SECURITY+ V4 LAB SERIES

Lab 21: PKI Management with Windows

Document Version: 2022-04-29

Material in this Lab Aligns to the Following	
CompTIA Security+ (SY0-601) Exam Objectives	3.9: Given a scenario, implement public key infrastructure
All-In-One CompTIA Security+ Sixth Edition ISBN-13: 978-1260464009 Chapters	25: Public Key Infrastructure

Contents

Introduction

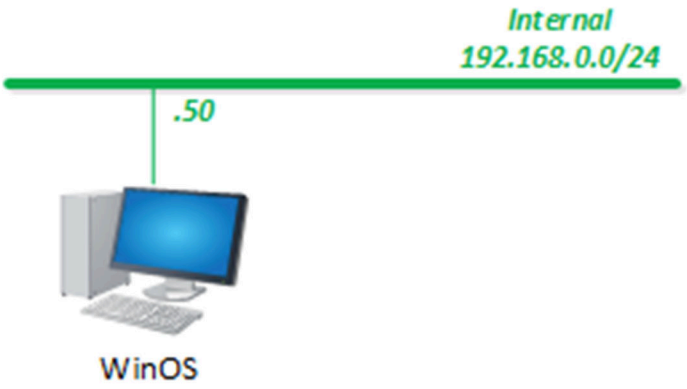
In this lab, you will add the Active Directory Certificate Services role to a Windows server. You will then customize and configure the Windows server as a Certificate Authority (CA).

Objective

In this lab, you will perform the following tasks:

- implement public key infrastructure

Lab Topology



Lab Settings

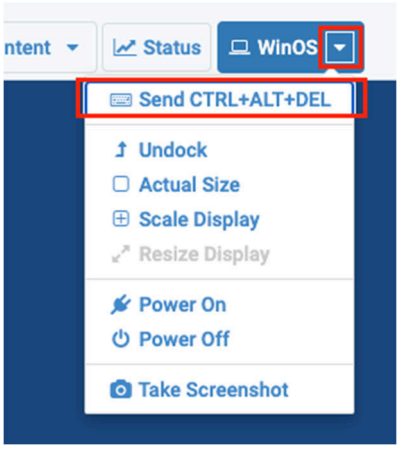
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
WinOS	`192.168.0.50`	`Administrator`	`NDGlabpass123!`

1 Add the Active Directory Certificate Services Role

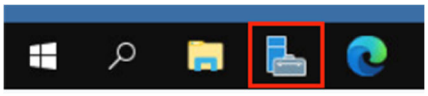
In this task, you will add the *Active Directory Certificate Services* role to the *Windows* server.

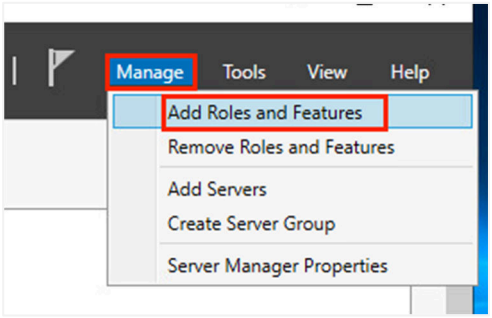
1. Launch the **WinOS** virtual machine to access the graphical login screen. While on the splash screen, focus on the *NETLAB+* tabs. Click the dropdown menu for the **WinOS** tab and click on **Send CTRL+ALT+DEL**.



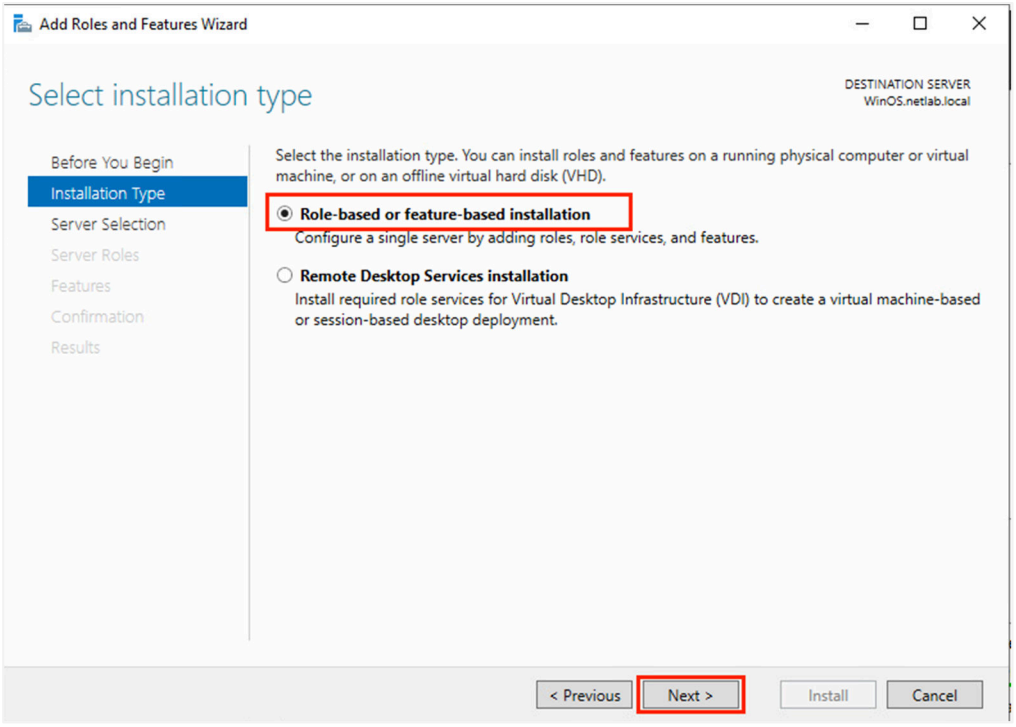
2. Log in as `Administrator` using the password `NDGlabpass123!`.

3. Once logged in, click the **Server Manager** icon to launch it. In the *Server Manager* window, click on **Manage** in the top-right corner and select **Add Roles and Features**.

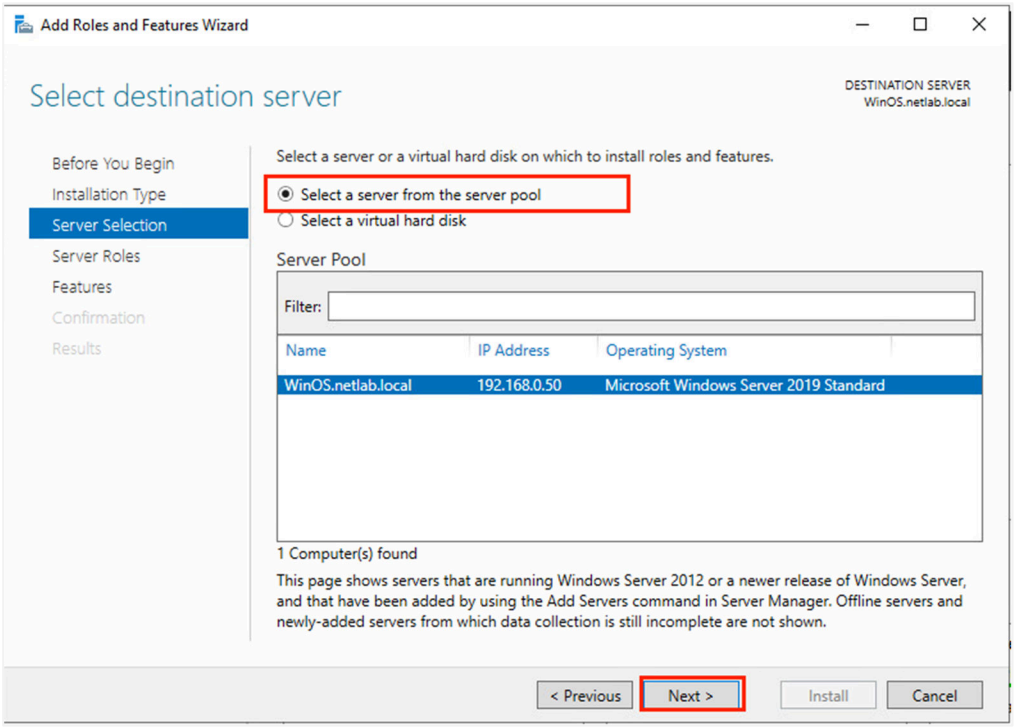




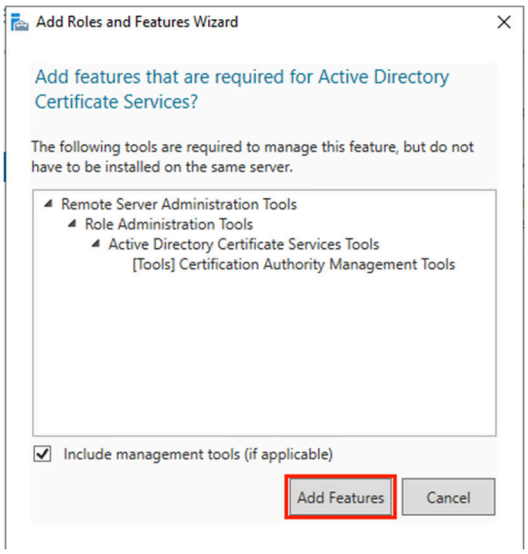
4. Notice the *Add Roles and Features Wizard* appears. On the *Installation Type* step, keep the default setting of **Role-based or feature-based Installation** and click **Next.**



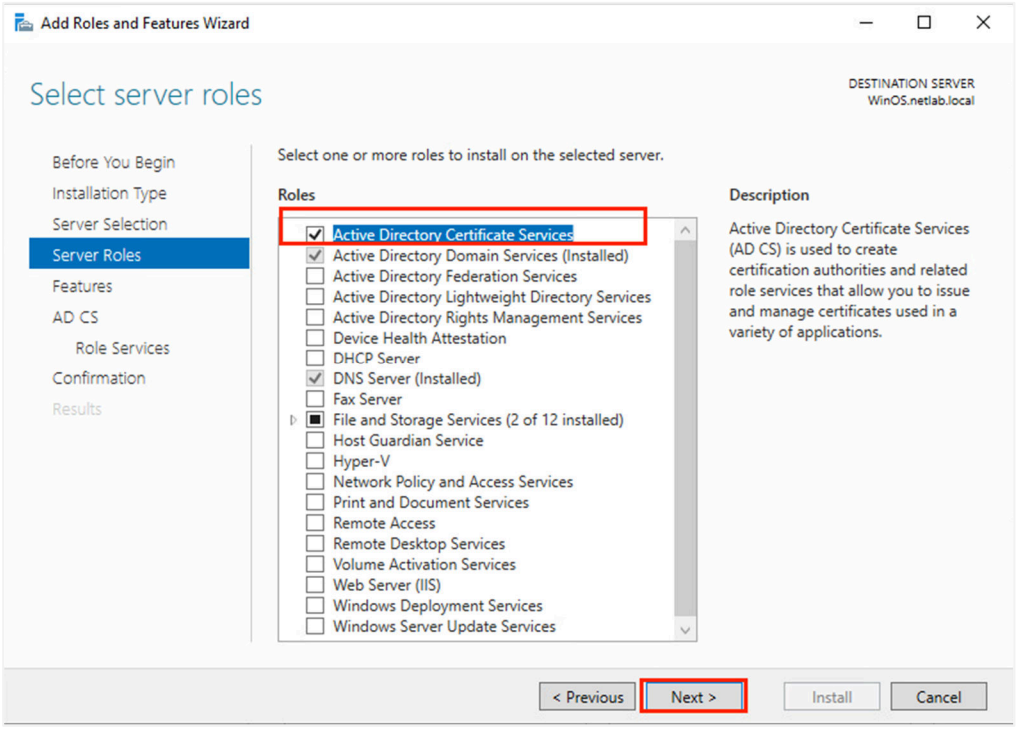
5. On the *Server Selection* step, select the **WinOS.netlab.local** server from the pool and click **Next.**



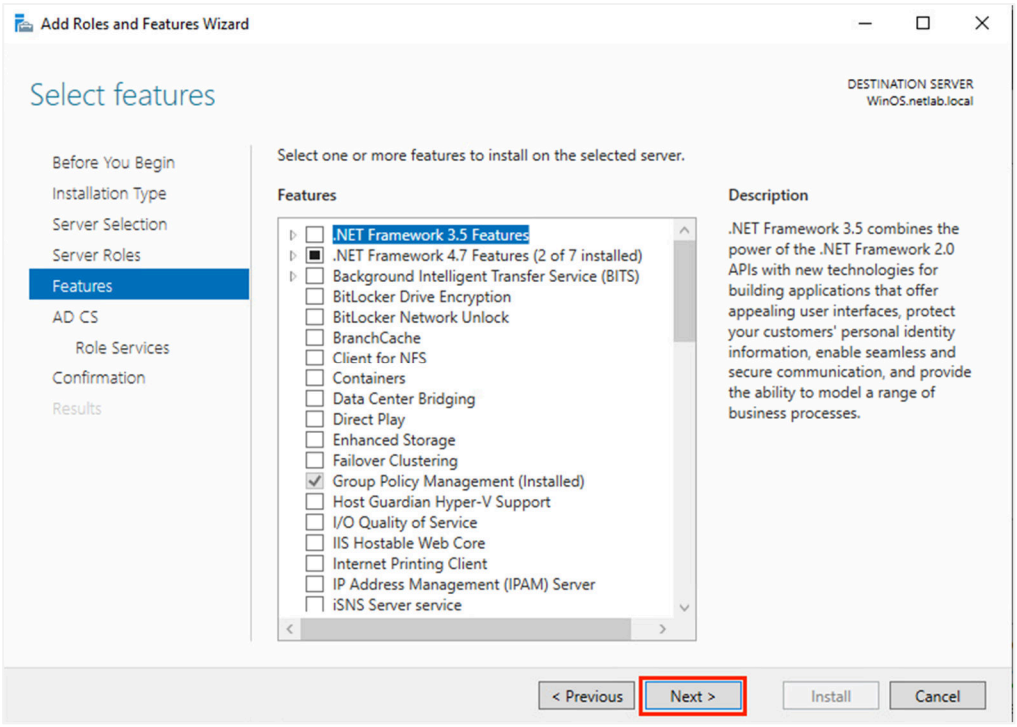
6. On the *Server Roles* step, check the checkbox for **Active Directory Certificate Services** and notice a pop-up window appears. Click the **Add Features** button.



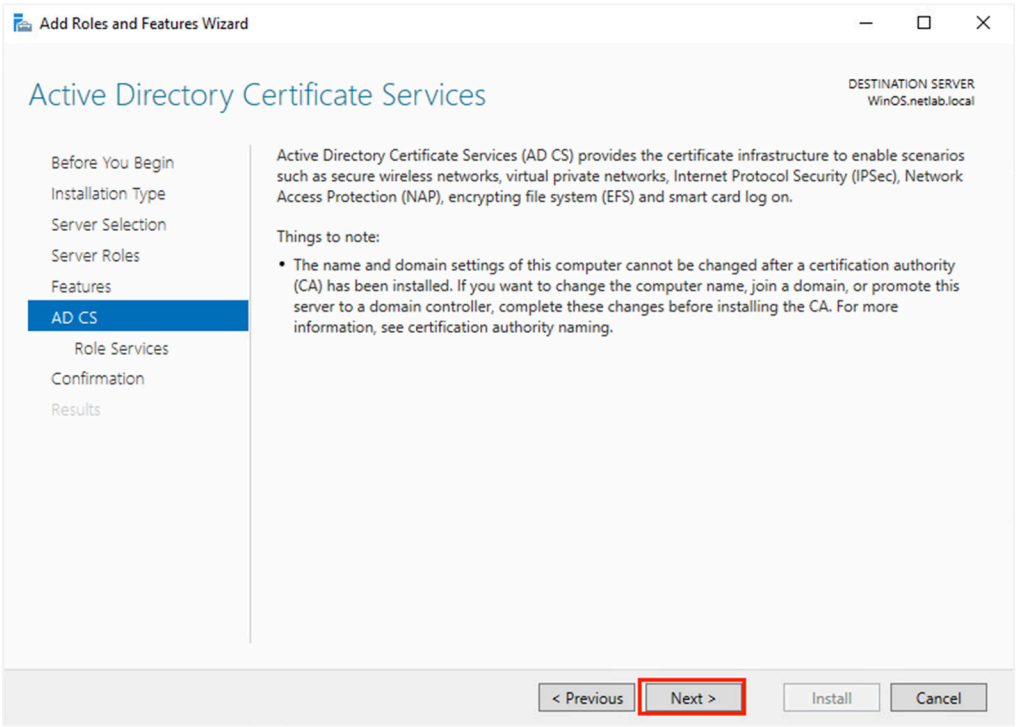
7. Back on the main wizard window, ensure that **Active Directory Certificate Services** is checked and click **Next.**



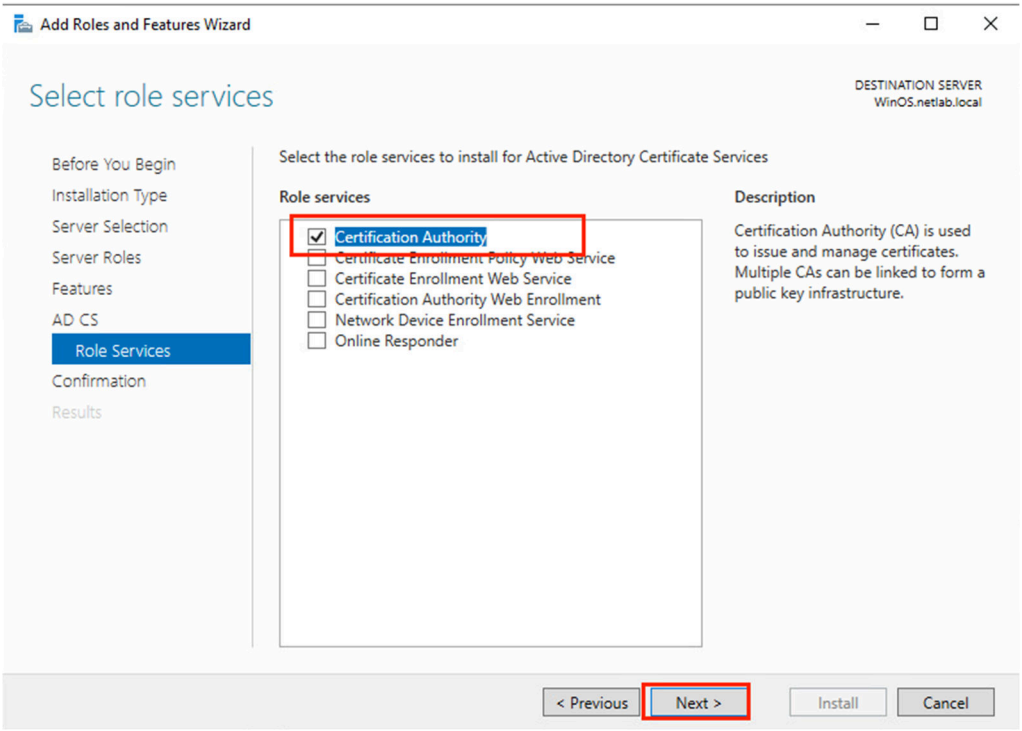
8. On the *Features* step, leave the defaults and click **Next.**



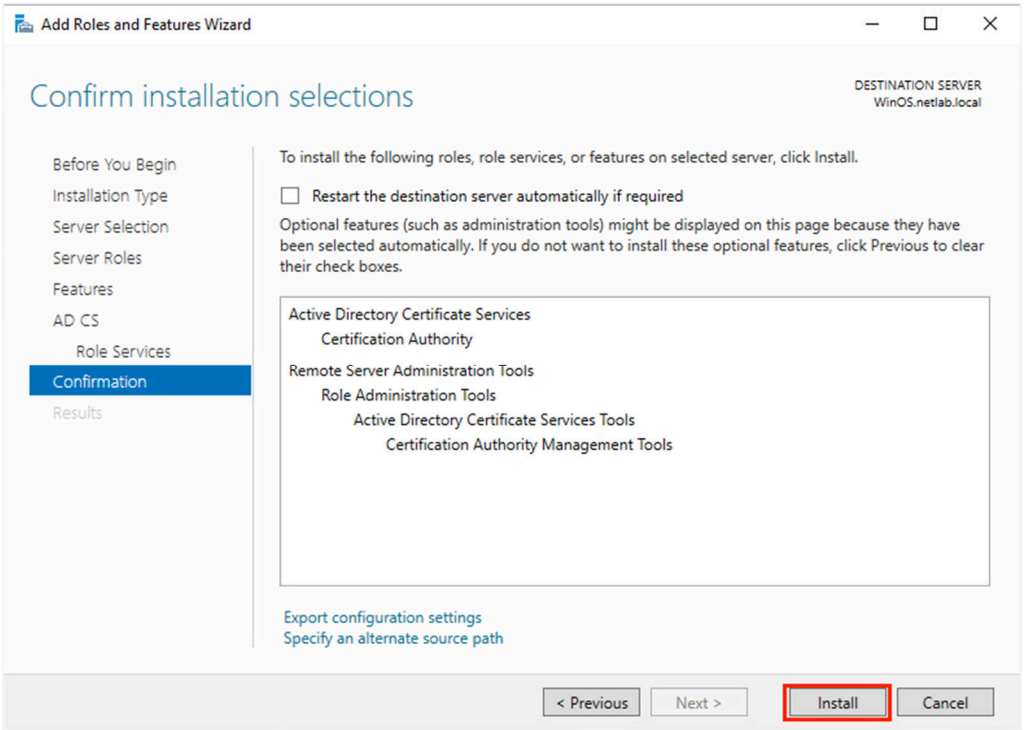
9. On the *AD CS* step, review the information and click **Next.**



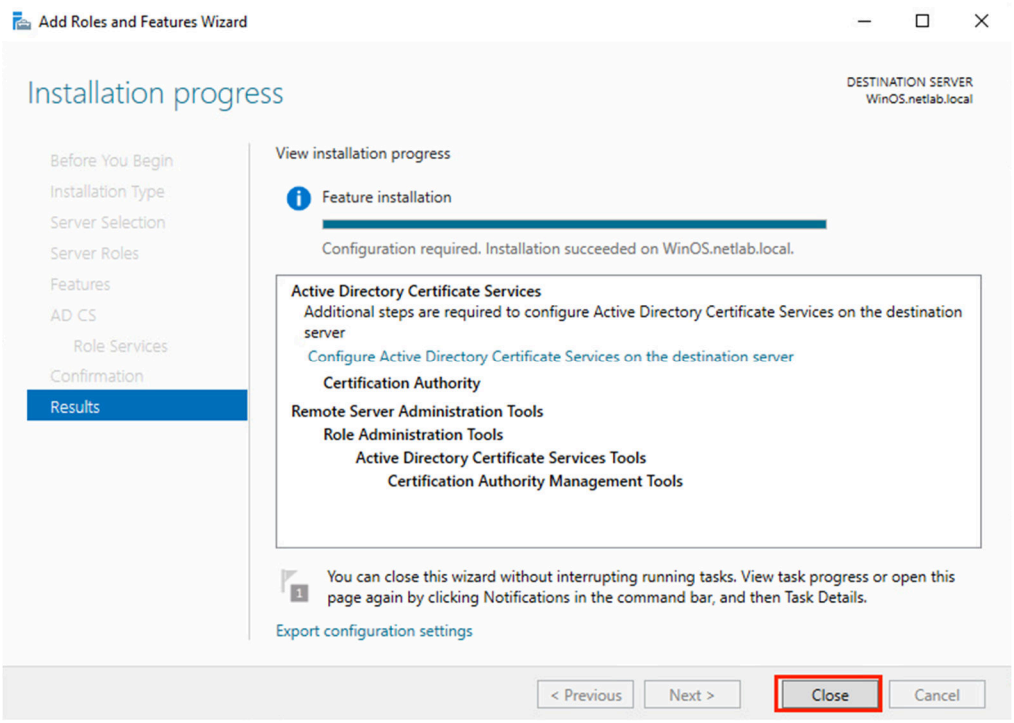
10. On the *Role Services* step, ensure that **Certification Authority** is checked and click **Next.**



11. On the *Confirmation* step, click **Install** to finish the installation of the *AD CS Server.*



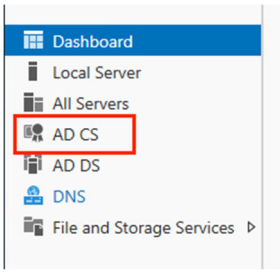
12. The installation will take about two minutes. After the install is complete, click **Close.**



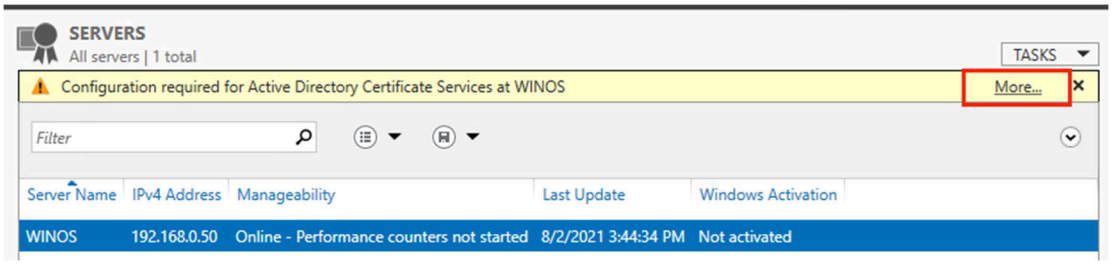
13. Leave the *WinOS* window open to continue with the next task.

2 Configure and Customize the Certificate Authority

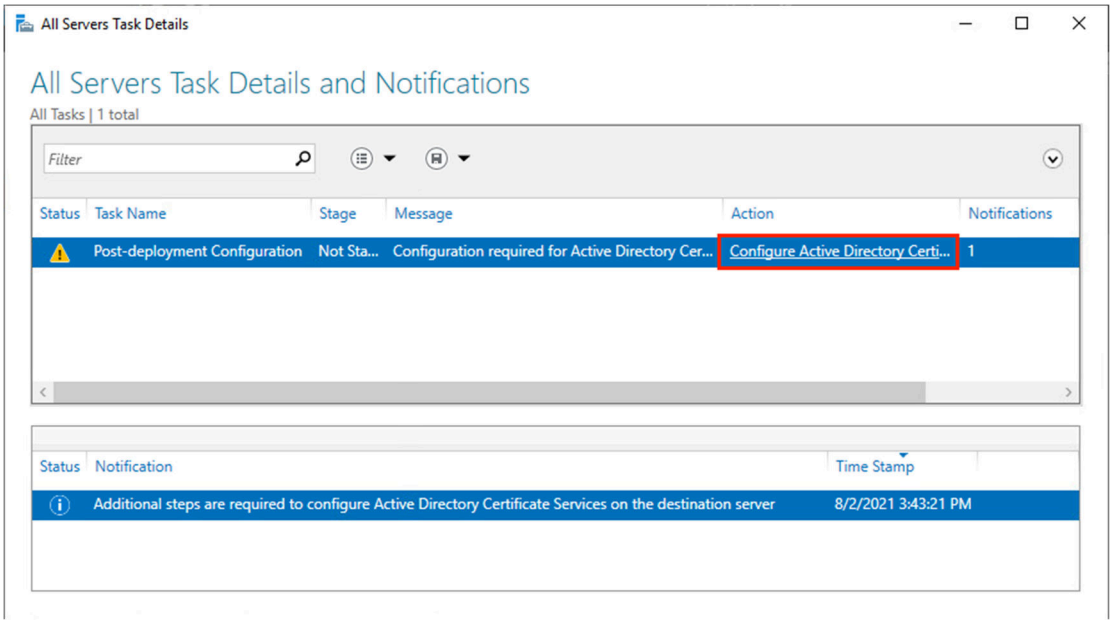
1. On the *Server Manager* window, in the left pane, click on **AD CS.**



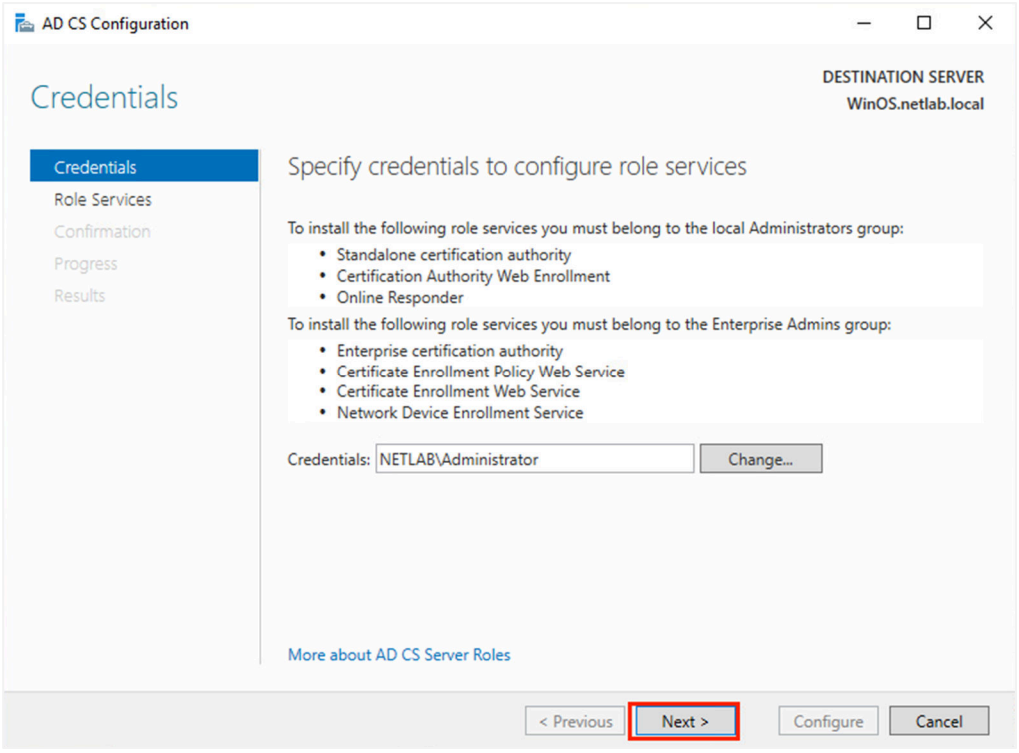
2. Notice the *Configuration required* message in yellow background. Click on the **More** link to launch the configuration wizard.



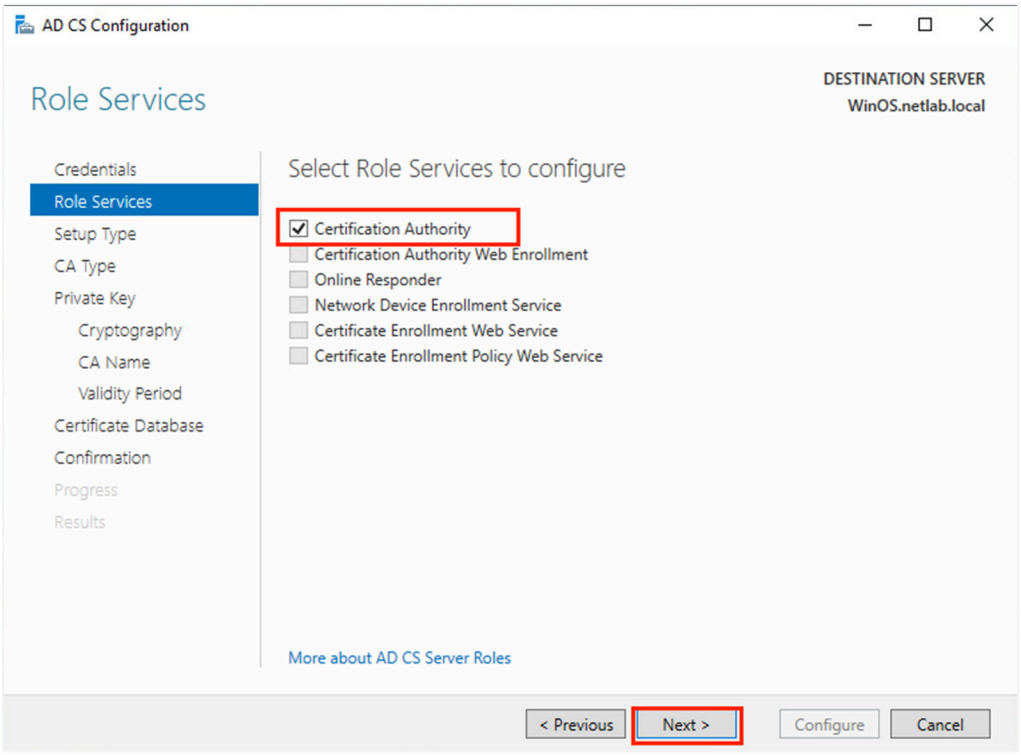
3. On the *All Servers Task Details* window, click on the **Configure Active Directory Certificate Services on the destination server** link.



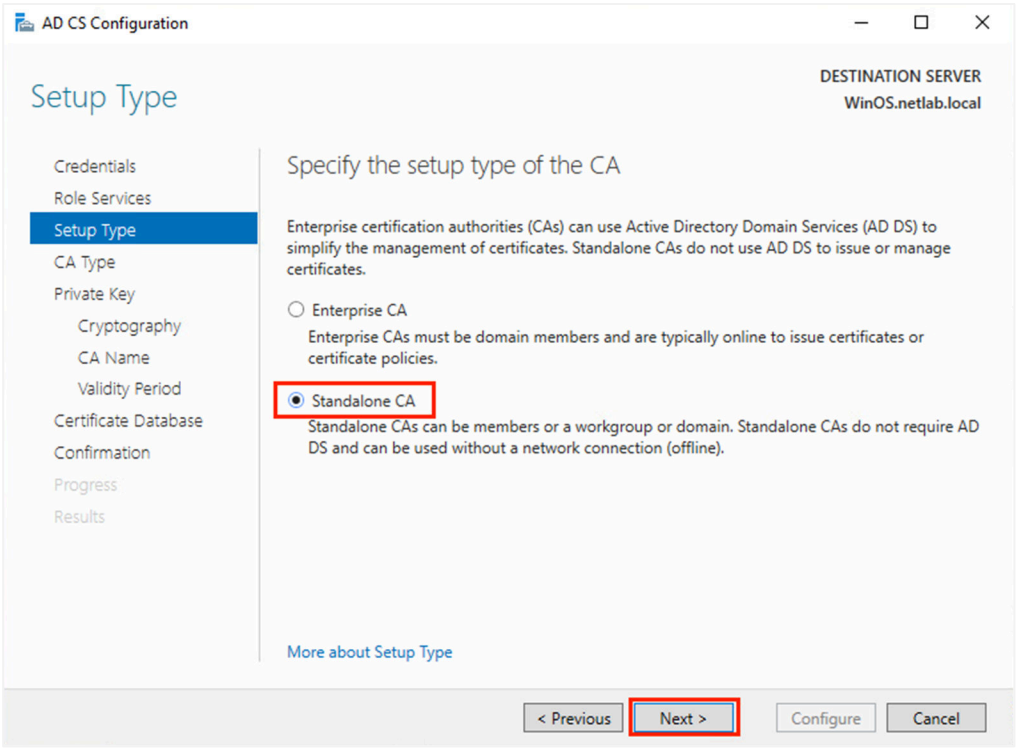
4. Notice the *AD CS Configuration* window appears. Review the information presented, leave the default credentials, and click **Next**.



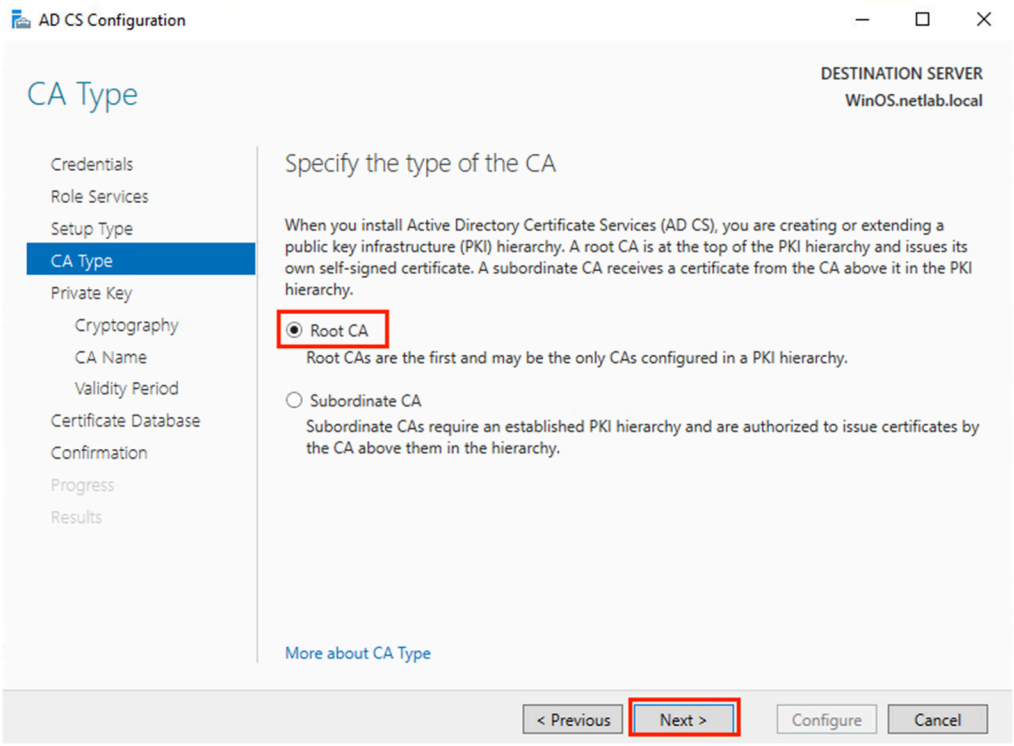
5. On the *Role Services* step, check the checkbox for **Certification Authority** and click **Next**.



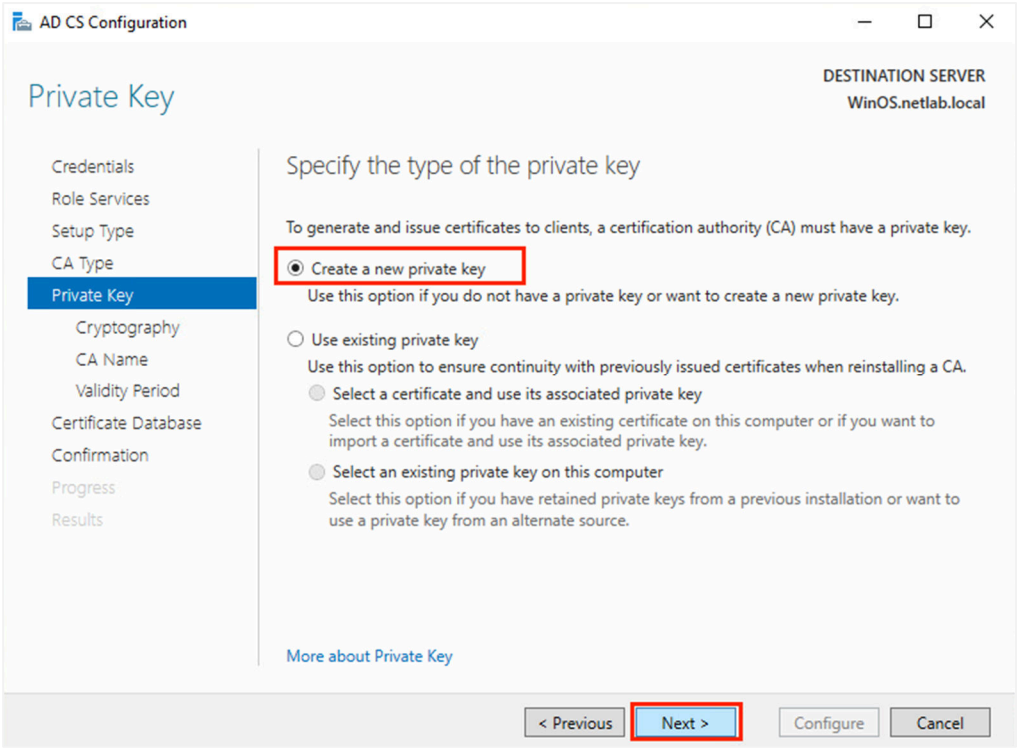
6. On the *Setup Type* step, select the radio button for **Standalone CA** and click **Next.**



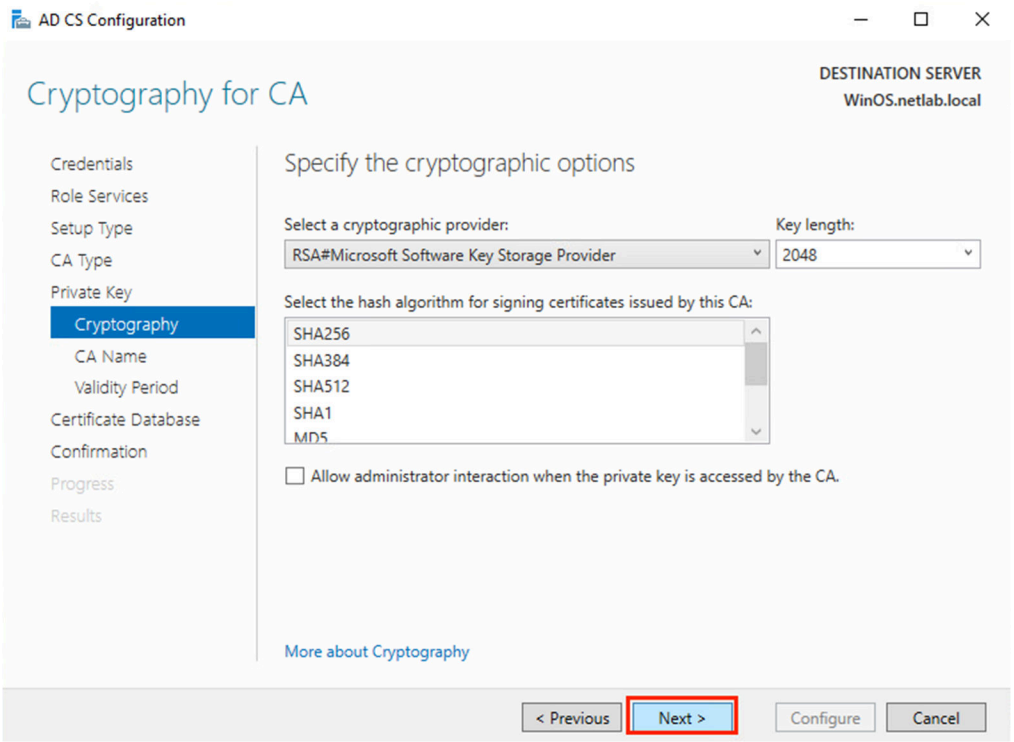
7. On the *CA Type* step, ensure that the radio button for **Root CA** is selected and click **Next.**



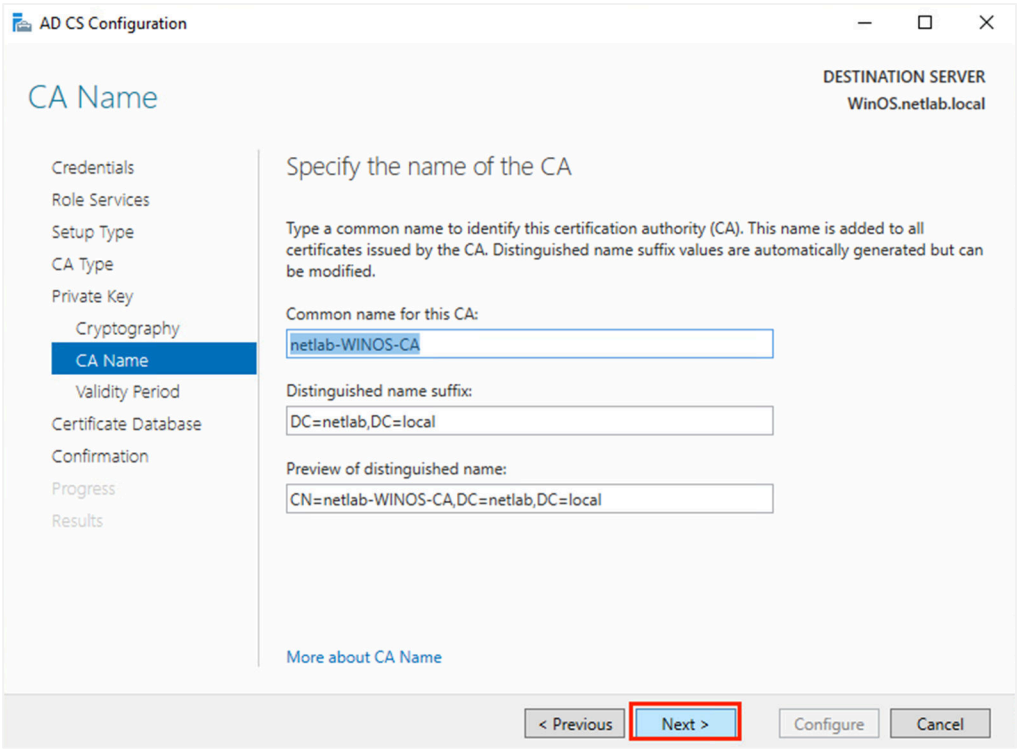
8. On the *Private Key* step, ensure that the radio button for **Create a new private key** is selected and click **Next.**



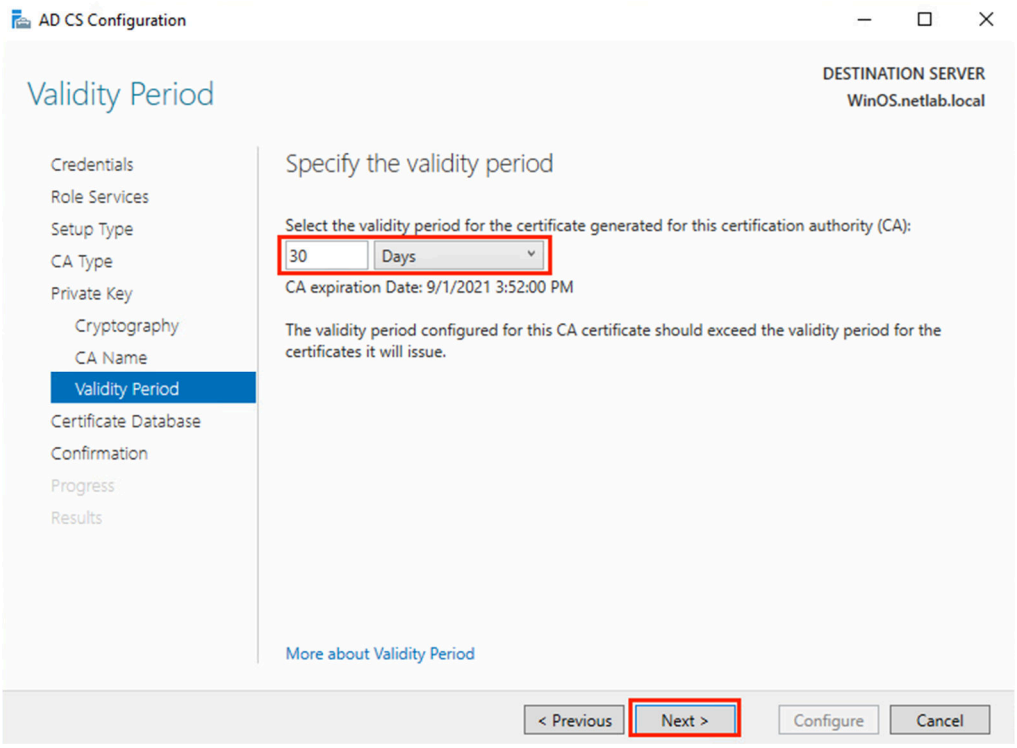
9. On the *Cryptography* step, leave the defaults and click **Next.**



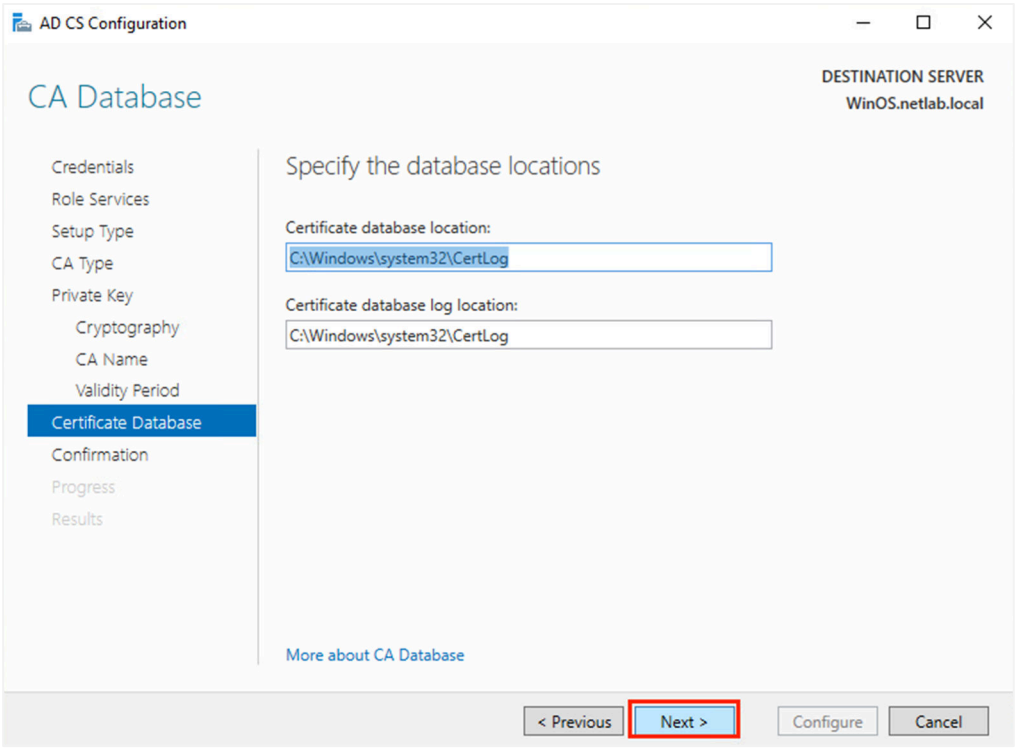
10. On the *CA Name* step, leave the defaults and click **Next**.



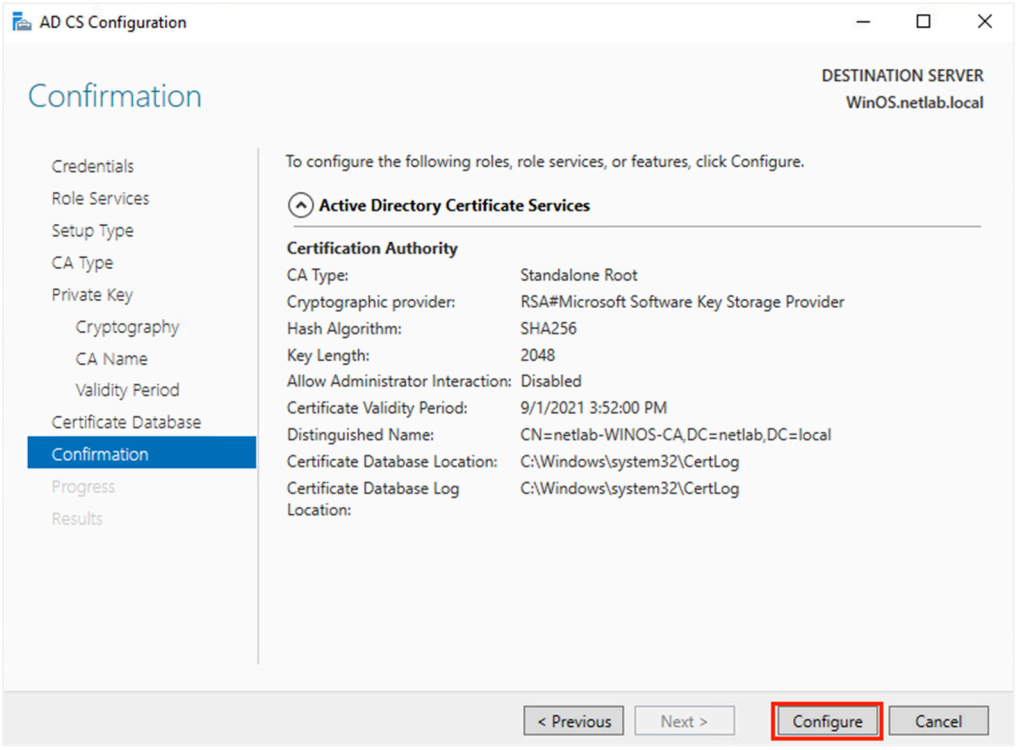
11. On the *Validity Period*, change the expiration period to **30 days** and click **Next**.



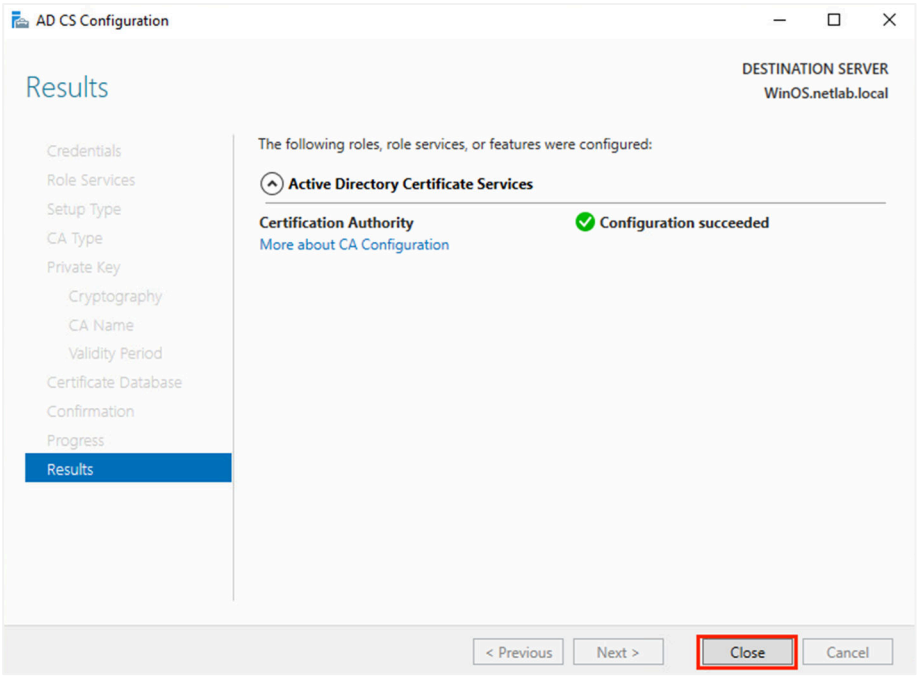
12. On the *Certificate Database* step, leave the default database location and click **Next.**



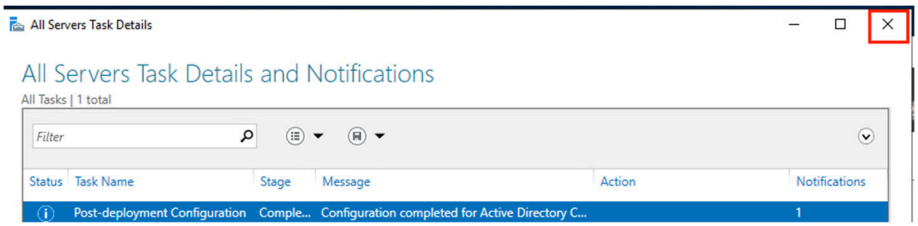
13. On the *Confirmation* step, review the configurations and click **Configure**.



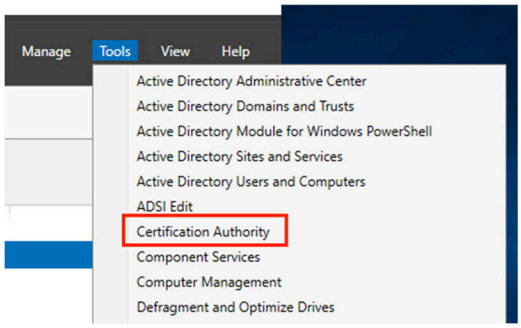
14. Once completed successfully, click **Close.**



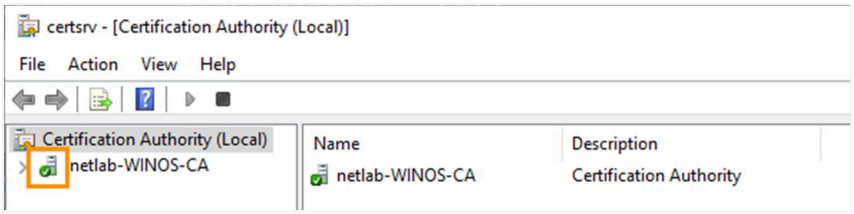
15. Then, close the *All Servers Task Details window.*



16. In the upper-right corner of the *Server Manager* window and then click on **Tools > Certification Authority.**



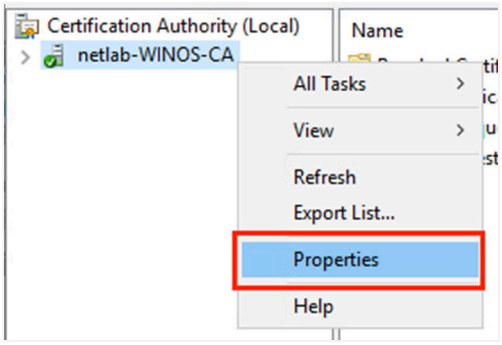
17. You should have a green icon next to your server, indicating that you are a certificate authority.



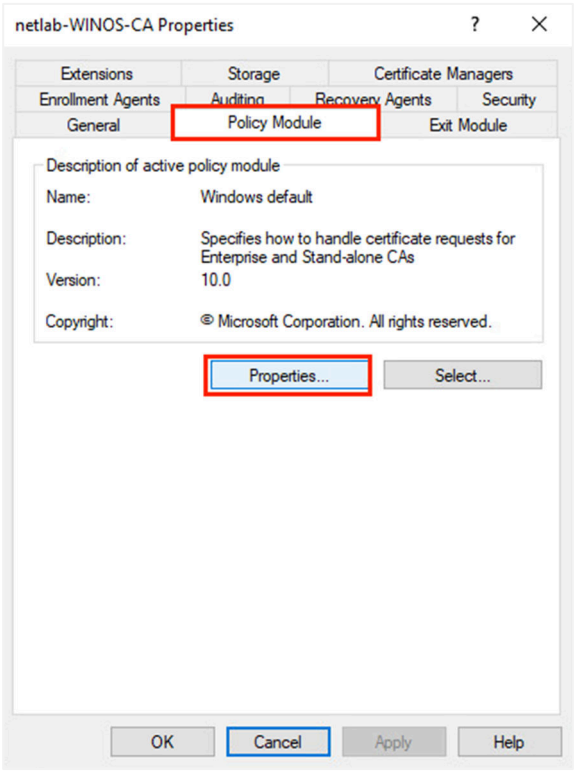
3 Issuing a Certificate from the Certificate Authority

3.1 Configure the Certificate Authority

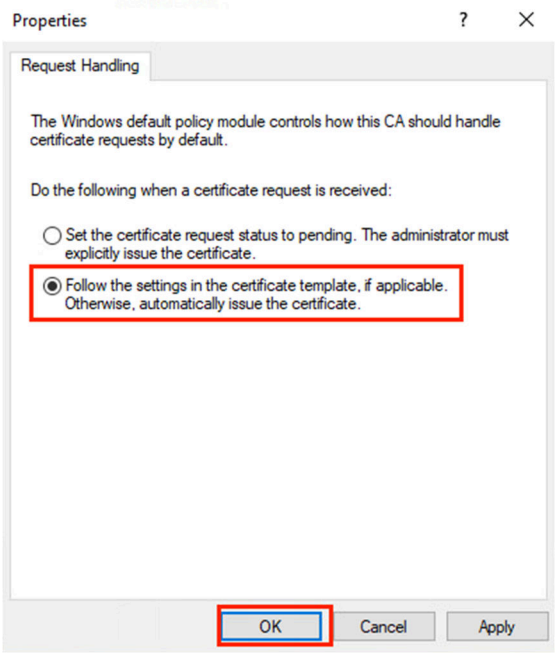
1. While you are in the *certsrv* window, right-click on the **netlab-WINOS-CA**, and select **Properties**.



2. In the newly opened *Properties* window, click the **Policy Module** tab, then the **Properties…** button.



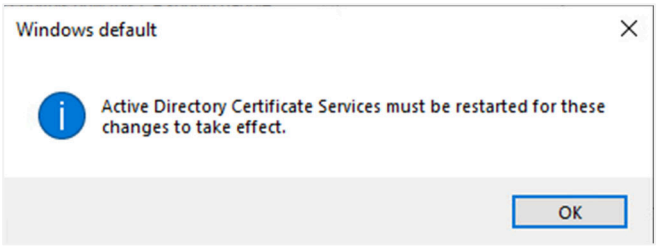
3. Click to check the radio button for **Following the settings in the certificate …** option, then click **OK** to confirm.



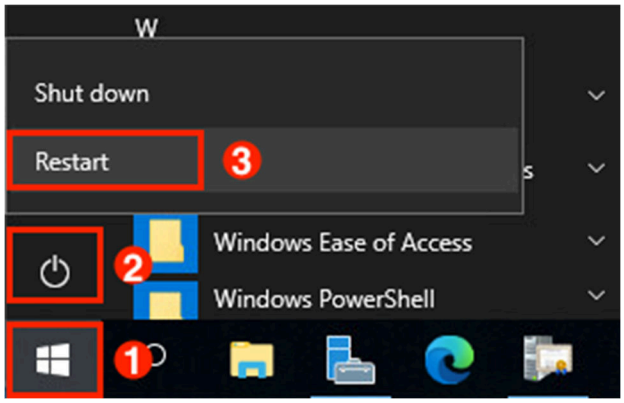
Please Note

You typically don't want the Certificate Authority to automatically issue the certificate, but for the purpose of this lab, we will enable this function.

4. When prompted to restart the computer, click **OK**. And **OK**, again.

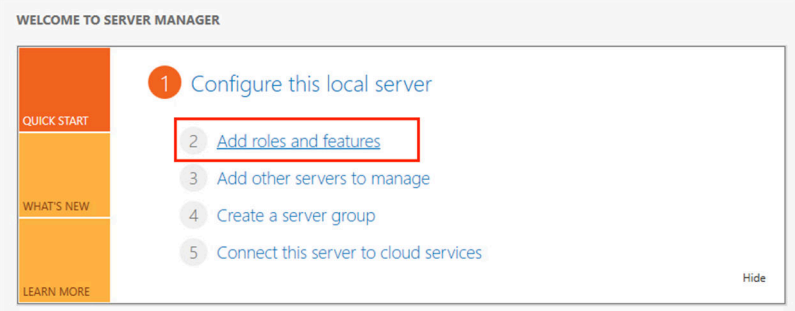


5. Restart the *WinOS* machine; when prompted to **Choose a reason**, click continue.

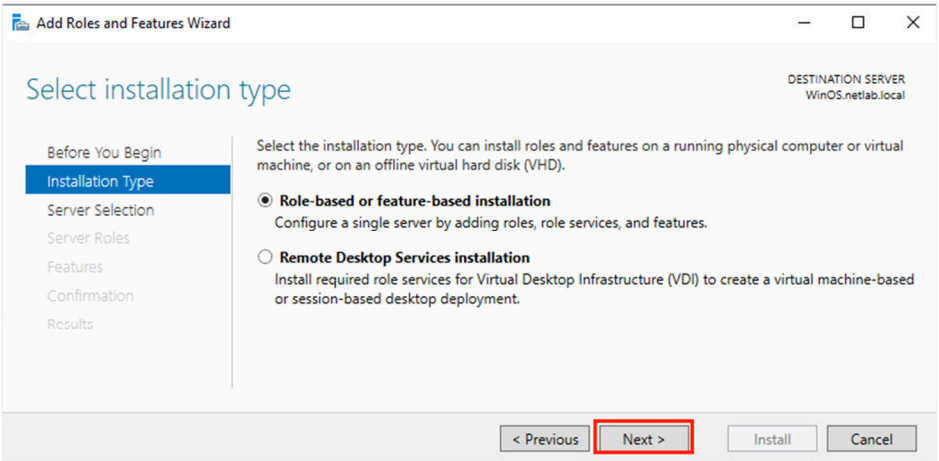


3.2 Install Internet Information Service (IIS) and Request a Certificate

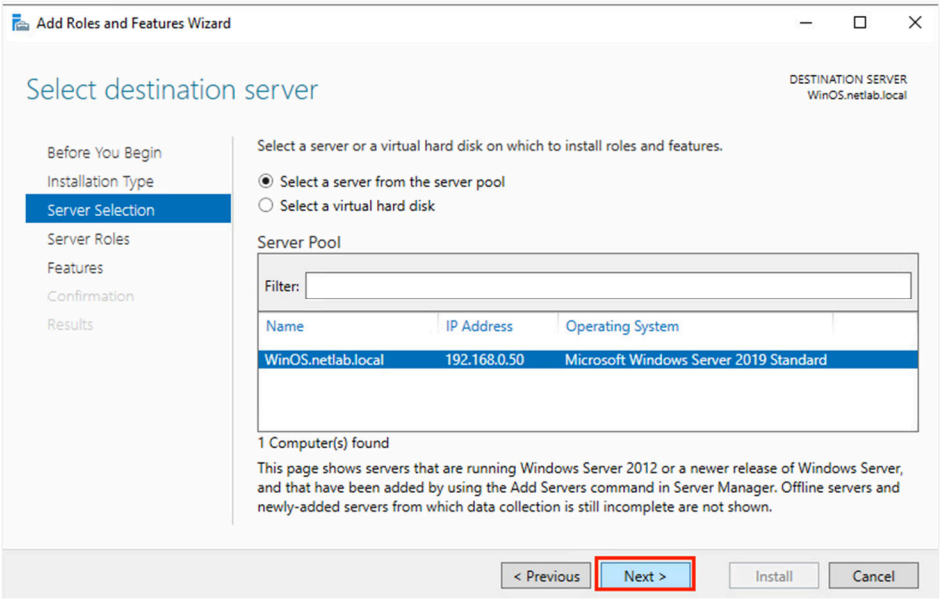
1. In the *Server Manager* window, click the **Add roles and features.**



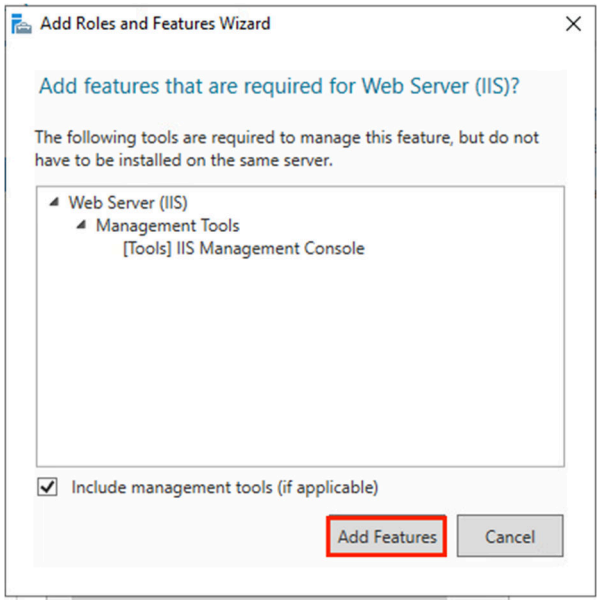
2. Notice the *Add Roles and Features Wizard* appears. On the *Installation Type* step, keep the default setting of **Role-based or feature-based installation** and click **Next.**



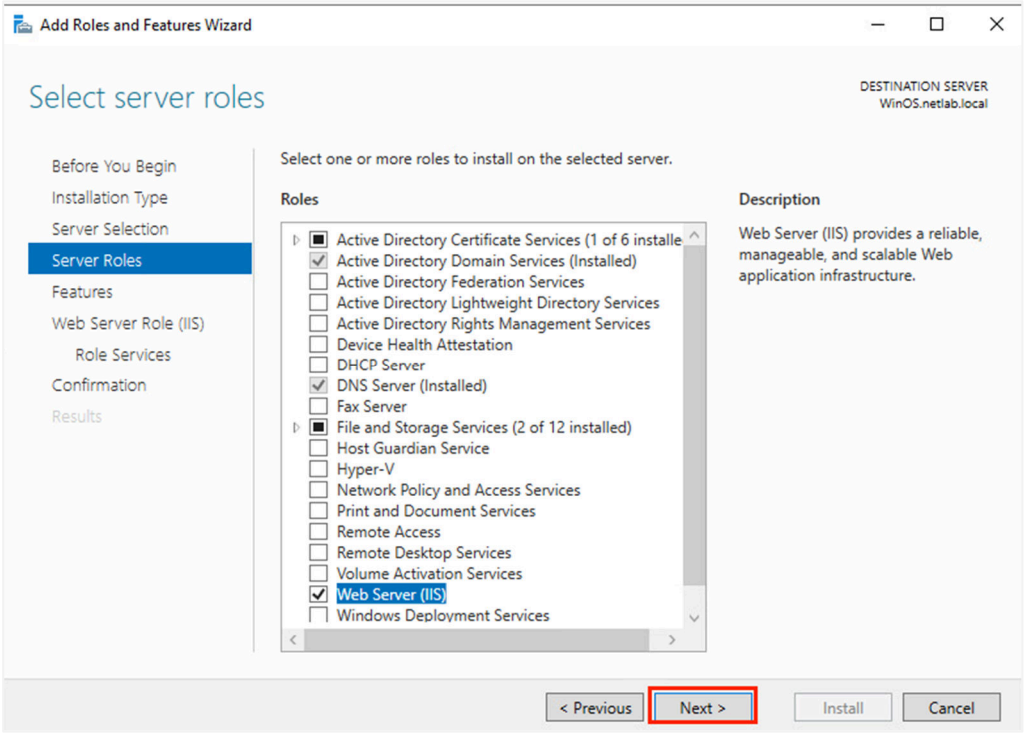
3. On the *Server Selection* step, select the **WinOS.netlab.local** server from the pool and click **Next.**



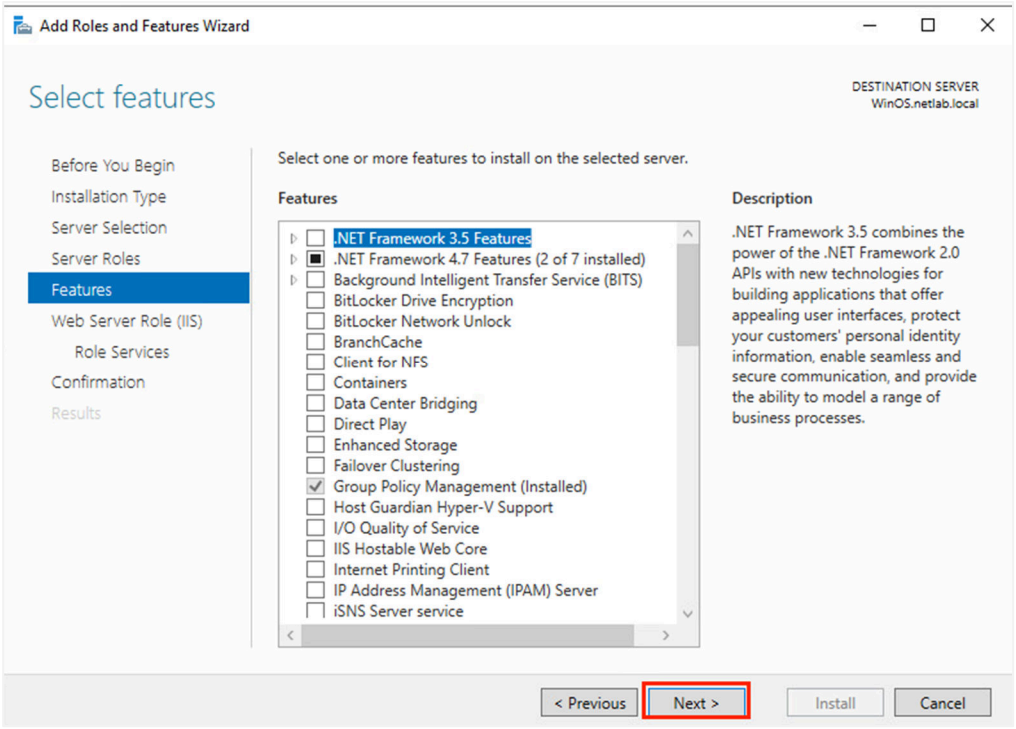
4. On the *Server Roles* step, check the checkbox for **Web Server (IIS)** and notice a pop-up window appears. Click the **Add Features** button.



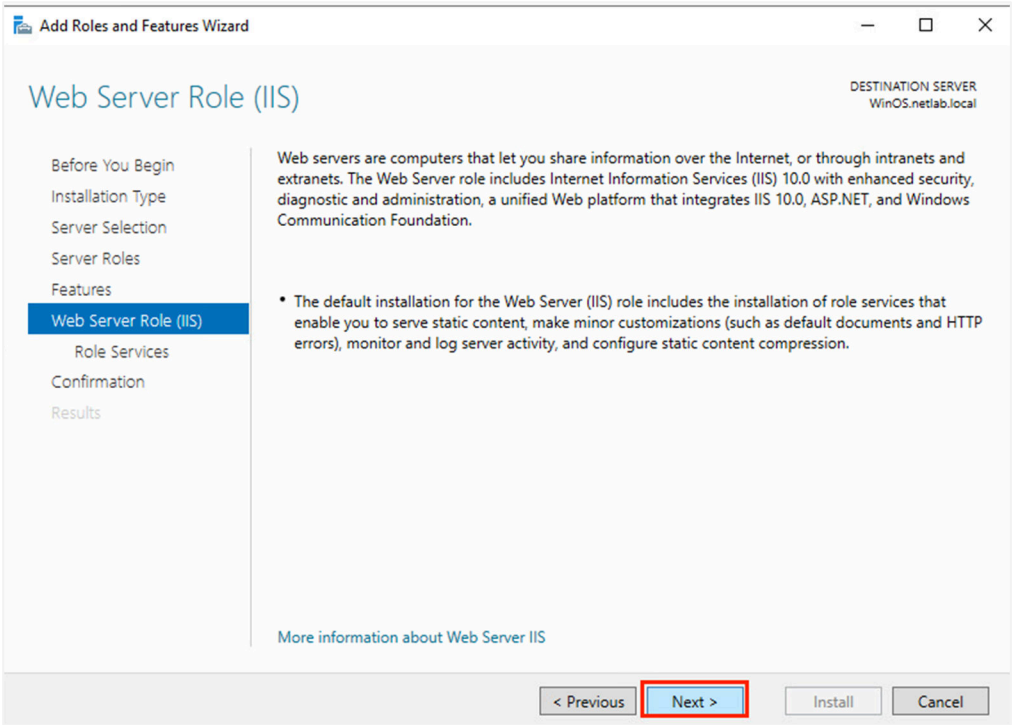
5. Back on the main wizard window, ensure that **Web Server (IIS)** is checked and click **Next.**



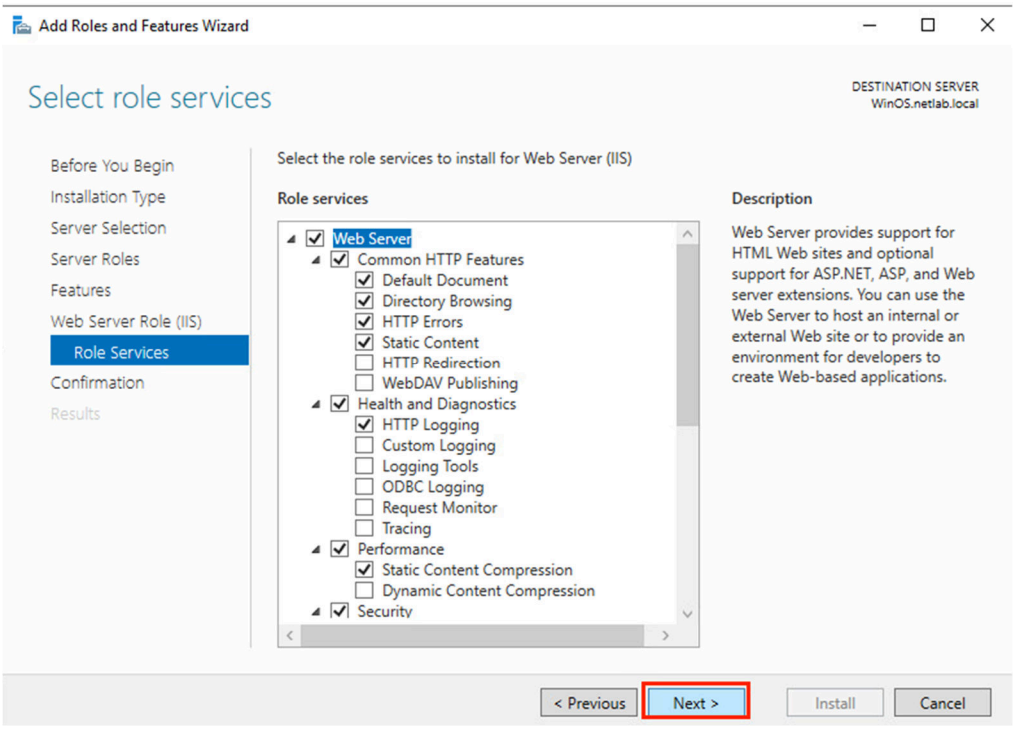
6. On the *Features* step, leave the defaults and click **Next.**



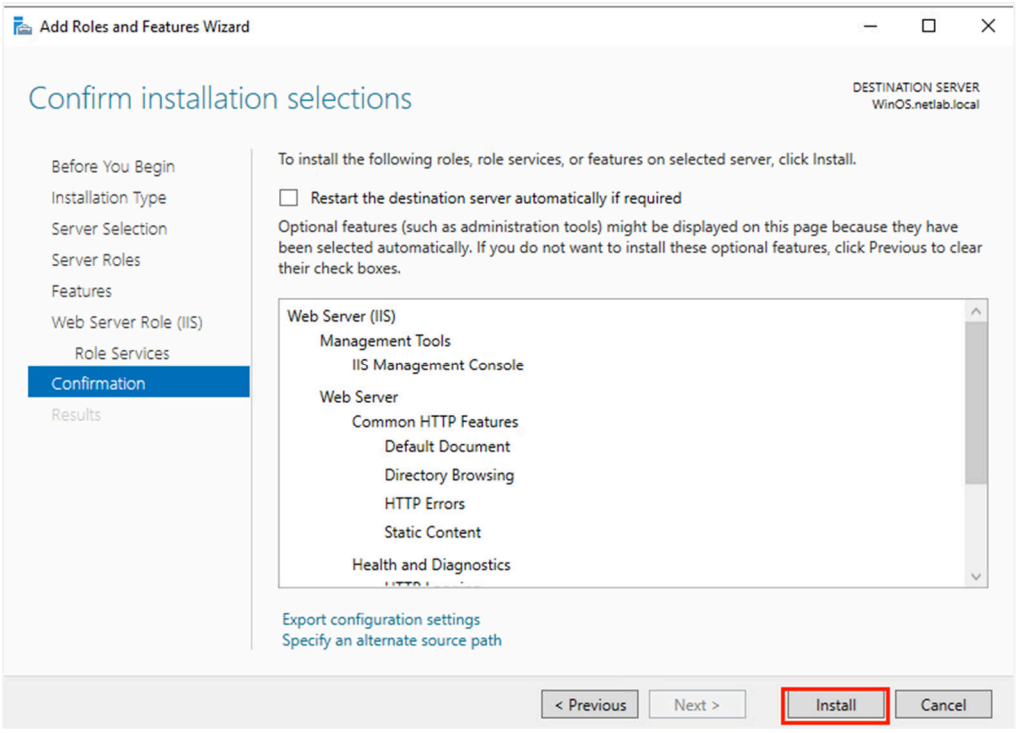
7. On the *Web Server Role (IIS)* step, review the information and click **Next.**



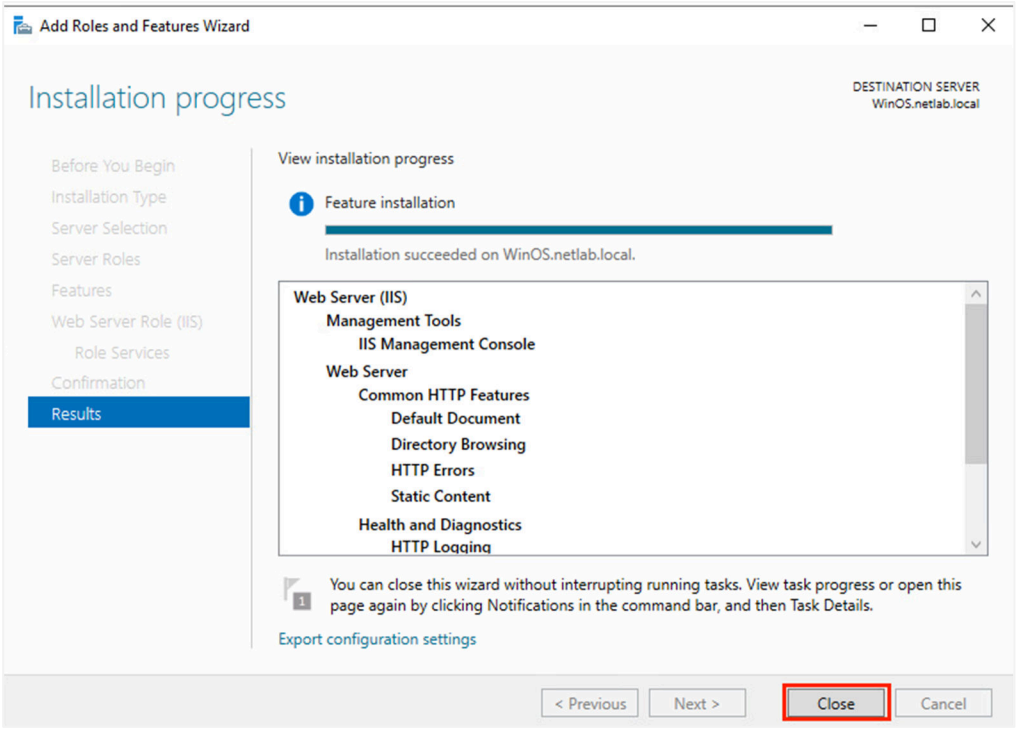
8. On the *Role Services* step, ensure that **Web Server** is checked and click **Next.**



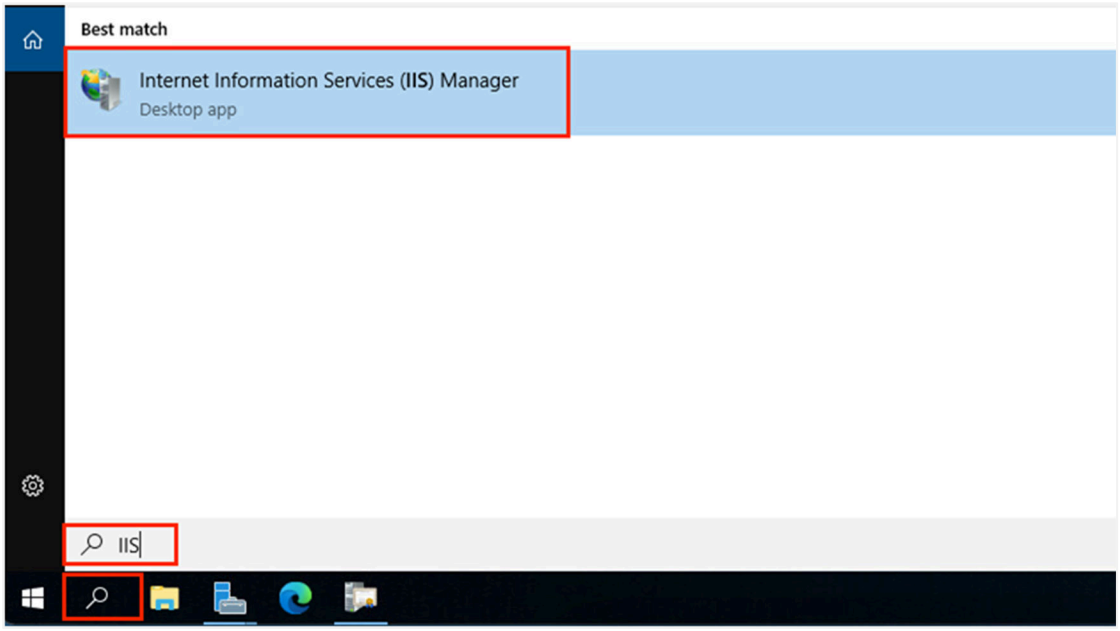
9. On the *Confirmation* step, click **Install** to finish the installation of the *Web Server.*



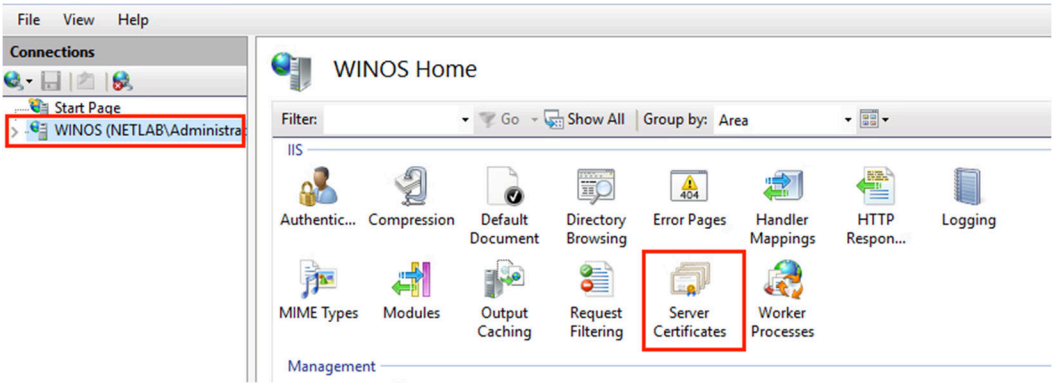
10. The installation will take a few minutes. Once the installation completes, click **Close.**



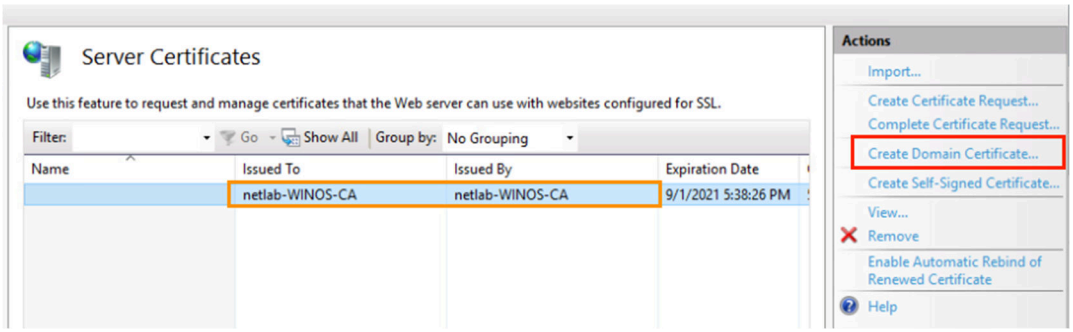
11. Click the search icon in the taskbar, type `IIS`, then click open the **Internet Information Service (IIS) Manager.**



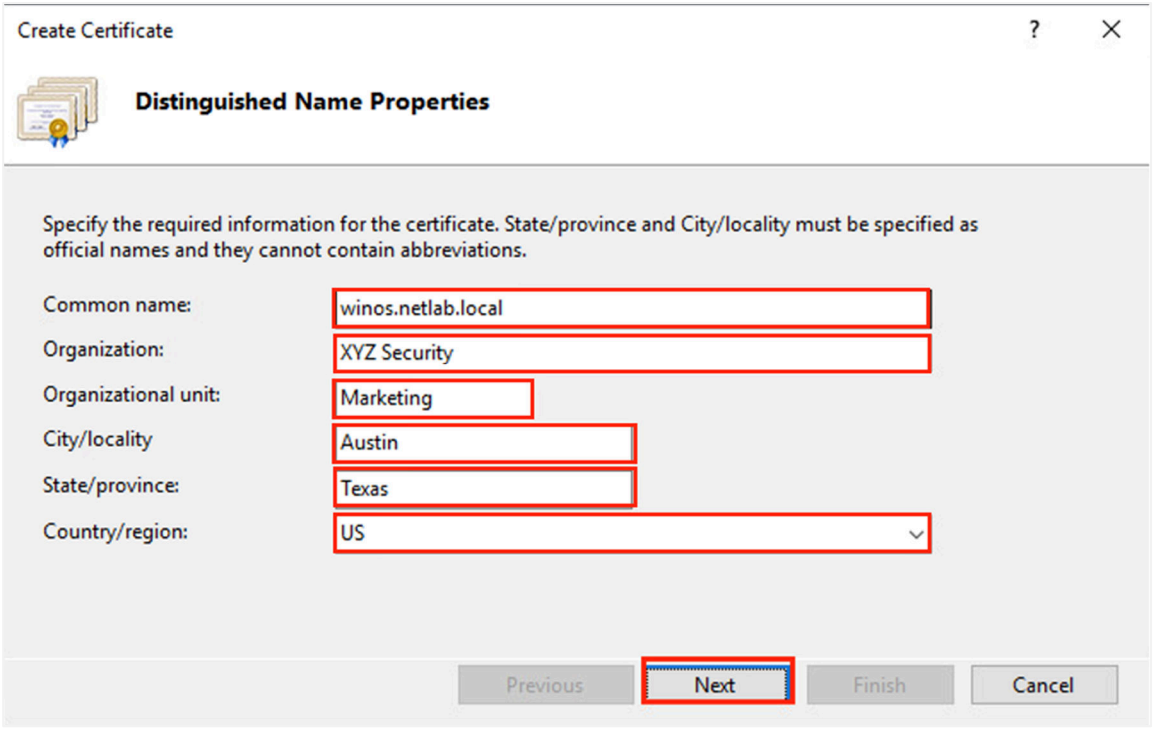
12. In the *Internet Information Service (IIS) Manager* window, click the **WINOS** in the left pane, then double-click to open the **Server Certificate.**



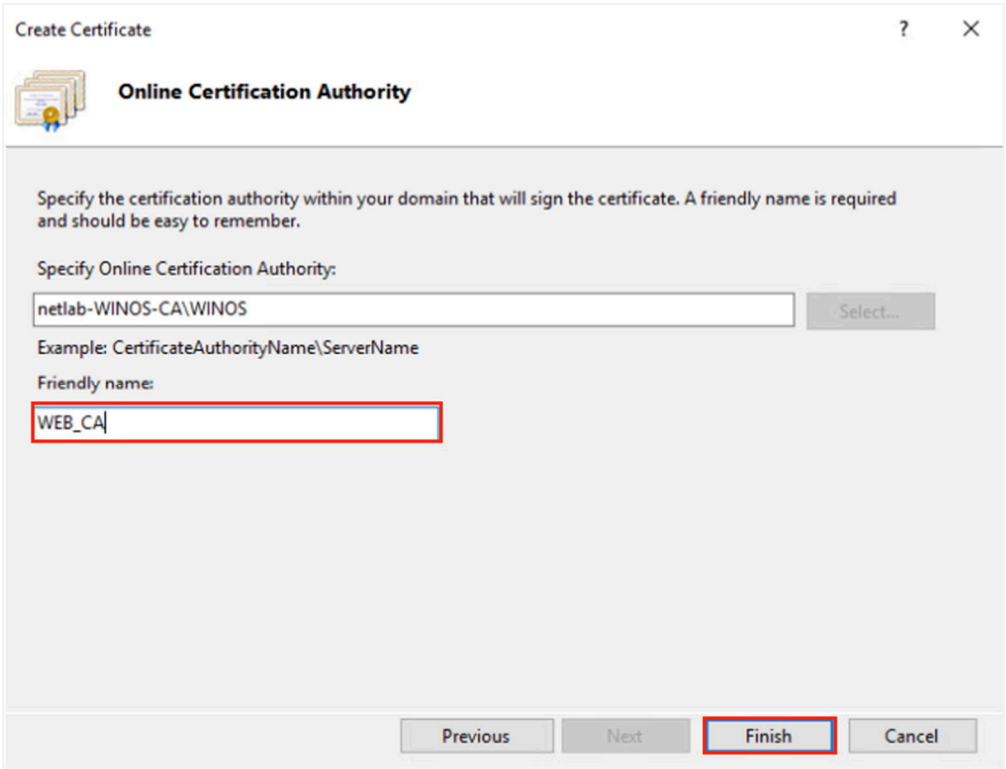
13. You will see that there is a personal certificate; we will ignore it. Let's click the **Create Domain Certificate…**



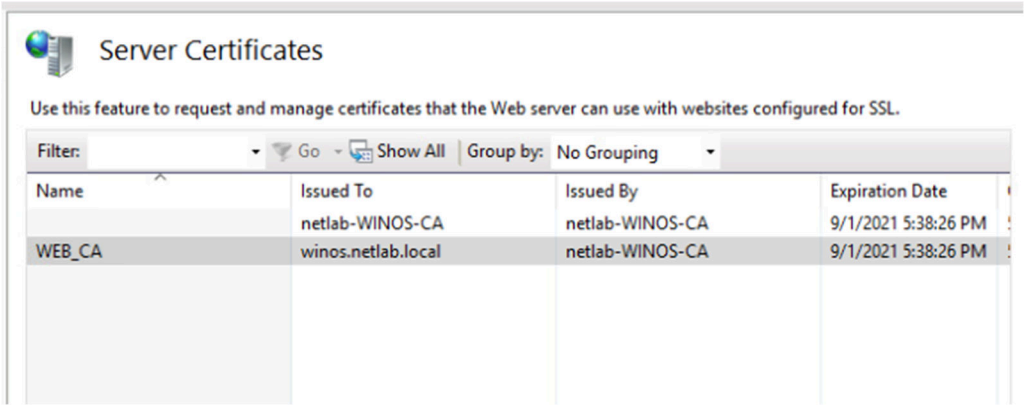
14. In the new window, fill in the information as shown below, then click the **Next** button.



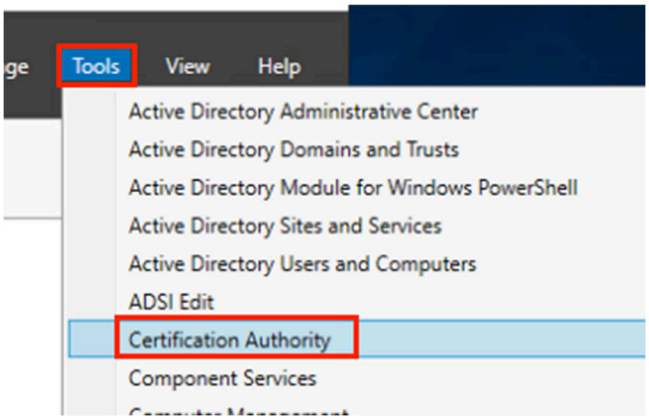
15. Then, fill in the information as shown below, then click the **Finish** button.



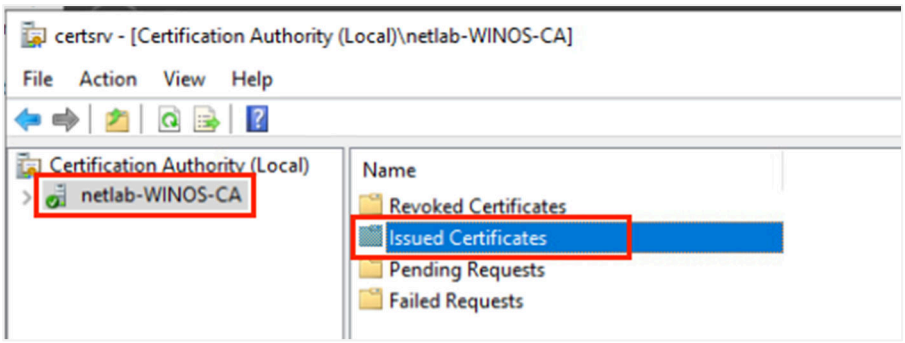
16. Notice the certificate with a *WEB_CA* as its name. Now you have your certificate issued from the *WINOS* server.



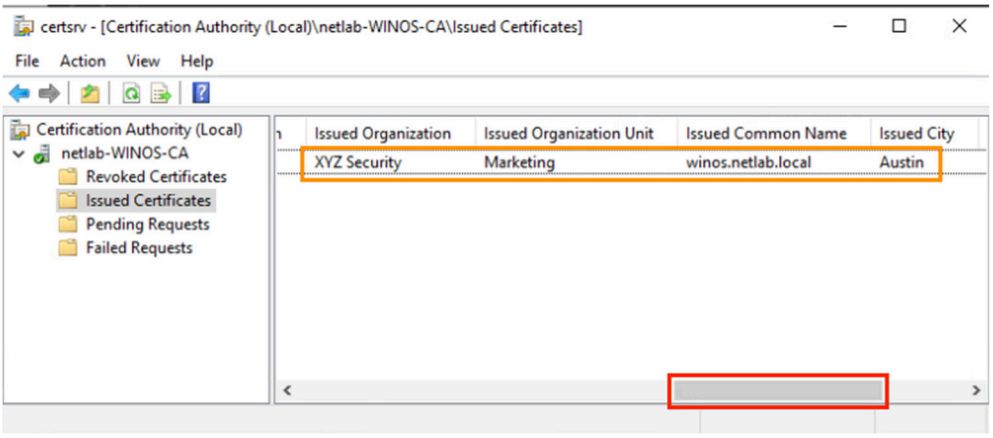
17. Switch back to the *Server Manager* window. Click on **Tools**, and select open **Certification Authority.**



18. In the new window, click the **netlab-WINOS-CA,** then double-click to open the **Issued Certificates** folder.



19. When it opens, scroll the horizontal bar to the right side to check the information on the certificate. You will see it was issued to *XYZ Security, Marketing, etc*. You can double-click on the certificate to check the details.



20. The lab is now complete; you may end the reservation.