Configure LDAPS on a Windows Server

The guide is split into 3 sections:

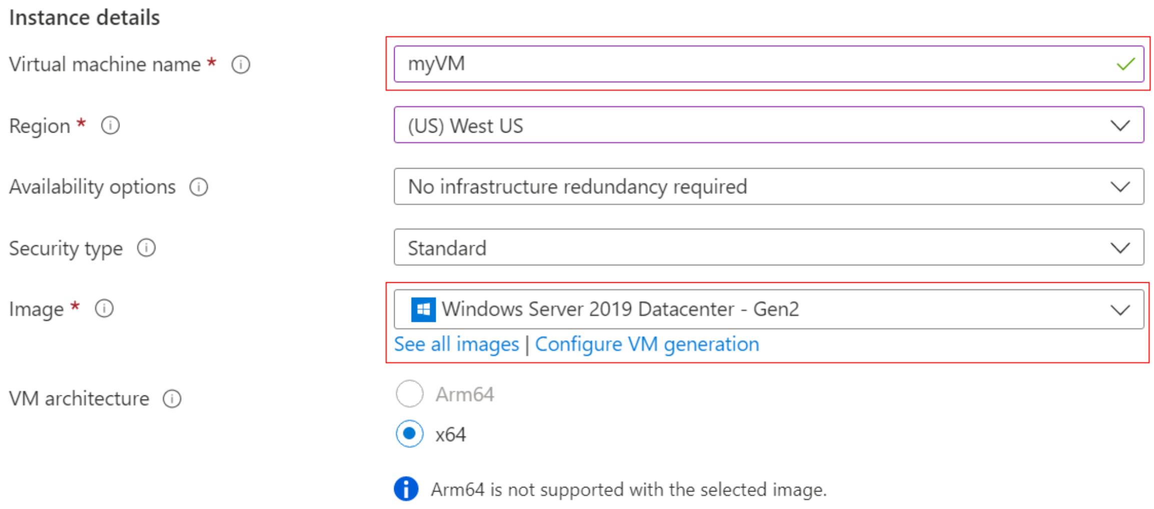
- Create a Windows Server VM in Azure
- Setup LDAP using AD LDS (Active Directory Lightweight Directory Services)
- Setup LDAPS (LDAP over SSL)

○ *Create a Windows Server VM in Azure*

Create a VM named “ldapstest” Windows Server 2012 R2 Datacenter Standard DS12 using the instructions here:

Create virtual machine

1. Enter *virtual machines* in the search.
2. Under **Services**, select **Virtual machines**.
3. In the **Virtual machines** page, select **Create** and then **Azure virtual machine**. The **Create a virtual machine** page opens.
4. Under **Instance details**, enter *myVM* for the **Virtual machine name** and choose *Windows Server 2019 Datacenter - Gen 2* for the **Image**. Leave the other defaults.



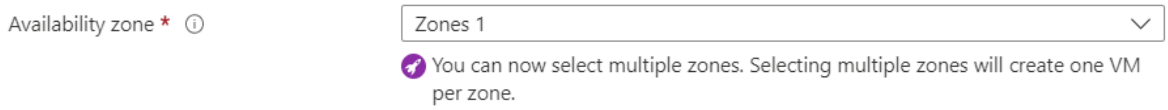
Instance details

Virtual machine name *	myVM
Region *	(US) West US
Availability options	No infrastructure redundancy required
Security type	Standard
Image *	Windows Server 2019 Datacenter - Gen2 See all images | Configure VM generation
VM architecture	○ Arm64 ● x64

Arm64 is not supported with the selected image.

Note

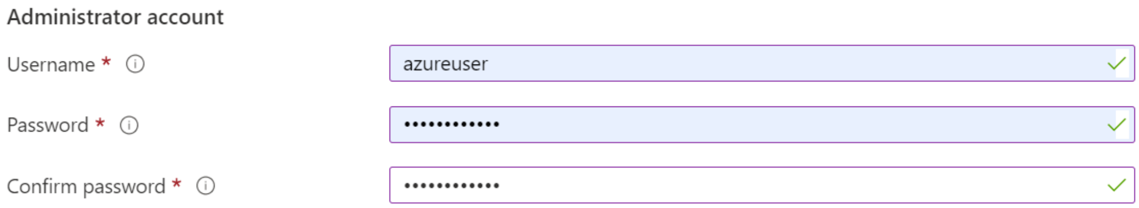
Some users will now see the option to create VMs in multiple zones.



Availability zone * ⓘ Zones 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone.

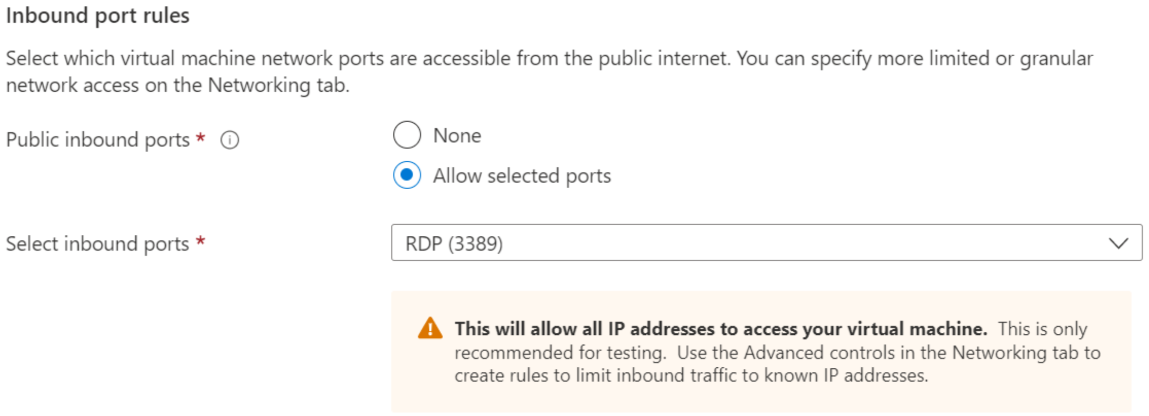
5. Under **Administrator account**, provide a username, such as *azureuser* and a password. The password must be at least 12 characters long and meet the defined complexity requirements.



Administrator account

Username * ⓘ	azureuser ✓
Password * ⓘ	•••••••••••• ✓
Confirm password * ⓘ	•••••••••••• ✓

6. Under **Inbound port rules**, choose **Allow selected ports** and then select **RDP (3389)** and **HTTP (80)** from the drop-down.



Inbound port rules

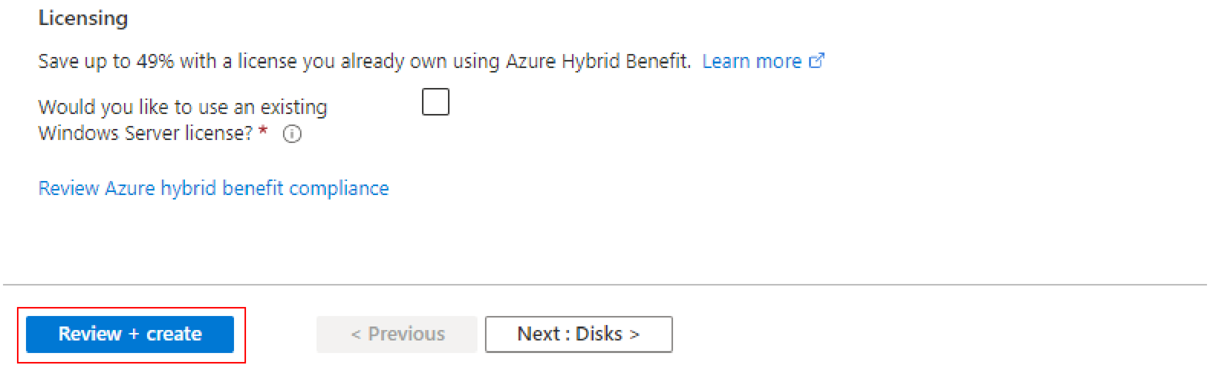
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ ○ None ● Allow selected ports

Select inbound ports * RDP (3389)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

7. Leave the remaining defaults and then select the **Review + create** button at the bottom of the page.



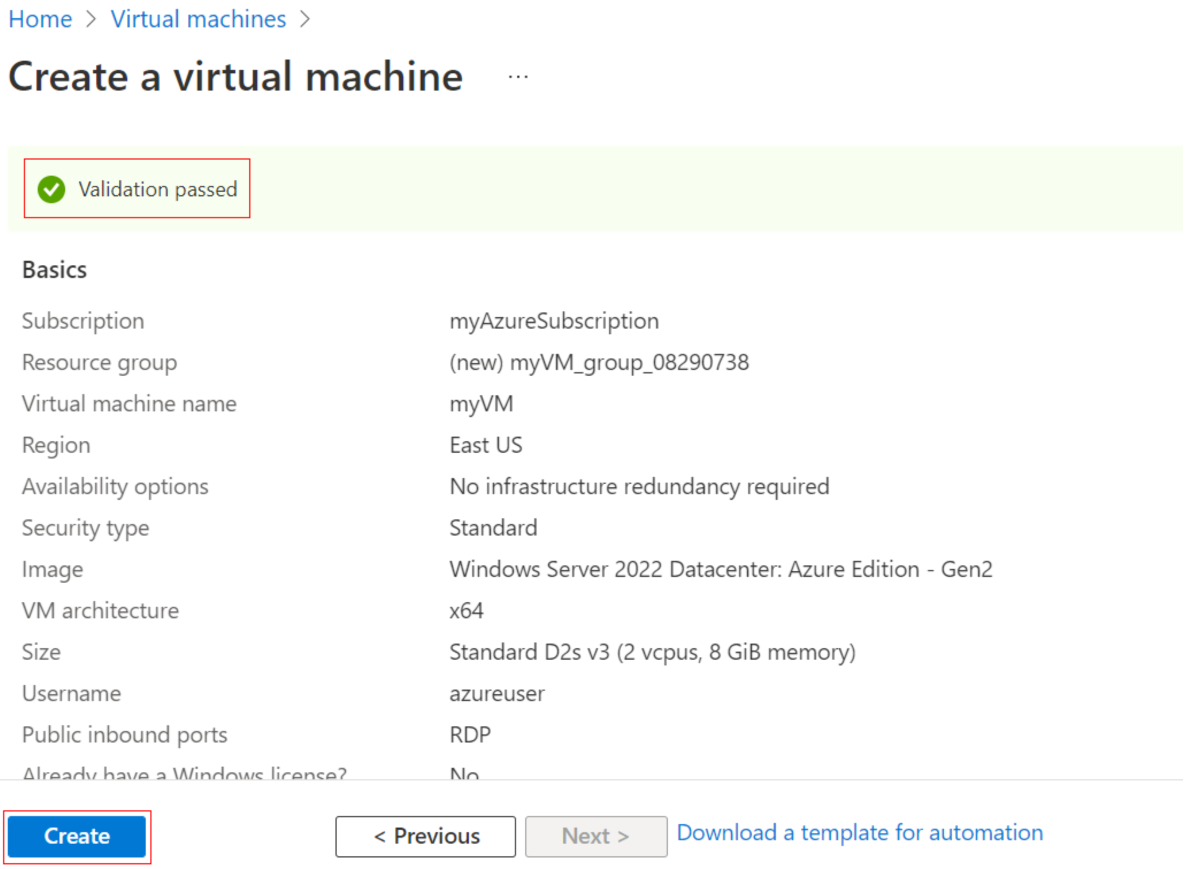
Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. Learn more

Would you like to use an existing Windows Server license? * ⓘ □

Review Azure hybrid benefit compliance

8. After validation runs, select the **Create** button at the bottom of the page.



Home > Virtual machines >

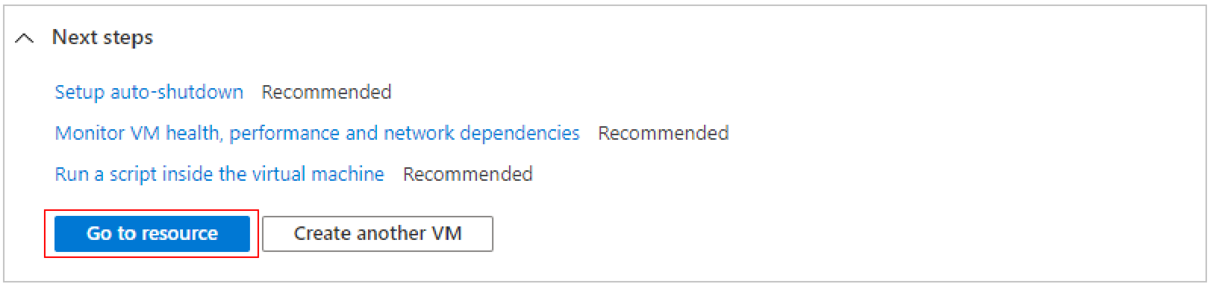
Create a virtual machine ...

Validation passed

Basics

Subscription	myAzureSubscription
Resource group	(new) myVM_group_08290738
Virtual machine name	myVM
Region	East US
Availability options	No infrastructure redundancy required
Security type	Standard
Image	Windows Server 2022 Datacenter: Azure Edition - Gen2
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Username	azureuser
Public inbound ports	RDP
Already have a Windows license?	No

9. After deployment is complete, select **Go to resource**.



Next steps

Setup auto-shutdown Recommended

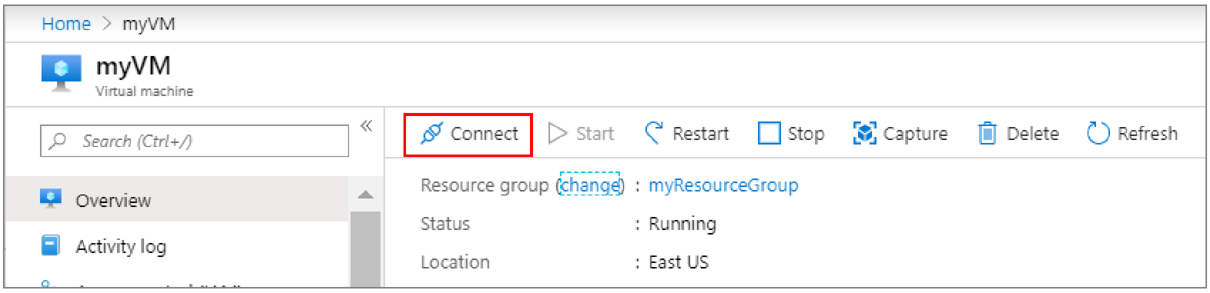
Monitor VM health, performance and network dependencies Recommended

Run a script inside the virtual machine Recommended

Connect to virtual machine

Create a remote desktop connection to the virtual machine. These directions tell you how to connect to your VM from a Windows computer. On a Mac, you need an RDP client such as this Remote Desktop Client from the Mac App Store.

1. On the overview page for your virtual machine, select the **Connect** > **RDP**.

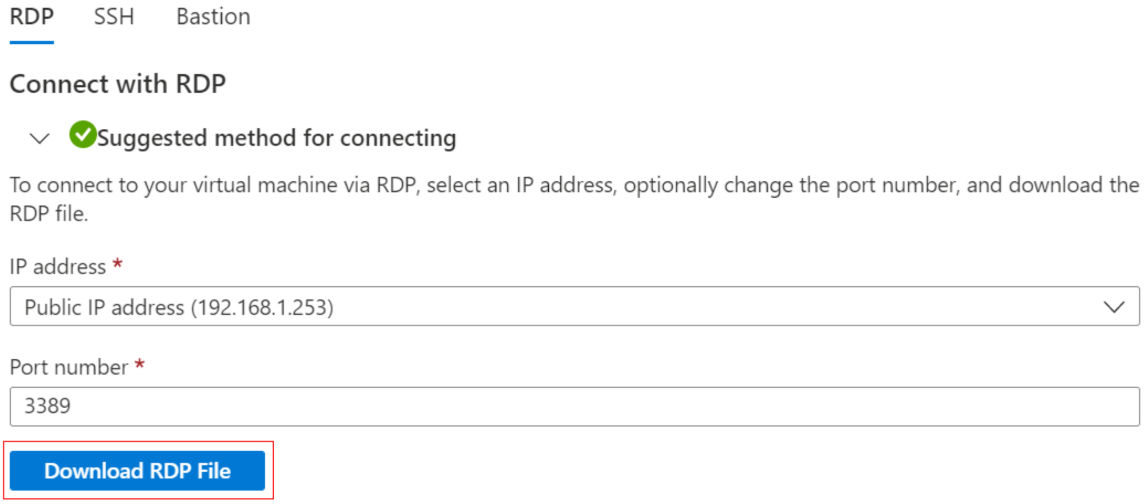


Resource group (change) : myResourceGroup

Status : Running

Location : East US

2. In the **Connect with RDP** tab, keep the default options to connect by IP address, over port 3389, and click **Download RDP file**.



Connect with RDP

Suggested method for connecting

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

IP address *

Public IP address (192.168.1.253)

Port number *

3389

3. Open the downloaded RDP file and click **Connect** when prompted.
4. In the **Windows Security** window, select **More choices** and then **Use a different account**. Type the username as **localhost**\username, enter the password you created for the virtual machine, and then click **OK**.
5. You may receive a certificate warning during the sign-in process.

   Click **Yes** or **Continue** to create the connection.

Install web server

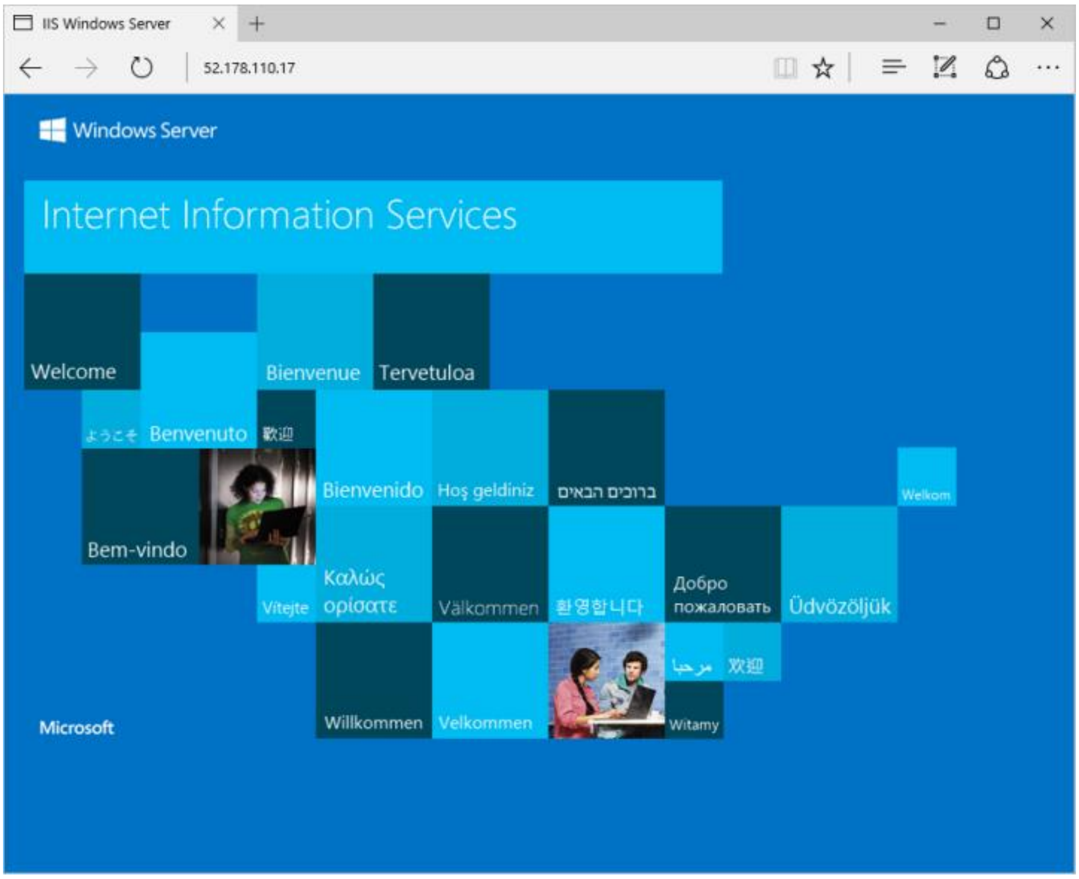
To see your VM in action, install the IIS web server. Open a PowerShell prompt on the VM and run the following command:

Install-WindowsFeature -name Web-Server -IncludeManagementTools

When done, close the RDP connection to the VM.

View the IIS welcome page

In the portal, select the VM and in the overview of the VM, hover over the IP address to show **Copy to clipboard**. Copy the IP address and paste it into a browser tab. The default IIS welcome page will open, and should look like this:

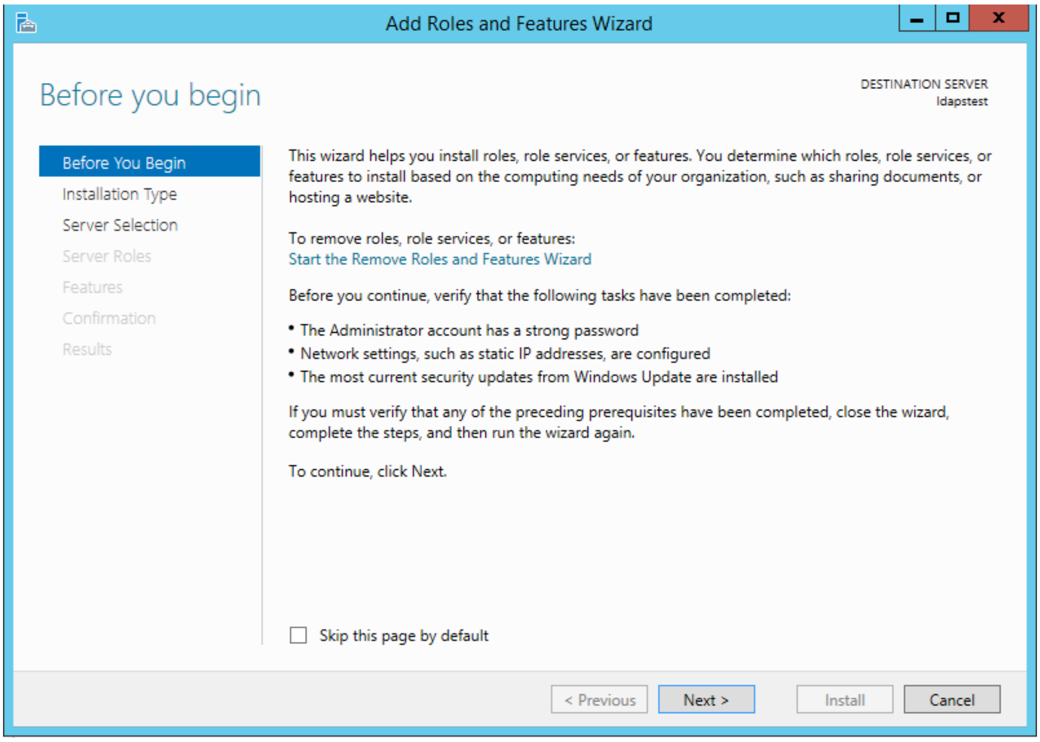


Connect to the VM ldapstest using Remote Desktop Connection.

○ *Setup LDAP using AD LDS*

Now let us add AD LDS in our VM ldapstest

Click on Start --> Server Manager --> Add Roles and Features. Click Next.



Before you begin

DESTINATION SERVER
ldapstest

This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

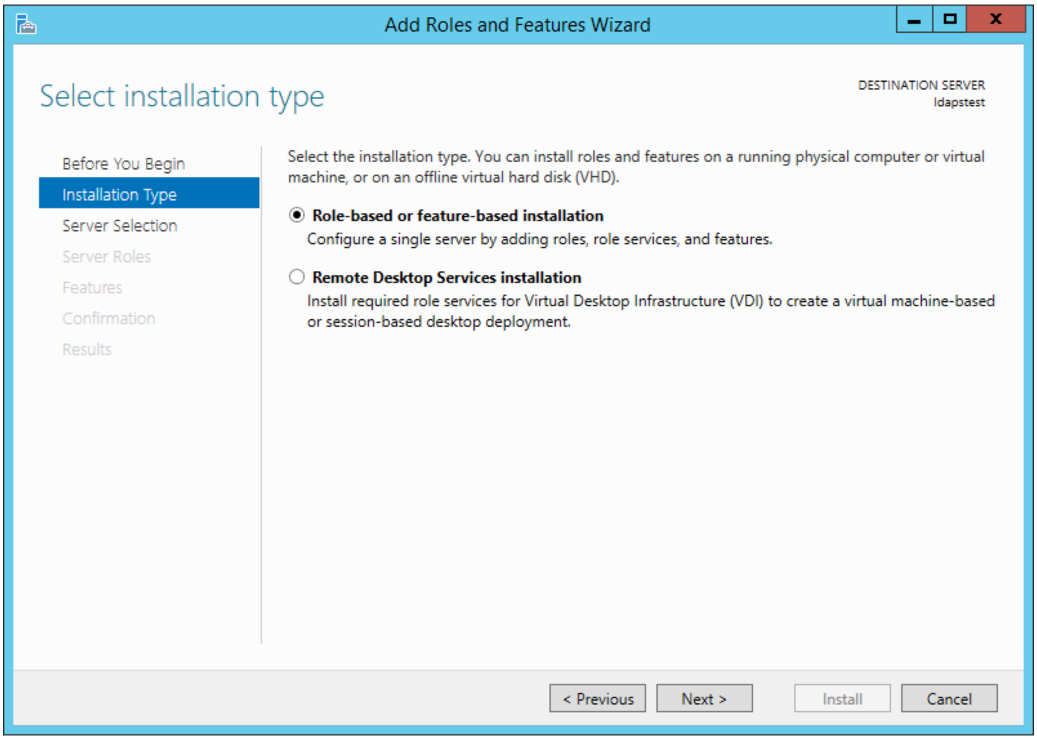
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Choose Role-based or feature-based installation. Click Next.



Select installation type

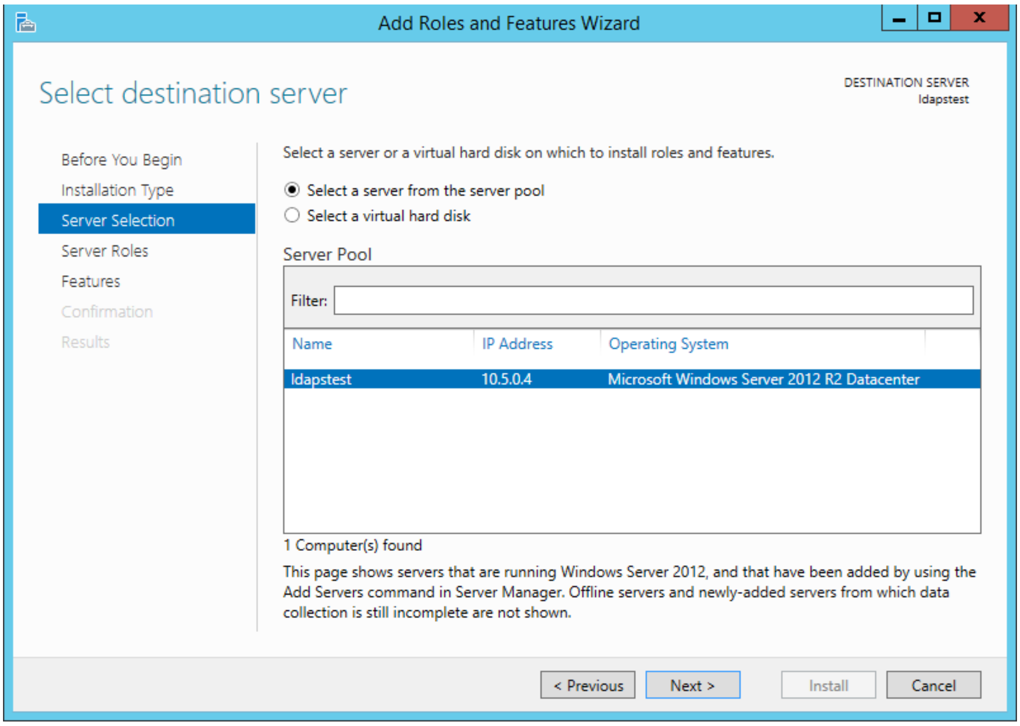
DESTINATION SERVER
ldapstest

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Select ldapstest server from the server pool. Click Next.



Select destination server

DESTINATION SERVER
ldapstest

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

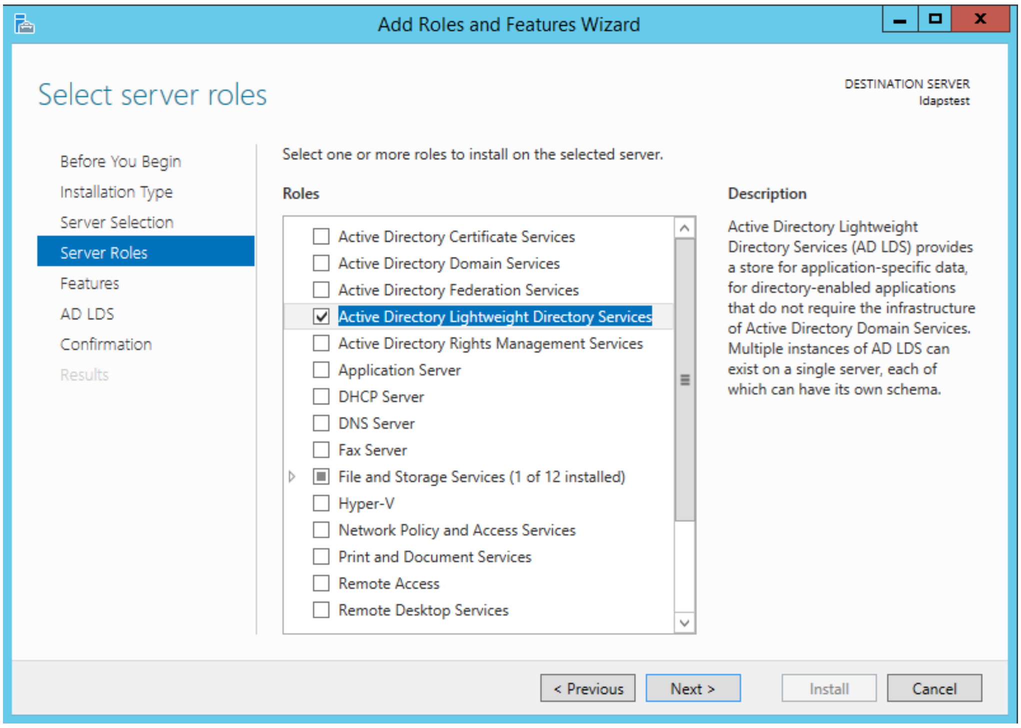
Filter:

Name	IP Address	Operating System
ldapstest	10.5.0.4	Microsoft Windows Server 2012 R2 Datacenter

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Mark Active Directory Lightweight Directory Services from the list of roles and click Next.



Select server roles

DESTINATION SERVER
ldapstest

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

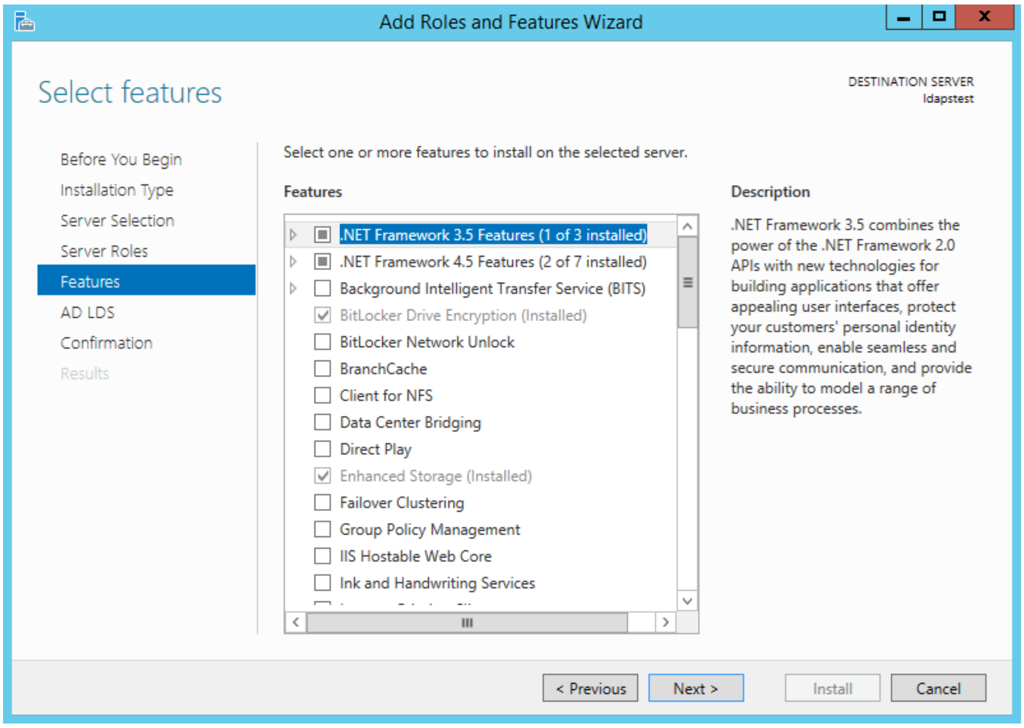
Roles

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- ☑ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ▪ File and Storage Services (1 of 12 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services

Description

Active Directory Lightweight Directory Services (AD LDS) provides a store for application-specific data, for directory-enabled applications that do not require the infrastructure of Active Directory Domain Services. Multiple instances of AD LDS can exist on a single server, each of which can have its own schema.

From the list of features, choose nothing – just click Next.



Select features

DESTINATION SERVER
ldapstest

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

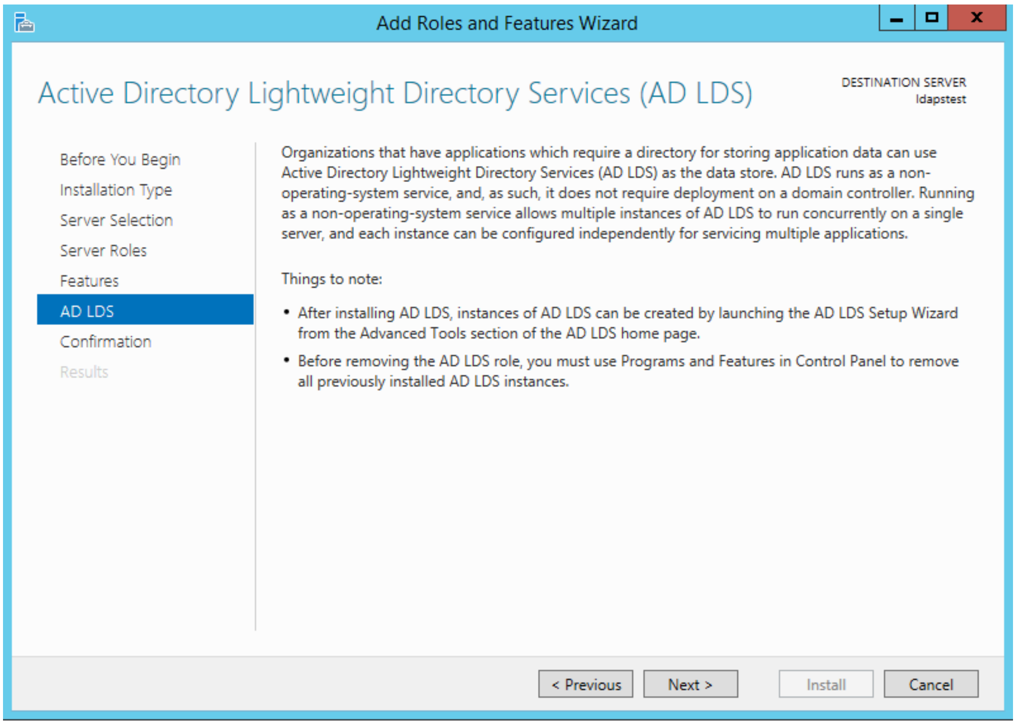
Features

- ▣ .NET Framework 3.5 Features (1 of 3 installed)
- ▣ .NET Framework 4.5 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- ☑ BitLocker Drive Encryption (Installed)
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Direct Play
- ☑ Enhanced Storage (Installed)
- □ Failover Clustering
- □ Group Policy Management
- □ IIS Hostable Web Core
- □ Ink and Handwriting Services

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

Click Next.



Active Directory Lightweight Directory Services (AD LDS)

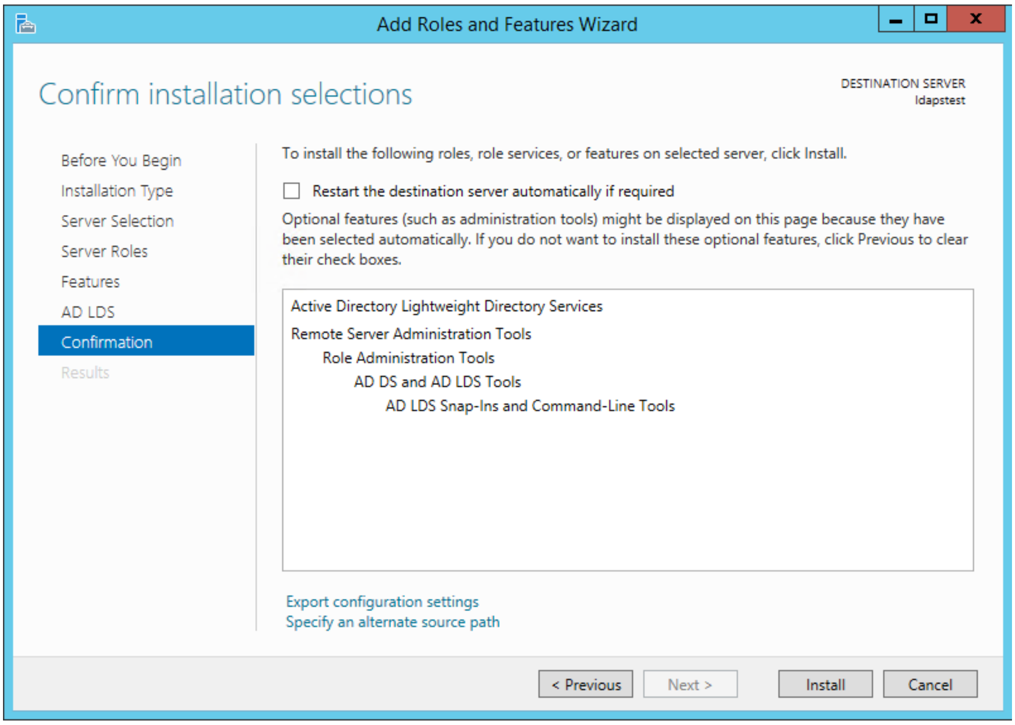
DESTINATION SERVER
ldapstest

Organizations that have applications which require a directory for storing application data can use Active Directory Lightweight Directory Services (AD LDS) as the data store. AD LDS runs as a non-operating-system service, and, as such, it does not require deployment on a domain controller. Running as a non-operating-system service allows multiple instances of AD LDS to run concurrently on a single server, and each instance can be configured independently for servicing multiple applications.

Things to note:

- After installing AD LDS, instances of AD LDS can be created by launching the AD LDS Setup Wizard from the Advanced Tools section of the AD LDS home page.
- Before removing the AD LDS role, you must use Programs and Features in Control Panel to remove all previously installed AD LDS instances.

Click Install to start installation.



To install the following roles, role services, or features on selected server, click Install.

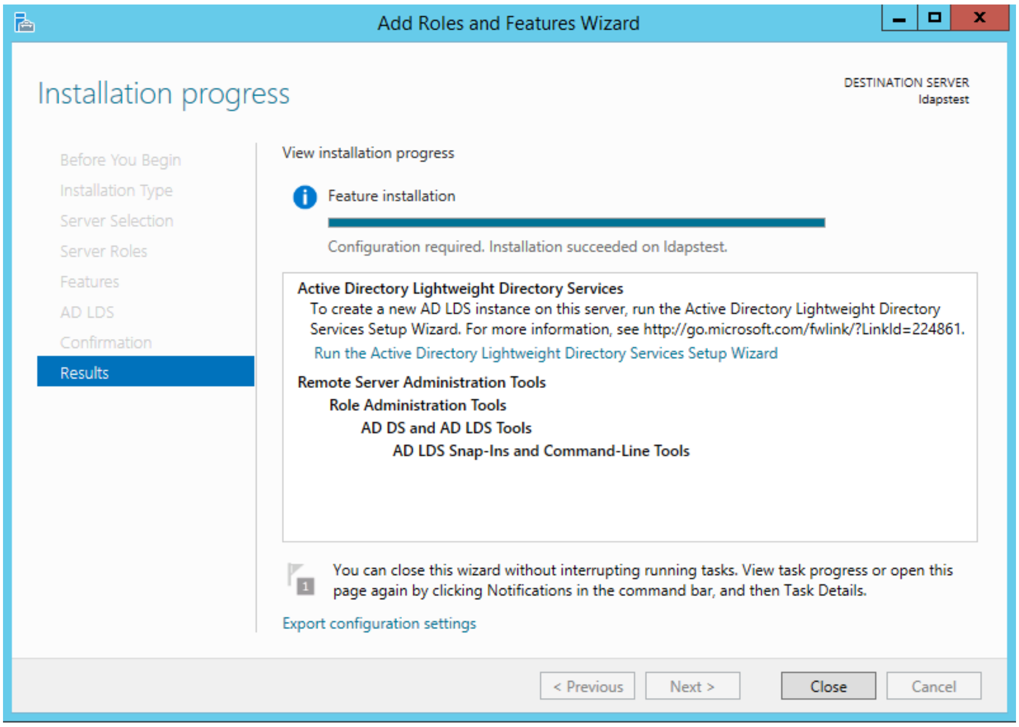
□ Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Lightweight Directory Services
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
AD LDS Snap-Ins and Command-Line Tools

Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

Once installation is complete, click Close.



View installation progress

Feature installation

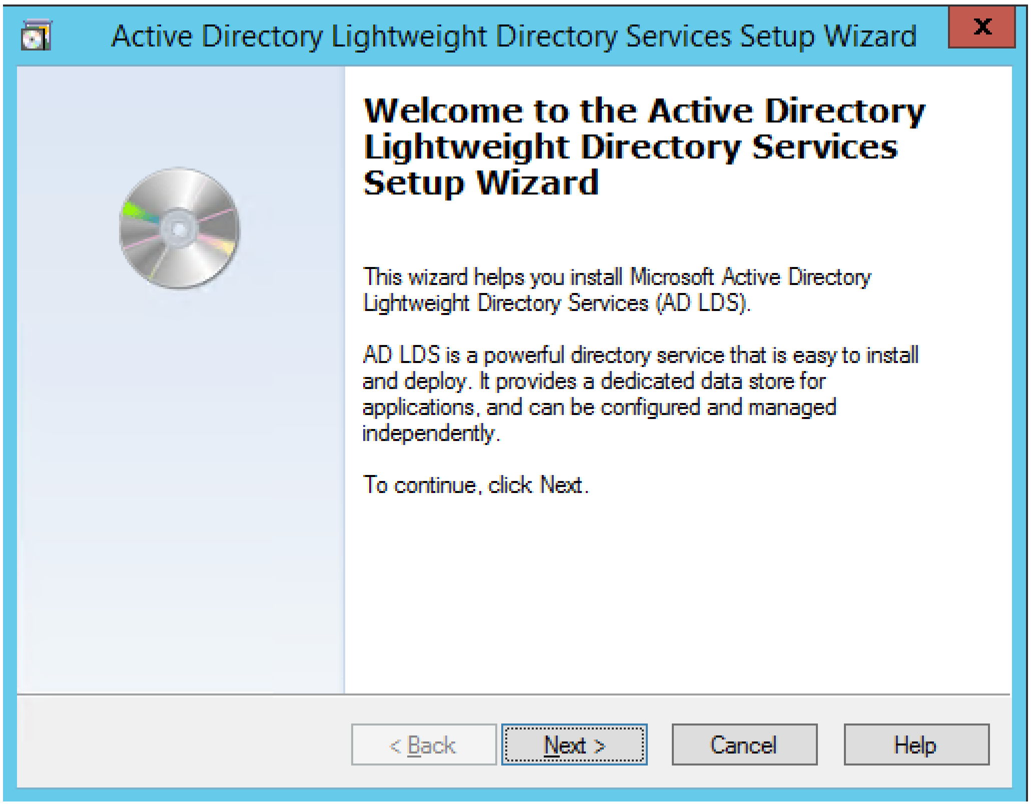
Configuration required. Installation succeeded on ldapstest.

Active Directory Lightweight Directory Services
To create a new AD LDS instance on this server, run the Active Directory Lightweight Directory Services Setup Wizard. For more information, see http://go.microsoft.com/fwlink/?LinkId=224861.
Run the Active Directory Lightweight Directory Services Setup Wizard

Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
AD LDS Snap-Ins and Command-Line Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Now we have successfully set up AD LDS Role. Let us create a new AD LDS Instance “CONTOSO” using the wizard. Click the “Run the Active Directory Lightweight Directory Services Setup Wizard” in the above screen. And then Click Close.



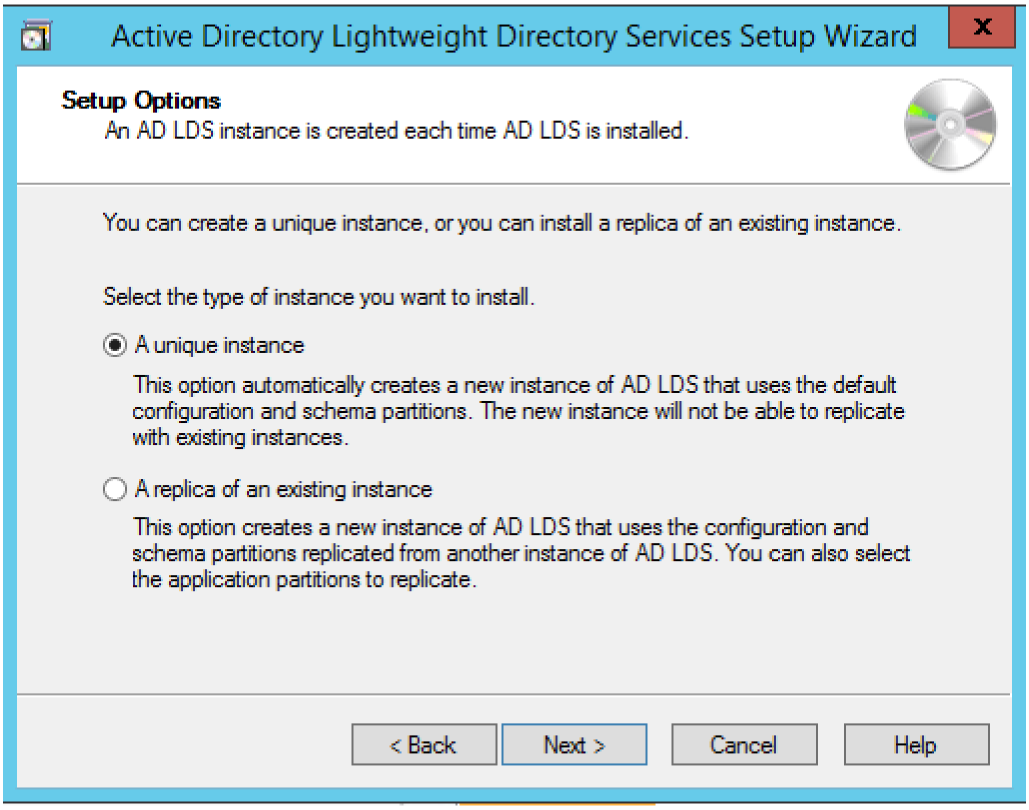
Welcome to the Active Directory Lightweight Directory Services Setup Wizard

This wizard helps you install Microsoft Active Directory Lightweight Directory Services (AD LDS).

AD LDS is a powerful directory service that is easy to install and deploy. It provides a dedicated data store for applications, and can be configured and managed independently.

To continue, click Next.

Choose Unique Instance since we are setting it up for the first time.



Setup Options

An AD LDS instance is created each time AD LDS is installed.

You can create a unique instance, or you can install a replica of an existing instance.

Select the type of instance you want to install.

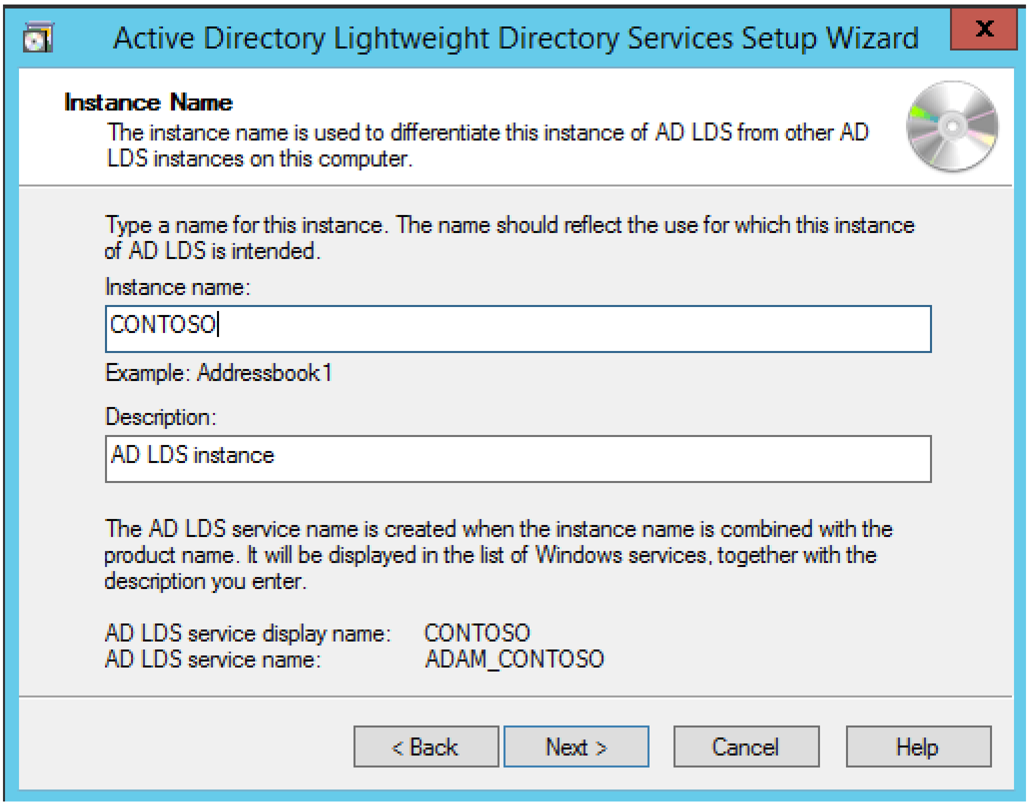
● A unique instance

This option automatically creates a new instance of AD LDS that uses the default configuration and schema partitions. The new instance will not be able to replicate with existing instances.

○ A replica of an existing instance

This option creates a new instance of AD LDS that uses the configuration and schema partitions replicated from another instance of AD LDS. You can also select the application partitions to replicate.

Type “CONTOSO” in Instance Name and click Next.



Active Directory Lightweight Directory Services Setup Wizard

Instance Name

The instance name is used to differentiate this instance of AD LDS from other AD LDS instances on this computer.

Type a name for this instance. The name should reflect the use for which this instance of AD LDS is intended.

Instance name:

CONTOSO

Example: Addressbook1

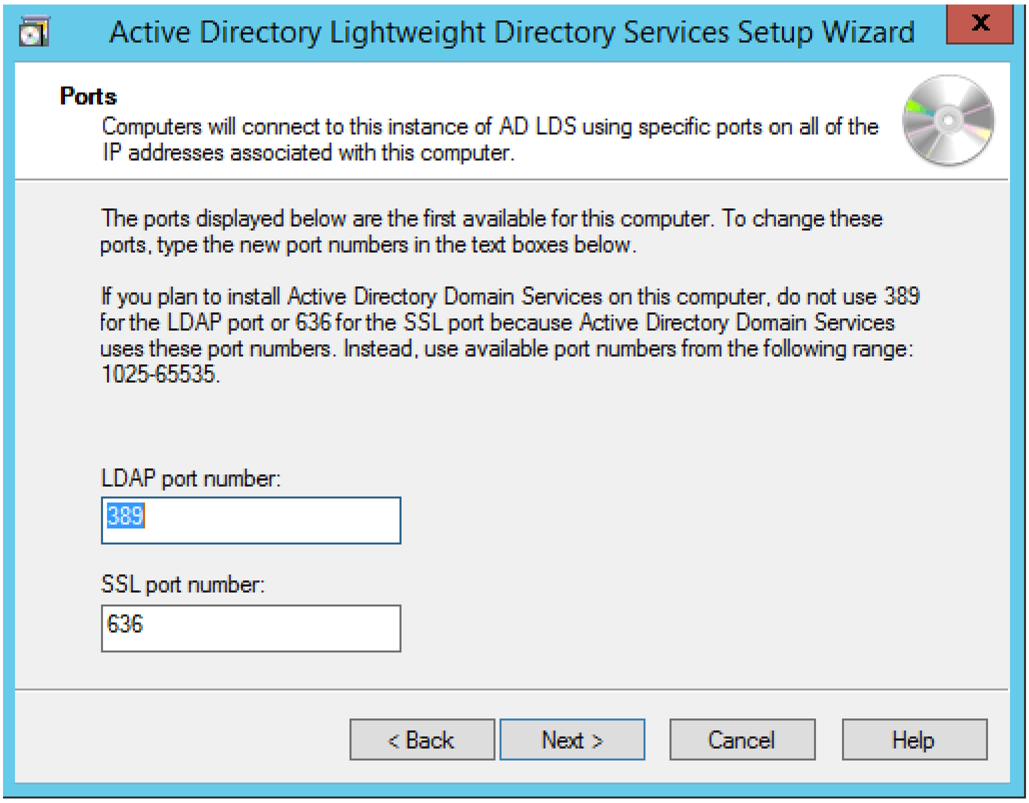
Description:

AD LDS instance

The AD LDS service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services, together with the description you enter.

AD LDS service display name: CONTOSO
AD LDS service name: ADAM_CONTOSO

By Default, LDAP Port is 389 and LDAPS port is 636, let us choose the default values - click Next.



Active Directory Lightweight Directory Services Setup Wizard

Ports

Computers will connect to this instance of AD LDS using specific ports on all of the IP addresses associated with this computer.

The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below.

If you plan to install Active Directory Domain Services on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory Domain Services uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.

LDAP port number:

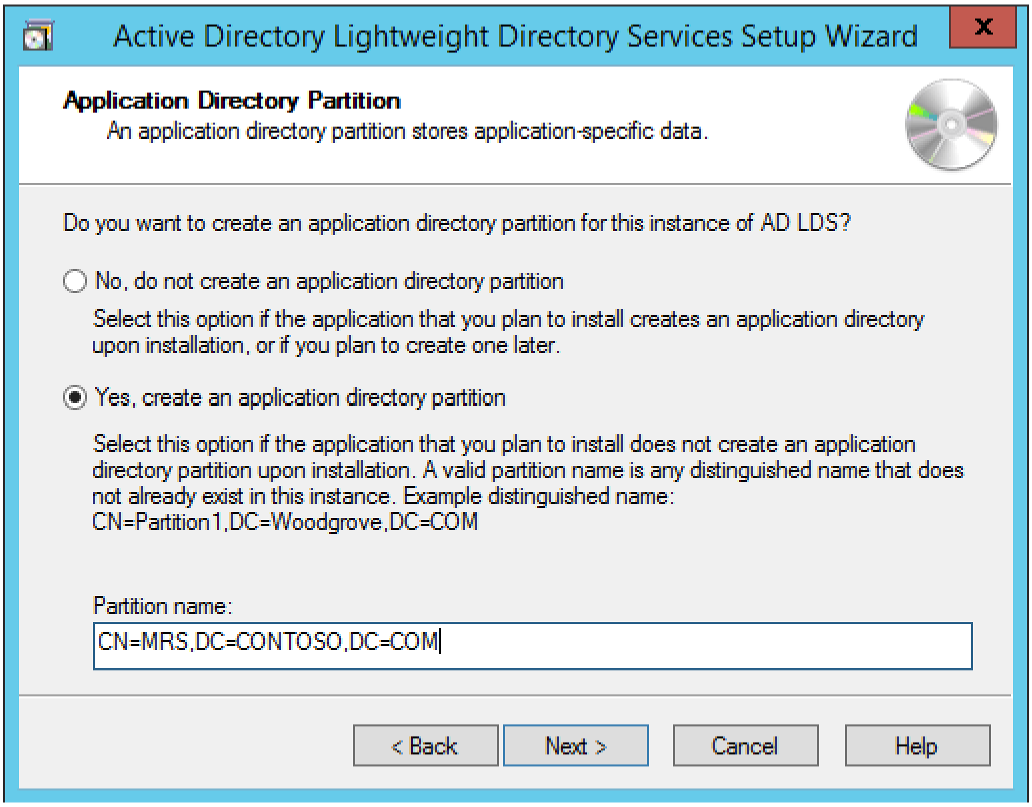
389

SSL port number:

636

Create a new Application Directory Partition named “CN=MRS,DC=CONTOSO,DC=COM”.

Click Next.



Active Directory Lightweight Directory Services Setup Wizard

Application Directory Partition

An application directory partition stores application-specific data.

Do you want to create an application directory partition for this instance of AD LDS?

○ No, do not create an application directory partition

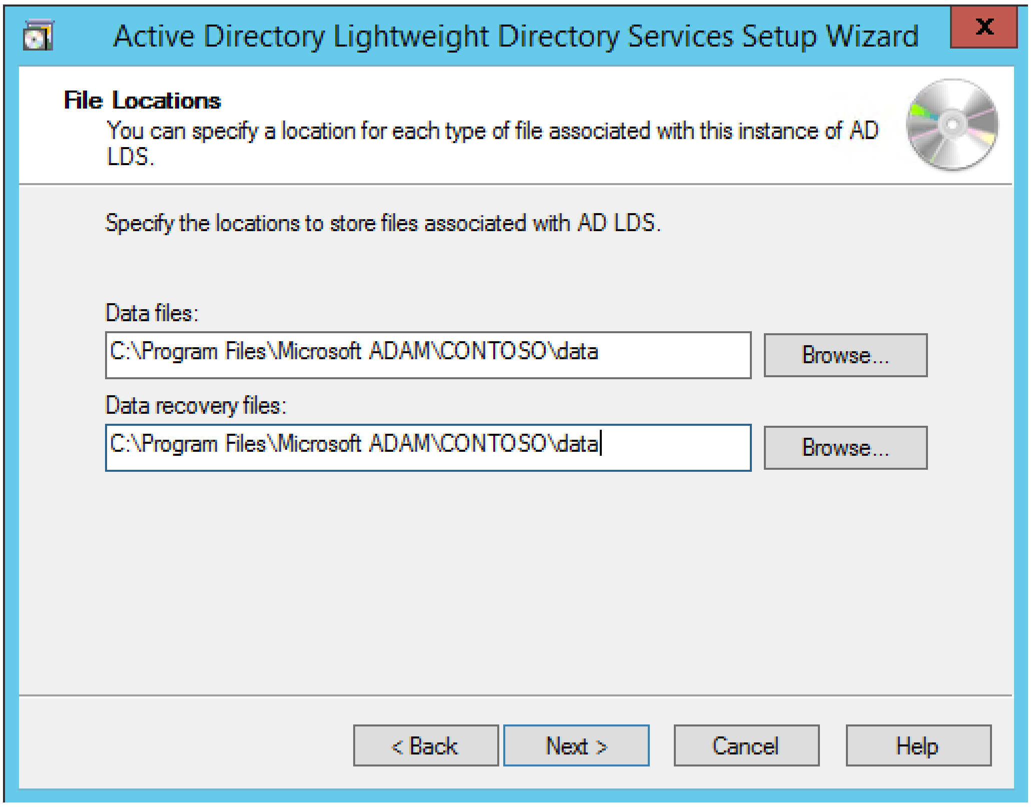
Select this option if the application that you plan to install creates an application directory upon installation, or if you plan to create one later.

● Yes, create an application directory partition

Select this option if the application that you plan to install does not create an application directory partition upon installation. A valid partition name is any distinguished name that does not already exist in this instance. Example distinguished name:
CN=Partition1,DC=Woodgrove,DC=COM

Partition name:
CN=MRS,DC=CONTOSO,DC=COM

Using the default values for storage location of ADLDS files- Click Next.



Active Directory Lightweight Directory Services Setup Wizard

File Locations

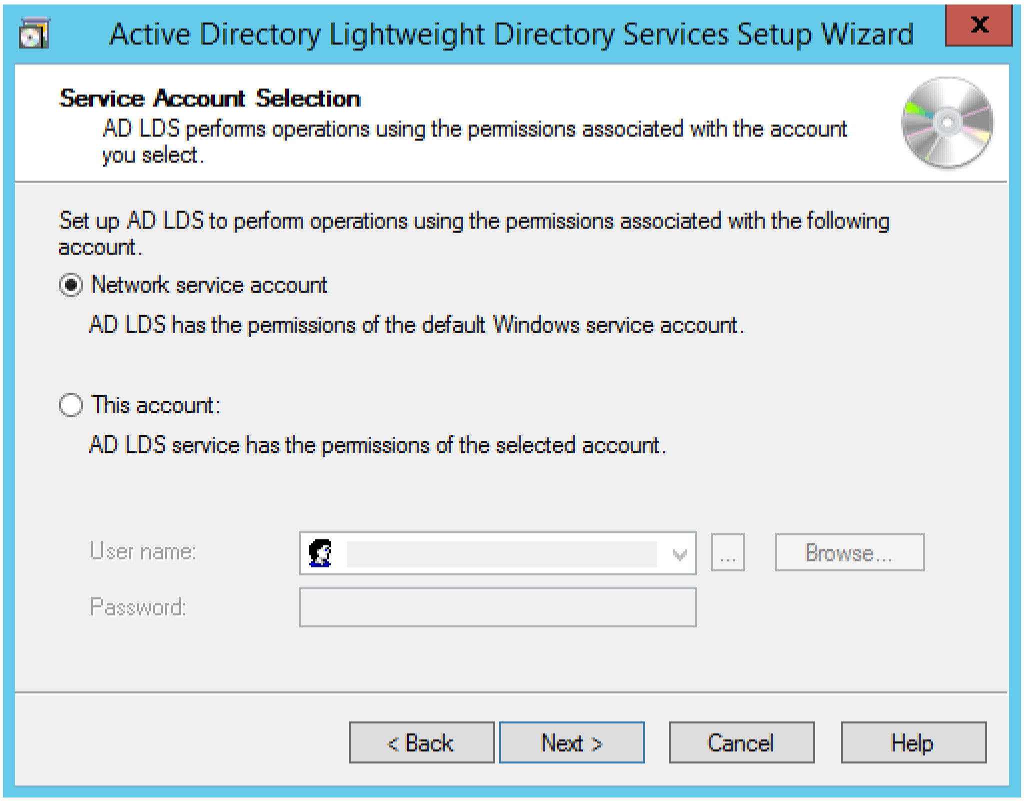
You can specify a location for each type of file associated with this instance of AD LDS.

Specify the locations to store files associated with AD LDS.

Data files:
C:\Program Files\Microsoft ADAM\CONTOSO\data

Data recovery files:
C:\Program Files\Microsoft ADAM\CONTOSO\data

Choosing Network Service Account for running the AD LDS Service.



Active Directory Lightweight Directory Services Setup Wizard

Service Account Selection

AD LDS performs operations using the permissions associated with the account you select.

Set up AD LDS to perform operations using the permissions associated with the following account.

● Network service account

AD LDS has the permissions of the default Windows service account.

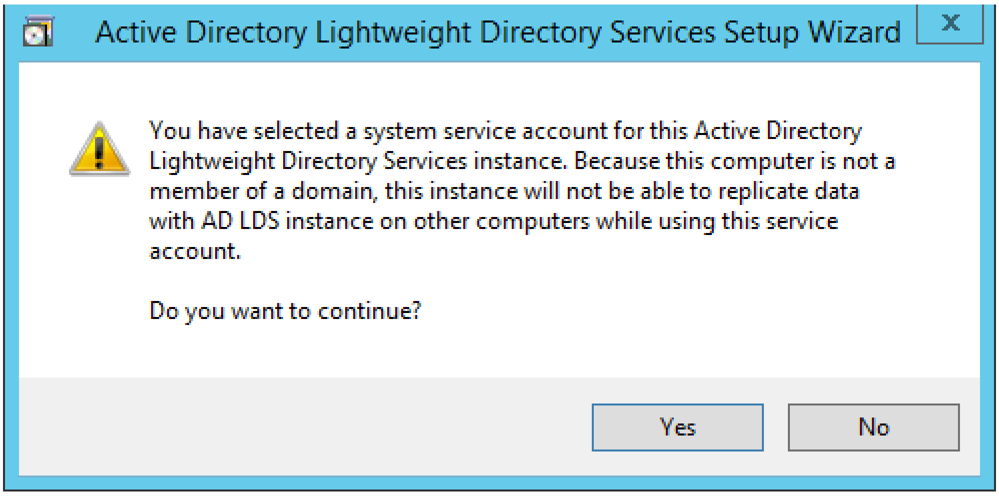
○ This account:

AD LDS service has the permissions of the selected account.

User name:

Password:

You will receive a prompt warning about data replication. Since we are using a single LDAP Server, we can click Yes.

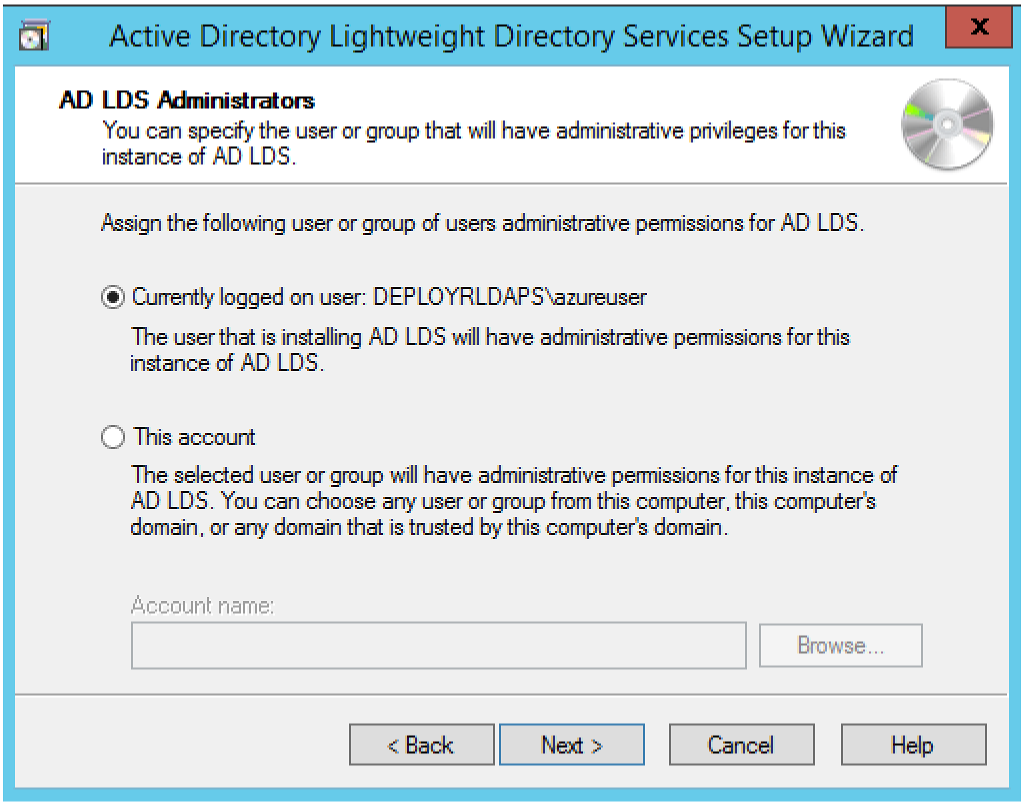


Active Directory Lightweight Directory Services Setup Wizard

You have selected a system service account for this Active Directory Lightweight Directory Services instance. Because this computer is not a member of a domain, this instance will not be able to replicate data with AD LDS instance on other computers while using this service account.

Do you want to continue?

Choosing the currently logged on user as an administrator for the AD LDS Instance. Click Next.



Active Directory Lightweight Directory Services Setup Wizard

AD LDS Administrators

You can specify the user or group that will have administrative privileges for this instance of AD LDS.

Assign the following user or group of users administrative permissions for AD LDS.

● Currently logged on user: DEPLOYRLDAPS\azureuser

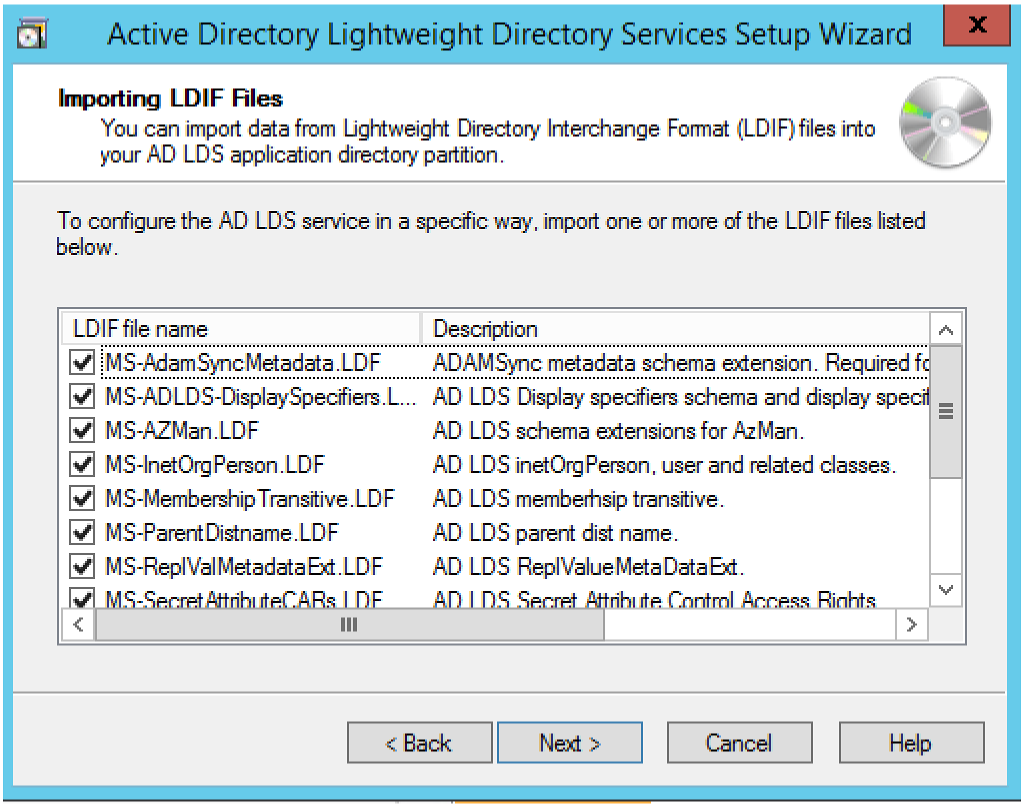
The user that is installing AD LDS will have administrative permissions for this instance of AD LDS.

○ This account

The selected user or group will have administrative permissions for this instance of AD LDS. You can choose any user or group from this computer, this computer's domain, or any domain that is trusted by this computer's domain.

Account name:

Mark all the required LDIF files to import (Here we are marking all files). Click Next.



Active Directory Lightweight Directory Services Setup Wizard

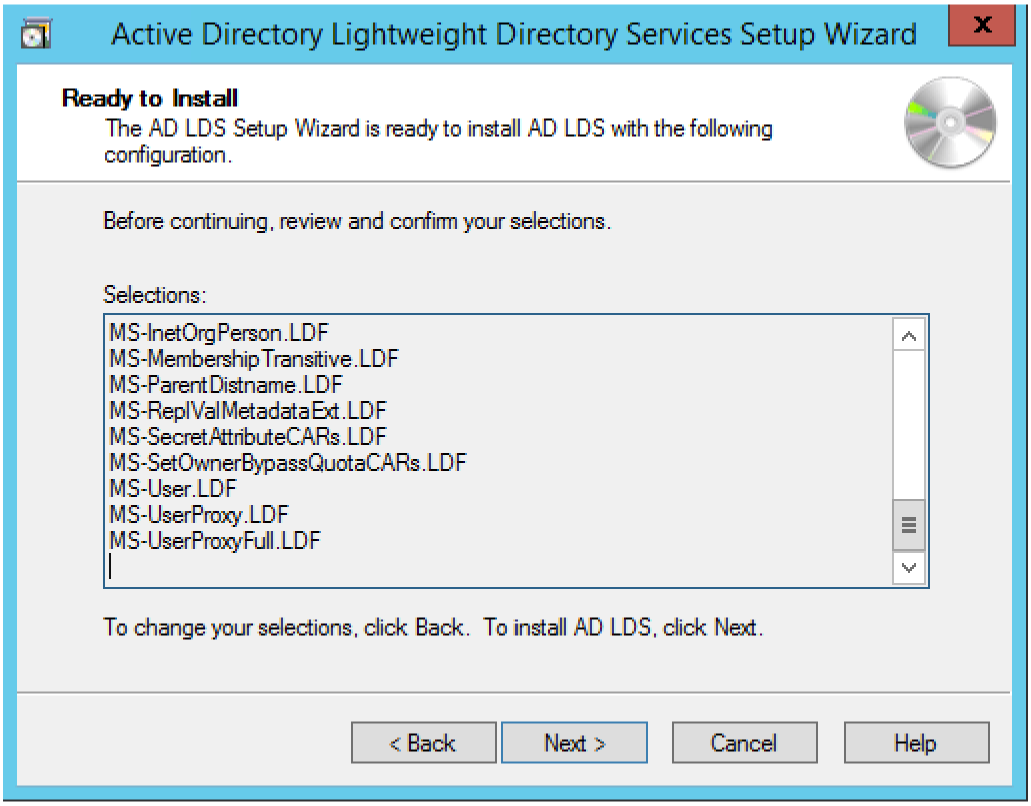
Importing LDIF Files

You can import data from Lightweight Directory Interchange Format (LDIF) files into your AD LDS application directory partition.

To configure the AD LDS service in a specific way, import one or more of the LDIF files listed below.

LDIF file name	Description
☑ MS-AdamSyncMetadata.LDF	ADAMSync metadata schema extension. Required fo
☑ MS-ADLDS-DisplaySpecifiers.L...	AD LDS Display specifiers schema and display speci
☑ MS-AZMan.LDF	AD LDS schema extensions for AzMan.
☑ MS-InetOrgPerson.LDF	AD LDS inetOrgPerson, user and related classes.
☑ MS-MembershipTransitive.LDF	AD LDS memberhsip transitive.
☑ MS-ParentDistname.LDF	AD LDS parent dist name.
☑ MS-ReplValMetadataExt.LDF	AD LDS ReplValueMetaDataExt.
☑ MS-SecretAttributeCARs.LDF	AD LDS Secret Attribute Control Access Rights

Verify that all the selections are right and then Click Next to confirm Installation.



Ready to Install

The AD LDS Setup Wizard is ready to install AD LDS with the following configuration.

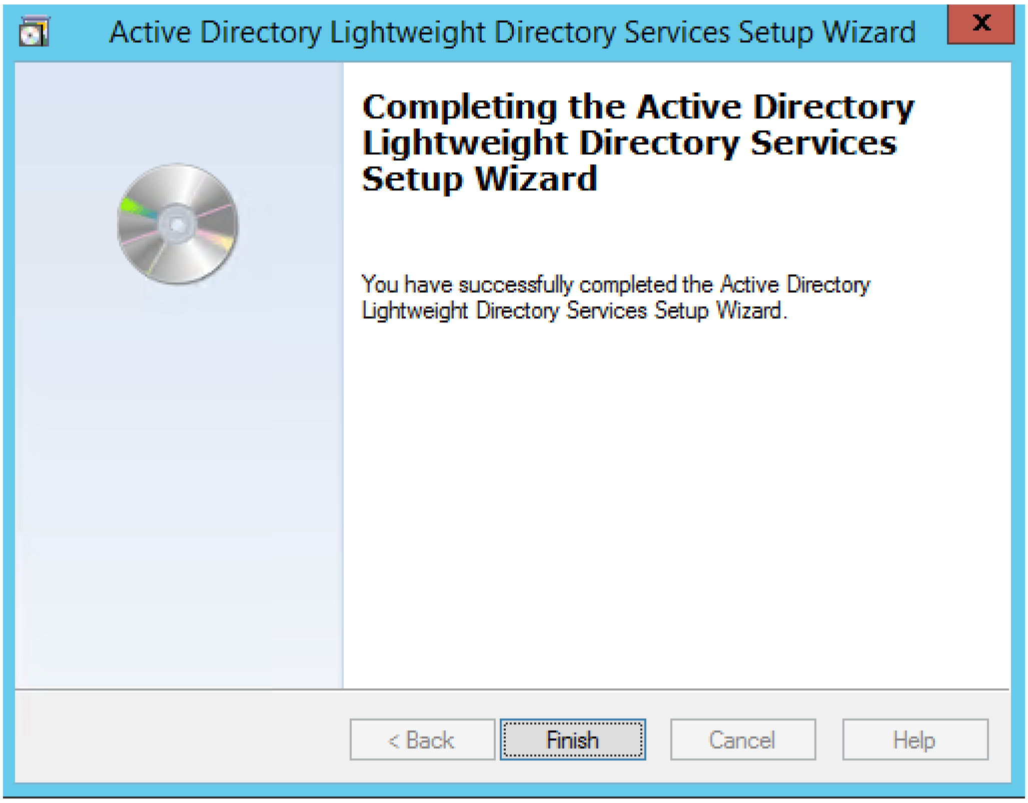
Before continuing, review and confirm your selections.

Selections:

```
MS-InetOrgPerson.LDF
MS-MembershipTransitive.LDF
MS-ParentDistname.LDF
MS-ReplValMetadataExt.LDF
MS-SecretAttributeCARs.LDF
MS-SetOwnerBypassQuotaCARs.LDF
MS-User.LDF
MS-UserProxy.LDF
MS-UserProxyFull.LDF
```

To change your selections, click Back. To install AD LDS, click Next.

Once the instance is setup successfully, click Finish.



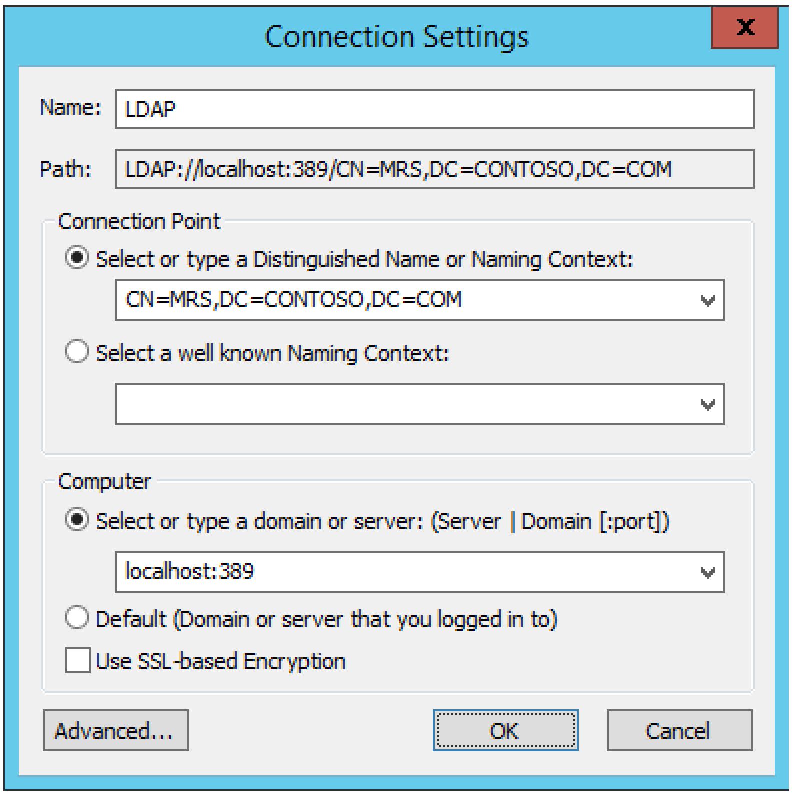
Completing the Active Directory Lightweight Directory Services Setup Wizard

You have successfully completed the Active Directory Lightweight Directory Services Setup Wizard.

< Back
Finish
Cancel
Help

Now let us try to connect to the AD LDS Instance CONTOSO using ADSI Edit. Click on Start --> Search “ADSI Edit” and open it.

Right Click on ADSI Edit Folder (on the left pane) and choose Connect To.. . Fill the following values and Click OK.



Name: LDAP

Path: LDAP://localhost:389/CN=MRS,DC=CONTOSO,DC=COM

Connection Point

● Select or type a Distinguished Name or Naming Context:

CN=MRS,DC=CONTOSO,DC=COM

○ Select a well known Naming Context:

Computer

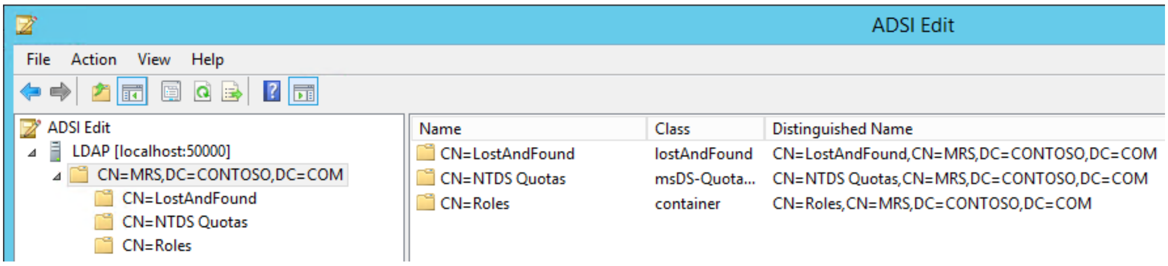
● Select or type a domain or server: (Server | Domain [:port])

localhost:389

○ Default (Domain or server that you logged in to)

□ Use SSL-based Encryption

If the connection is successful, we will be able to browse the Directory CN=MRS,DC=CONTOSO,DC=COM :



ADSI Edit
- LDAP [localhost:50000]
  - CN=MRS,DC=CONTOSO,DC=COM
    - CN=LostAndFound
    - CN=NTDS Quotas
    - CN=Roles

Name	Class	Distinguished Name
CN=LostAndFound	lostAndFound	CN=LostAndFound,CN=MRS,DC=CONTOSO,DC=COM
CN=NTDS Quotas	msDS-Quota...	CN=NTDS Quotas,CN=MRS,DC=CONTOSO,DC=COM
CN=Roles	container	CN=Roles,CN=MRS,DC=CONTOSO,DC=COM

○ *Setup LDAPS (LDAP over SSL)*

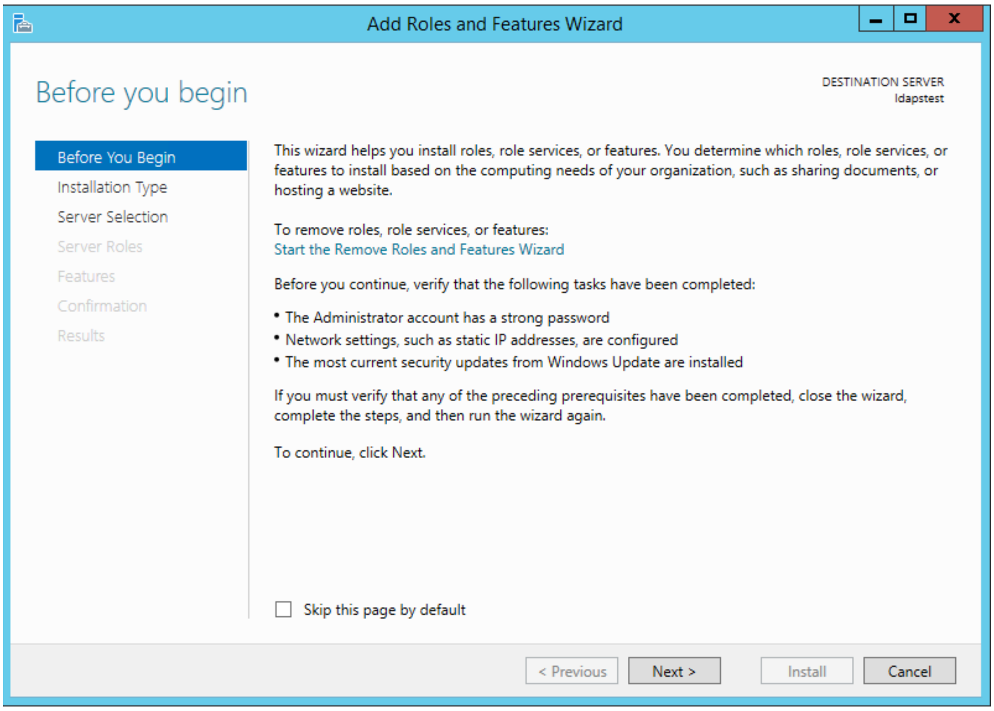
The Certificate to be used for LDAPS must satisfy the following 3 requirements:

- Certificate must be valid for the purpose of Server Authentication. This means that it must also contains the Server Authentication object identifier (OID): 1.3.6.1.5.5.7.3.1

- The Subject name or the first name in the Subject Alternative Name (SAN) must match the Fully Qualified Domain Name (FQDN) of the host machine, such as Subject:CN=contosoldaps. For more information, see How to add a Subject Alternative Name to a secure LDAP certificate.
- The host machine account must have access to the private key.

Now, let's use Active Directory Certificate Services to create a certificate to be used for LDAPS. If you already have a certificate satisfying the above requirements, you can skip this step.

Click on Start --> Server Manager --> Add Roles and Features. Click Next.



This wizard helps you install roles, role services, or features. You determine which roles, role services, or features to install based on the computing needs of your organization, such as sharing documents, or hosting a website.

To remove roles, role services, or features:
Start the Remove Roles and Features Wizard

Before you continue, verify that the following tasks have been completed:

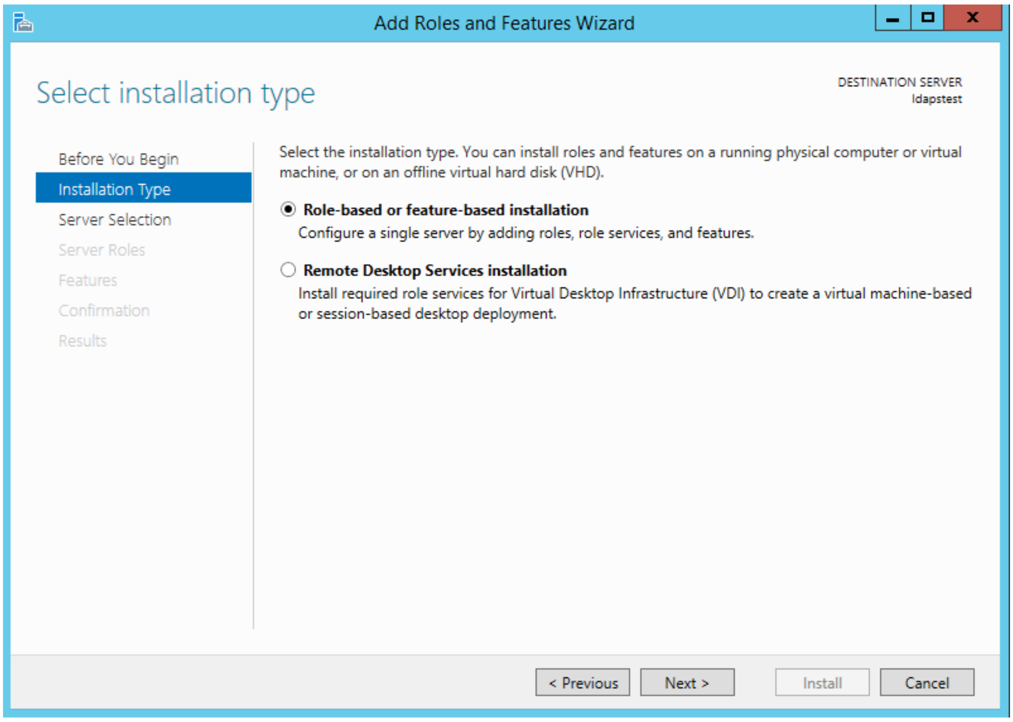
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Choose Role-based or feature-based installation. Click Next.



Add Roles and Features Wizard

Select installation type

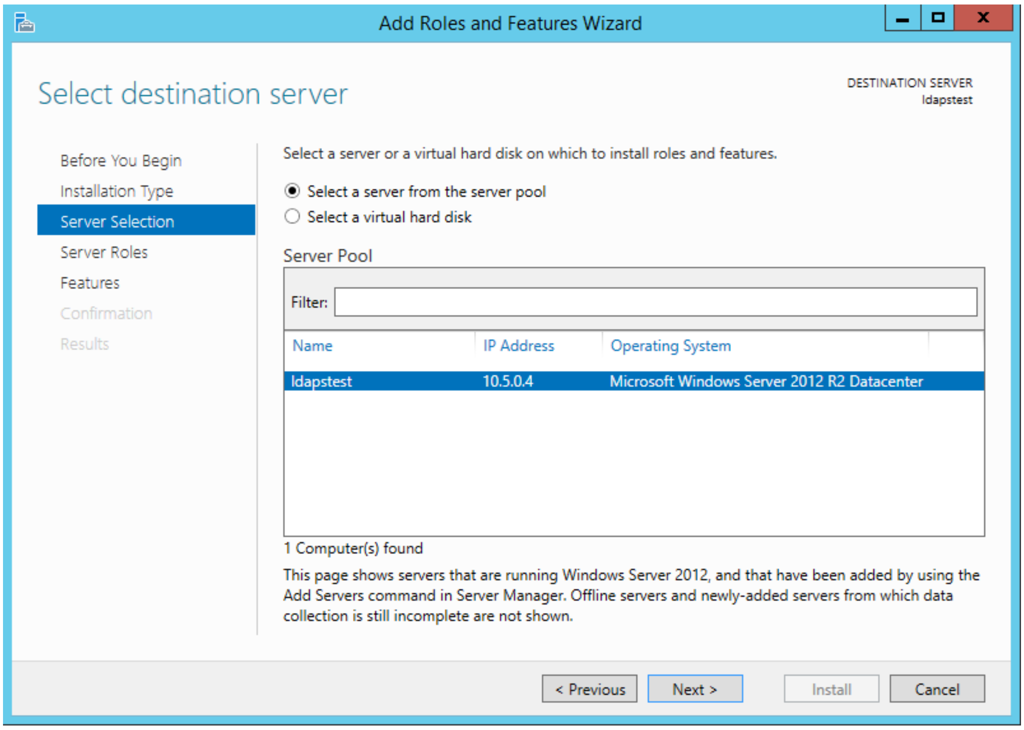
DESTINATION SERVER
ldapstest

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

Select ldapstest server from the server pool. Click Next.



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
ldapstest

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

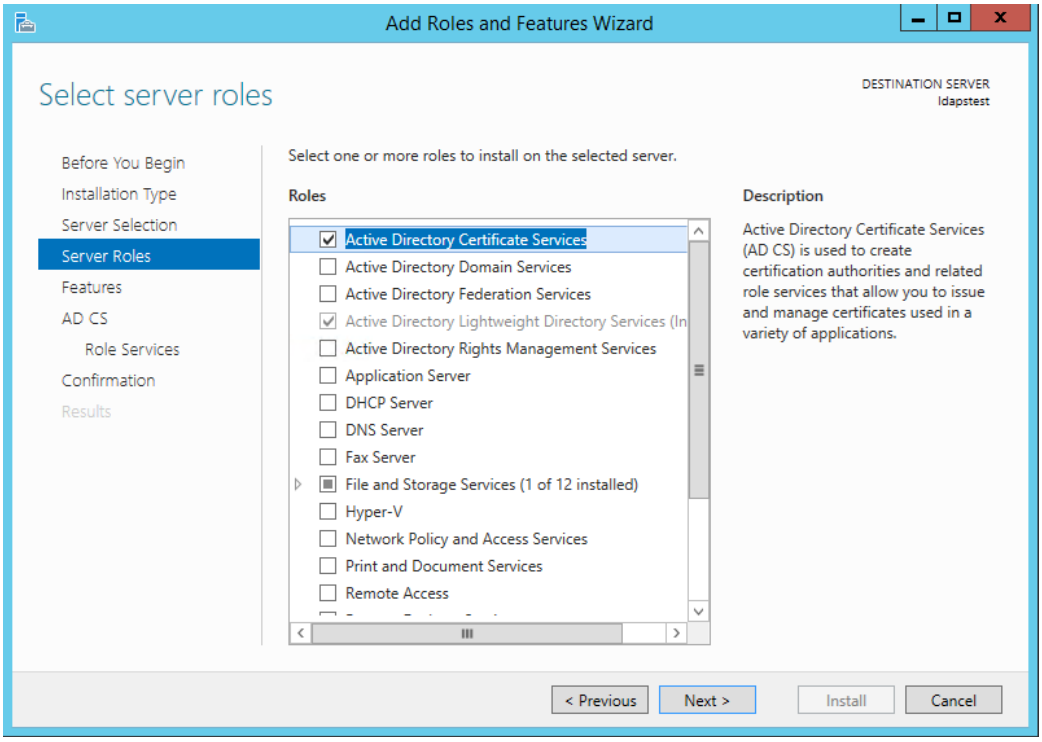
Filter:

Name	IP Address	Operating System
ldapstest	10.5.0.4	Microsoft Windows Server 2012 R2 Datacenter

1 Computer(s) found

This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Choose Active Directory Certificate Services from the list of roles and click Next.



Select server roles

DESTINATION SERVER
ldapstest

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

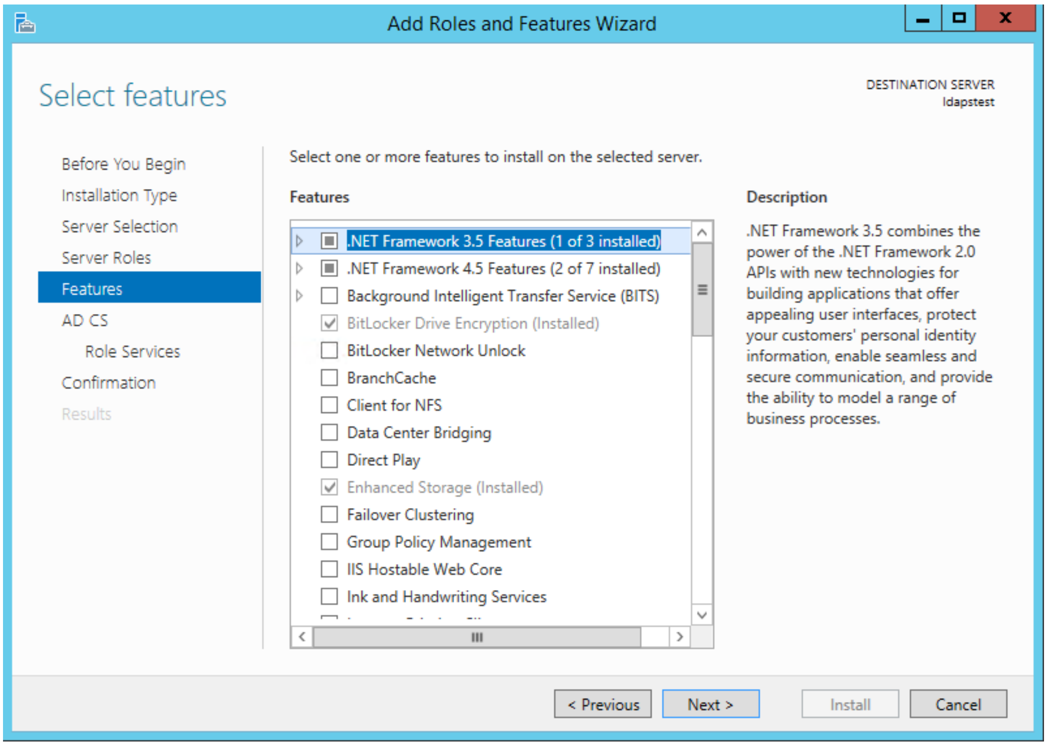
Roles

- ☑ Active Directory Certificate Services
- □ Active Directory Domain Services
- □ Active Directory Federation Services
- ☑ Active Directory Lightweight Directory Services (In
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access

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.

Choose nothing from the list of features and click Next.



Select features

DESTINATION SERVER
ldapstest

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

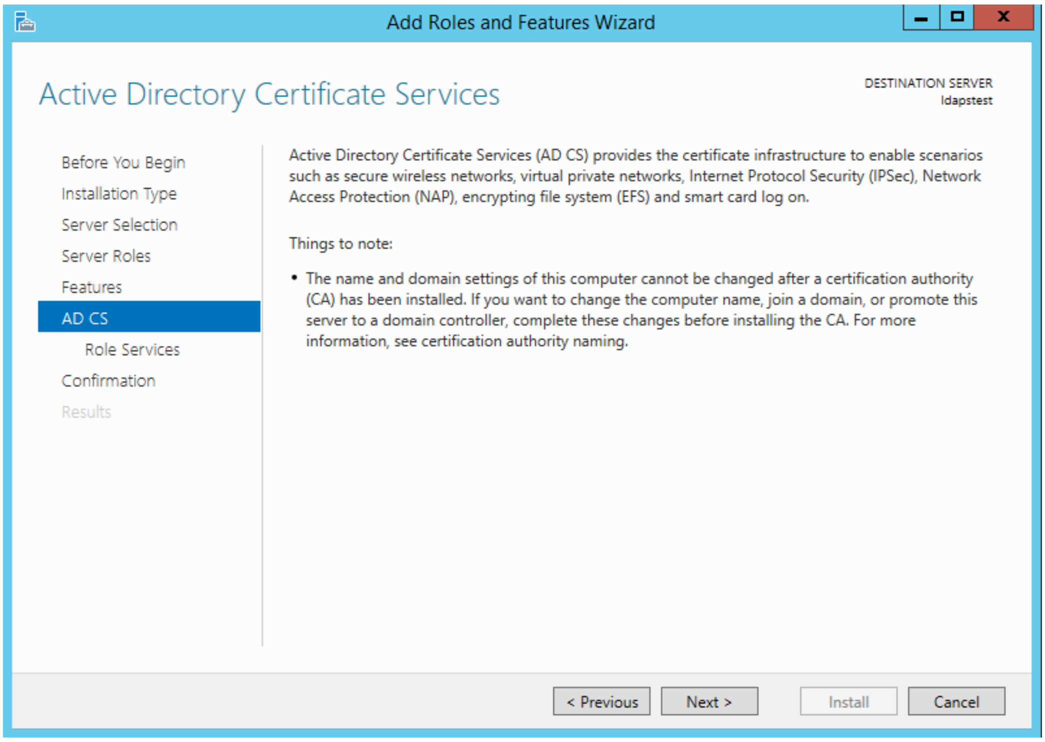
Features

- ▣ .NET Framework 3.5 Features (1 of 3 installed)
- ▣ .NET Framework 4.5 Features (2 of 7 installed)
- □ Background Intelligent Transfer Service (BITS)
- ☑ BitLocker Drive Encryption (Installed)
- □ BitLocker Network Unlock
- □ BranchCache
- □ Client for NFS
- □ Data Center Bridging
- □ Direct Play
- ☑ Enhanced Storage (Installed)
- □ Failover Clustering
- □ Group Policy Management
- □ IIS Hostable Web Core
- □ Ink and Handwriting Services

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.

Click Next.



Active Directory Certificate Services

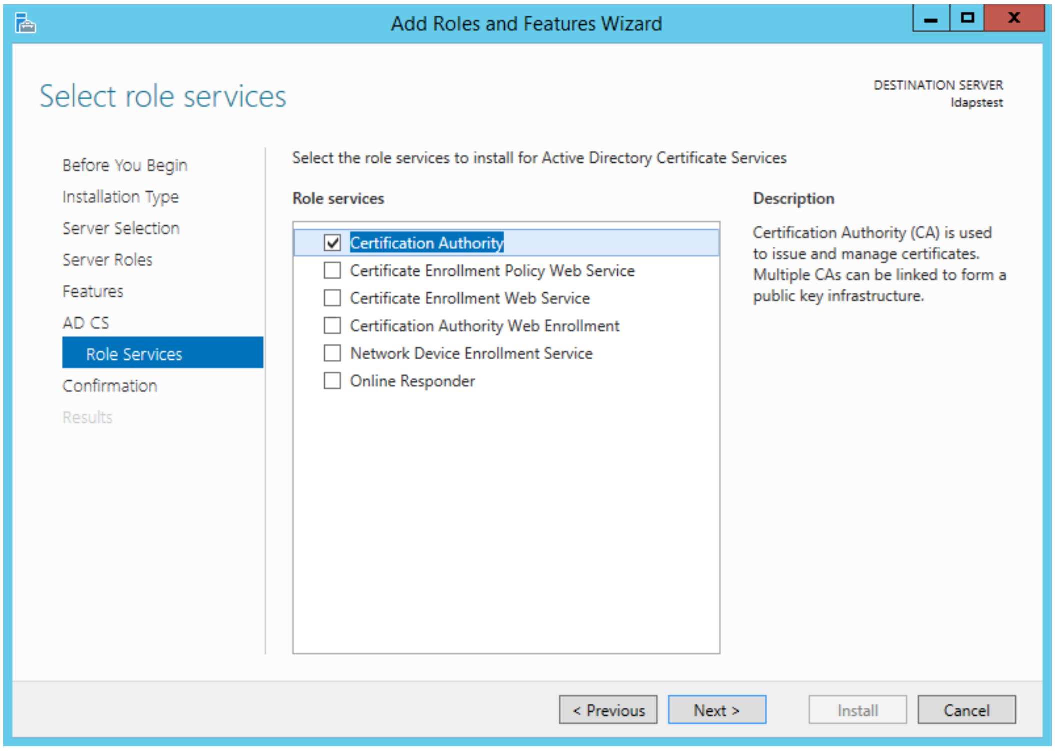
DESTINATION SERVER
ldapstest

Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card log on.

Things to note:

- The name and domain settings of this computer cannot be changed after a certification authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see certification authority naming.

Mark “Certificate Authority” from the list of roles and click Next.



Select role services

DESTINATION SERVER
ldapstest

Select the role services to install for Active Directory Certificate Services

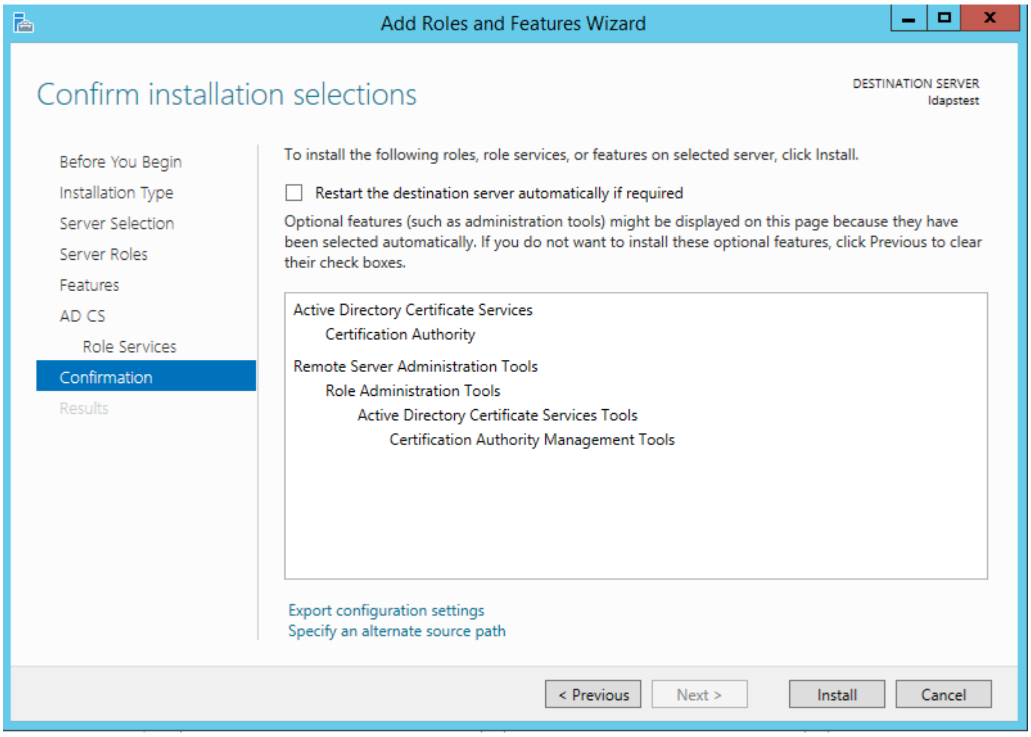
Role services

☑ 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.

Click Install to confirm installation.



Confirm installation selections

DESTINATION SERVER
ldapstest

To install the following roles, role services, or features on selected server, click Install.

□ Restart the destination server automatically if required

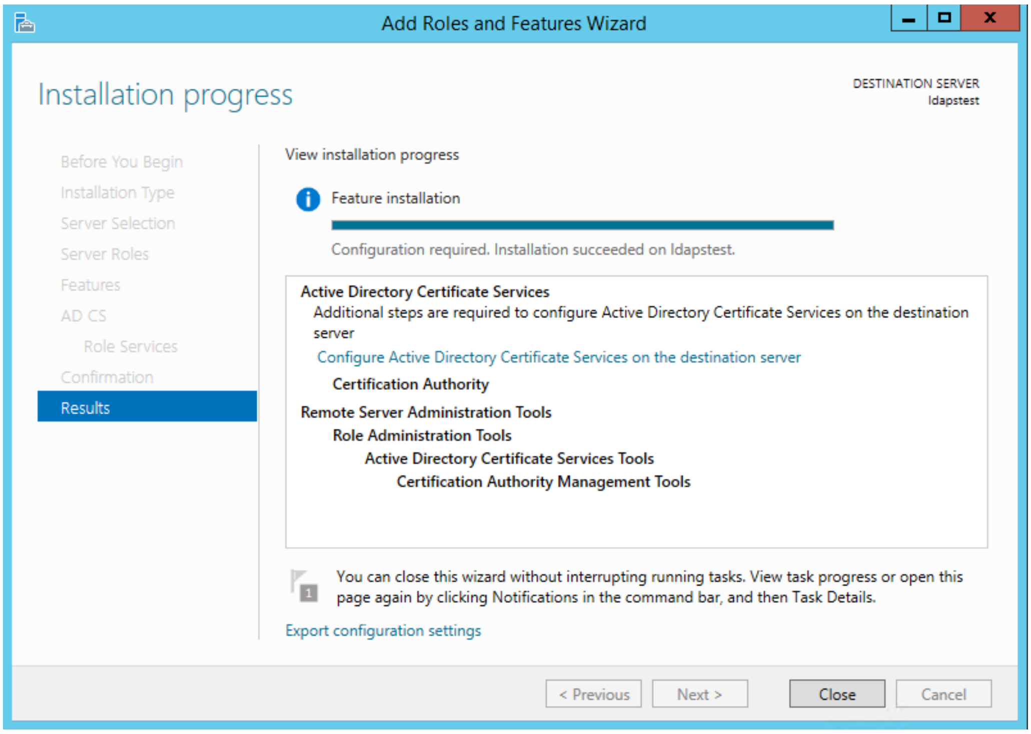
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Certificate Services
    Certification Authority

Remote Server Administration Tools
    Role Administration Tools
        Active Directory Certificate Services Tools
            Certification Authority Management Tools

Export configuration settings
Specify an alternate source path

Once installation is complete, Click Close.



Installation progress

DESTINATION SERVER
ldapstest

View installation progress

Feature installation

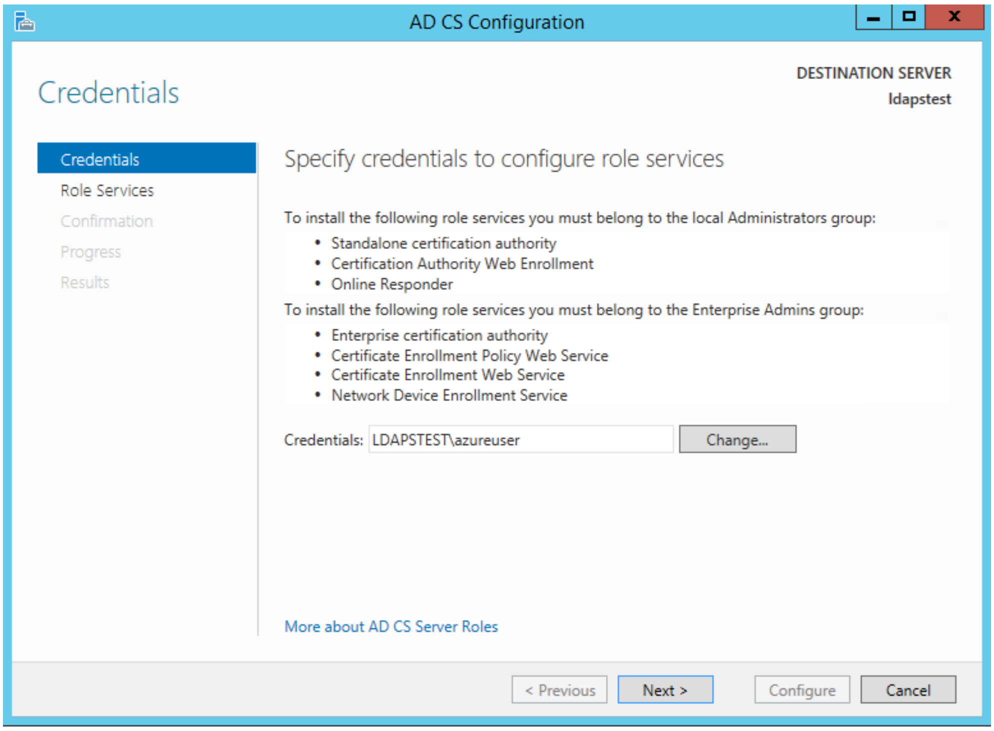
Configuration required. Installation succeeded on ldapstest.

Active Directory Certificate Services
    Additional steps are required to configure Active Directory Certificate Services on the destination server
    Configure Active Directory Certificate Services on the destination server
        Certification Authority
Remote Server Administration Tools
        Role Administration Tools
            Active Directory Certificate Services Tools
                Certification Authority Management Tools

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

Now let’s create a certificate using AD CS Configuration Wizard. To open the wizard, click on “Configure Active Directory Certificate Services on the destination server” in the above screen. And then click Close. We can use the currently logged on user azureuser to configure role services since it belongs to the local Administrators group. Click Next.



Credentials

DESTINATION SERVER
ldapstest

Specify credentials to configure role services

To install the following role services you must belong to the local Administrators group:

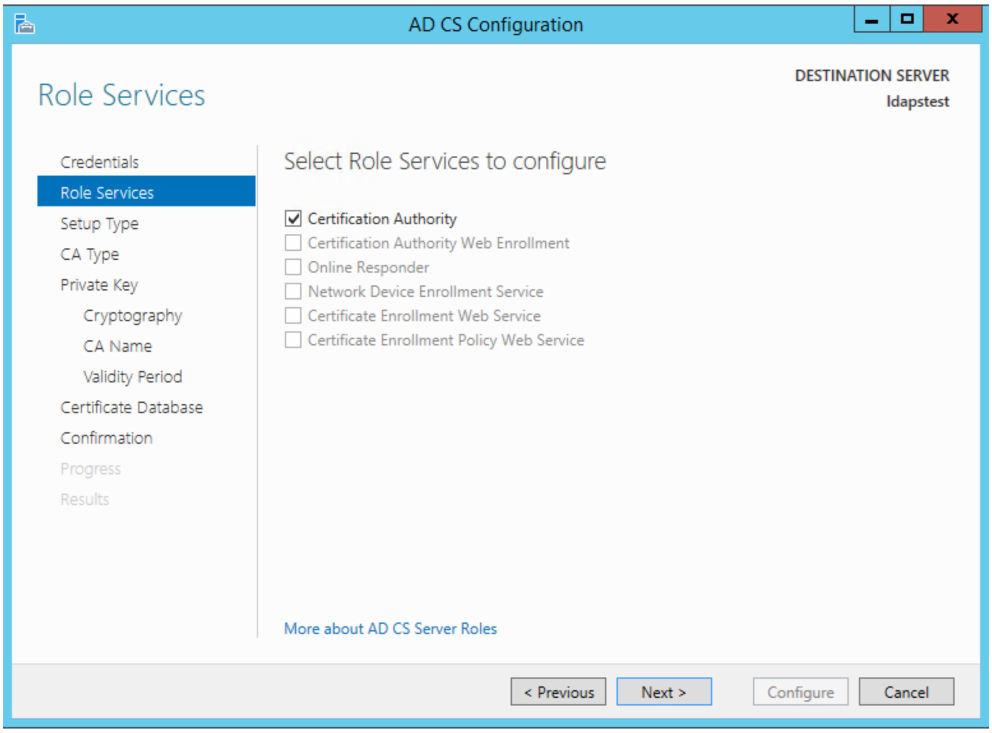
- Standalone certification authority
- Certification Authority Web Enrollment
- Online Responder

To install the following role services you must belong to the Enterprise Admins group:

- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: LDAPSTEST\azureuser

Choose Certification Authority from the list of roles. Click Next.



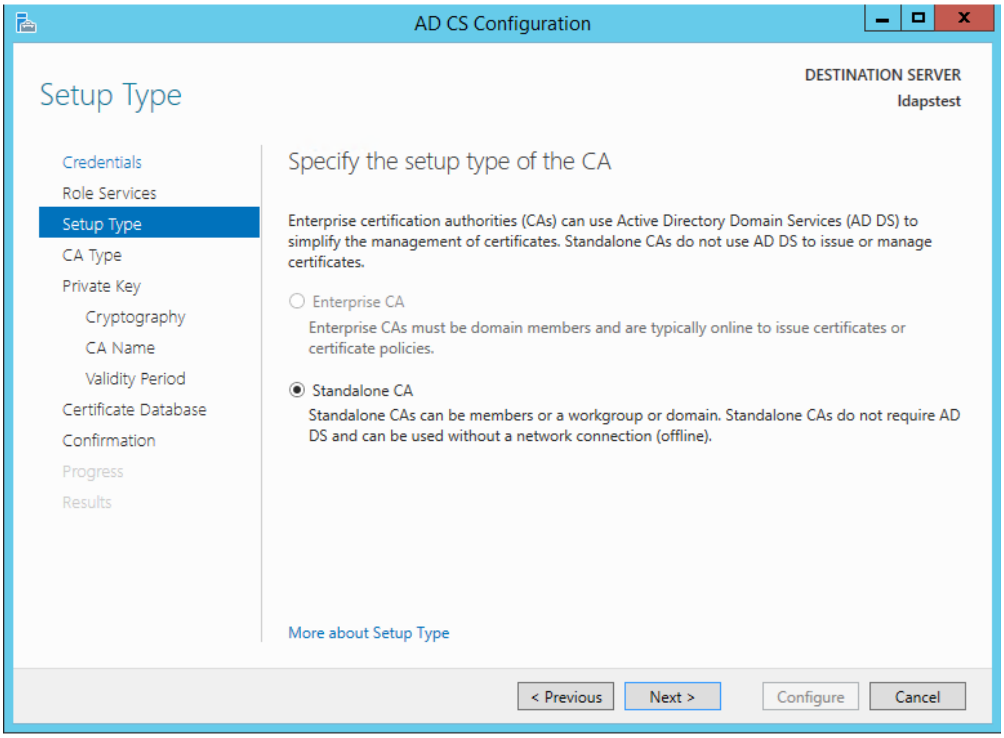
Role Services

DESTINATION SERVER
ldapstest

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

Since this is a local box setup without a domain, we are going to choose a Standalone CA. Click Next.



Setup Type

DESTINATION SERVER
ldapstest

Specify the setup type of the CA

Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

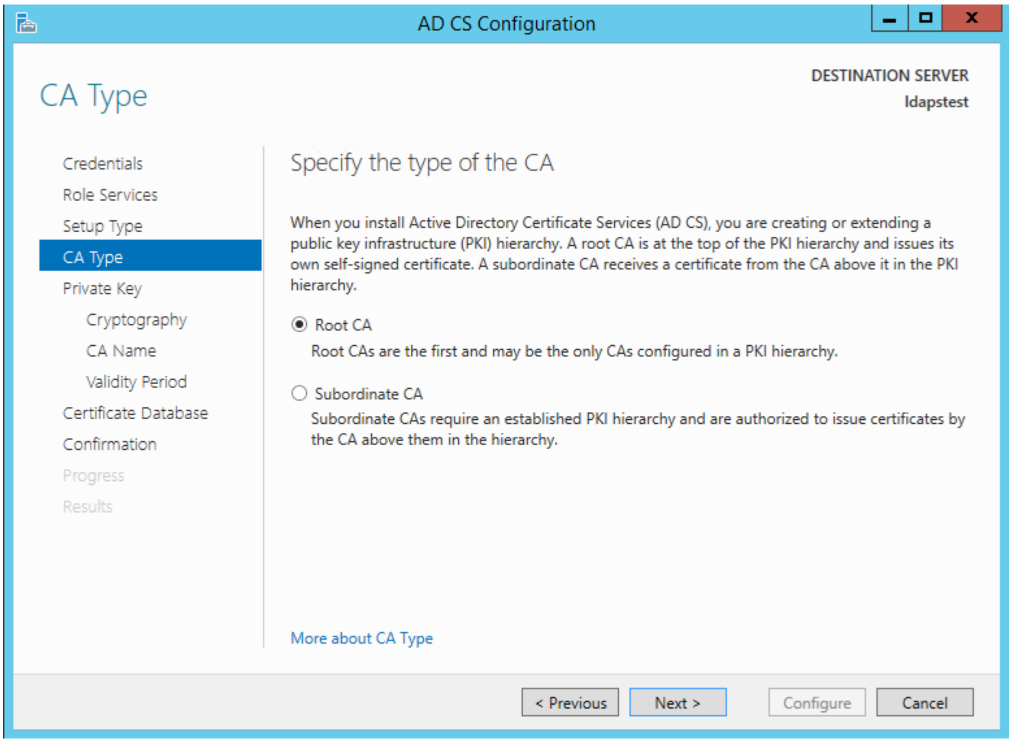
○ Enterprise CA

Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.

● Standalone CA

Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

Choosing Root CA as the type of CA, click Next.



CA Type

DESTINATION SERVER
ldapstest

Specify the type of the CA

When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

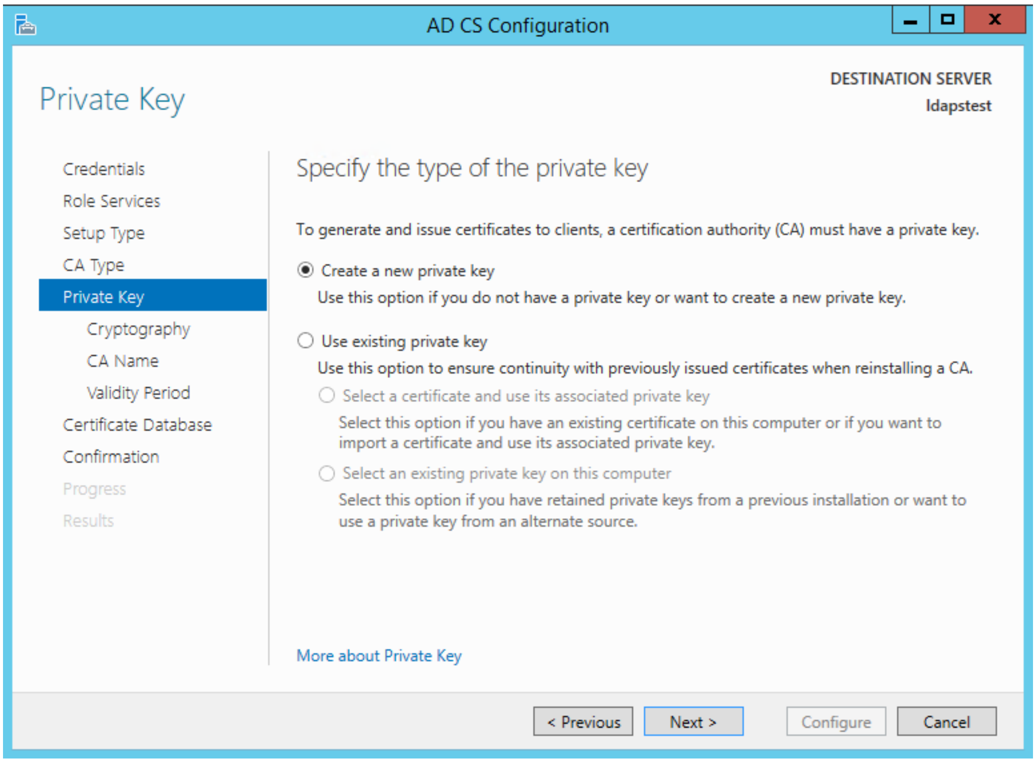
● Root CA

Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

○ Subordinate CA

Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

Since we do not possess a private key – let's create a new one. Click Next.



AD CS Configuration

DESTINATION SERVER
ldapstest

Private Key

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

● Create a new private key
Use this option if you do not have a private key or want to create a new private key.

○ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

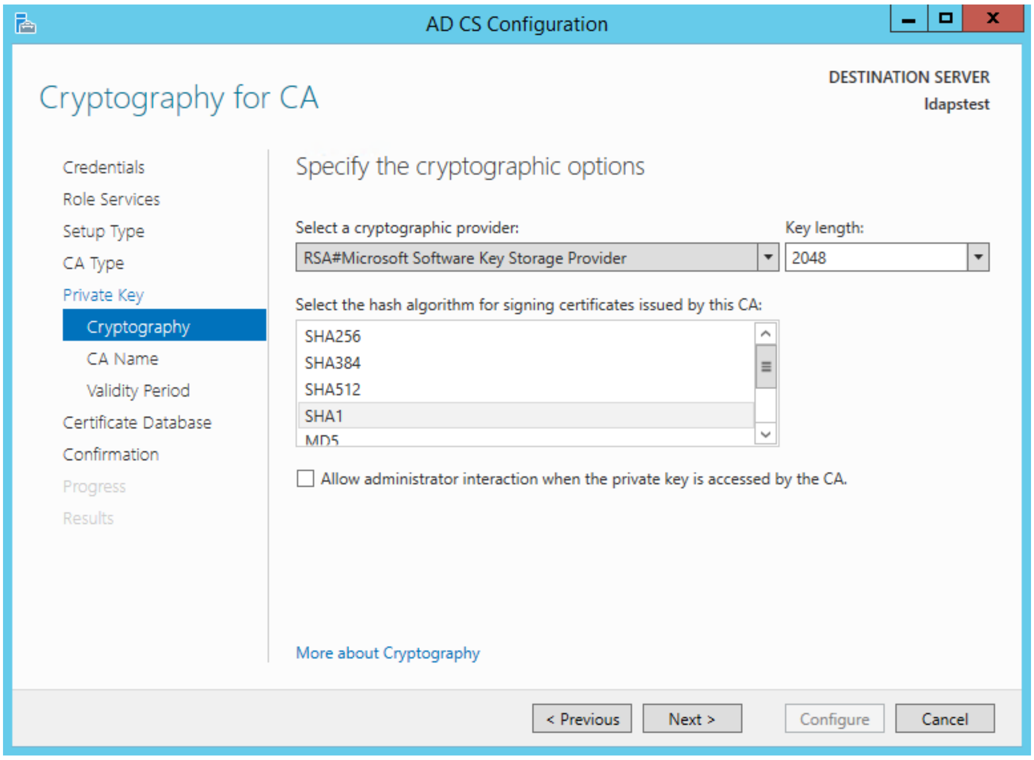
○ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

More about Private Key

Choosing SHA1 as the Hash algorithm. Click Next.

UPDATE: Recommended to select the most recent hashing algorithm since SHA-1 deprecation countdown



AD CS Configuration

DESTINATION SERVER
ldapstest

Cryptography for CA

Specify the cryptographic options

Select a cryptographic provider: RSA#Microsoft Software Key Storage Provider

Key length: 2048

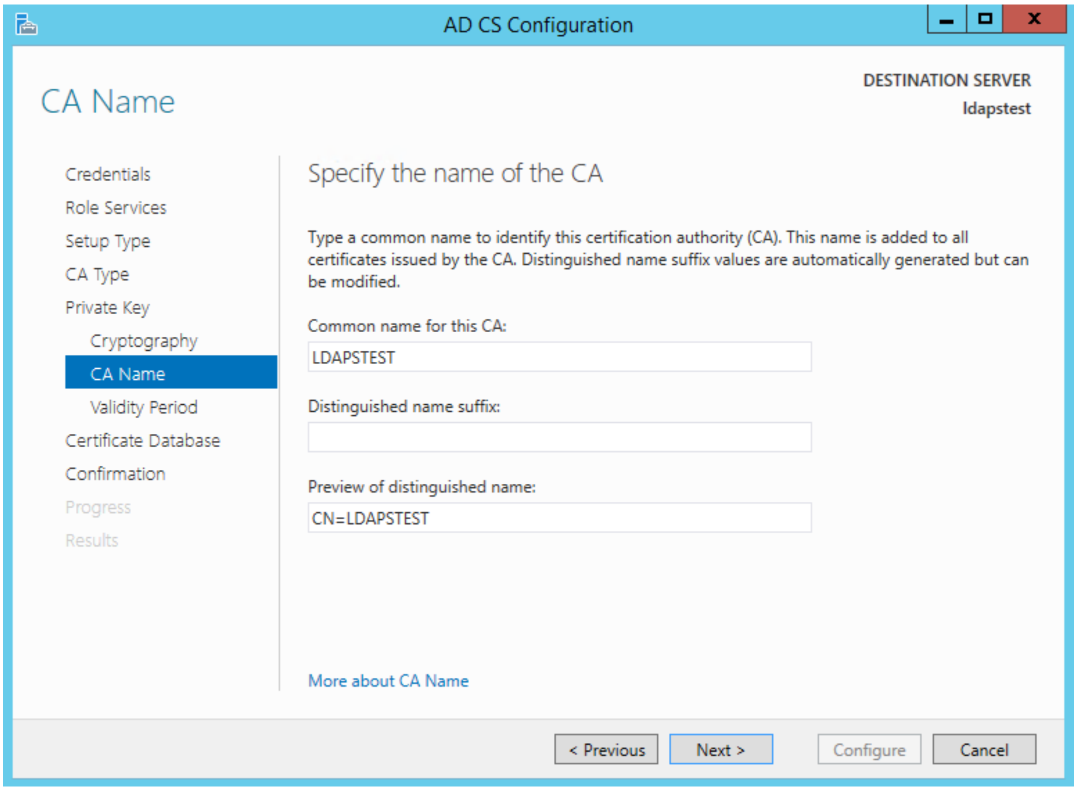
Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

□ Allow administrator interaction when the private key is accessed by the CA.

More about Cryptography

The name of the CA must match the Hostname (requirement number 2). Enter “LDAPSTEST” and Click Next.



AD CS Configuration

DESTINATION SERVER
ldapstest

CA Name

Specify the name of the CA

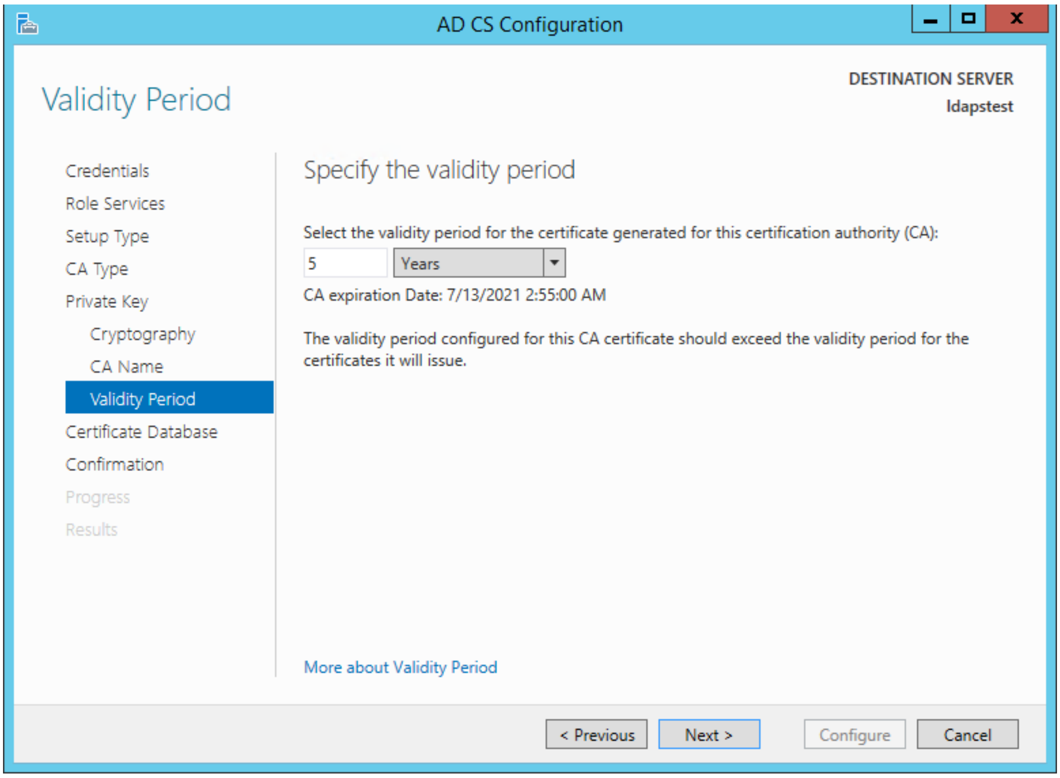
Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA: LDAPSTEST

Distinguished name suffix:

Preview of distinguished name: CN=LDAPSTEST

Specifying validity period of the certificate. Choosing Default 5 years. Click Next.



AD CS Configuration

DESTINATION SERVER
ldapstest

Validity Period

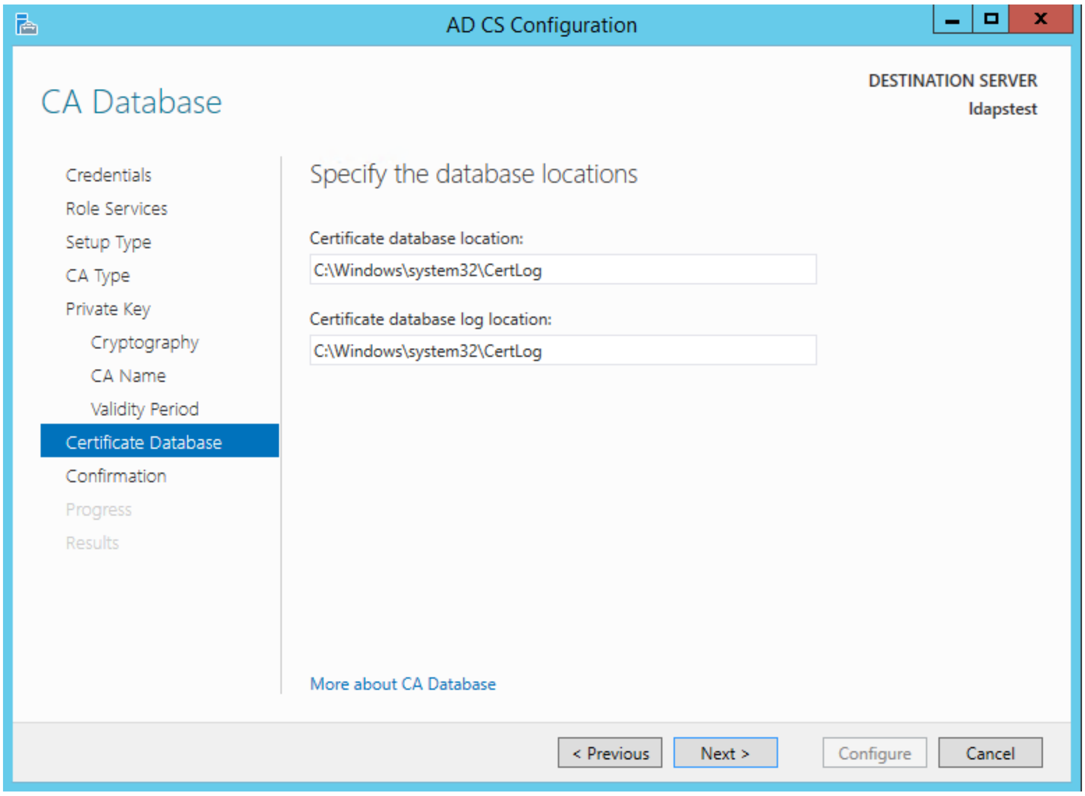
Specify the validity period

Select the validity period for the certificate generated for this certification authority (CA): 5 Years

CA expiration Date: 7/13/2021 2:55:00 AM

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

Choosing default database locations, click Next.



CA Database

DESTINATION SERVER
ldapstest

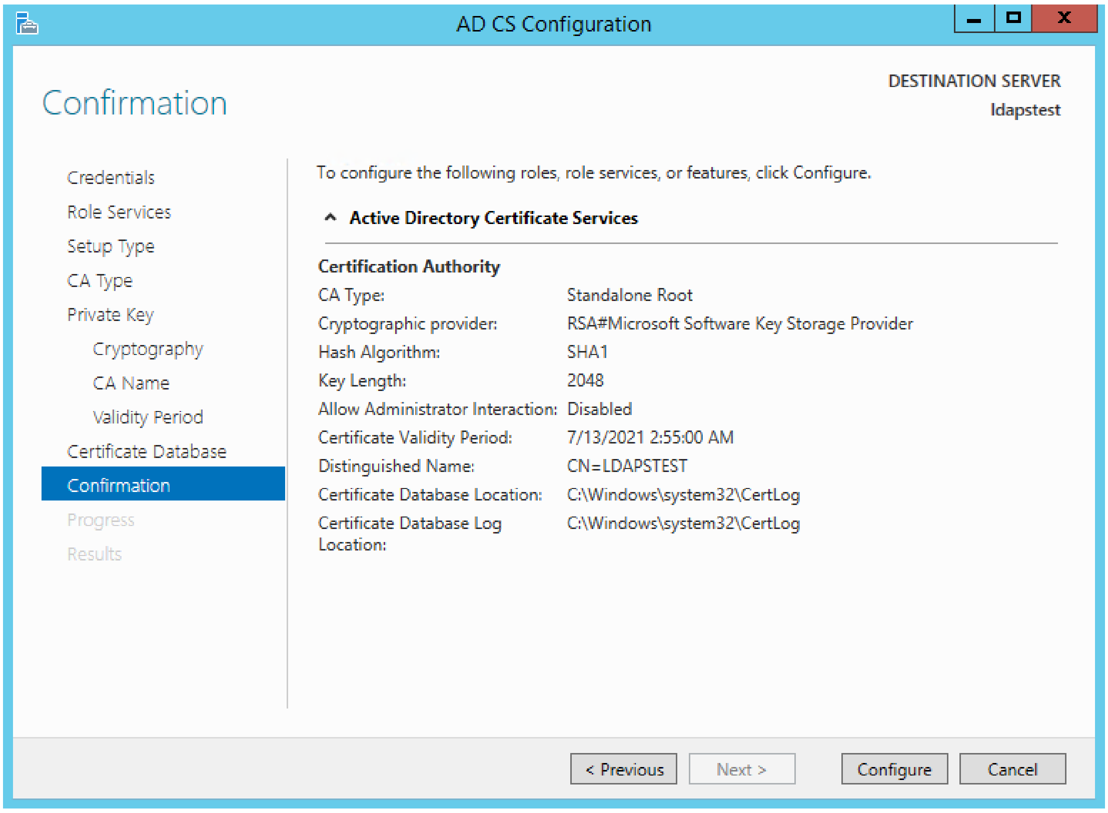
Specify the database locations

Certificate database location:
C:\Windows\system32\CertLog

Certificate database log location:
C:\Windows\system32\CertLog

More about CA Database

Click Configure to confirm.



Confirmation

DESTINATION SERVER
ldapstest

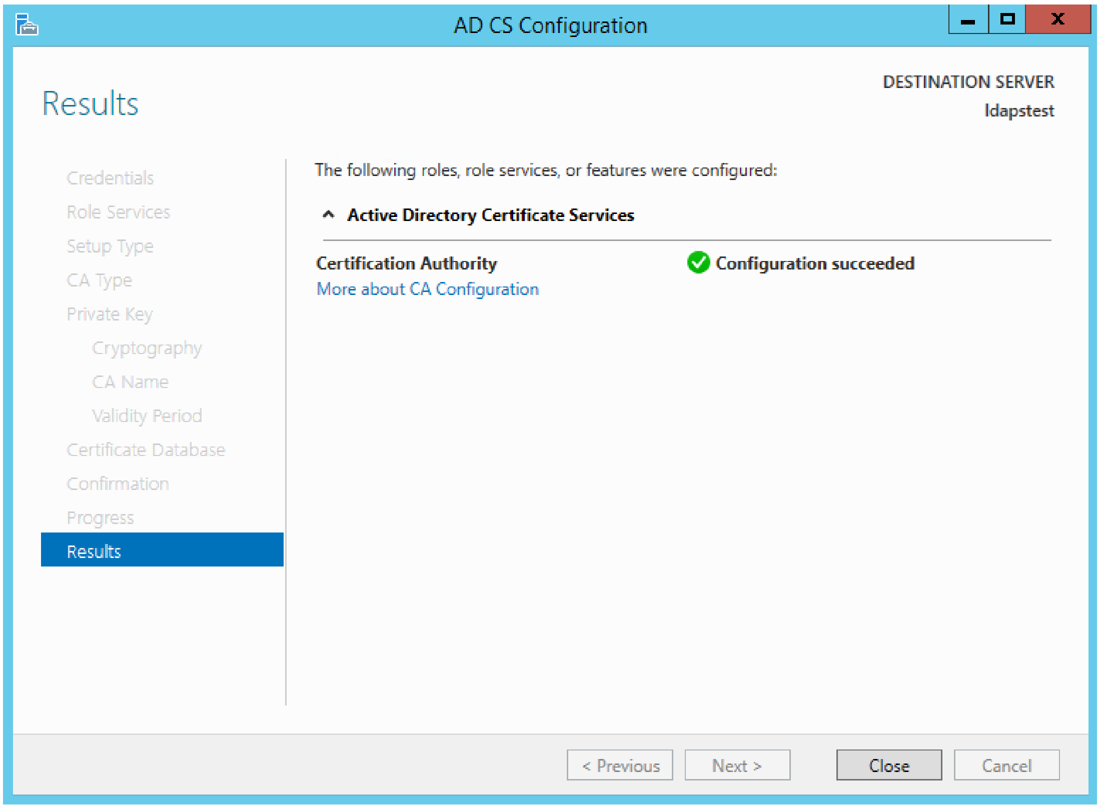
To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certification Authority

CA Type:	Standalone Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA1
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	7/13/2021 2:55:00 AM
Distinguished Name:	CN=LDAPSTEST
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Once the configuration is successful/complete. Click Close.



Results

DESTINATION SERVER
ldapstest

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

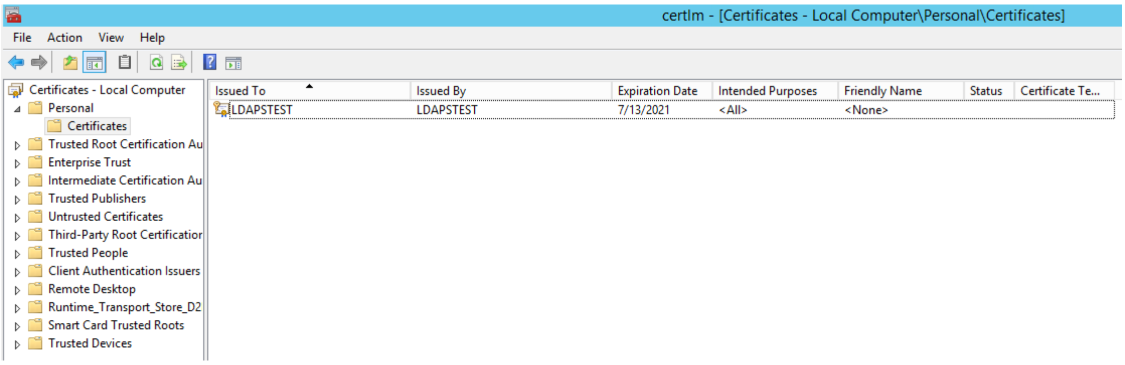
Active Directory Certificate Services

Certification Authority ✓ Configuration succeeded
More about CA Configuration

Now let us view the generated certificate.

Click on Start à Search “Manage Computer Certificates” and open it.

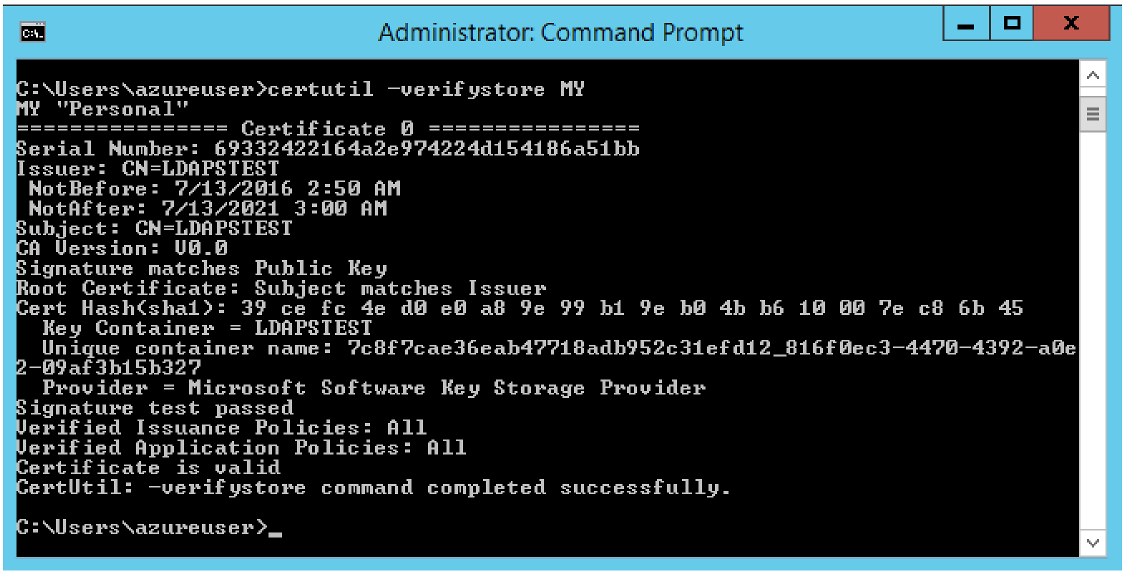
Click on Personal Certificates and verify that the certificate “LDAPSTEST” is present:


File
Action
View
Help
Certificates - Local Computer
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Remote Desktop
Runtime_Transport_Store_D2
Smart Card Trusted Roots
Trusted Devices

certlm - [Certificates - Local Computer\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
LDAPSTEST	LDAPSTEST	7/13/2021	<All>	<None>		

Now to fulfill the third requirement, let us ensure host machine account has access to the private key. Using the Certutil utility, find the Unique Container Name. Open Command Prompt in Administrator mode and run the following command: certutil -verifystore MY

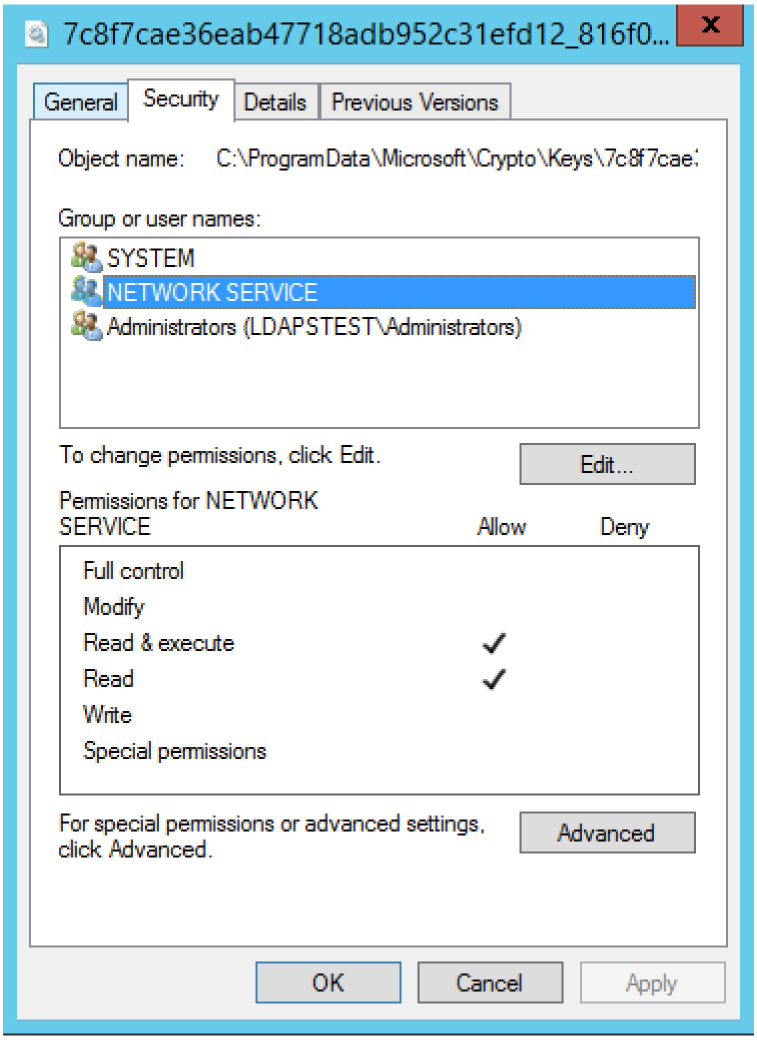


```
C:\Users\azureuser>certutil -verifystore MY
MY "Personal"
================ Certificate 0 ================
Serial Number: 69332422164a2e974224d154186a51bb
Issuer: CN=LDAPSTEST
 NotBefore: 7/13/2016 2:50 AM
 NotAfter: 7/13/2021 3:00 AM
Subject: CN=LDAPSTEST
CA Version: V0.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): 39 ce fc 4e d0 e0 a8 9e 99 b1 9e b0 4b b6 10 00 7e c8 6b 45
  Key Container = LDAPSTEST
  Unique container name: 7c8f7cae36eab47718adb952c31efd12_816f0ec3-4470-4392-a0e
2-09af3b15b327
  Provider = Microsoft Software Key Storage Provider
Signature test passed
Verified Issuance Policies: All
Verified Application Policies: All
Certificate is valid
CertUtil: -verifystore command completed successfully.

C:\Users\azureuser>_
```

The private key will be present in the following location
C:\ProgramData\Microsoft\Crypto\Keys\<UniqueContainerName>

Right Click C:\ProgramData\Microsoft\Crypto\Keys\874cb49a696726e9f435c1888b69f317_d3e61130-4cd8-4288-a344-7784647ff8c4 and click properties --> Security and add read permissions for NETWORK SERVICE.



Object name: C:\ProgramData\Microsoft\Crypto\Keys\7c8f7cae:

Group or user names:

- SYSTEM
- NETWORK SERVICE
- Administrators (LDAPSTEST\Administrators)

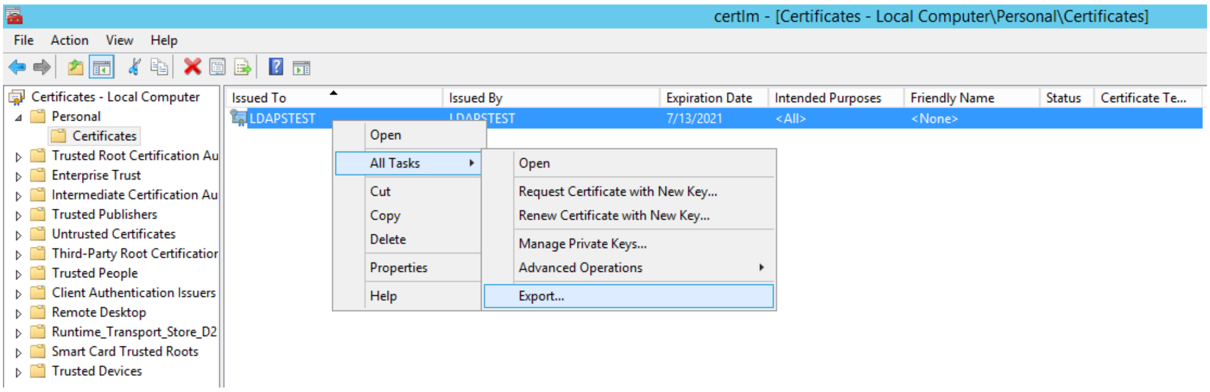
To change permissions, click Edit.

Permissions for NETWORK SERVICE	Allow	Deny
Full control		
Modify		
Read & execute	✓	
Read	✓	
Write		
Special permissions		

For special permissions or advanced settings, click Advanced.

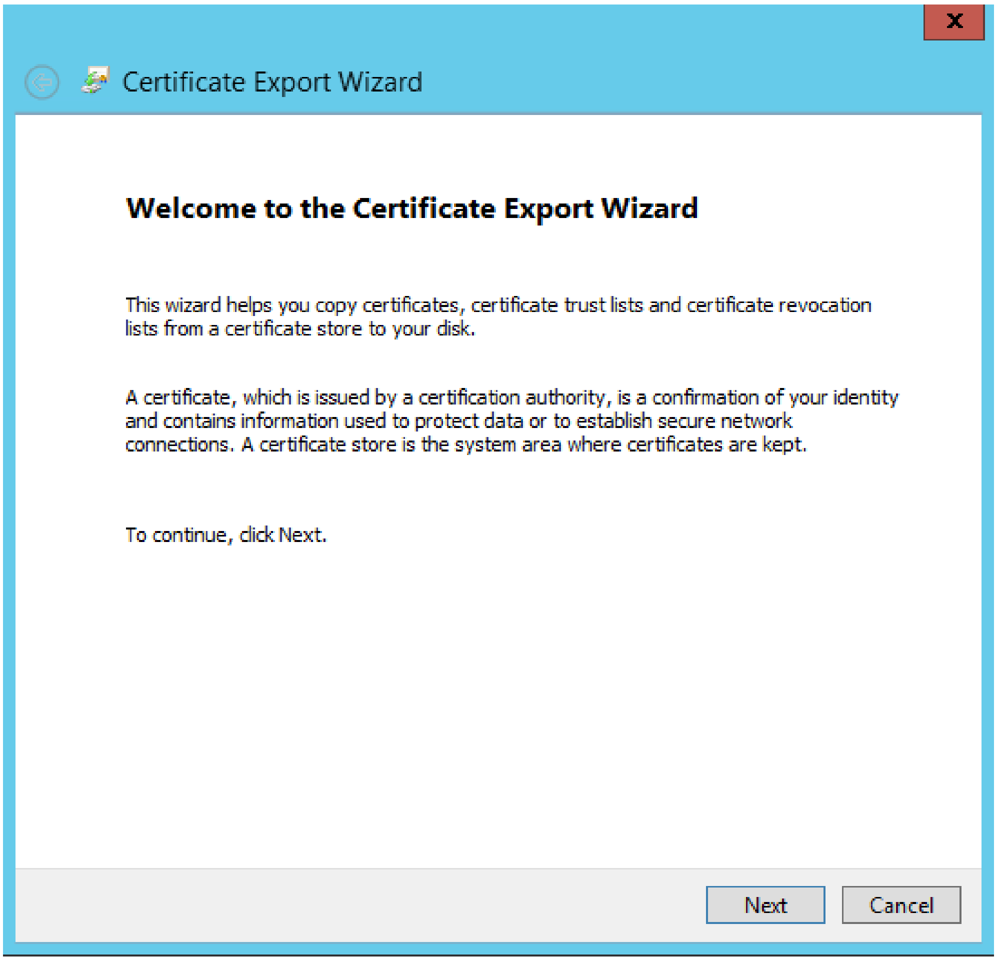
We need to import this certificate into JRE key store since our certificate "CN=LDAPSTEST" is not signed by any by any trusted Certification Authority(CA) which is configured in you JRE keystore e.g Verisign, Thwate, goDaddy or entrust etc. In order to import this certificate using the keytool utility, let us first export this cert as a .CER from the machine certificate store:

Click Start --> Search "Manage Computer Certificates" and open it. Open personal, right click LDAPSTEST cert and click "Export".


certlm - [Certificates - Local Computer\Personal\Certificates]
File
Action
View
Help
Certificates - Local Computer
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Client Authentication Issuers
Remote Desktop
Runtime_Transport_Store_D2
Smart Card Trusted Roots
Trusted Devices
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Renew Certificate with New Key...
Manage Private Keys...
Advanced Operations
Export...

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
LDAPSTEST	LDAPSTEST	7/13/2021	<All>	<None>		

This opens the Certificate Export Wizard. Click Next.



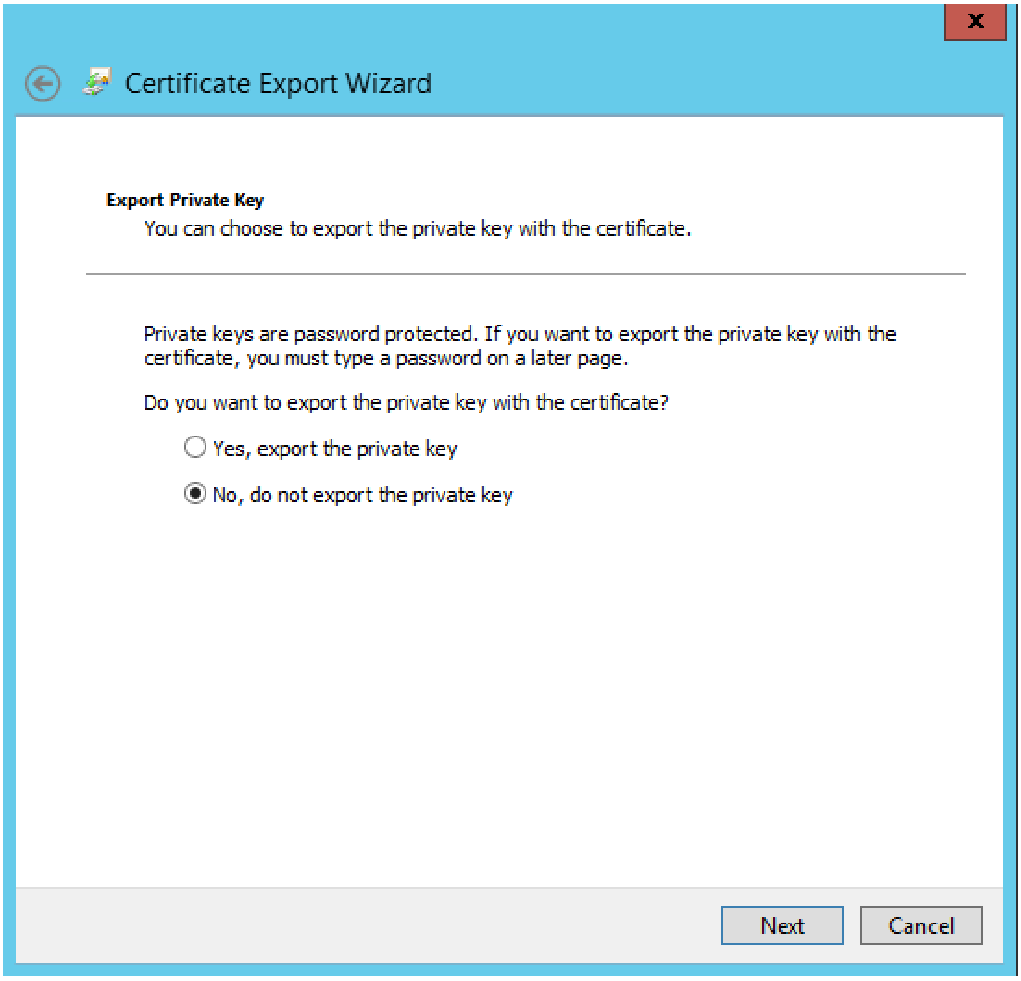
Welcome to the Certificate Export Wizard

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

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.

To continue, click Next.

Do not export the private key. Click Next.



Export Private Key

You can choose to export the private key with the certificate.

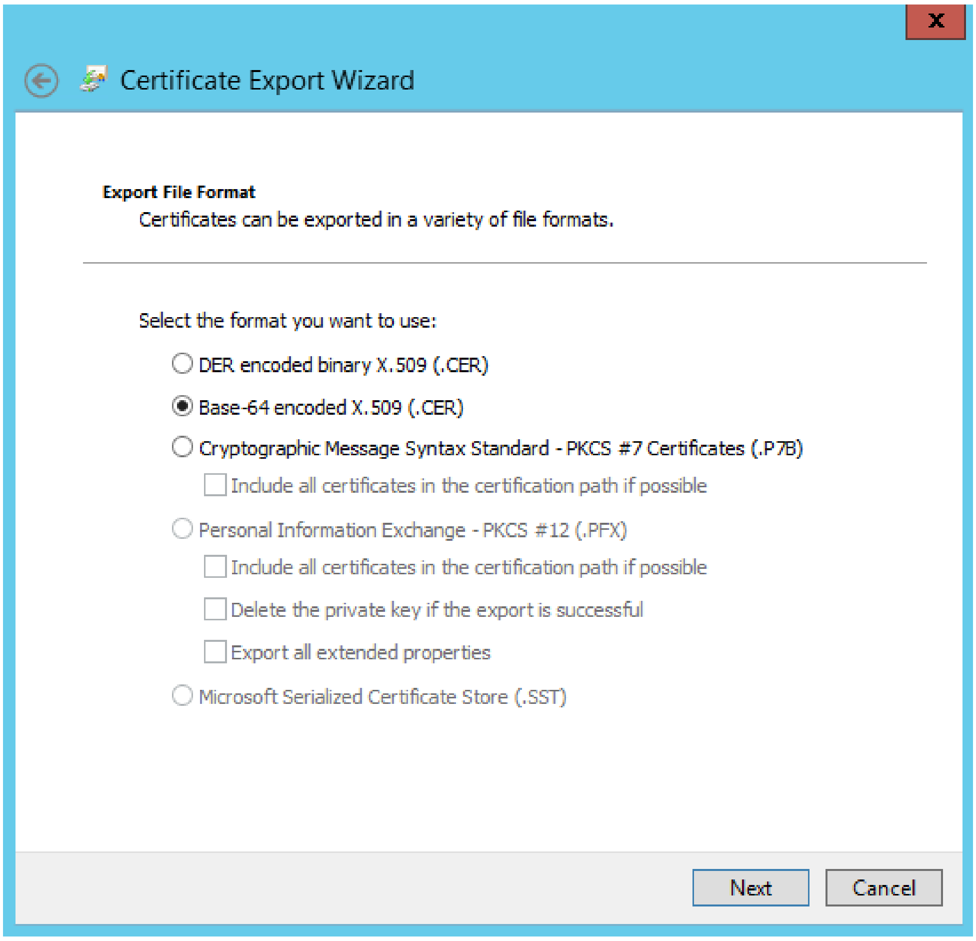
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

Choose Base-64 encoded X .509 file format. Click Next.



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

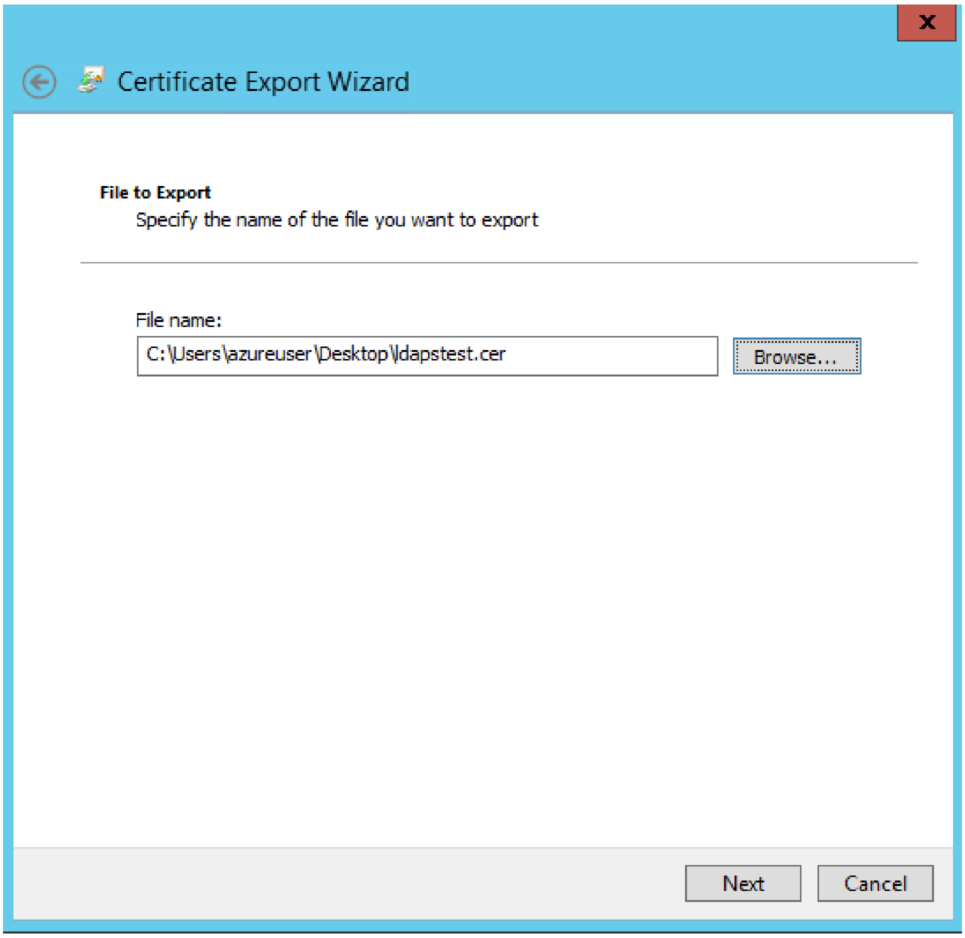
□ Include all certificates in the certification path if possible

□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Exporting the .CER to Desktop. Click Next.



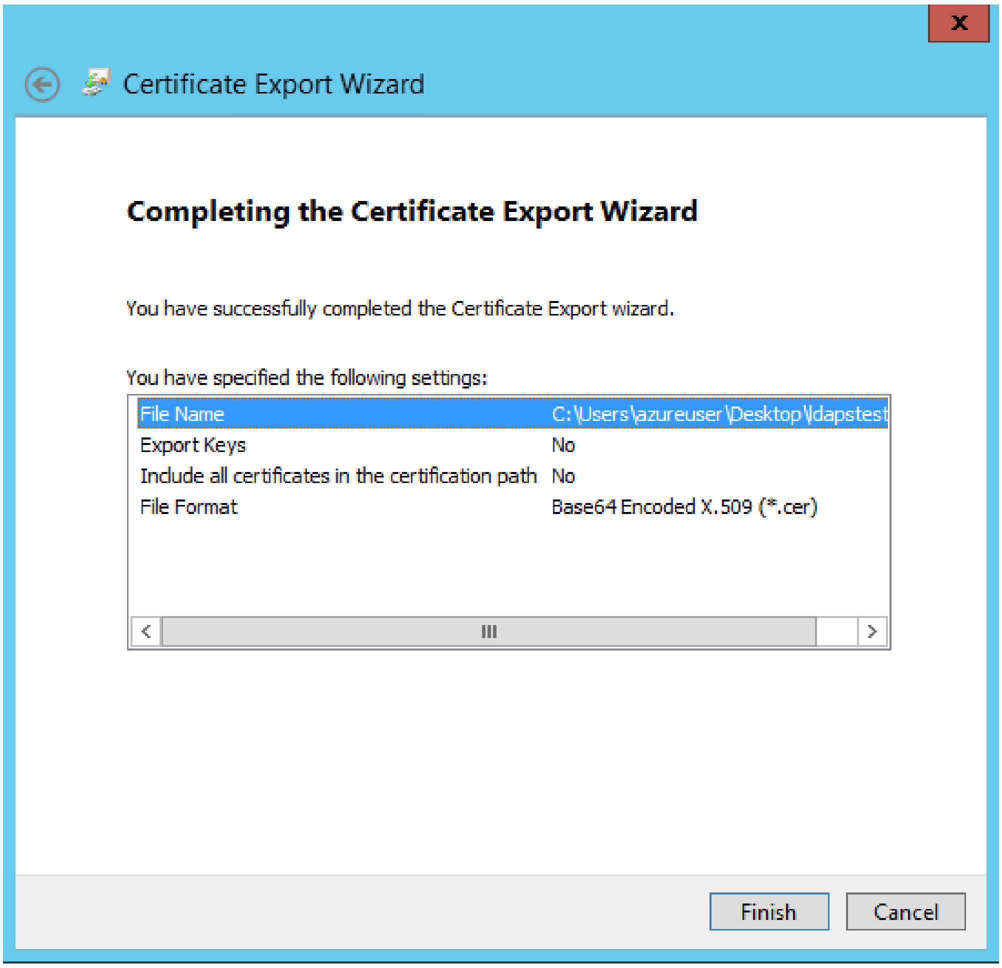
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name: C:\Users\azureuser\Desktop\ldapstest.cer

Click Finish to complete the certificate export.



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

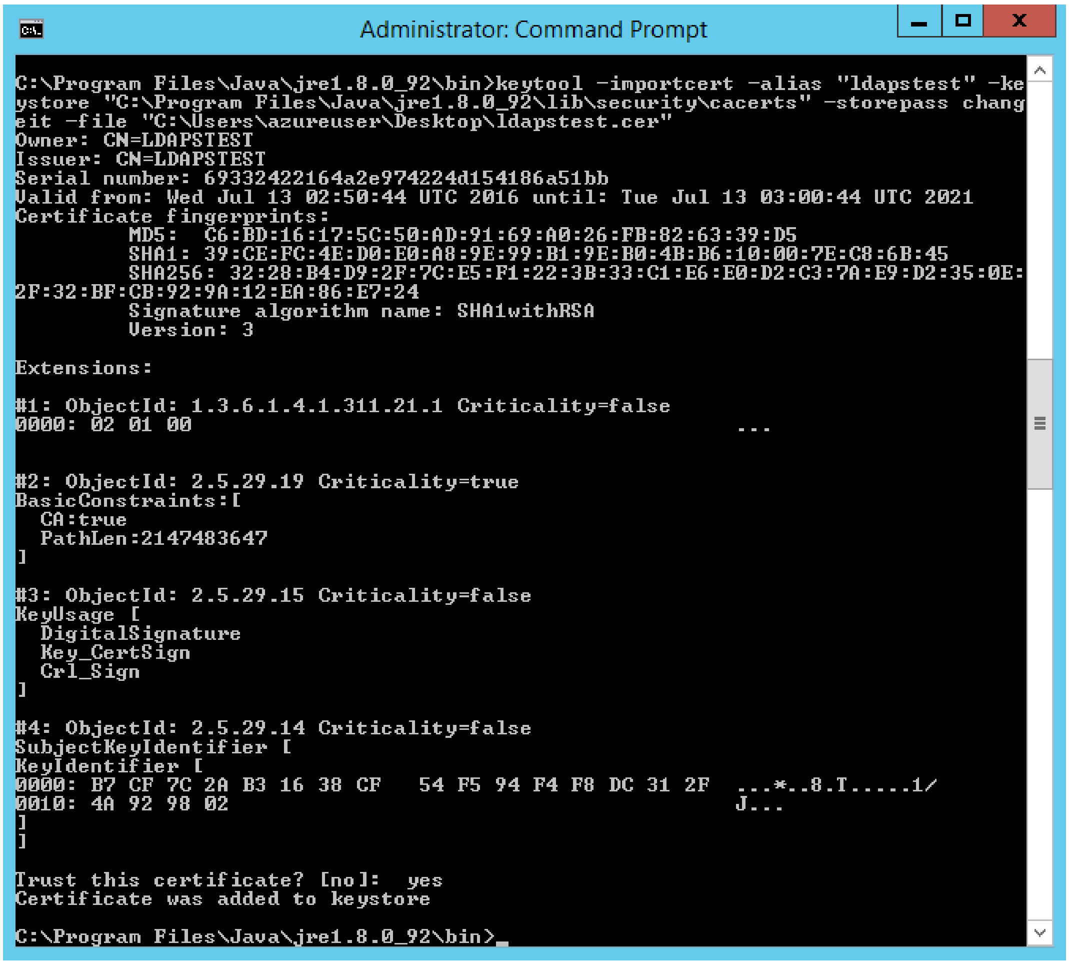
File Name	C:\Users\azureuser\Desktop\ldapstest
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64 Encoded X.509 (*.cer)

Certificate is now successfully exported to "C:\Users\azureuser\Desktop\ldapstest.cer".

Now we shall import it to JRE Keystore using the keytool command present in this location:

C:\Program Files\Java\jre1.8.0_92\bin\keytool.exe.

Open Command Prompt in administrator mode. Navigate to "C:\Program Files\Java\jre1.8.0_92\bin\" and run the following command:
keytool -importcert -alias "ldapstest" -keystore "C:\Program Files\Java\jre1.8.0_92\lib\security\cacerts" -storepass changeit -file "C:\Users\azureuser\Desktop\ldapstest.cer"



```
C:\Program Files\Java\jre1.8.0_92\bin>keytool -importcert -alias "ldapstest" -ke
ystore "C:\Program Files\Java\jre1.8.0_92\lib\security\cacerts" -storepass chang
eit -file "C:\Users\azureuser\Desktop\ldapstest.cer"
Owner: CN=LDAPSTEST
Issuer: CN=LDAPSTEST
Serial number: 69332422164a2e974224d154186a51bb
Valid from: Wed Jul 13 02:50:44 UTC 2016 until: Tue Jul 13 03:00:44 UTC 2021
Certificate fingerprints:
         MD5:  C6:BD:16:17:5C:50:AD:91:69:A0:26:FB:82:63:39:D5
         SHA1: 39:CE:FC:4E:D0:E0:A8:9E:99:B1:9E:B0:4B:B6:10:00:7E:C8:6B:45
         SHA256: 32:28:B4:D9:2F:7C:E5:F1:22:3B:33:C1:E6:E0:D2:C3:7A:E9:D2:35:0E:
2F:32:BF:CB:92:9A:12:EA:86:E7:24
         Signature algorithm name: SHA1withRSA
         Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00                                          ...


#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: B7 CF 7C 2A B3 16 38 CF   54 F5 94 F4 F8 DC 31 2F  ...*..8.T.....1/
0010: 4A 92 98 02                                        J...
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore

C:\Program Files\Java\jre1.8.0_92\bin>_
```

Type “yes” in the Trust this certificate prompt.

Once certificate is successfully added to the JRE keystore, we can connect to the LDAP server over SSL.

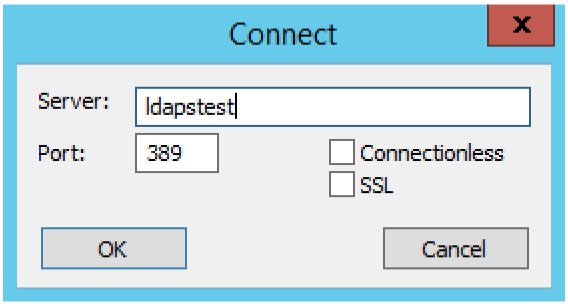
Now let us try to connect to LDAP Server (with and without SSL) using the ldp.exe tool.

Connection strings for

LDAP:\\ldapstest:389

LDAPS:\\ldapstest:636

Click on Start --> Search ldp.exe --> Connection and fill in the following parameters and click OK to connect:



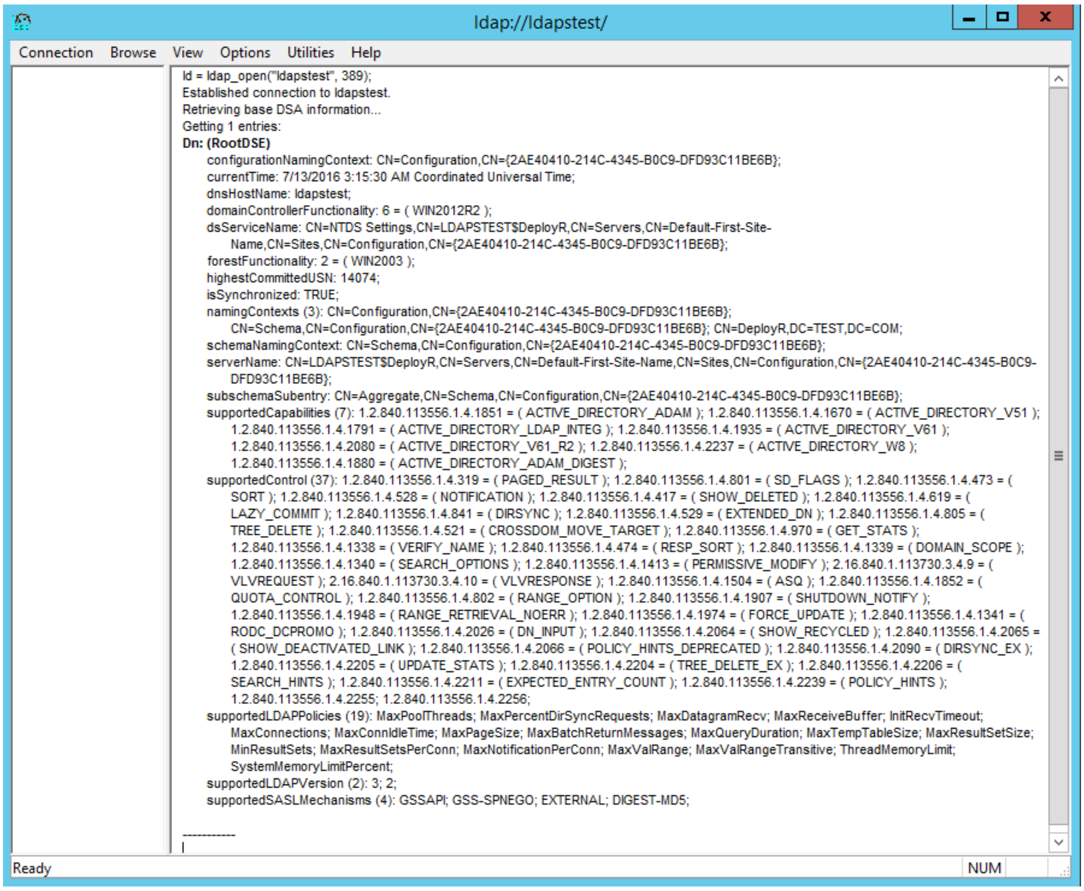
Server: ldapstest

Port: 389

□ Connectionless

□ SSL

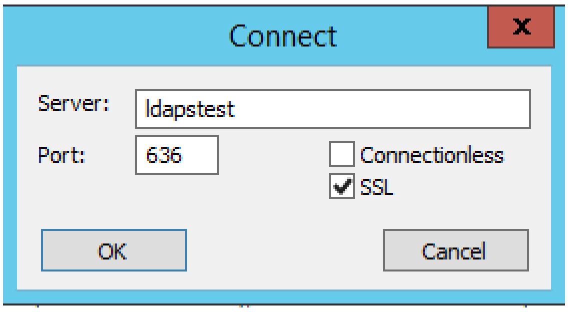
If Connection is successful, you will see the following message in the ldp.exe tool:



```
ld = ldap_open("ldapstest", 389);
Established connection to ldapstest.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
    configurationNamingContext: CN=Configuration,CN={2AE40410-214C-4345-B0C9-DFD93C11BE6B};
    currentTime: 7/13/2016 3:15:30 AM Coordinated Universal Time;
    dnsHostName: ldapstest;
    domainControllerFunctionality: 6 = ( WIN2012R2 );
    dsServiceName: CN=NTDS Settings,CN=LDAPSTEST$DeployR,CN=Servers,CN=Default-First-Site-
        Name,CN=Sites,CN=Configuration,CN={2AE40410-214C-4345-B0C9-DFD93C11BE6B};
    forestFunctionality: 2 = ( WIN2003 );
    highestCommittedUSN: 14074;
    isSynchronized: TRUE;
    namingContexts (3): CN=Configuration,CN={2AE40410-214C-4345-B0C9-DFD93C11BE6B};
        CN=Schema,CN=Configuration,CN={2AE40410-214C-4345-B0C9-DFD93C11BE6B}; CN=DeployR,DC=TEST,DC=COM;
    schemaNamingContext: CN=Schema,CN=Configuration,CN={2AE40410-214C-4345-B0C9-DFD93C11BE6B};
    serverName: CN=LDAPSTEST$DeployR,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,CN={2AE40410-214C-4345-B0C9-
        DFD93C11BE6B};
    subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,CN={2AE40410-214C-4345-B0C9-DFD93C11BE6B};
    supportedCapabilities (7): 1.2.840.113556.1.4.1851 = ( ACTIVE_DIRECTORY_ADAM ); 1.2.840.113556.1.4.1670 = ( ACTIVE_DIRECTORY_V51 );
        1.2.840.113556.1.4.1791 = ( ACTIVE_DIRECTORY_LDAP_INTEG ); 1.2.840.113556.1.4.1935 = ( ACTIVE_DIRECTORY_V61 );
        1.2.840.113556.1.4.2080 = ( ACTIVE_DIRECTORY_V61_R2 ); 1.2.840.113556.1.4.2237 = ( ACTIVE_DIRECTORY_W8 );
        1.2.840.113556.1.4.1880 = ( ACTIVE_DIRECTORY_ADAM_DIGEST );
    supportedControl (37): 1.2.840.113556.1.4.319 = ( PAGED_RESULT ); 1.2.840.113556.1.4.801 = ( SD_FLAGS ); 1.2.840.113556.1.4.473 = (
        SORT ); 1.2.840.113556.1.4.528 = ( NOTIFICATION ); 1.2.840.113556.1.4.417 = ( SHOW_DELETED ); 1.2.840.113556.1.4.619 = (
        LAZY_COMMIT ); 1.2.840.113556.1.4.841 = ( DIRSYNC ); 1.2.840.113556.1.4.529 = ( EXTENDED_DN ); 1.2.840.113556.1.4.805 = (
        TREE_DELETE ); 1.2.840.113556.1.4.521 = ( CROSSDOM_MOVE_TARGET ); 1.2.840.113556.1.4.970 = ( GET_STATS );
        1.2.840.113556.1.4.1338 = ( VERIFY_NAME ); 1.2.840.113556.1.4.474 = ( RESP_SORT ); 1.2.840.113556.1.4.1339 = ( DOMAIN_SCOPE );
        1.2.840.113556.1.4.1340 = ( SEARCH_OPTIONS ); 1.2.840.113556.1.4.1413 = ( PERMISSIVE_MODIFY ); 2.16.840.1.113730.3.4.9 = (
        VLVREQUEST ); 2.16.840.1.113730.3.4.10 = ( VLVRESPONSE ); 1.2.840.113556.1.4.1504 = ( ASQ ); 1.2.840.113556.1.4.1852 = (
        QUOTA_CONTROL ); 1.2.840.113556.1.4.802 = ( RANGE_OPTION ); 1.2.840.113556.1.4.1907 = ( SHUTDOWN_NOTIFY );
        1.2.840.113556.1.4.1948 = ( RANGE_RETRIEVAL_NOERR ); 1.2.840.113556.1.4.1974 = ( FORCE_UPDATE ); 1.2.840.113556.1.4.1341 = (
        RODC_DCPROMO ); 1.2.840.113556.1.4.2026 = ( DN_INPUT ); 1.2.840.113556.1.4.2064 = ( SHOW_RECYCLED ); 1.2.840.113556.1.4.2065 =
        ( SHOW_DEACTIVATED_LINK ); 1.2.840.113556.1.4.2066 = ( POLICY_HINTS_DEPRECATED ); 1.2.840.113556.1.4.2090 = ( DIRSYNC_EX );
        1.2.840.113556.1.4.2205 = ( UPDATE_STATS ); 1.2.840.113556.1.4.2204 = ( TREE_DELETE_EX ); 1.2.840.113556.1.4.2206 = (
        SEARCH_HINTS ); 1.2.840.113556.1.4.2211 = ( EXPECTED_ENTRY_COUNT ); 1.2.840.113556.1.4.2239 = ( POLICY_HINTS );
        1.2.840.113556.1.4.2255; 1.2.840.113556.1.4.2256;
    supportedLDAPPolicies (19): MaxPoolThreads; MaxPercentDirSyncRequests; MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout;
        MaxConnections; MaxConnIdleTime; MaxPageSize; MaxBatchReturnMessages; MaxQueryDuration; MaxTempTableSize; MaxResultSetSize;
        MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit;
        SystemMemoryLimitPercent;
    supportedLDAPVersion (2): 3; 2;
    supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
```

To Connect to LDAPS (LDAP over SSL), use port 636 and mark SSL. Click OK to connect.



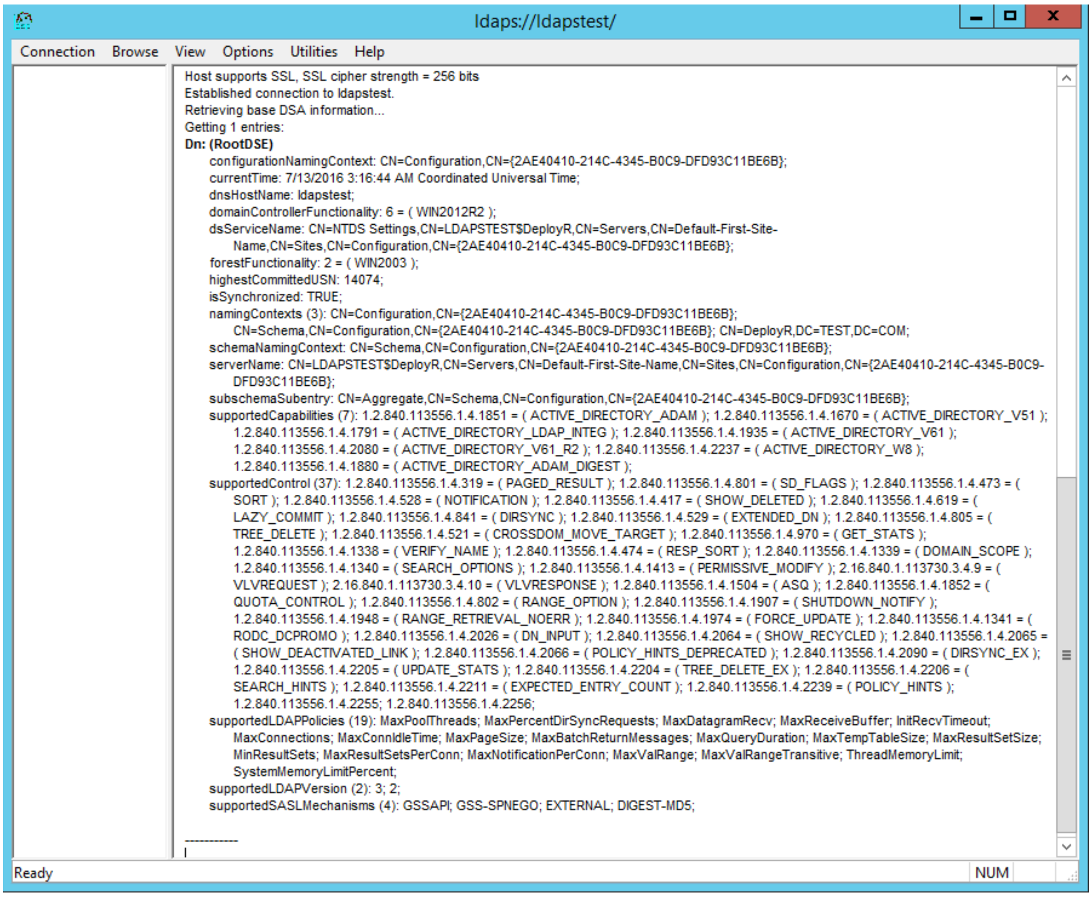
Server: ldapstest

Port: 636

□ Connectionless

☑ SSL

If connection is successful, you will see the following message in the ldp.exe tool:



```
Host supports SSL, SSL cipher strength = 256 bits
Established connection to ldapstest.
Retrieving base DSA information...
Getting 1 entries:
Dn: (RootDSE)
    configurationNamingContext: CN=Configuration,CN={2AE40410-214C-4345-B0C9-DFD93C11BE6B};
    currentTime: 7/13/2016 3:16:44 AM Coordinated Universal Time;
    dnsHostName: ldapstest;
    domainControllerFunctionality: 6 = ( WIN2012R2 );
    dsServiceName: CN=NTDS Settings,CN=LDAPSTEST$DeployR,CN=Servers,CN=Default-First-Site-
        Name,CN=Sites,CN=Configuration,CN={2AE40410-214C-4345-B0C9-DFD93C11BE6B};
    forestFunctionality: 2 = ( WIN2003 );
    highestCommittedUSN: 14074;
    isSynchronized: TRUE;
    namingContexts (3): CN=Configuration,CN={2AE40410-214C-4345-B0C9-DFD93C11BE6B};
        CN=Schema,CN=Configuration,CN={2AE40410-214C-4345-B0C9-DFD93C11BE6B}; CN=DeployR,DC=TEST,DC=COM;
    schemaNamingContext: CN=Schema,CN=Configuration,CN={2AE40410-214C-4345-B0C9-DFD93C11BE6B};
    serverName: CN=LDAPSTEST$DeployR,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,CN={2AE40410-214C-4345-B0C9-
        DFD93C11BE6B};
    subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,CN={2AE40410-214C-4345-B0C9-DFD93C11BE6B};
    supportedCapabilities (7): 1.2.840.113556.1.4.1851 = ( ACTIVE_DIRECTORY_ADAM ); 1.2.840.113556.1.4.1670 = ( ACTIVE_DIRECTORY_V51 );
        1.2.840.113556.1.4.1791 = ( ACTIVE_DIRECTORY_LDAP_INTEG ); 1.2.840.113556.1.4.1935 = ( ACTIVE_DIRECTORY_V61 );
        1.2.840.113556.1.4.2080 = ( ACTIVE_DIRECTORY_V61_R2 ); 1.2.840.113556.1.4.2237 = ( ACTIVE_DIRECTORY_W8 );
        1.2.840.113556.1.4.1880 = ( ACTIVE_DIRECTORY_ADAM_DIGEST );
    supportedControl (37): 1.2.840.113556.1.4.319 = ( PAGED_RESULT ); 1.2.840.113556.1.4.801 = ( SD_FLAGS ); 1.2.840.113556.1.4.473 = (
        SORT ); 1.2.840.113556.1.4.528 = ( NOTIFICATION ); 1.2.840.113556.1.4.417 = ( SHOW_DELETED ); 1.2.840.113556.1.4.619 = (
        LAZY_COMMIT ); 1.2.840.113556.1.4.841 = ( DIRSYNC ); 1.2.840.113556.1.4.529 = ( EXTENDED_DN ); 1.2.840.113556.1.4.805 = (
        TREE_DELETE ); 1.2.840.113556.1.4.521 = ( CROSSDOM_MOVE_TARGET ); 1.2.840.113556.1.4.970 = ( GET_STATS );
        1.2.840.113556.1.4.1338 = ( VERIFY_NAME ); 1.2.840.113556.1.4.474 = ( RESP_SORT ); 1.2.840.113556.1.4.1339 = ( DOMAIN_SCOPE );
        1.2.840.113556.1.4.1340 = ( SEARCH_OPTIONS ); 1.2.840.113556.1.4.1413 = ( PERMISSIVE_MODIFY ); 2.16.840.1.113730.3.4.9 = (
        VLVREQUEST ); 2.16.840.1.113730.3.4.10 = ( VLVRESPONSE ); 1.2.840.113556.1.4.1504 = ( ASQ ); 1.2.840.113556.1.4.1852 = (
        QUOTA_CONTROL ); 1.2.840.113556.1.4.802 = ( RANGE_OPTION ); 1.2.840.113556.1.4.1907 = ( SHUTDOWN_NOTIFY );
        1.2.840.113556.1.4.1948 = ( RANGE_RETRIEVAL_NOERR ); 1.2.840.113556.1.4.1974 = ( FORCE_UPDATE ); 1.2.840.113556.1.4.1341 = (
        RODC_DCPROMO ); 1.2.840.113556.1.4.2026 = ( DN_INPUT ); 1.2.840.113556.1.4.2064 = ( SHOW_RECYCLED ); 1.2.840.113556.1.4.2065 =
        ( SHOW_DEACTIVATED_LINK ); 1.2.840.113556.1.4.2066 = ( POLICY_HINTS_DEPRECATED ); 1.2.840.113556.1.4.2090 = ( DIRSYNC_EX );
        1.2.840.113556.1.4.2205 = ( UPDATE_STATS ); 1.2.840.113556.1.4.2204 = ( TREE_DELETE_EX ); 1.2.840.113556.1.4.2206 = (
        SEARCH_HINTS ); 1.2.840.113556.1.4.2211 = ( EXPECTED_ENTRY_COUNT ); 1.2.840.113556.1.4.2239 = ( POLICY_HINTS );
        1.2.840.113556.1.4.2255; 1.2.840.113556.1.4.2256;
    supportedLDAPPolicies (19): MaxPoolThreads; MaxPercentDirSyncRequests; MaxDatagramRecv; MaxReceiveBuffer; InitRecvTimeout;
        MaxConnections; MaxConnIdleTime; MaxPageSize; MaxBatchReturnMessages; MaxQueryDuration; MaxTempTableSize; MaxResultSetSize;
        MinResultSets; MaxResultSetsPerConn; MaxNotificationPerConn; MaxValRange; MaxValRangeTransitive; ThreadMemoryLimit;
        SystemMemoryLimitPercent;
    supportedLDAPVersion (2): 3; 2;
    supportedSASLMechanisms (4): GSSAPI; GSS-SPNEGO; EXTERNAL; DIGEST-MD5;

-----------
```