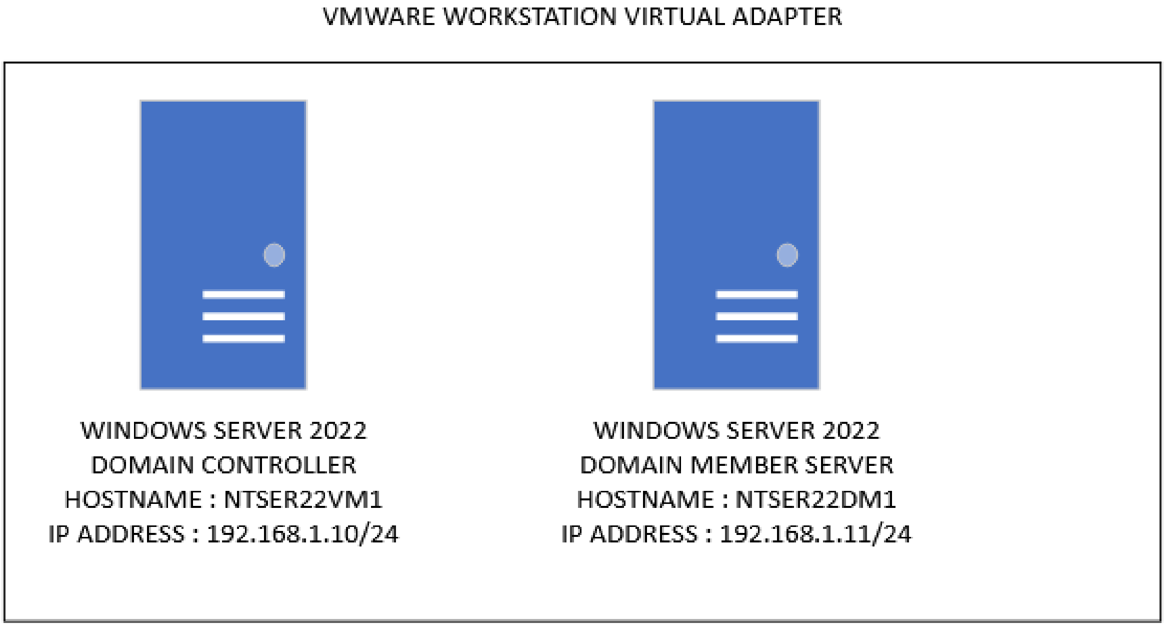
Exercise 1 - Install and Configure Active Directory Certificate Services

An organization can use Active Directory Certificate Services (AD CS) to create a public key infrastructure (PKI). Its purpose is to provide the following features:

1. Public key cryptography
2. Digital certificates
3. Digital signature

In this exercise, we will cover Install Active Directory Enterprise Root Certificate Service, Configure Active Directory Certificate Services, Install Subordinate CA and Configure Subordinate CA

Topology



DOMAIN = networktute.com

NTSER22VM1 = Windows Server 2022 – Domain Controller

NTSER22DM1 = Windows Server 2022 – Domain Member Server

Prerequisite

- *VMware Workstation 16 Pro*
  - When making this tutorial, we used the "Windows Server 2019" VM Template and "Windows 10 & later" VM Template. Since VMware didn't have the updated templates.
- *Microsoft Windows Server 2022*

Task 1: Install Active Directory Enterprise Root Certificate Service

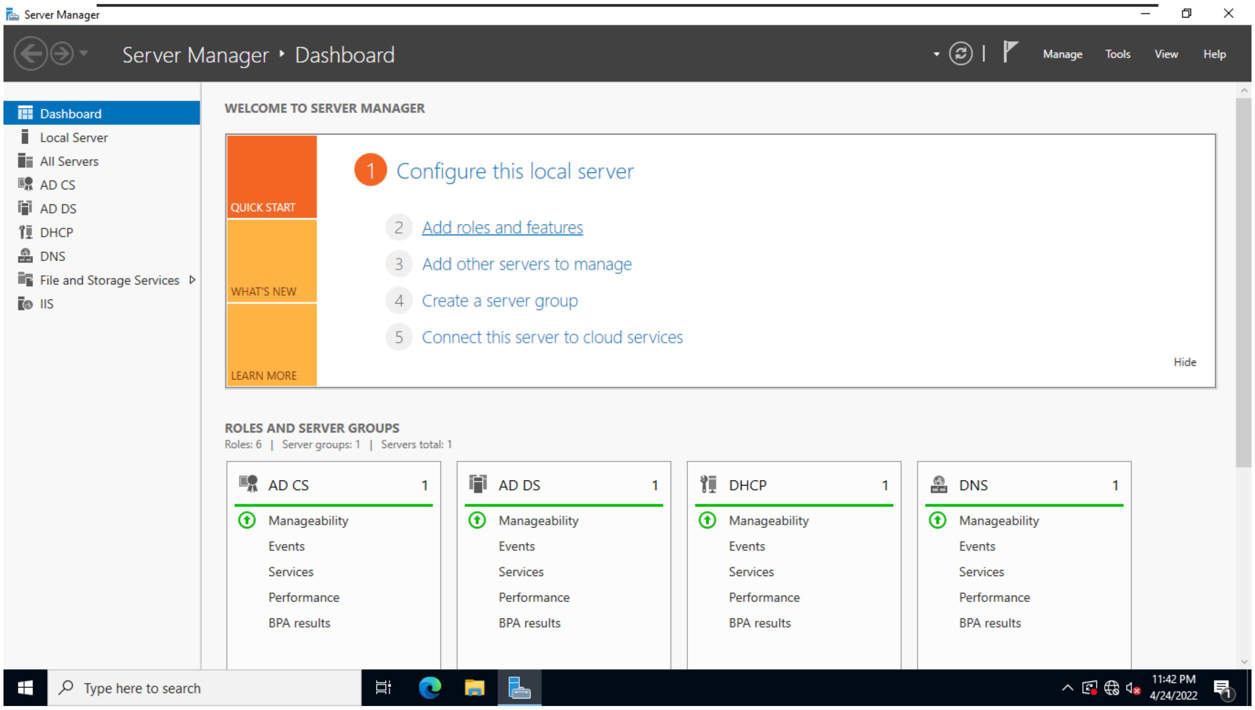
An Active Directory Enterprise CA is a certificate authority that is connected with Active Directory. The CA's initial server might be any Root server. In the Active Directory context, an Enterprise CA can be set to auto-enroll certificates.

Now let’s install AD Certificate Services on the Domain Controller device.

Step 1:

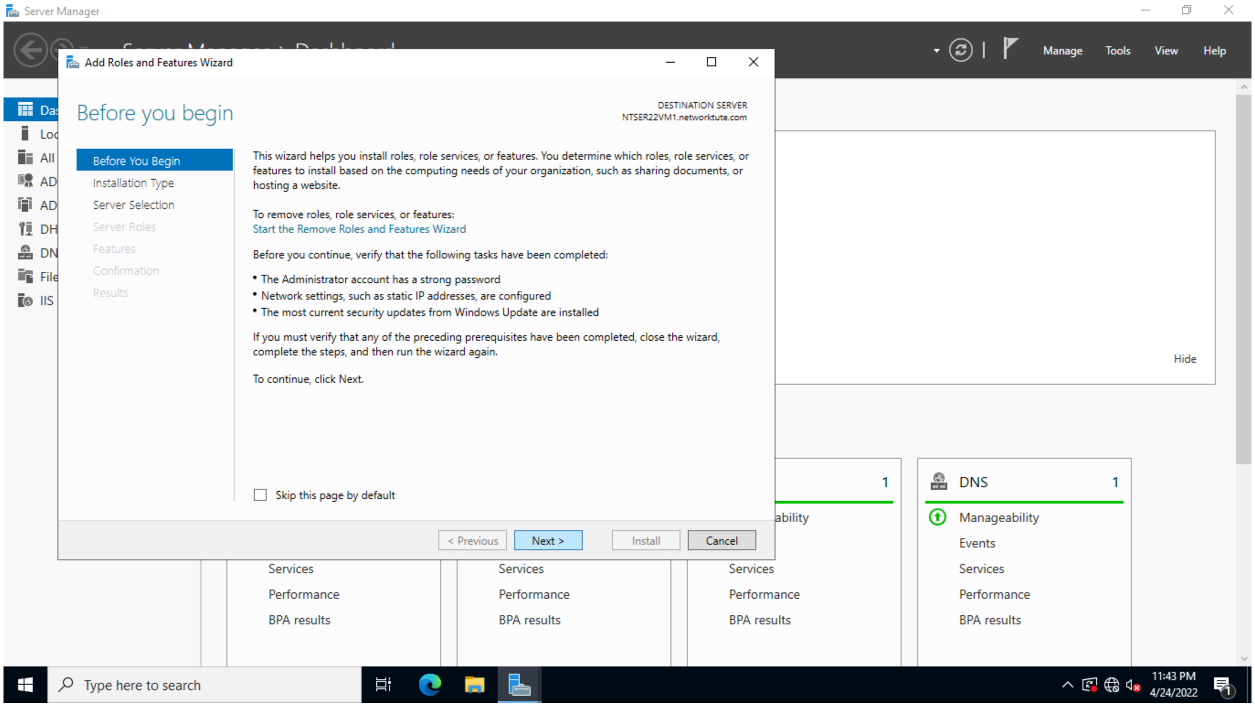
Connect to **NTSER22VM1**.

The **Server Manager** window is displayed automatically and Click **Add roles and features.**



Step 2:

On the **Before you begin** page of the **Add Roles and Features Wizard**, click **Next**.



Before you begin

DESTINATION SERVER
NTSER22VM1.networktute.com

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

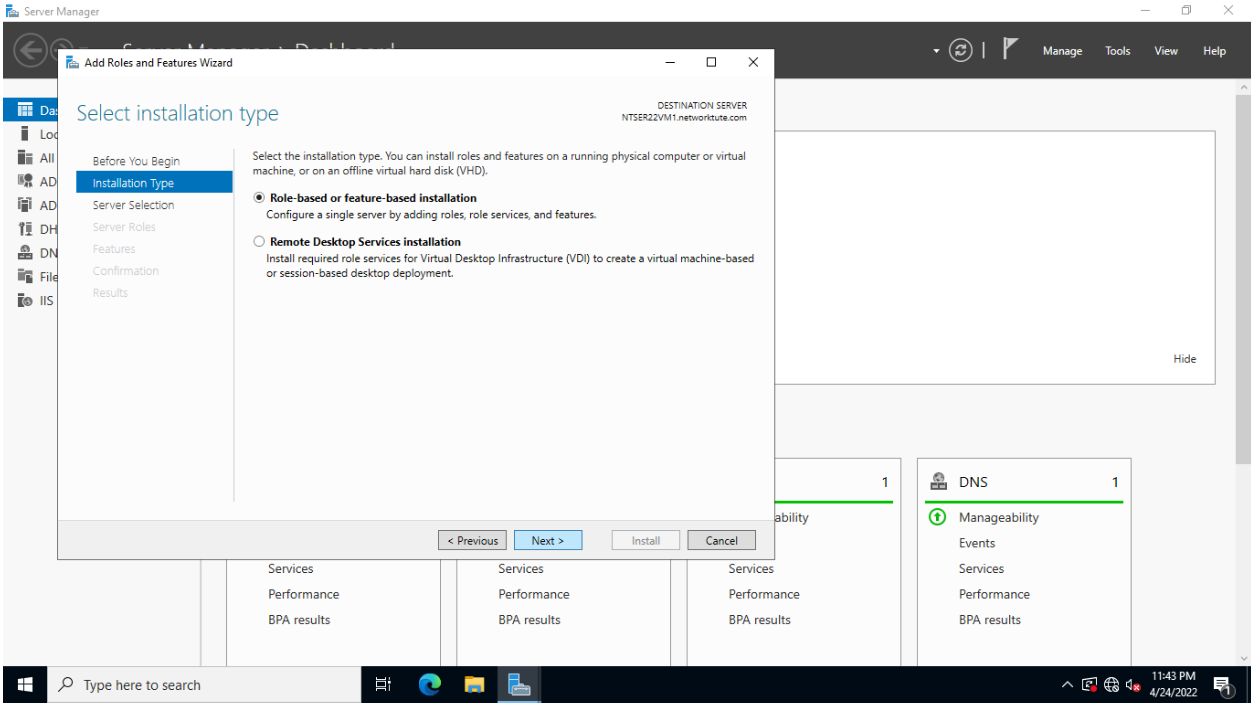
If you must verify that any of the preceding prerequisites have been completed, close the wizard, complete the steps, and then run the wizard again.

To continue, click Next.

□ Skip this page by default

Step 3:

On the **Select installation type** page, keep the default selection and click **Next**.



Select installation type

DESTINATION SERVER
NTSER22VM1.networktute.com

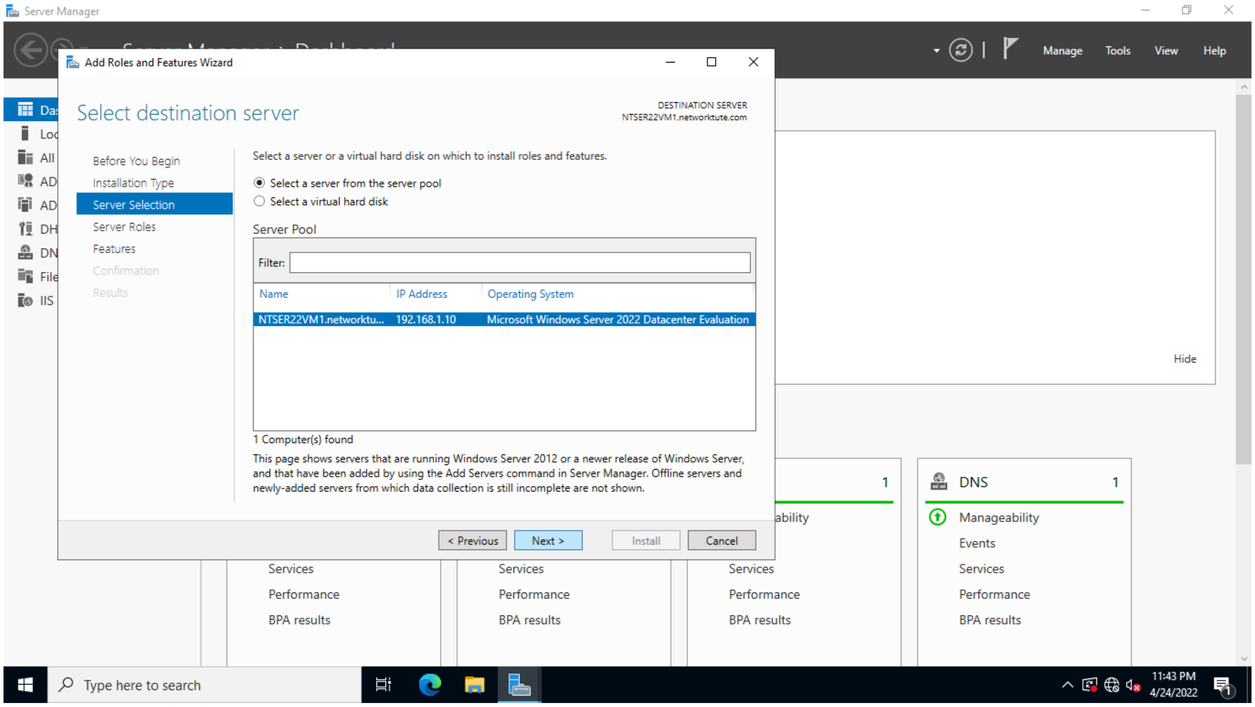
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **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.

Step 4:

In **Select destination server**, keep the default options and click **Next**.


Select destination server

DESTINATION SERVER
NTSER22VM1.networktute.com

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results

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
NTSER22VM1.networktu...	192.168.1.10	Microsoft Windows Server 2022 Datacenter Evaluation

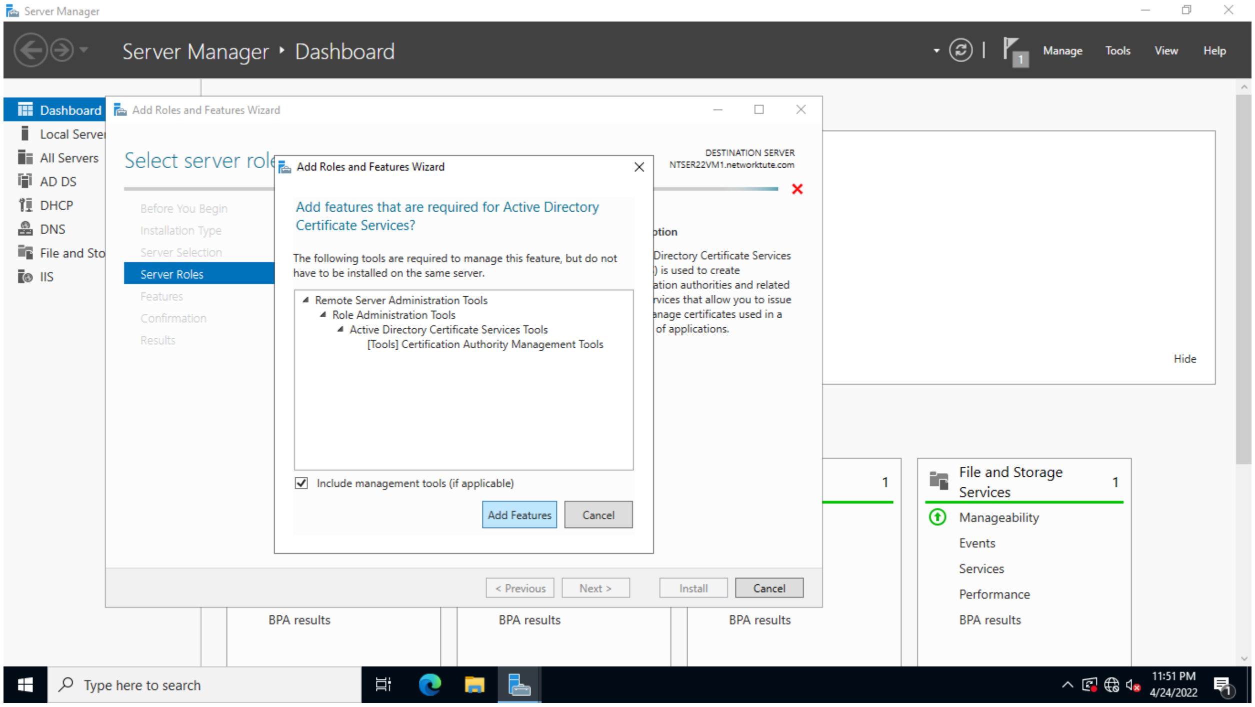
1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, 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.

Step 5:

From the **Select server roles** page, select the **Active Directory Certificate Services** checkbox.

The **Add Roles and Features Wizard** automatically appears. Click **Add Features**.


Add features that are required for Active Directory Certificate Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

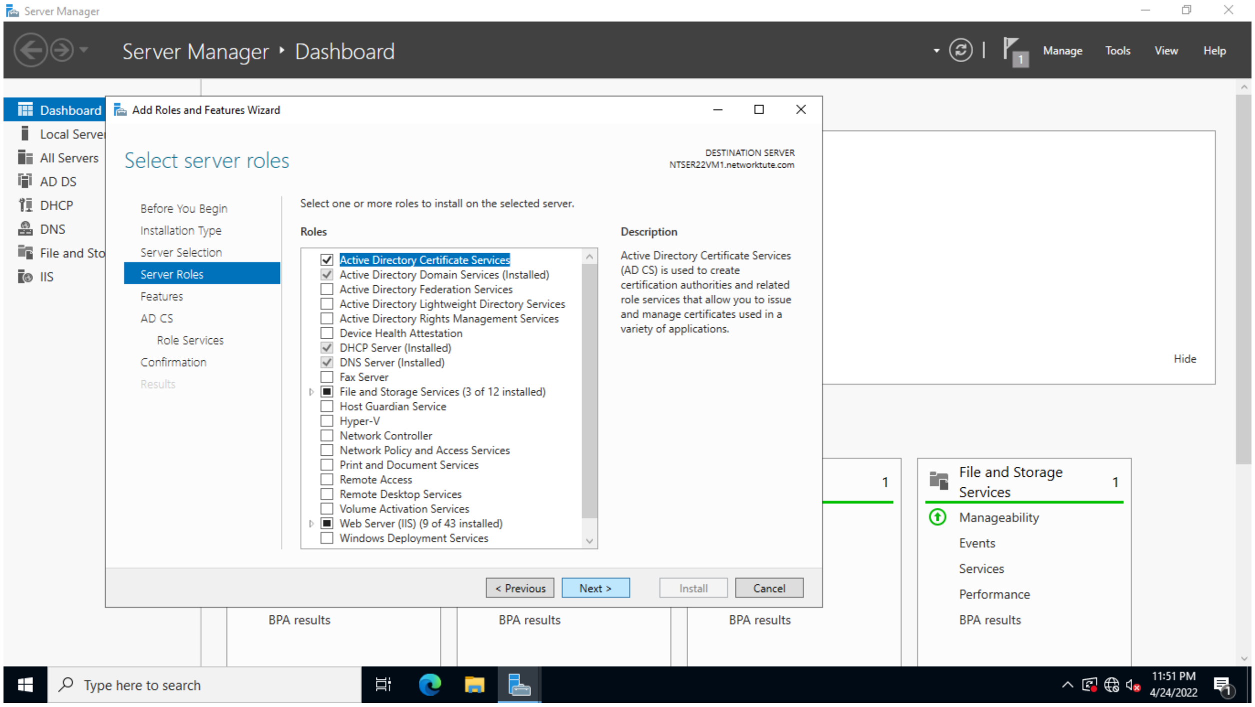
- Remote Server Administration Tools
  - Role Administration Tools
    - Active Directory Certificate Services Tools
      - [Tools] Certification Authority Management Tools

☑ Include management tools (if applicable)

Step 6:

Back on the **Select server roles** page, notice the **Active Directory Certificate Services** checkbox is now selected.

Click **Next** to continue.



Select server roles

DESTINATION SERVER
NTSER22VM1.networktute.com

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

Roles

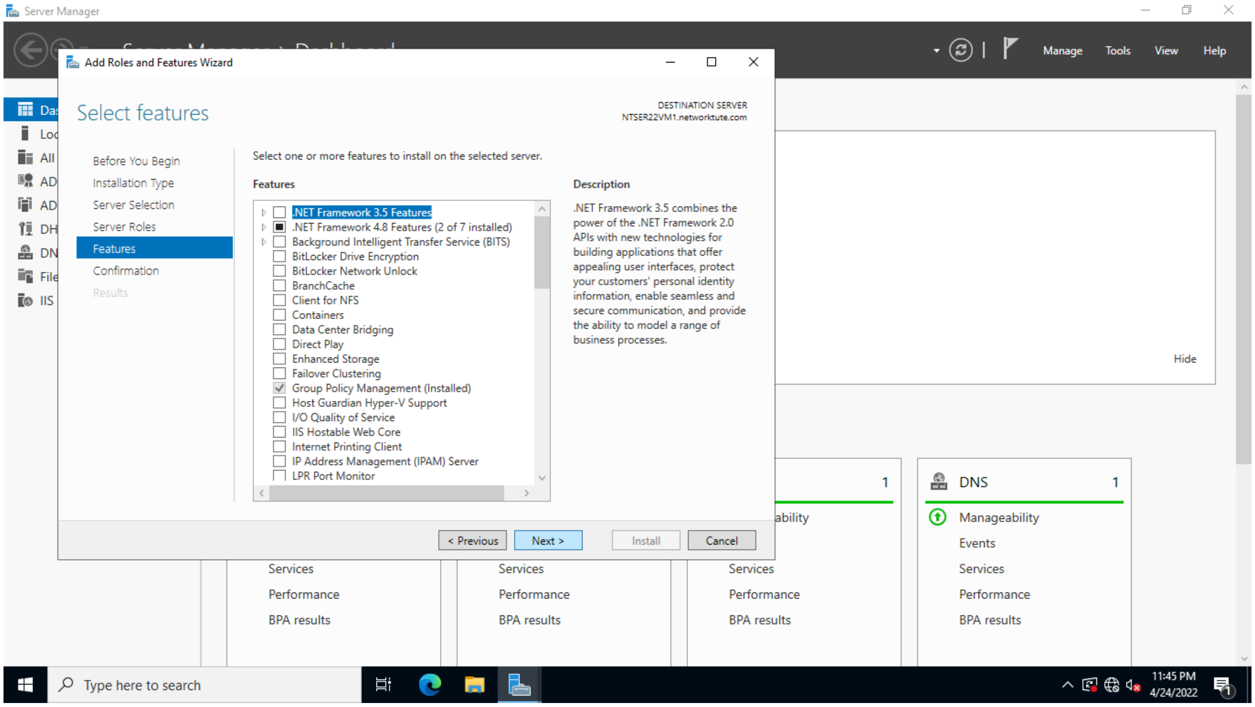
- ☑ Active Directory Certificate Services
- ☑ Active Directory Domain Services (Installed)
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- ☑ DHCP Server (Installed)
- ☑ DNS Server (Installed)
- □ Fax Server
- ■ File and Storage Services (3 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ Network Controller
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ■ Web Server (IIS) (9 of 43 installed)
- □ Windows Deployment 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.

Step 7:

On the **Select features** page, keep the default settings and then click **Next**.



Select features

DESTINATION SERVER
NTSER22VM1.networktute.com

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

Features

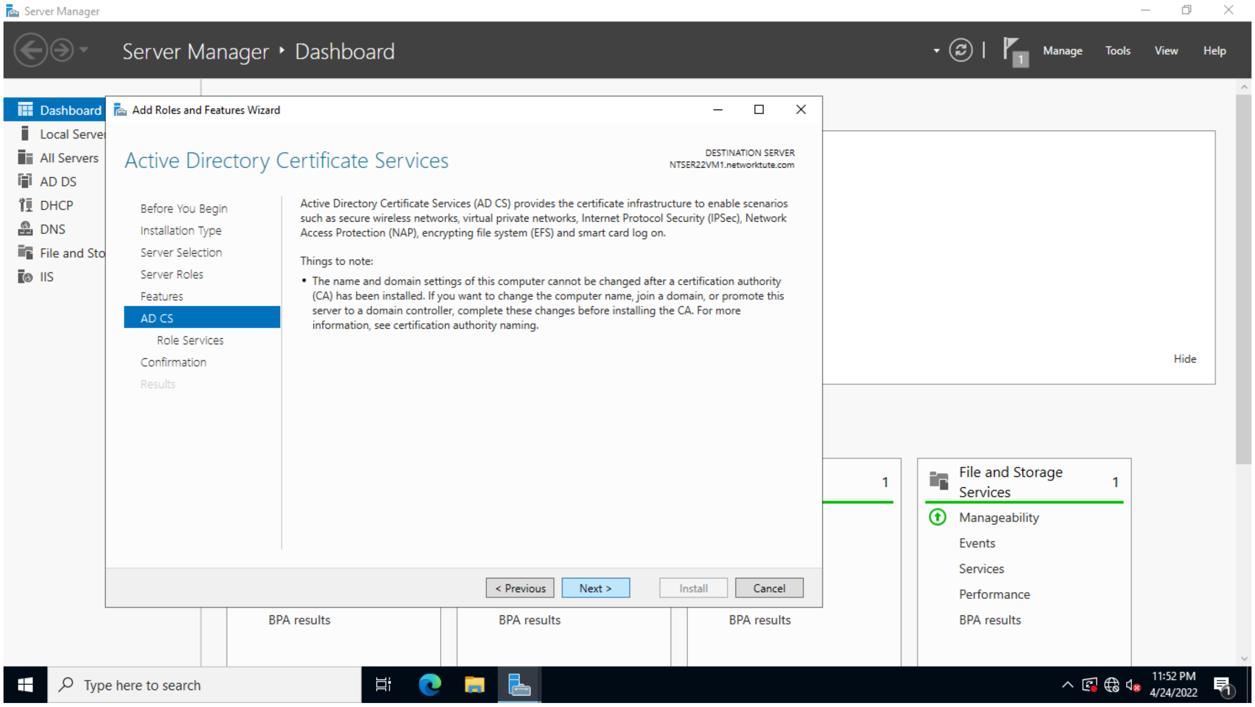
- ☐ .NET Framework 3.5 Features
- ■ .NET Framework 4.8 Features (2 of 7 installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache
- ☐ Client for NFS
- ☐ Containers
- ☐ Data Center Bridging
- ☐ Direct Play
- ☐ Enhanced Storage
- ☐ Failover Clustering
- ☑ Group Policy Management (Installed)
- ☐ Host Guardian Hyper-V Support
- ☐ I/O Quality of Service
- ☐ IIS Hostable Web Core
- ☐ Internet Printing Client
- ☐ IP Address Management (IPAM) Server
- ☐ LPR Port Monitor

Description

.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building 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.

Step 8:

On the **Active Directory Certificate Services** page, read the given information and click **Next**.



Active Directory Certificate Services

DESTINATION SERVER
NTSER22VM1.networktute.com

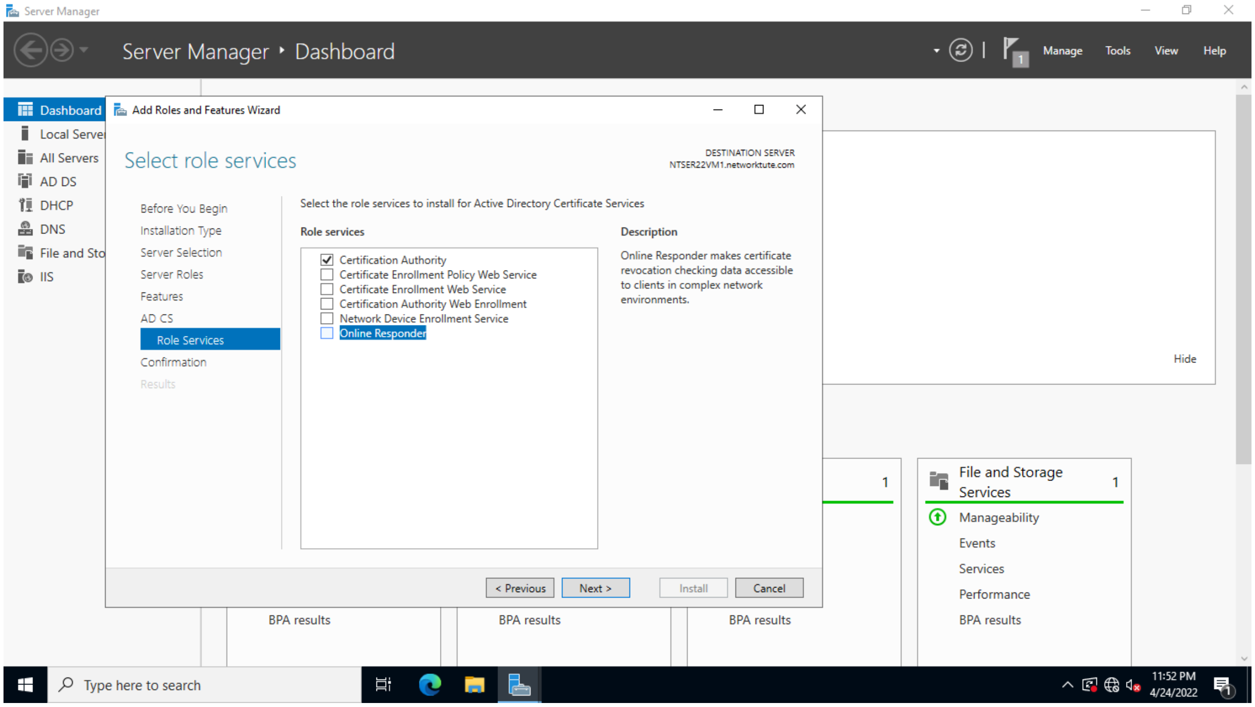
Active Directory Certificate Services (AD CS) provides the certificate infrastructure to enable scenarios such as secure wireless networks, virtual private networks, Internet Protocol Security (IPSec), Network Access Protection (NAP), encrypting file system (EFS) and smart card log on.

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.

Step 9:

From the **Select role services** page, ensure that the **Certification Authority** checkbox is selected, and then select the **Online Responder** checkbox.



Select role services

DESTINATION SERVER
NTSER22VM1.networktute.com

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

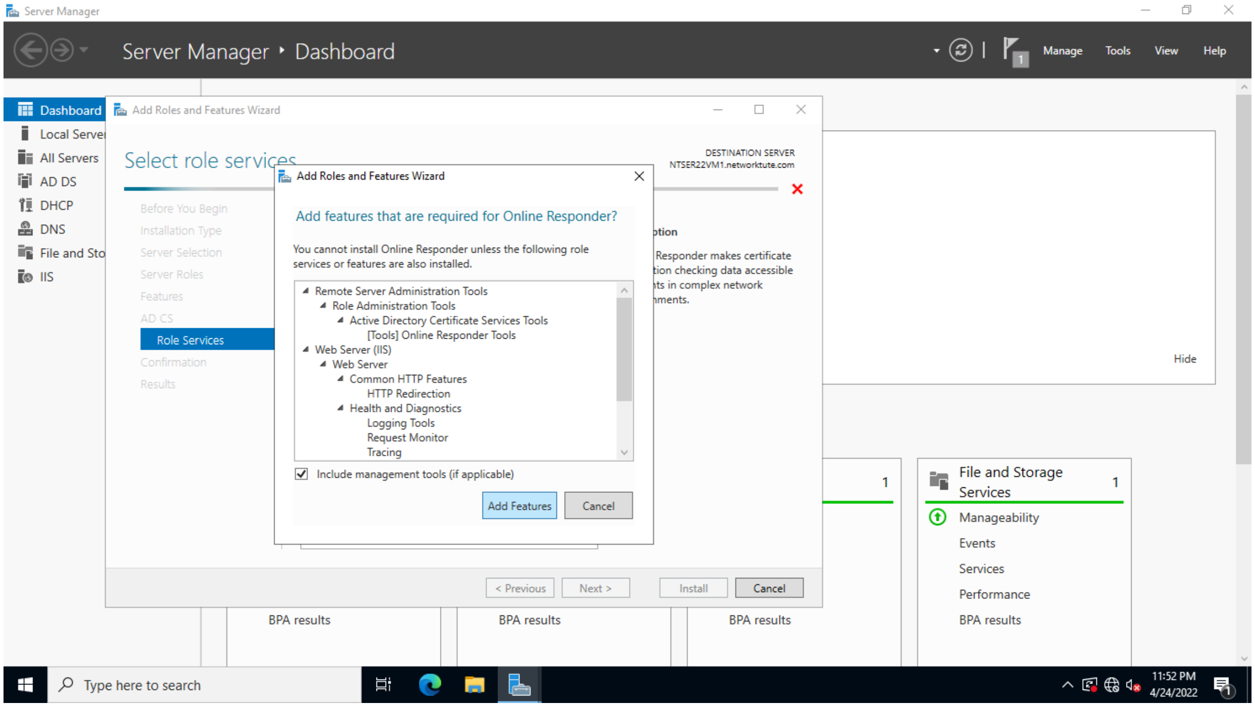
Description

Online Responder makes certificate revocation checking data accessible to clients in complex network environments.

Step 10:

The **Add Roles and Features Wizard** box appears as the component you selected will require other components for it to run.

Click **Add Features** to proceed.



Add Roles and Features Wizard

Add features that are required for Online Responder?

You cannot install Online Responder unless the following role services or features are also installed.

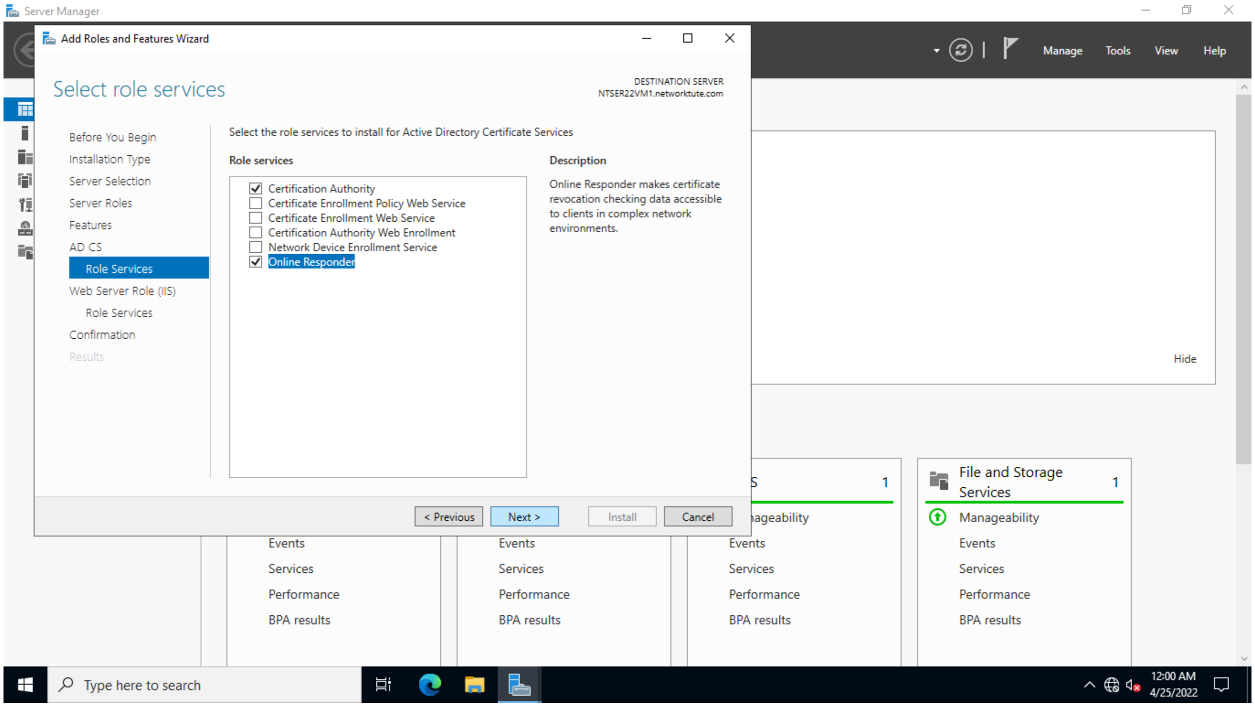
- Remote Server Administration Tools
  - Role Administration Tools
    - Active Directory Certificate Services Tools
      - [Tools] Online Responder Tools
- Web Server (IIS)
  - Web Server
    - Common HTTP Features
      - HTTP Redirection
    - Health and Diagnostics
      - Logging Tools
      - Request Monitor
      - Tracing

☑ Include management tools (if applicable)

Step 11:

Back on the Select role services page, now, the **Certification Authority** and **Online Responder** checkboxes are selected.

Click **Next**.



Select role services

DESTINATION SERVER
NTSER22VM1.networktute.com

Select the role services to install for Active Directory Certificate Services

Role services

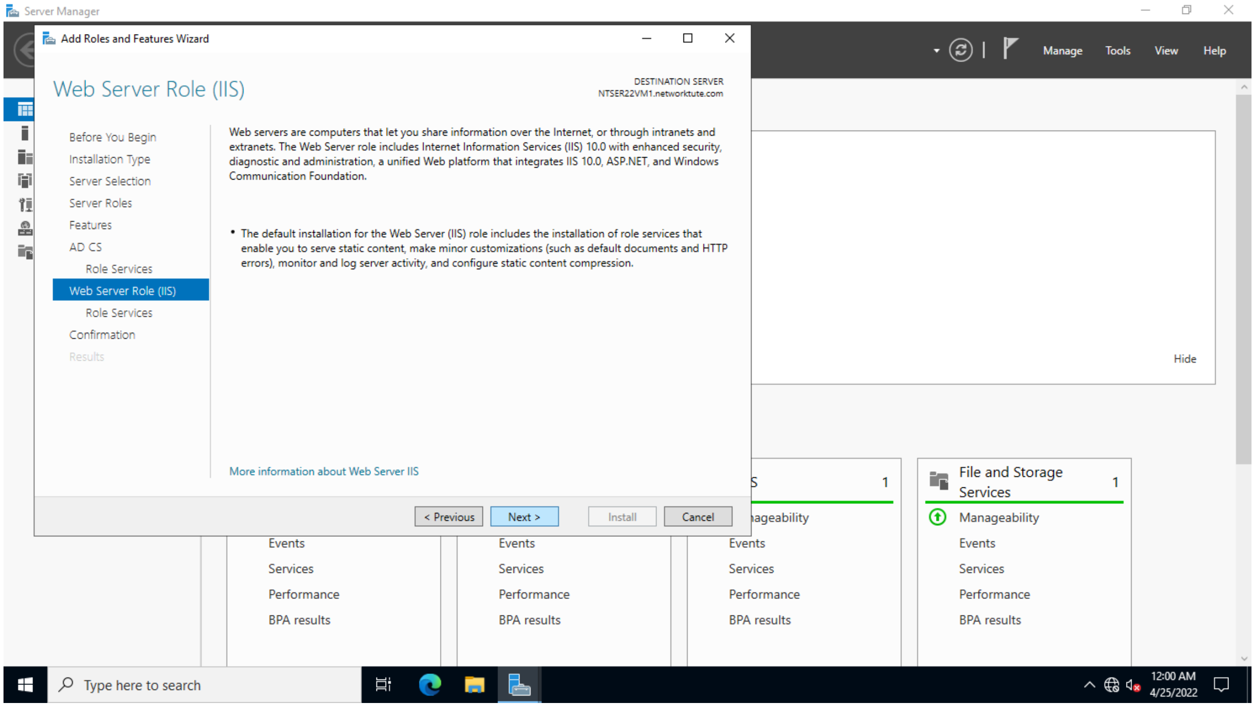
- ☑ Certification Authority
- □ Certificate Enrollment Policy Web Service
- □ Certificate Enrollment Web Service
- □ Certification Authority Web Enrollment
- □ Network Device Enrollment Service
- ☑ Online Responder

Description

Online Responder makes certificate revocation checking data accessible to clients in complex network environments.

Step 12:

On the **Web Server Role** (**IIS**) page, read the given information and then click **Next**.



Web Server Role (IIS)

DESTINATION SERVER
NTSER22VM1.networktute.com

Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.

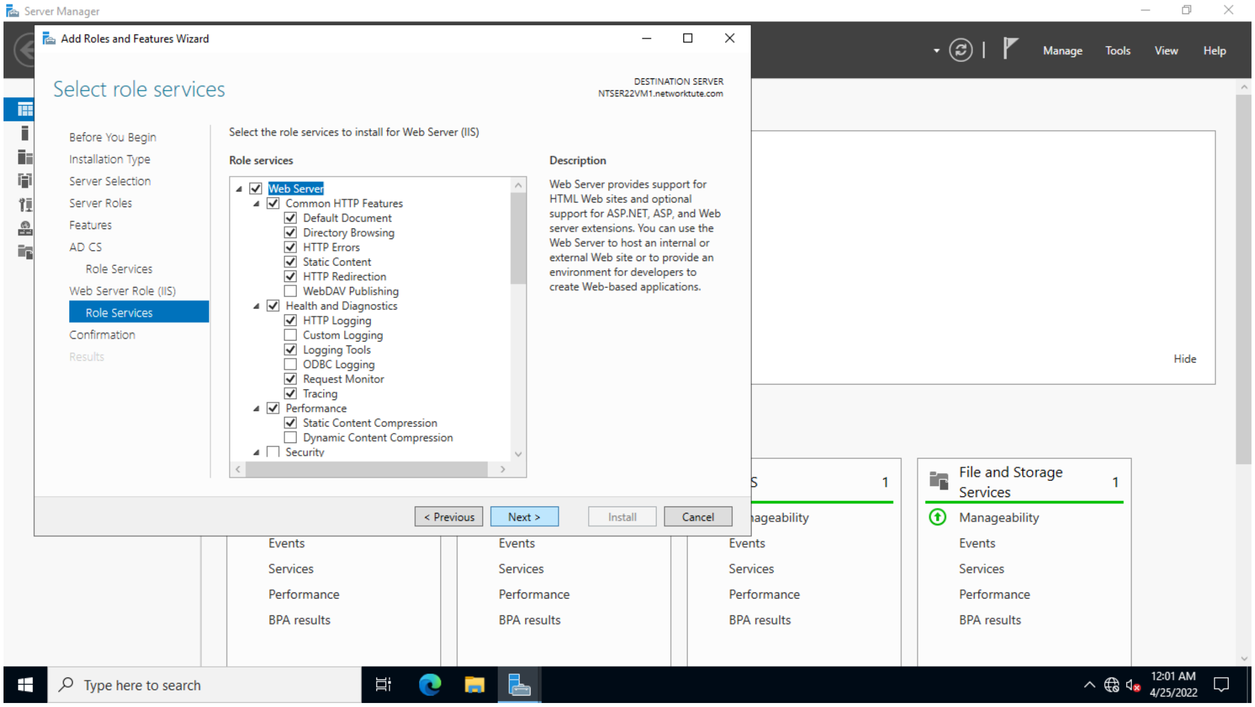
- The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.

More information about Web Server IIS

Step 13:

In the **Select role services** page, accept the default role services that will be added by IIS.

Click **Next**.



Select role services

DESTINATION SERVER
NTSER22VM1.networktute.com

Select the role services to install for Web Server (IIS)

Role services

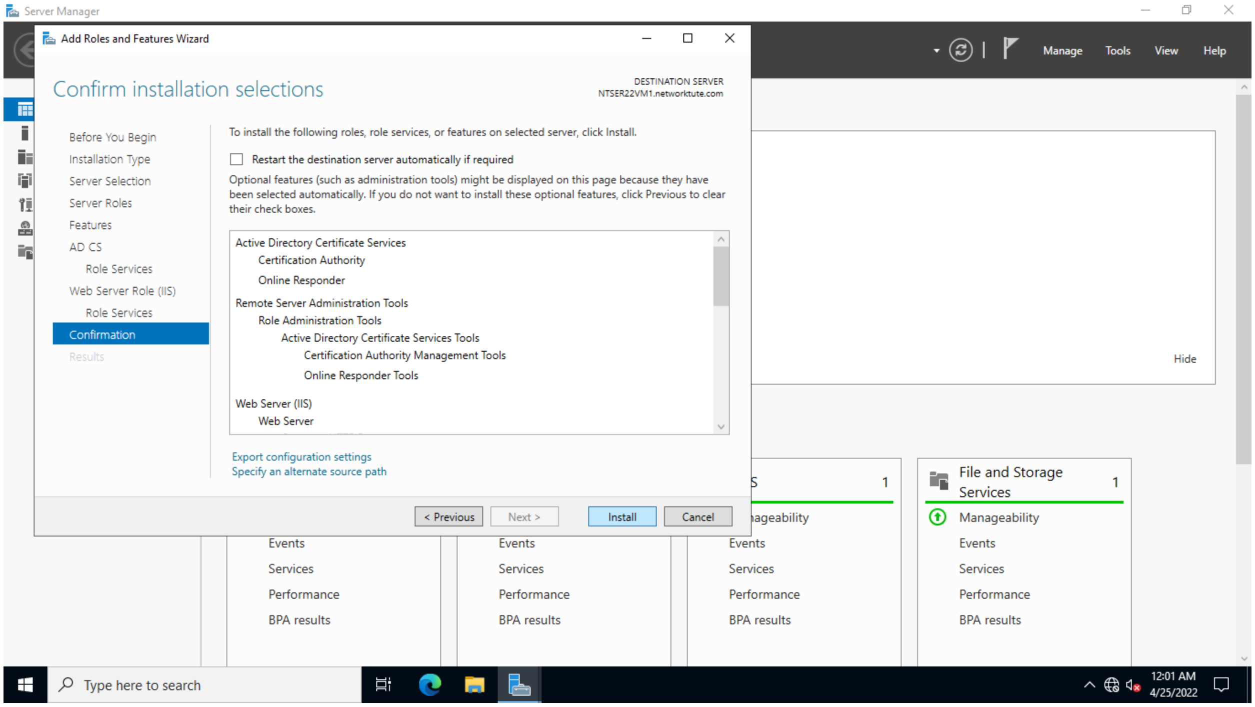
- ☑ Web Server
  - ☑ Common HTTP Features
    - ☑ Default Document
    - ☑ Directory Browsing
    - ☑ HTTP Errors
    - ☑ Static Content
    - ☑ HTTP Redirection
    - □ WebDAV Publishing
  - ☑ Health and Diagnostics
    - ☑ HTTP Logging
    - □ Custom Logging
    - ☑ Logging Tools
    - □ ODBC Logging
    - ☑ Request Monitor
    - ☑ Tracing
  - ☑ Performance
    - ☑ Static Content Compression
    - □ Dynamic Content Compression
  - □ Security

Description

Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

Step 14:

On the **Confirm installation selections** page, click **Install**.



Add Roles and Features Wizard

Confirm installation selections

DESTINATION SERVER
NTSER22VM1.networktute.com

- Before You Begin
- Installation Type
- Server Selection
- Server Roles
- Features
- AD CS
  - Role Services
- Web Server Role (IIS)
  - Role Services
- Confirmation
- Results

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
  - Online Responder
- Remote Server Administration Tools
  - Role Administration Tools
    - Active Directory Certificate Services Tools
      - Certification Authority Management Tools
      - Online Responder Tools
- Web Server (IIS)
  - Web Server

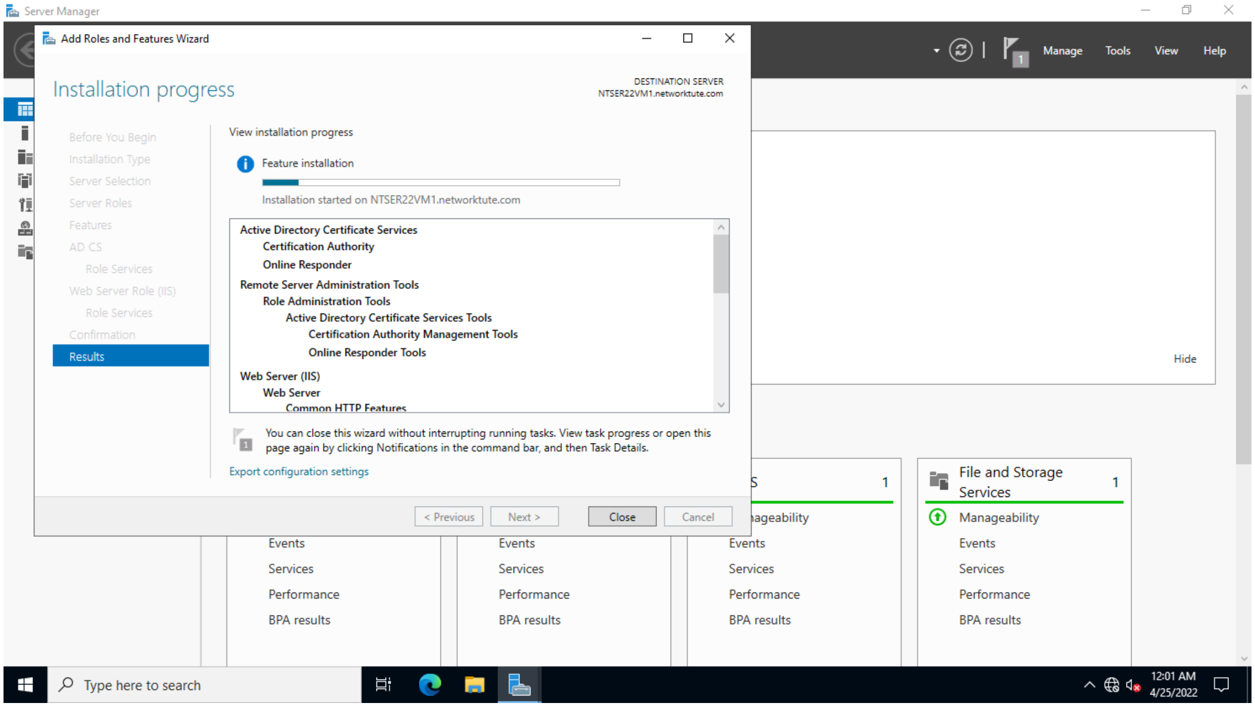
Export configuration settings
Specify an alternate source path

< Previous | Next > | Install | Cancel

Step 15:

The installation will begin, which will take a few minutes.

Important: "The request to add or remove features on the specified server failed," if you get an error message. Close the window. When the Server Manager is busy collecting system information about the server after a recent start-up or reboot, this happens. Wait around 1 minute before continuing with the Windows feature installation in this task. If the problem persists, restart the infected computer and reinstall the Windows features from scratch.



Installation progress

DESTINATION SERVER
NTSER22VM1.networktute.com

View installation progress

Feature installation

Installation started on NTSER22VM1.networktute.com

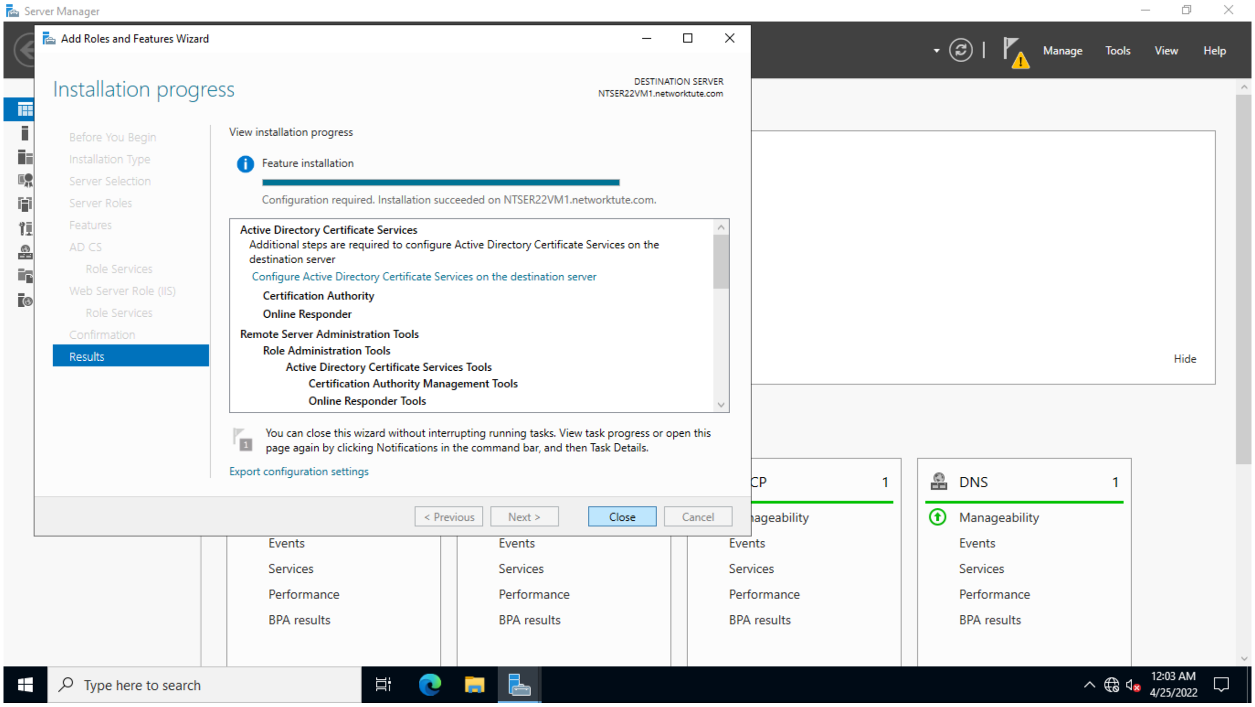
```
Active Directory Certificate Services
    Certification Authority
    Online Responder
Remote Server Administration Tools
    Role Administration Tools
        Active Directory Certificate Services Tools
            Certification Authority Management Tools
            Online Responder Tools
Web Server (IIS)
    Web Server
        Common HTTP Features
```

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

Step 16:

Click **Close** when **Installation progress** reports a successful operation. You are back on the **Server Manager** console.



Installation progress

DESTINATION SERVER
NTSER22VM1.networktute.com

View installation progress

Feature installation

Configuration required. Installation succeeded on NTSER22VM1.networktute.com.

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

Task 2: Configure Active Directory Certificate Services

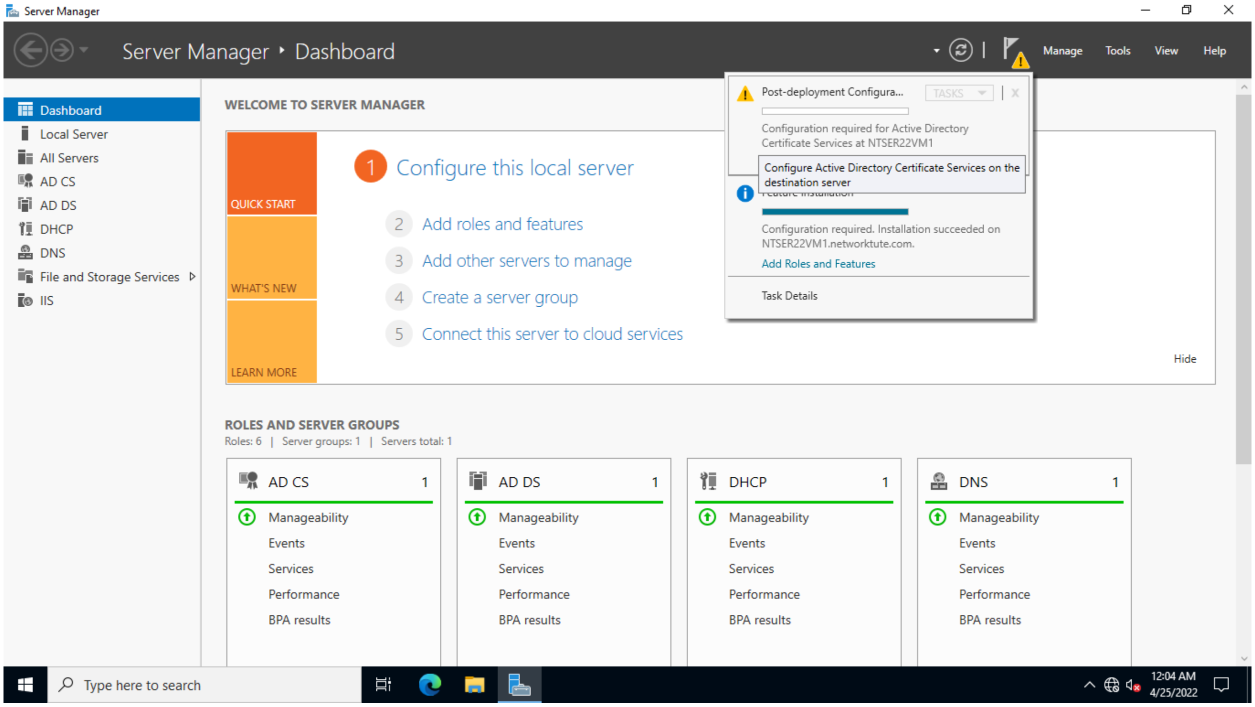
After you've installed Active Directory Certificate Services and Online Responder on **NTSER22VM1**, you'll need to configure these services with the correct settings. This will allow these services to fulfill their intended functions.

Follow these steps to configure Active Directory Certificate Services

Step 1:

On **NTSER22VM1**, ensure that you are on the **Server Manager** console.

Click the flag icon and click the **Configure Active Directory Certificate Services on the destination server** link.



Post-deployment Configura...

Configuration required for Active Directory Certificate Services at NTSER22VM1

Configure Active Directory Certificate Services on the destination server

Feature installation

Configuration required. Installation succeeded on NTSER22VM1.networktute.com.

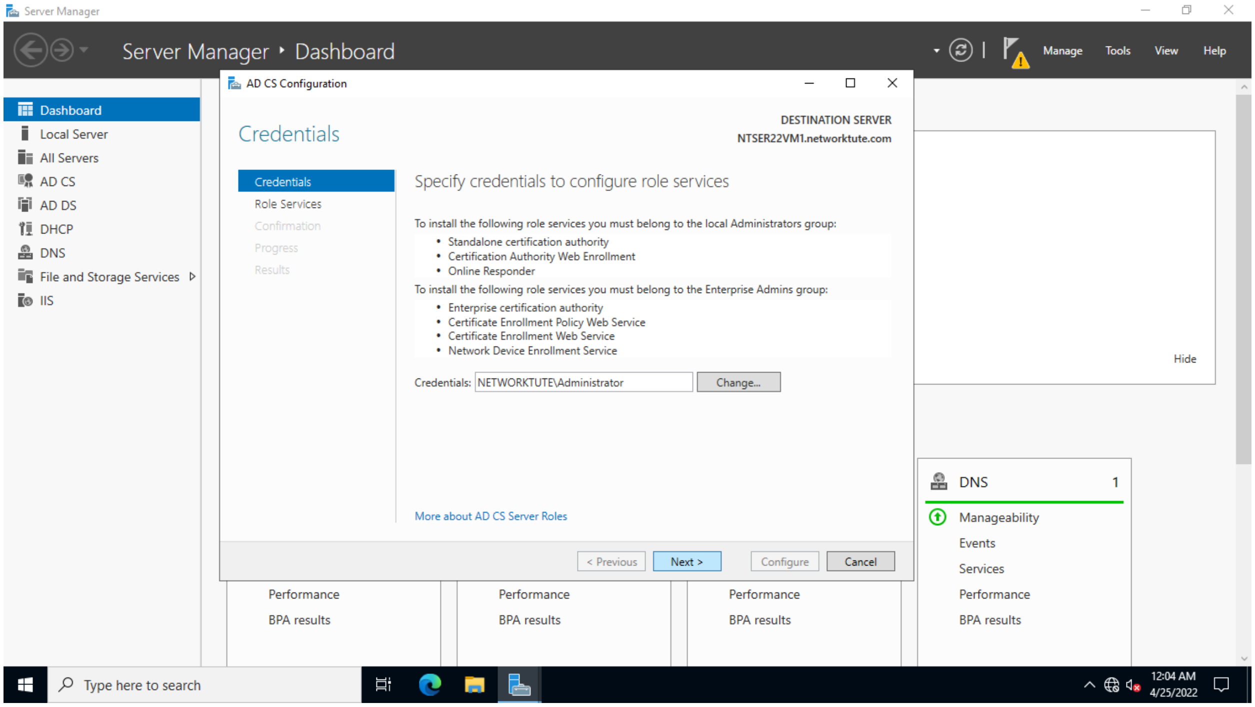
Add Roles and Features

Task Details

Step 2:

On the **Credentials** page of the **AD CS Configuration** wizard, the system has detected that you are currently signed in as **NETWORKTUTE\Administrator**.

Click **Next.**



Credentials

DESTINATION SERVER
NTSER22VM1.networktute.com

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:

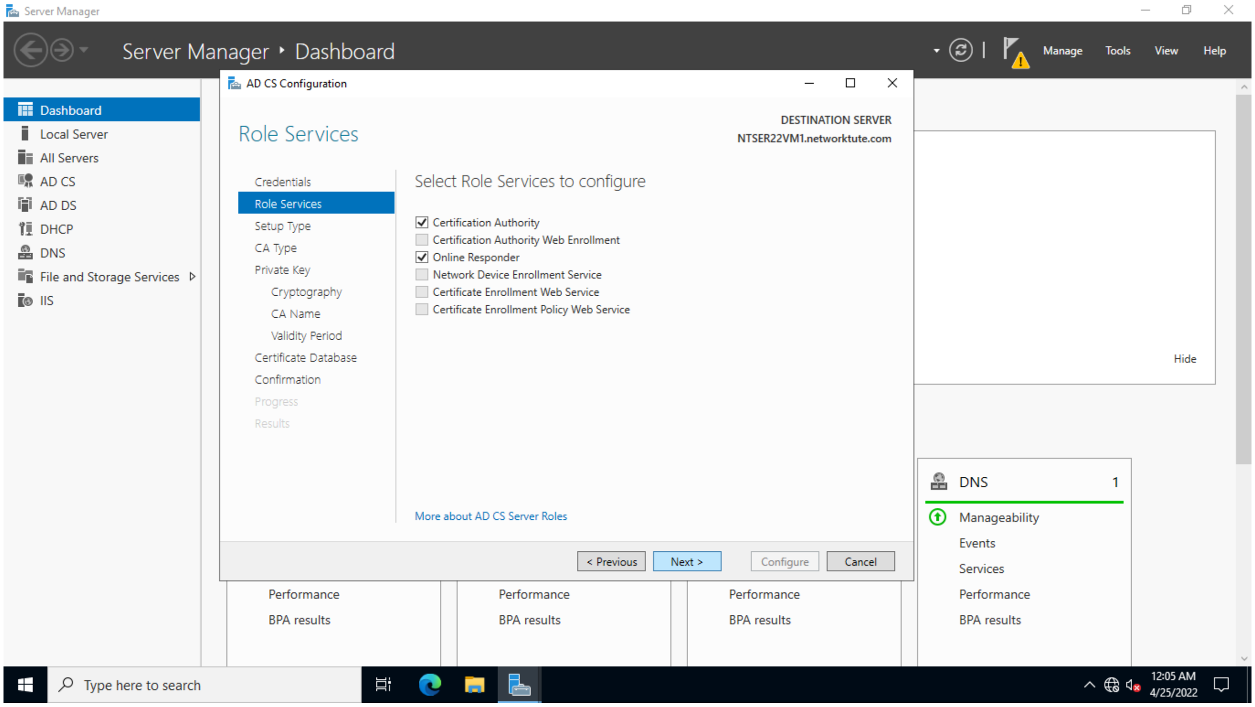
- Enterprise certification authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Network Device Enrollment Service

Credentials: NETWORKTUTE\Administrator

Step 3:

In **Role Services**, select the **Certification Authority** checkbox. There will be a momentary pause when you select this.

Then, select the **Online Responder** checkbox and click **Next**.



Role Services

DESTINATION SERVER
NTSER22VM1.networktute.com

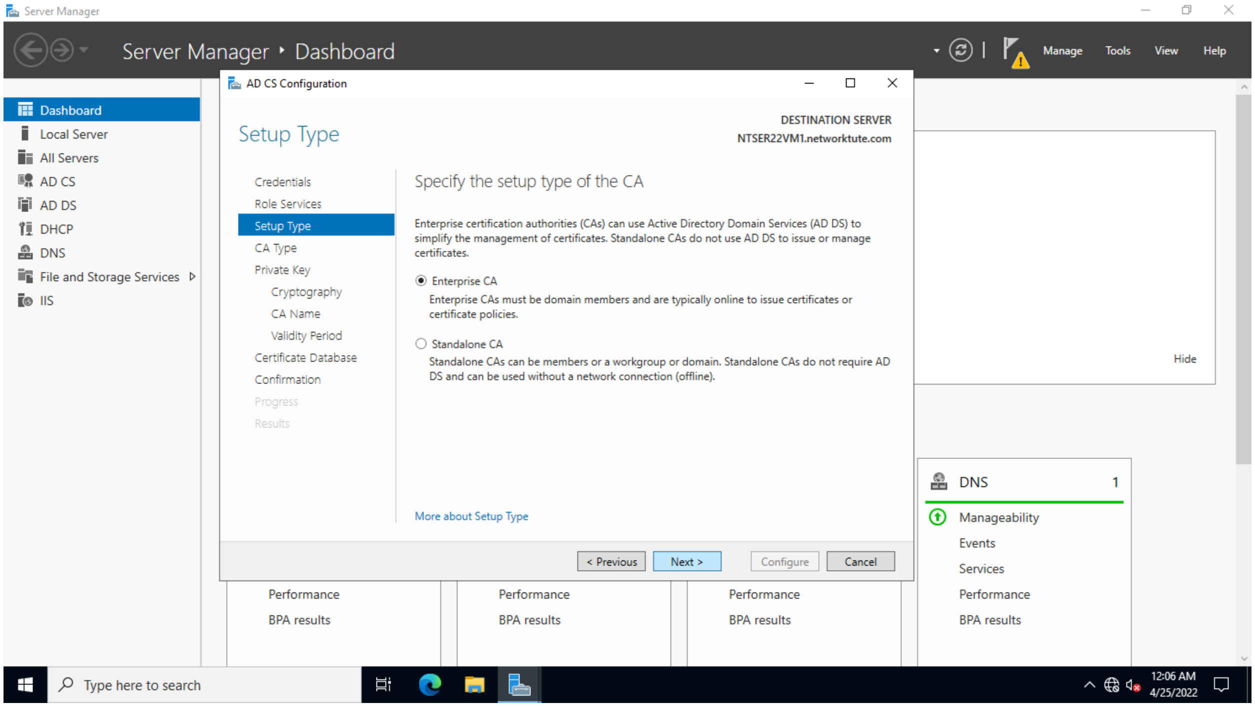
Select Role Services to configure

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

Step 4:

On the **Setup** Type page, ensure that the **Enterprise CA** option is selected.

Click **Next.**



Setup Type

DESTINATION SERVER
NTSER22VM1.networktute.com

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.

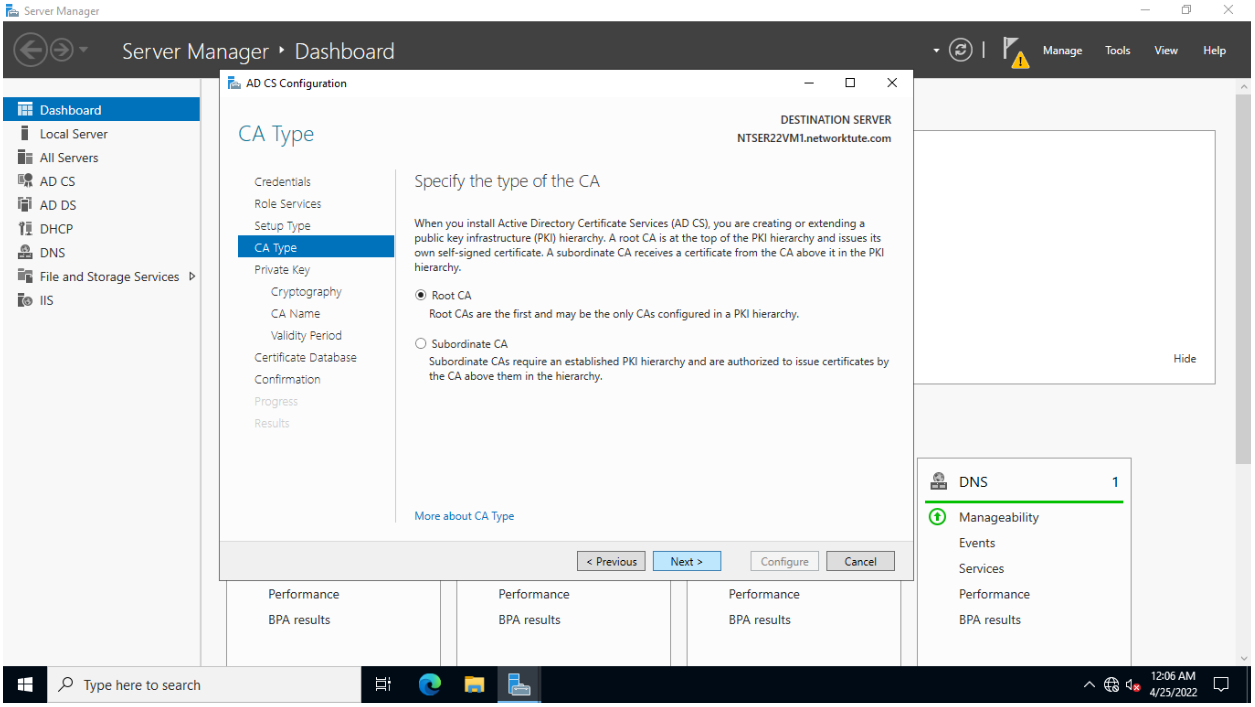
○ Standalone CA

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).

Step 5:

On the **CA Type** page, ensure that **Root CA** is selected.

Click **Next**.



CA Type

DESTINATION SERVER
NTSER22VM1.networktute.com

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.

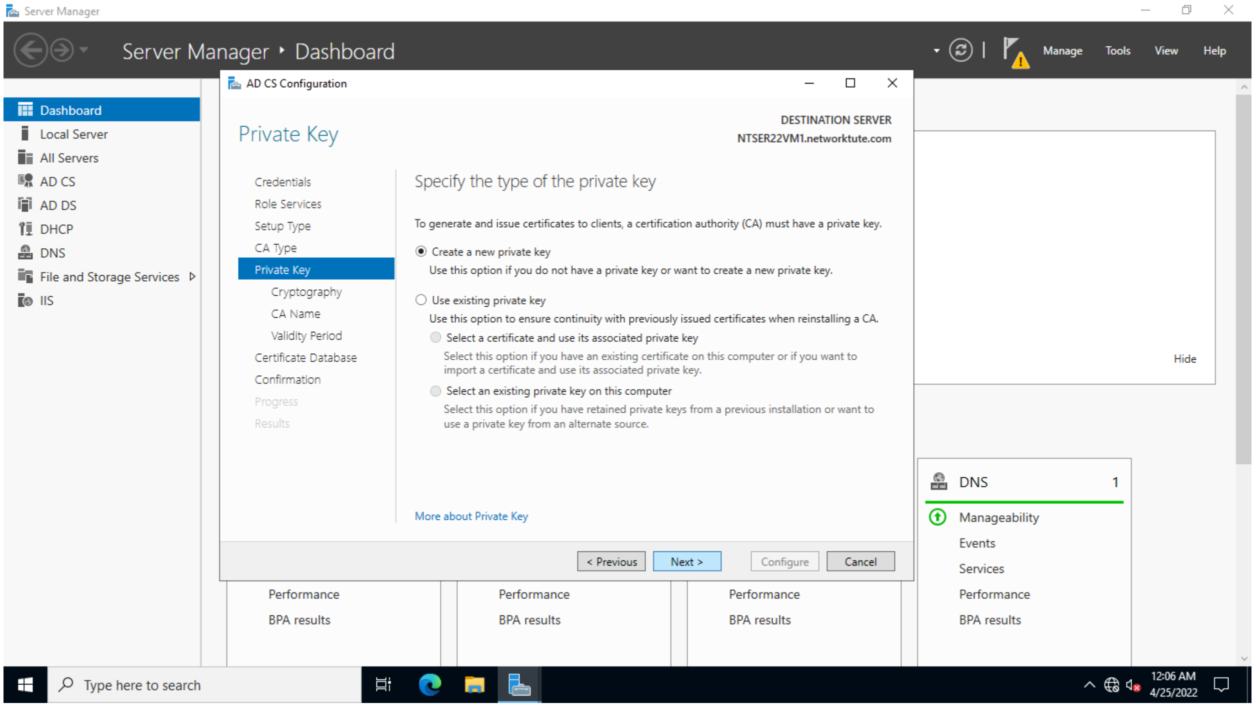
● Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.

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

Step 6:

On the **Private Key** page, verify that the **Create a new private key** radio button is selected.

Click **Next.**



Private Key

DESTINATION SERVER
NTSER22VM1.networktute.com

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.

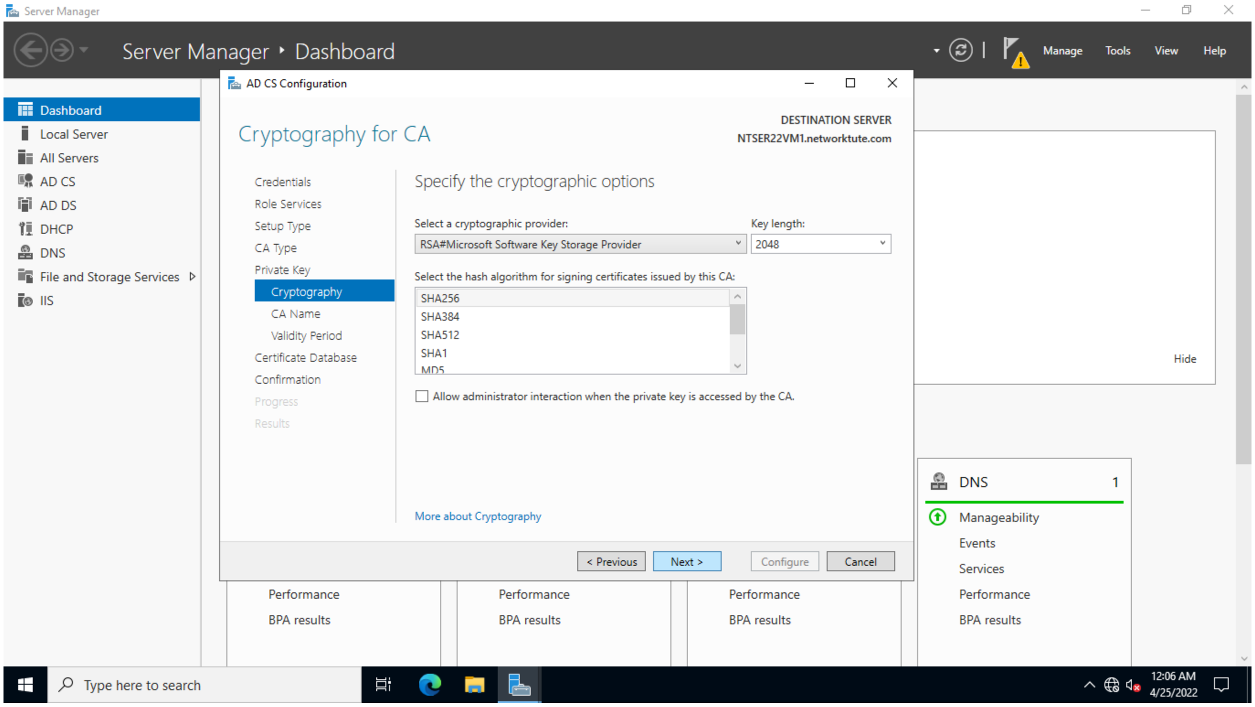
○ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

○ 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.

Step 7:

On the **Cryptography for CA** page, keep the default cryptographic settings and click **Next**.



Cryptography for CA

DESTINATION SERVER
NTSER22VM1.networktute.com

Specify the cryptographic options

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

Key length: 2048

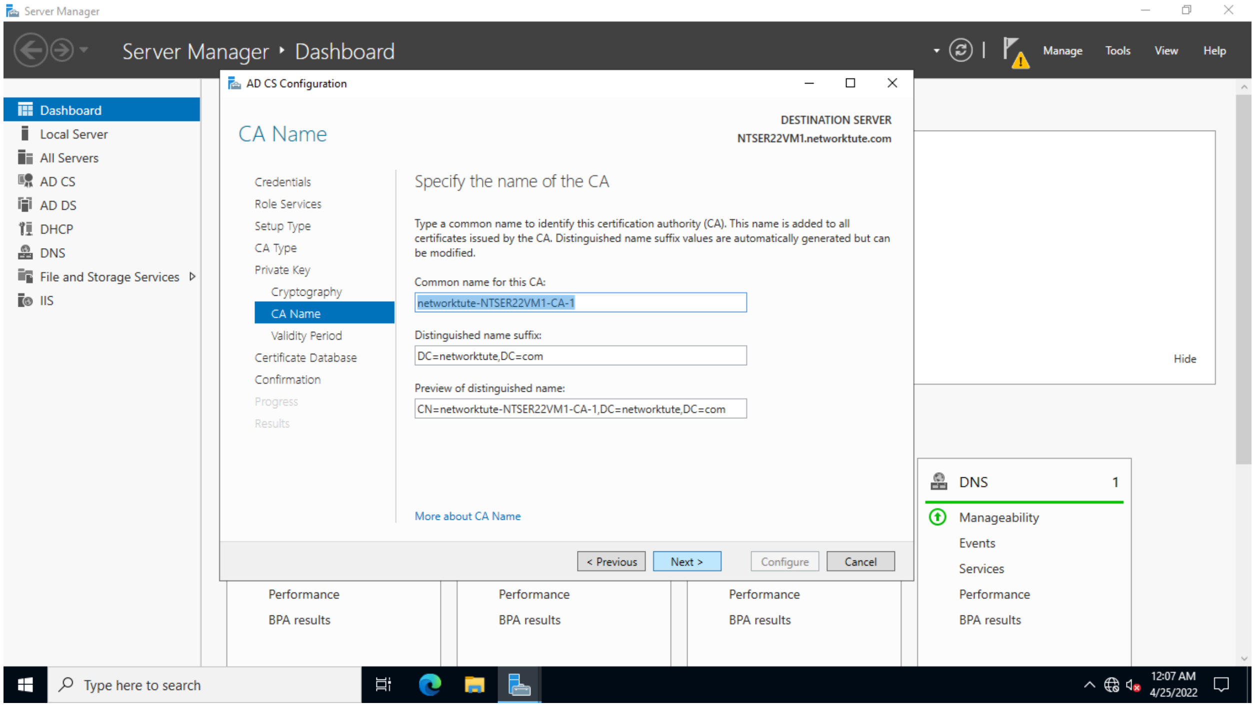
Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

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

Step 8:

On the **CA Name** page, keep the default **CA Name** supplied by the **AD CS Configuration** and then click **Next**



CA Name

DESTINATION SERVER
NTSER22VM1.networktute.com

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.

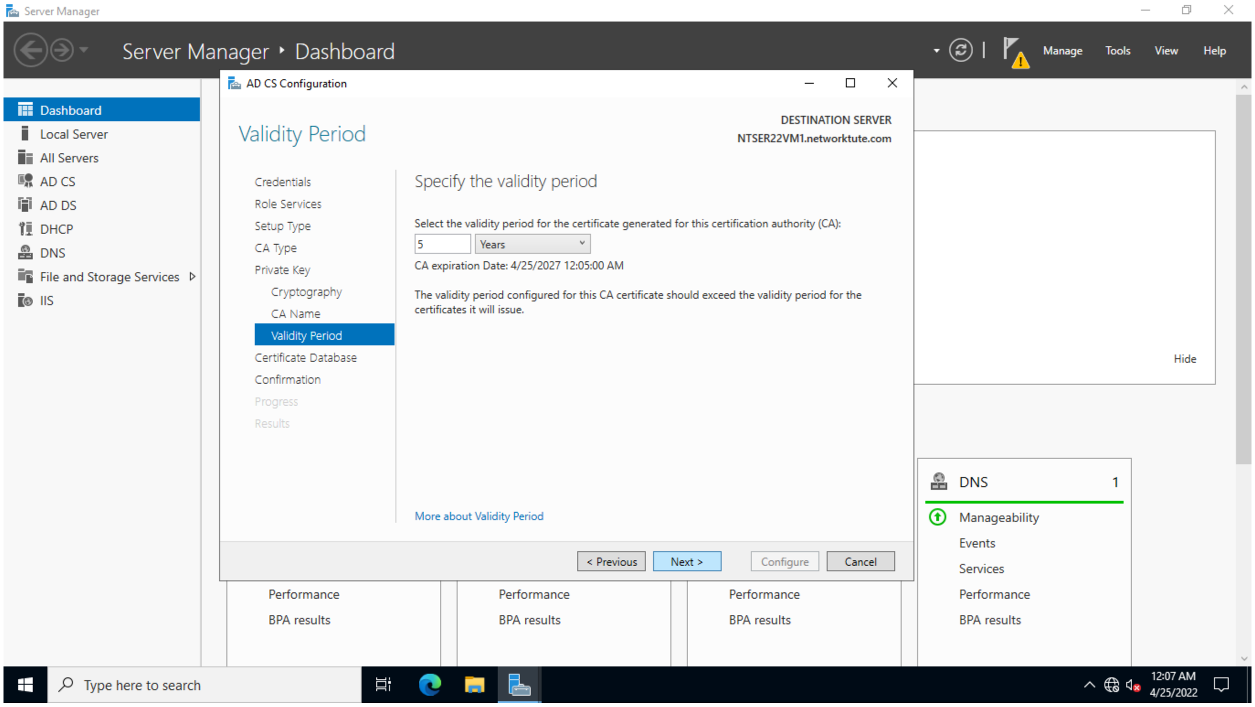
Common name for this CA: networktute-NTSER22VM1-CA-1

Distinguished name suffix: DC=networktute,DC=com

Preview of distinguished name: CN=networktute-NTSER22VM1-CA-1,DC=networktute,DC=com

Step 9:

On the **Validity Period** page, keep the default settings and click **Next**.



Validity Period

DESTINATION SERVER
NTSER22VM1.networktute.com

Specify the validity period

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

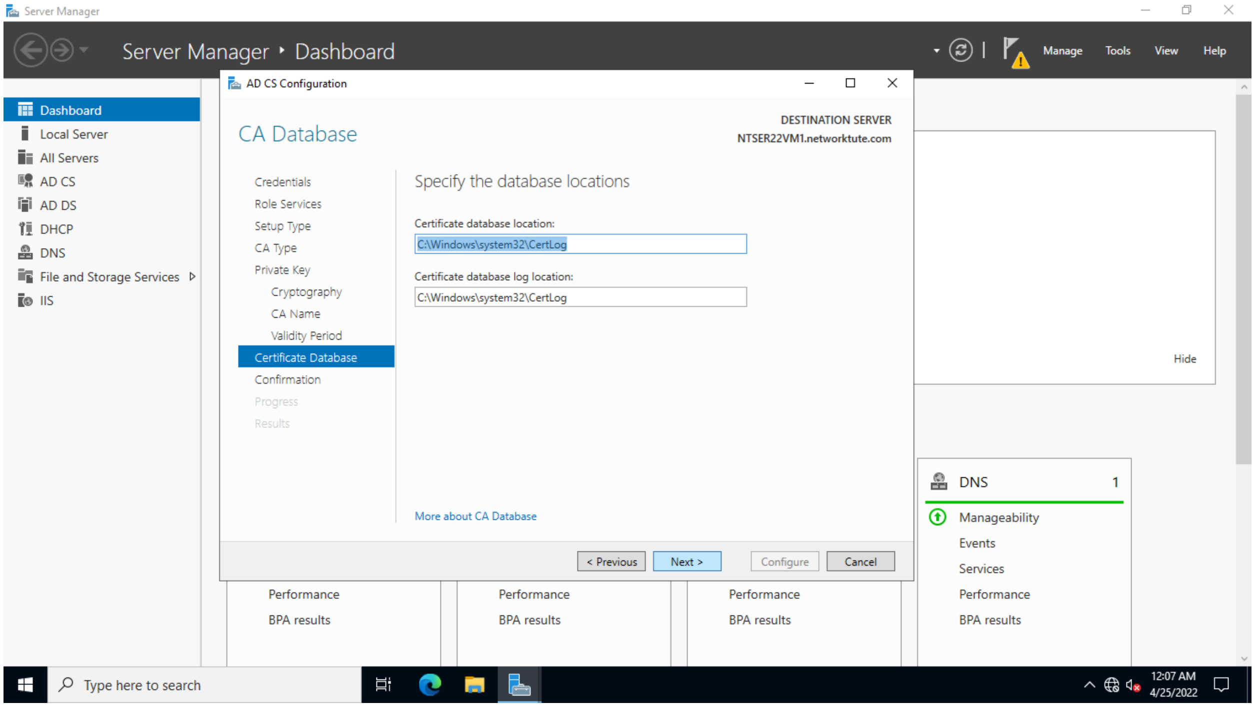
5 Years

CA expiration Date: 4/25/2027 12:05:00 AM

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

Step 10:

On the **CA Database** page, keep the default settings and then click **Next**.



CA Database

DESTINATION SERVER
NTSER22VM1.networktute.com

Specify the database locations

Certificate database location:

C:\Windows\system32\CertLog

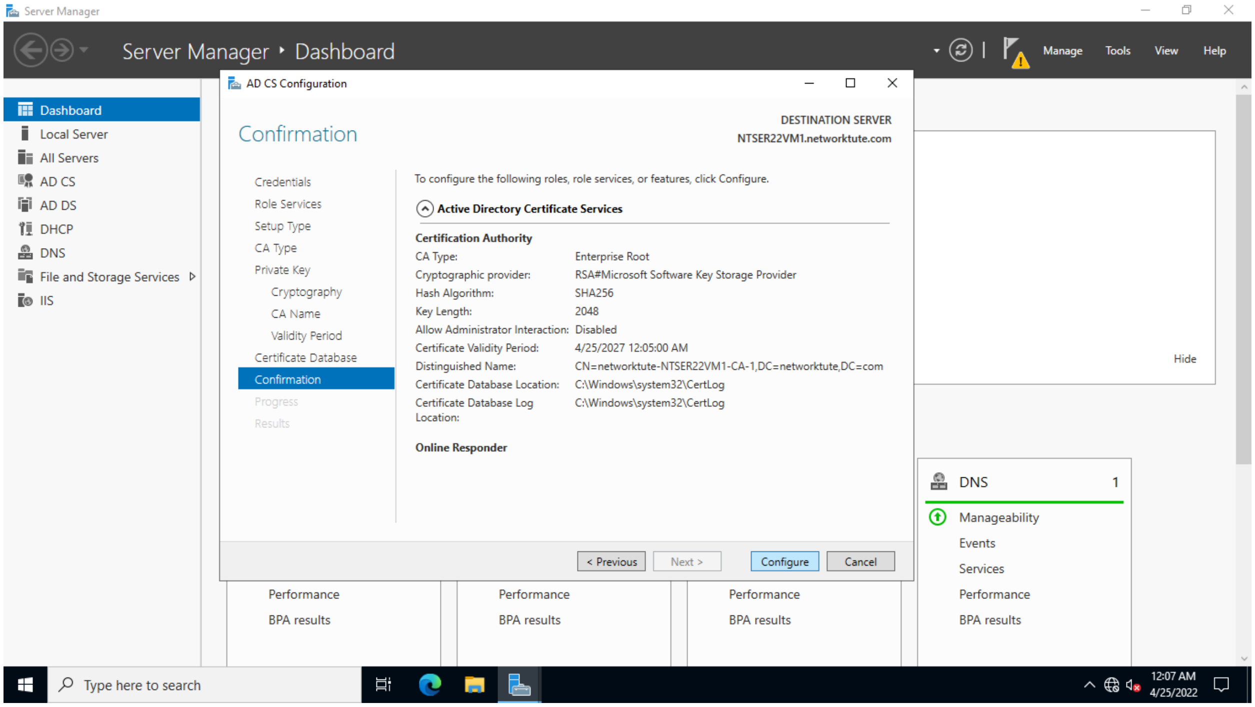
Certificate database log location:

C:\Windows\system32\CertLog

Step 11:

On the **Confirmation** page, read through the summary settings of this **Active Directory Certificate Services** that are about to be set up.

Click **Configure** to proceed with the configuration of AD CS.



DESTINATION SERVER
NTSER22VM1.networktute.com

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

Active Directory Certificate Services

Certification Authority

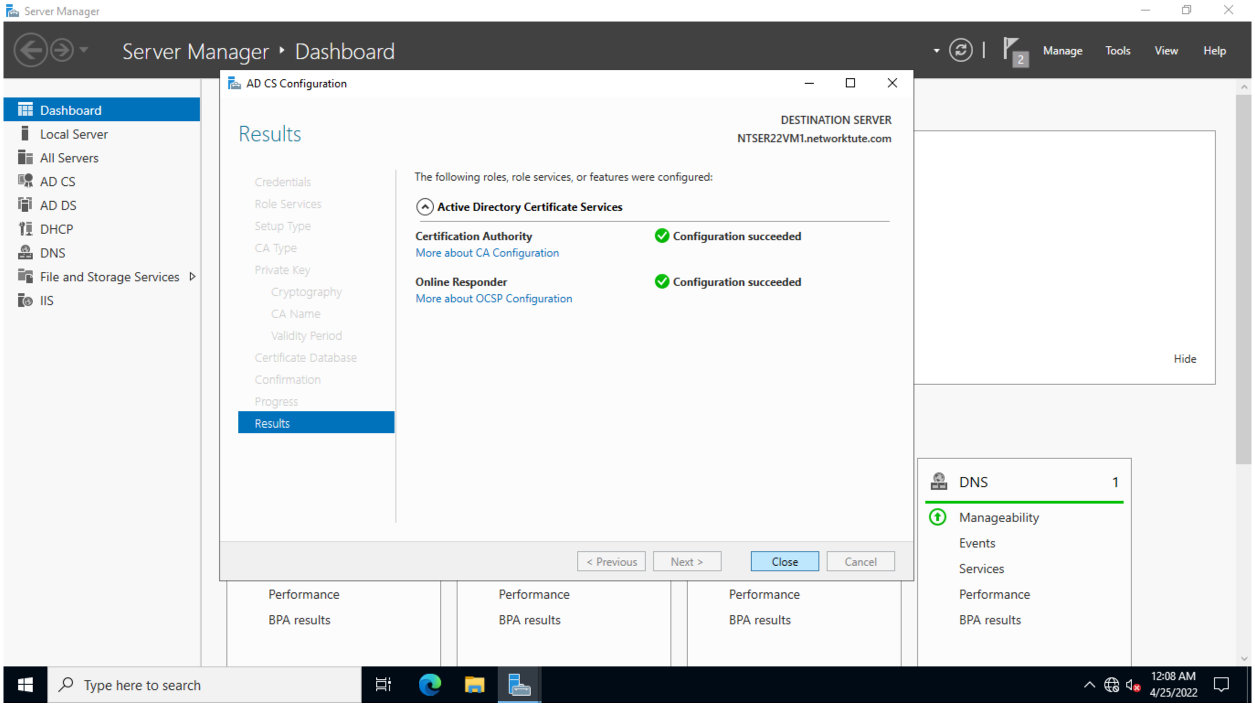
CA Type:	Enterprise Root
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	2048
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	4/25/2027 12:05:00 AM
Distinguished Name:	CN=networktute-NTSER22VM1-CA-1,DC=networktute,DC=com
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Online Responder

Step 12:

Please wait while the service is being set up.

On the **Results** page, when the results are displayed with **Configuration succeeded**, click **Close**



DESTINATION SERVER
NTSER22VM1.networktute.com

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

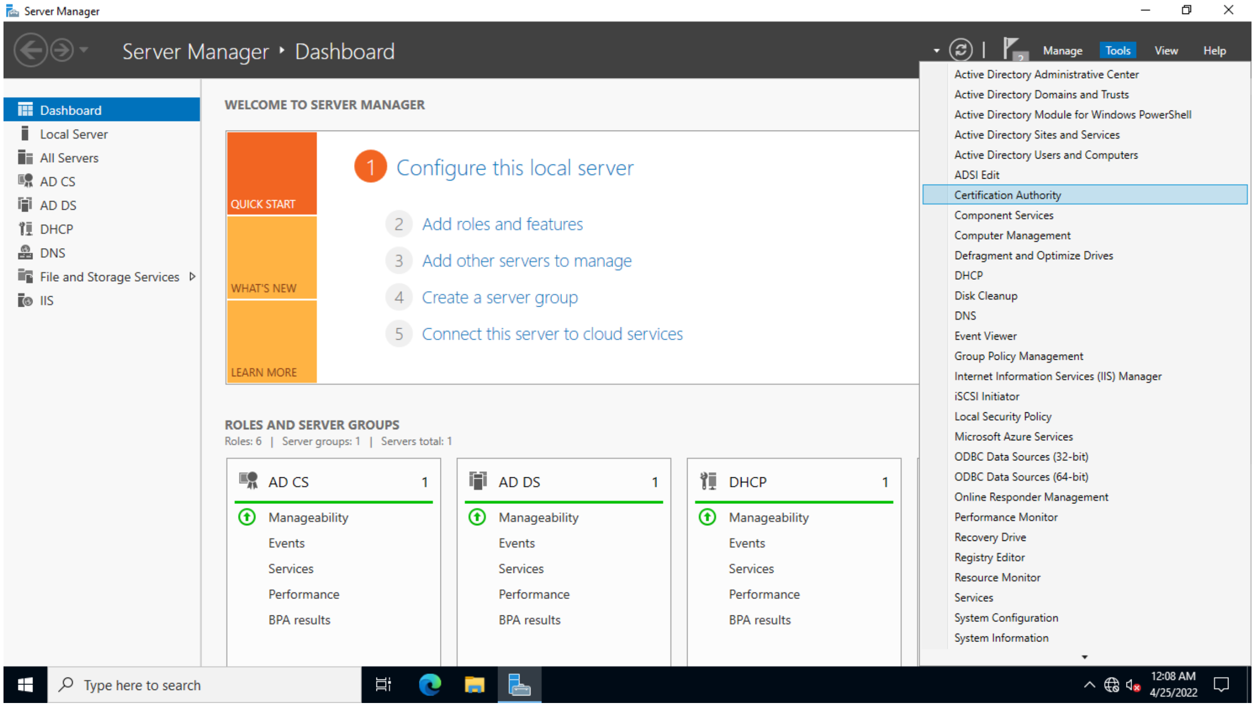
Active Directory Certificate Services

Certification Authority More about CA Configuration	Configuration succeeded
Online Responder More about OCSP Configuration	Configuration succeeded

Step 13:

You are back on the **Server Manager** console. You need to verify now that AD CS is working.

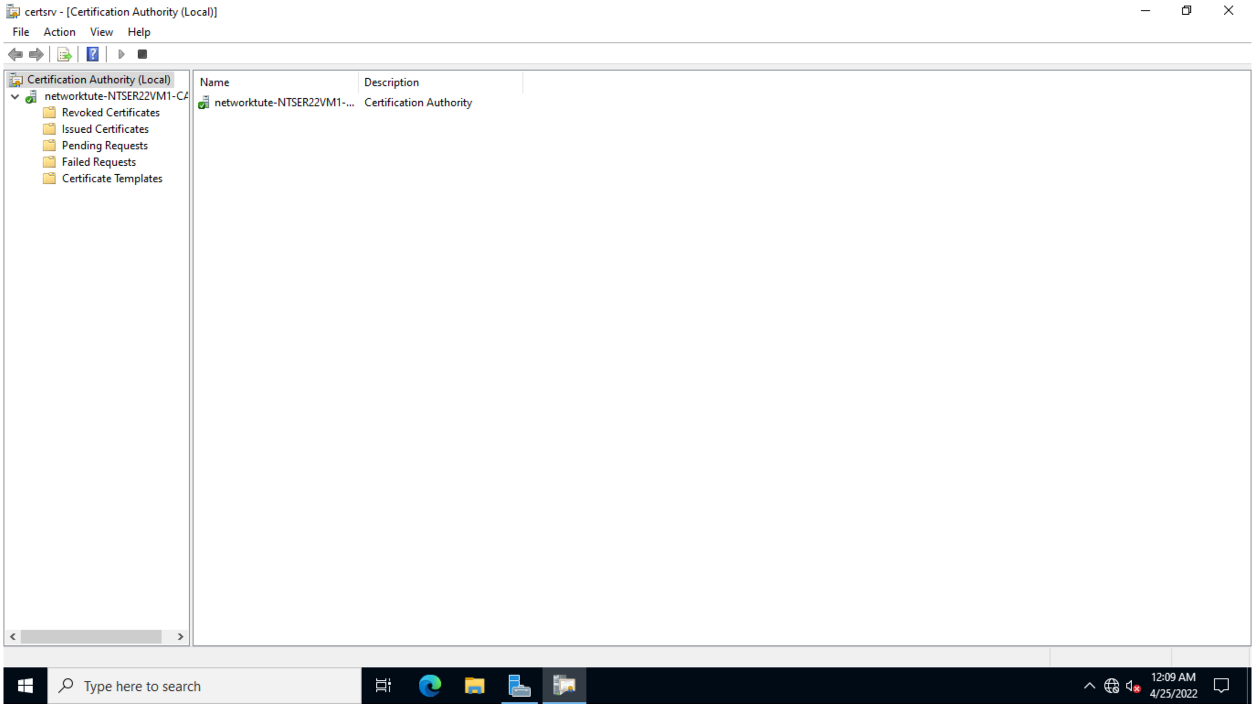
From the **Server Manager** console, click **Tools** and then select **Certification Authority**.



Step 14:

Verify **Certification Authority** snap-in works by expanding the **networktute-NTSER22VM1-CA** node.

Minimize the **Certification Authority** and **Server Manager** windows.



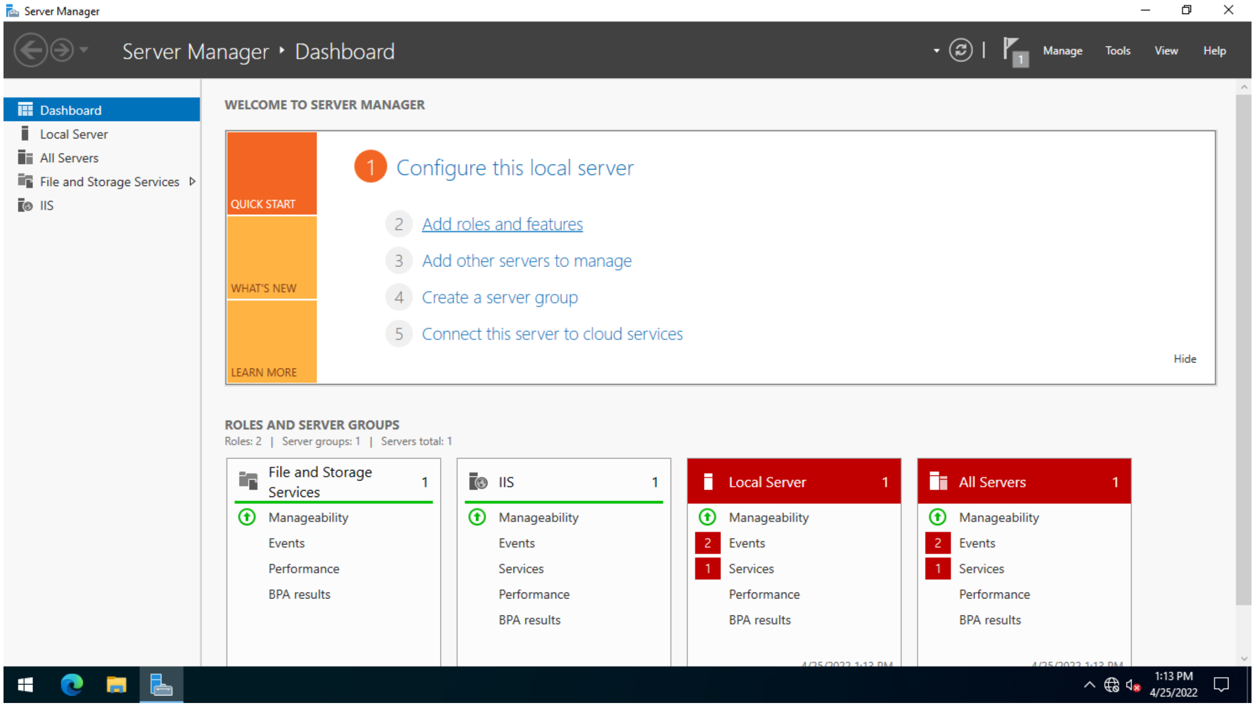
Task 3: Install Subordinate CA

On a domain member server named **NTSER22DM1**, you will install a subordinate CA of Networktute.com. The steps will be the same as when you installed the Enterprise Root CA previously.

Step 1:

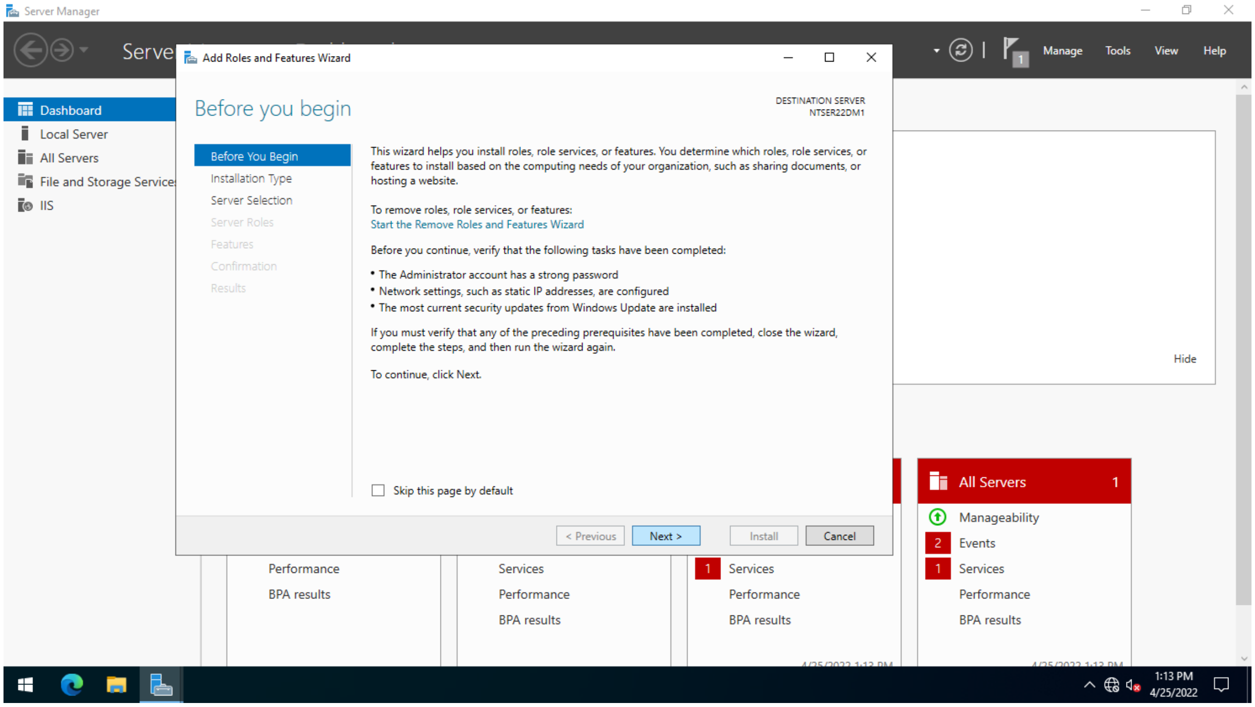
Connect to **NTSER22DM1**.

The **Server Manager** console opens automatically. Click **Add roles and features**.



Step 2:

On the **Before you begin** page of the **Add Roles and Features Wizard**, 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.

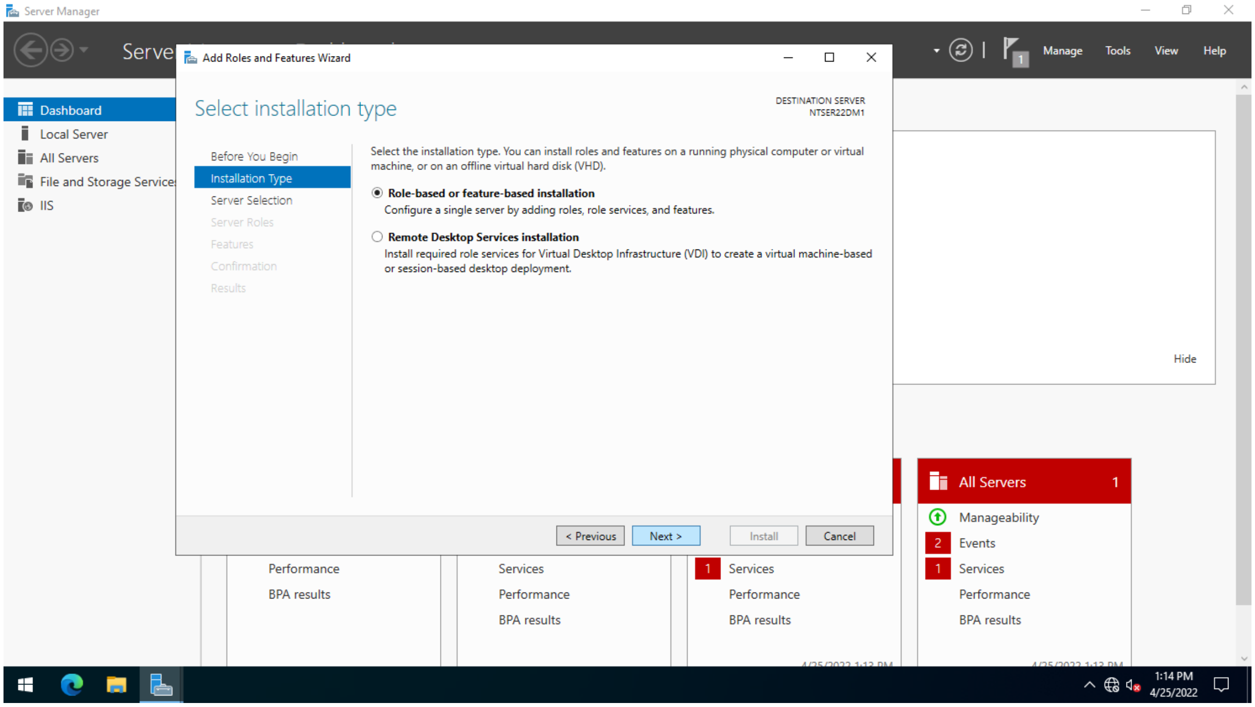
To continue, click Next.

☐ Skip this page by default

Step 3:

On the **Select installation type** page, keep the default setting **Role-based or feature-based installation** option.

Click **Next**.



Add Roles and Features Wizard

Select installation type

DESTINATION SERVER
NTSER22DM1

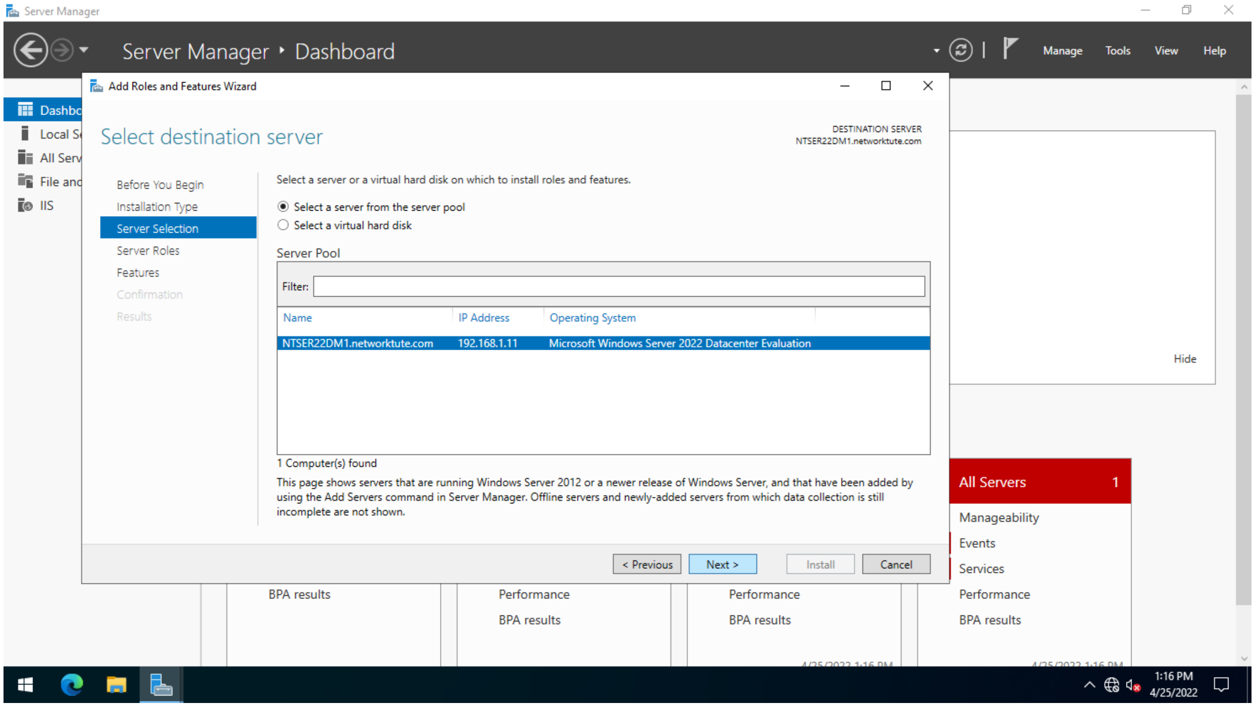
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **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.

Step 4:

From **Select destination server** page, click **Next**.



Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
NTSER22DM1.networktute.com

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
NTSER22DM1.networktute.com	192.168.1.11	Microsoft Windows Server 2022 Datacenter Evaluation

1 Computer(s) found

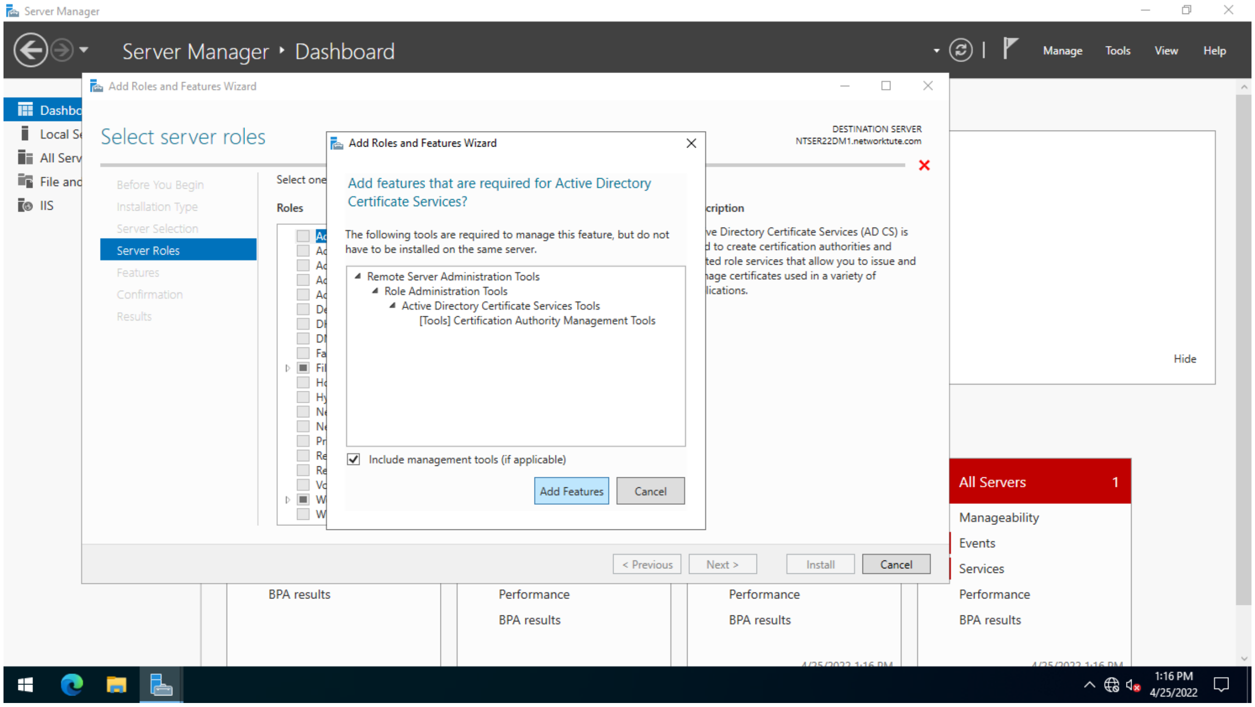
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

Step 5:

From the **Select server roles** page, click the **Active Directory Certificate Services** checkbox.

The Add Roles and Features Wizard displays, just as it did in the last assignment. For Active Directory Certificate services to work on this computer, further components are necessary.

Click **Add Features**.



Add features that are required for Active Directory Certificate Services?

The following tools are required to manage this feature, but do not have to be installed on the same server.

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

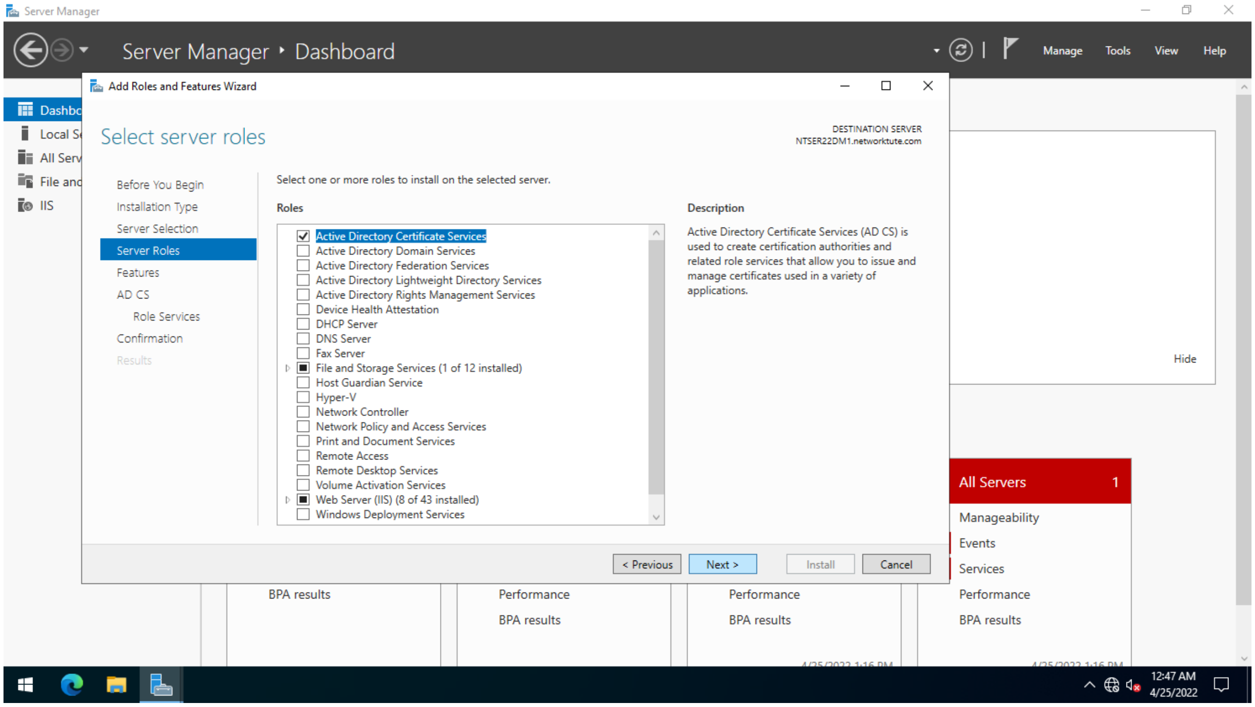
☑ Include management tools (if applicable)

DESTINATION SERVER
NTSER22DM1.networktute.com

Step 6:

You are back on the **Select server roles** page.

Click **Next**.



Select server roles

DESTINATION SERVER
NTSER22DM1.networktute.com

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

Roles

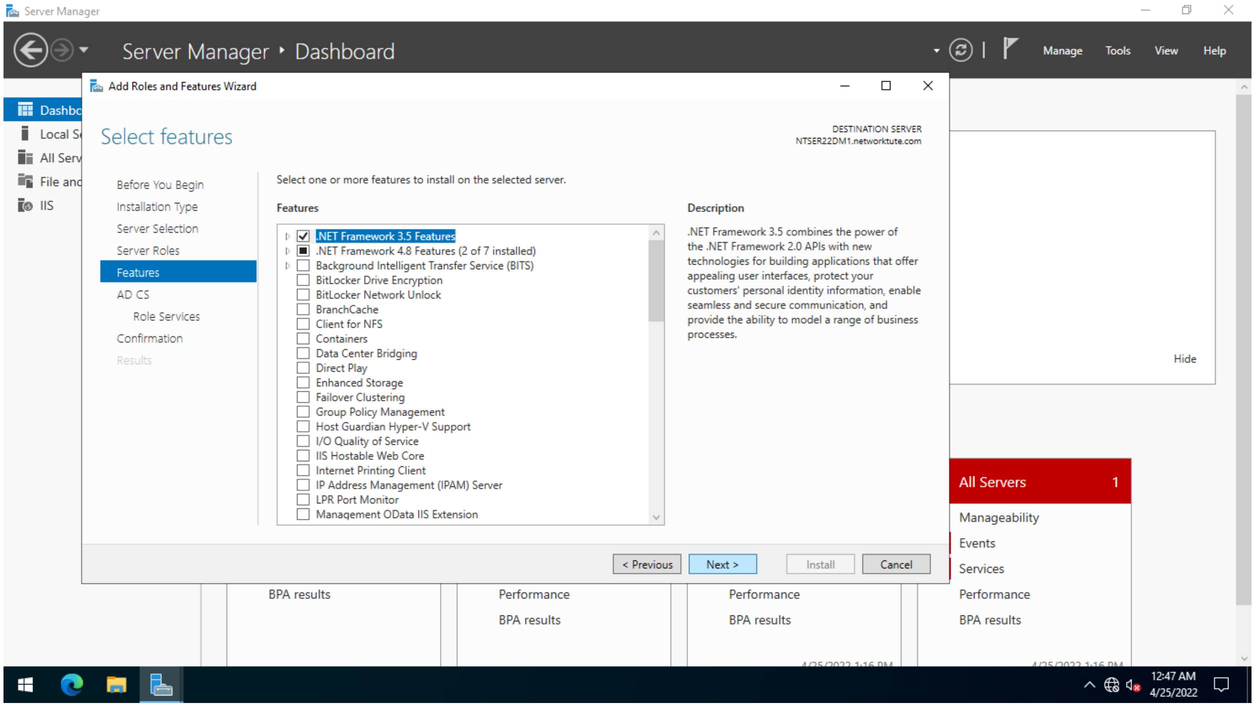
- ☑ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ Network Controller
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ■ Web Server (IIS) (8 of 43 installed)
- ☐ Windows Deployment 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.

Step 7:

In the **Select features** page, keep the default settings and click **Next**.



Select features

DESTINATION SERVER
NTSER22DM1.networktute.com

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

Features

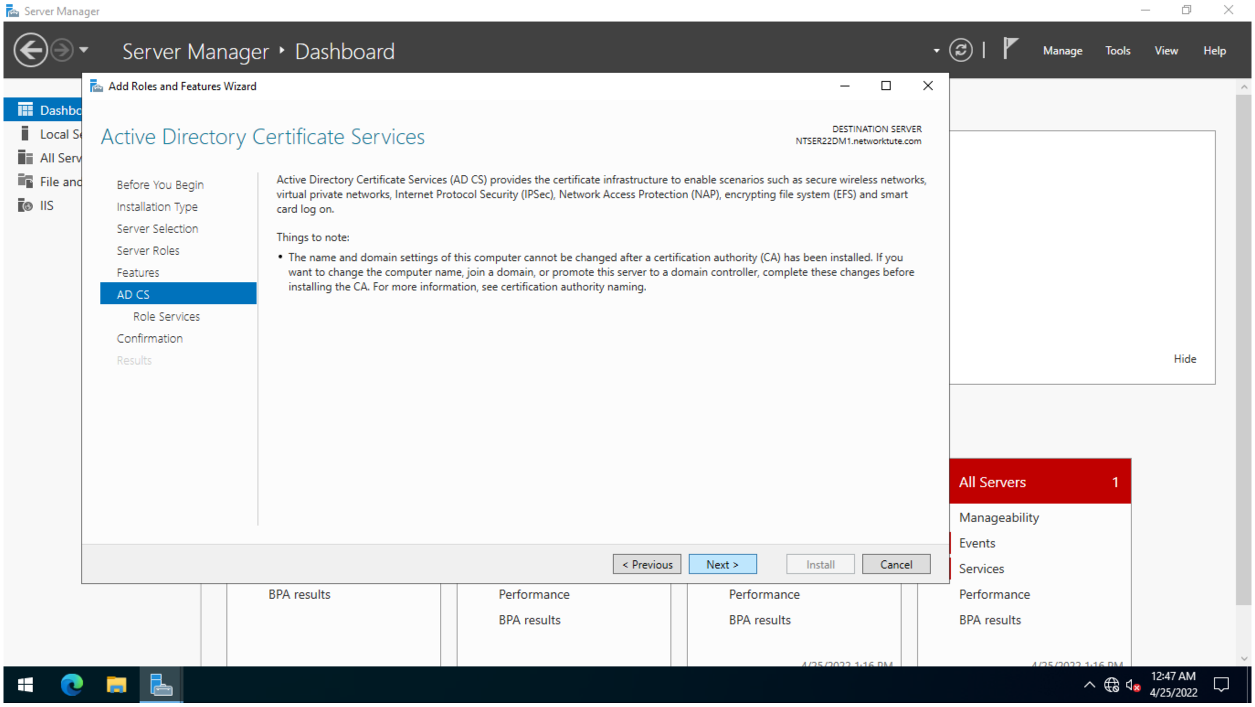
- ☑ .NET Framework 3.5 Features
- ■ .NET Framework 4.8 Features (2 of 7 installed)
- ☐ Background Intelligent Transfer Service (BITS)
- ☐ BitLocker Drive Encryption
- ☐ BitLocker Network Unlock
- ☐ BranchCache
- ☐ Client for NFS
- ☐ Containers
- ☐ Data Center Bridging
- ☐ Direct Play
- ☐ Enhanced Storage
- ☐ Failover Clustering
- ☐ Group Policy Management
- ☐ Host Guardian Hyper-V Support
- ☐ I/O Quality of Service
- ☐ IIS Hostable Web Core
- ☐ Internet Printing Client
- ☐ IP Address Management (IPAM) Server
- ☐ LPR Port Monitor
- ☐ Management OData IIS Extension

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.

Step 8:

On the **Active Directory Certificate Services**, click **Next**.



Active Directory Certificate Services

DESTINATION SERVER
NTSER22DM1.networktute.com

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:

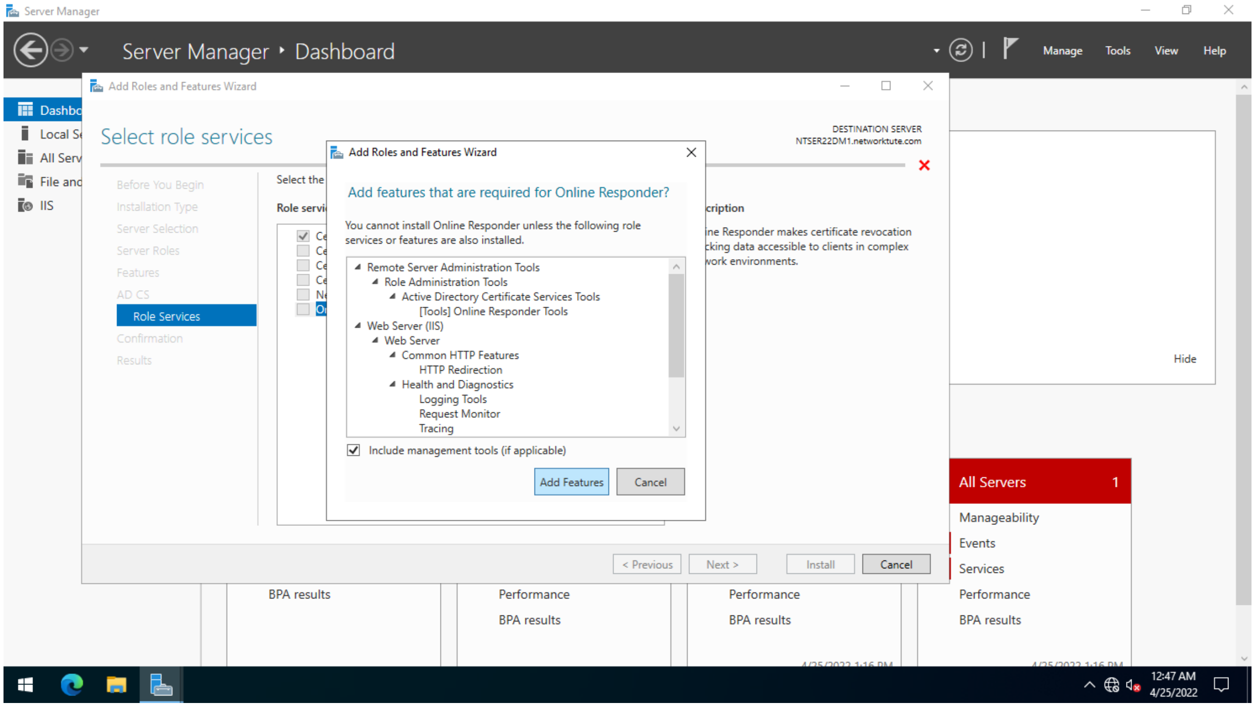
- The name and domain settings of this computer cannot be changed after a certification authority (CA) has been installed. If you want to change the computer name, join a domain, or promote this server to a domain controller, complete these changes before installing the CA. For more information, see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

Step 9:

In the **Select role services** page, select the **Online Responder** checkbox.

The **Add Roles and Features Wizard** is displayed.

Click **Add Features**.



Add Roles and Features Wizard

Add features that are required for Online Responder?

You cannot install Online Responder unless the following role services or features are also installed.

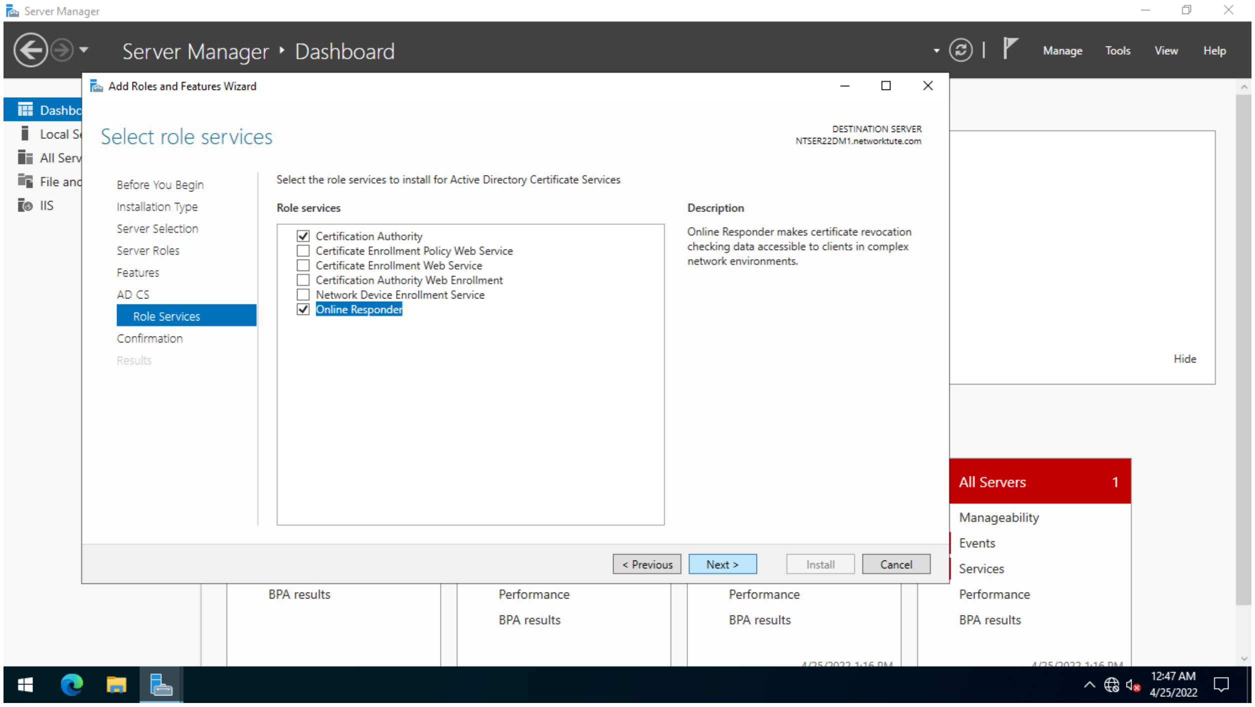
```
◢ Remote Server Administration Tools
   ◢ Role Administration Tools
      ◢ Active Directory Certificate Services Tools
            [Tools] Online Responder Tools
◢ Web Server (IIS)
   ◢ Web Server
      ◢ Common HTTP Features
            HTTP Redirection
      ◢ Health and Diagnostics
            Logging Tools
            Request Monitor
            Tracing
```

☑ Include management tools (if applicable)

Step 10:

You are back on the **Select role services** page.

When both the **Certification Authority** and **Online Responder** are selected, click **Next**



Select role services

DESTINATION SERVER
NTSER22DM1.networktute.com

Select the role services to install for Active Directory Certificate Services

Role services

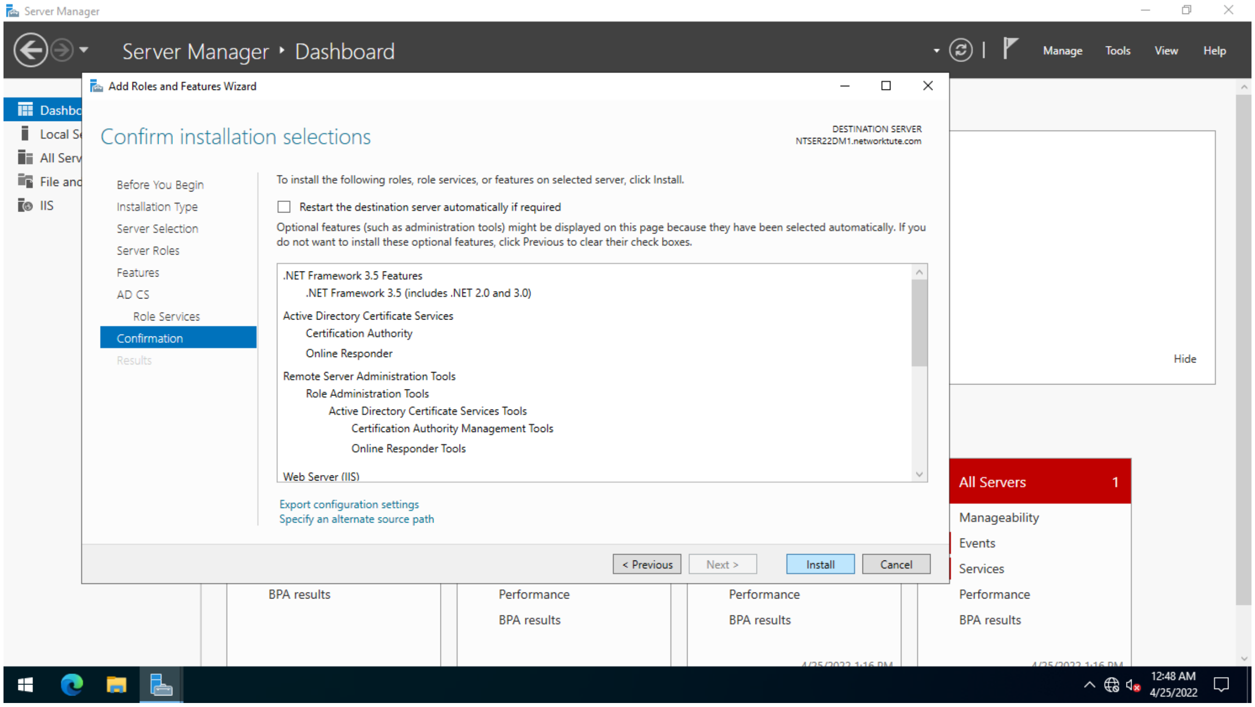
- ☑ Certification Authority
- ☐ Certificate Enrollment Policy Web Service
- ☐ Certificate Enrollment Web Service
- ☐ Certification Authority Web Enrollment
- ☐ Network Device Enrollment Service
- ☑ Online Responder

Description

Online Responder makes certificate revocation checking data accessible to clients in complex network environments.

Step 11:

In **Confirm installation selections**, click **Install**.



Confirm installation selections

DESTINATION SERVER
NTSER22DM1.networktute.com

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.

```
.NET Framework 3.5 Features
    .NET Framework 3.5 (includes .NET 2.0 and 3.0)
Active Directory Certificate Services
    Certification Authority
    Online Responder
Remote Server Administration Tools
    Role Administration Tools
        Active Directory Certificate Services Tools
            Certification Authority Management Tools
            Online Responder Tools
Web Server (IIS)
```

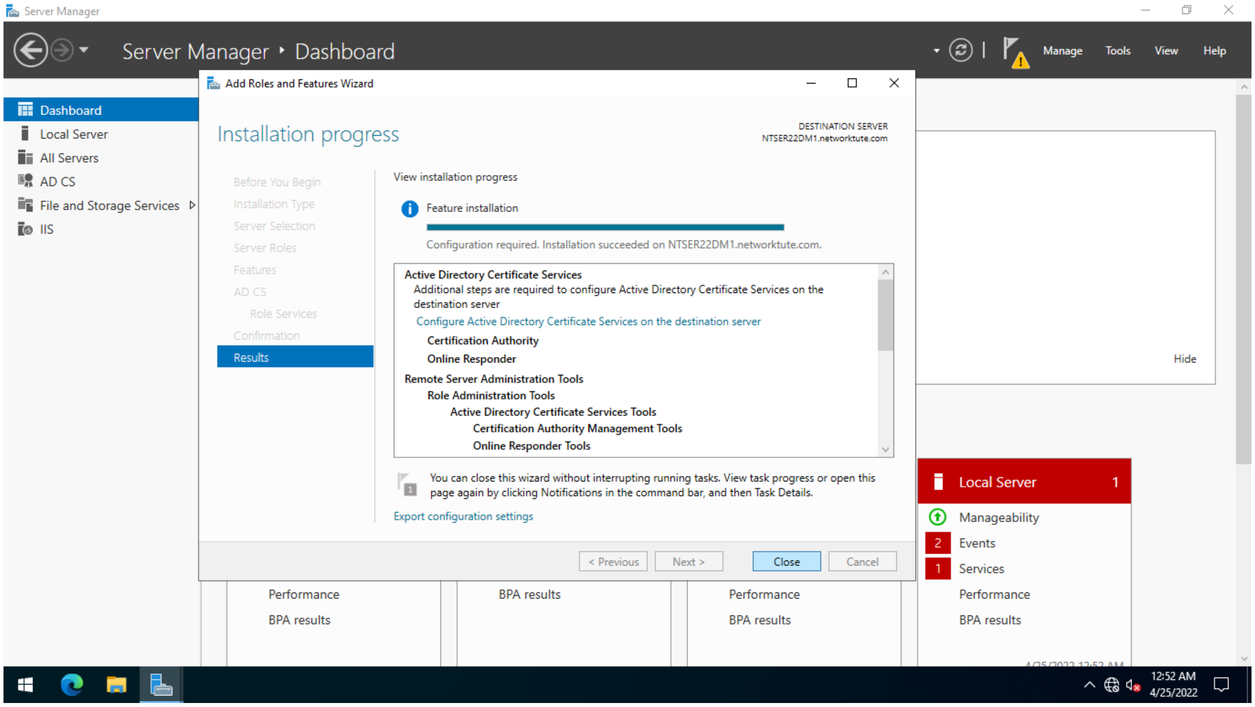
Export configuration settings
Specify an alternate source path

Step 12:

On the **Installation progress** page, wait while the services and its components are getting installed.

When **Installation progress** is completed, click **Close**.

Important: "The request to add or remove features on the specified failed," if you get an error message. Close the window. When the Server Manager is busy collecting system information about the server after a recent start-up or reboot, this error occurs. Wait around 1 minute before continuing with the Windows feature installation in this task. If the problem persists, restart the machine and reinstall the Windows features from the beginning.



Installation progress

DESTINATION SERVER
NTSER22DM1.networktute.com

View installation progress

Feature installation

Configuration required. Installation succeeded on NTSER22DM1.networktute.com.

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

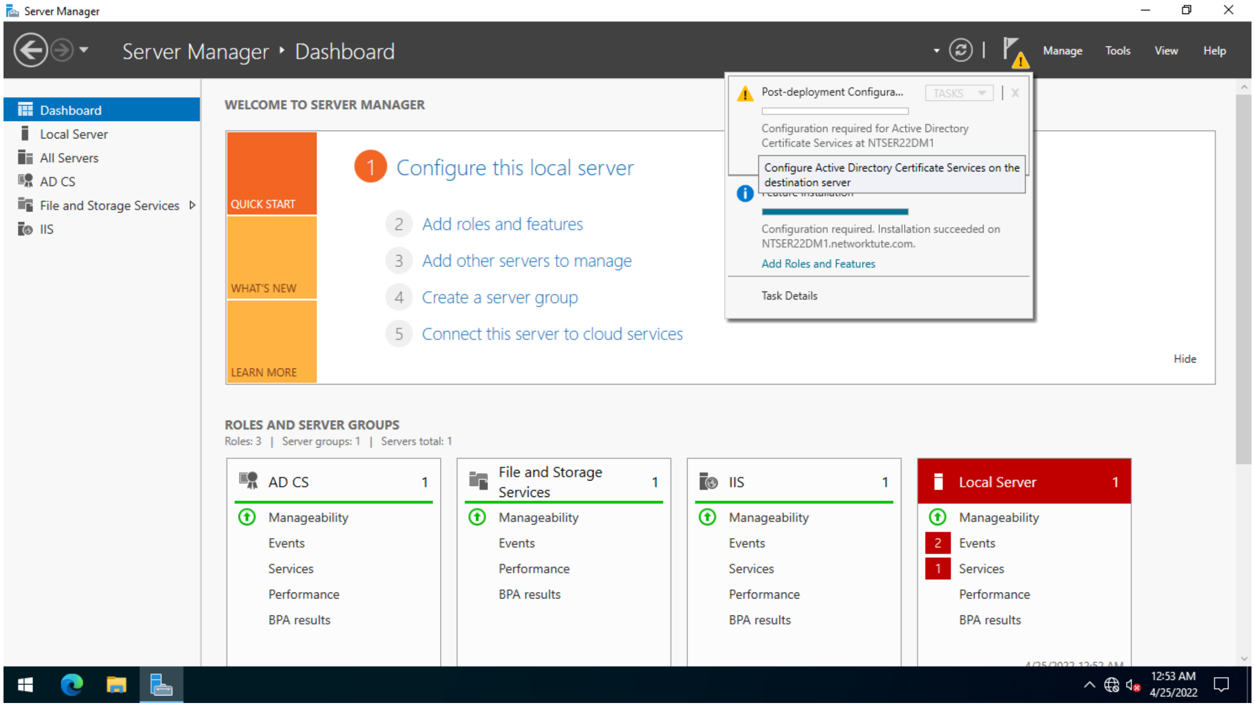
Task 4: Configure Subordinate CA

You must set up this Certificate service on **NTSER22DM1** to assume the role of a subordinate CA to **NTSER22VM1-NETWORKTUTE.COM-CA** after a brief installation of Active Directory Certificate Services and Online Responder.

Step 1:

On **NTSER22DM1**, you are back in the Server Manager window.

Select the flag icon with an exclamation point and click the **Configure Active Directory Certificate Services on the destination server** link.



Post-deployment Configura...

Configuration required for Active Directory Certificate Services at NTSER22DM1

Configure Active Directory Certificate Services on the destination server

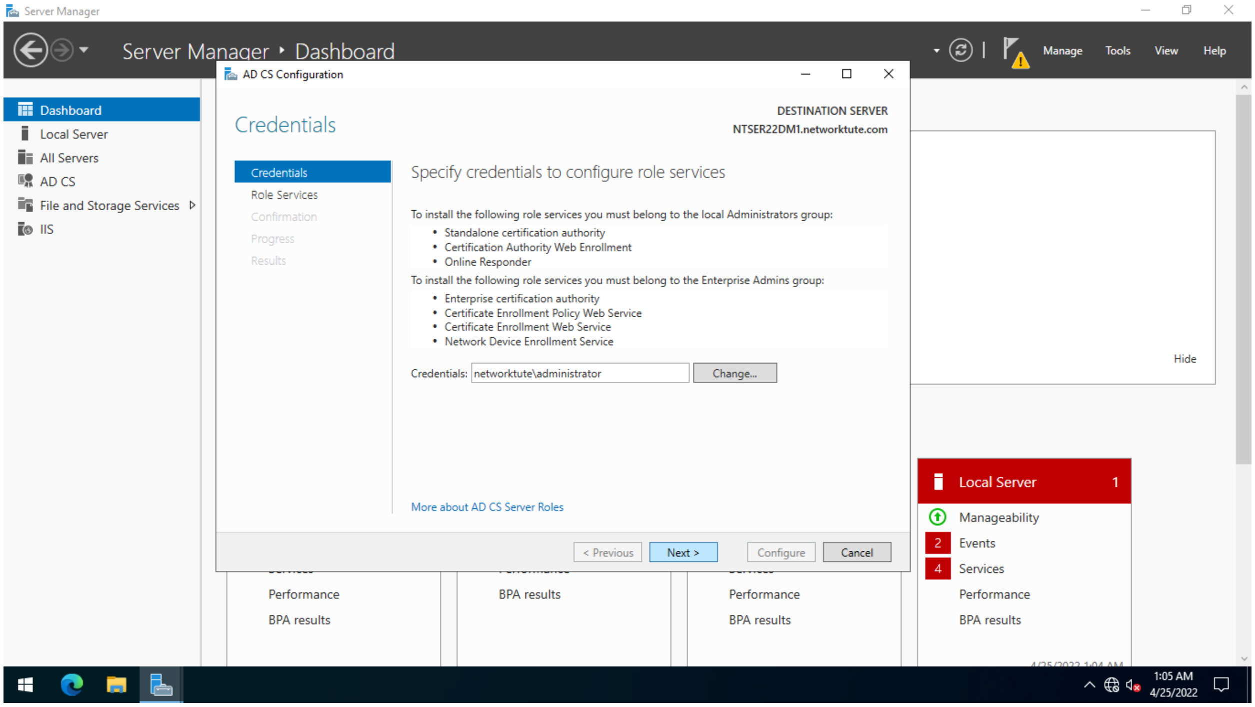
Configuration required. Installation succeeded on NTSER22DM1.networktute.com.

Add Roles and Features

Task Details

Step 2:

On the **Credentials** page of the **AD CS Configuration** wizard, keep the default settings and click **Next**.



Credentials

DESTINATION SERVER
NTSER22DM1.networktute.com

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

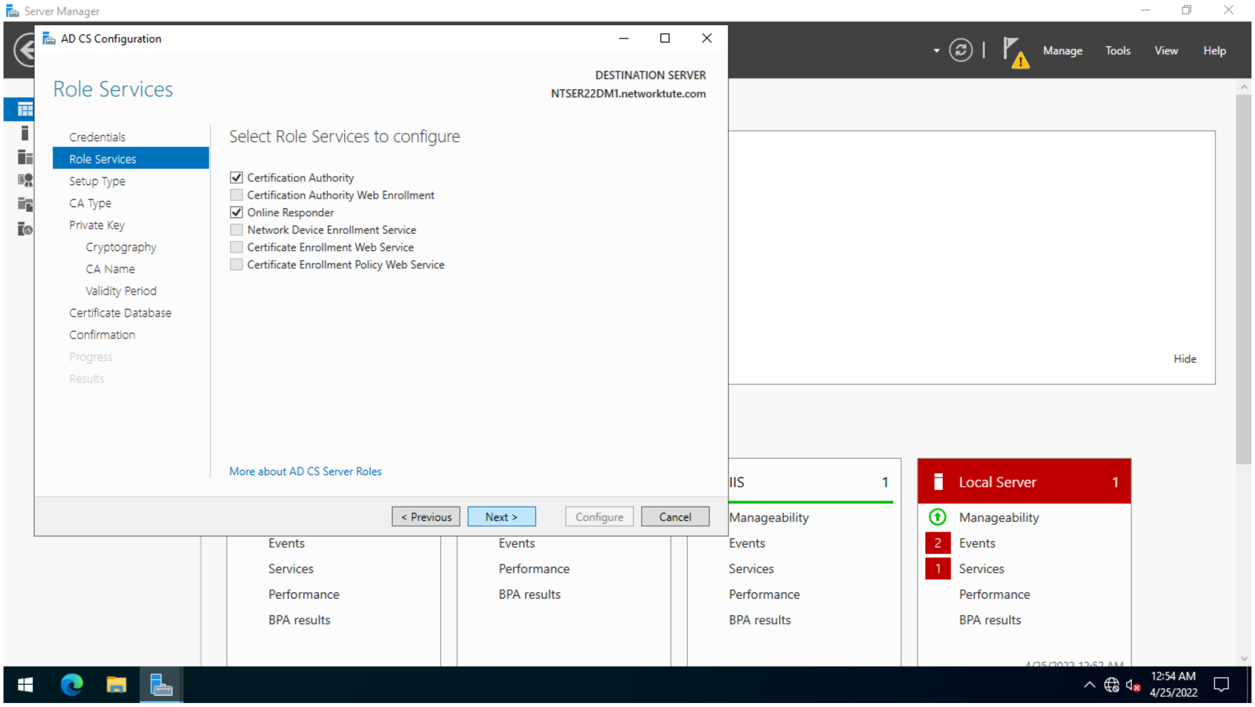
Credentials: networktute\administrator [Change...]

More about AD CS Server Roles

Step 3:

Similar to the task done earlier about configuring the **Enterprise Root CA**, select the **Certification Authority** and **Online Responder** checkboxes.

Then, click **Next**.



Role Services

DESTINATION SERVER
NTSER22DM1.networktute.com

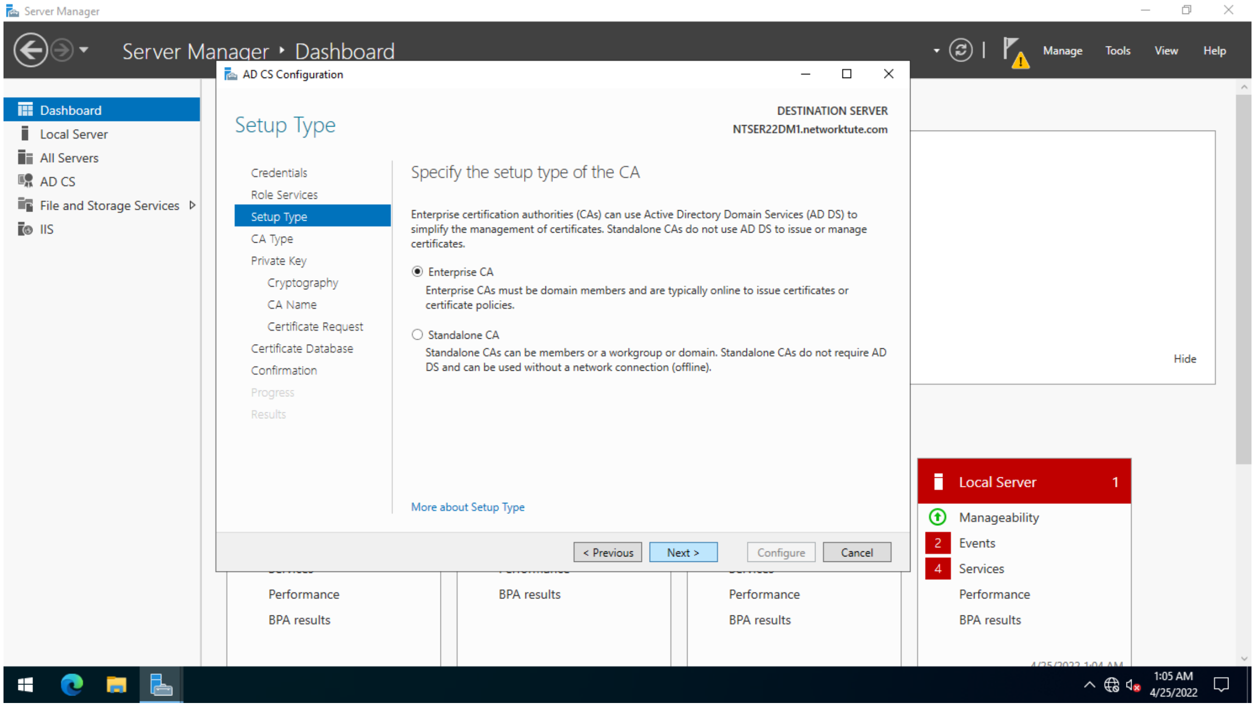
Select Role Services to configure

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

Step 4:

In the **Setup Type** page, verify that the **Enterprise CA** radio button is selected.

Click **Next** to accept default settings.



Setup Type

DESTINATION SERVER
NTSER22DM1.networktute.com

Specify the setup type of the CA

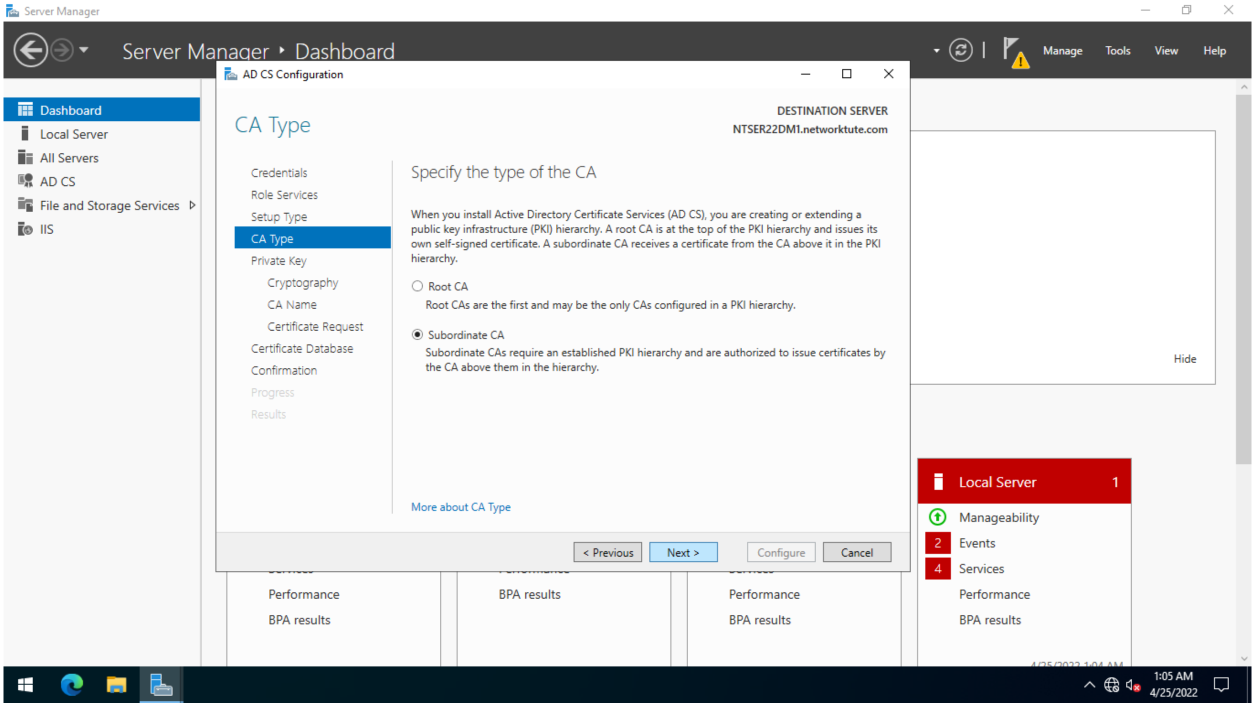
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

● 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).

Step 5:

From **CA Type**, ensure that the **Subordinate CA** option is selected and click **Next**.



CA Type

DESTINATION SERVER
NTSER22DM1.networktute.com

Specify the type of the CA

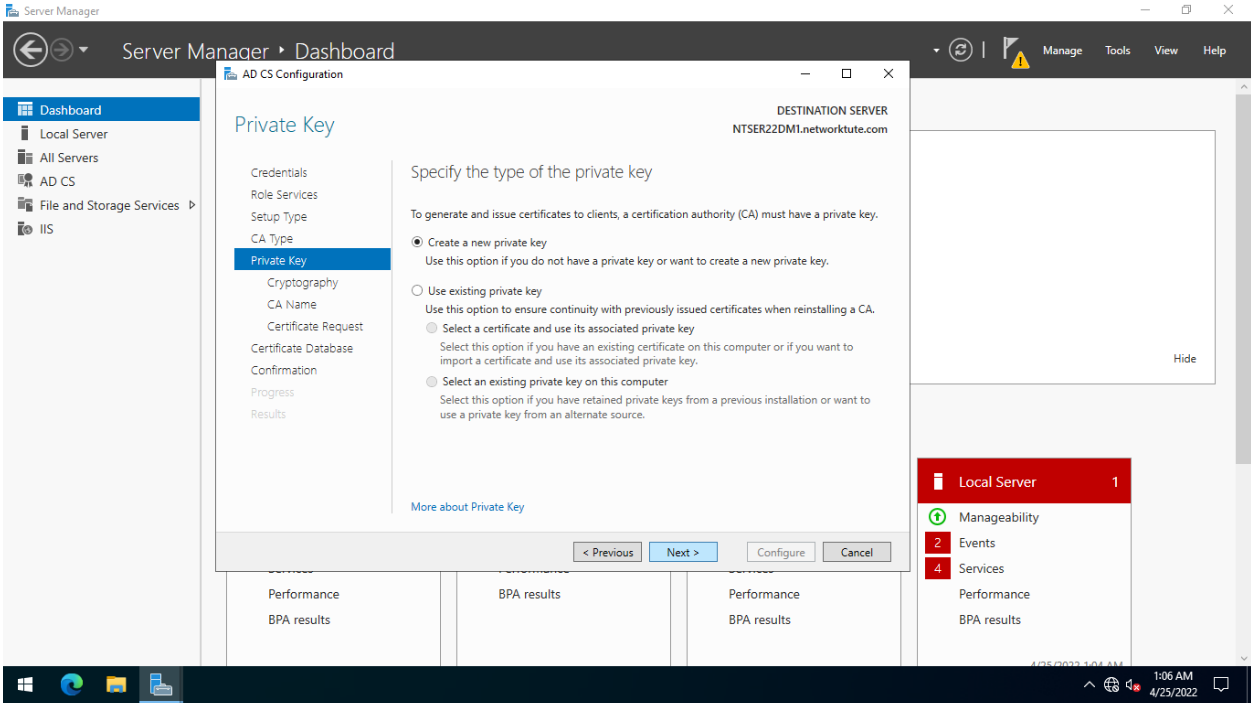
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

○ 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.

Step 6:

On the **Private Key** page, keep the default setting, **create a new private key** and click **Next**



Private Key

DESTINATION SERVER
NTSER22DM1.networktute.com

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.

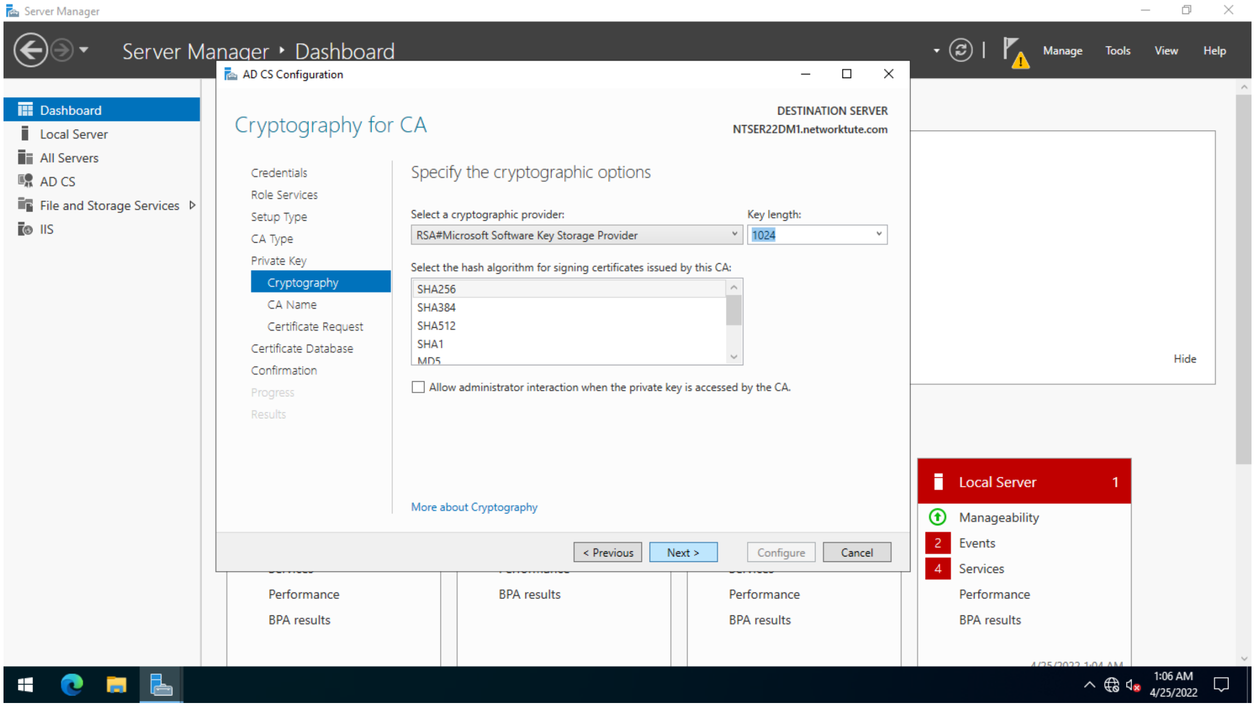
○ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

○ 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

Step 7:

On the **Cryptography for CA** page, change the **Key length to 1024**, and then click **Next**.



Cryptography for CA

DESTINATION SERVER
NTSER22DM1.networktute.com

Specify the cryptographic options

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

Key length: 1024

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

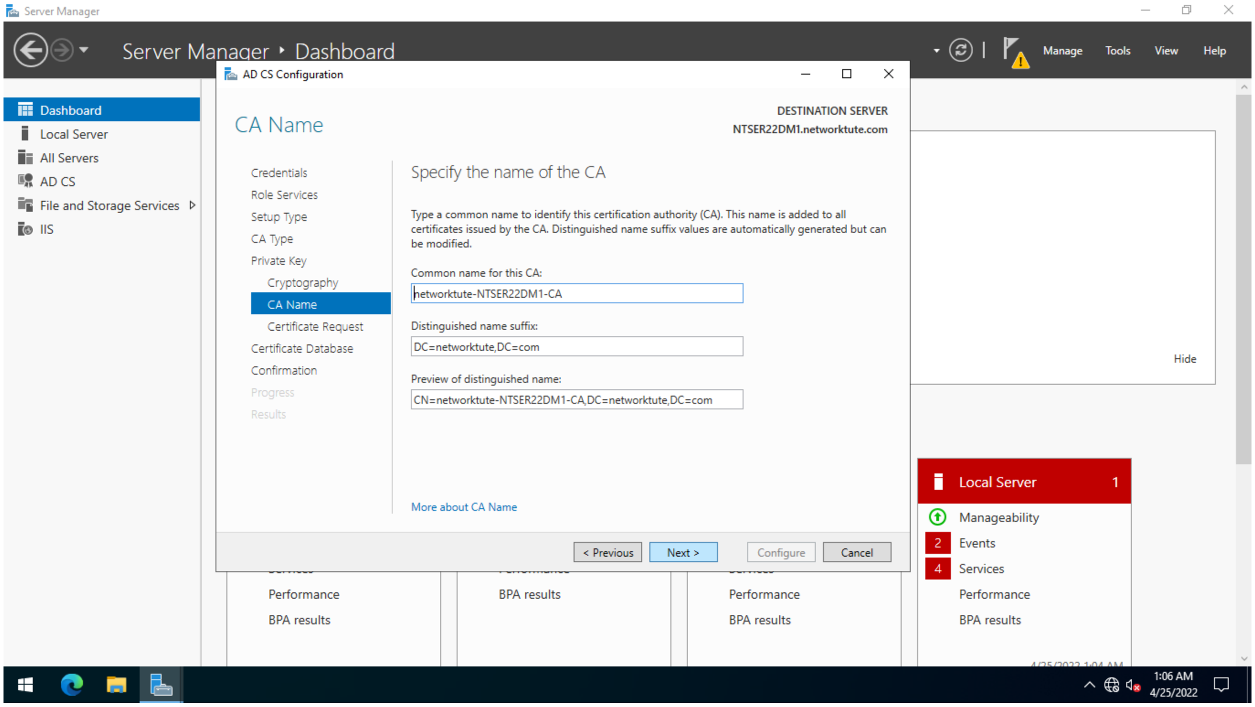
SHA256
SHA384
SHA512
SHA1
MD5

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

More about Cryptography

Step 8:

On the **CA Name** page, accept the name automatically assigned by Windows, click **Next** to continue



CA Name

DESTINATION SERVER
NTSER22DM1.networktute.com

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: networktute-NTSER22DM1-CA

Distinguished name suffix: DC=networktute,DC=com

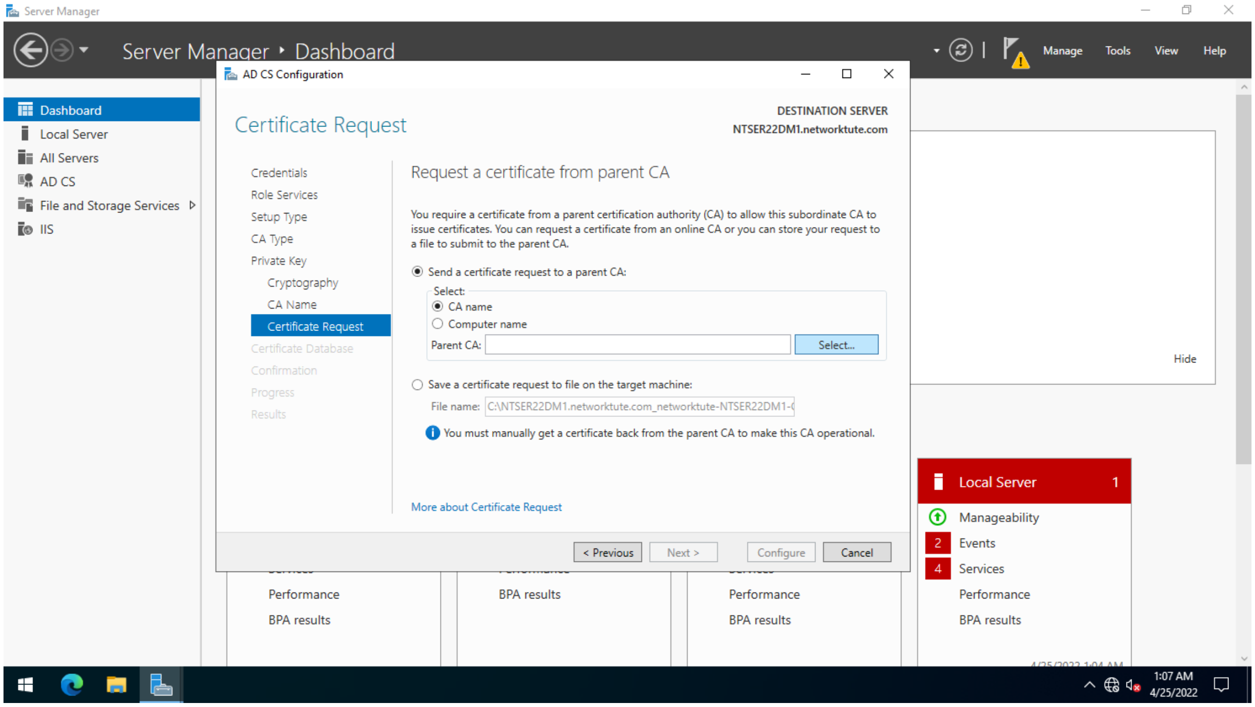
Preview of distinguished name: CN=networktute-NTSER22DM1-CA,DC=networktute,DC=com

Step 9:

On the **Certificate Request** page, select the following radio buttons:

- Send a certificate request to a parent CA
- CA Name

Click the **Select**… button next to the **Parent CA** text field.



Certificate Request

DESTINATION SERVER
NTSER22DM1.networktute.com

Request a certificate from parent CA

You require a certificate from a parent certification authority (CA) to allow this subordinate CA to issue certificates. You can request a certificate from an online CA or you can store your request to a file to submit to the parent CA.

● Send a certificate request to a parent CA:

Select:
● CA name
○ Computer name

Parent CA: [Select...]

○ Save a certificate request to file on the target machine:

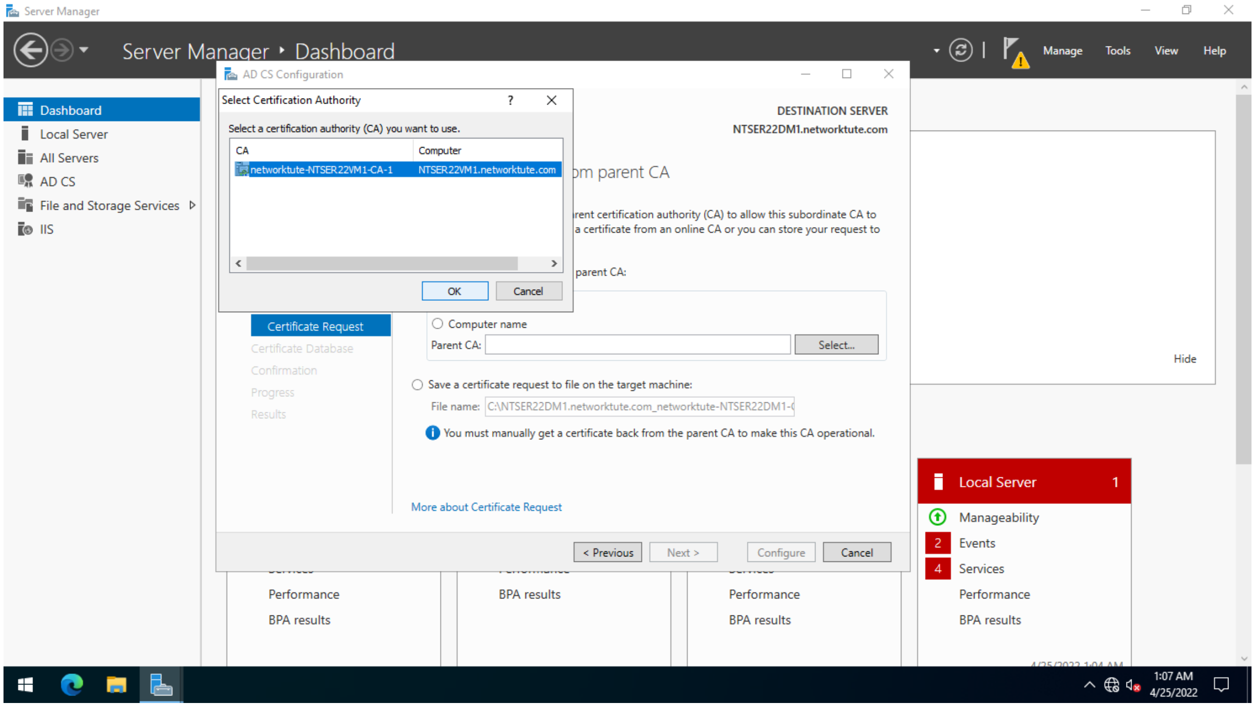
File name: C:\NTSER22DM1.networktute.com_networktute-NTSER22DM1-(

You must manually get a certificate back from the parent CA to make this CA operational.

Step 10:

The **Select Certification Authority** dialog box displays the detected **CA** in the network called **networktute-NTSER22VM1-CA** automatically.

Keep the default selection and click **OK.**



Select Certification Authority

Select a certification authority (CA) you want to use.

CA	Computer
networktute-NTSER22VM1-CA-1	NTSER22VM1.networktute.com

OK Cancel

DESTINATION SERVER
NTSER22DM1.networktute.com

...om parent CA

...rent certification authority (CA) to allow this subordinate CA to ... a certificate from an online CA or you can store your request to

... parent CA:

○ Computer name

Parent CA: Select...

○ Save a certificate request to file on the target machine:

File name: C:\NTSER22DM1.networktute.com_networktute-NTSER22DM1-(

You must manually get a certificate back from the parent CA to make this CA operational.

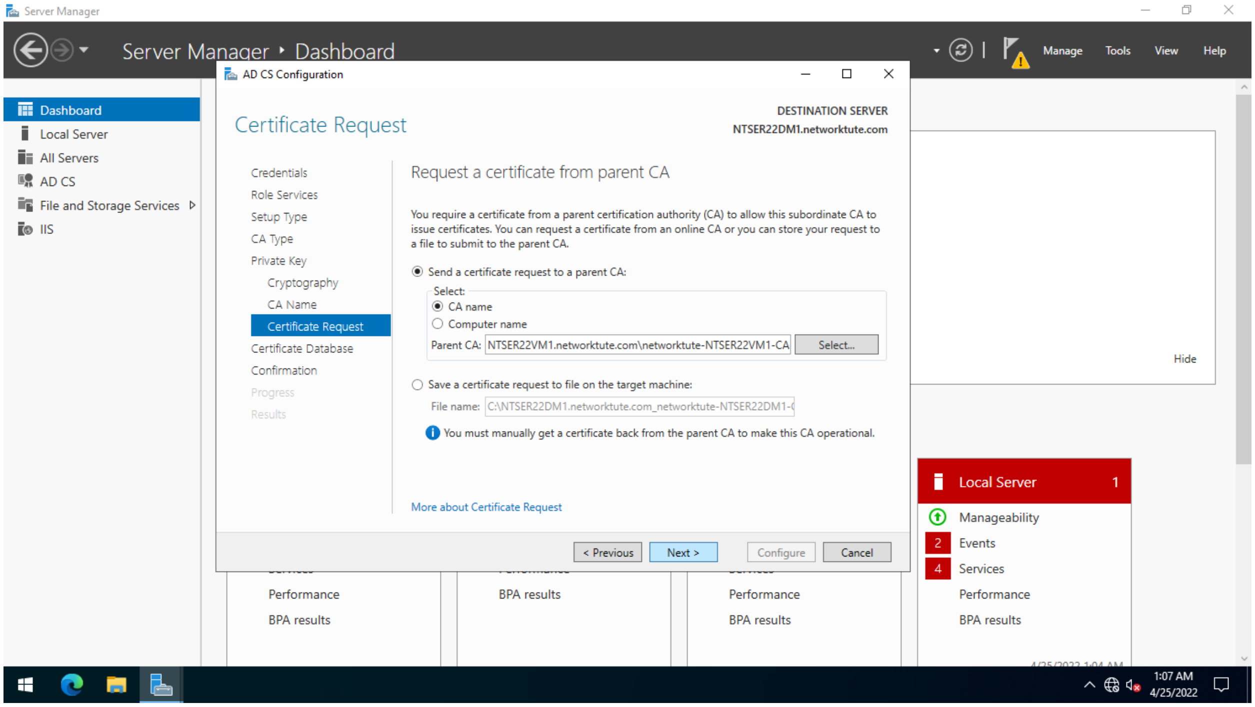
More about Certificate Request

< Previous Next > Configure Cancel

Step 11:

You are redirected back to the **Certificate Request** page.

It is now filled in with the correct information. Click **Next**.



AD CS Configuration

Certificate Request

DESTINATION SERVER
NTSER22DM1.networktute.com

Request a certificate from parent CA

You require a certificate from a parent certification authority (CA) to allow this subordinate CA to issue certificates. You can request a certificate from an online CA or you can store your request to a file to submit to the parent CA.

● Send a certificate request to a parent CA:

Select:

● CA name

○ Computer name

Parent CA: NTSER22VM1.networktute.com\networktute-NTSER22VM1-CA Select...

○ Save a certificate request to file on the target machine:

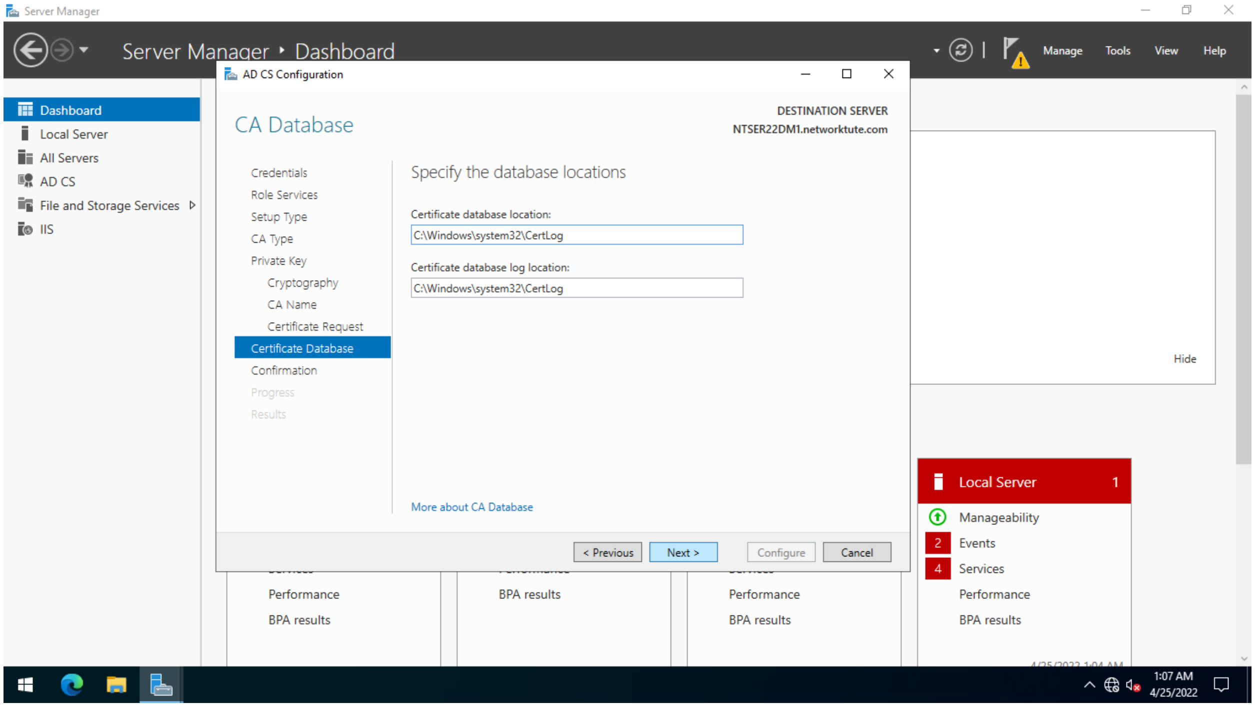
File name: C:\NTSER22DM1.networktute.com_networktute-NTSER22DM1-(

You must manually get a certificate back from the parent CA to make this CA operational.

More about Certificate Request

Step 12:

On the **CA Database** page, keep the default settings and click **Next**.



AD CS Configuration

CA Database

DESTINATION SERVER
NTSER22DM1.networktute.com

Specify the database locations

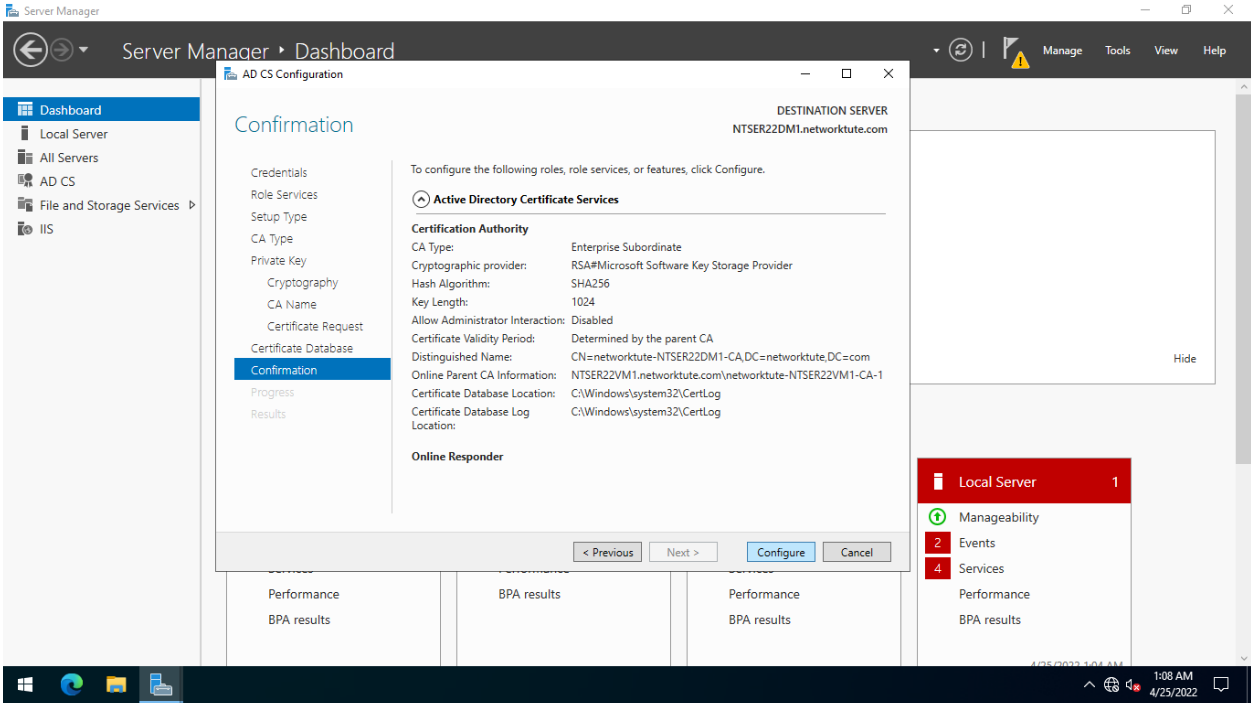
Certificate database location:
C:\Windows\system32\CertLog

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

More about CA Database

Step 13:

On the **Confirmation** page, click **Configure** to proceed.



Confirmation

DESTINATION SERVER
NTSER22DM1.networktute.com

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

Active Directory Certificate Services

Certification Authority

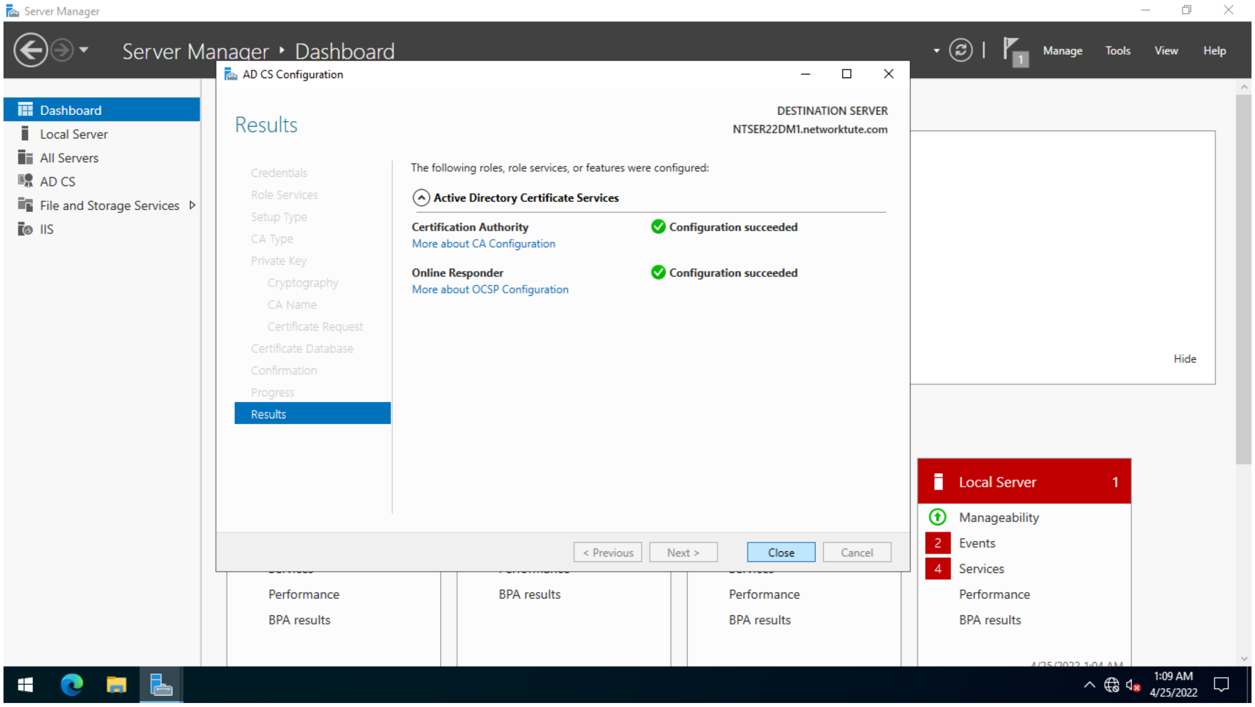
CA Type:	Enterprise Subordinate
Cryptographic provider:	RSA#Microsoft Software Key Storage Provider
Hash Algorithm:	SHA256
Key Length:	1024
Allow Administrator Interaction:	Disabled
Certificate Validity Period:	Determined by the parent CA
Distinguished Name:	CN=networktute-NTSER22DM1-CA,DC=networktute,DC=com
Online Parent CA Information:	NTSER22VM1.networktute.com\networktute-NTSER22VM1-CA-1
Certificate Database Location:	C:\Windows\system32\CertLog
Certificate Database Log Location:	C:\Windows\system32\CertLog

Online Responder

Step 14:

It will take a while for the subordinate CA to be configured on **NTSER22DM1**.

Server Manager will then report that **Certification Authority** and **Online Responder** are successfully configured. Click **Close** to close the **AD CS Configuration** wizard.



Results

DESTINATION SERVER
NTSER22DM1.networktute.com

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

Active Directory Certificate Services

Certification Authority ✓ Configuration succeeded
More about CA Configuration

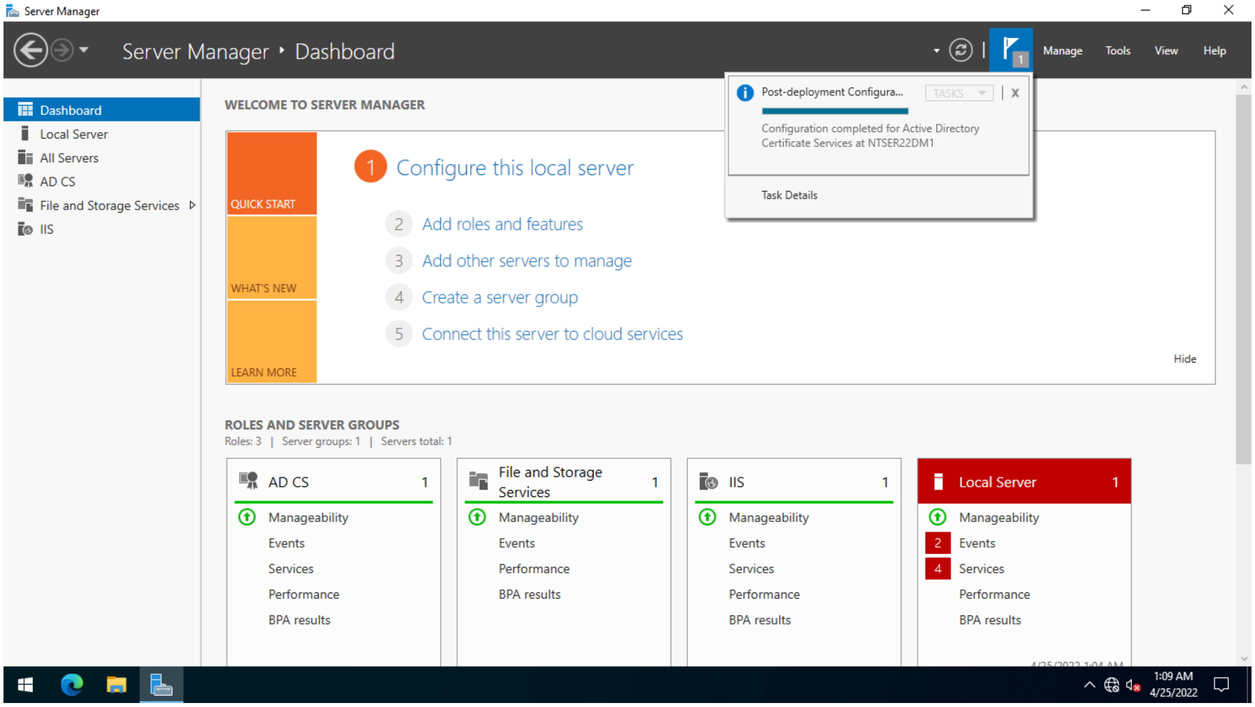
Online Responder ✓ Configuration succeeded
More about OCSP Configuration

Step 15:

You are redirected back to the **Server Manager** console.

Tip - Click on the refresh dashboard button to refresh the display.

Now you can confirm that there are no errors in this CA configuration on this server.



Post-deployment Configura...

Configuration completed for Active Directory Certificate Services at NTSER22DM1