Setup Server 2019 Enterprise CA 3/5: Subordinate CA

vmlabblog.com/2019/09/setup-server-2019-enterprise-ca-3-5-subordinate-ca

Aad Lutgert

September 25, 2019

51 Comments on Setup Server 2019 Enterprise CA 3/5: Subordinate CA

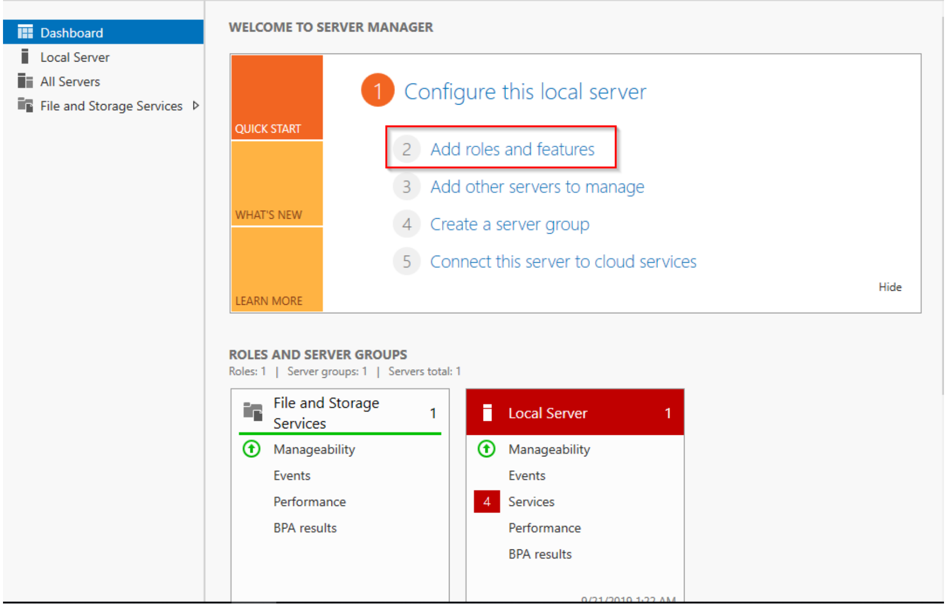
Previous: Offline Root CA

Updated 11-12-2020: Added missing role service “Basic Authentication” step 14.

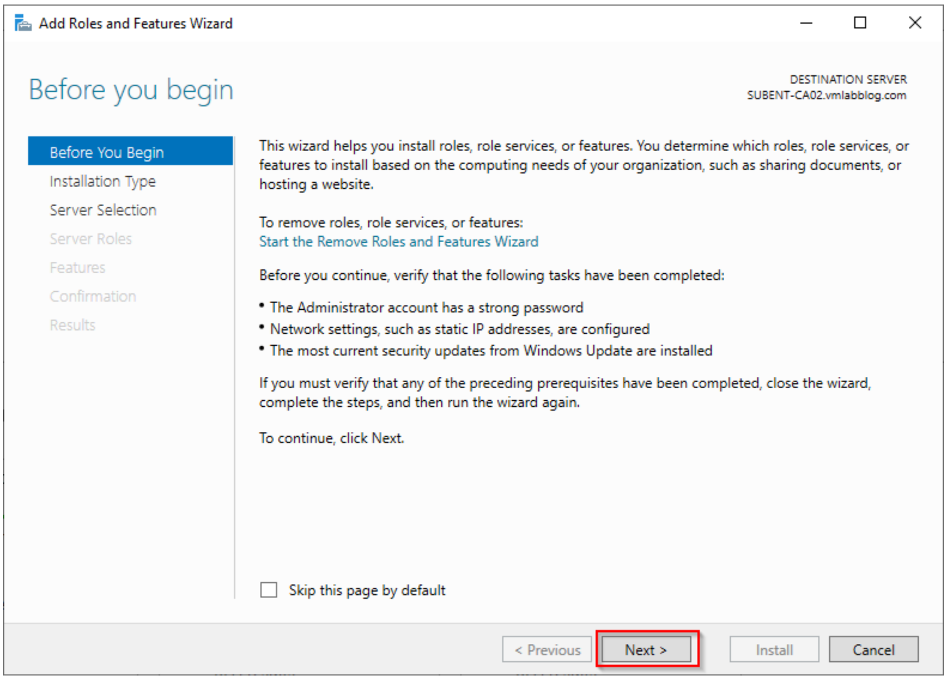
With the Offline Root CA completed, we can now setup of the Subordinate CA server. This server is authorized by the Root CA to issue the certificates. During the setup the CA role will be added and configured. The server will also be authorized by the Root CA The Subordinate CA Server is the SUBENT-CA02. Make sure that the server Subordinate server is domain joined before you start with the ADCS setup and that you have a domain account which is member of the Enterprise admins group.

Setup Subordinate CA

1. Start the Server manager and select “Add roles and features”



2. The “Add Roles and Features Wizard” will start, press “Next” to continue.



Before you begin

DESTINATION SERVER
SUBENT-CA02.vmlabblog.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:

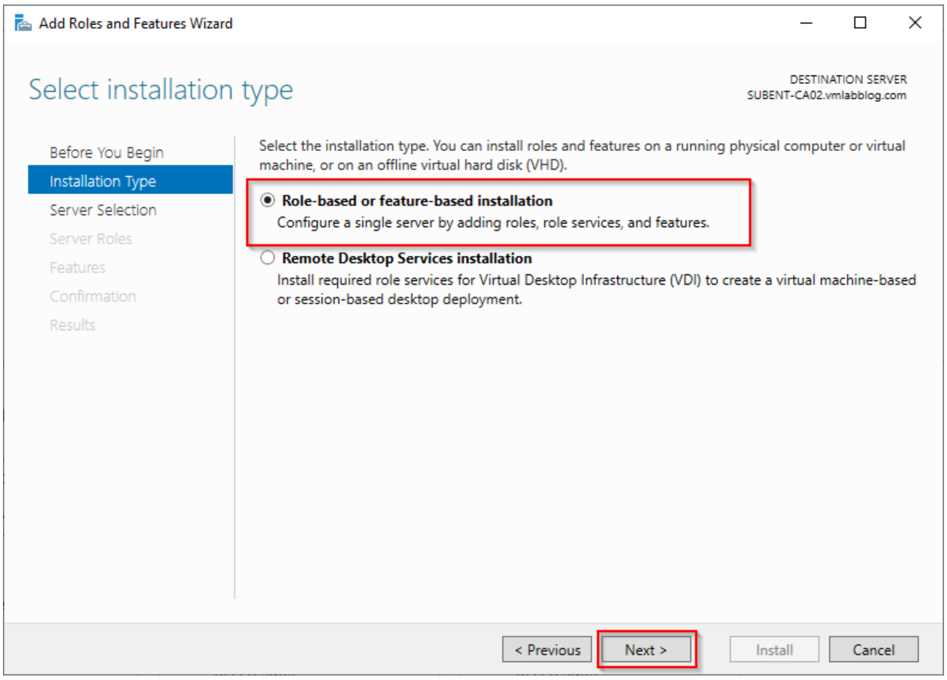
- The Administrator account has a strong password
- Network settings, such as static IP addresses, are configured
- The most current security updates from Windows Update are installed

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

3. Select “Role-based or feature-based installation” and press “Next”



Select installation type

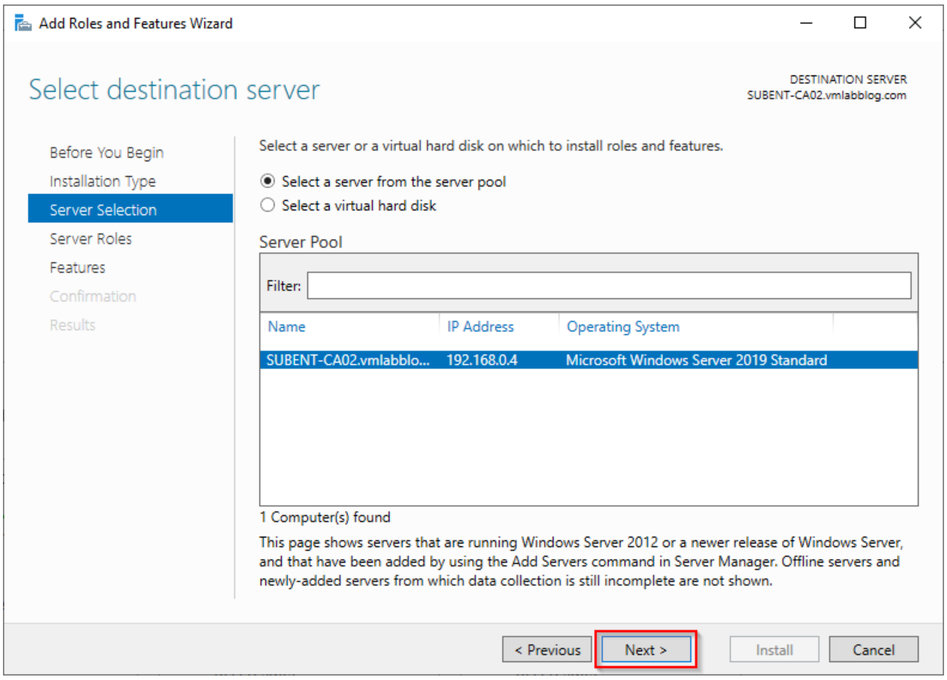
DESTINATION SERVER
SUBENT-CA02.vmlabblog.com

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.

4. Use the default settings and press “Next” to continue.



Select destination server

DESTINATION SERVER
SUBENT-CA02.vmlabblog.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

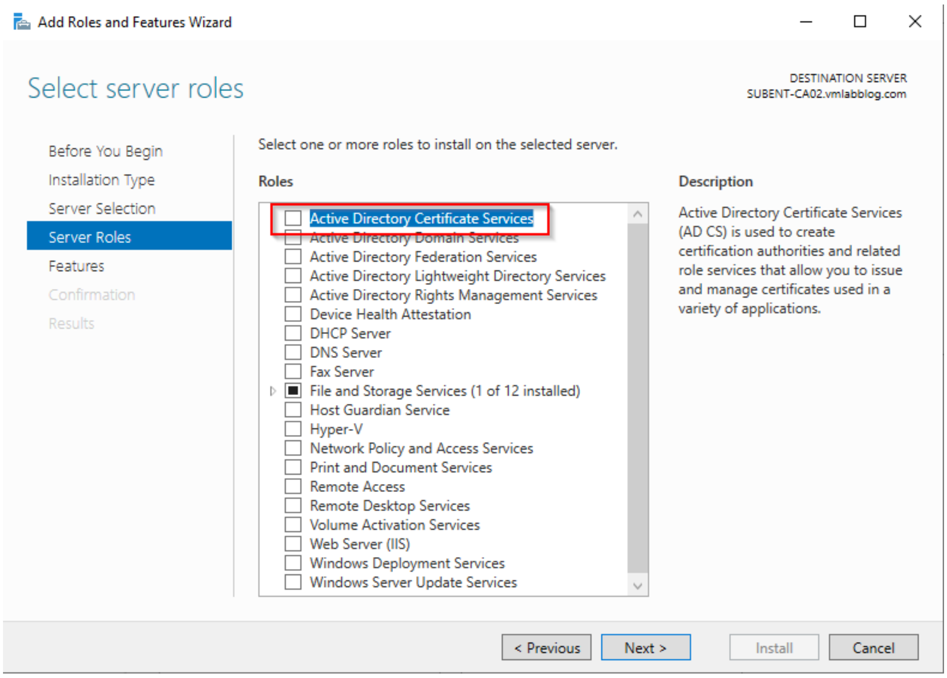
Filter:

Name	IP Address	Operating System
SUBENT-CA02.vmlabblo...	192.168.0.4	Microsoft Windows Server 2019 Standard

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.

5. Select “Active Directory Certificate Services”



Select server roles

DESTINATION SERVER
SUBENT-CA02.vmlabblog.com

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

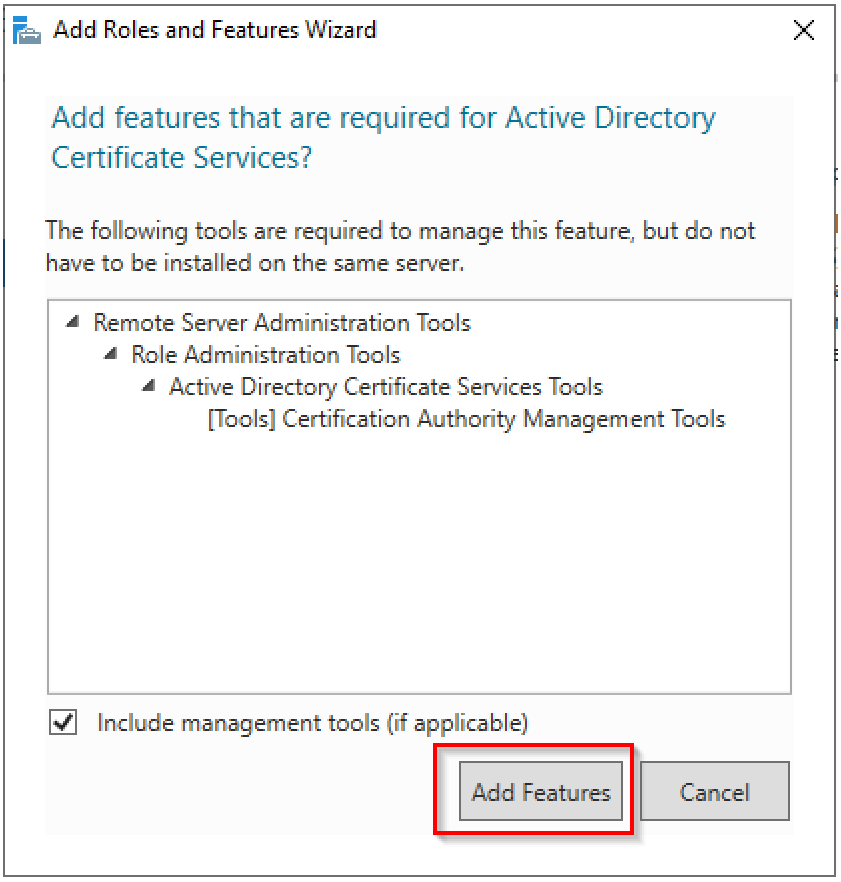
Roles

- □ 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 Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- □ Web Server (IIS)
- □ Windows Deployment Services
- □ Windows Server Update Services

Description

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

6. A pop-up will appear, press “Add Features” to continue.



Add Roles and Features Wizard

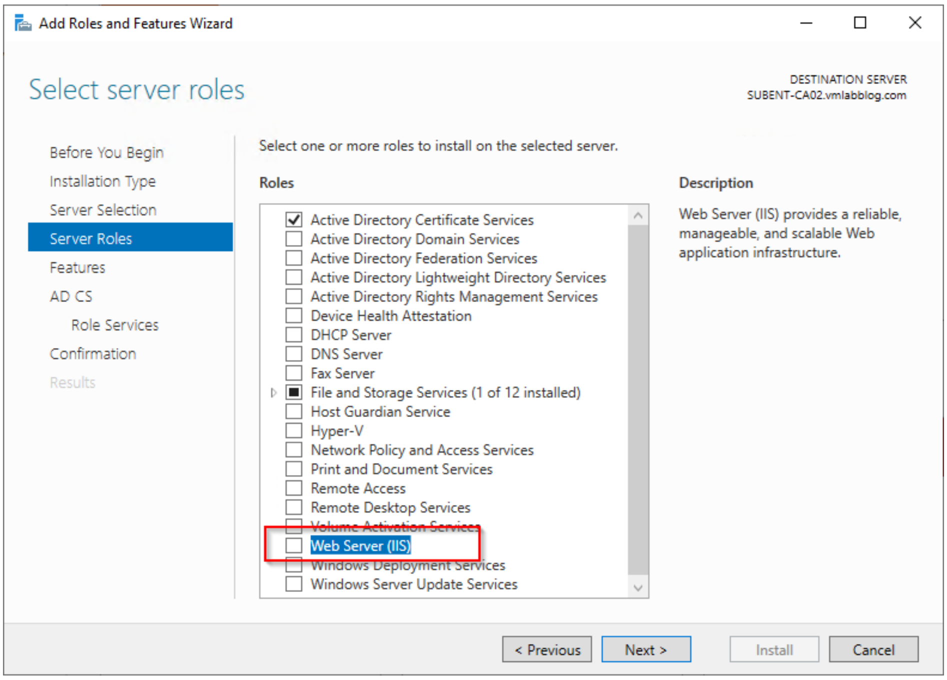
Add features that are required for Active Directory Certificate Services?

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)

7. Select “Web Server (IIS)



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
SUBENT-CA02.vmlabblog.com

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

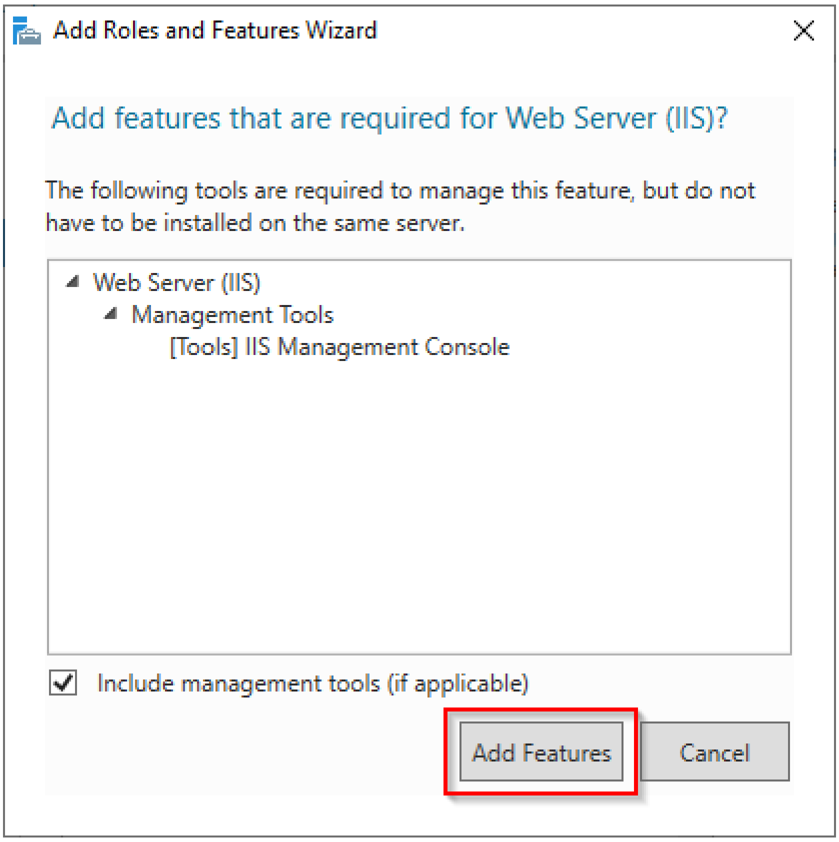
Roles

☑ 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 Policy and Access Services
□ Print and Document Services
□ Remote Access
□ Remote Desktop Services
□ Volume Activation Services
□ Web Server (IIS)
□ Windows Deployment Services
□ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

8. A pop-up will appear, press “Add Features” to continue.


Add Roles and Features Wizard

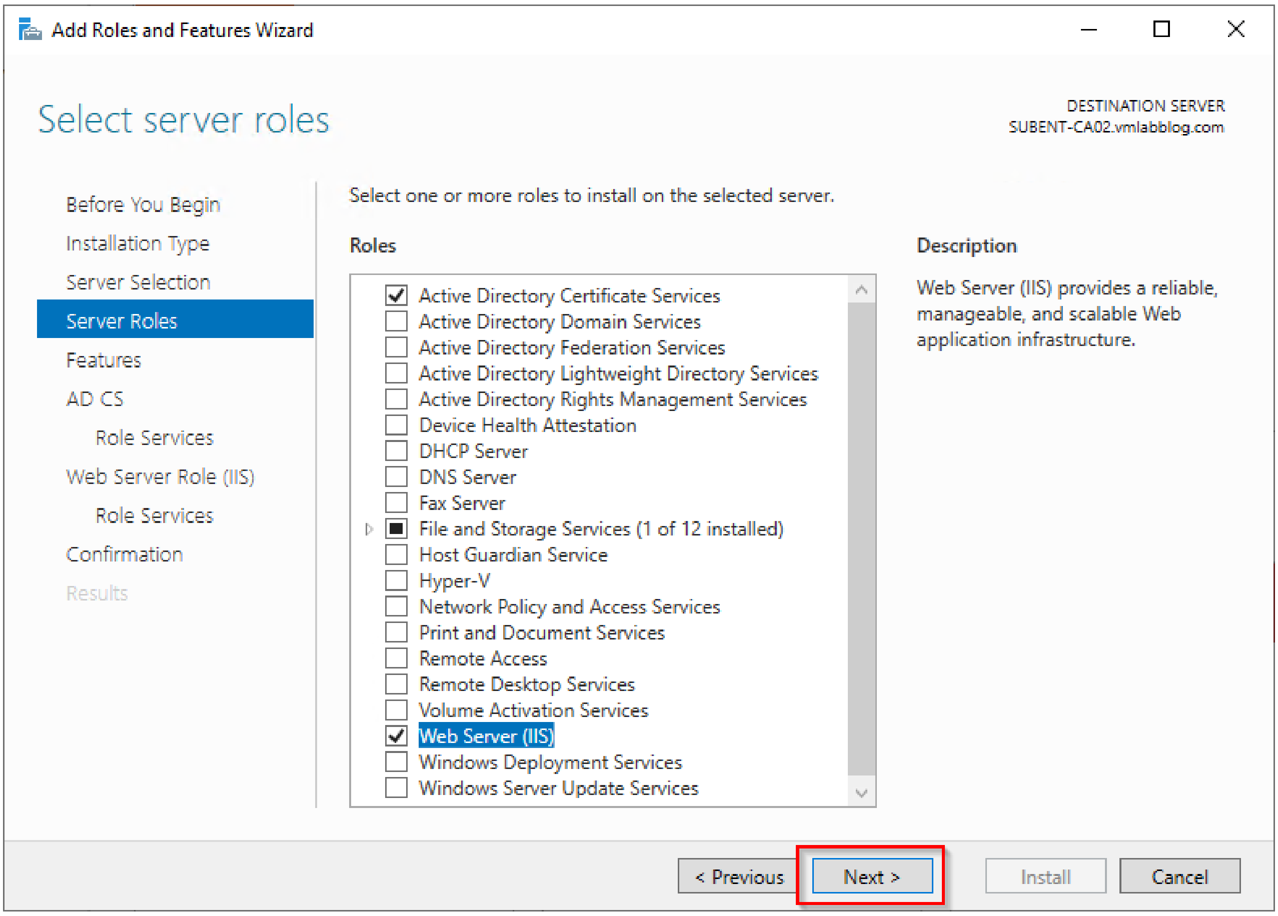
Add features that are required for Web Server (IIS)?

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

- Web Server (IIS)
  - Management Tools
    - [Tools] IIS Management Console

☑ Include management tools (if applicable)

9. Press “Next” to continue


Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
SUBENT-CA02.vmlabblog.com

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

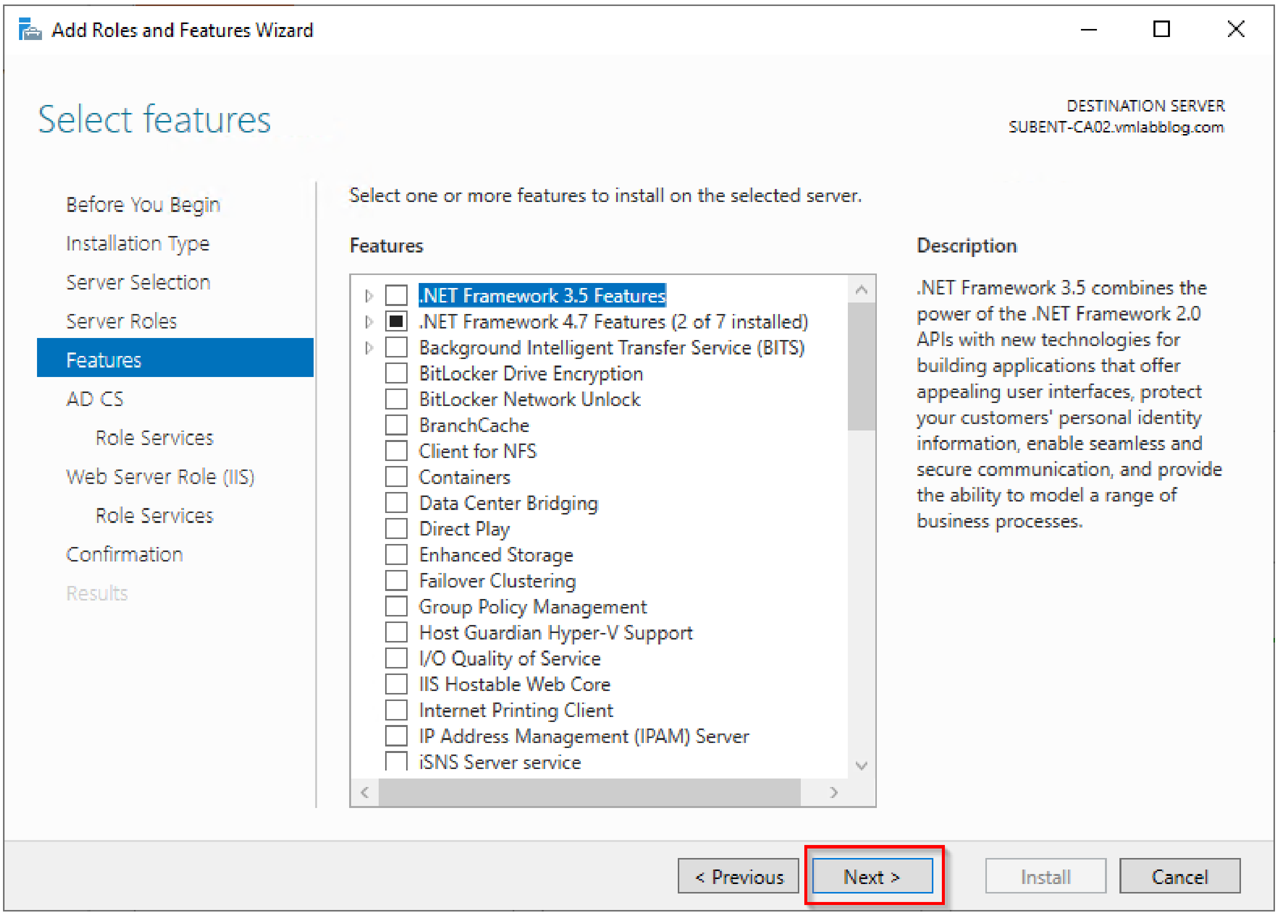
Roles

☑ 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 Policy and Access Services
☐ Print and Document Services
☐ Remote Access
☐ Remote Desktop Services
☐ Volume Activation Services
☑ Web Server (IIS)
☐ Windows Deployment Services
☐ Windows Server Update Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

10. Press “Next” to continue.



Select features

DESTINATION SERVER
SUBENT-CA02.vmlabblog.com

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

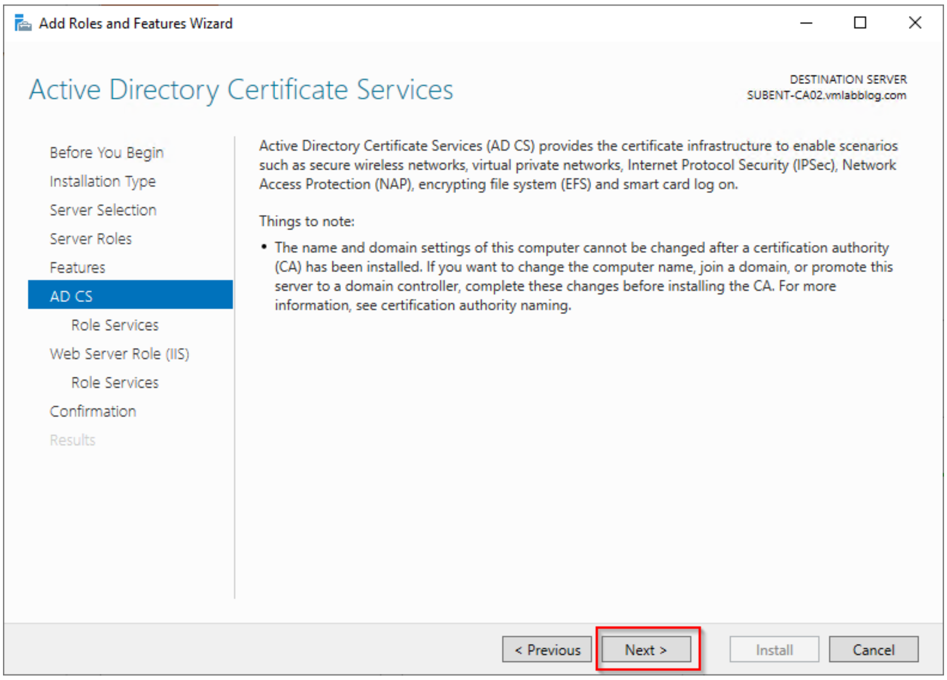
Features

- □ .NET Framework 3.5 Features
- ■ .NET Framework 4.7 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
- □ iSNS Server service

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.

11. Check if the Servername before you start, this cannot be changed after the AD CS role has been installed and press “Next” to continue.



Active Directory Certificate Services

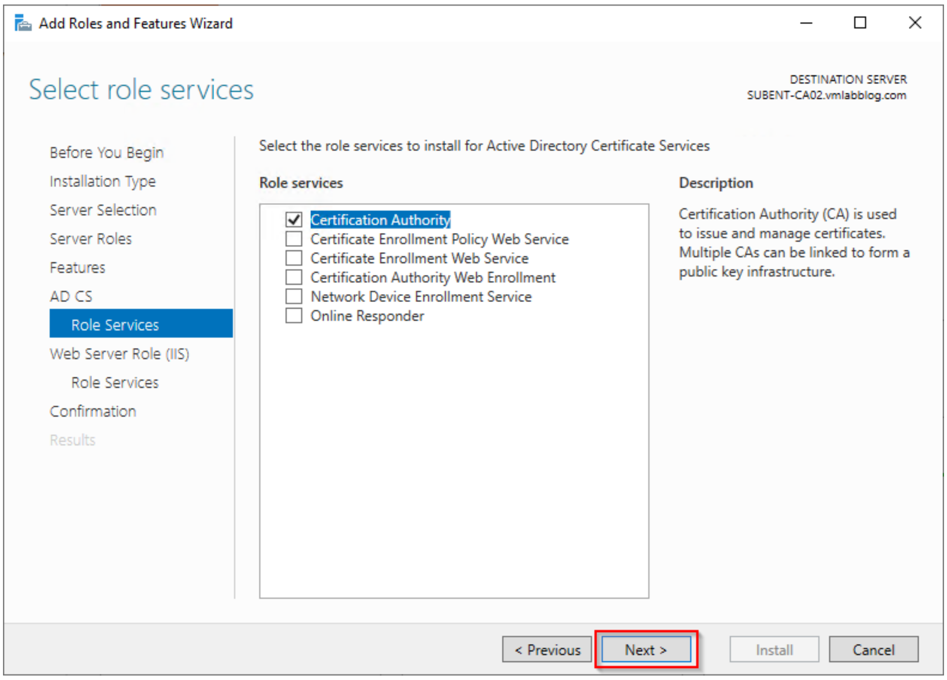
DESTINATION SERVER
SUBENT-CA02.vmlabblog.com

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.

12. Keep the default role services (Certication Authority) and press “Next”



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
SUBENT-CA02.vmlabblog.com

Select the role services to install for Active Directory Certificate Services

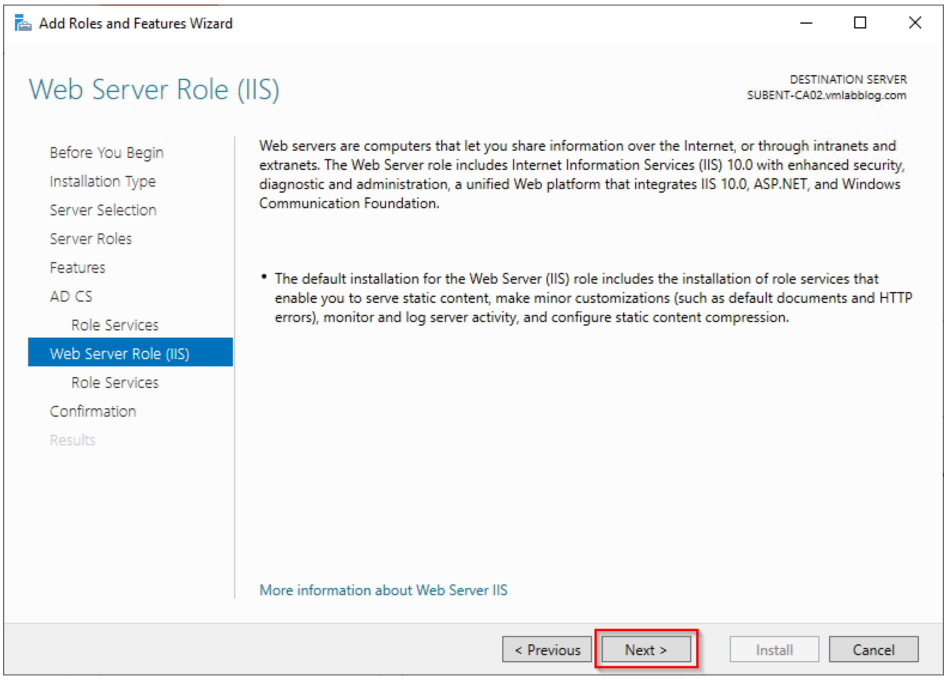
Role services

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

Description

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

13. On the Web Server Role (IIS) page press “Next”



Add Roles and Features Wizard

Web Server Role (IIS)

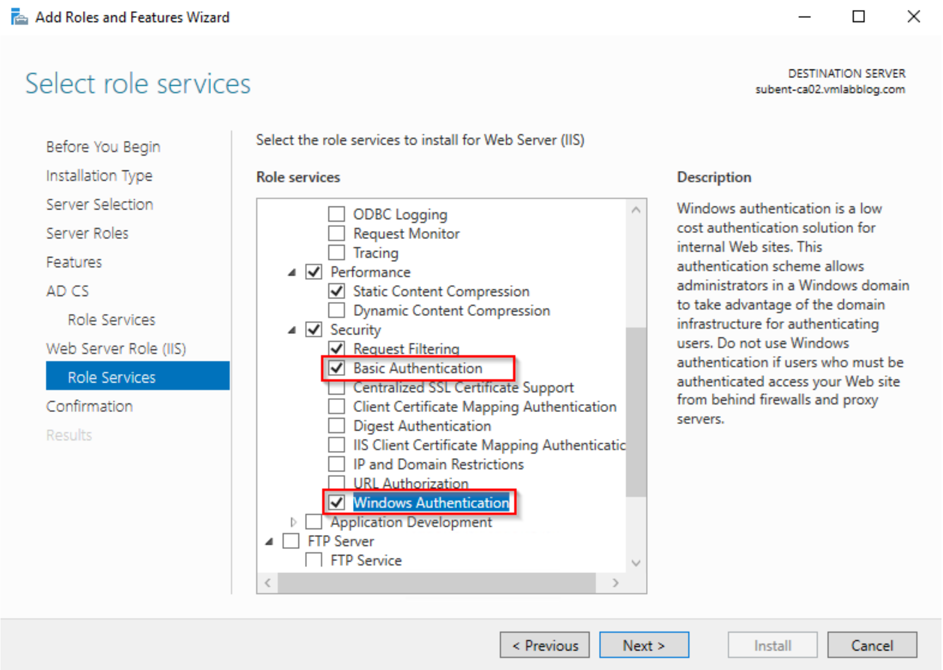
DESTINATION SERVER
SUBENT-CA02.vmlabblog.com

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

14. On the Role Services page select “Basic Authentication” and “Windows Authentication”. Press “Next” to continue.



Select role services

DESTINATION SERVER
subent-ca02.vmlabblog.com

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

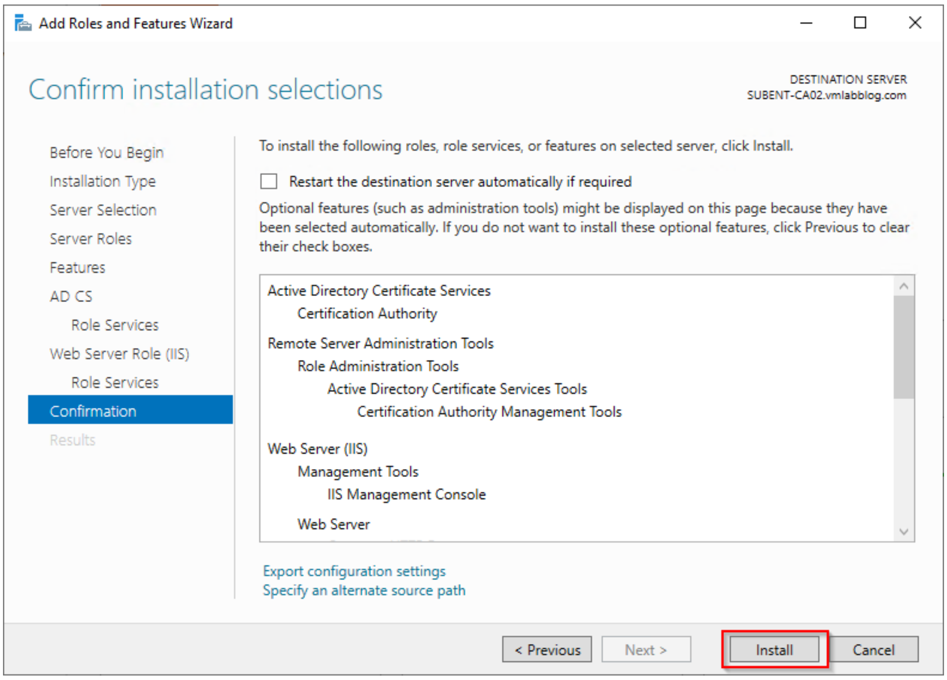
Role services

- □ ODBC Logging
- □ Request Monitor
- □ Tracing
- ☑ Performance
  - ☑ Static Content Compression
  - □ Dynamic Content Compression
- ☑ Security
  - ☑ Request Filtering
  - ☑ Basic Authentication
  - □ Centralized SSL Certificate Support
  - □ Client Certificate Mapping Authentication
  - □ Digest Authentication
  - □ IIS Client Certificate Mapping Authenticatic
  - □ IP and Domain Restrictions
  - □ URL Authorization
  - ☑ Windows Authentication
- □ Application Development
- □ FTP Server
  - □ FTP Service

Description

Windows authentication is a low cost authentication solution for internal Web sites. This authentication scheme allows administrators in a Windows domain to take advantage of the domain infrastructure for authenticating users. Do not use Windows authentication if users who must be authenticated access your Web site from behind firewalls and proxy servers.

15. In the confirmation screen press “Install” to start the installation.



Confirm installation selections

DESTINATION SERVER
SUBENT-CA02.vmlabblog.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.

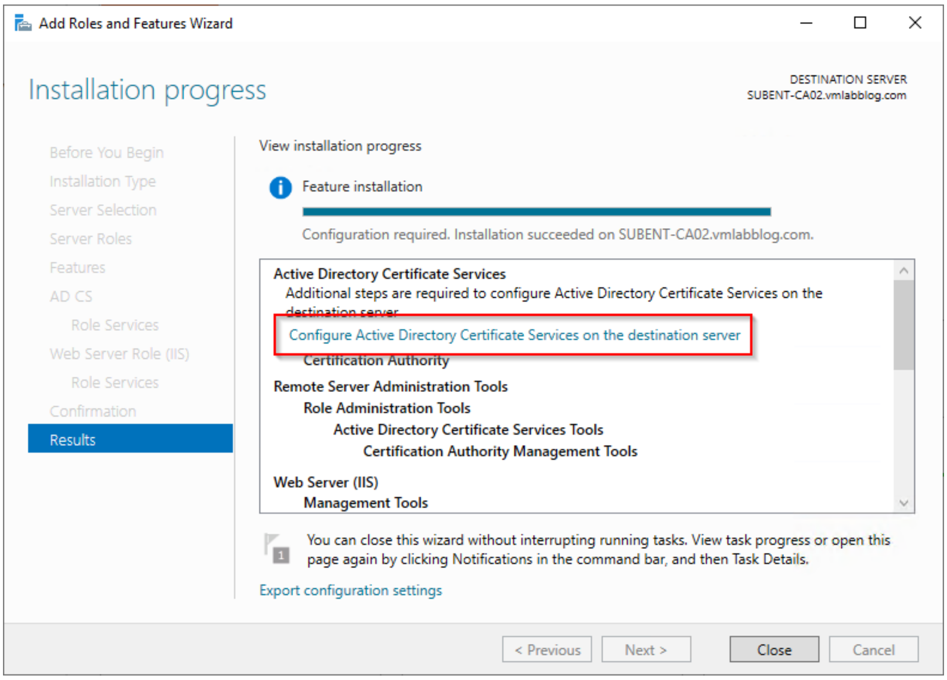
Active Directory Certificate Services
  Certification Authority

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

Web Server (IIS)
  Management Tools
    IIS Management Console
  Web Server

Export configuration settings
Specify an alternate source path

16. When the installation has completed, press the link “Configure Active Directory Certificate Services on the destination server”



Installation progress

DESTINATION SERVER
SUBENT-CA02.vmlabblog.com

View installation progress

Feature installation

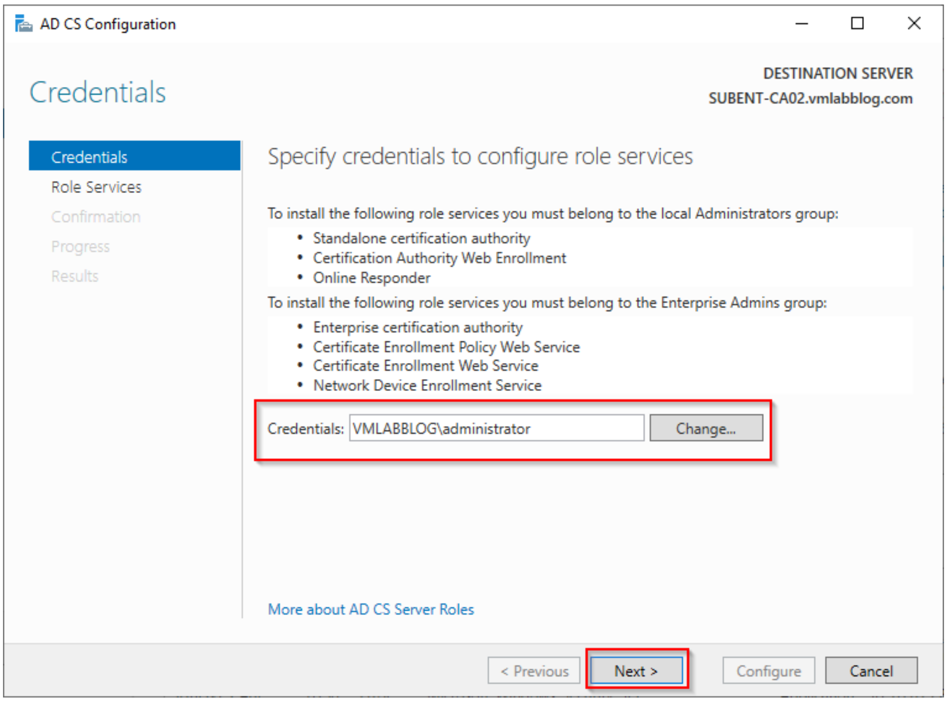
Configuration required. Installation succeeded on SUBENT-CA02.vmlabblog.com.

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

17. Make sure your Domain credentials have been entered and not your local admin credentials. Otherwise you will not be able to configure a Enterprise CA. Press “Next” to continue.



Credentials

DESTINATION SERVER
SUBENT-CA02.vmlabblog.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

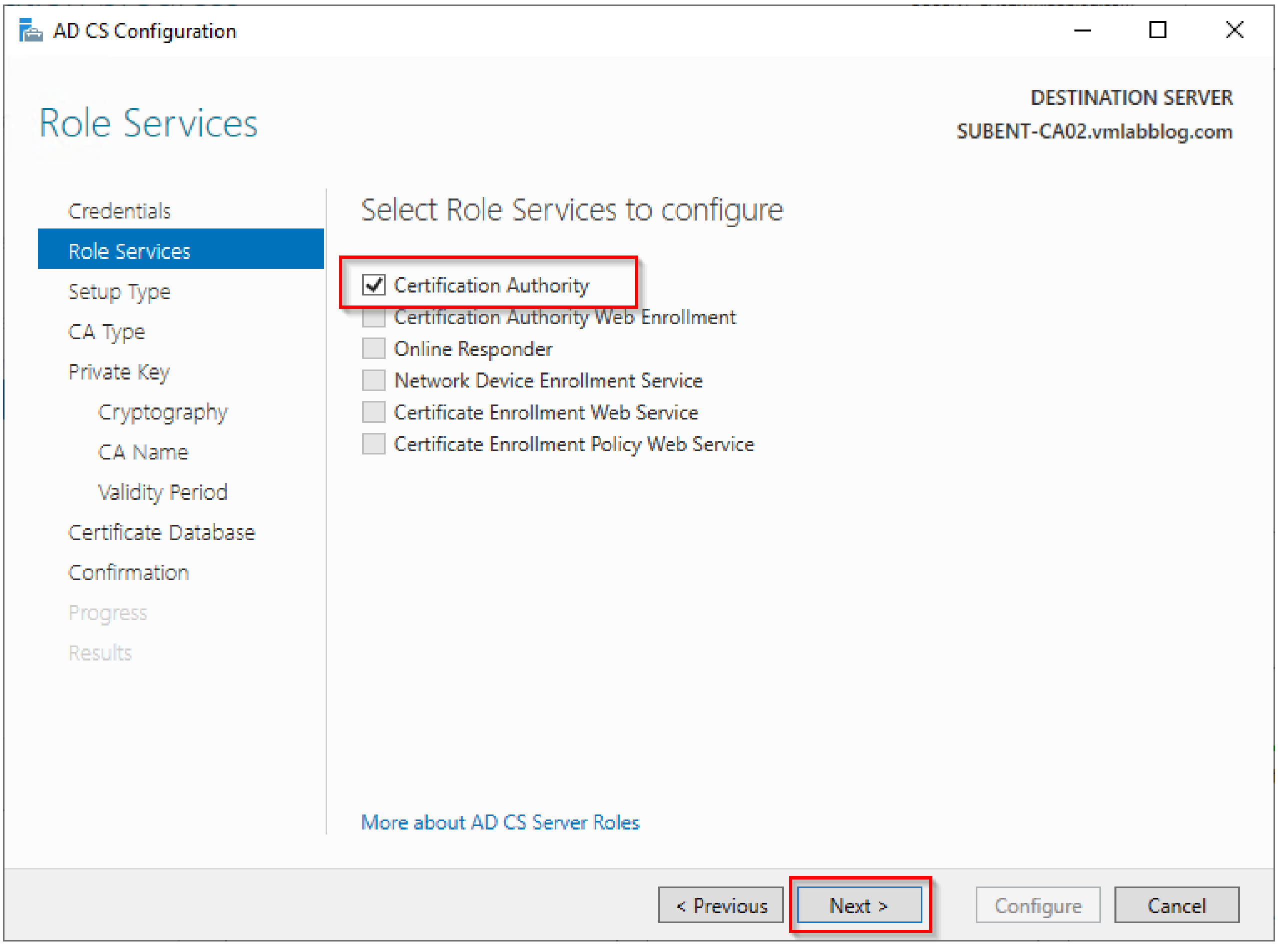
To install the following role services you must belong to the Enterprise Admins group:

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

Credentials: VMLABBLOG\administrator Change...

More about AD CS Server Roles

18. Select the box “Certification Authority” and press “Next” to continue.



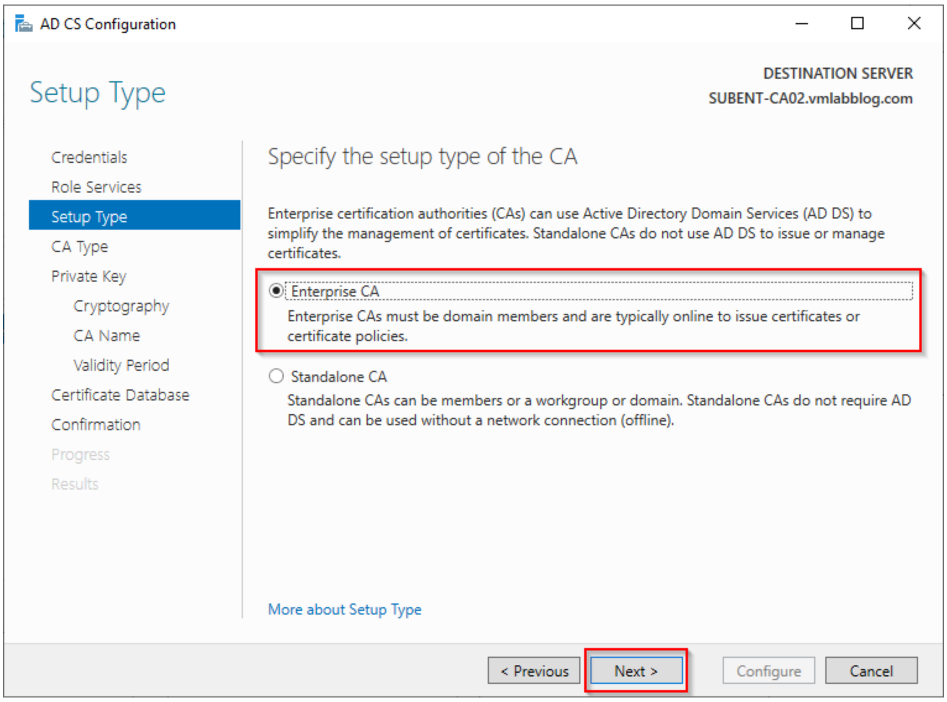
Role Services

DESTINATION SERVER
SUBENT-CA02.vmlabblog.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

19. Select “Enterprise CA” and press “Next” to continue. (if Enterprise CA is not available check if the server is domain joined and the credentials entered in step 17)



Setup Type

DESTINATION SERVER
SUBENT-CA02.vmlabblog.com

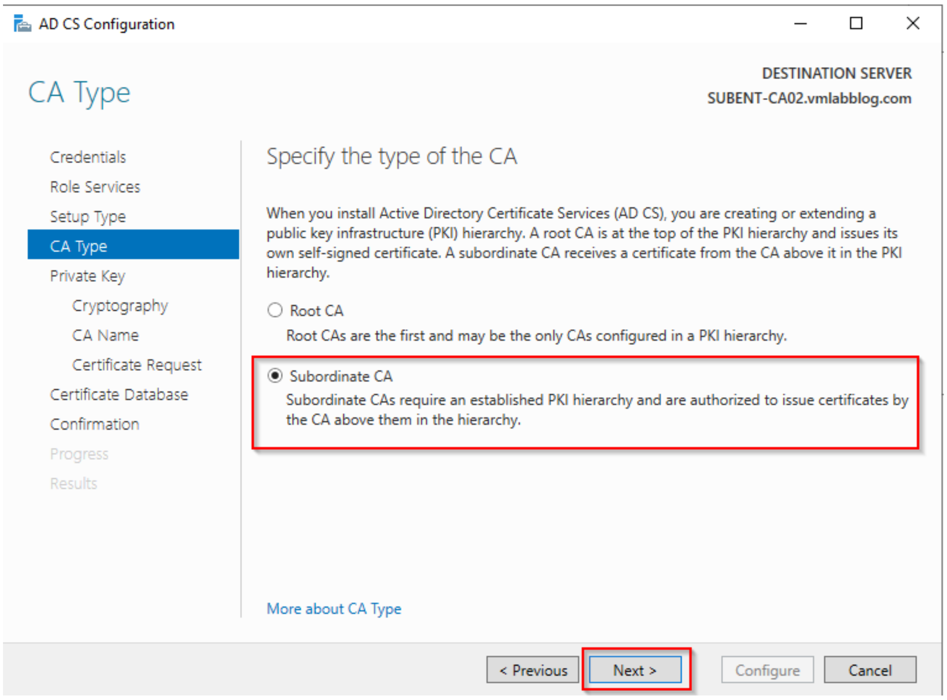
Specify the setup type of the CA

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).

20. Select “Subordinate CA” and press “Next” to continue.



AD CS Configuration

CA Type

DESTINATION SERVER
SUBENT-CA02.vmlabblog.com

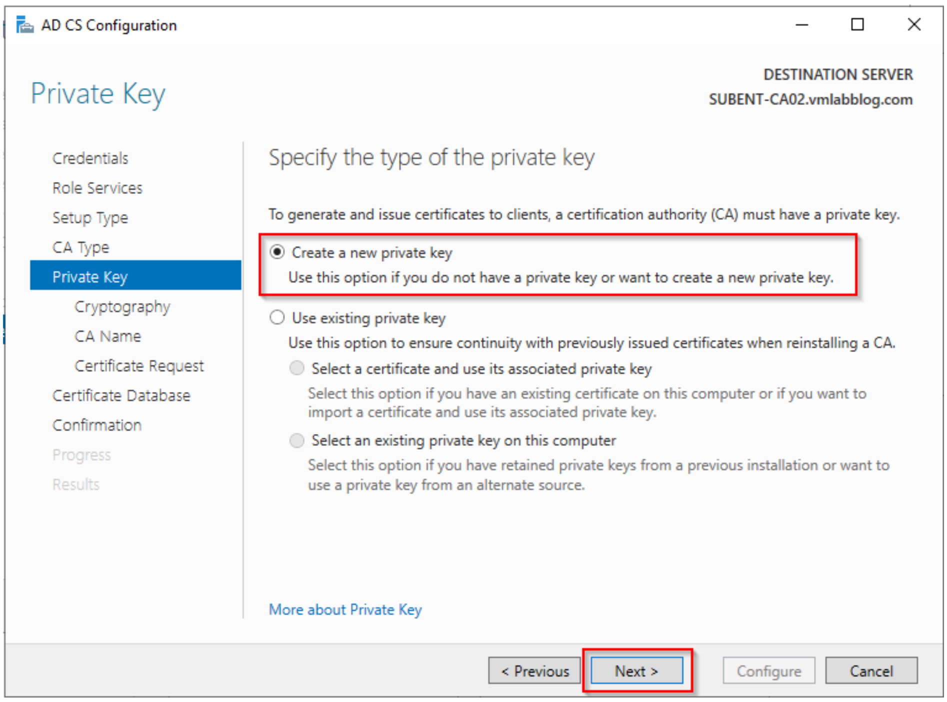
Specify the type of the CA

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.

21. Select “Create a new private key” and press “Next”.



AD CS Configuration

Private Key

DESTINATION SERVER
SUBENT-CA02.vmlabblog.com

Specify the type of the private key

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

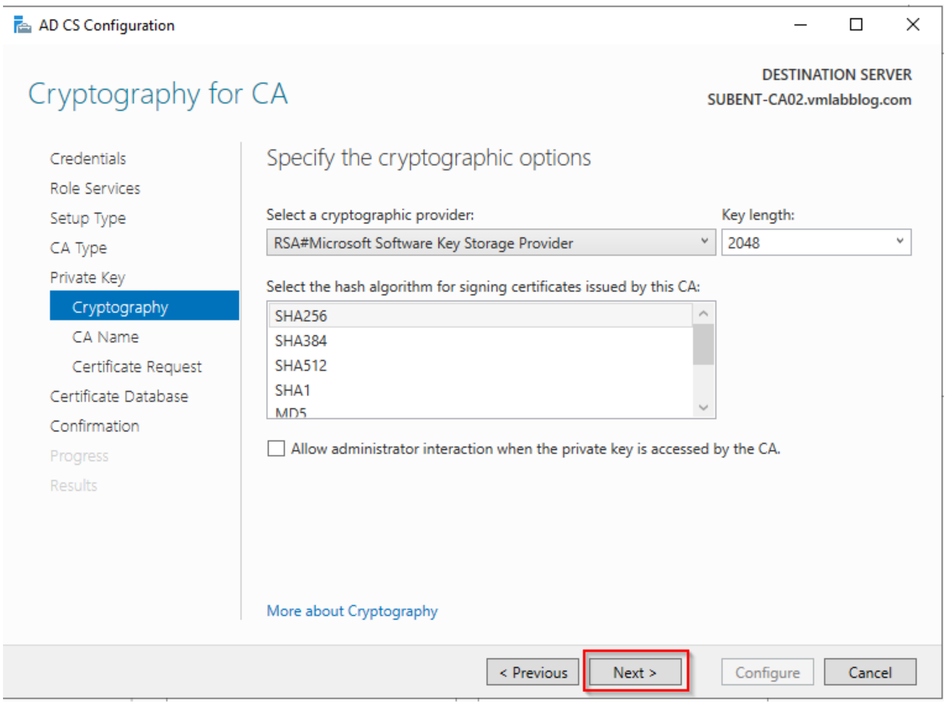
● Create a new private key
Use this option if you do not have a private key or want to create a new private key.

○ 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.

22. Use the default settings and press “Next” to continue.


AD CS Configuration

Cryptography for CA

DESTINATION SERVER
SUBENT-CA02.vmlabblog.com

Specify the cryptographic options

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

Key length: 2048

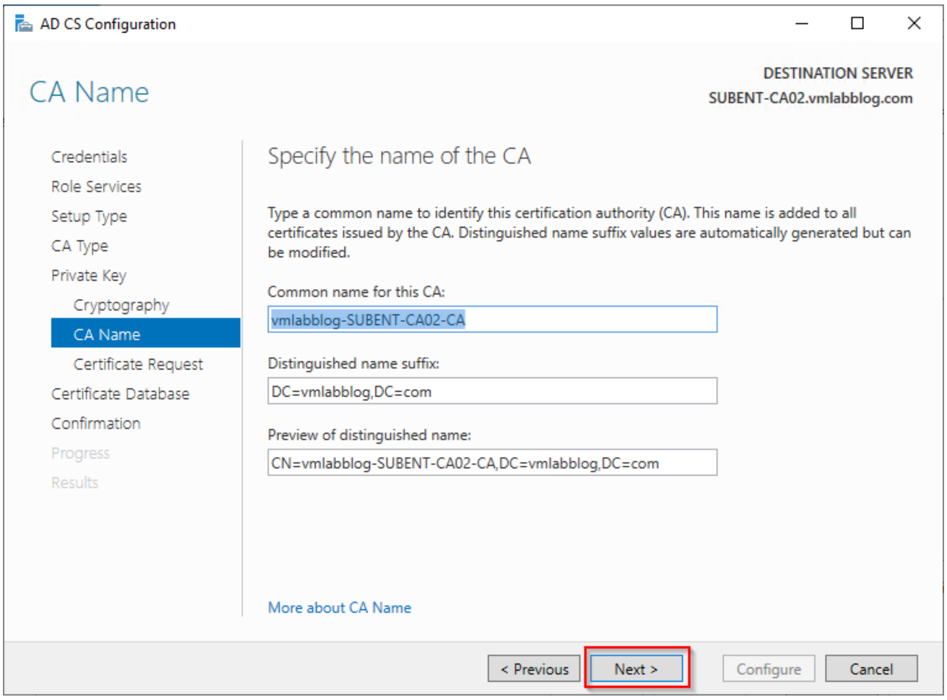
Select the hash algorithm for signing certificates issued by this CA:

SHA256
SHA384
SHA512
SHA1
MD5

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

More about Cryptography

23. Use the default settings and press “Next” to continue


AD CS Configuration

CA Name

DESTINATION SERVER
SUBENT-CA02.vmlabblog.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.

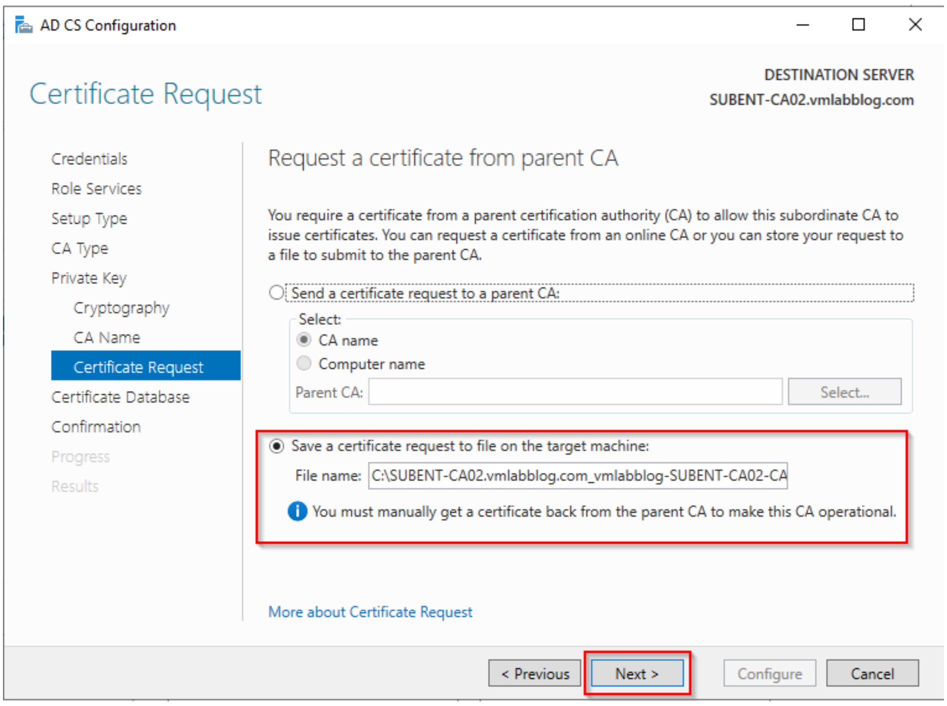
Common name for this CA: vmlabblog-SUBENT-CA02-CA

Distinguished name suffix: DC=vmlabblog,DC=com

Preview of distinguished name: CN=vmlabblog-SUBENT-CA02-CA,DC=vmlabblog,DC=com

More about CA Name

24. Select the folder to save the Certificate Request and press “Next” to continue. (default is “c:\”)



Certificate Request

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

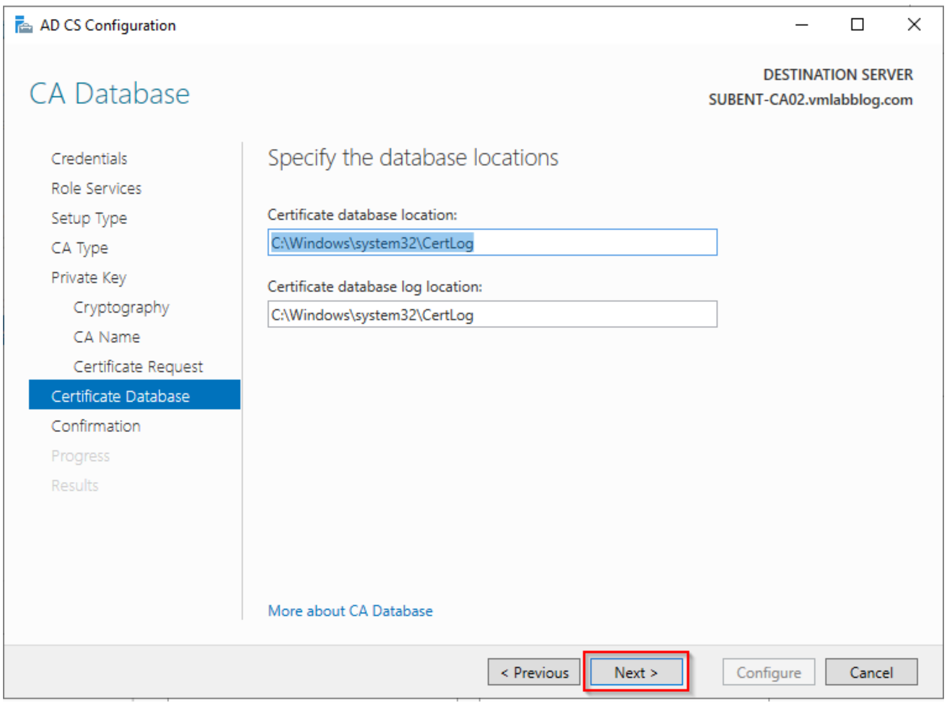
Parent CA:

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

File name: C:\SUBENT-CA02.vmlabblog.com_vmlabblog-SUBENT-CA02-CA

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

25. Use the default settings and press “Next” to continue.



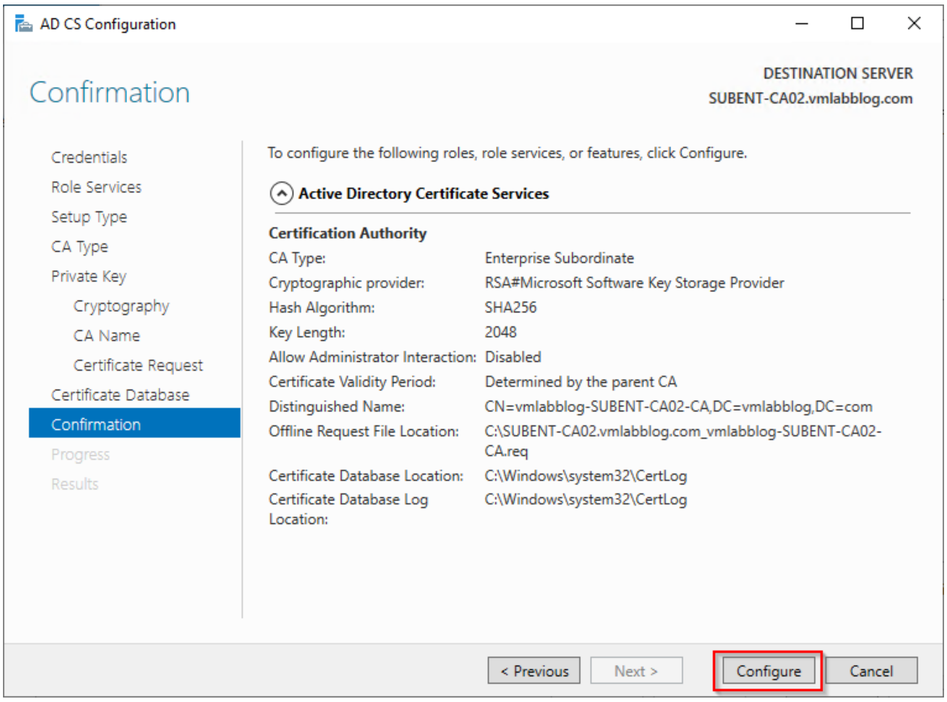
CA Database

Specify the database locations

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

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

26. Press “Configure” to apply the configuration.



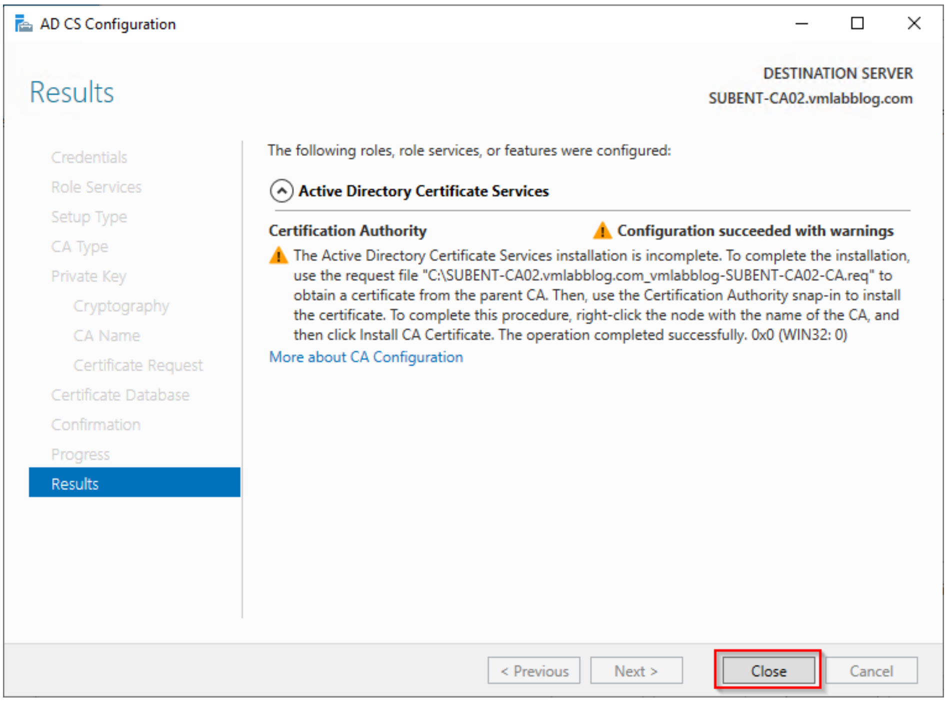
To configure the following roles, role services, or features, click Configure.

Active Directory Certificate Services

Certification Authority

CA Type: Enterprise Subordinate
Cryptographic provider: RSA#Microsoft Software Key Storage Provider
Hash Algorithm: SHA256
Key Length: 2048
Allow Administrator Interaction: Disabled
Certificate Validity Period: Determined by the parent CA
Distinguished Name: CN=vmlabblog-SUBENT-CA02-CA,DC=vmlabblog,DC=com
Offline Request File Location: C:\SUBENT-CA02.vmlabblog.com_vmlabblog-SUBENT-CA02-CA.req
Certificate Database Location: C:\Windows\system32\CertLog
Certificate Database Log Location: C:\Windows\system32\CertLog

27. When the configuration has succeeded a warning is shown. This is just a notification that the untill a certificate of the RootCA has been obtained and applied to the subordinate ca the Configuration is not completed.



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

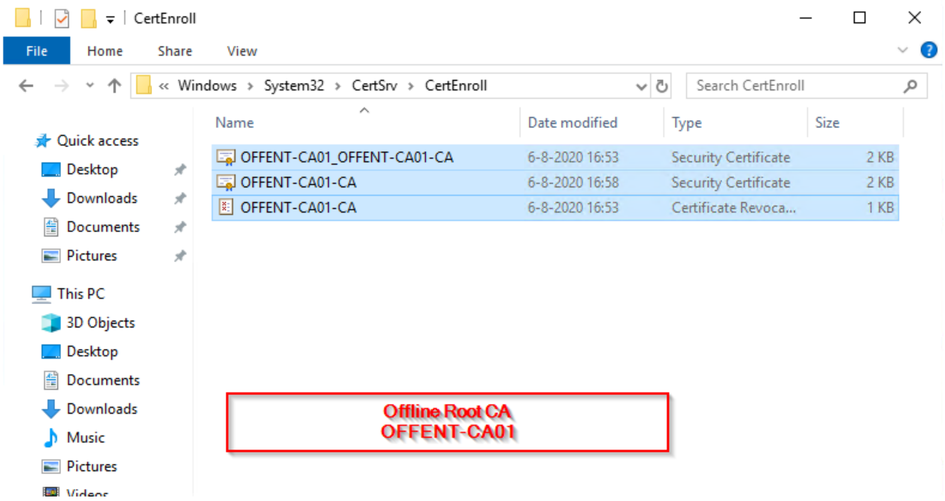
Active Directory Certificate Services

Certification Authority ⚠ Configuration succeeded with warnings

⚠ The Active Directory Certificate Services installation is incomplete. To complete the installation, use the request file "C:\SUBENT-CA02.vmlabblog.com_vmlabblog-SUBENT-CA02-CA.req" to obtain a certificate from the parent CA. Then, use the Certification Authority snap-in to install the certificate. To complete this procedure, right-click the node with the name of the CA, and then click Install CA Certificate. The operation completed successfully. 0x0 (WIN32: 0)

More about CA Configuration

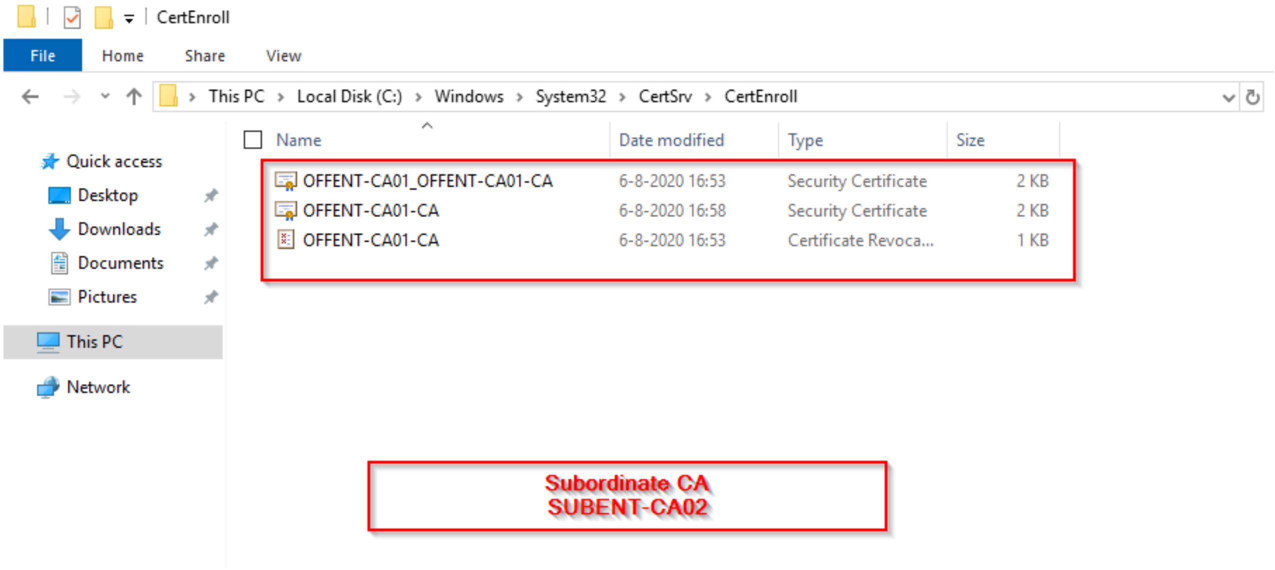
28. Switch over to the Offline Root CA (OFFENT-CA01) and browse to the folder “c:\windows\system32\certsrv\certenroll”. There should be three files, select and copy all files.



Name	Date modified	Type	Size
OFFENT-CA01_OFFENT-CA01-CA	6-8-2020 16:53	Security Certificate	2 KB
OFFENT-CA01-CA	6-8-2020 16:58	Security Certificate	2 KB
OFFENT-CA01-CA	6-8-2020 16:53	Certificate Revoca...	1 KB

Offline Root CA
OFFENT-CA01

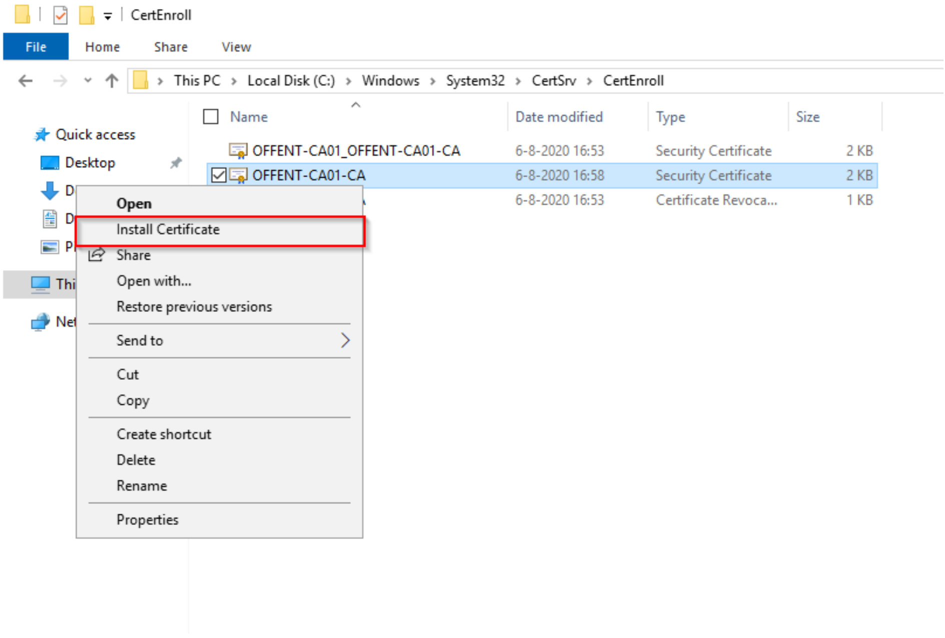
29. Switch back to the Subordinate CA (SUBENT-CA02) and browse to the folder “c:\windows\system32\certsrv\certenroll”. Paste all the files copied in the previous step.



Name	Date modified	Type	Size
OFFENT-CA01_OFFENT-CA01-CA	6-8-2020 16:53	Security Certificate	2 KB
OFFENT-CA01-CA	6-8-2020 16:58	Security Certificate	2 KB
OFFENT-CA01-CA	6-8-2020 16:53	Certificate Revoca...	1 KB

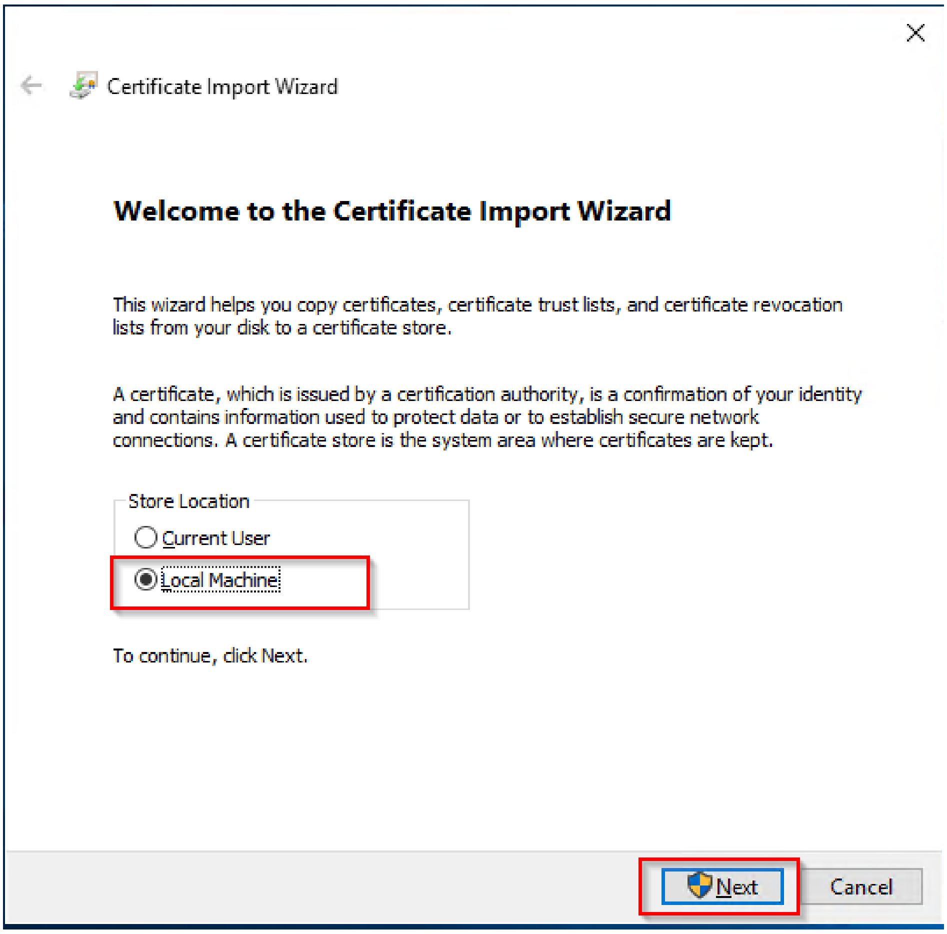
Subordinate CA
SUBENT-CA02

30. Rightclick the Root CA certificate which you just copied and select “Install Certificate”



Name	Date modified	Type	Size
OFFENT-CA01_OFFENT-CA01-CA	6-8-2020 16:53	Security Certificate	2 KB
☑ OFFENT-CA01-CA	6-8-2020 16:58	Security Certificate	2 KB
	6-8-2020 16:53	Certificate Revoca...	1 KB

31. Select “Local Machine” and press “Next”



Welcome to the Certificate Import Wizard

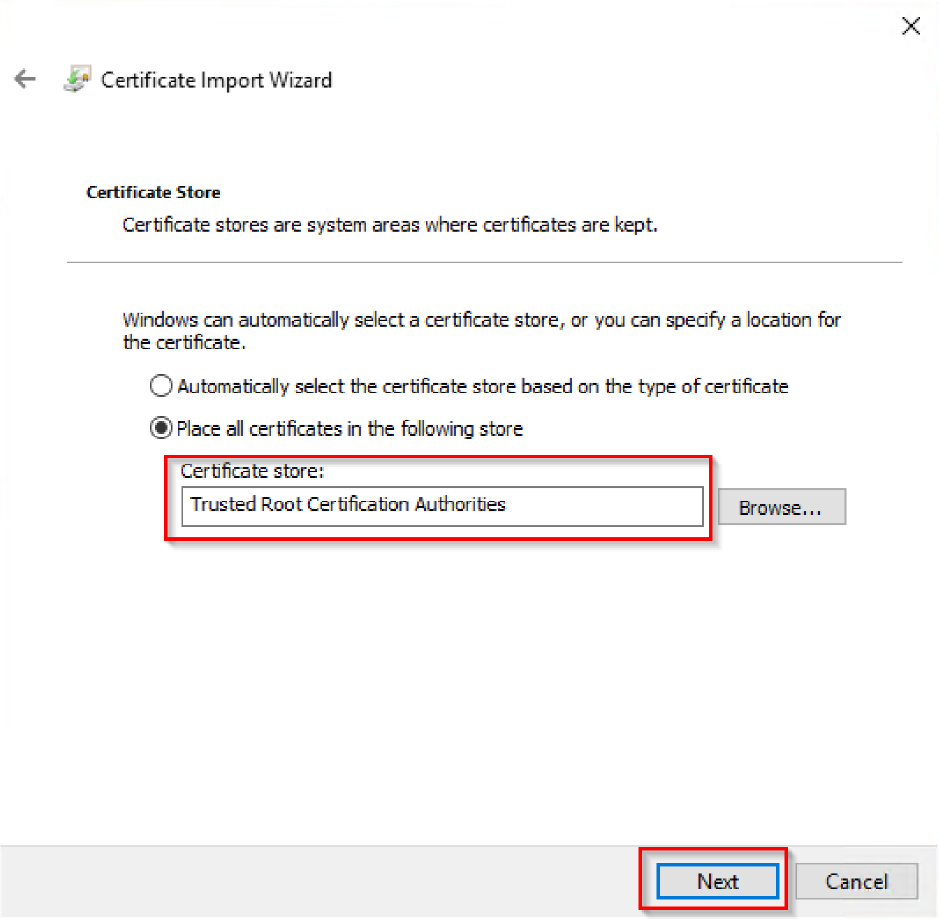
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

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

Store Location
○ Current User
● Local Machine

To continue, click Next.

32. Press “Browse” and select the “Trusted Root Certification Authorities” store. Press “Next” to continue.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

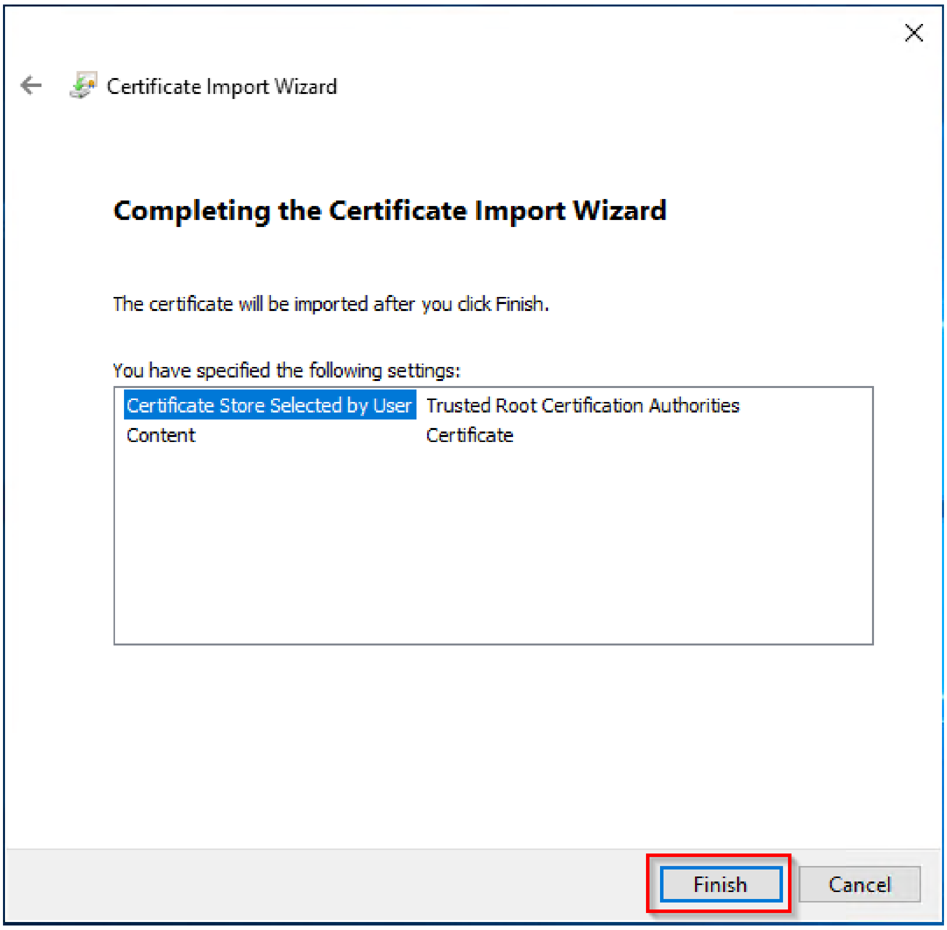
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

33. Press “Finish” to continue.



Certificate Import Wizard

Completing the Certificate Import Wizard

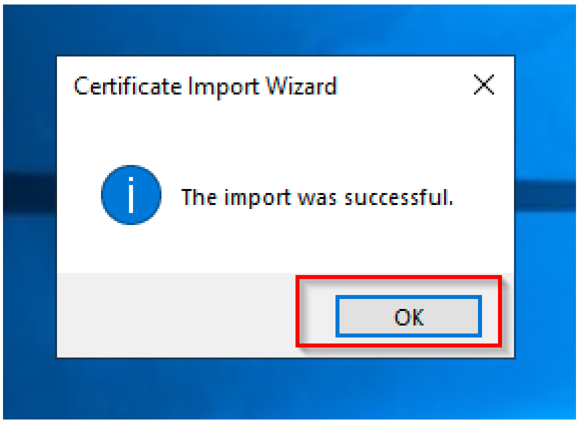
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

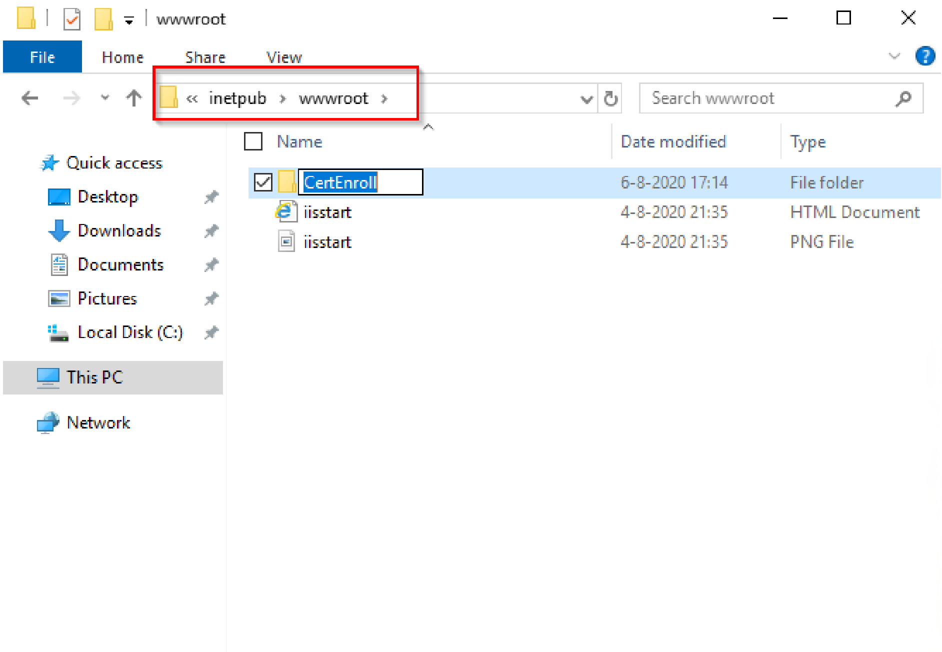
34. After some time a popup will appear when the import has finished. Press “OK” to continue

35. Create a new folder in “C:\inetpub\wwwroot” with the name “CertEnroll”



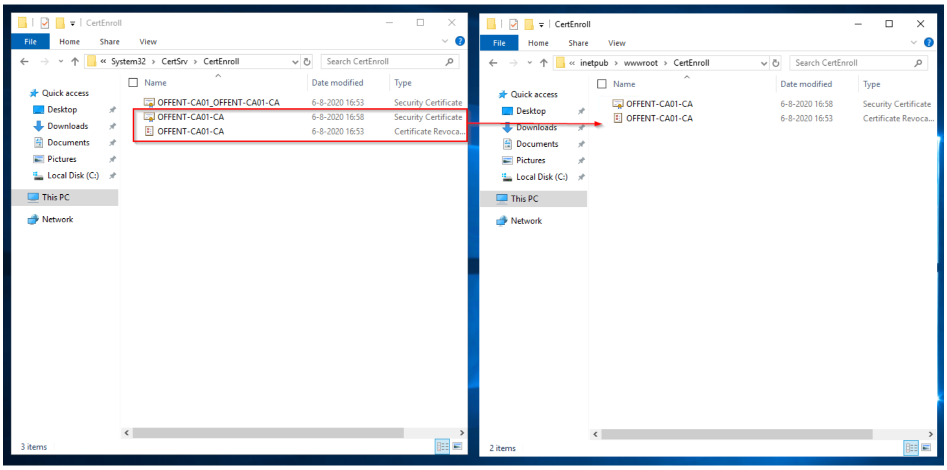
Certificate Import Wizard

The import was successful.



Name	Date modified	Type
☑ CertEnroll	6-8-2020 17:14	File folder
iisstart	4-8-2020 21:35	HTML Document
iisstart	4-8-2020 21:35	PNG File

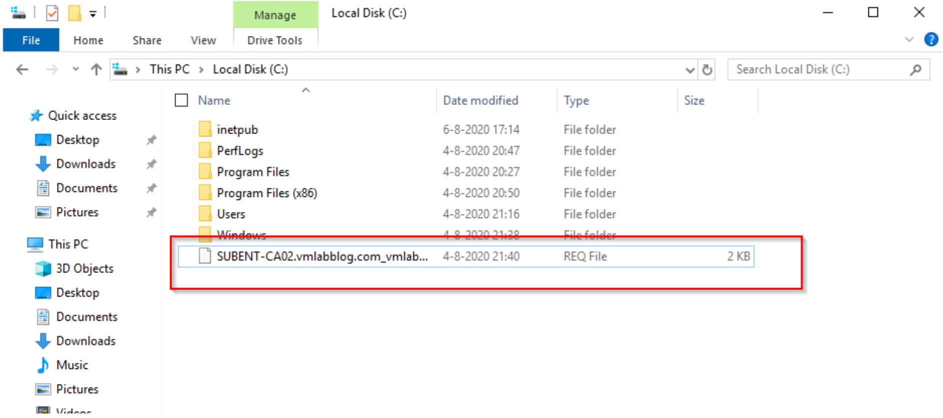
36. Copy the RootCA Certificate and Certifate Revocation List from “C:\Windows\System32\CertSrv\CertEnroll” to “C:\inetpub\wwwroot\CertEnroll”



Name	Date modified	Type
OFFENT-CA01_OFFENT-CA01-CA	6-8-2020 16:53	Security Certificate
OFFENT-CA01-CA	6-8-2020 16:58	Security Certificate
OFFENT-CA01-CA	6-8-2020 16:53	Certificate Revoca...

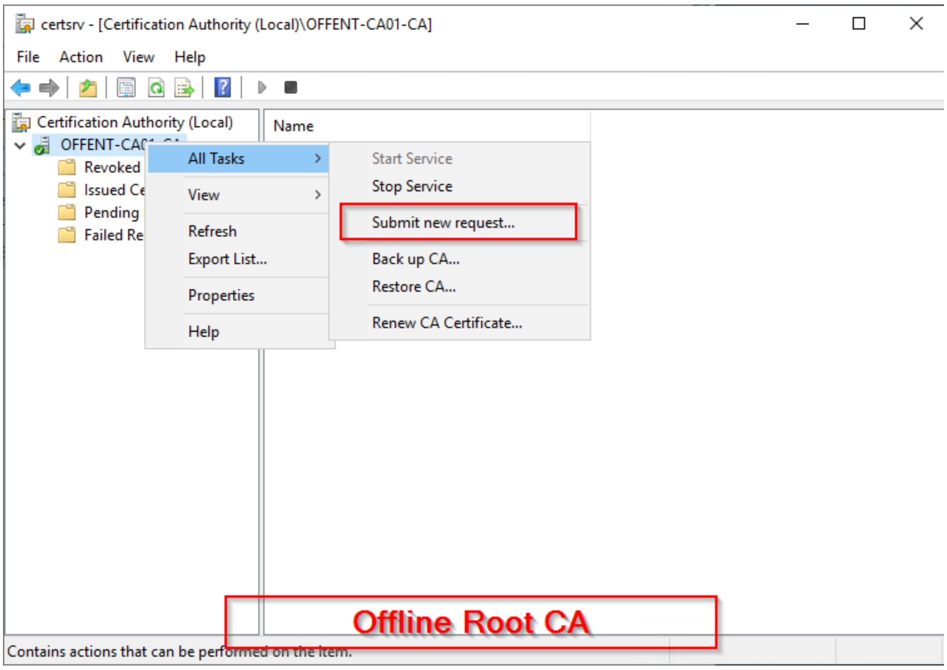
Name	Date modified	Type
OFFENT-CA01-CA	6-8-2020 16:58	Security Certificate
OFFENT-CA01-CA	6-8-2020 16:53	Certificate Revoca...

37. Browse to the location entered in step 20 (default “c:\”) and copy the “*.Req” file to the C: Drive on RootCA server.



Name	Date modified	Type	Size
inetpub	6-8-2020 17:14	File folder	
PerfLogs	4-8-2020 20:47	File folder	
Program Files	4-8-2020 20:27	File folder	
Program Files (x86)	4-8-2020 20:50	File folder	
Users	4-8-2020 21:16	File folder	
Windows	4-8-2020 21:38	File folder	
SUBENT-CA02.vmlabblog.com_vmlab...	4-8-2020 21:40	REQ File	2 KB

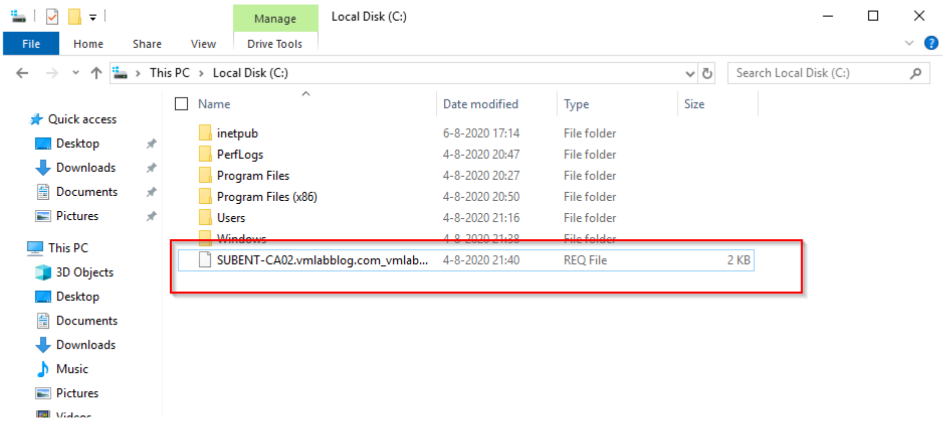
38. On the Root CA Server open ” Certification Authority” rightclick the servername and select “All Tasks” -> Submit new request…”



Offline Root CA

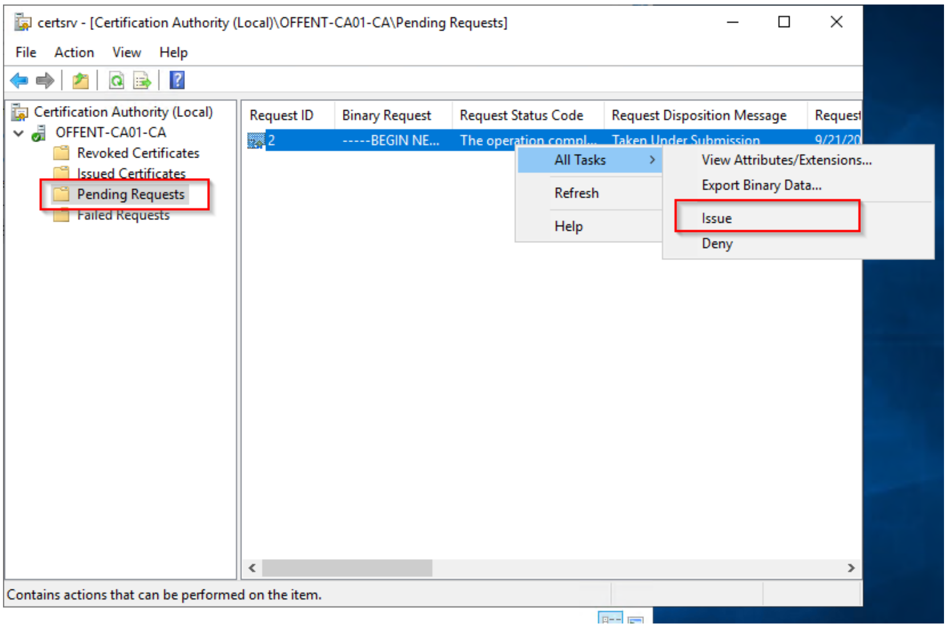
Contains actions that can be performed on the item.

39. Browse to the request file on the C: driver and press “Open”

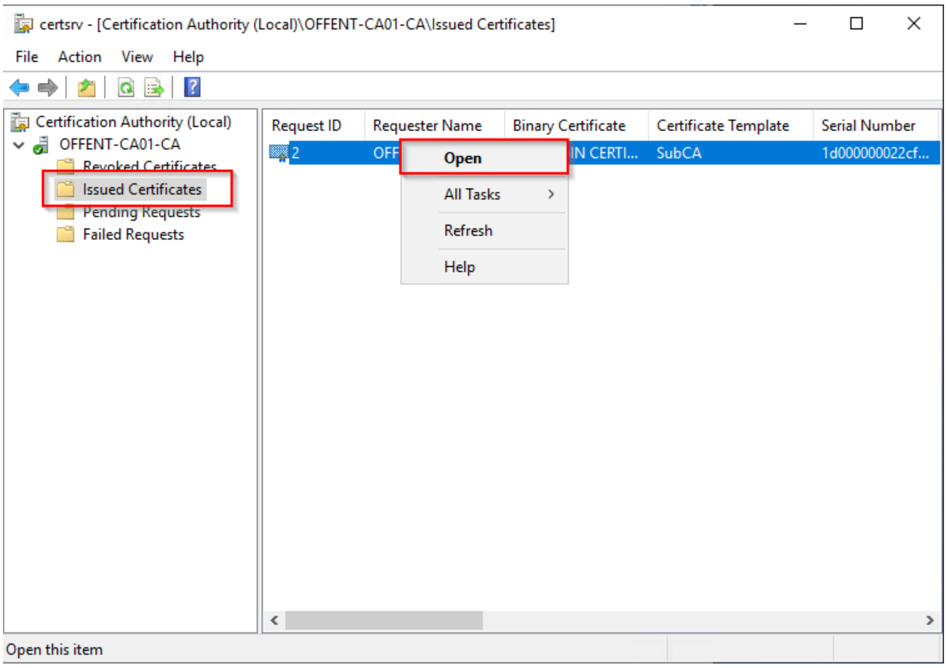


Name	Date modified	Type	Size
inetpub	6-8-2020 17:14	File folder	
PerfLogs	4-8-2020 20:47	File folder	
Program Files	4-8-2020 20:27	File folder	
Program Files (x86)	4-8-2020 20:50	File folder	
Users	4-8-2020 21:16	File folder	
Windows	4-8-2020 21:38	File folder	
SUBENT-CA02.vmlabblog.com_vmlab...	4-8-2020 21:40	REQ File	2 KB

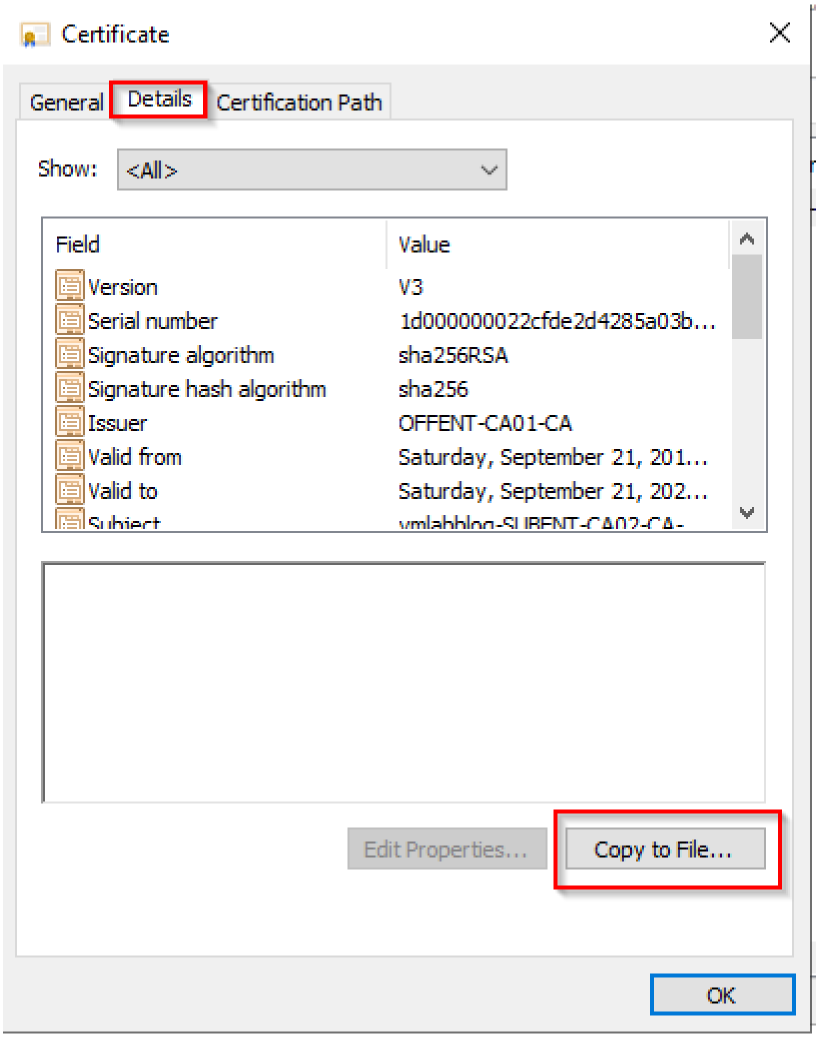
40. Select “Pending Requests”. Rightclick the pending request and select “All Tasks” -> “Issue”



41. Select “Issued Certificates”. Rightclick the issued certificate and select “Open”

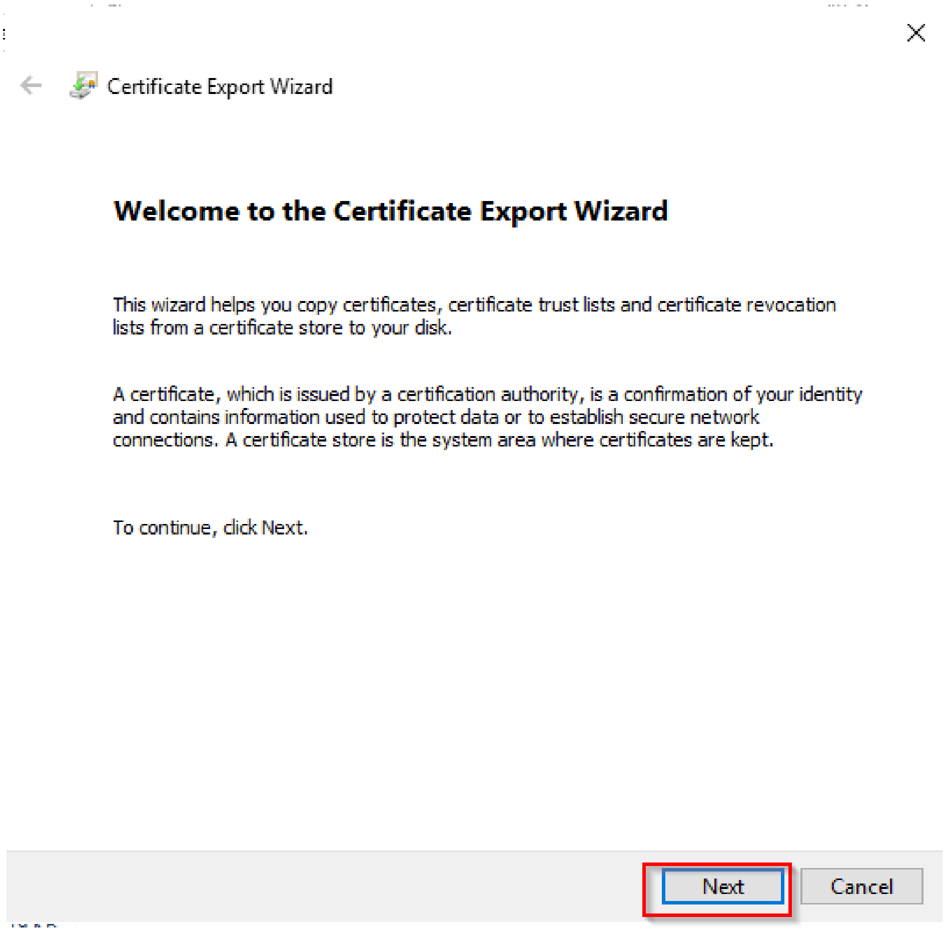


42. Select “Details” and press “Copy to file…”



Field	Value
Version	V3
Serial number	1d000000022cfde2d4285a03b...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	OFFENT-CA01-CA
Valid from	Saturday, September 21, 201...
Valid to	Saturday, September 21, 202...
Subject	vmlabblog-SUBENT-CA02-CA-

43. Press “Next” to continue



Certificate Export Wizard

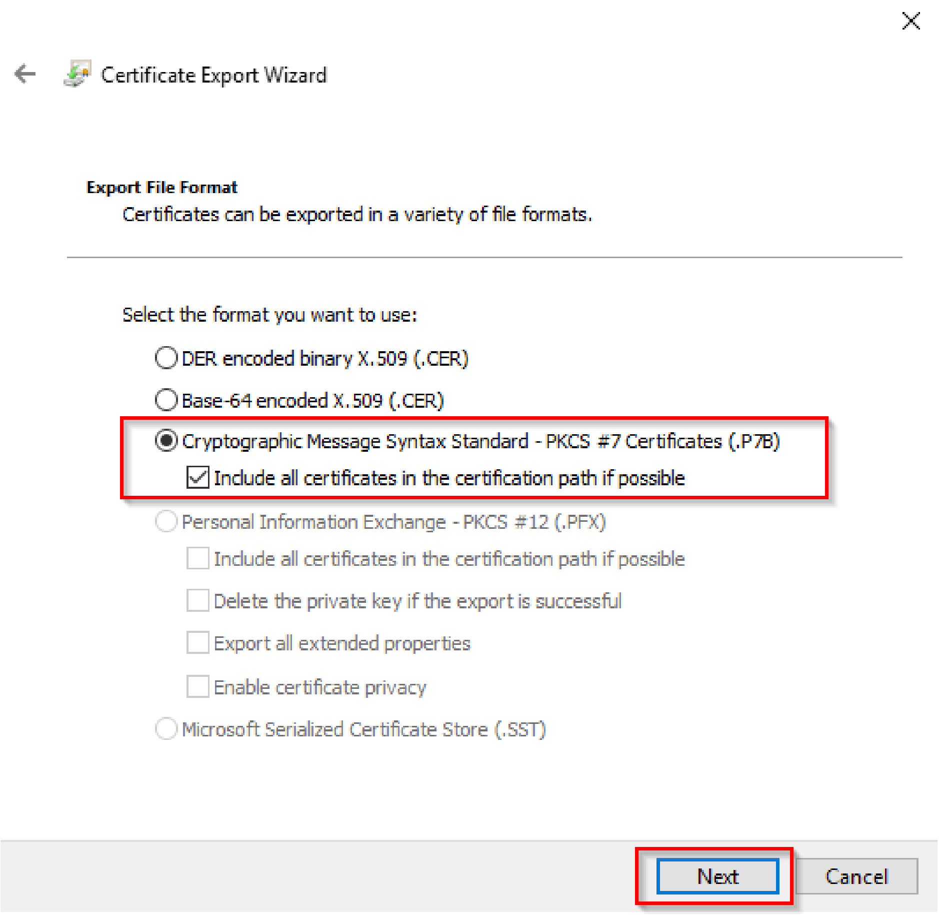
Welcome to the Certificate Export Wizard

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.

44. Select “Cryptographic Message Syntax Standard – PKCS #7 Certificates (.P7B)” and check the box “Include all certificates in the certification path if possible”. Press “Next” to continue.



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

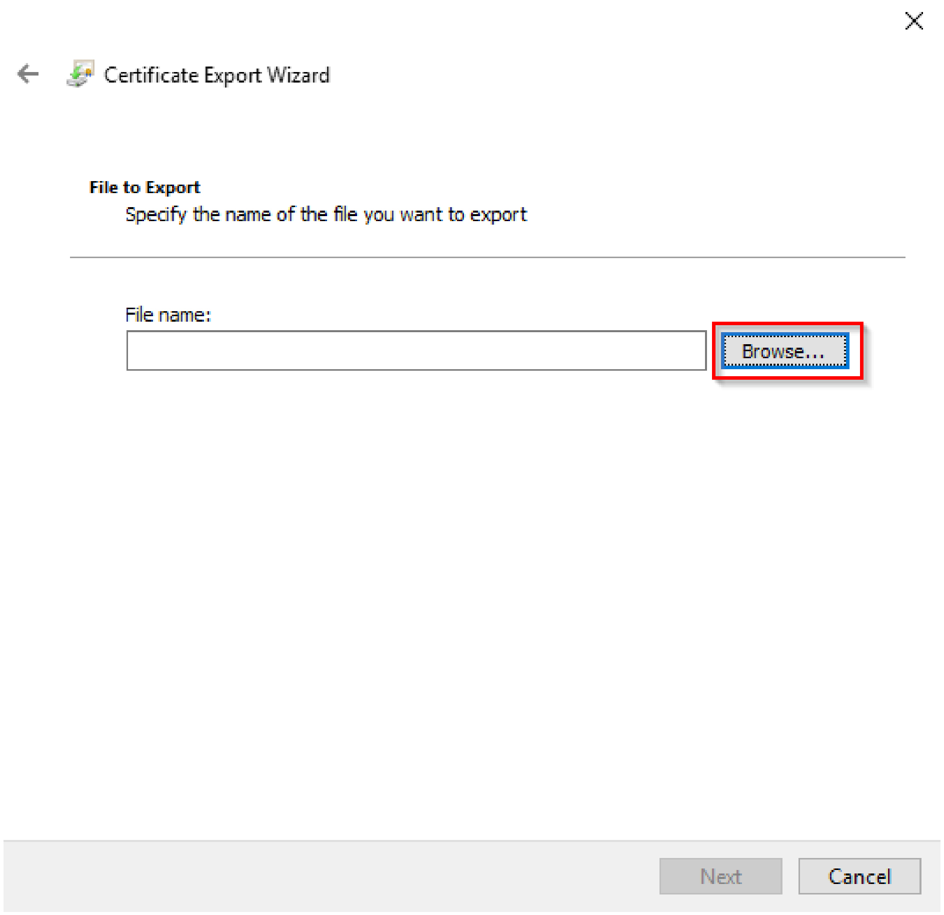
□ Delete the private key if the export is successful

□ Export all extended properties

□ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

45. Press “Browse…”



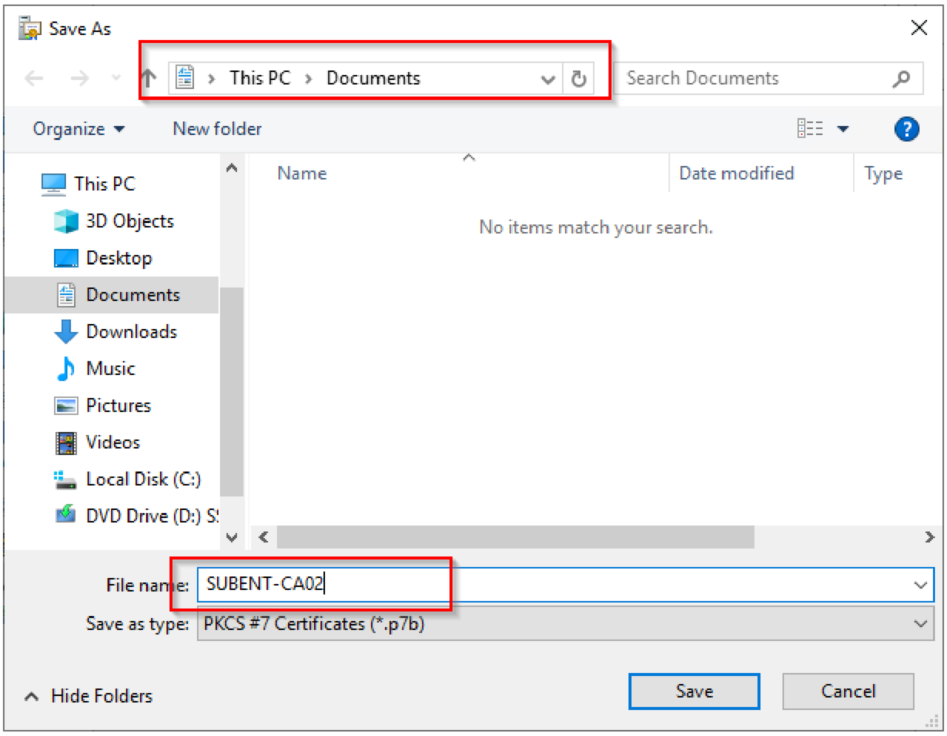
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:

46. Enter a name for the certificate and press “Save” (the default location is the Documents folder)



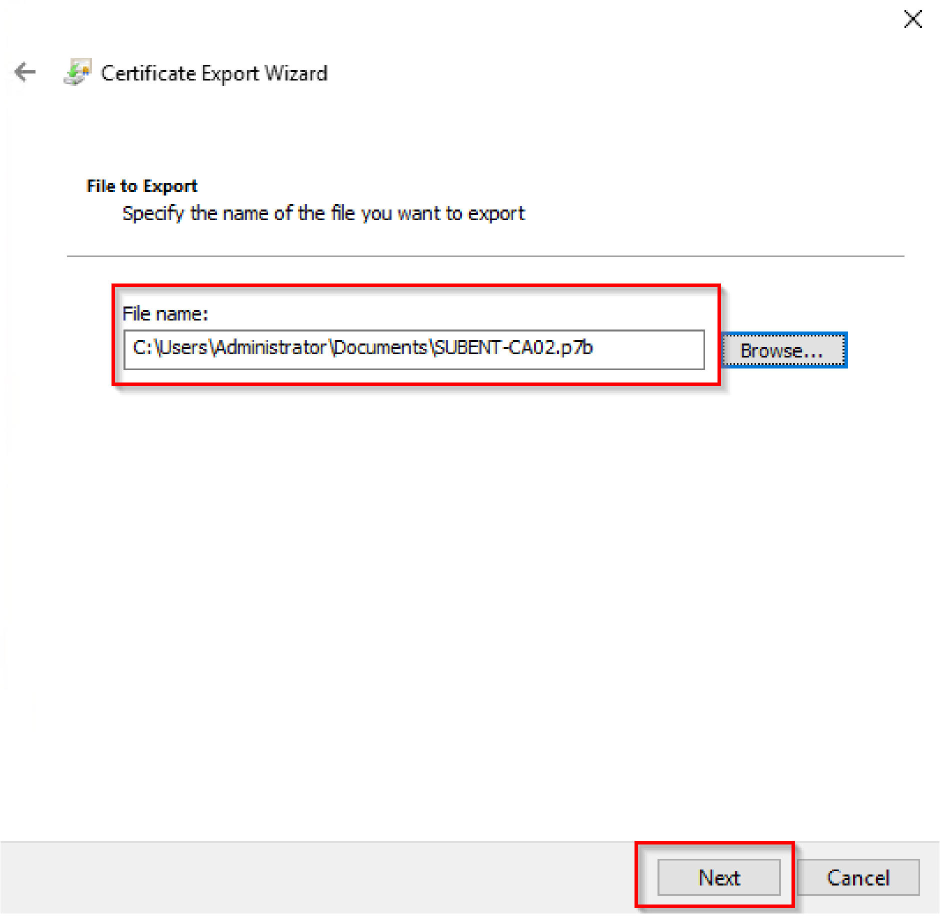
This PC › Documents

No items match your search.

File name: SUBENT-CA02

Save as type: PKCS #7 Certificates (*.p7b)

47. Press “Next” to continue.



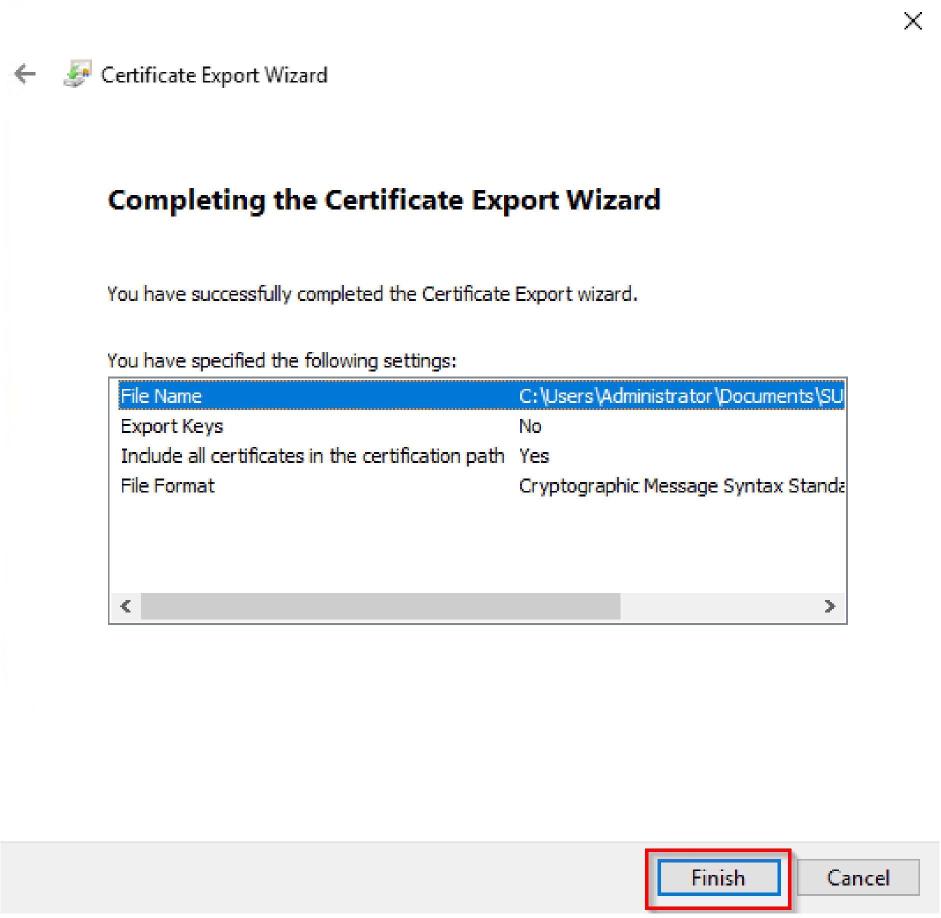
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name: C:\Users\Administrator\Documents\SUBENT-CA02.p7b

48. Press “Finish” to export the CA Certificate.



Certificate Export Wizard

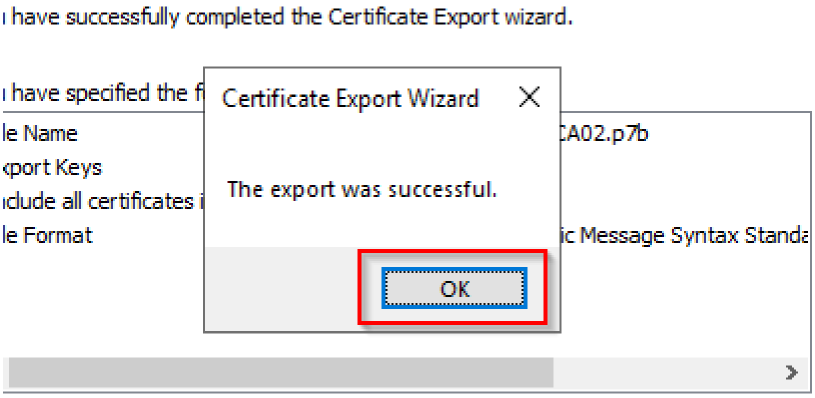
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Users\Administrator\Documents\SU
Export Keys	No
Include all certificates in the certification path	Yes
File Format	Cryptographic Message Syntax Standa

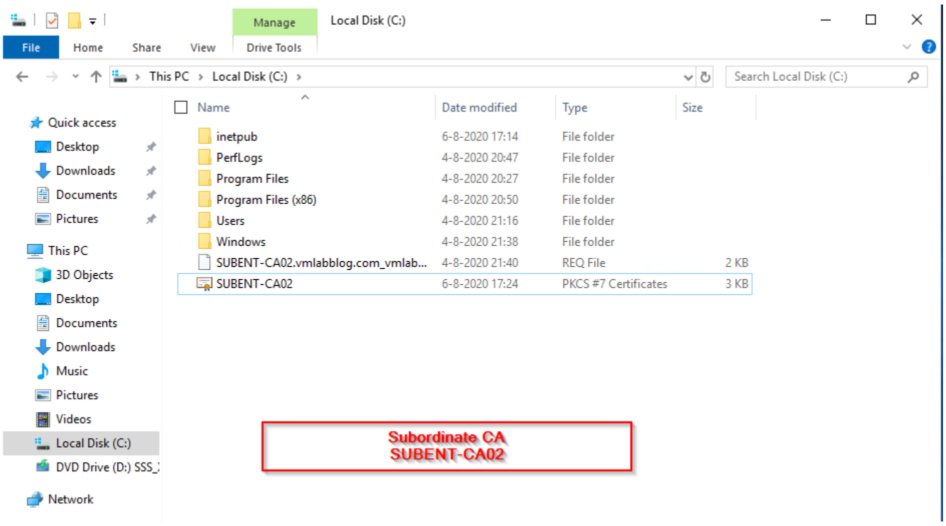
49. After some time a popup will appear when the export has finished. Press “OK” to continue.



Certificate Export Wizard

The export was successful.

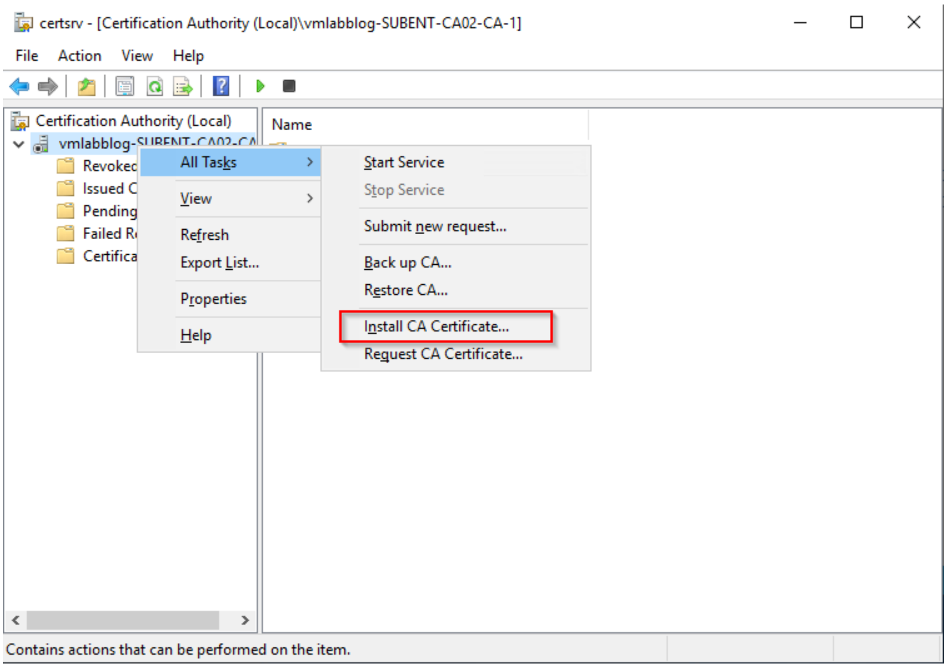
50. Copy the CA Certificate from the RootCA (step 46) and switch to the subordinate server to paste the file.



Name	Date modified	Type	Size
inetpub	6-8-2020 17:14	File folder	
PerfLogs	4-8-2020 20:47	File folder	
Program Files	4-8-2020 20:27	File folder	
Program Files (x86)	4-8-2020 20:50	File folder	
Users	4-8-2020 21:16	File folder	
Windows	4-8-2020 21:38	File folder	
SUBENT-CA02.vmlabblog.com_vmlab...	4-8-2020 21:40	REQ File	2 KB
SUBENT-CA02	6-8-2020 17:24	PKCS #7 Certificates	3 KB

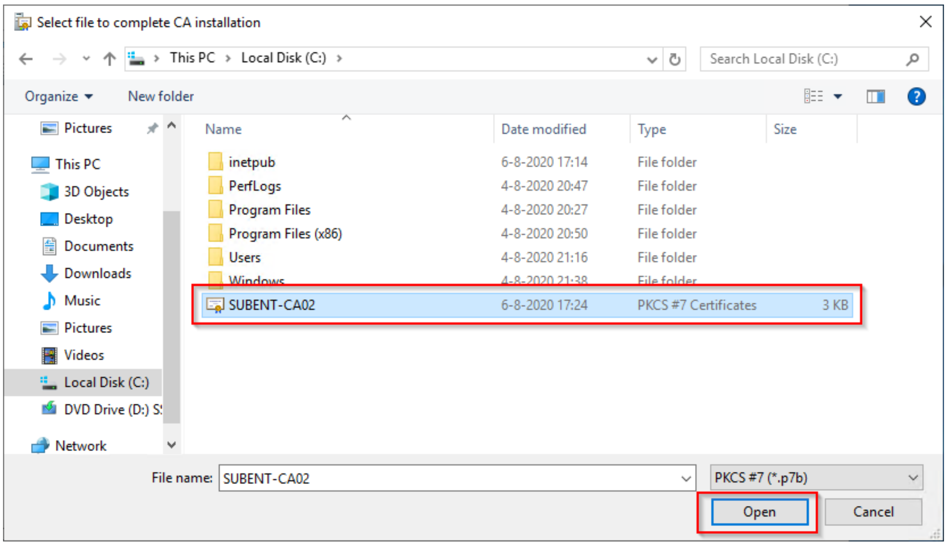
Subordinate CA
SUBENT-CA02

51. On the Subordinate CA open the Certification Authority. Rightclick the Servername and select “All Tasks” -> “Install CA Certificate”


certsrv - [Certification Authority (Local)\vmlabblog-SUBENT-CA02-CA-1]

Contains actions that can be performed on the item.

52. Select the copied CA Certificate and press “Open”

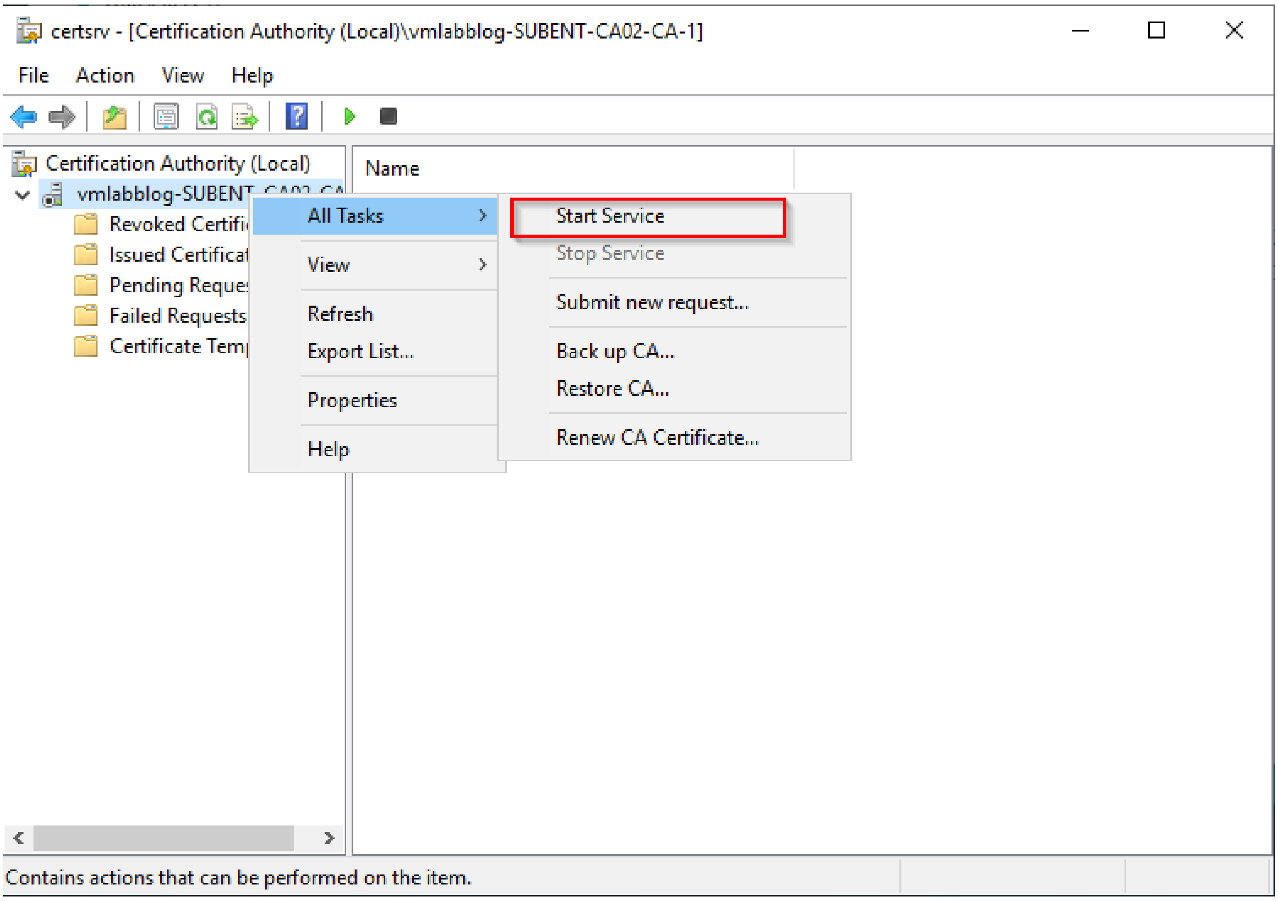


Name	Date modified	Type	Size
inetpub	6-8-2020 17:14	File folder	
PerfLogs	4-8-2020 20:47	File folder	
Program Files	4-8-2020 20:27	File folder	
Program Files (x86)	4-8-2020 20:50	File folder	
Users	4-8-2020 21:16	File folder	
Windows	4-8-2020 21:38	File folder	
SUBENT-CA02	6-8-2020 17:24	PKCS #7 Certificates	3 KB

File name: SUBENT-CA02

PKCS #7 (*.p7b)

53. Rightclick the Servername and select “All Tasks” -> “Start Service”



Contains actions that can be performed on the item.

The setup of the Subordinate CA is now completed

Next: Setup Group Policy