
☑ Integration Services
☐ Client Tools Backwards Compatibility
☐ Client Tools SDK
☐ Documentation Components
☐ Distributed Replay Controller
☐ Distributed Replay Client
☑ SQL Client Connectivity SDK
☐ Master Data Services
Redistributable Features

Feature description:

Includes the designer, runtime, and utilities that enable Integration Services to move, integrate, and transform data between data stores.

Prerequisites for selected features:

Already installed:
Microsoft .NET Framework 4.5
To be installed from media:

Disk Space Requirements

Drive C: 306 MB required, 118728 MB available

Instance root directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

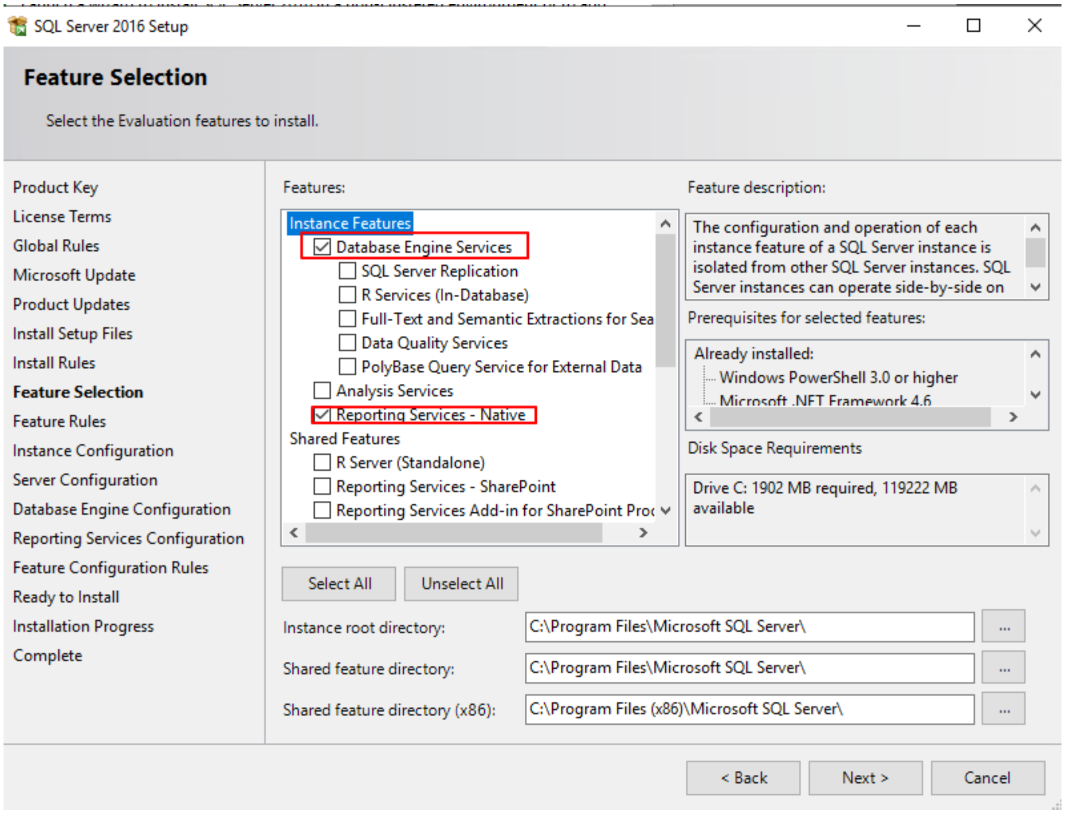
3. Complete the setup, and verify that the installation was successful.

1.12 Set up SSRS

SQL Server must be installed on the SSRS machines. SSRS must be installed in Native mode on the SSRS machines.(Ref. docs)

Do not configure the SSRS instance. The reporting service will automatically configure everything.

1. On the Feature Selection page, select **Database Engine Services, Reporting Services - Native**



SQL Server 2016 Setup

Feature Selection

Select the Evaluation features to install.

Features:

Instance Features
- ☑ Database Engine Services
  - ☐ SQL Server Replication
  - ☐ R Services (In-Database)
  - ☐ Full-Text and Semantic Extractions for Sea
  - ☐ Data Quality Services
  - ☐ PolyBase Query Service for External Data
- ☐ Analysis Services
- ☑ Reporting Services - Native

Shared Features
- ☐ R Server (Standalone)
- ☐ Reporting Services - SharePoint
- ☐ Reporting Services Add-in for SharePoint Proc

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on

Prerequisites for selected features:

Already installed:
- Windows PowerShell 3.0 or higher
- Microsoft .NET Framework 4.6

Disk Space Requirements

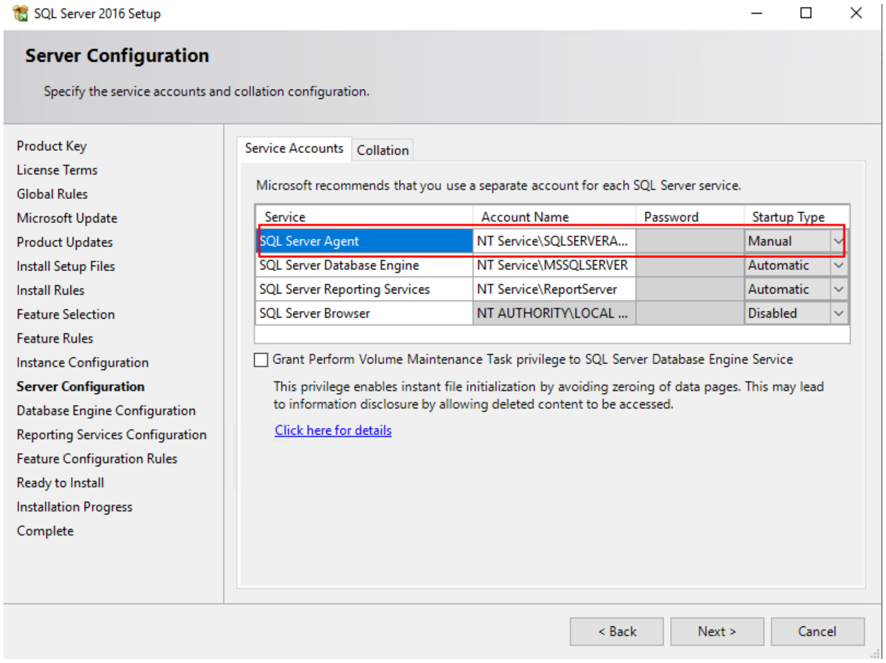
Drive C: 1902 MB required, 119222 MB available

Instance root directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\

2. On the Server Configuration, if you plan to use the Reporting Services subscription feature, then on the Server Configuration page, configure SQL Server Agent Automatic Startup type. The default is manual.



SQL Server 2016 Setup

Server Configuration

Specify the service accounts and collation configuration.

Microsoft recommends that you use a separate account for each SQL Server service.

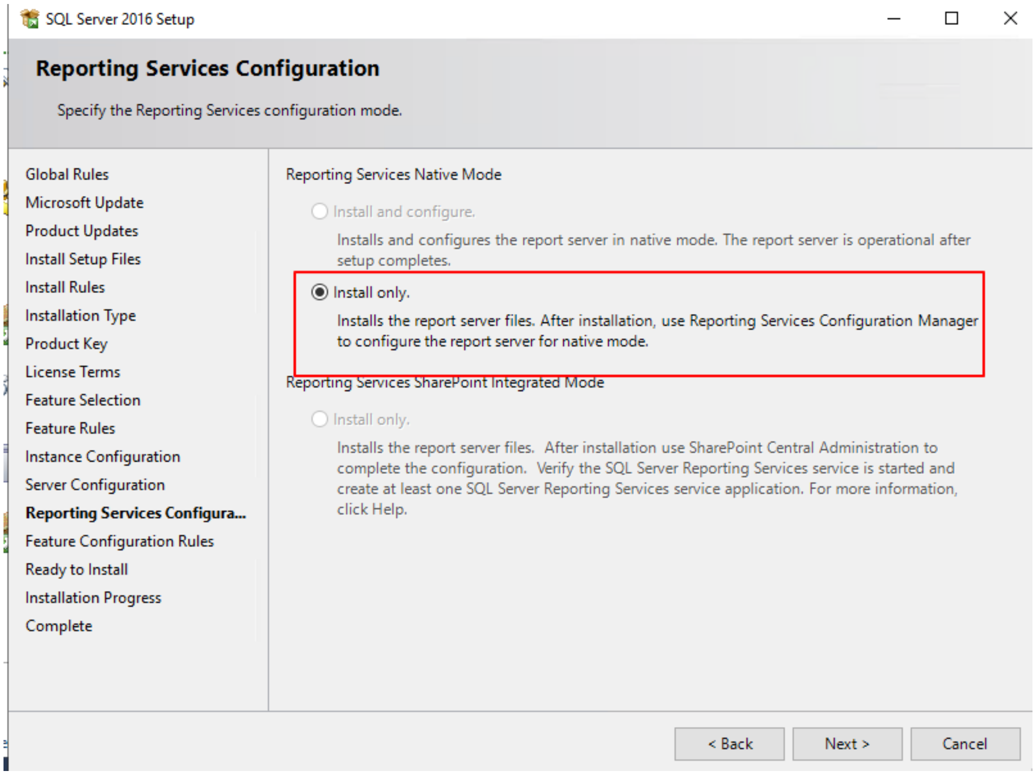
Service	Account Name	Password	Startup Type
SQL Server Agent	NT Service\SQLSERVERA...		Manual
SQL Server Database Engine	NT Service\MSSQLSERVER		Automatic
SQL Server Reporting Services	NT Service\ReportServer		Automatic
SQL Server Browser	NT AUTHORITY\LOCAL ...		Disabled

☐ Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service

This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.

Click here for details

3. On the Reporting Services Configuration page select Install only.



Reporting Services Configuration

Specify the Reporting Services configuration mode.

Reporting Services Native Mode

○ Install and configure.

Installs and configures the report server in native mode. The report server is operational after setup completes.

● Install only.

Installs the report server files. After installation, use Reporting Services Configuration Manager to configure the report server for native mode.

Reporting Services SharePoint Integrated Mode

○ Install only.

Installs the report server files. After installation use SharePoint Central Administration to complete the configuration. Verify the SQL Server Reporting Services service is started and create at least one SQL Server Reporting Services service application. For more information, click Help.

4. SSRS should be configured manually according to Configure SQL Server Reporting Services for on-premises deployments.

5. After SSRS in installed, copy the infrastructure folder. Then open Windows PowerShell in elevated mode, and go to the folder.

6. Run the following commands.

```
.₩Initialize-Database.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml -ComponentName BI
```

```
.₩Configure-Database.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml -ComponentName BI
```

- The Initialize-Database.ps1 script maps the gMSA to the following databases and roles.

User	Database	Database role
svc-ReportSvc$	master	db_owner
svc-ReportSvc$	msdb	db_datareader, db_datawriter, db_securityadmin

- The Configure-Database.ps1 script performs the following action
  - Grant the CREATE ANY DATABASE permission to [contoso₩svc-ReportSvc$]

1.13 Set up VMs

1. Running following code to export the scripts

```
# Exports the script files to be executed on each VM into a directory VMs₩<VMName>.
.₩Export-Scripts.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml
```

2. Download the following Microsoft Windows Installers (MSIs) into a file share that is accessible by all VMs.

Component	Download Link	Expected file name
SNAC – ODBC driver 13	ODBC Driver 13.1	msodbcsql.msi
SNAC – ODBC driver 17.5.x	ODBC Driver 17.5.2	msodbcsql_17.msi
SQL Server Management Studio 17.9.1	SSMS 17.9.1	SSMS-Setup-*.exe
Visual C++ Redistributable Packages for Microsoft Visual Studio 2013	https://support.microsoft.com/help/3179560	vcredist_x64.exe
Visual C++ Redistributable Packages for Microsoft Visual Studio 2017	Go to https://lcs.dynamics.com/V2/SharedAssetLibrary, select Model as the asset type, and then select VC++ 17 Redistributables.	vc_redist.x64_14_16_27024.exe
Access Database Engine 2010 Redistributable	https://www.microsoft.com/download/details.aspx?id=13255	AccessDatabaseEngine_x64.exe

The .NET Framework version 4.8 (CLR 4.0)	https://dotnet.microsoft.com/download/thank-you/net48-offline	ndp48-x86-x64-allos-enu.exe
The .NET Framework version 4.7.2 (CLR 4.0)	https://dotnet.microsoft.com/download/thank-you/net472-offline	ndp472-x86-x64-allos-enu.exe

- When you download VC++ 17 Redistributables, the executable file is inside the zip file.

3. Copy the contents of each **infrastructure₩VMs₩<VMName>** folder to the corresponding VM. Then run the following command as an administrator.

```
.₩Configure-PreReqs.ps1 -MSIFilePath <path of the MSIs>
```

4. Each time that you're prompted, restart the machine. Make sure that you rerun the .₩Configure-PreReqs.ps1 command after each restart, until all the prerequisites are installed.

5. Run the following command to complete the VM setup.

```
.₩Complete-PreReqs.ps1
```

```
.₩Test-D365FOConfiguration.ps1
```

1.14 Set up a standalone Service Fabric cluster

1. Download the Service Fabric standalone installation package to one of your Service Fabric nodes.

2. After the zip file is downloaded, select and hold (or right-click) it, and then select **Properties**. In the **Properties** dialog box, select the **Unblock** checkbox.

3. Copy the zip file to one of the nodes in the Service Fabric cluster, and unzip it. Make sure that the **infrastructure** folder has access to this folder.

4. Go to the infrastructure folder, and run the following command to generate the Service Fabric **ClusterConfig.json** file.

```
.₩New-SFClusterConfig.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml -TemplateConfig <ServiceFabricStandaloneInstallerPath>₩ClusterConfig.X509.MultiMachine.json
```

5. Copy the ClusterConfig.json file that is generated to <ServiceFabricStandaloneInstallerPath>.

6. Open Windows PowerShell in elevated mode, go to <ServiceFabricStandaloneInstallerPath>, and run the following command to test the ClusterConfig.json file.

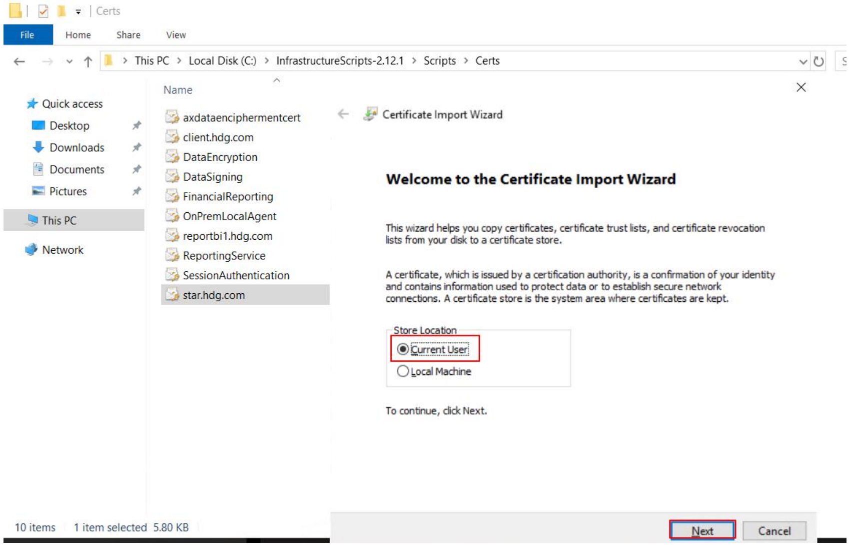
```
.₩TestConfiguration.ps1 -ClusterConfigFilePath .₩clusterConfig.json
```

7. If the test is successful, run the following command to deploy the cluster.

```
.₩CreateServiceFabricCluster.ps1 -ClusterConfigFilePath .₩ClusterConfig.json
```

8. After the cluster is created, open Service Fabric Explorer on any client machine, and validate the installation:

   A. Install the Service Fabric client certificate in the **CurrentUser₩My** certificate store if it isn't already installed.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
● Current User
○ Local Machine

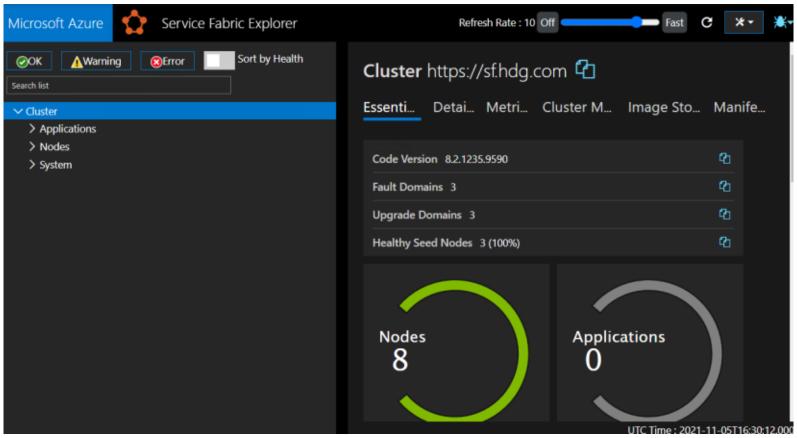
To continue, click Next.

   B. In Internet Explorer, select **Tools** (the gear symbol), and then select **Compatibility View settings**. Clear the **Display intranet sites in Compatibility View** checkbox.

   C. Go to https://sf.hdg.com:19080, where sf.hdg.com is the host name of the Service Fabric cluster that is specified in the zone. If DNS name resolution isn't configured, use the IP address of the machine.

   D. Select the client certificate. The **Service Fabric Explorer** page appears.

   E. Verify that all nodes appear as green.

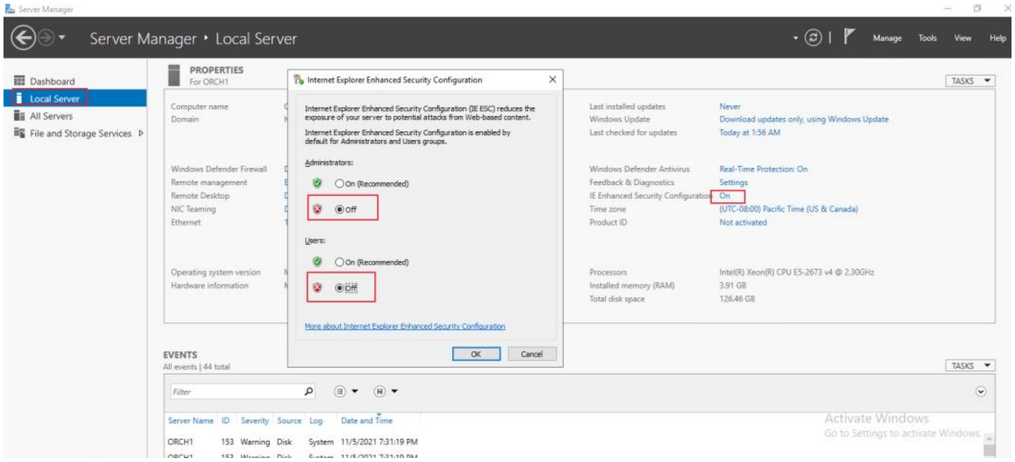


Cluster https://sf.hdg.com

Code Version 8.2.1235.9590
Fault Domains 3
Upgrade Domains 3
Healthy Seed Nodes 3 (100%)

UTC Time : 2021-11-05T16:30:12.000

- If you run this in a server machine like Windows Server 2016, you must turn off the IE Enhanced Security Configuration temporarily. If you don't, the Azure login window content will be blocked.



Computer name
Domain
Windows Defender Firewall
Remote management
Remote Desktop
NIC Teaming
Ethernet
Operating system version
Hardware information

Last installed updates: Never
Windows Update: Download updates only, using Windows Update
Last checked for updates: Today at 1:56 AM
Windows Defender Antivirus: Real-Time Protection: On
Feedback & Diagnostics: Settings
IE Enhanced Security Configuration: On
Time zone: (UTC-08:00) Pacific Time (US & Canada)
Product ID: Not activated
Processors: Intel(R) Xeon(R) CPU E5-2673 v4 @ 2.30GHz
Installed memory (RAM): 3.91 GB
Total disk space: 126.46 GB

Internet Explorer Enhanced Security Configuration

Internet Explorer Enhanced Security Configuration (IE ESC) reduces the exposure of your server to potential attacks from Web-based content.

Internet Explorer Enhanced Security Configuration is enabled by default for Administrators and Users groups.

Administrators:
○ On (Recommended)
● Off

Users:
○ On (Recommended)
● Off

More about Internet Explorer Enhanced Security Configuration

OK Cancel

Server Name	ID	Severity	Source	Log	Date and Time
ORCH1	153	Warning	Disk	System	11/5/2021 7:31:19 PM

1.15 LCS Connectivity for the tenant

An on-premises local agent is used to orchestrate deployment and servicing of Finance + Operations through LCS. To establish connectivity from LCS to the Finance + Operations tenant, you must configure a certificate that enables the local agent to act on behalf on your Azure AD tenant (for example, contoso.onmicrosoft.com).

Use the on-premises agent certificate that you acquired from a CA or the self-signed certificate that you generated by using scripts. The on-premises agent certificate can be reused across multiple sandbox and production environments per tenant.

Only user accounts that have the **Global Administrator directory role** can add certificates to authorize LCS.

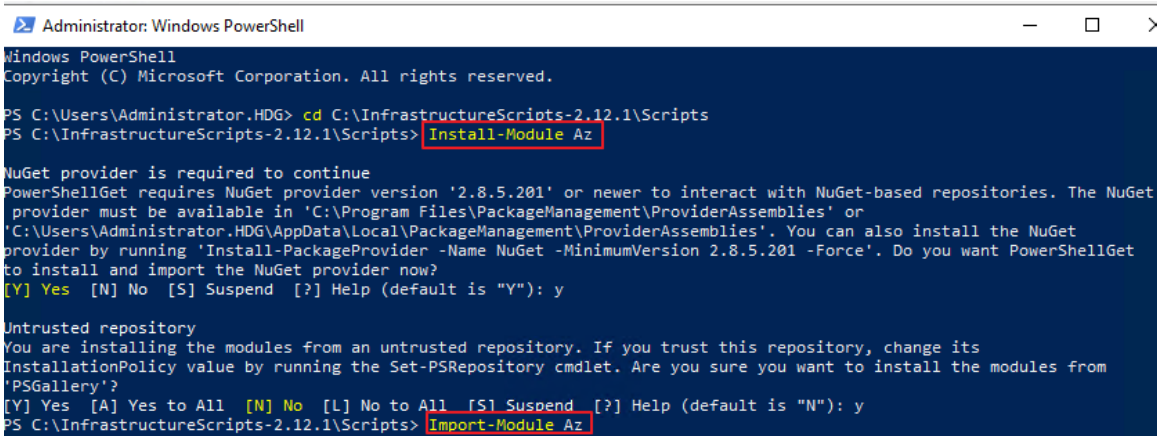
1. Determine whether the certificate is already registered by running the following script from the

Infrastructure folder.

Install-Module Az

Import-Module Az

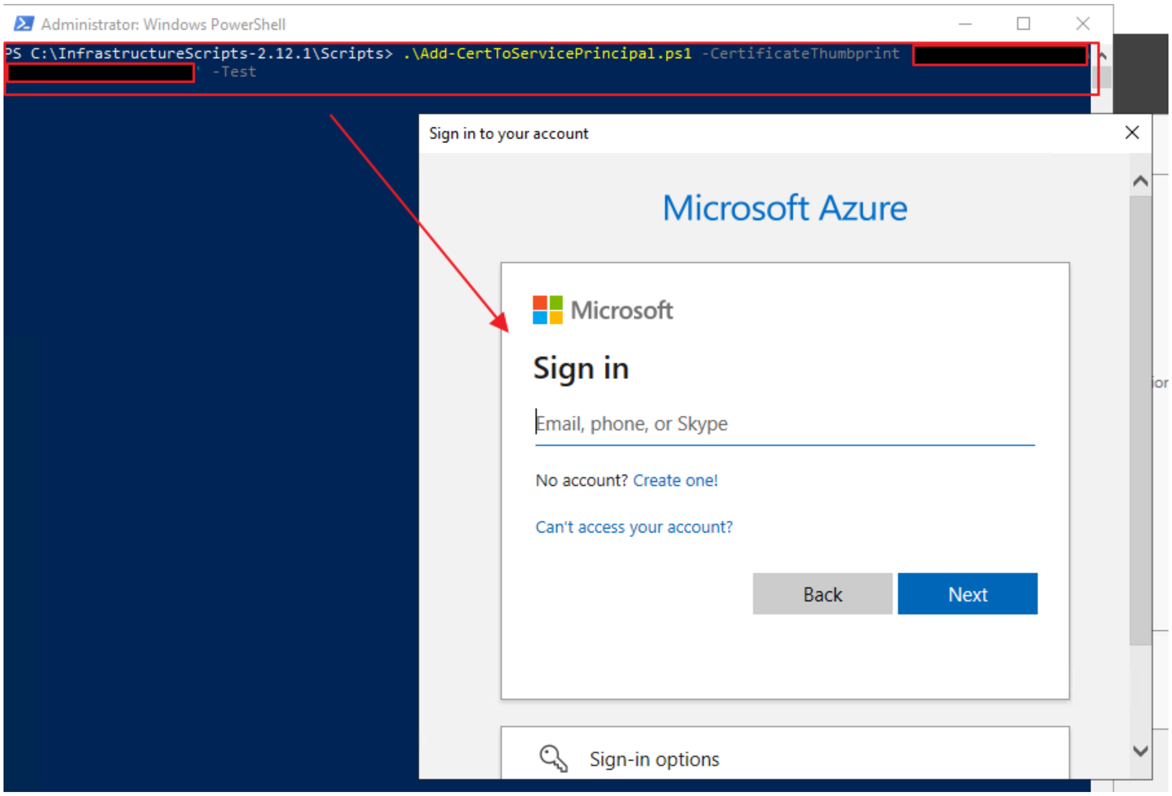
.₩Add-CertToServicePrincipal.ps1 -CertificateThumbprint 'OnPremLocalAgent Certificate Thumbprint' -Test



Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.HDG> cd C:\InfrastructureScripts-2.12.1\Scripts
PS C:\InfrastructureScripts-2.12.1\Scripts> Install-Module Az

NuGet provider is required to continue
PowerShellGet requires NuGet provider version '2.8.5.201' or newer to interact with NuGet-based repositories. The NuGet
 provider must be available in 'C:\Program Files\PackageManagement\ProviderAssemblies' or
'C:\Users\Administrator.HDG\AppData\Local\PackageManagement\ProviderAssemblies'. You can also install the NuGet
provider by running 'Install-PackageProvider -Name NuGet -MinimumVersion 2.8.5.201 -Force'. Do you want PowerShellGet
to install and import the NuGet provider now?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y

Untrusted repository
You are installing the modules from an untrusted repository. If you trust this repository, change its
InstallationPolicy value by running the Set-PSRepository cmdlet. Are you sure you want to install the modules from
'PSGallery'?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "N"): y
PS C:\InfrastructureScripts-2.12.1\Scripts> Import-Module Az
```

- Login User that have global Administrator role.



Administrator: Windows PowerShell

```
PS C:\InfrastructureScripts-2.12.1\Scripts> .\Add-CertToServicePrincipal.ps1 -CertificateThumbprint [redacted]
' -Test
```

- If you have multiple tenants that are associated with the login account, you can run the following command to pass the tenant ID as a parameter. In this way, you can ensure that the context is set to the correct tenant.

```
.₩Add-CertToServicePrincipal.ps1 -CertificateThumbprint 'OnPremLocalAgent Certificate Thumbprint' -TenantId 'xxxx-xxxx-xxxx-xxxx'
```

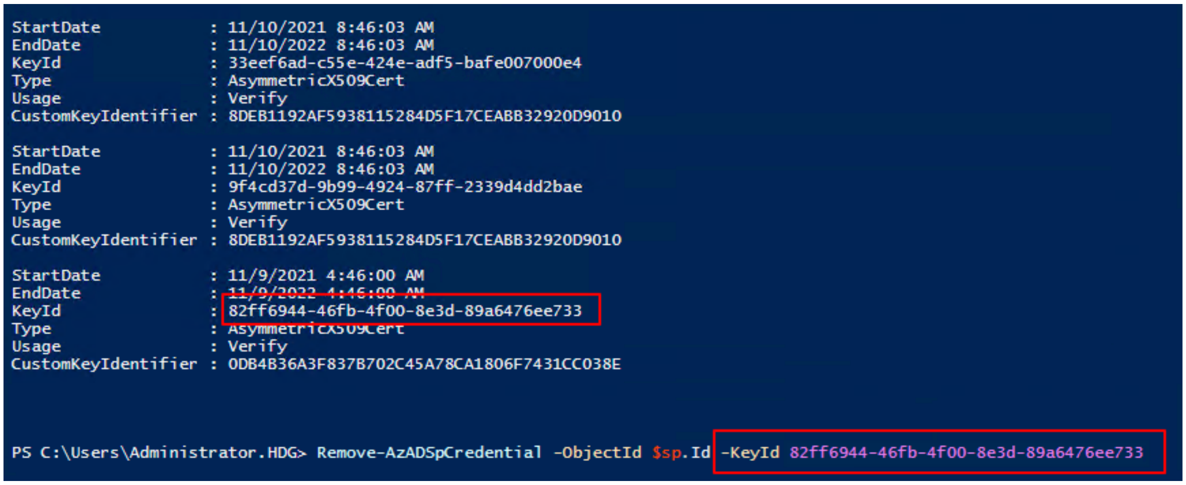
2. If the script indicates that the certificate isn't registered, run the following command.

```
.₩Add-CertToServicePrincipal.ps1 -CertificateThumbprint 'OnPremLocalAgent Certificate Thumbprint'
```

- You can get registered certificate list, run follow code

```
Connect-AzAccount
# If you have Multi Tenant
# Connect-AzAccount -TenantId 'Your TenantId'
$sp = Get-AzADServicePrincipal -ServicePrincipalName 00000015-0000-0000-c000-000000000000
Get-AzADSpCredential -ObjectId $sp.Id
```

➔ If there is active but non-used certificate, Remove that to use follow code.



```
StartDate           : 11/10/2021 8:46:03 AM
EndDate             : 11/10/2022 8:46:03 AM
KeyId               : 33eef6ad-c55e-424e-adf5-bafe007000e4
Type                : AsymmetricX509Cert
Usage               : Verify
CustomKeyIdentifier : 8DEB1192AF5938115284D5F17CEABB32920D9010

StartDate           : 11/10/2021 8:46:03 AM
EndDate             : 11/10/2022 8:46:03 AM
KeyId               : 9f4cd37d-9b99-4924-87ff-2339d4dd2bae
Type                : AsymmetricX509Cert
Usage               : Verify
CustomKeyIdentifier : 8DEB1192AF5938115284D5F17CEABB32920D9010

StartDate           : 11/9/2021 4:46:00 AM
EndDate             : 11/9/2022 4:46:00 AM
KeyId               : 82ff6944-46fb-4f00-8e3d-89a6476ee733
Type                : AsymmetricX509Cert
Usage               : Verify
CustomKeyIdentifier : 0DB4B36A3F837B702C45A78CA1806F7431CC038E


PS C:\Users\Administrator.HDG> Remove-AzADSpCredential -ObjectId $sp.Id -KeyId 82ff6944-46fb-4f00-8e3d-89a6476ee733
```

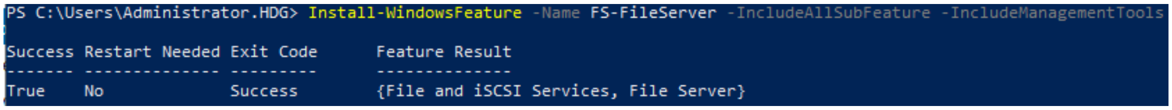
```
Remove-AzADSpCredential -ObjectId $sp.Id -KeyId 'Insert Key Id that you want to delete'
```

1.16 Set up file storage

- A file share that stores user documents that are uploaded to AOS (for example, ₩₩DAX7SQLAOFILE1₩aos-storage).
- A file share that stores the latest build and configuration files to orchestrate the deployment (for example, ₩₩DAX7SQLAOFILE1₩agent).

1. On the file share machine, run the following command.

Install-WindowsFeature -Name FS-FileServer -IncludeAllSubFeature -IncludeManagementTools

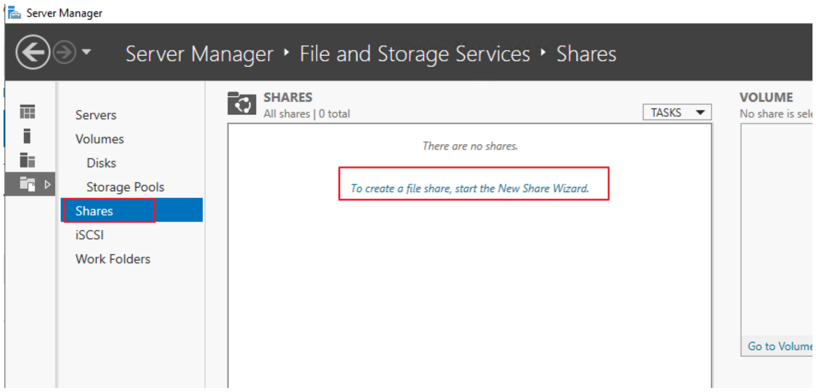


```
PS C:\Users\Administrator.HDG> Install-WindowsFeature -Name FS-FileServer -IncludeAllSubFeature -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {File and iSCSI Services, File Server}
```

2. Follow these steps to set up the **₩₩DAX7SQLAOFILE1₩aos-storage** file share:

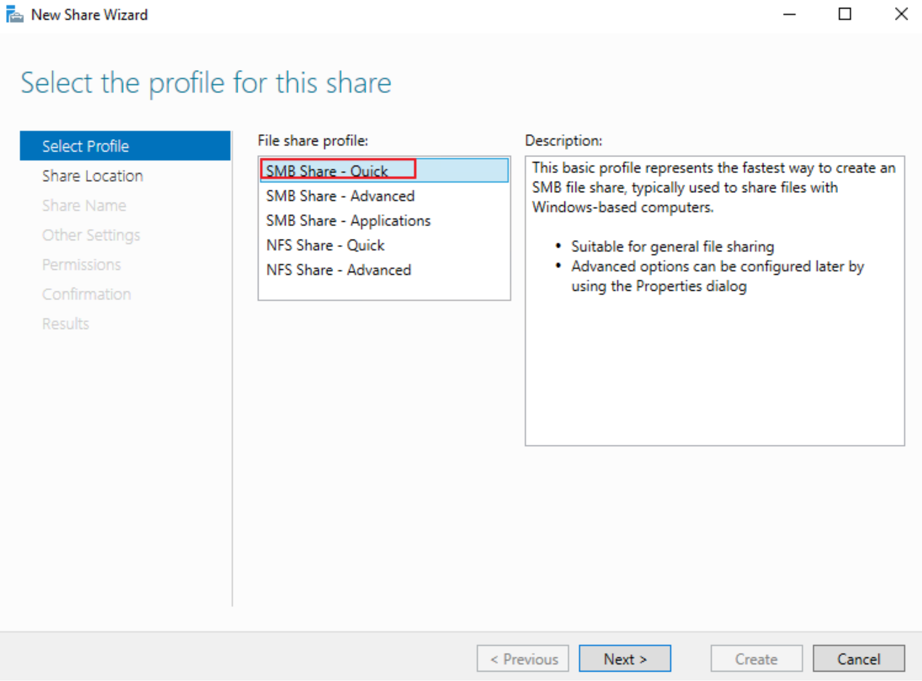
   A. In Server Manager, select **File and Storage Services** > **Shares**. (If Share page doesn't appear, restart server)

   B. Select **Tasks** > **New Share** to create a new share. Name the share **aos-storage**.



There are no shares.

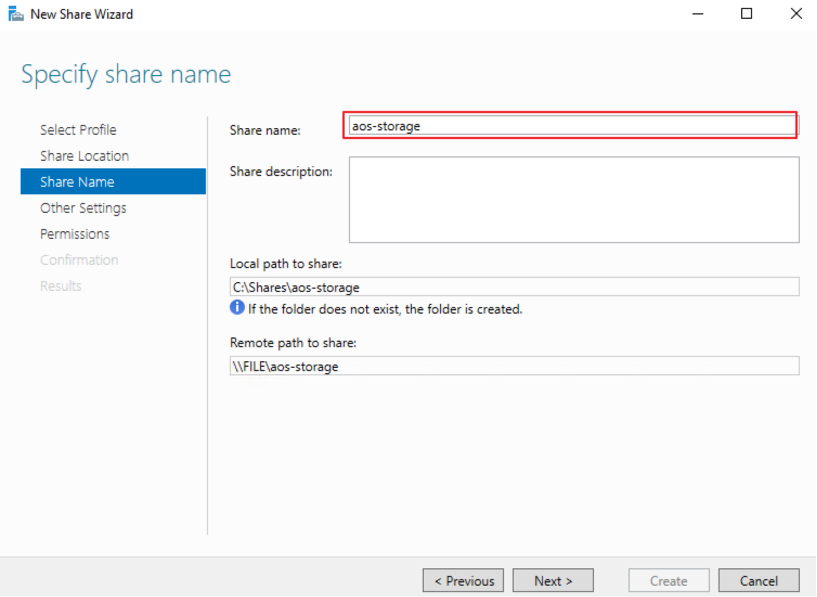
To create a file share, start the New Share Wizard.



Select the profile for this share

This basic profile represents the fastest way to create an SMB file share, typically used to share files with Windows-based computers.

- Suitable for general file sharing
- Advanced options can be configured later by using the Properties dialog



Specify share name

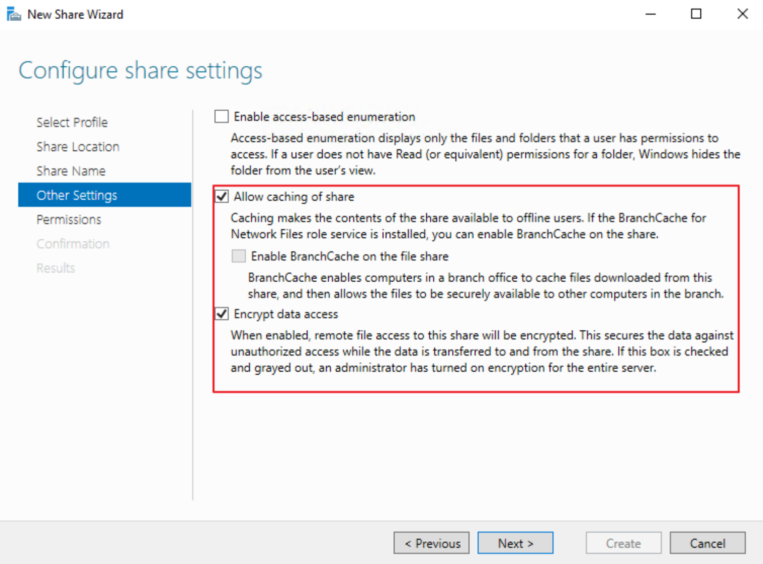
Share name: aos-storage

Share description:

Local path to share:
C:\Shares\aos-storage
If the folder does not exist, the folder is created.

Remote path to share:
\\FILE\aos-storage

C. Leave **Allow caching of share selected** and check **Encrypt data access**.



Configure share settings

□ Enable access-based enumeration

Access-based enumeration displays only the files and folders that a user has permissions to access. If a user does not have Read (or equivalent) permissions for a folder, Windows hides the folder from the user's view.

☑ Allow caching of share

Caching makes the contents of the share available to offline users. If the BranchCache for Network Files role service is installed, you can enable BranchCache on the share.

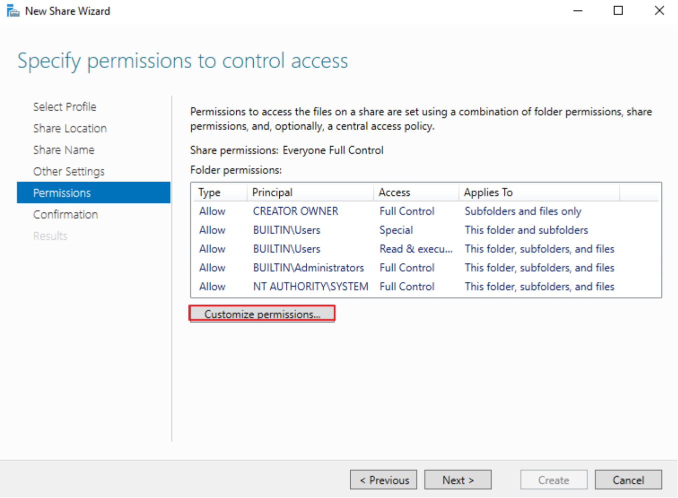
□ Enable BranchCache on the file share

BranchCache enables computers in a branch office to cache files downloaded from this share, and then allows the files to be securely available to other computers in the branch.

☑ Encrypt data access

When enabled, remote file access to this share will be encrypted. This secures the data against unauthorized access while the data is transferred to and from the share. If this box is checked and grayed out, an administrator has turned on encryption for the entire server.

D. Grant **Modify** permissions for every machine in the Service Fabric cluster except OrchestratorType. (You may need to enable **Computers** under **Object Types** to add machines or enable **Service Accounts** under **Object Types** to add service accounts.)



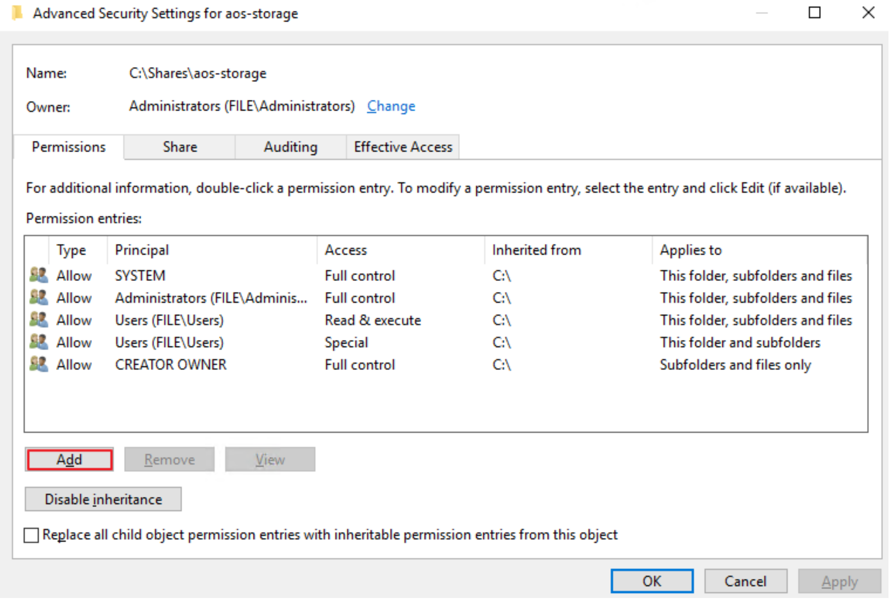
Specify permissions to control access

Permissions to access the files on a share are set using a combination of folder permissions, share permissions, and, optionally, a central access policy.

Share permissions: Everyone Full Control

Folder permissions:

Type	Principal	Access	Applies To
Allow	CREATOR OWNER	Full Control	Subfolders and files only
Allow	BUILTIN\Users	Special	This folder and subfolders
Allow	BUILTIN\Users	Read & execu...	This folder, subfolders, and files
Allow	BUILTIN\Administrators	Full Control	This folder, subfolders, and files
Allow	NT AUTHORITY\SYSTEM	Full Control	This folder, subfolders, and files



Name: C:\Shares\aos-storage

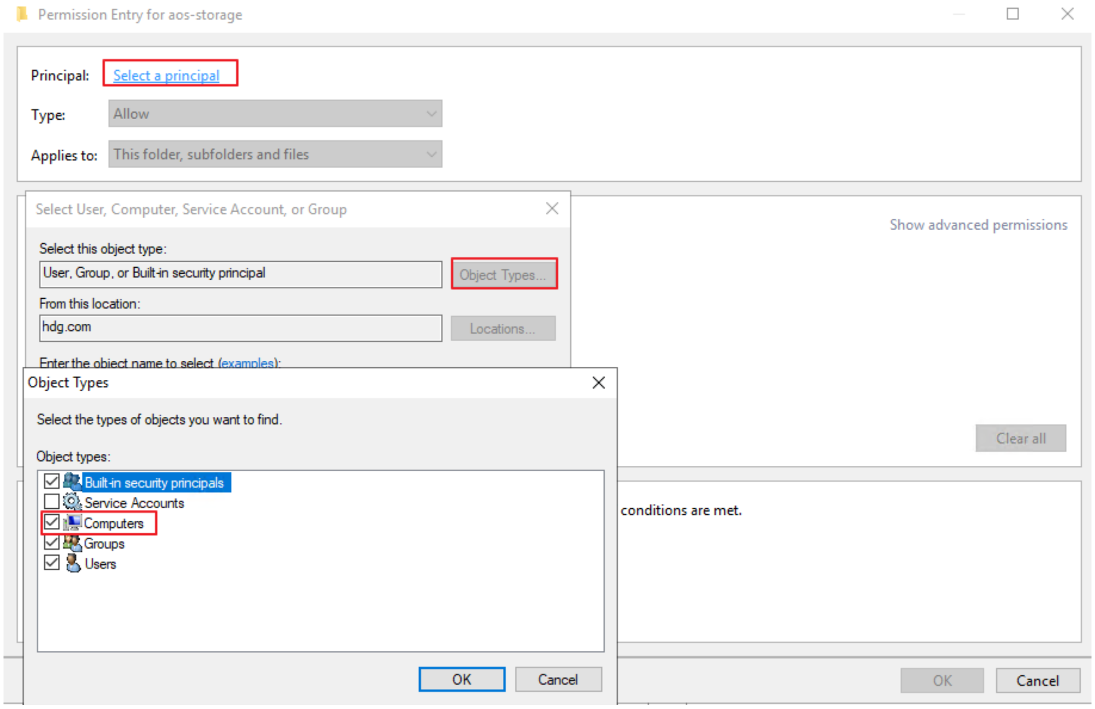
Owner: Administrators (FILE\Administrators)

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	SYSTEM	Full control	C:\	This folder, subfolders and files
Allow	Administrators (FILE\Adminis...	Full control	C:\	This folder, subfolders and files
Allow	Users (FILE\Users)	Read & execute	C:\	This folder, subfolders and files
Allow	Users (FILE\Users)	Special	C:\	This folder and subfolders
Allow	CREATOR OWNER	Full control	C:\	Subfolders and files only

□ Replace all child object permission entries with inheritable permission entries from this object



Permission Entry for aos-storage

Principal: Select a principal

Type: Allow

Applies to: This folder, subfolders and files

Select User, Computer, Service Account, or Group

Select this object type:

User, Group, or Built-in security principal

From this location:

hdg.com

Enter the object name to select (examples):

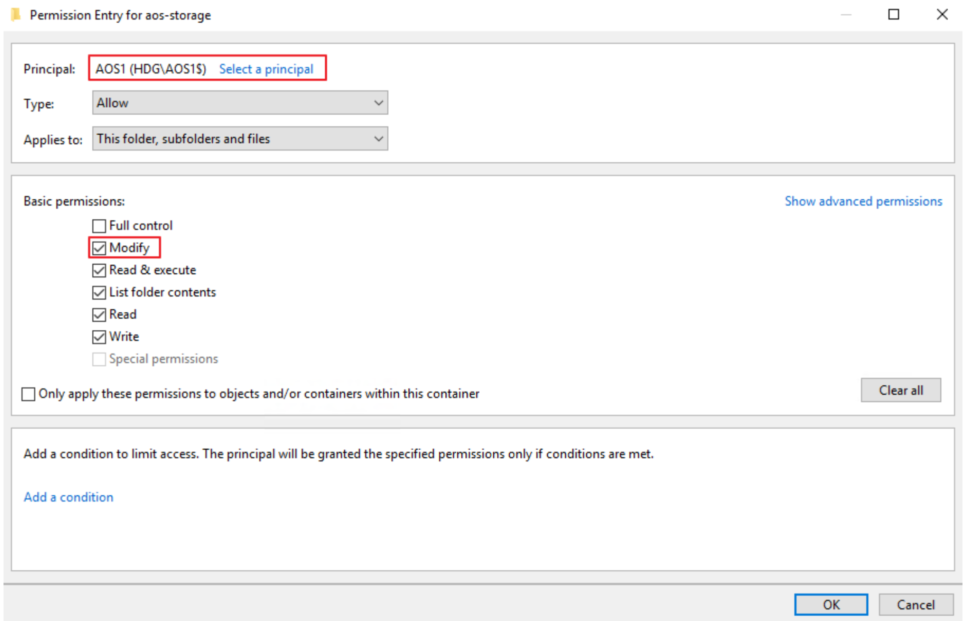
Object Types

Select the types of objects you want to find.

Object types:

- ☑ Built-in security principals
- ☐ Service Accounts
- ☑ Computers
- ☑ Groups
- ☑ Users

conditions are met.



Permission Entry for aos-storage

Principal: AOS1 (HDG\AOS1$) Select a principal

Type: Allow

Applies to: This folder, subfolders and files

Basic permissions:

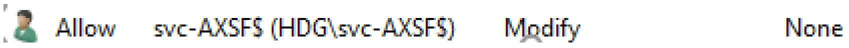
- ☐ Full control
- ☑ Modify
- ☑ Read & execute
- ☑ List folder contents
- ☑ Read
- ☑ Write
- ☐ Special permissions

☐ Only apply these permissions to objects and/or containers within this container

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

Add a condition

E. Grant **Modify** permissions for the gMSA user (**hdg₩svc-AXSF$).**



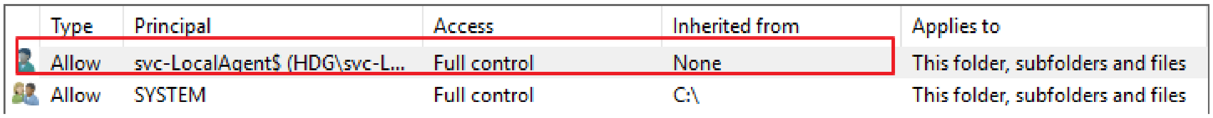
Allow svc-AXSF$ (HDG\svc-AXSF$) Modify None

3. Follow these steps to set up the ₩₩DAX7SQLAOFILE1₩agent file share:

A. In Server Manager, select **File and Storage Services > Shares.**

B. Select **Tasks > New Share** to create a new share. Name the share **agent**.

C. Grant **Full-Control** permissions to the gMSA user for the local deployment agent (contoso₩svc-LocalAgent$).

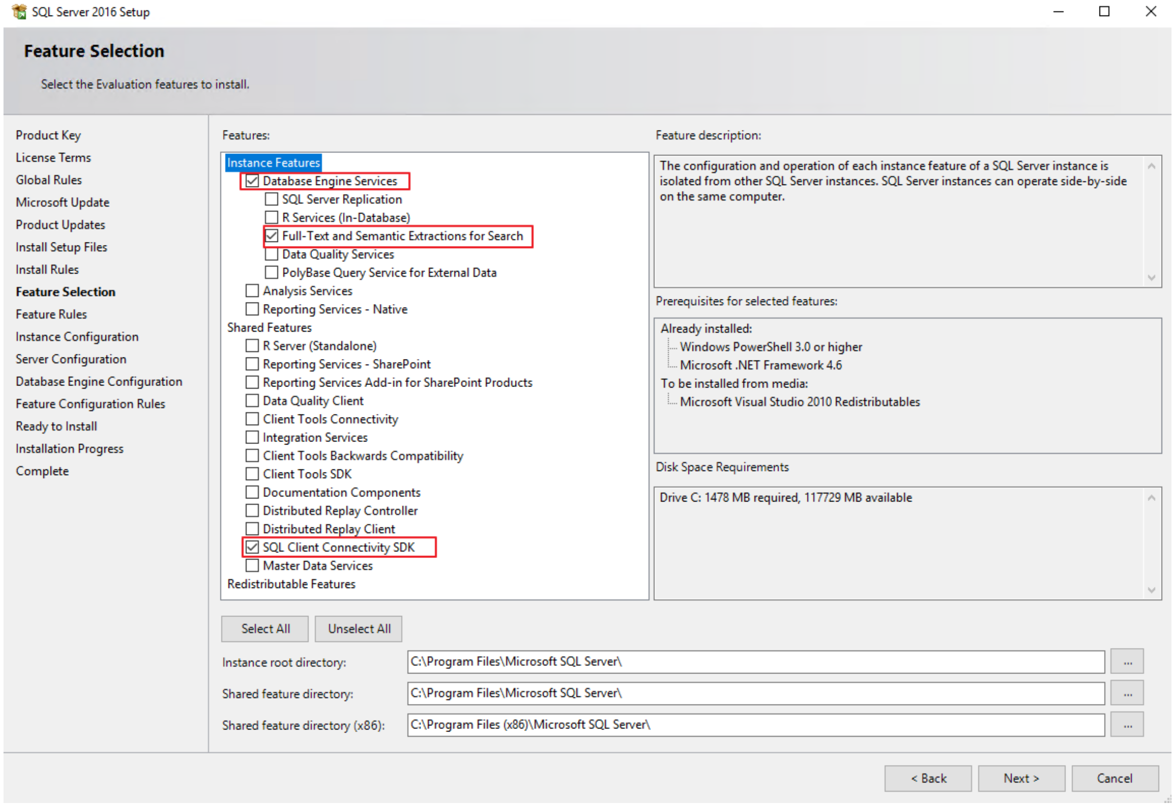


Type	Principal	Access	Inherited from	Applies to
Allow	svc-LocalAgent$ (HDG\svc-L...	Full control	None	This folder, subfolders and files
Allow	SYSTEM	Full control	C:\	This folder, subfolders and files

1.17 Set up SQL server

1. Install SQL Server 2016 SP2 with high availability. (Unless you're deploying in a sandbox environment, where one instance of SQL Server is sufficient. You may want to install SQL Server with high availability in sandbox environments to test high-availability scenarios.).

- You must enable the **SQL Server and Windows Authentication mode.**



SQL Server 2016 Setup

Feature Selection

Select the Evaluation features to install.

Features:

Instance Features
- ☑ Database Engine Services
  - □ SQL Server Replication
  - □ R Services (In-Database)
  - ☑ Full-Text and Semantic Extractions for Search
  - □ Data Quality Services
  - □ PolyBase Query Service for External Data
- □ Analysis Services
- □ Reporting Services - Native

Shared Features
- □ R Server (Standalone)
- □ Reporting Services - SharePoint
- □ Reporting Services Add-in for SharePoint Products
- □ Data Quality Client
- □ Client Tools Connectivity
- □ Integration Services
- □ Client Tools Backwards Compatibility
- □ Client Tools SDK
- □ Documentation Components
- □ Distributed Replay Controller
- □ Distributed Replay Client
- ☑ SQL Client Connectivity SDK
- □ Master Data Services

Redistributable Features

Feature description:

The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on the same computer.

Prerequisites for selected features:

Already installed:
- Windows PowerShell 3.0 or higher
- Microsoft .NET Framework 4.6

To be installed from media:
- Microsoft Visual Studio 2010 Redistributables

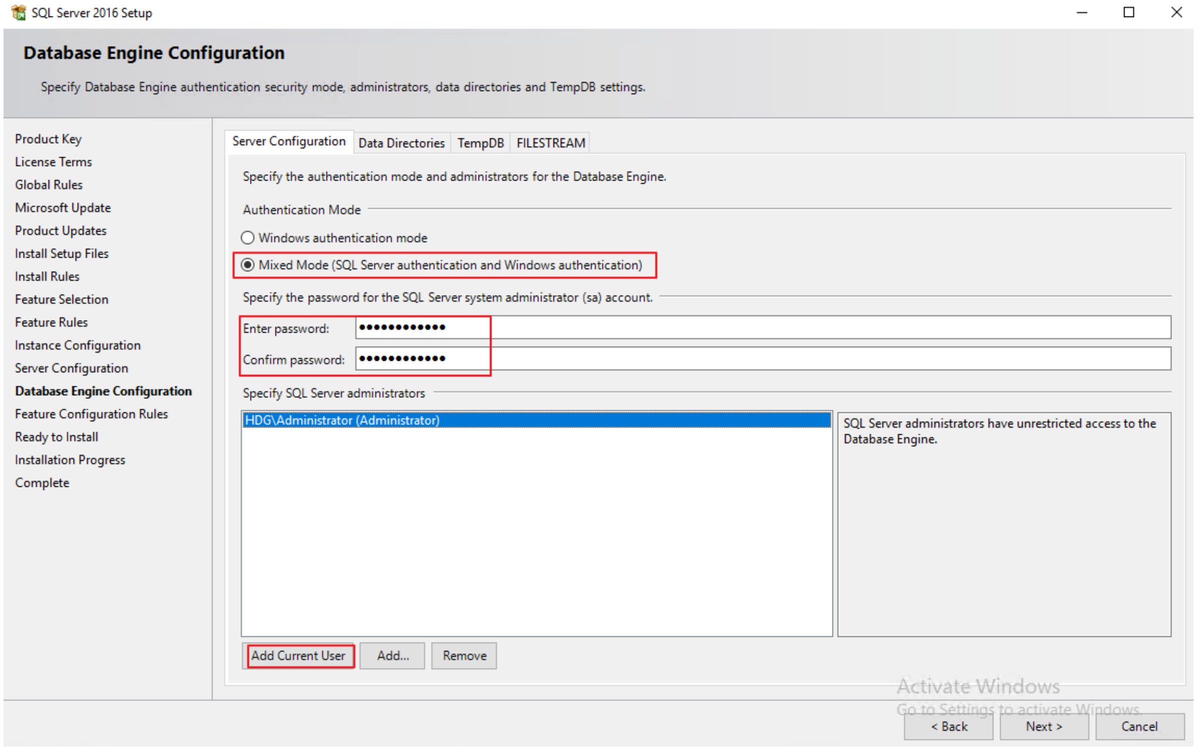
Disk Space Requirements

Drive C: 1478 MB required, 117729 MB available

Instance root directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory: C:\Program Files\Microsoft SQL Server\

Shared feature directory (x86): C:\Program Files (x86)\Microsoft SQL Server\



SQL Server 2016 Setup

Database Engine Configuration

Specify Database Engine authentication security mode, administrators, data directories and TempDB settings.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

○ Windows authentication mode

● Mixed Mode (SQL Server authentication and Windows authentication)

Specify the password for the SQL Server system administrator (sa) account.

Enter password: ●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●

Specify SQL Server administrators

HDG\Administrator (Administrator)

SQL Server administrators have unrestricted access to the Database Engine.

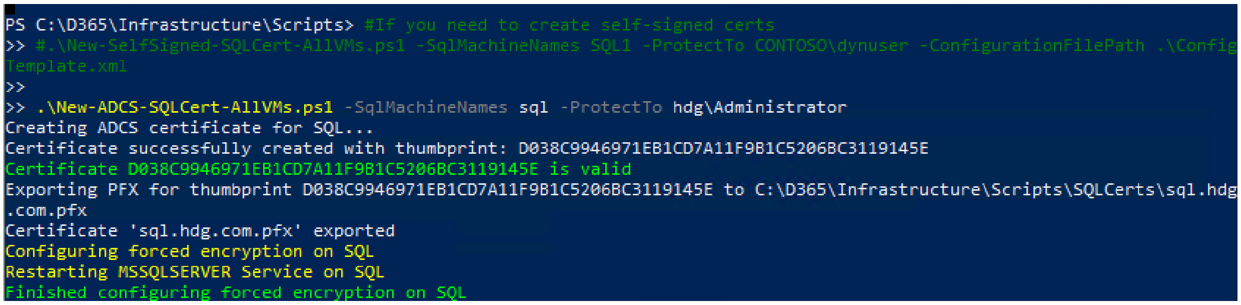
2. Verify that the Database Engine, SSRS, Full-Text Search, and SQL Server Management Tools are already installed.

3. Run the SQL service as a domain user or a group-managed service account.

4. Get an SSL certificate from a certificate authority to configure SQL Server for Finance + Operations. For testing purposes, you can create and use a self-signed certificate or an AD CS certificate. You will need to replace the computer name and domain name in the following examples. Run follow code in **domain controller server**.

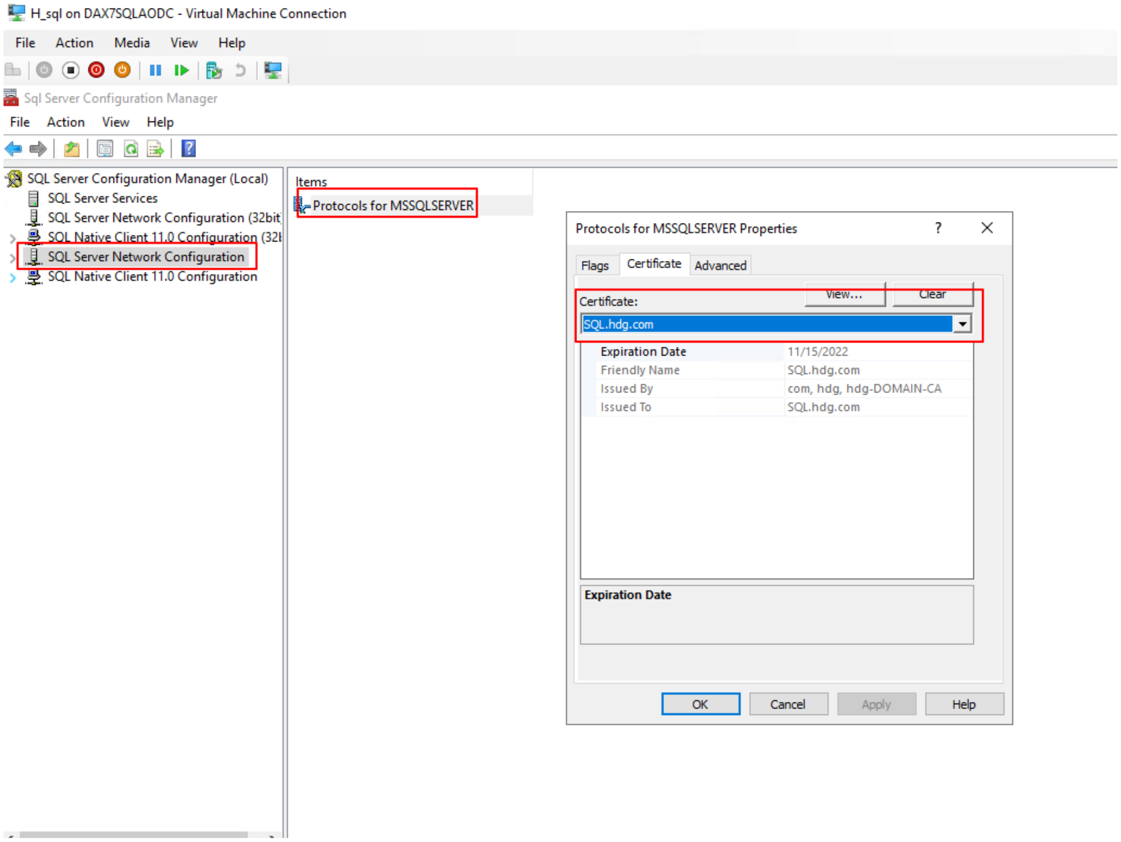
   AD CS certificate for a single SQL availability group

   .₩New-ADCS-SQLCert-AllVMs.ps1 -SqlMachineNames SQL1 -ProtectTo CONTOSO₩dynuser



```
PS C:\D365\Infrastructure\Scripts> #If you need to create self-signed certs
>> #.\New-SelfSigned-SQLCert-AllVMs.ps1 -SqlMachineNames SQL1 -ProtectTo CONTOSO\dynuser -ConfigurationFilePath .\Config
Template.xml
>>
>> .\New-ADCS-SQLCert-AllVMs.ps1 -SqlMachineNames sql -ProtectTo hdg\Administrator
Creating ADCS certificate for SQL...
Certificate successfully created with thumbprint: D038C9946971EB1CD7A11F9B1C5206BC3119145E
Certificate D038C9946971EB1CD7A11F9B1C5206BC3119145E is valid
Exporting PFX for thumbprint D038C9946971EB1CD7A11F9B1C5206BC3119145E to C:\D365\Infrastructure\Scripts\SQLCerts\sql.hdg
.com.pfx
Certificate 'sql.hdg.com.pfx' exported
Configuring forced encryption on SQL
Restarting MSSQLSERVER Service on SQL
Finished configuring forced encryption on SQL
```

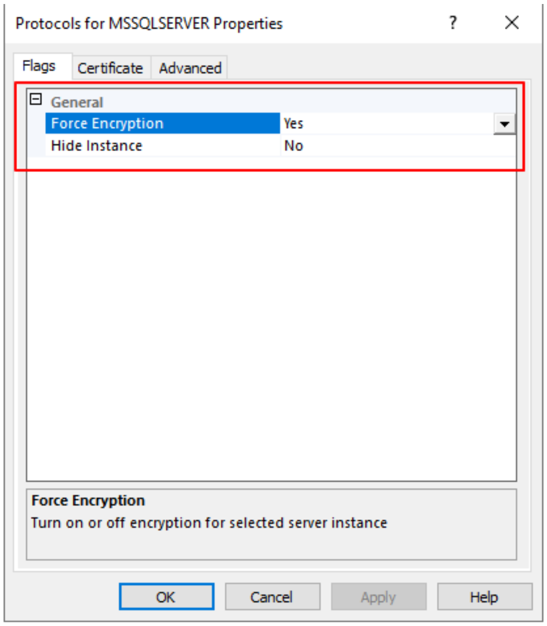
5. Make sure that certificate is setup in SQL server and Force Encryption is Yes.


H_sql on DAX7SQLAODC - Virtual Machine Connection
File Action Media View Help
Sql Server Configuration Manager
File Action View Help
SQL Server Configuration Manager (Local)
SQL Server Services
SQL Server Network Configuration (32bit
SQL Native Client 11.0 Configuration (32
SQL Server Network Configuration
SQL Native Client 11.0 Configuration
Items
Protocols for MSSQLSERVER
Protocols for MSSQLSERVER Properties
Flags
Certificate
Advanced
View...
Clear
OK
Cancel
Apply
Help

Certificate: SQL.hdg.com

Expiration Date	11/15/2022
Friendly Name	SQL.hdg.com
Issued By	com, hdg, hdg-DOMAIN-CA
Issued To	SQL.hdg.com

Expiration Date



Force Encryption	Yes
Hide Instance	No

Force Encryption
Turn on or off encryption for selected server instance

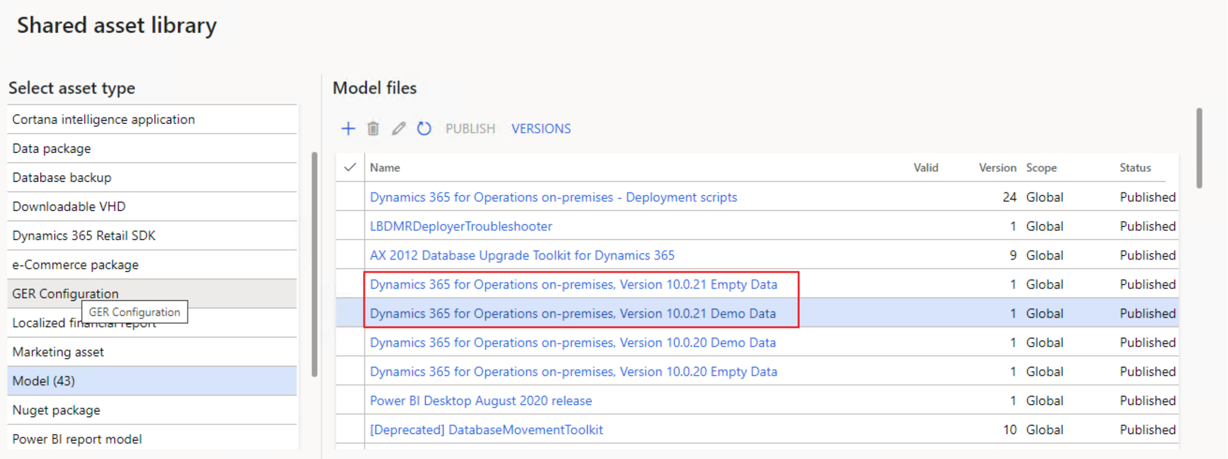
6. After all process is completed, open **1433** port named **MSSQL** manually.

1.18 Configure the databases

1. Sign in to LCS.

2. On the dashboard, select the **Shared asset library** tile.

3. Select **Model** as the asset type. Then, in the grid, select the data type for the release that you want, and download the zip file.



Shared asset library

Select asset type

- Cortana intelligence application
- Data package
- Database backup
- Downloadable VHD
- Dynamics 365 Retail SDK
- e-Commerce package
- GER Configuration
- Localized financial report
- Marketing asset
- Model (43)
- Nuget package
- Power BI report model

Model files

Name	Valid	Version	Scope	Status
Dynamics 365 for Operations on-premises - Deployment scripts		24	Global	Published
LBDMRDeployerTroubleshooter		1	Global	Published
AX 2012 Database Upgrade Toolkit for Dynamics 365		9	Global	Published
Dynamics 365 for Operations on-premises, Version 10.0.21 Empty Data		1	Global	Published
Dynamics 365 for Operations on-premises, Version 10.0.21 Demo Data		1	Global	Published
Dynamics 365 for Operations on-premises, Version 10.0.20 Demo Data		1	Global	Published
Dynamics 365 for Operations on-premises, Version 10.0.20 Empty Data		1	Global	Published
Power BI Desktop August 2020 release		1	Global	Published
[Deprecated] DatabaseMovementToolkit		10	Global	Published

4. The zip file contains a single backup (.bak) file. Select the file to download, based on your requirements.

5. After file is downloaded, Copy to the SQL server.

6. After the zip file is copied, verify that it's unblocked. Select and hold (or right-click) the file, and then select Properties. In the Properties dialog box, select the Unblock checkbox.

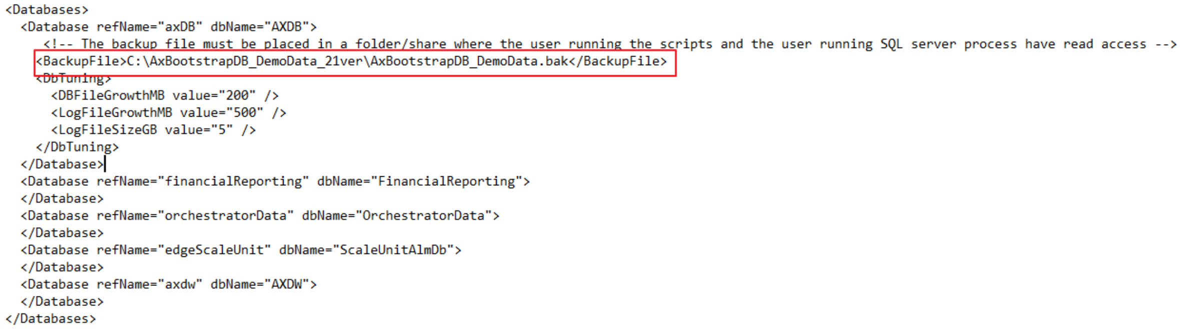
7. Make sure that the database section in the infrastructure₩ConfigTempate.xml file is correctly configured with the following information:

   A. The database name.

   B. **The database file and log settings**. The database settings should not be lower than the default values that are specified.

   C. The path of the backup file that you downloaded earlier. The default name of the Finance + Operations database is **AXDB**.

   D. Update the Config template file with the file **Location of the downloaded bak file**.



```
<Databases>
  <Database refName="axDB" dbName="AXDB">
     <!-- The backup file must be placed in a folder/share where the user running the scripts and the user running SQL server process have read access -->
    <BackupFile>C:\AxBootstrapDB_DemoData_21ver\AxBootstrapDB_DemoData.bak</BackupFile>
    <DbTuning>
      <DBFileGrowthMB value="200" />
      <LogFileGrowthMB value="500" />
      <LogFileSizeGB value="5" />
    </DbTuning>
  </Database>
  <Database refName="financialReporting" dbName="FinancialReporting">
  </Database>
  <Database refName="orchestratorData" dbName="OrchestratorData">
  </Database>
  <Database refName="edgeScaleUnit" dbName="ScaleUnitAlmDb">
  </Database>
  <Database refName="axdw" dbName="AXDW">
  </Database>
</Databases>
```

1.18.1 Configure the OrchestratorData database

Run the following command.

```
.₩Initialize-Database.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml -ComponentName Orchestrator
```

The Initialize-Database.ps1 script performs the following actions:

1. Create an empty database that is named **OrchestratorData**. This database is used by the on-premises local agent to orchestrate deployments.
2. Grant **db_owner** permissions on the database to the local agent gMSA (**svc-LocalAgent$).**

1.18.2 Configure the Finance + Operations database

1. Run the following commands.

```
.₩Initialize-Database.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml -ComponentName AOS
```

```
.₩Configure-Database.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml -ComponentName AOS
```

The Initialize-Database.ps1 script performs the following actions:

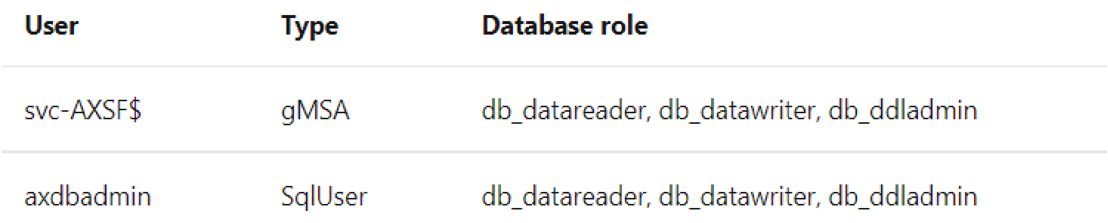
a. Restore the database from the specified backup file.

b. Create a new user that SQL authentication is enabled for (**axdbadmin**).

c. Map users to database roles, based on the following table for the **AXDB** database.

User	Type	Database role
svc-AXSF$	gMSA	db_owner
svc-LocalAgent$	gMSA	db_owner
svc-FRPS$	gMSA	db_owner
svc-FRAS$	gMSA	db_owner
axdbadmin	SqlUser	db_owner

d. Map users to database roles, based on the following table for the **TempDB** database.



User	Type	Database role
svc-AXSF$	gMSA	db_datareader, db_datawriter, db_ddladmin
axdbadmin	SqlUser	db_datareader, db_datawriter, db_ddladmin

The Configure-Database.ps1 script performs the following actions:

a. Set READ_COMMITTED_SNAPSHOT to ON.

b. Set ALLOW_SNAPSHOT_ISOLATION to ON.

c. Set the specified database file and log settings.

d. Grant the VIEW SERVER STATE permission to axdbadmin.

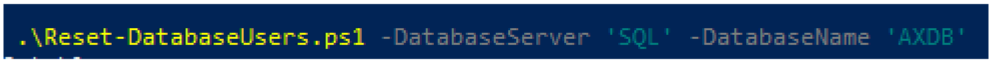
e. Grant the ALTER ANY EVENT SESSION permission to axdbadmin.

f. Grant the VIEW SERVER STATE permission to [contoso₩svc-AXSF$].

g. Grant the ALTER ANY EVENT SESSION permission to [contoso₩svc-AXSF$].

2. Run the following command to reset the database users.

```
.₩Reset-DatabaseUsers.ps1 -DatabaseServer '<FQDN of the SQL server>' -DatabaseName '<AX database name>'
```



```
.\Reset-DatabaseUsers.ps1 -DatabaseServer 'SQL' -DatabaseName 'AXDB'
```

1.18.3 Configure the Financial Reporting database

Run the following command.

```
.₩Initialize-Database.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml -ComponentName MR
```

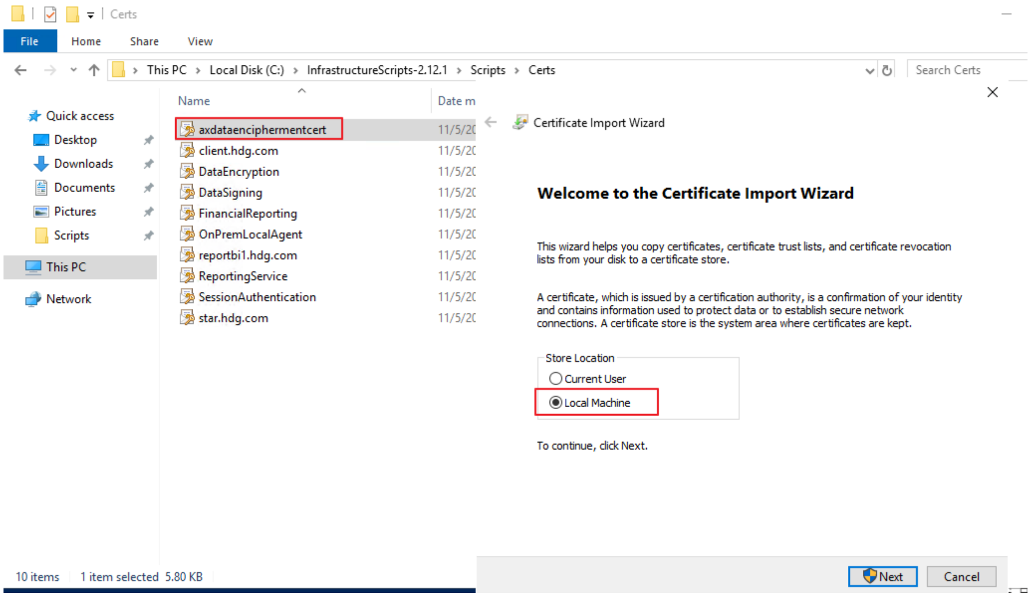
The Initialize-Database.ps1 script performs the following actions:

A. Create an empty database that is named **FinancialReporting**.

B. Map the users to database roles, based on the following table.

1.19 Encrypt credentials

1. On any client machine, install the encipherment certificate in the **LocalMachine₩My** certificate store.



Welcome to the Certificate Import Wizard

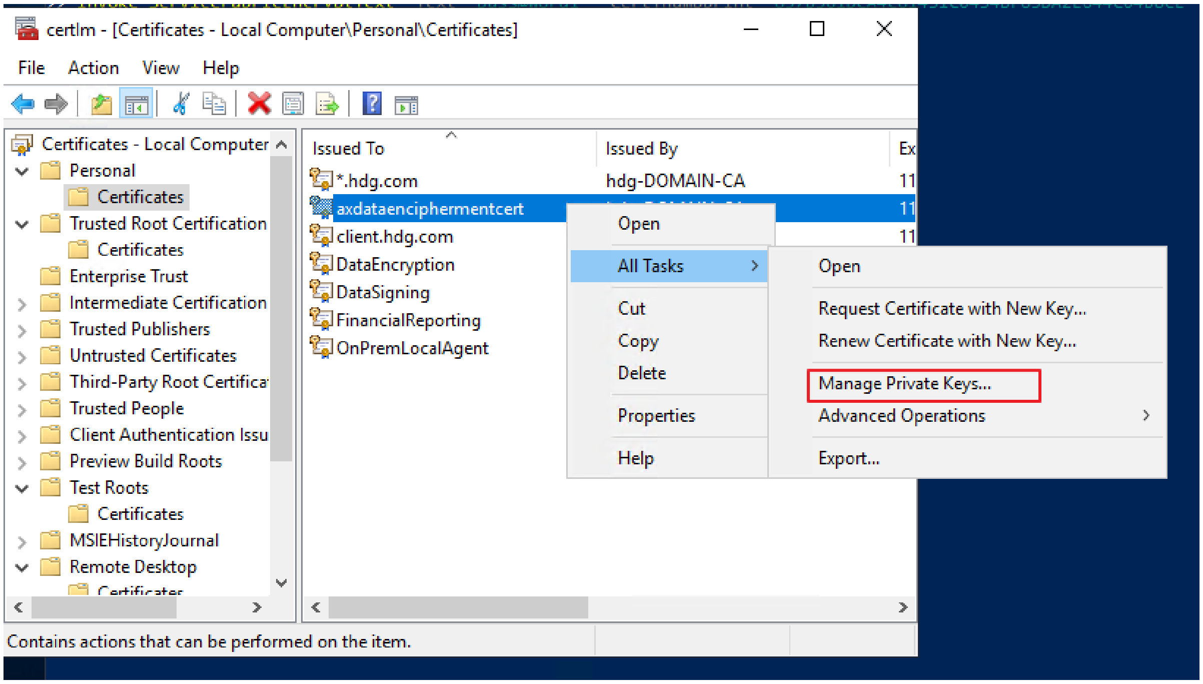
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location
○ Current User
● Local Machine

To continue, click Next.

2. Grant the current user **Read** access to the private key of this certificate.



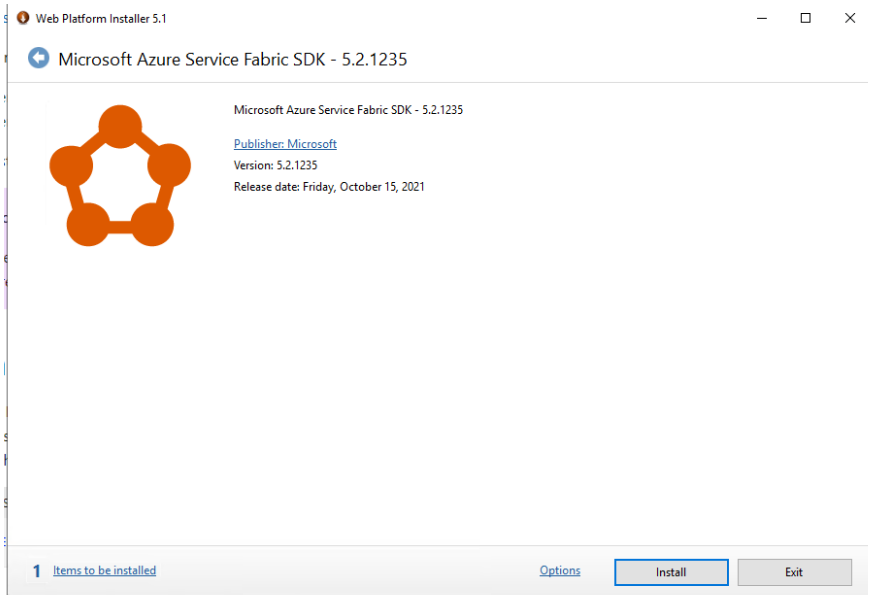
Contains actions that can be performed on the item.

3. Edit the **Credentials.json** file that is included **Infrastructure** folder, as shown here.

```
{
    "AosPrincipal": {
        "AccountPassword": "<encryptedDomainUserPassword>"
    },
    "AosSqlAuth": {
        "SqlUser": "<encryptedSqlUser>",
        "SqlPwd": "<encryptedSqlPassword>"
    }
}
```

- **AccountPassword** – The encrypted domain user password for the AOS domain user (**contoso₩axserviceuser**).
- **SqlUser** – The encrypted SQL user (axdbadmin) that has access to the Finance + Operations database (**AXDB**)
- **SqlPassword** – The encrypted SQL password.

4. Before you can invoke the **Invoke-ServiceFabricEncryptText** command, you must install the Microsoft Azure Service Fabric software development kit (SDK).



Microsoft Azure Service Fabric SDK - 5.2.1235

Microsoft Azure Service Fabric SDK - 5.2.1235

Publisher: Microsoft

Version: 5.2.1235

Release date: Friday, October 15, 2021

   A. After you install the Service Fabric SDK, you might receive the following error message: "Invoke-ServiceFabricEncryptText is not recognized command." In this case, restart the computer, and try again.

5. Update the **Credentials.json** file with encrypted values.

```
# Service fabric API to encrypt text and copy it to the clipboard.
Invoke-ServiceFabricEncryptText -Text '<textToEncrypt>' -CertThumbprint '<DataEncipherment Thumbprint>' -CertStore -StoreLocation LocalMachine -StoreName My | Set-Clipboard
```

- textToEncypt : That you want to encrypt word (ex : axdbadmin, password)
- DataEnciphermentThumbprint : Use **ServiceFabricEncryption** thumbprint in **ConfigTemplate.xml**

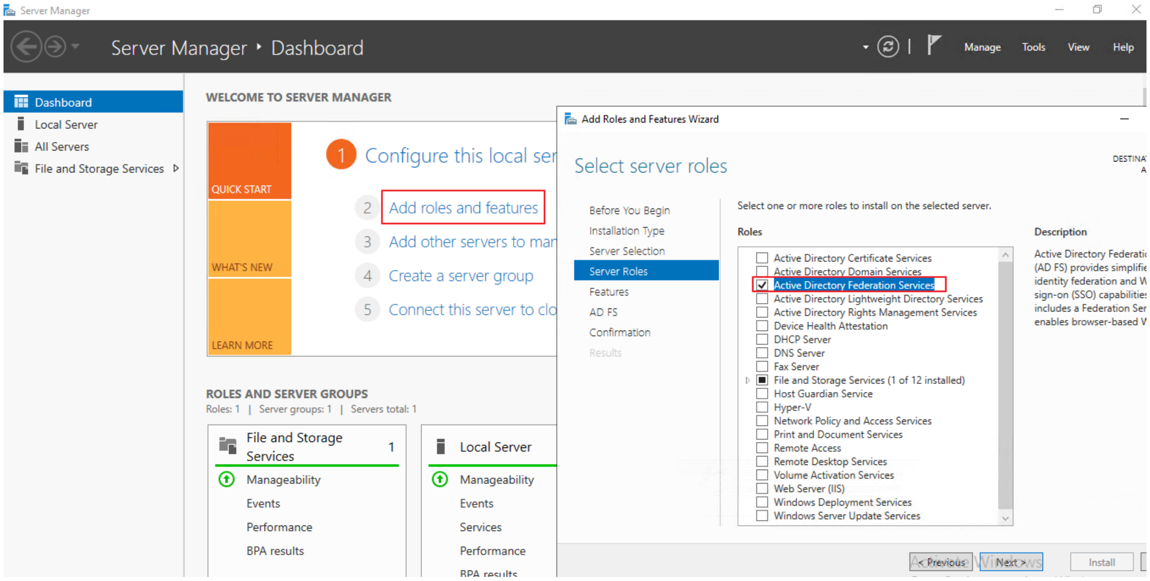
6. Copy the .json file to the SMB file share: **₩₩FILE₩agent₩Credentials₩Credentials.json**.

1.20 Configure AD FS

1.20.1 Install ADFS

Here is document.

1. In **server manager – Add roles and features**



Select one or more roles to install on the selected server.

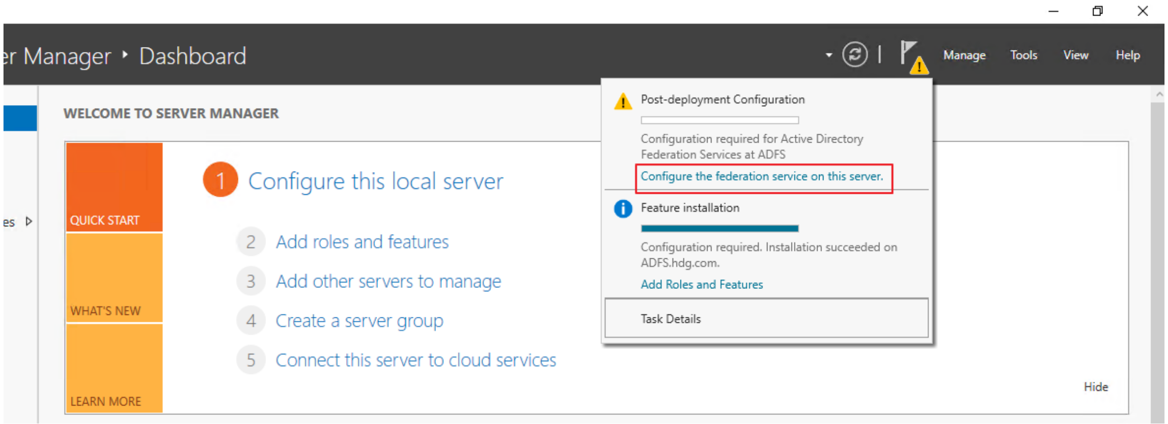
Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☑ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Update Services

Description

Active Directory Federati (AD FS) provides simplifie identity federation and W sign-on (SSO) capabilitie includes a Federation Ser enables browser-based W

2. After Add roles, **Configure ADFS**



Post-deployment Configuration

Configuration required for Active Directory Federation Services at ADFS

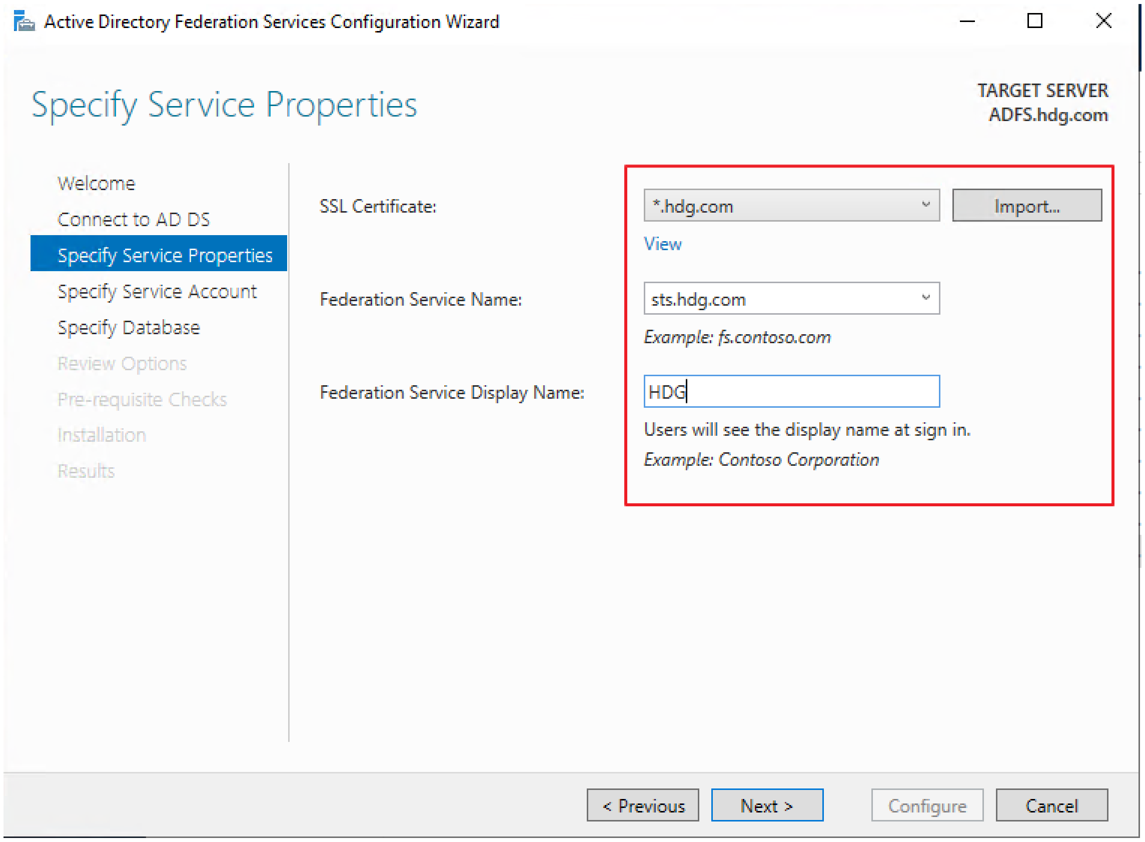
Configure the federation service on this server.

Feature installation

Configuration required. Installation succeeded on ADFS.hdg.com.

Add Roles and Features

3. Set **star cetificate**, and Federation Service Name.



Active Directory Federation Services Configuration Wizard

Specify Service Properties

TARGET SERVER
ADFS.hdg.com

SSL Certificate: *.hdg.com

Federation Service Name: sts.hdg.com

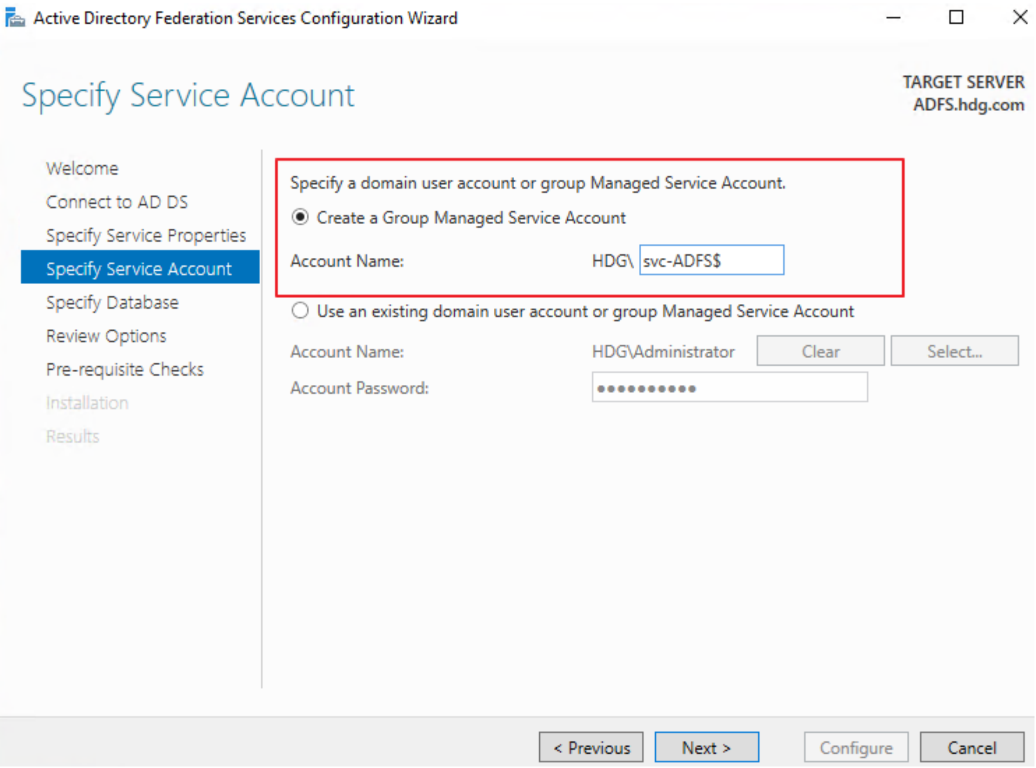
Example: fs.contoso.com

Federation Service Display Name: HDG

Users will see the display name at sign in.

Example: Contoso Corporation

4. Create Account Name



Active Directory Federation Services Configuration Wizard

Specify Service Account

TARGET SERVER
ADFS.hdg.com

Specify a domain user account or group Managed Service Account.

● Create a Group Managed Service Account

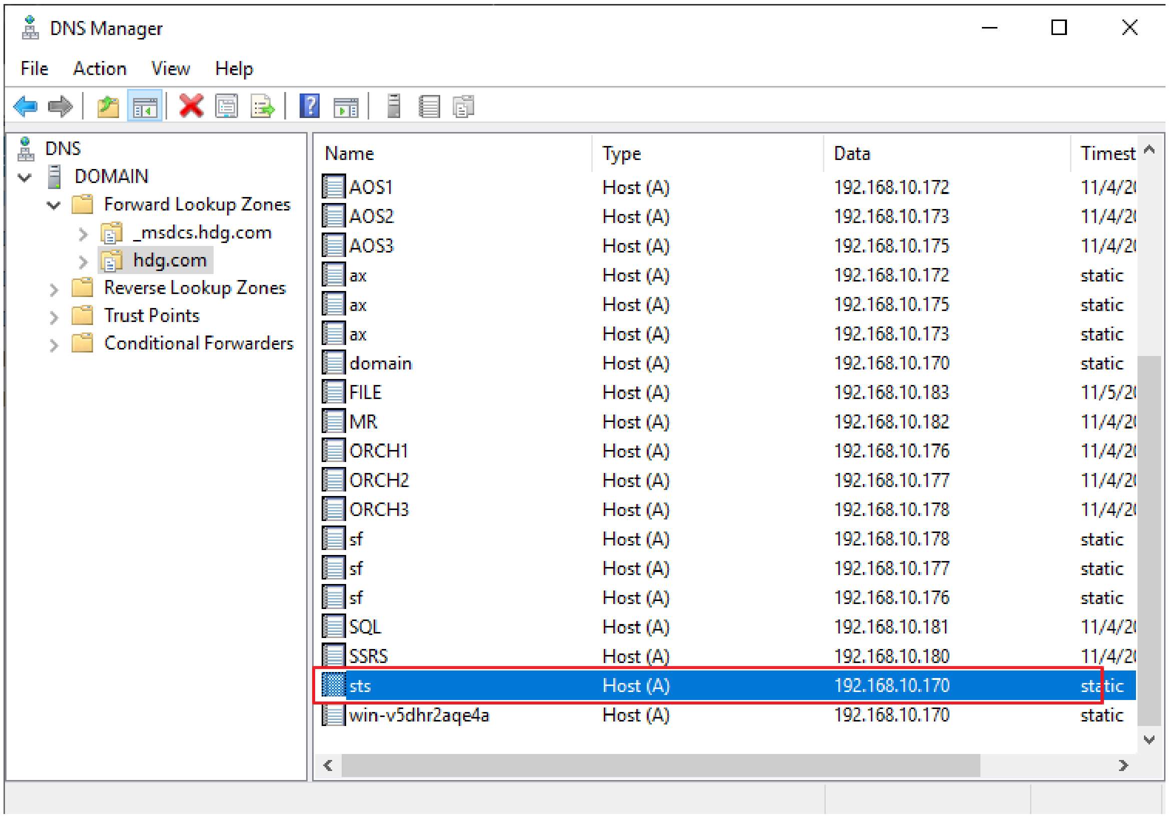
Account Name: HDG\ svc-ADFS$

○ Use an existing domain user account or group Managed Service Account

Account Name: HDG\Administrator

Account Password: ●●●●●●●●●●

5. **Add Host** that name is Ferderation service name and IP Address is Federation Server's IP.



Name	Type	Data	Timest
AOS1	Host (A)	192.168.10.172	11/4/20
AOS2	Host (A)	192.168.10.173	11/4/20
AOS3	Host (A)	192.168.10.175	11/4/20
ax	Host (A)	192.168.10.172	static
ax	Host (A)	192.168.10.175	static
ax	Host (A)	192.168.10.173	static
domain	Host (A)	192.168.10.170	static
FILE	Host (A)	192.168.10.183	11/5/20
MR	Host (A)	192.168.10.182	11/4/20
ORCH1	Host (A)	192.168.10.176	11/4/20
ORCH2	Host (A)	192.168.10.177	11/4/20
ORCH3	Host (A)	192.168.10.178	11/4/20
sf	Host (A)	192.168.10.178	static
sf	Host (A)	192.168.10.177	static
sf	Host (A)	192.168.10.176	static
SQL	Host (A)	192.168.10.181	11/4/20
SSRS	Host (A)	192.168.10.180	11/4/20
sts	Host (A)	192.168.10.170	static
win-v5dhr2aqe4a	Host (A)	192.168.10.170	static

6. Verify to open https://<adfs-dns-name>/adfs/fs/federationserverservice.asmx

1.20.2 Configure

1. Configure the AD FS identifier so that it matches the AD FS token issuer.

This command is related to adding new users by using the **Import users** option on the Users page (**System administration** > **Users** > **Users**) in the Finance + Operations client.

```
$adfsProperties = Get-AdfsProperties
```

```
Set-AdfsProperties -Identifier $adfsProperties.IdTokenIssuer
```

2. You should disable Windows Integrated Authentication (WIA) for intranet authentication connections, unless you've configured AD FS for mixed environments. For more information about how to configure WIA so that it can be used with AD FS, see Configure browsers to use Windows Integrated Authentication (WIA) with AD FS.

   This command is related to using forms authentication upon sign-in to the Finance + Operations client. Other options, such as single sign-on, are not supported.

```
Set-AdfsGlobalAuthenticationPolicy -PrimaryIntranetAuthenticationProvider FormsAuthentication, MicrosoftPassportAuthentication
```

3. For sign-in, the user's email address must be acceptable authentication input.

   This command is related to setting up email claims. Other options, such as transformation rules, might be available but require additional setup.

   ```
   Add-Type -AssemblyName System.Net
   $fqdn = ([System.Net.Dns]::GetHostEntry('localhost').HostName).ToLower()
   $domainName = $fqdn.Substring($fqdn.IndexOf('.')+1)
   Set-AdfsClaimsProviderTrust -TargetIdentifier 'AD AUTHORITY' -AlternateLoginID mail -LookupForests $domainName
   ```

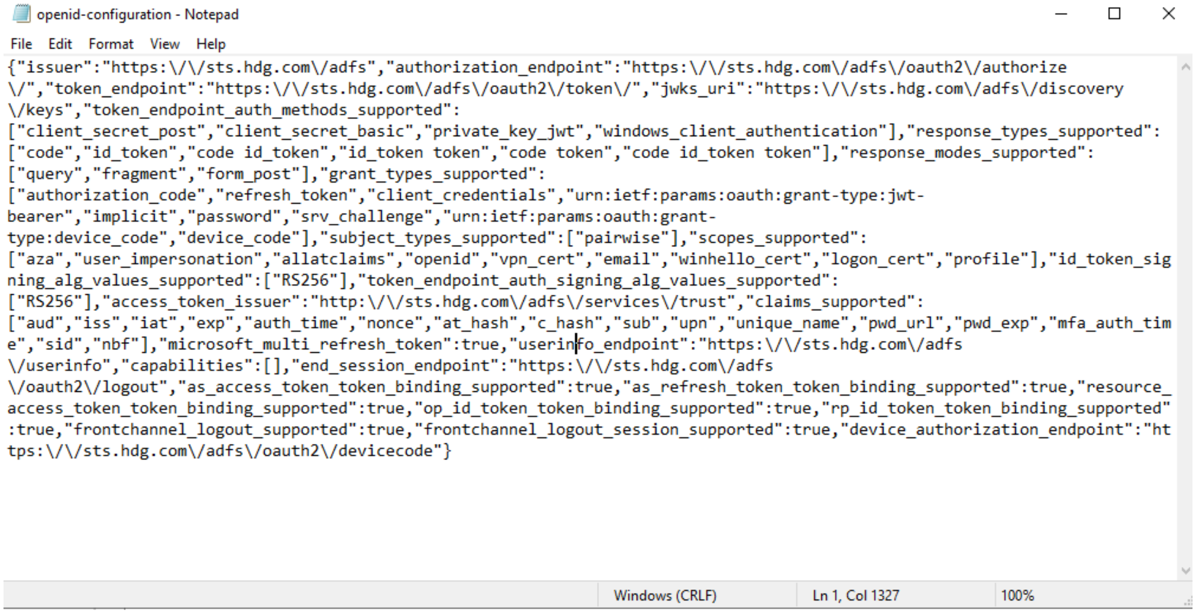
4. Copy infrastructure script and the D365FO-OP directory to a machine where the AD FS role service is installed. Then run the script by using a user account that has enough permissions to administer AD FS.

   ```
   # Host URL is your DNS record₩host name for accessing the AOS
   .₩Publish-ADFSApplicationGroup.ps1 -HostUrl 'https://ax.d365ffo.onprem.contoso.com'
   ```

5. Finally, verify that you can access the AD FS OpenID configuration URL on a Service Fabric node of the AOSNodeType type. To do this check, try to open https://<adfs-dns-name>/adfs/.well-known/openid-configuration in a web browser. If you receive a message that states that the site isn't secure, you haven't added your AD FS SSL certificate to the Trusted Root Certification Authorities store. This step is described in the AD FS deployment guide. If you're using remoting, you can run the following command to install the certificate on all nodes in the Service Fabric cluster.

```
# If remoting, execute
.₩Install-ADFSCert-AllVMs.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml
```

6. If you can access the URL, a JavaScript Object Notation (JSON) file is returned. This file contains your AD FS configuration, and it will indicate that your AD FS URL is trusted.

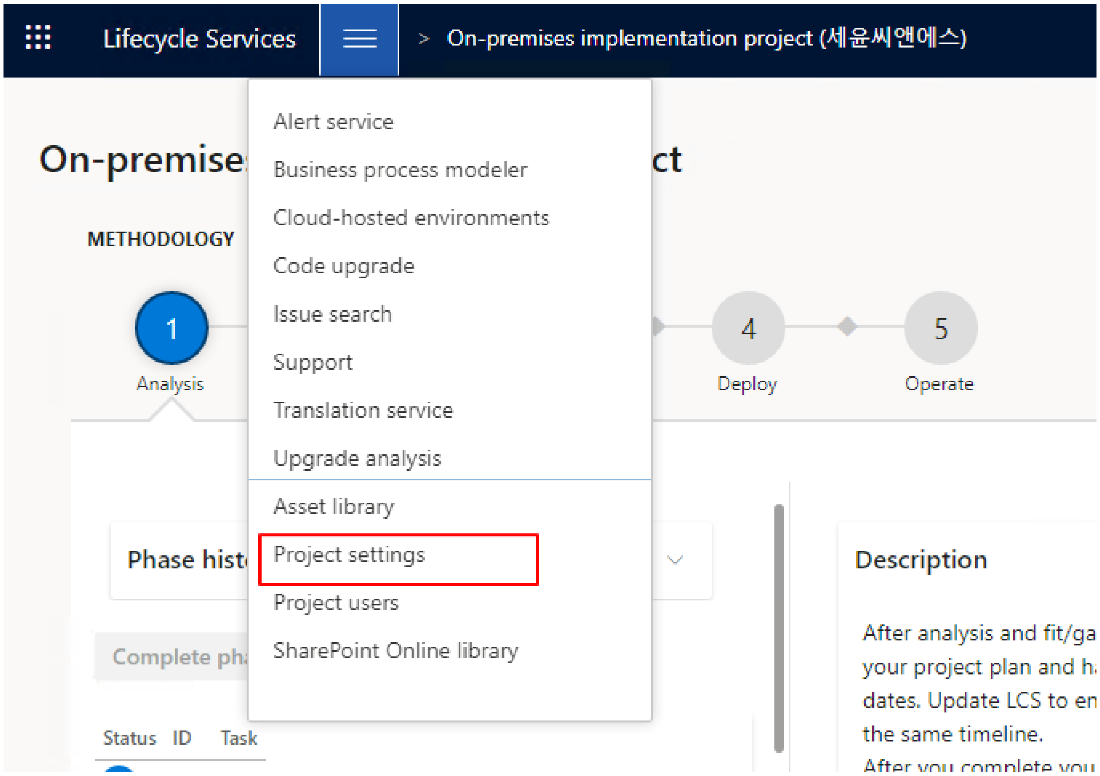


```
{"issuer":"https:\/\/sts.hdg.com\/adfs","authorization_endpoint":"https:\/\/sts.hdg.com\/adfs\/oauth2\/authorize
\/","token_endpoint":"https:\/\/sts.hdg.com\/adfs\/oauth2\/token\/","jwks_uri":"https:\/\/sts.hdg.com\/adfs\/discovery
\/keys","token_endpoint_auth_methods_supported":
["client_secret_post","client_secret_basic","private_key_jwt","windows_client_authentication"],"response_types_supported":
["code","id_token","code id_token","id_token token","code token","code id_token token"],"response_modes_supported":
["query","fragment","form_post"],"grant_types_supported":
["authorization_code","refresh_token","client_credentials","urn:ietf:params:oauth:grant-type:jwt-
bearer","implicit","password","srv_challenge","urn:ietf:params:oauth:grant-
type:device_code","device_code"],"subject_types_supported":["pairwise"],"scopes_supported":
["aza","user_impersonation","allatclaims","openid","vpn_cert","email","winhello_cert","logon_cert","profile"],"id_token_sig
ning_alg_values_supported":["RS256"],"token_endpoint_auth_signing_alg_values_supported":
["RS256"],"access_token_issuer":"http:\/\/sts.hdg.com\/adfs\/services\/trust","claims_supported":
["aud","iss","iat","exp","auth_time","nonce","at_hash","c_hash","sub","upn","unique_name","pwd_url","pwd_exp","mfa_auth_tim
e","sid","nbf"],"microsoft_multi_refresh_token":true,"userinfo_endpoint":"https:\/\/sts.hdg.com\/adfs
\/userinfo","capabilities":[],"end_session_endpoint":"https:\/\/sts.hdg.com\/adfs
\/oauth2\/logout","as_access_token_token_binding_supported":true,"as_refresh_token_token_binding_supported":true,"resource_
access_token_token_binding_supported":true,"op_id_token_token_binding_supported":true,"rp_id_token_token_binding_supported"
:true,"frontchannel_logout_supported":true,"frontchannel_logout_session_supported":true,"device_authorization_endpoint":"ht
tps:\/\/sts.hdg.com\/adfs\/oauth2\/devicecode"}
```

1.21 Configure a connector and install an on-premises local agent

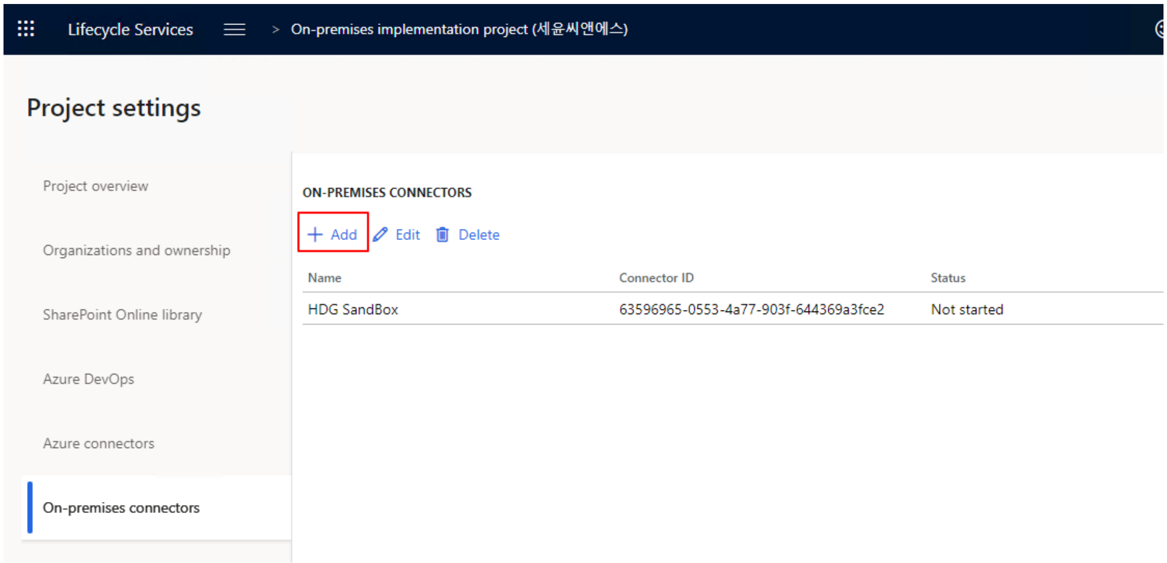
1. Sign in to LCS, and open your on-premises implementation project.

2. Select the Menu button (sometimes referred to as the hamburger or the hamburger button), and then select **Project settings**.



3. Select **On-premises connectors**.

4. Select **Add** to create a new on-premises connector.



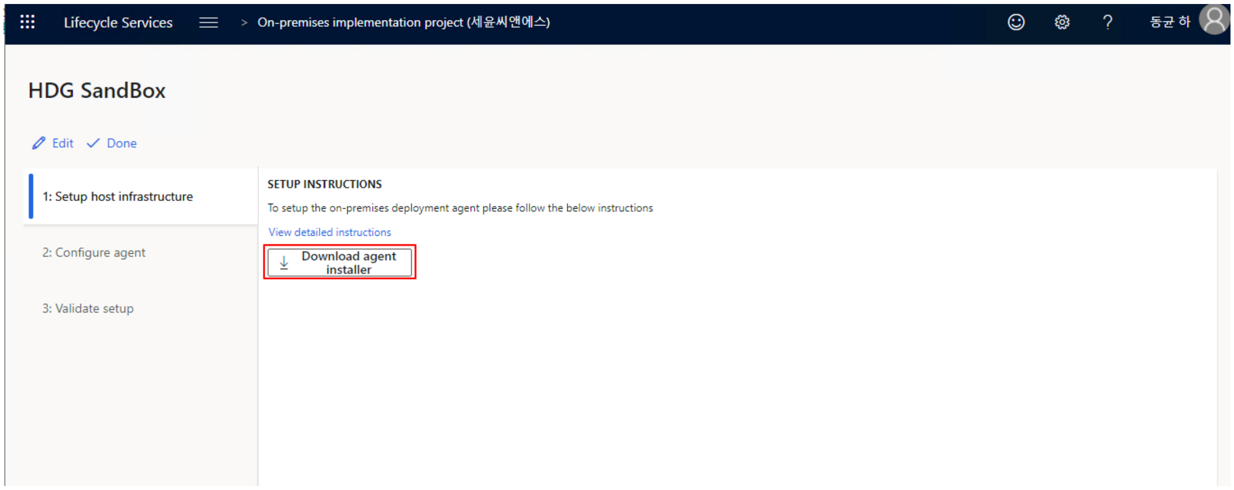
Lifecycle Services
> On-premises implementation project (세윤씨앤에스)
Project overview
Organizations and ownership
SharePoint Online library
Azure DevOps
Azure connectors
On-premises connectors
+ Add
Edit
Delete

Project settings

ON-PREMISES CONNECTORS

Name	Connector ID	Status
HDG SandBox	63596965-0553-4a77-903f-644369a3fce2	Not started

5. On the **1: Setup host infrastructure** tab, select **Download agent installer.**



Lifecycle Services
> On-premises implementation project (세윤씨앤에스)
동균 하
Edit
Done
1: Setup host infrastructure
2: Configure agent
3: Validate setup
View detailed instructions
Download agent installer

HDG SandBox

SETUP INSTRUCTIONS

To setup the on-premises deployment agent please follow the below instructions

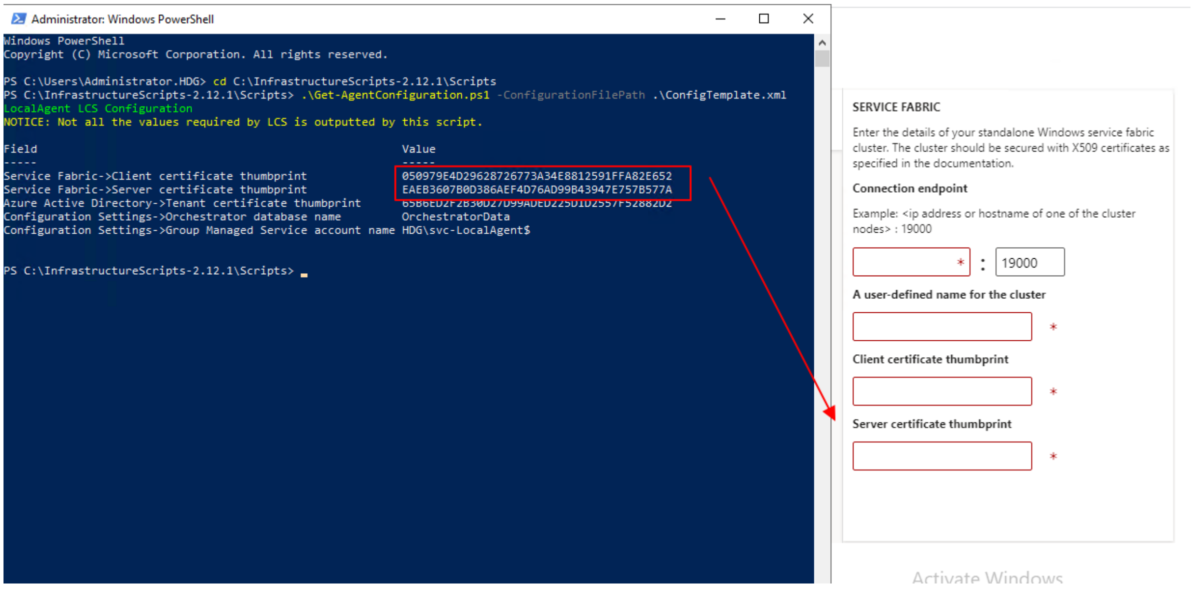
6. After the zip file is downloaded, verify that it's unblocked. Select and hold (or right-click) the file, and then select Properties. In the Properties dialog box, select the Unblock checkbox.

7. Unzip the agent installer on one of the Service Fabric nodes of the OrchestratorType type.

8. After the file is unzipped, go back to your on-premises connector in LCS.

9. On the **2: Configure agent tab**, select **Enter configuration**, and enter the configuration settings. To get the required values, run the following command on any machine that has the **infrastructure** folder and up-to-date configuration files.

```
.₩Get-AgentConfiguration.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.HDG> cd C:\InfrastructureScripts-2.12.1\Scripts
PS C:\InfrastructureScripts-2.12.1\Scripts> .\Get-AgentConfiguration.ps1 -ConfigurationFilePath .\ConfigTemplate.xml
LocalAgent LCS Configuration
NOTICE: Not all the values required by LCS is outputted by this script.

Field                                               Value
-----                                               -----
Service Fabric->Client certificate thumbprint       050979E4D29628726773A34E8812591FFA82E652
Service Fabric->Server certificate thumbprint       EAEB3607B0D386AEF4D76AD99B43947E757B577A
Azure Active Directory->Tenant certificate thumbprint       65B6ED2F2B30D27D99ADED225D1D2557F52882D2
Configuration Settings->Orchestrator database name  OrchestratorData
Configuration Settings->Group Managed Service account name HDG\svc-LocalAgent$


PS C:\InfrastructureScripts-2.12.1\Scripts> _
```

SERVICE FABRIC

Enter the details of your standalone Windows service fabric cluster. The cluster should be secured with X509 certificates as specified in the documentation.

Connection endpoint

Example: <ip address or hostname of one of the cluster nodes> : 19000

* : 19000

A user-defined name for the cluster *

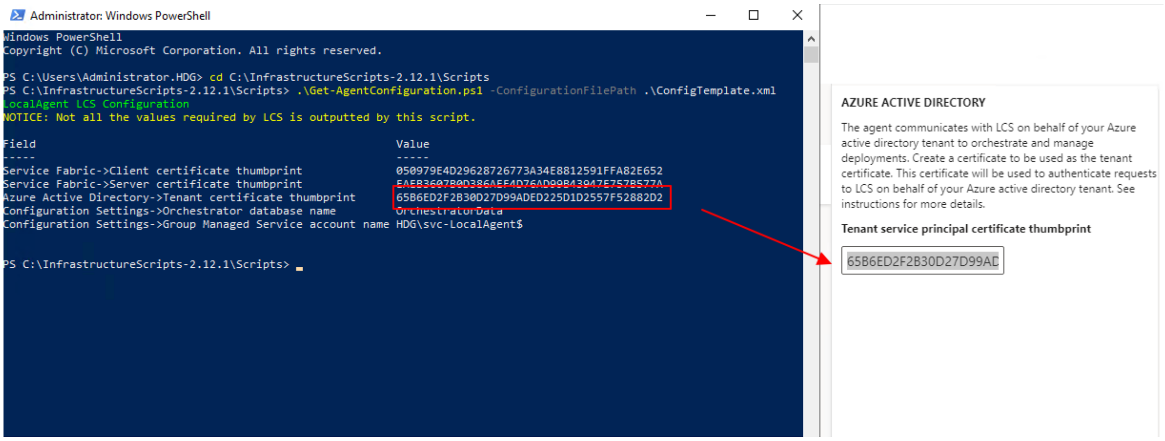
Client certificate thumbprint *

Server certificate thumbprint *

Activate Windows

- Connection endpoint : sf.hdg.com:19000 (Enter Host name or IP Adrress from one of Orchestrator Type node)

- A user-defined name for the cluster – ClusterName Node value from ConfigTemplate.xml

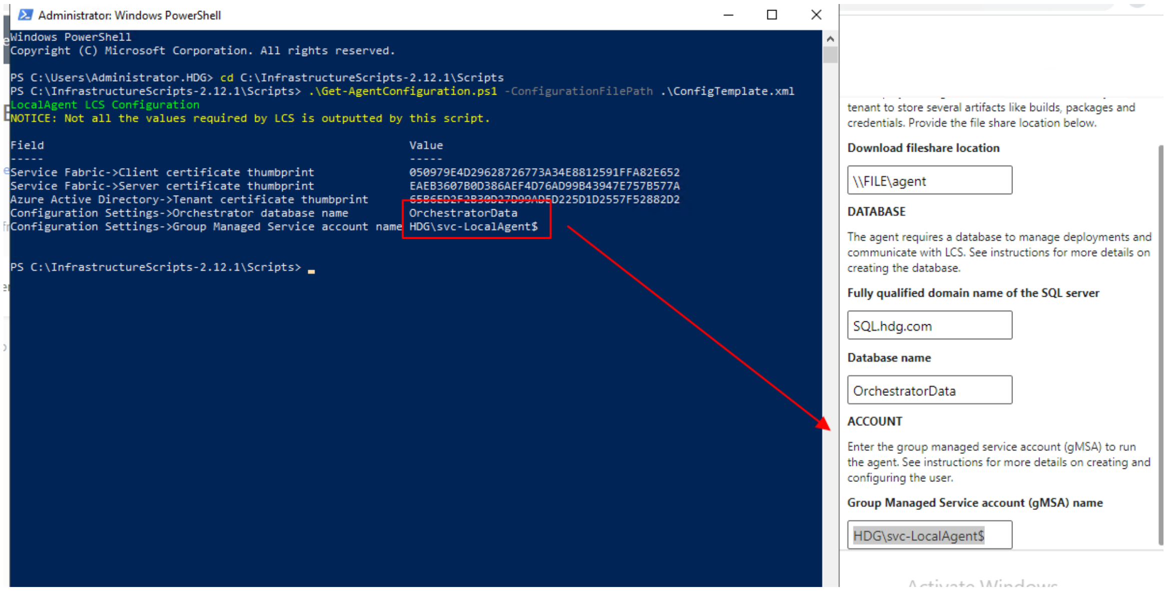


```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.HDG> cd C:\InfrastructureScripts-2.12.1\Scripts
PS C:\InfrastructureScripts-2.12.1\Scripts> .\Get-AgentConfiguration.ps1 -ConfigurationFilePath .\ConfigTemplate.xml
LocalAgent LCS Configuration
NOTICE: Not all the values required by LCS is outputted by this script.

Field                                               Value
-----                                               -----
Service Fabric->Client certificate thumbprint       050979E4D29628726773A34E8812591FFA82E652
Service Fabric->Server certificate thumbprint       EAEB3607B0D386AEF4D76AD99B43947E757B577A
Azure Active Directory->Tenant certificate thumbprint       65B6ED2F2B30D27D99ADED225D1D2557F52882D2
Configuration Settings->Orchestrator database name  OrchestratorData
Configuration Settings->Group Managed Service account name HDG\svc-LocalAgent$


PS C:\InfrastructureScripts-2.12.1\Scripts> _
```

AZURE ACTIVE DIRECTORY

The agent communicates with LCS on behalf of your Azure active directory tenant to orchestrate and manage deployments. Create a certificate to be used as the tenant certificate. This certificate will be used to authenticate requests to LCS on behalf of your Azure active directory tenant. See instructions for more details.

Tenant service principal certificate thumbprint: 65B6ED2F2B30D27D99AD



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator.HDG> cd C:\InfrastructureScripts-2.12.1\Scripts
PS C:\InfrastructureScripts-2.12.1\Scripts> .\Get-AgentConfiguration.ps1 -ConfigurationFilePath .\ConfigTemplate.xml
LocalAgent LCS Configuration
NOTICE: Not all the values required by LCS is outputted by this script.

Field                                                   Value
-----                                                   -----
Service Fabric->Client certificate thumbprint           050979E4D29628726773A34E8812591FFA82E652
Service Fabric->Server certificate thumbprint           EAEB3607B0D386AEF4D76AD99B43947E757B577A
Azure Active Directory->Tenant certificate thumbprint   65B6ED2F2B30D27D99ADED225D1D2557F52882D2
Configuration Settings->Orchestrator database name      OrchestratorData
Configuration Settings->Group Managed Service account name HDG\svc-LocalAgent$


PS C:\InfrastructureScripts-2.12.1\Scripts> _
```

tenant to store several artifacts like builds, packages and credentials. Provide the file share location below.

Download fileshare location

\\FILE\agent

DATABASE

The agent requires a database to manage deployments and communicate with LCS. See instructions for more details on creating the database.

Fully qualified domain name of the SQL server

SQL.hdg.com

Database name

OrchestratorData

ACCOUNT

Enter the group managed service account (gMSA) to run the agent. See instructions for more details on creating and configuring the user.

Group Managed Service account (gMSA) name

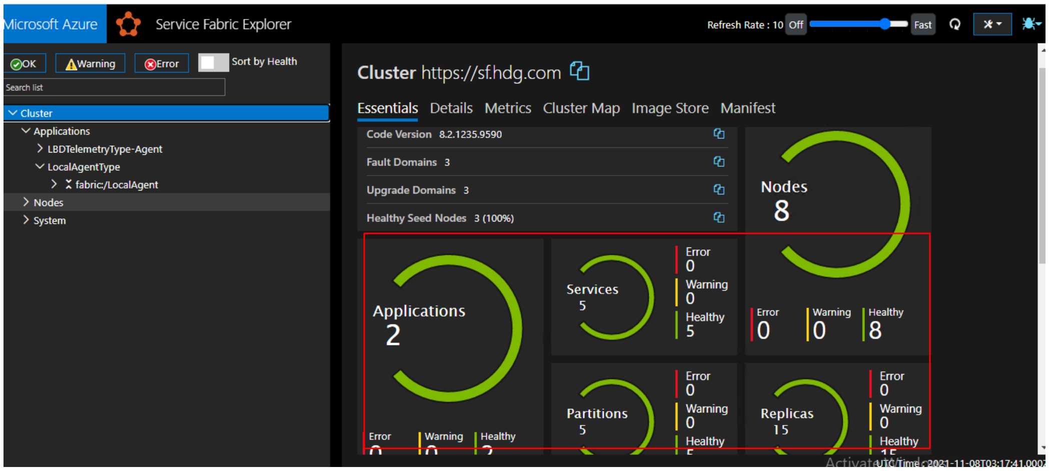
HDG\svc-LocalAgent$

- Download fileshare location : agent folder location to file server
- Fully qualified domain name of the SQL Server : erntrie domain name of SQL Server

10. Save the configuration, and then select Download configurations to download the localagent-config.json configuration file.
11. Copy the localagent-config.json file to the machine where the agent installer package is located.
12. In a Command Prompt window, run the following command by navigating to the folder that contains the agent installer.

LocalAgentCLI.exe Install <path of config.json>

- After the Local Agent is successfully executed, you can find 2 application is created in Service Fabric.



Cluster https://sf.hdg.com

Code Version 8.2.1235.9590

Fault Domains 3

Upgrade Domains 3

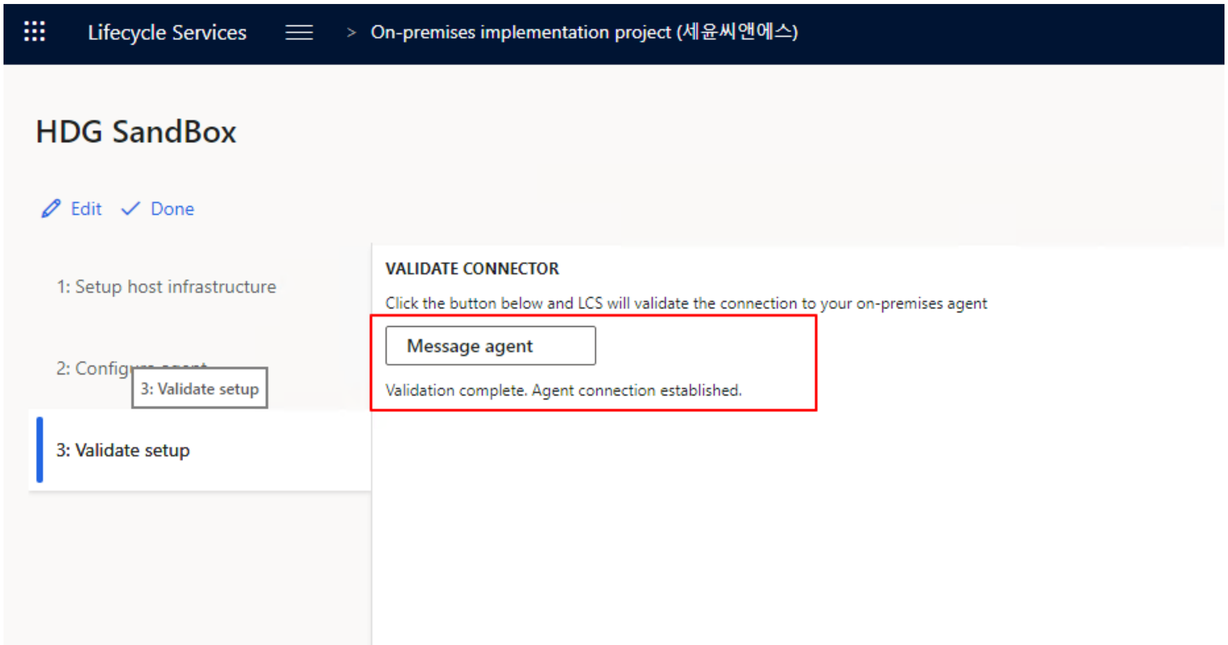
Healthy Seed Nodes 3 (100%)

	Total	Error	Warning	Healthy
Nodes	8	0	0	8
Applications	2	0	0	2
Services	5	0	0	5
Partitions	5	0	0	5
Replicas	15	0	0	15

UTC Time : 2021-11-08T03:17:41.000Z

13. After the local agent is successfully installed, navigate back to your on-premises connector in LCS.

14. On the Validate setup tab, select Message agent to test for LCS connectivity to your local agent. When a connection is successfully established, the page will resemble the following illustration.



VALIDATE CONNECTOR

Click the button below and LCS will validate the connection to your on-premises agent

Validation complete. Agent connection established.

1.22 Tear down CredSSP, if remoting was used

If any of the remoting scripts were used during setup, be sure to execute the following script when there are breaks in the setup process, or the setup has finished.

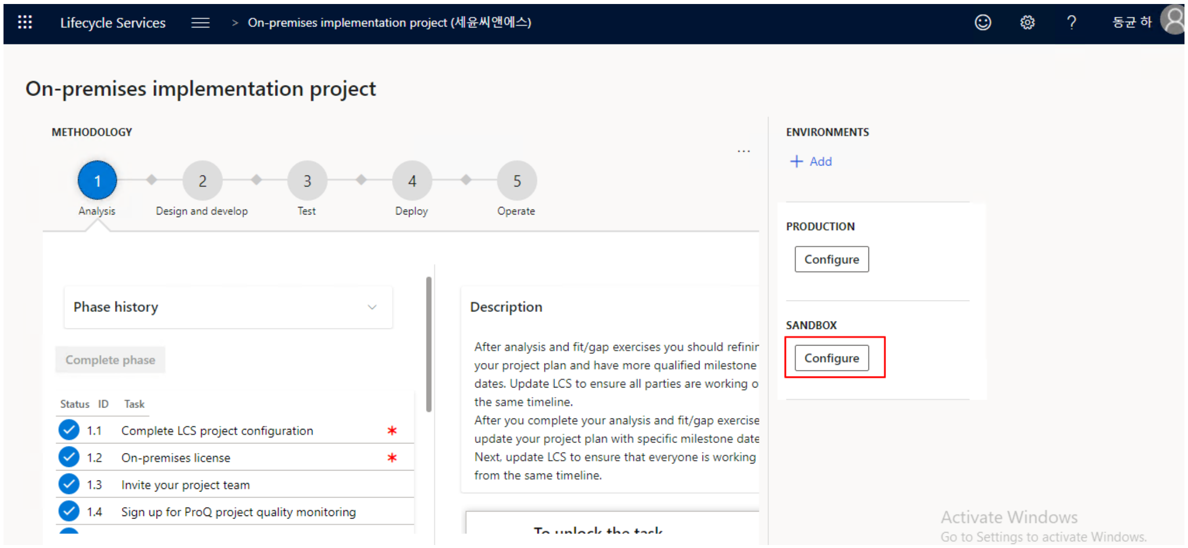
```
.₩Disable-CredSSP-AllVMs.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml
```

If the previous remoting PowerShell window was accidentally closed and CredSSP was left enabled, the script will disable it on all the machines specified in the configuration file.

1.23 Deploy your Finance + Operations environment from LCS

1. In LCS, navigate to your on-premises project, go to **Environment** > **Sandbox**, and then select Configure. Execute the following script on the **primary domain controller VM**, which must have access to ADFS and the DNS server settings, to get the needed values.

```
.₩Get-DeploymentSettings.ps1 -ConfigurationFilePath .₩ConfigTemplate.xml
```



Lifecycle Services > On-premises implementation project (세윤씨엔에스)

On-premises implementation project

METHODOLOGY

1 Analysis · 2 Design and develop · 3 Test · 4 Deploy · 5 Operate

Phase history

Complete phase

Status	ID	Task	
✓	1.1	Complete LCS project configuration	*
✓	1.2	On-premises license	*
✓	1.3	Invite your project team	
✓	1.4	Sign up for ProQ project quality monitoring	

Description

After analysis and fit/gap exercises you should refinir your project plan and have more qualified milestone dates. Update LCS to ensure all parties are working o the same timeline.
After you complete your analysis and fit/gap exercise update your project plan with specific milestone date Next, update LCS to ensure that everyone is working from the same timeline.

To unlock the task

ENVIRONMENTS

+ Add

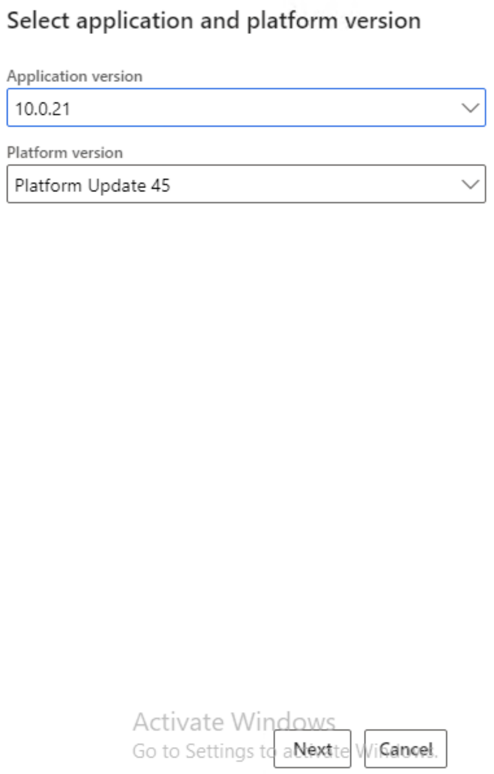
PRODUCTION

Configure

SANDBOX

Configure

Activate Windows
Go to Settings to activate Windows.

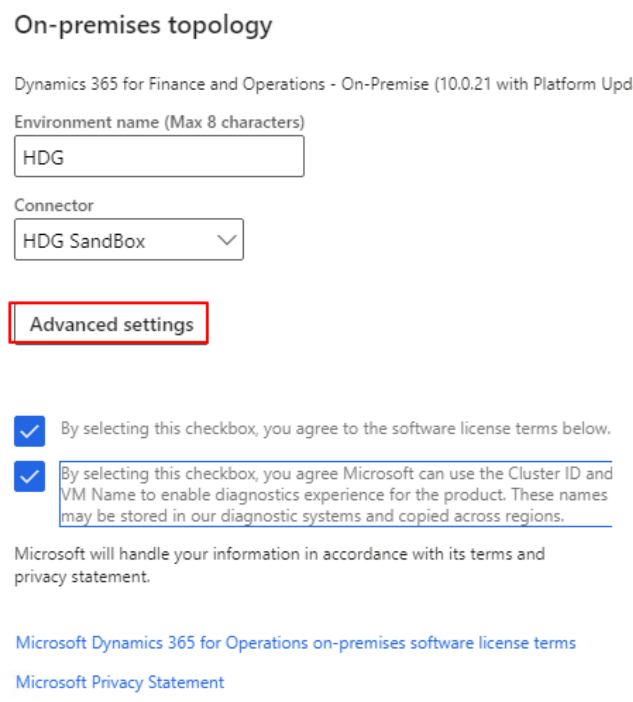


Select application and platform version

Application version: 10.0.21

Platform version: Platform Update 45

Activate Windows
Go to Settings to activate Windows.



On-premises topology

Dynamics 365 for Finance and Operations - On-Premise (10.0.21 with Platform Update 45) v 20

Environment name (Max 8 characters)

HDG

Connector

HDG SandBox

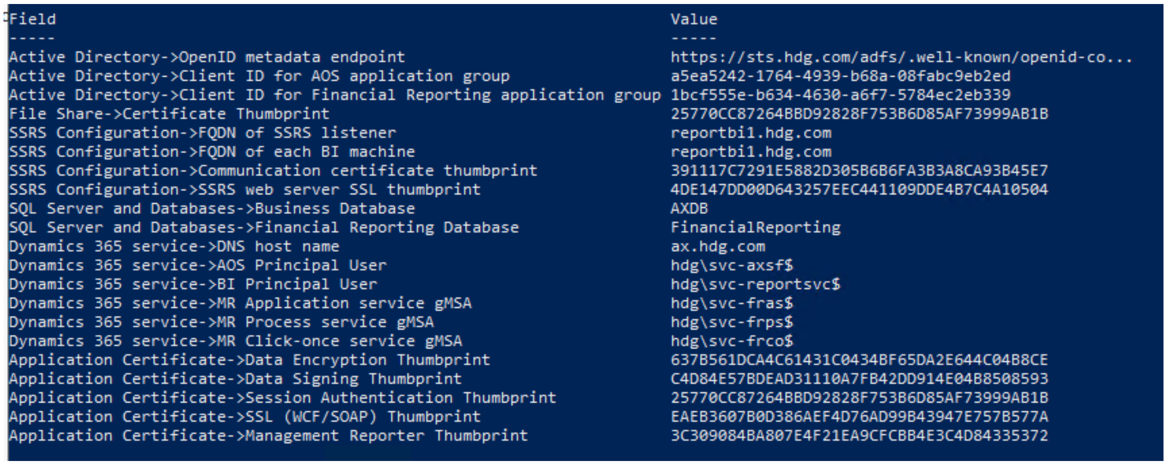
☑ By selecting this checkbox, you agree to the software license terms below.

☑ By selecting this checkbox, you agree Microsoft can use the Cluster ID and VM Name to enable diagnostics experience for the product. These names may be stored in our diagnostic systems and copied across regions.

Microsoft will handle your information in accordance with its terms and privacy statement.

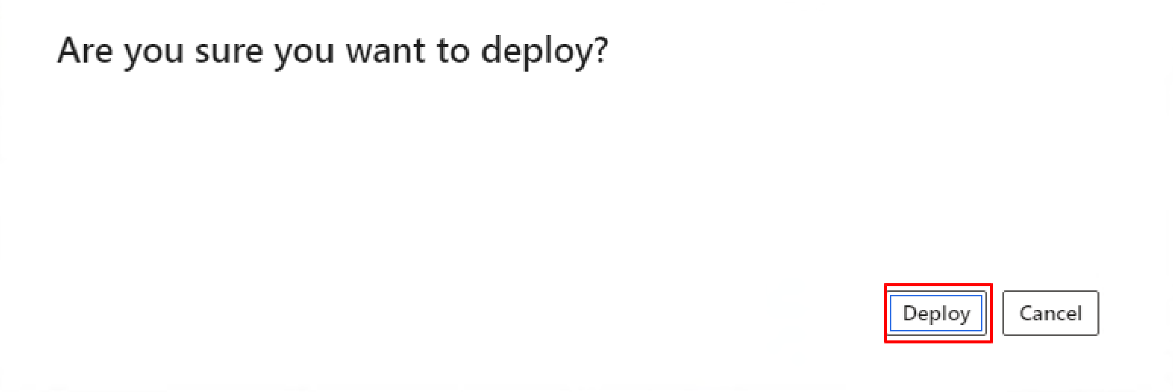
Microsoft Dynamics 365 for Operations on-premises software license terms

Microsoft Privacy Statement



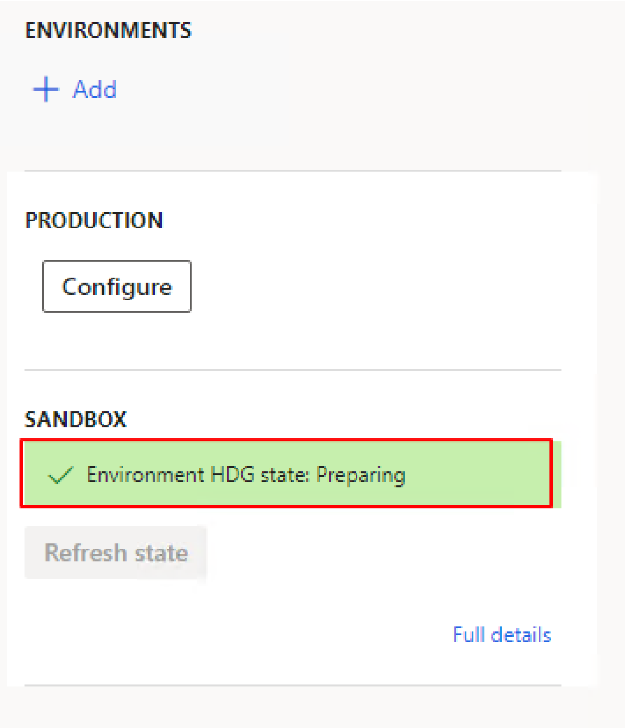
```
Field                                                                 Value
-----                                                                 -----
Active Directory->OpenID metadata endpoint                            https://sts.hdg.com/adfs/.well-known/openid-co...
Active Directory->Client ID for AOS application group                 a5ea5242-1764-4939-b68a-08fabc9eb2ed
Active Directory->Client ID for Financial Reporting application group 1bcf555e-b634-4630-a6f7-5784ec2eb339
File Share->Certificate Thumbprint                                    25770CC87264BBD92828F753B6D85AF73999AB1B
SSRS Configuration->FQDN of SSRS listener                             reportbi1.hdg.com
SSRS Configuration->FQDN of each BI machine                           reportbi1.hdg.com
SSRS Configuration->Communication certificate thumbprint              391117C7291E5882D305B6B6FA3B3A8CA93B45E7
SSRS Configuration->SSRS web server SSL thumbprint                    4DE147DD00D643257EEC441109DDE4B7C4A10504
SQL Server and Databases->Business Database                           AXDB
SQL Server and Databases->Financial Reporting Database                FinancialReporting
Dynamics 365 service->DNS host name                                   ax.hdg.com
Dynamics 365 service->AOS Principal User                              hdg\svc-axsf$
Dynamics 365 service->BI Principal User                               hdg\svc-reportsvc$
Dynamics 365 service->MR Application service gMSA                     hdg\svc-fras$
Dynamics 365 service->MR Process service gMSA                         hdg\svc-frps$
Dynamics 365 service->MR Click-once service gMSA                      hdg\svc-frco$
Application Certificate->Data Encryption Thumbprint                   637B561DCA4C61431C0434BF65DA2E644C04B8CE
Application Certificate->Data Signing Thumbprint                      C4D84E57BDEAD31110A7FB42DD914E04B8508593
Application Certificate->Session Authentication Thumbprint            25770CC87264BBD92828F753B6D85AF73999AB1B
Application Certificate->SSL (WCF/SOAP) Thumbprint                    EAEB3607B0D386AEF4D76AD99B43947E757B577A
Application Certificate->Management Reporter Thumbprint               3C309084BA807E4F21EA9CFCBB4E3C4D84335372
```

- Insert proper value to accurate field.



Are you sure you want to deploy?

3. LCS will assemble the Service Fabric application packages for your environment during the preparation phase. It then sends a message to the local agent to start deployment. You will notice the Preparing status as below.



ENVIRONMENTS

+ Add

PRODUCTION

Configure

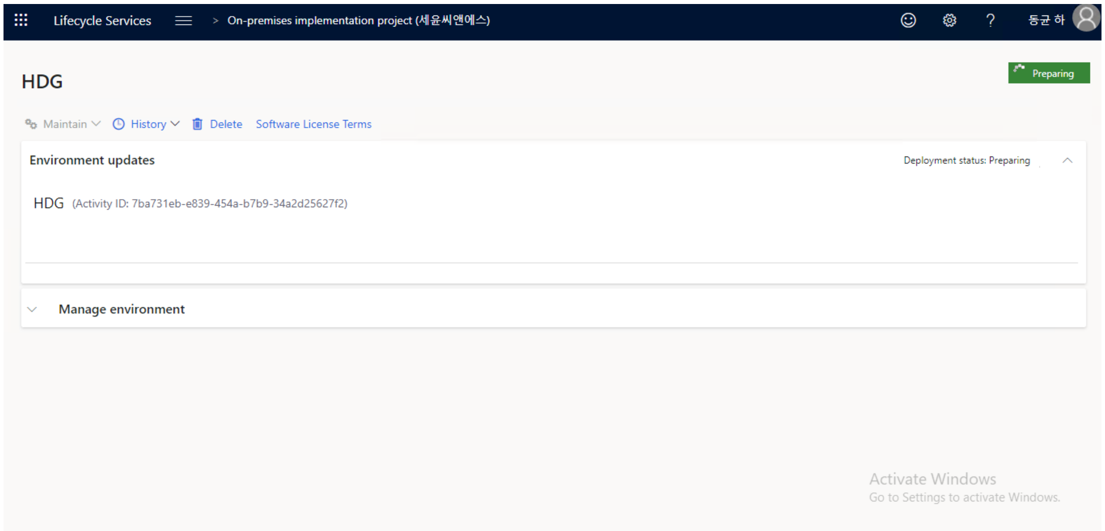
SANDBOX

✓ Environment HDG state: Preparing

Refresh state

Full details

4. Click Full details to take you to the environment details page, as shown below.



Lifecycle Services > On-premises implementation project (세윤씨앤에스) 동균 하

HDG

Preparing

Maintain History Delete Software License Terms

Environment updates

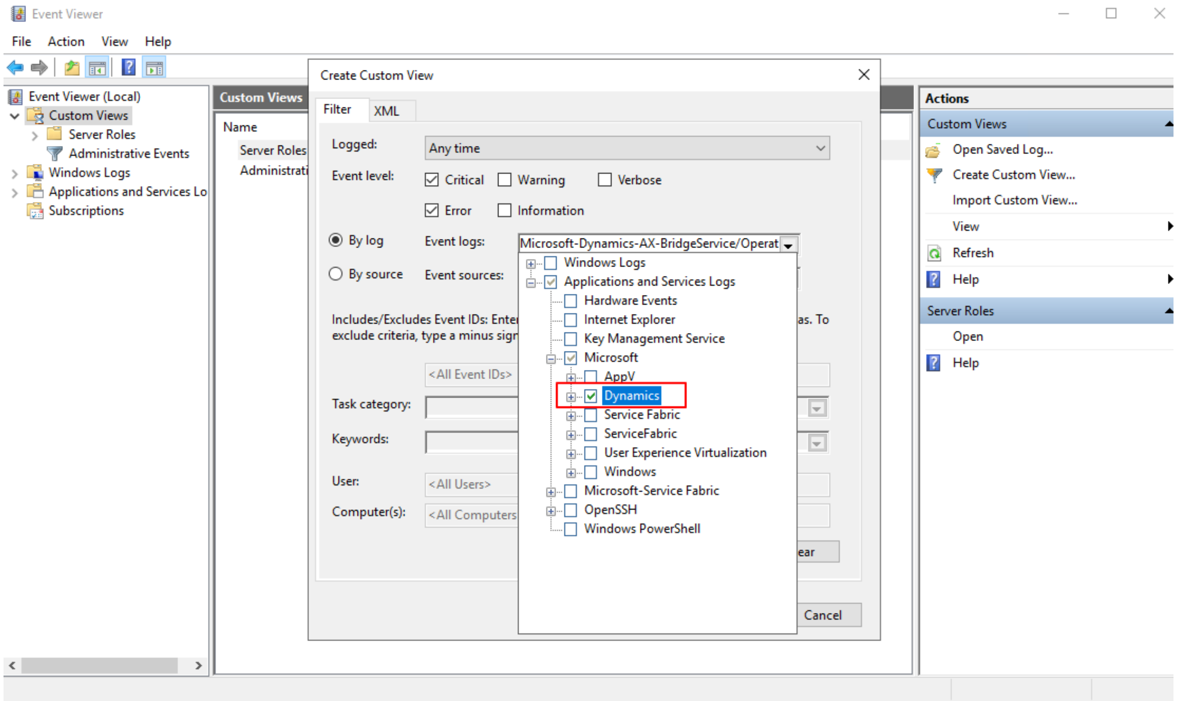
Deployment status: Preparing

HDG (Activity ID: 7ba731eb-e839-454a-b7b9-34a2d25627f2)

Manage environment

Activate Windows
Go to Settings to activate Windows.

5. If the deployment fails, check Event viwer for each service fabric nodes.



Logged: Any time

Event level: ☑ Critical ☐ Warning ☐ Verbose

☑ Error ☐ Information

● By log Event logs: Microsoft-Dynamics-AX-BridgeService/Operat

○ By source Event sources:

Includes/Excludes Event IDs: Ente… exclude criteria, type a minus sign… as. To

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers

- ☐ Windows Logs
- ☑ Applications and Services Logs
  - ☐ Hardware Events
  - ☐ Internet Explorer
  - ☐ Key Management Service
  - ☑ Microsoft
    - ☐ AppV
    - ☑ Dynamics
    - ☐ Service Fabric
    - ☐ ServiceFabric
    - ☐ User Experience Virtualization
    - ☐ Windows
  - ☐ Microsoft-Service Fabric
  - ☐ OpenSSH
  - ☐ Windows PowerShell

1.24 Connect to your Finance + Operations environement

In a web browser, go to https://[yourD365FOdomain]/namespaces/AXSF.