The objective of this lab is to provide students with hands-on experience in deploying a Public Key Infrastructure (PKI) using Active Directory Certificate Services (AD CS).

Lab Assignment 3 (Part I) - GPO420-636-AB-Network Installationand Administration II

Teacher: Antoine Tohme
Student: Monica Perez Mata
Student id : 2498056

Table of Contents

Lab Assignment 3 (Part I) – Deploying a Certificate Authority Server

1 Lab Objective

The objective of this lab is to provide students with hands-on experience in deploying a **Public Key Infrastructure (PKI)** using **Active Directory Certificate Services (AD CS)**.

By the end of this lab, you should be able to:

- Deploy a **Standalone Root CA** in an **offline** environment.
- Deploy an **Enterprise Subordinate CA** that integrates with **Active Directory**.
- Configure the **Root CA to issue a certificate** for the Subordinate CA.
- Enable secure **certificate issuance and management** in an AD domain.

2 Lab Environment Requirements

- **DC101** → Online **Enterprise Subordinate CA** (Domain-joined)
- **DC201** → Offline **Standalone Root CA** (Not domain-joined)

3 Task 1: Deploy an Offline Standalone Root CA on DC201

3.1 Install DC225.

On DC101

```
# Step 3: Remove the Computer Object from AD (On DC101)
# Run this command on the domain controller (DC101) to delete the object from Active Directory:
Get-ADComputer DC201 | Remove-ADObject -Recursive -Confirm:$false
```

```
# RUN FROM DC101
# Step 4: Remove the Server from AD Sites and Services (On Active Directory DC101)
Set-Location AD:
Remove-Item -Path "AD:\CN=DC201,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs1,DC=com" -Force
exit
```

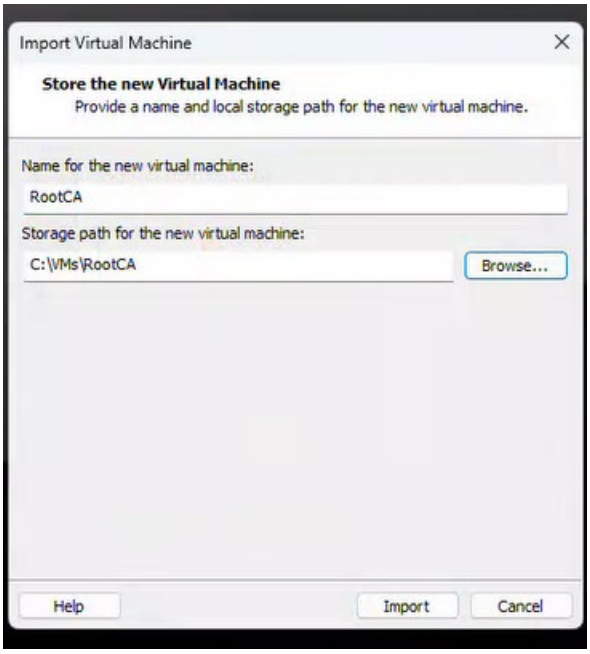
```
PS C:\Users\Administrator> Get-ADComputer DC201 | Remove-ADObject -Recursive -Confirm:$false
```

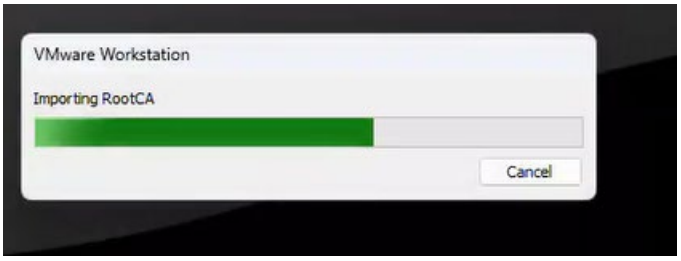
Download and import the DC225 VM using the following link:
https://johnabbott-my.sharepoint.com/:f:/g/personal/antoine_tohme_johnabbott_qc_ca/EoLwKowRqTxCnLP6lffX3XcBj-7MbN9qCICvM8EuBc-ntA?e=k2wi1N

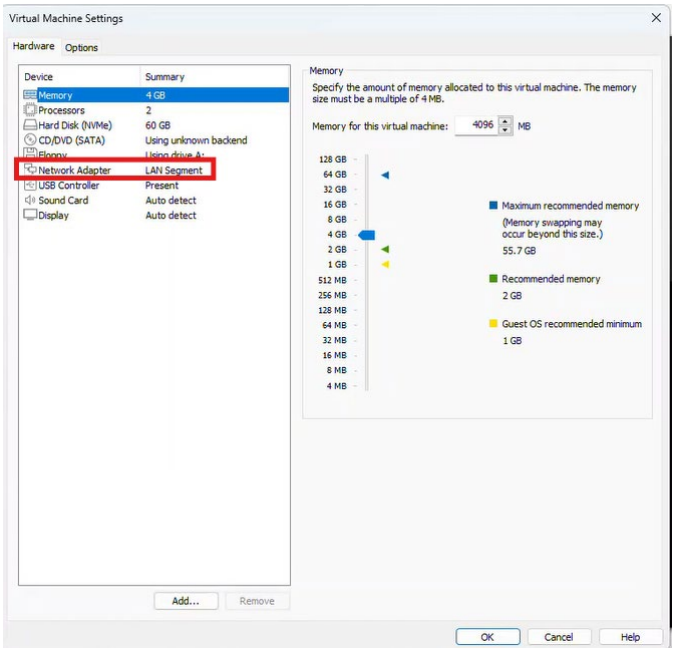
Before starting the VM, make sure to:

- Modify the NIC setting to **LAN1**
- Assign an IP address that matches your current LAN IP range.

Additionally, you'll need to remove the old DC2XX object from the domain.







Change IP and DNS

netsh interface ipv4 set address name="Ethernet0" static 192.168.1.2 255.255.255.0 192.168.1.50

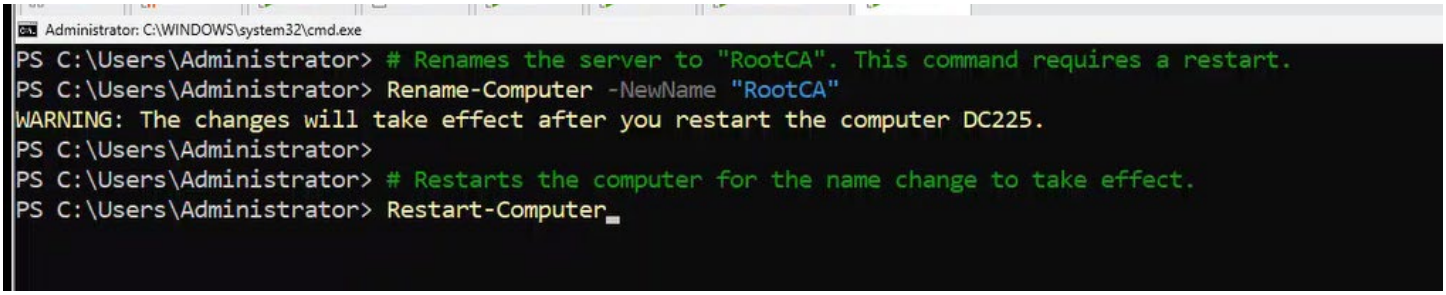
netsh interface ipv4 set dns name="Ethernet0" static 192.168.1.1

3.2 Rename DC225 to RootCA.

Rename the Server to RootCA (Run on DC201)

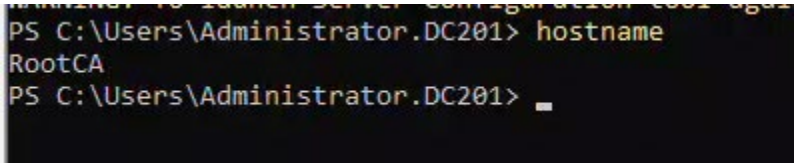
Purpose: Change the hostname from DC201 to RootCA to align with the lab's naming for the offline Root CA. (Run on DC201

```
# Renames the server to "RootCA". This command requires a restart.
Rename-Computer -NewName "RootCA"

# Restarts the computer for the name change to take effect.
Restart-Computer
```



Restart initiates

Check hostname



3.3 Install Active Directory Certificate Services (AD CS) on RootCA.

```
# Install Active Directory Certificate Services (AD CS) on Windows Server Core:
Add-WindowsFeature Adcs-Cert-Authority
Get-WindowsFeature AD-Certificate
```

Installs the AD CS role to set up a certification authority.
Verify that the installation was successful.

```
PS C:\Users\Administrator> # Install Active Directory Certificate Services (AD CS) on Windows Server Core:
PS C:\Users\Administrator> Add-WindowsFeature Adcs-Cert-Authority

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Certificate Services, Ce...


PS C:\Users\Administrator> Get-WindowsFeature AD-Certificate

Display Name                                            Name                       Install State
------------                                            ----                       -------------
[X] Active Directory Certificate Services               AD-Certificate                 Installed


PS C:\Users\Administrator>
```

Verify IP Configuration

 # Confirm IP Configuration

Get-NetIPAddress -InterfaceAlias "Ethernet0" | Format-Table InterfaceAlias, IPAddress, PrefixLength

Get-DnsClientServerAddress -InterfaceAlias "Ethernet0"

Test-Connection -ComputerName 192.168.1.1 -Count 2

```
   NetBIOS over Tcpip. . . . . . . . : Enabled
PS C:\Users\Administrator> # Confirm IP Configuration
PS C:\Users\Administrator> Get-NetIPAddress -InterfaceAlias "Ethernet0" | Format-Table InterfaceAlias, IPAddress, PrefixLength

InterfaceAlias IPAddress                  PrefixLength
-------------- ---------                  ------------
Ethernet0      fe80::8dda:2fc2:238d:9729%2          64
Ethernet0      192.168.1.2                          24


PS C:\Users\Administrator> Get-DnsClientServerAddress -InterfaceAlias "Ethernet0"

InterfaceAlias               Interface Address ServerAddresses
                             Index     Family
--------------               --------- ------- ---------------
Ethernet0                            2 IPv4    {192.168.1.1}
Ethernet0                            2 IPv6    {}


PS C:\Users\Administrator> Test-Connection -ComputerName 192.168.1.1 -Count 2

Source        Destination     IPV4Address      IPV6Address                              Bytes    Time(ms)
------        -----------     -----------      -----------                              -----    --------
ROOTCA        192.168.1.1     192.168.1.1                                               32       0
ROOTCA        192.168.1.1     192.168.1.1                                               32       0


PS C:\Users\Administrator>
PS C:\Users\Administrator>
```

 # Test DNS resolution

Resolve-DnsName -Name DC101.vlabs1.com -Server 192.168.1.1

```
PS C:\Users\Administrator>
PS C:\Users\Administrator> # Test DNS resolution
PS C:\Users\Administrator> Resolve-DnsName -Name DC101.vlabs1.com -Server 192.168.1.1

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
DC101.vlabs1.com                               A      3600  Answer     192.168.1.1


PS C:\Users\Administrator>
PS C:\Users\Administrator>
```

3.4 Configure RootCA as a Standalone Root CA.

3.4.1 Configure

 # Initialize the Standalone Root CA:
Install-AdcsCertificationAuthority -CAType StandaloneRootCA -CACommonName "RootCA" -KeyLength 4096 -HashAlgorithm SHA256 -CryptoProviderName "RSA#Microsoft Software Key Storage Provider"

Type: **A** (For Yes to all)CATypeshould be StandaloneRootCa

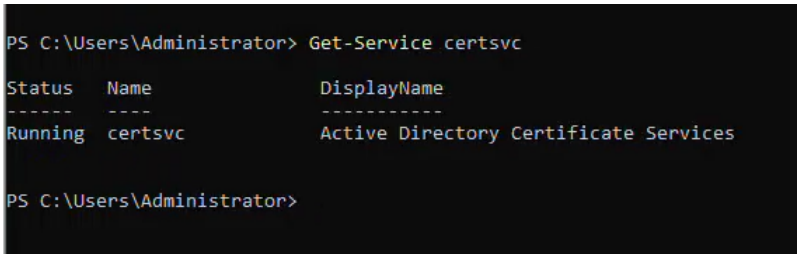
- **CACommonNameit** is the name of your RootCA
- Sets up the CA with **SHA-256** and a **4096**-bit key for security.
- Use the Microsoft RSA algorithm to create the private/public keys.

Now your Root CA is already up and running but needs some additional configuration.

3.4.2 Verify

Check the Certificate Authority Service Status
A running Certificate Authority service is the primary indicator that the CA has been successfully set up.

Get-Service certsvc



Verify the Root CA Certificate in the Certificate Store
The Install-AdcsCertificationAuthority command generates the Root CA's self-signed certificate. You can verify its presence in the local computer's certificate store.

Get-ChildItem Cert:\LocalMachine\Root | Where-Object {$_.Subject -like "CN=RootCA*" -and $_.Issuer -like "CN=RootCA*"}

```
PS C:\Users\Administrator> Get-ChildItem Cert:\LocalMachine\Root | Where-Object {$_.Subject -lik
e "CN=RootCA*" -and $_.Issuer -like "CN=RootCA*"}


   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\Root

Thumbprint                                Subject
----------                                -------
C9CA38C101211A5C0D5480F956D1B786B7C4C41B  CN=RootCA


PS C:\Users\Administrator>
```

3.5 Configure the Server Registry keys.

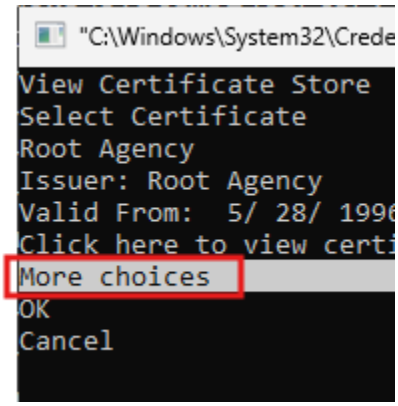
Manually configure CA distribution points in the Server Registry:

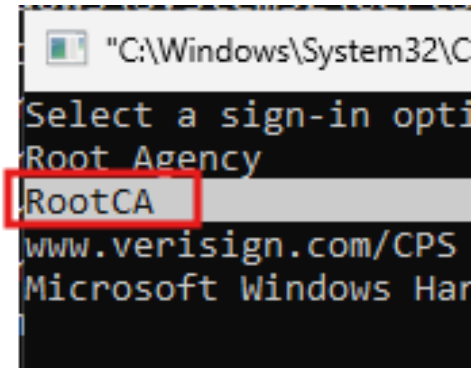
certutil -setreg CA\ValidityPeriod "Years"
certutil -setreg CA\ValidityPeriodUnits 5
certutil -setreg CA\DSConfigDN "CN=Configuration,DC=vlabs1,DC=com"
certutil -setreg CA\DSDomainDN "DC=vlabs1,DC=com"
Restart-Service certsvc

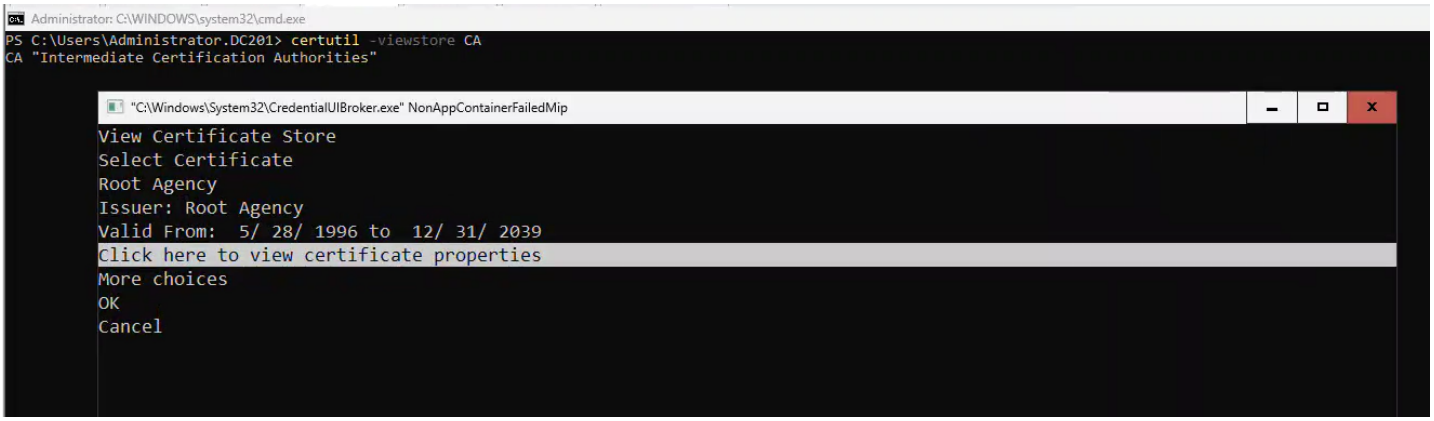
- ValidityPeriodis already default / just for confirmation
- ValidityPeriodUnitsto be 5 years not 1 year
- The DSConfigDNand DSDomainDNare important parameters for adding an Enterprise Subordinate CA which is domain joined, so you need to replace the “DC=”value with your AD Domain values.
- Restart the CertSvcservice for changes to take effect.

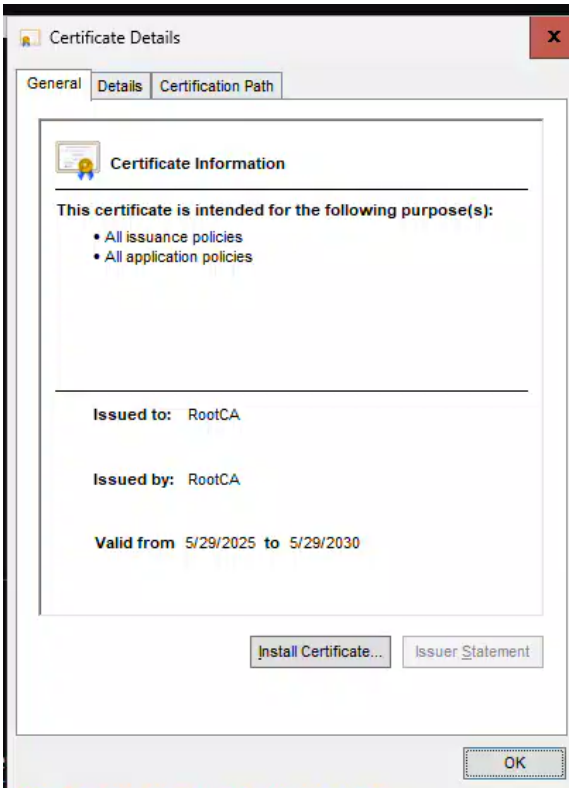
```
PS C:\Users\Administrator> # Manually configure CA distribution points in the Server Registry:
PS C:\Users\Administrator> certutil -setreg CA\ValidityPeriod "Years"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\RootCA\ValidityPeriod:

Old Value:
  ValidityPeriod REG_SZ = Years

New Value:
  ValidityPeriod REG_SZ = Years
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
PS C:\Users\Administrator> certutil -setreg CA\ValidityPeriodUnits 5
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\RootCA\ValidityPeriodUnits:

Old Value:
  ValidityPeriodUnits REG_DWORD = 1

New Value:
  ValidityPeriodUnits REG_DWORD = 5
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
PS C:\Users\Administrator> certutil -setreg CA\DSConfigDN "CN=Configuration,DC=vlabs1,DC=com"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\RootCA\DSConfigDN:

New Value:
  DSConfigDN REG_SZ = CN=Configuration,DC=vlabs1,DC=com
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
PS C:\Users\Administrator> certutil -setreg CA\DSDomainDN "DC=vlabs1,DC=com"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\RootCA\DSDomainDN:

New Value:
  DSDomainDN REG_SZ = DC=vlabs1,DC=com
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
PS C:\Users\Administrator> Restart-Service certsvc
PS C:\Users\Administrator>
```

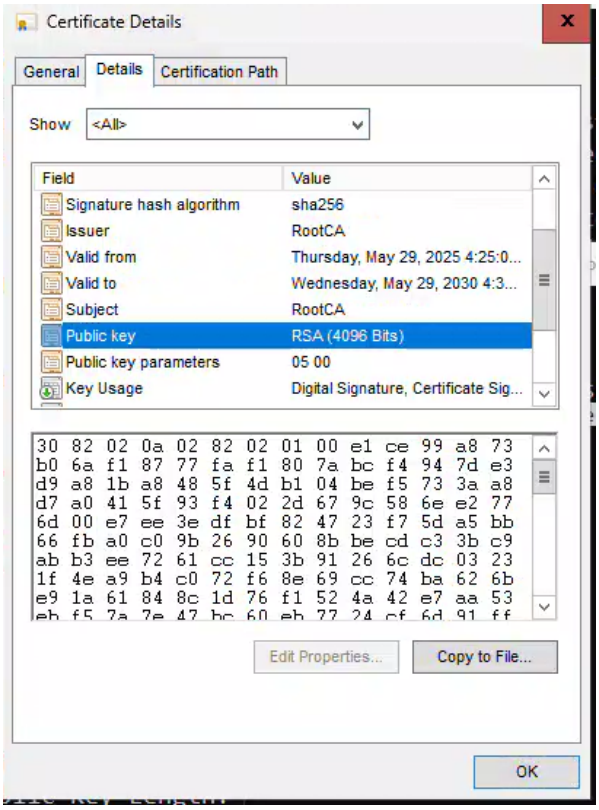
certutil -viewstore CA

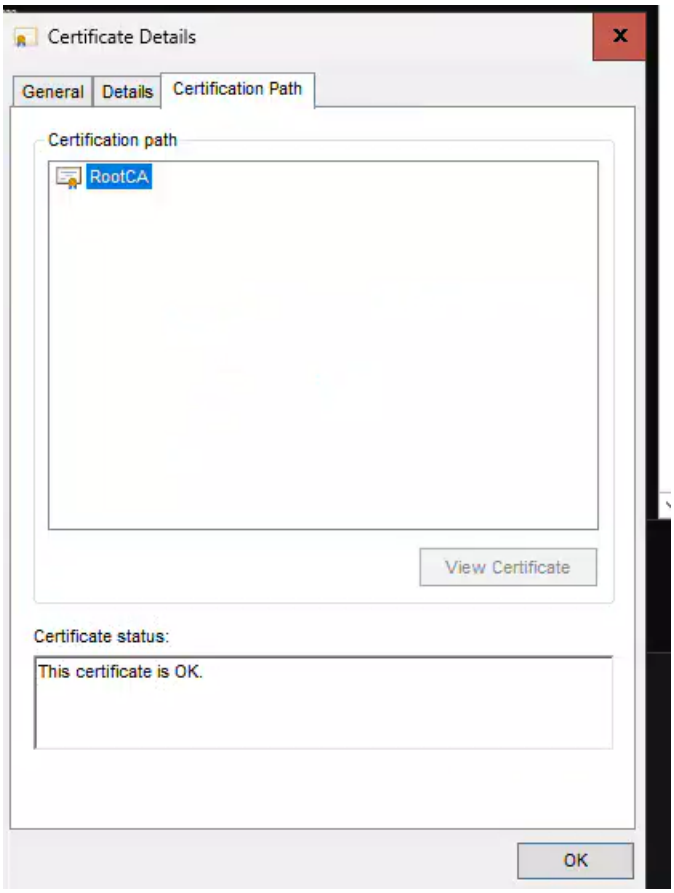





Administrator: C:\WINDOWS\system32\cmd.exe
PS C:\Users\Administrator.DC201> certutil -viewstore CA
CA "Intermediate Certification Authorities"
"C:\Windows\System32\CredentialUIBroker.exe" NonAppContainerFailedMip
View Certificate Store
Select Certificate
Root Agency
Issuer: Root Agency
Valid From: 5/ 28/ 1996 to 12/ 31/ 2039
Click here to view certificate properties
More choices
OK
Cancel


Certificate Details
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• All issuance policies
• All application policies
Issued to: RootCA
Issued by: RootCA
Valid from 5/29/2025 to 5/29/2030
Install Certificate...
Issuer Statement
OK

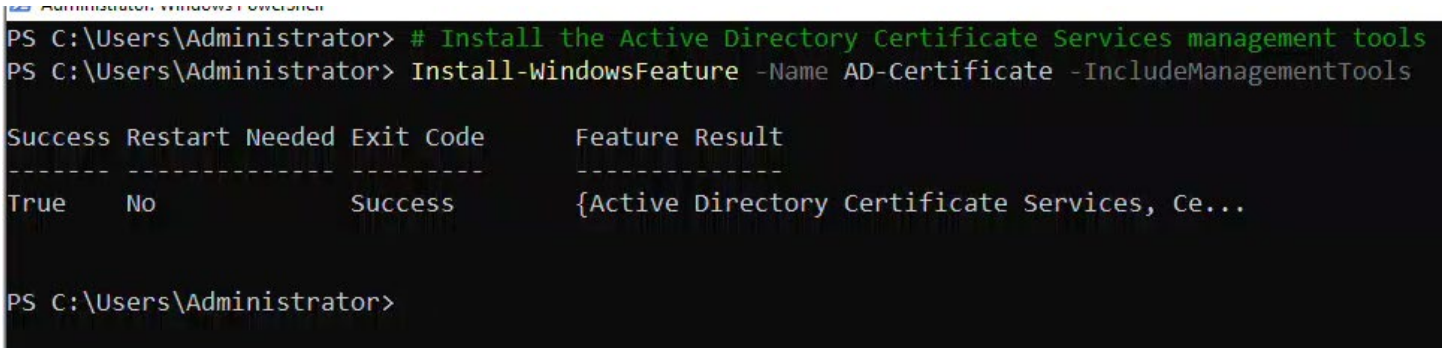

Certificate Details
General
Details
Certification Path
Show
<All>
Field
Value
Signature hash algorithm
sha256
Issuer
RootCA
Valid from
Thursday, May 29, 2025 4:25:0...
Valid to
Wednesday, May 29, 2030 4:3...
Subject
RootCA
Public key
RSA (4096 Bits)
Public key parameters
05 00
Key Usage
Digital Signature, Certificate Sig...
30 82 02 0a 02 82 02 01 00 e1 ce 99 a8 73
b0 6a f1 87 77 fa f1 80 7a bc f4 94 7d e3
d9 a8 1b a8 48 5f 4d b1 04 be f5 73 3a a8
d7 a0 41 5f 93 f4 02 2d 67 9c 58 6e e2 77
6d 00 e7 ee 3e df bf 82 47 23 f7 5d a5 bb
66 fb a0 c0 9b 26 90 60 8b be cd c3 3b c9
ab b3 ee 72 61 cc 15 3b 91 26 6c dc 03 23
1f 4e a9 b4 c0 72 f6 8e 69 cc 74 ba 62 6b
e9 1a 61 84 8c 1d 76 f1 52 4a 42 e7 aa 53
Edit Properties...
Copy to File...
OK


Certificate Details
General
Details
Certification Path
Certification path
RootCA
View Certificate
Certificate status:
This certificate is OK.
OK

3.6 Modify the CRL Distribution Points (CDP) and Authority Information Access (AIA) settings from DC201 to DC101.

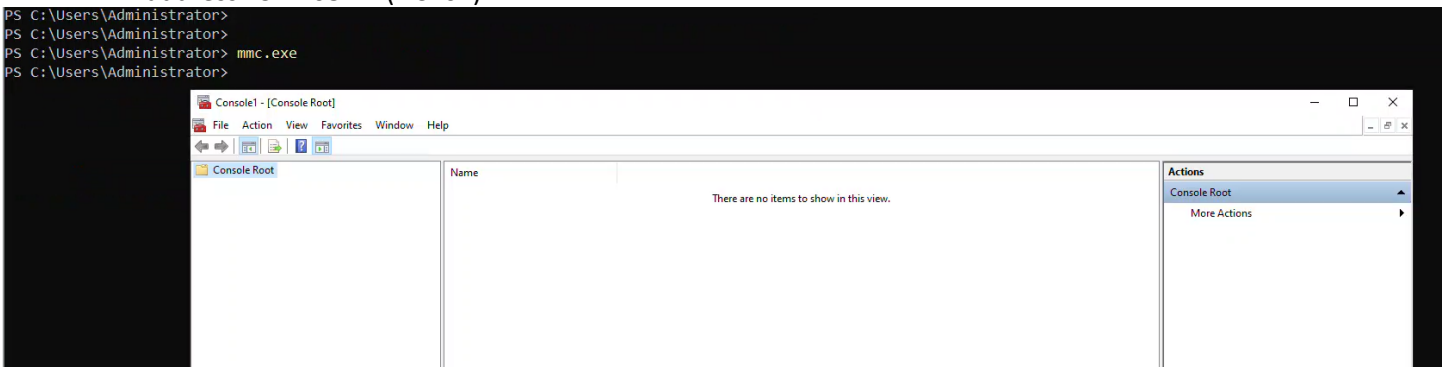
1. Install AD CS on the Root Domain controller:
   Login in the AD DC101 and install the Active Directory Certificate Services (AD CS) and the management tools:

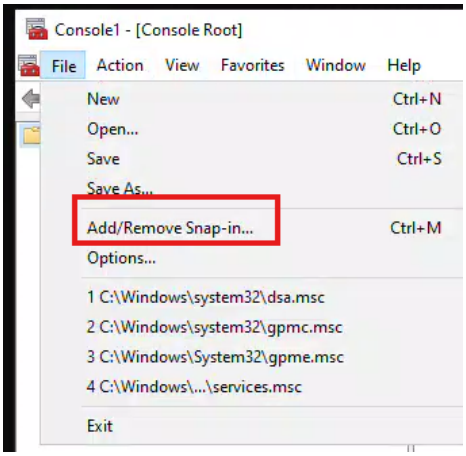
   ```
   # Install the Active Directory Certificate Services management tools
   Install-WindowsFeature -Name AD-Certificate -IncludeManagementTools
   ```

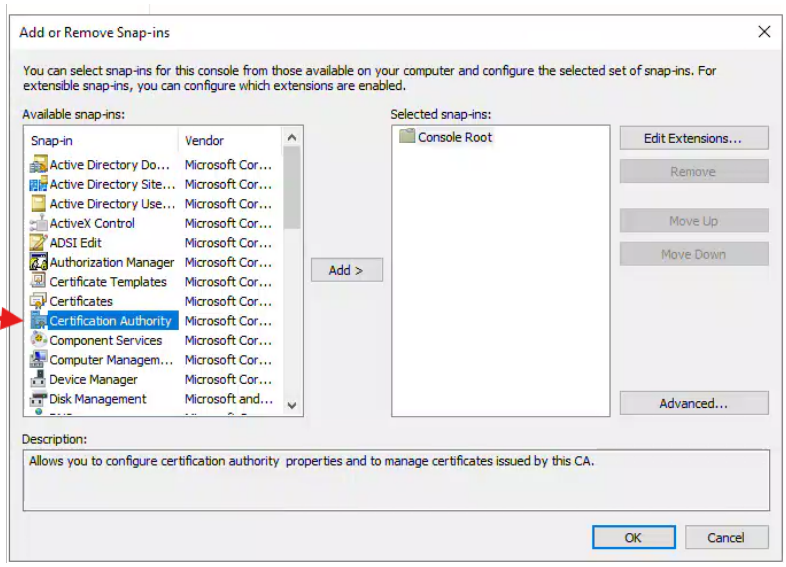


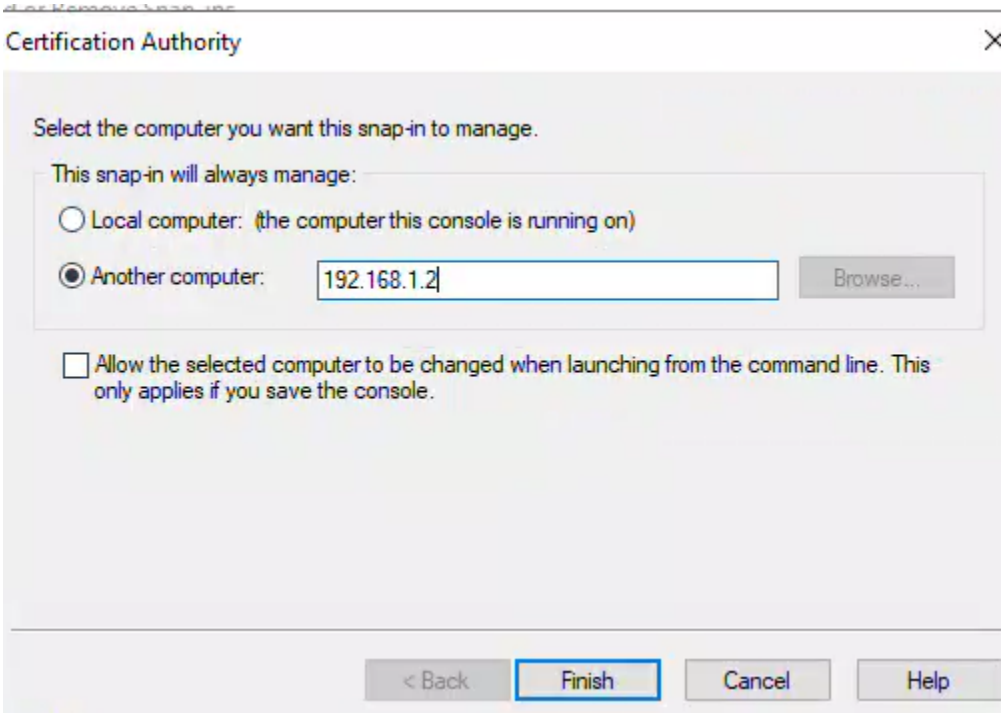
2. Define where CDP and AIA can be accessed:

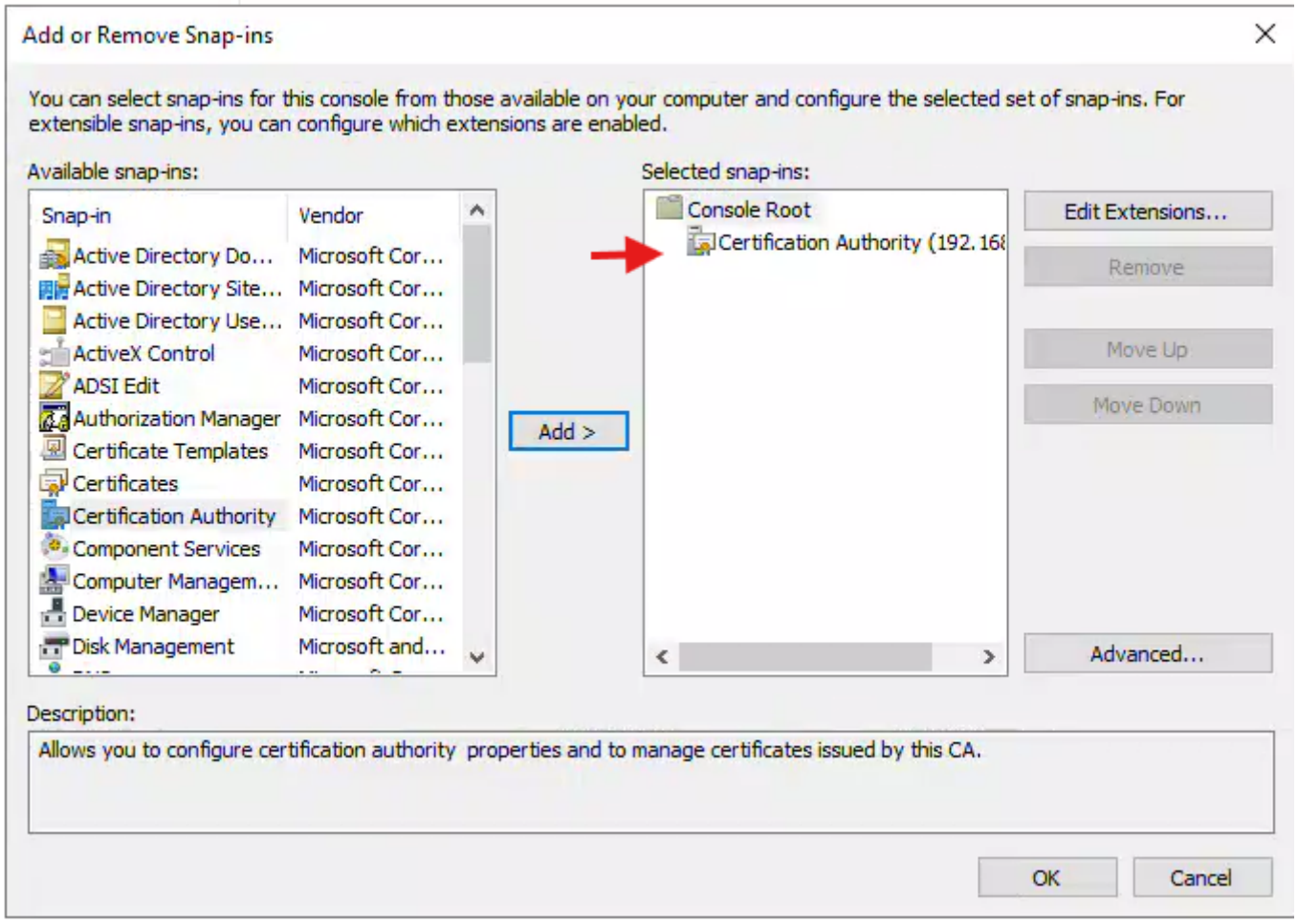
   a) Open the Certification Authority Snap-in using mmc.exe and connect to your RootCA server using its IP address 192.168.1.2(DC201)

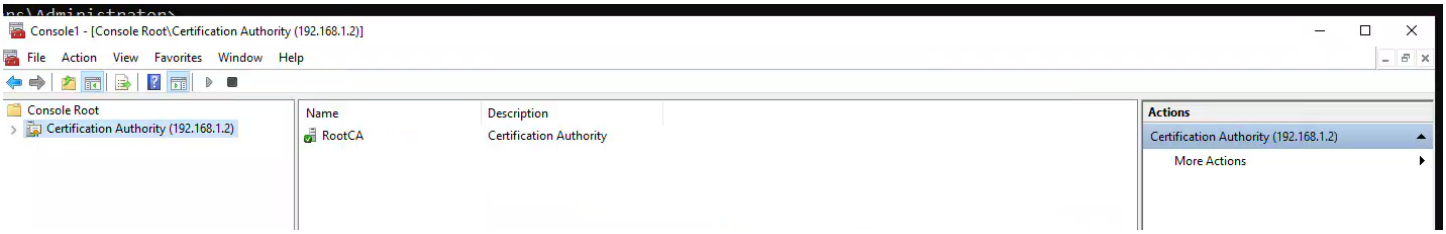


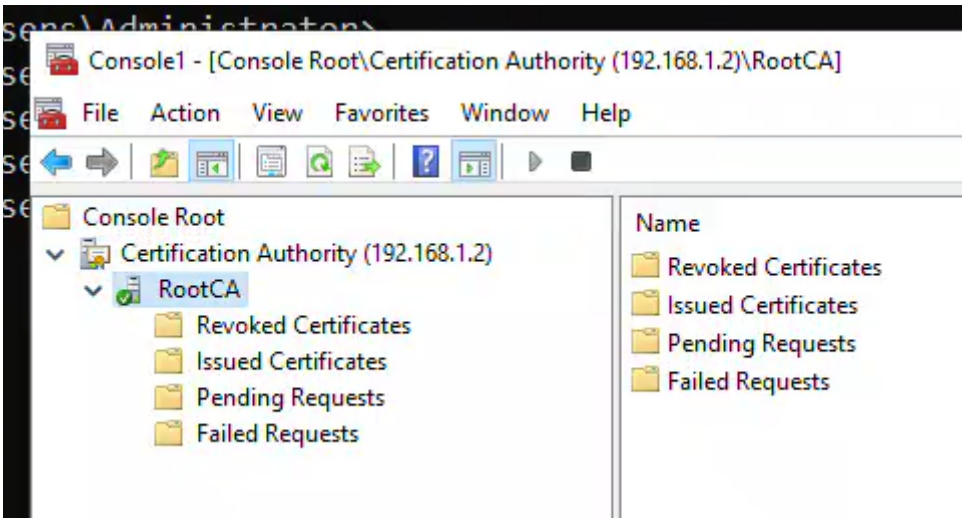

Console1 - [Console Root]
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\Windows\system32\dsa.msc
2 C:\Windows\system32\gpmc.msc
3 C:\Windows\System32\gpme.msc
4 C:\Windows\...\services.msc
Exit


Add or Remove Snap-ins
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.
Available snap-ins:
Snap-in
Vendor
Active Directory Do... Microsoft Cor...
Active Directory Site... Microsoft Cor...
Active Directory Use... Microsoft Cor...
ActiveX Control Microsoft Cor...
ADSI Edit Microsoft Cor...
Authorization Manager Microsoft Cor...
Certificate Templates Microsoft Cor...
Certificates Microsoft Cor...
Certification Authority Microsoft Cor...
Component Services Microsoft Cor...
Computer Managem... Microsoft Cor...
Device Manager Microsoft Cor...
Disk Management Microsoft and...
Add >
Selected snap-ins:
Console Root
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
Description:
Allows you to configure certification authority properties and to manage certificates issued by this CA.
OK
Cancel

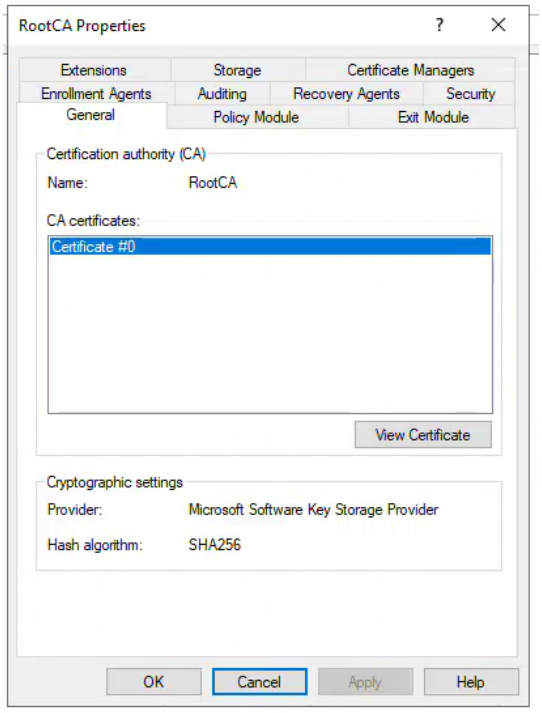

Certification Authority
Select the computer you want this snap-in to manage.
This snap-in will always manage:
Local computer: (the computer this console is running on)
Another computer:
192.168.1.2
Browse...
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.
< Back
Finish
Cancel
Help


Add or Remove Snap-ins
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.
Available snap-ins:
Snap-in
Vendor
Active Directory Do... Microsoft Cor...
Active Directory Site... Microsoft Cor...
Active Directory Use... Microsoft Cor...
ActiveX Control Microsoft Cor...
ADSI Edit Microsoft Cor...
Authorization Manager Microsoft Cor...
Certificate Templates Microsoft Cor...
Certificates Microsoft Cor...
Certification Authority Microsoft Cor...
Component Services Microsoft Cor...
Computer Managem... Microsoft Cor...
Device Manager Microsoft Cor...
Disk Management Microsoft and...
Add >
Selected snap-ins:
Console Root
Certification Authority (192.168
Edit Extensions...
Remove
Move Up
Move Down
Advanced...
Description:
Allows you to configure certification authority properties and to manage certificates issued by this CA.
OK
Cancel

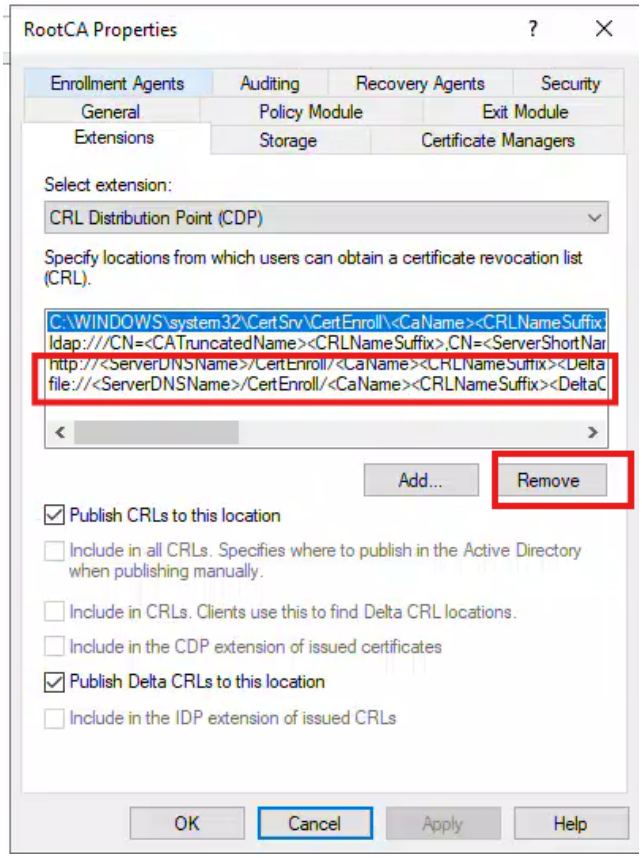

Console1 - [Console Root\Certification Authority (192.168.1.2)]
File Action View Favorites Window Help
Console Root
Certification Authority (192.168.1.2)
Name
Description
RootCA
Certification Authority
Actions
Certification Authority (192.168.1.2)
More Actions


Console1 - [Console Root\Certification Authority (192.168.1.2)\RootCA]
File Action View Favorites Window Help
Console Root
Certification Authority (192.168.1.2)
RootCA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Name
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests

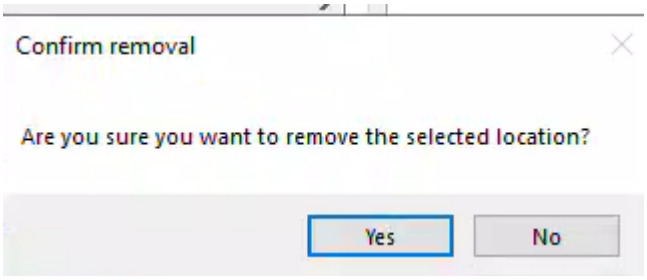
b) Right click on RootCA and click Properties (wait it might take some time).

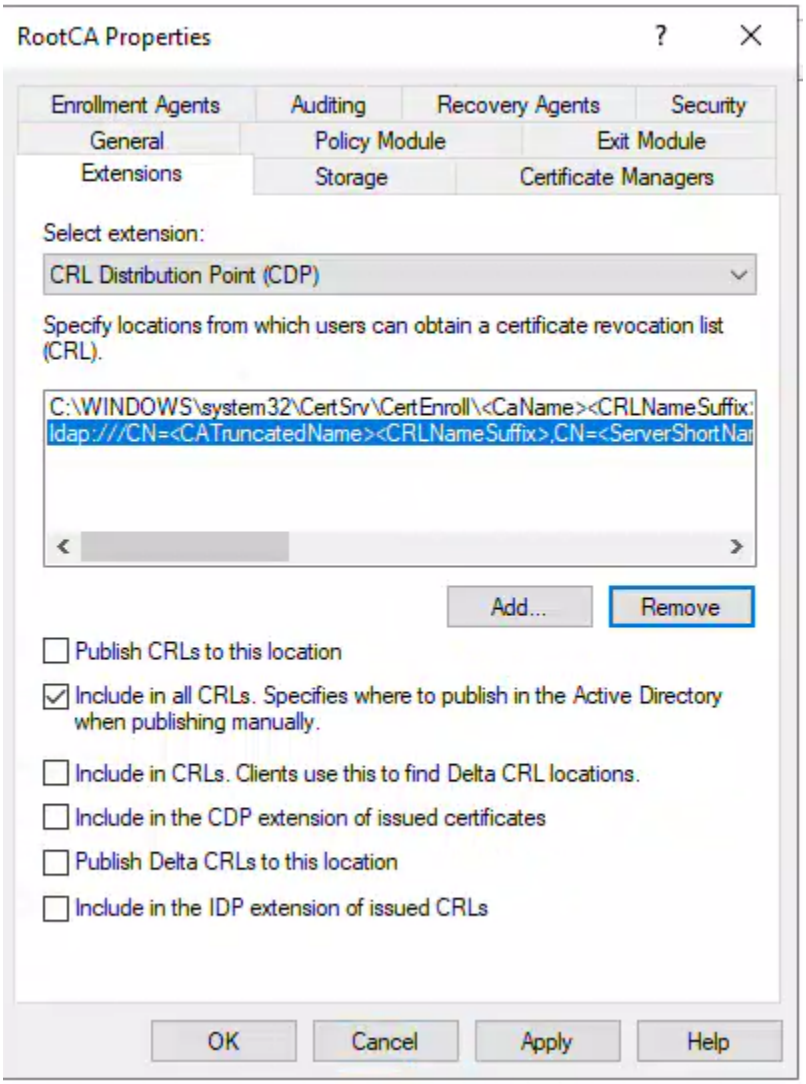


c) Navigate to Extensions tab, here we need to modify both, the CRL Distribution Point (CDP) and the Authority Information Access (AIA) because the Root CA will not be available for accessing the CRL or Root Certificate, so we need to define where these items can be accessed.



d) In CRL remove the entries for http and file entries.

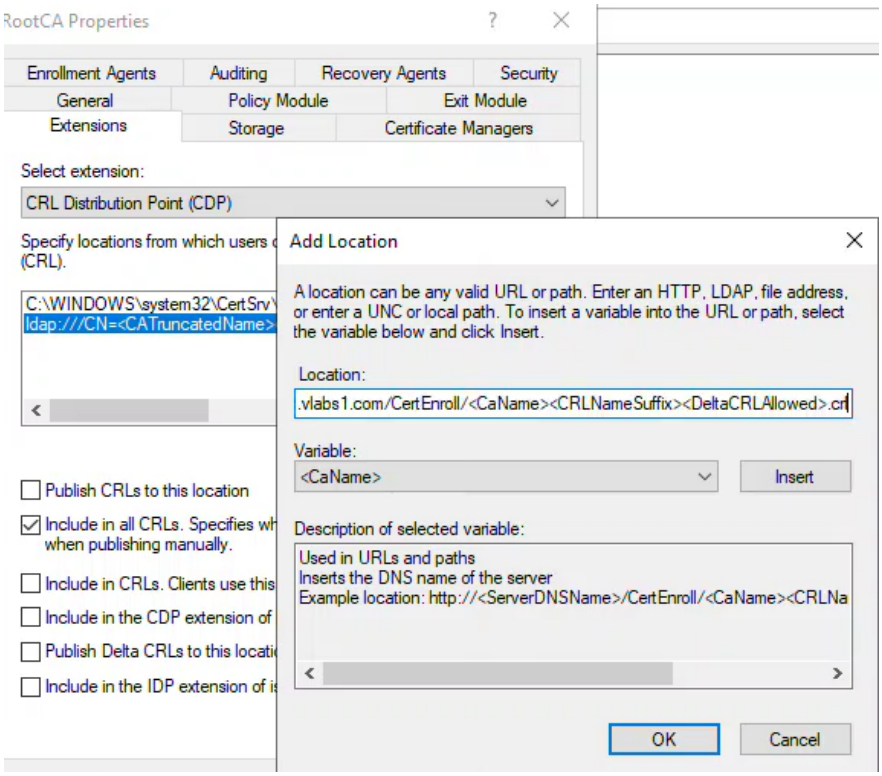




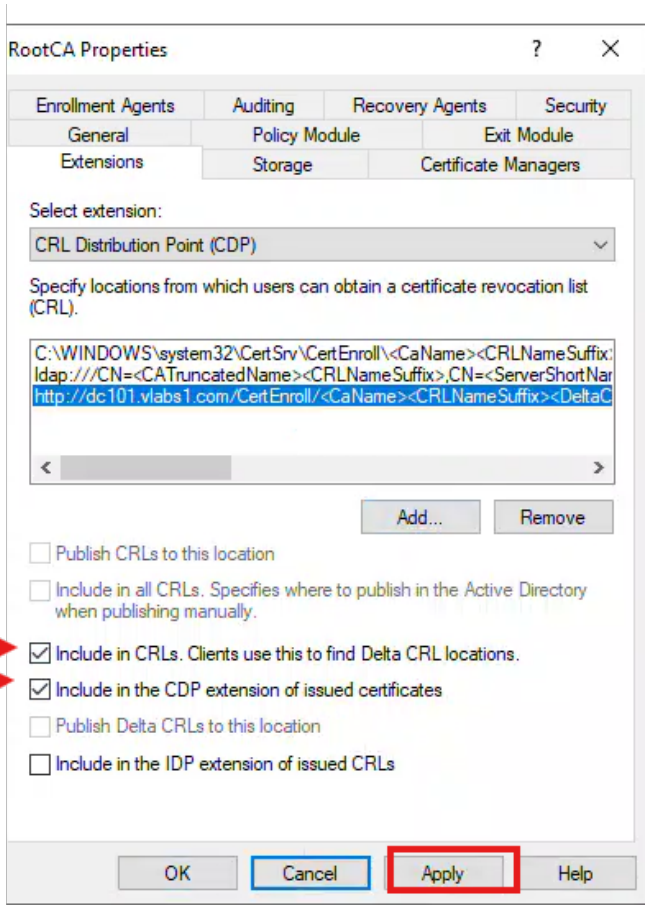
e) Add a new entry with your URL of the Enterprise Subordinate CA server (DC1XX).

Example URL:

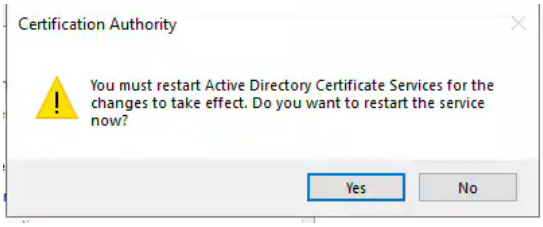
http://dc101.vlabs1.com/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl



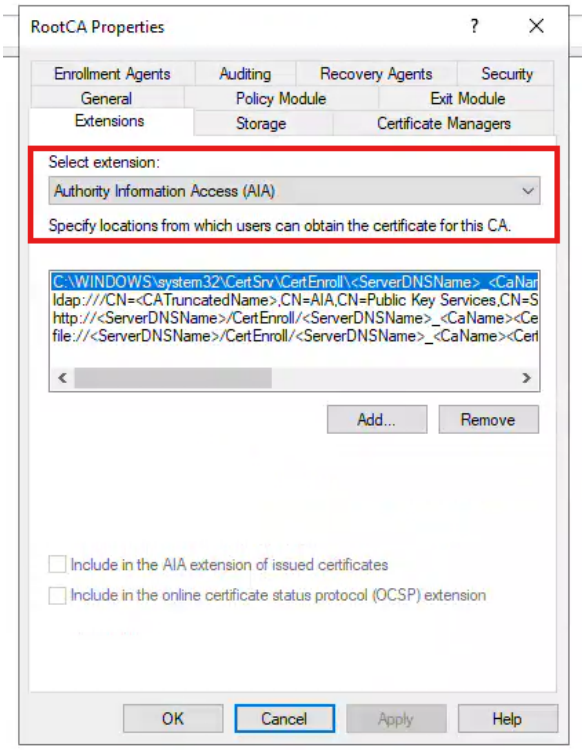
f) Check Include in CRLs and Include in the CDP then click on Apply.

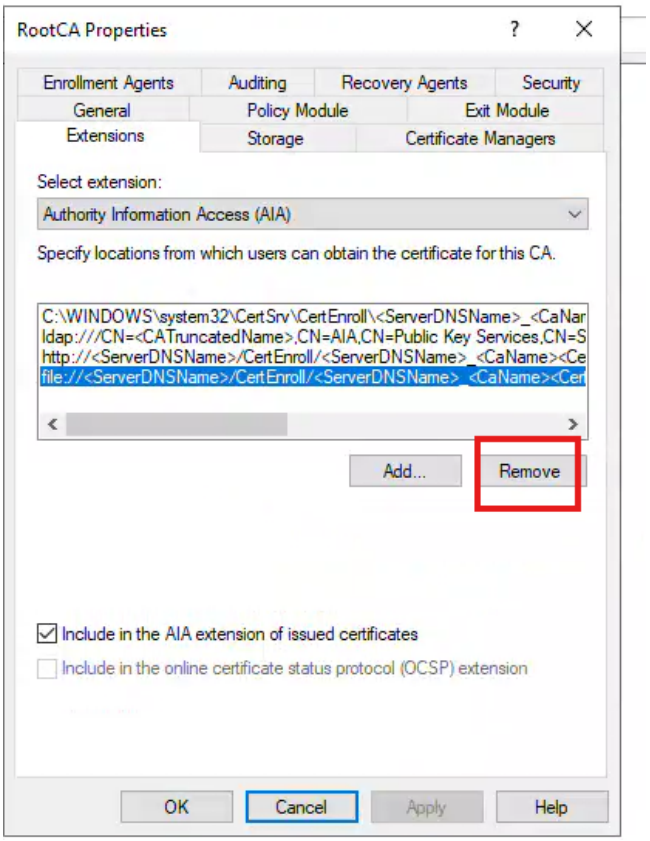


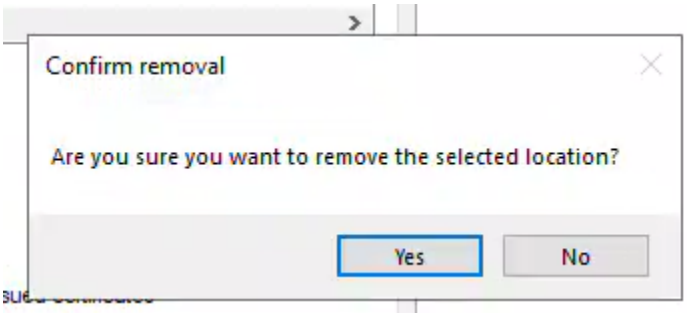
g) Wait until it finished restarting the service.



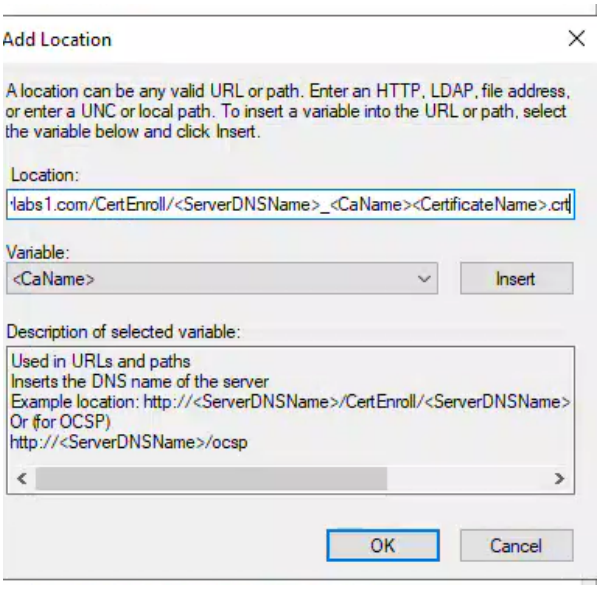
h) In the extension drop down select Authority Information Access (AIA) and remove http and file entries.

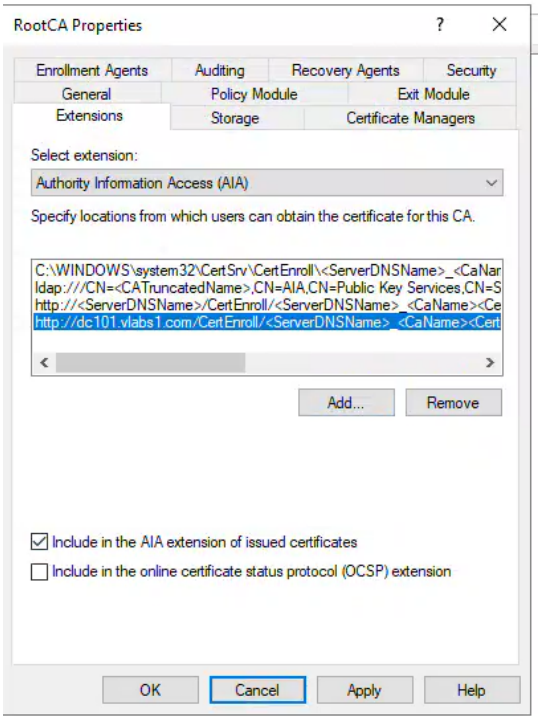




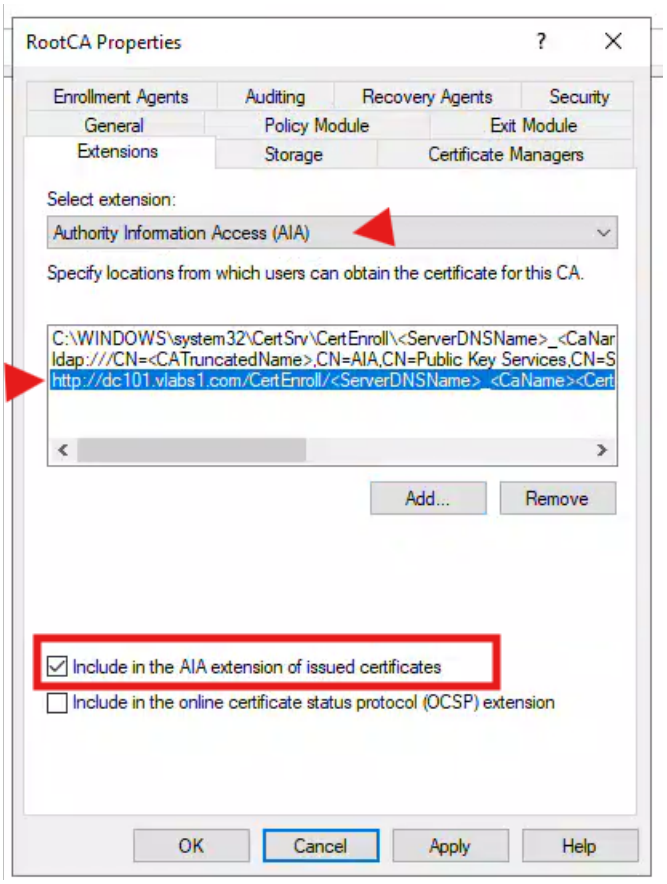


i) Add a new entry, again with your Alias URL:
http://dc101.vlabs1.com/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt

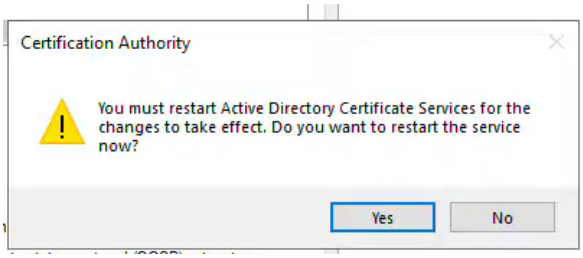




j) Check Include in the AIA extension of issued certificates then click on Apply.

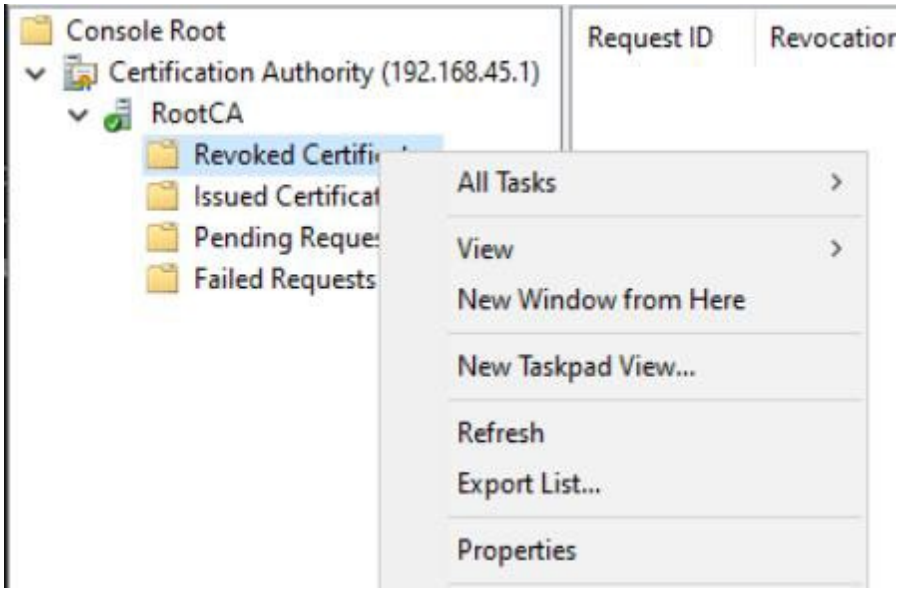


k) Wait until it finished restarting the service.

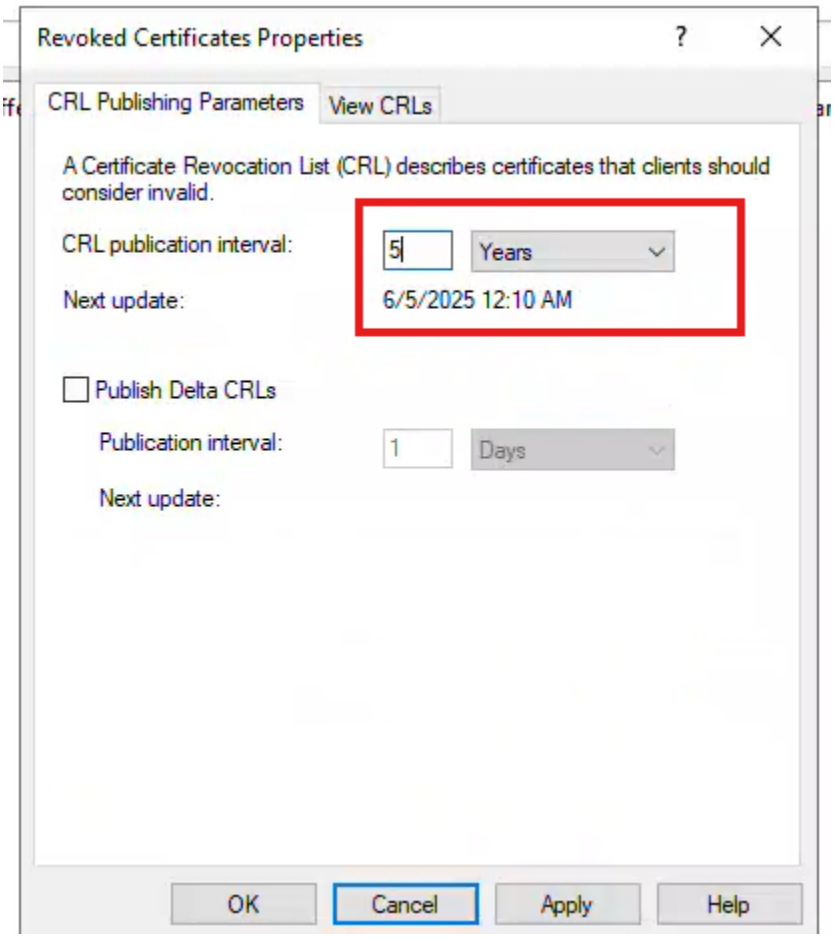


l) Click Ok to close this window.

m) Navigate to Revoked Certificates and select Properties.

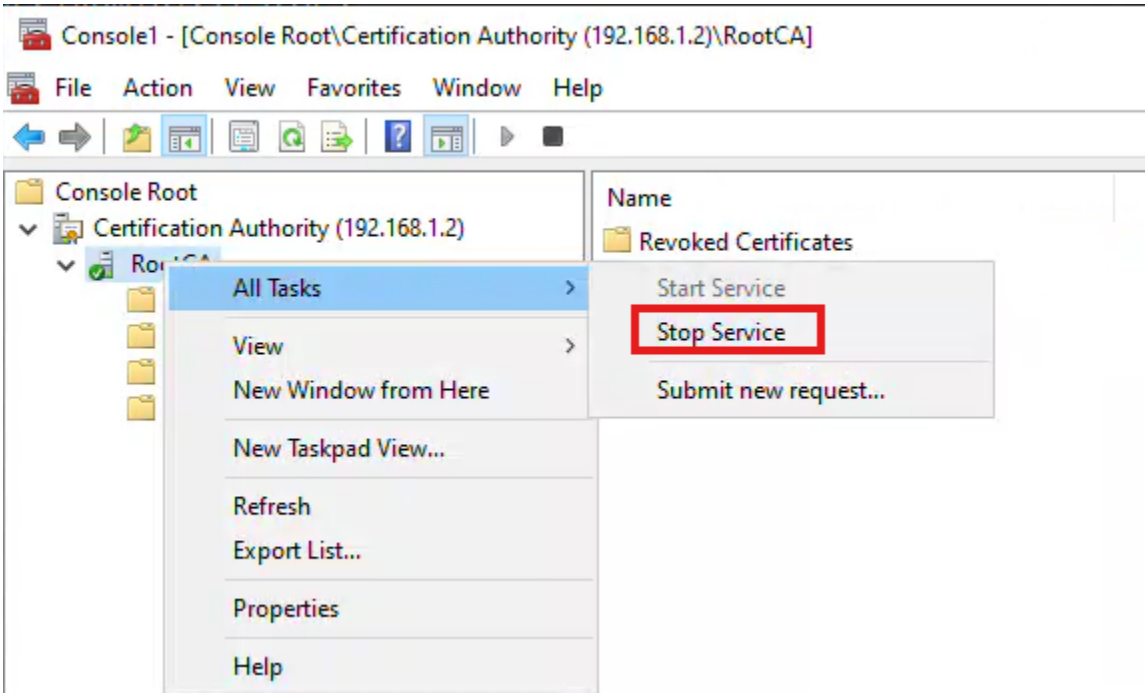


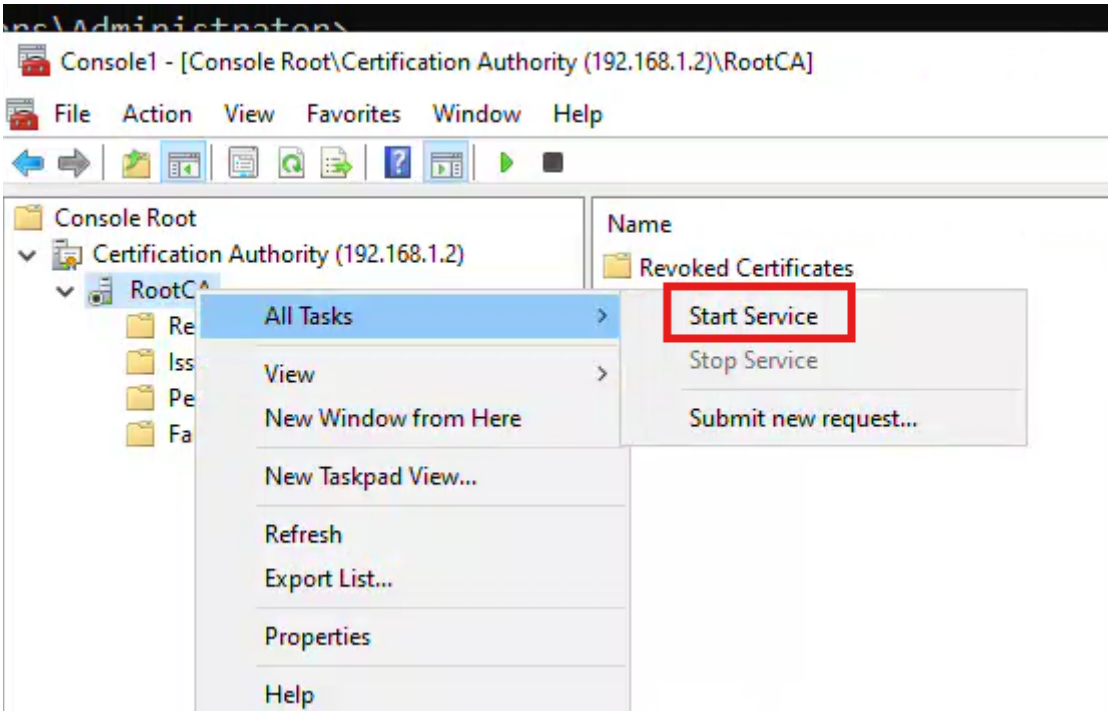
n) Since the RootCA will be offline for 5 years, modify the CRL publication interval for 5 years, so we don't have to use the RootCA.



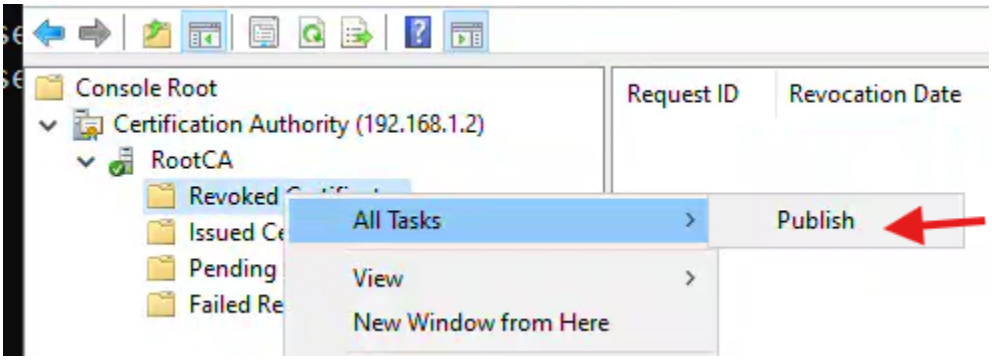
o) Click Ok to close this window.

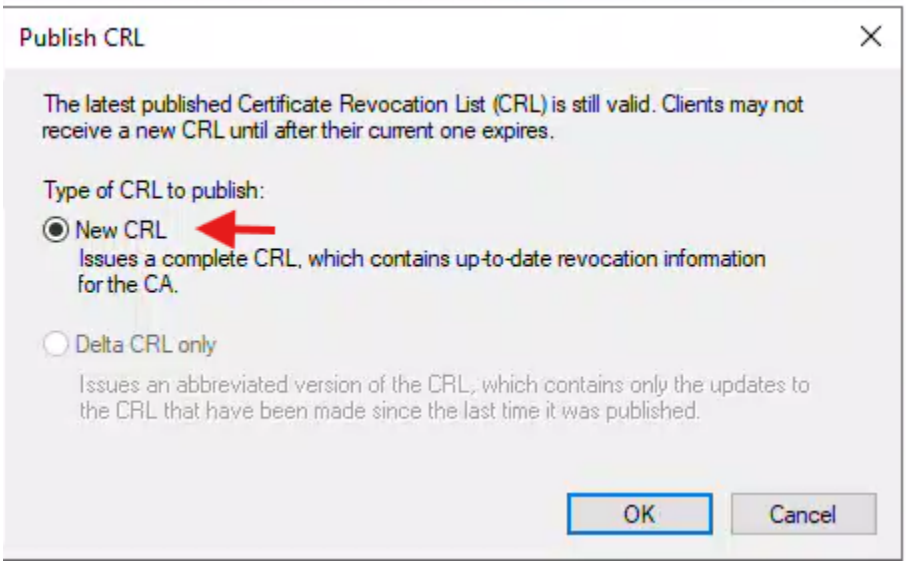
p) Now restart Root CA Server so that settings are applied.



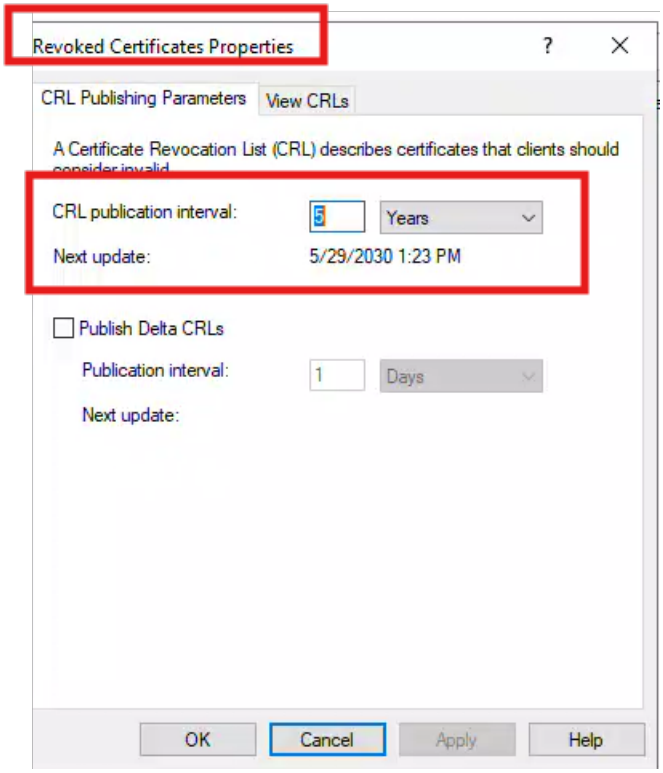


q) Finally Publish the CRL.





r) Verify the Revoked Certificates Properties.



3.7 Copy the Root CA Certificate, Certificate Revocation List (CRL) and CA private key to DC101.

3.7.1 From DC201

Copy-Item "C:\Windows\System32\CertSrv\CertEnroll*" \\192.168.1.1\C$

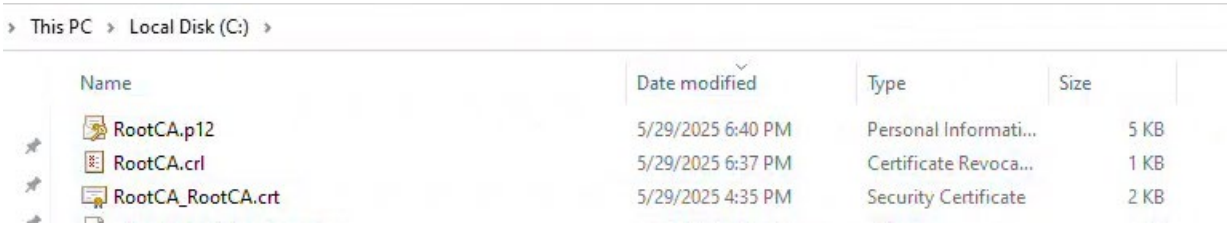
certutil -backup \\192.168.1.1\C$

Enter a password to protect the private key.

It is recommended to copy the private key on a USB key and hide it.

```
PS C:\Users\Administrator> Copy-Item "C:\Windows\System32\CertSrv\CertEnroll\*" \\192.168.1.1\C$
PS C:\Users\Administrator> certutil -backup \\192.168.1.1\C$
Enter new password:

Confirm new password:

Backed up keys and certificates for RootCA\RootCA to \\192.168.1.1\C$\RootCA.p12.
Full database backup for RootCA\RootCA.
Backing up Database files: 100%
Backing up Log files: 100%
Truncating Logs: 100%
Backed up database to \\192.168.1.1\C$.
Database logs successfully truncated.
CertUtil: -backup command completed successfully.
PS C:\Users\Administrator>
```

3.7.2 On DC101

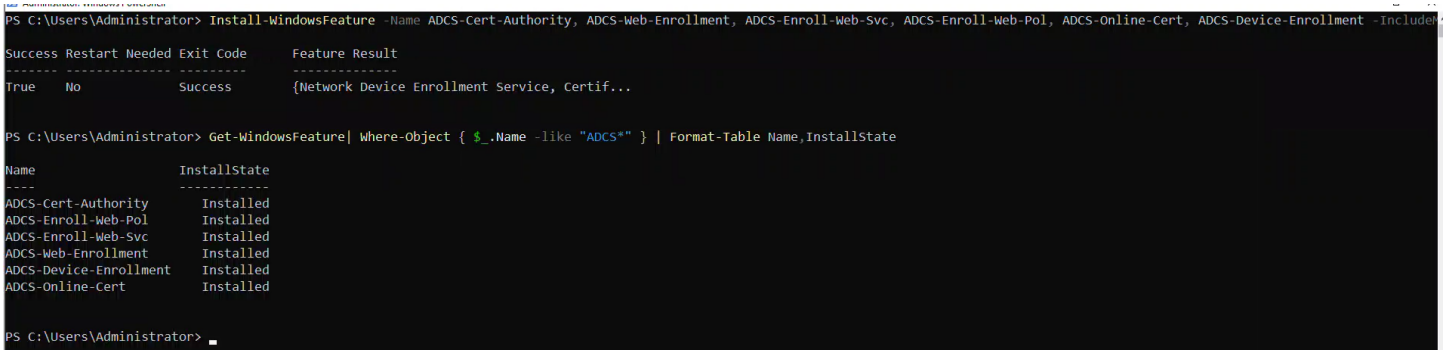


4 Task 2: Deploy an Enterprise Subordinate CA on DC101

4.1 Install Active Directory Certificate Services (AD CS) including all AD CS features on DC101.

Install-WindowsFeature -Name ADCS-Cert-Authority, ADCS-Web-Enrollment, ADCS-Enroll-Web-Svc, ADCS-Enroll-Web-Pol, ADCS-Online-Cert, ADCS-Device-Enrollment -IncludeManagementTools

Get-WindowsFeature| Where-Object { $_.Name -like "ADCS*" } | Format-Table Name,InstallState



4.2 Configure DC101 as an Enterprise Subordinate CA.

1. Initialize the Enterprise Subordinate CA
   On AD DC101:
   Install-AdcsCertificationAuthority -CAType EnterpriseSubordinateCa -CACommonName vlabs1-CA -KeyLength

4096 -HashAlgorithm SHA256 -CryptoProviderName "RSA#Microsoft Software Key Storage Provider"

Type: A (For Yes to all)

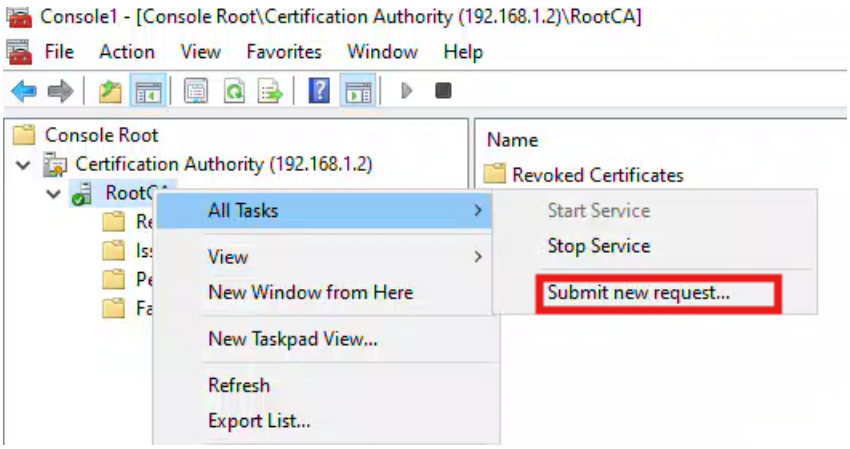
- CAType should be EnterpriseSubordinateCa
- CACommonNameit is the name of your new certificate: vlabs1-CA
- Sets up the CA with SHA-256 and a 4096-bit key for security.
- Use the Microsoft RSA algorithm to create the private/public keys.

After that command is executed and CA is installed, you will get a warning which is normal:

```
PS C:\Users\Administrator> Install-AdcsCertificationAuthority -CAType EnterpriseSubordinateCa -CACommonName vlabs1-CA -KeyLength 4096 -HashAlgorithm SHA256 -CryptoProviderName "RSA#Microsoft Software Key Storage Provider"

Confirm
Are you sure you want to perform this action?
Performing the operation "Install-AdcsCertificationAuthority" on target "DC101".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A
WARNING: The Active Directory Certificate Services installation is incomplete. To complete the installation, use the request file "C:\DC101.vlabs1.com_vlabs1-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)

ErrorId ErrorString
------- -----------
    398 The Active Directory Certificate Services installation is incomplete. To complete the installation, use the request file "C:\DC101.vlabs1.com_vlabs1-CA.req" to obtain a certificate from the parent CA. Then, use the Certificat..


PS C:\Users\Administrator>
```

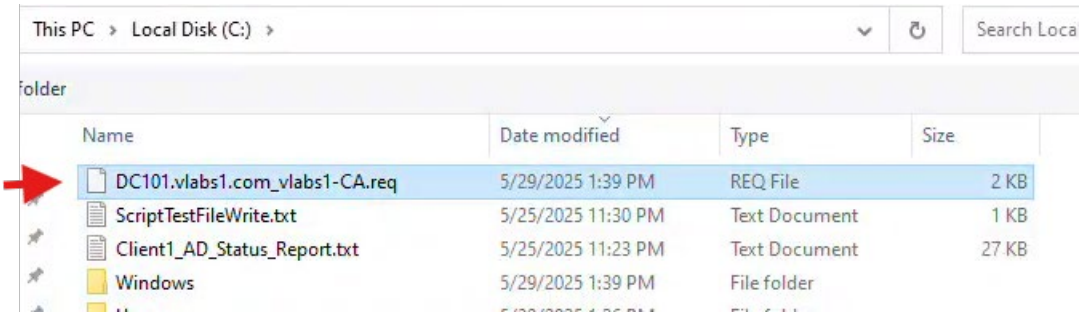
2. Submit a new Certificate Request

a) Open the Certification Authority Snap-in suing mmc.exe and connect to your RootCA server using its IP address 192.168.1.2(DC201)

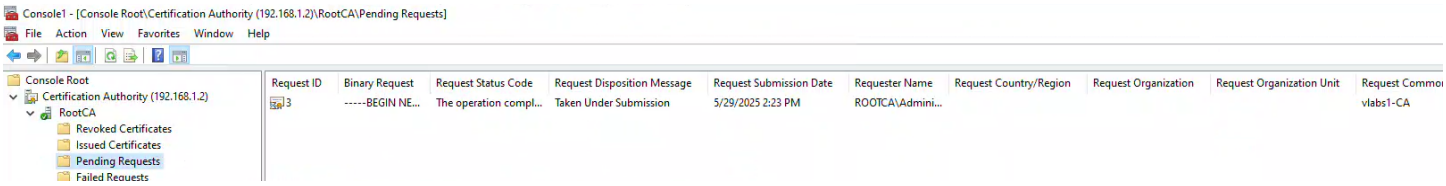


b) On the RootCA Server Submit a new Certificate Request

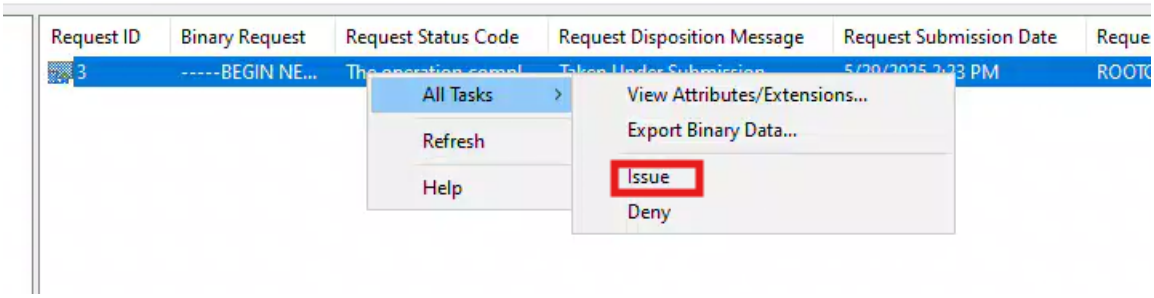
c) Browse to your C: drive, select the certificate request file→C:\DC101.vlabs1.com_vlabs1-CA.req,then select Open.



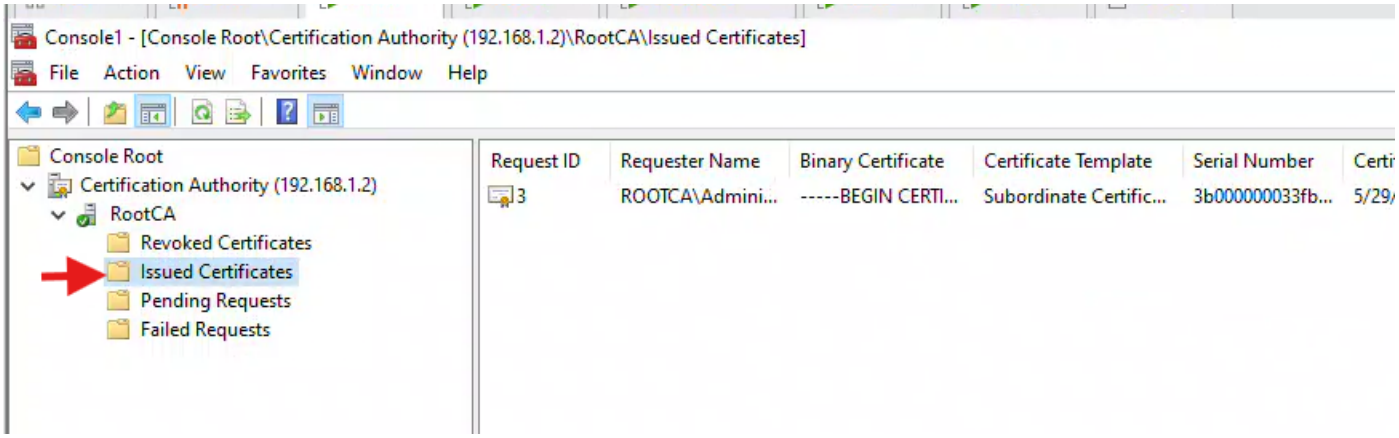
d) The certificate will now show up in the Pending Requests section (it may take some seconds →Refresh).



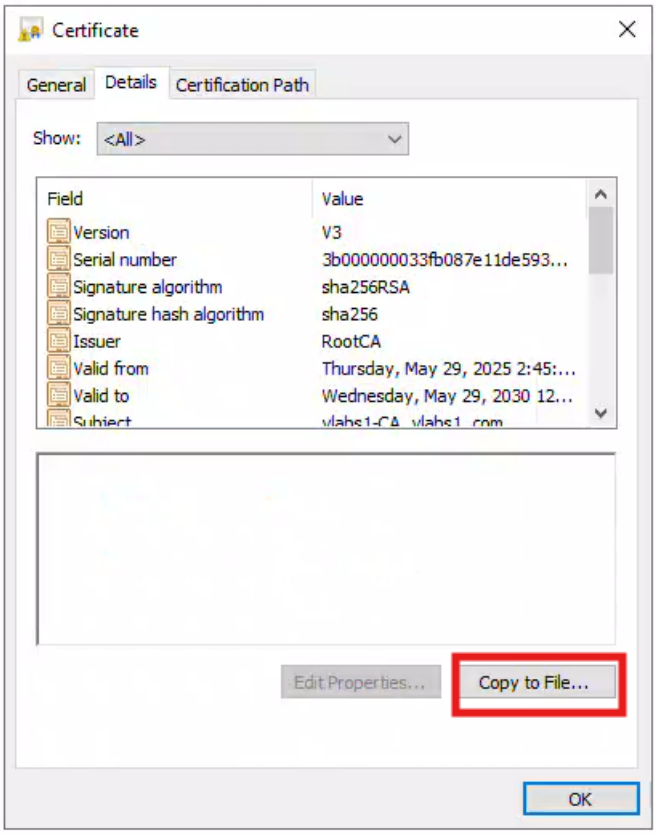
e) Right click on the certificate and click All Tasks > Issue



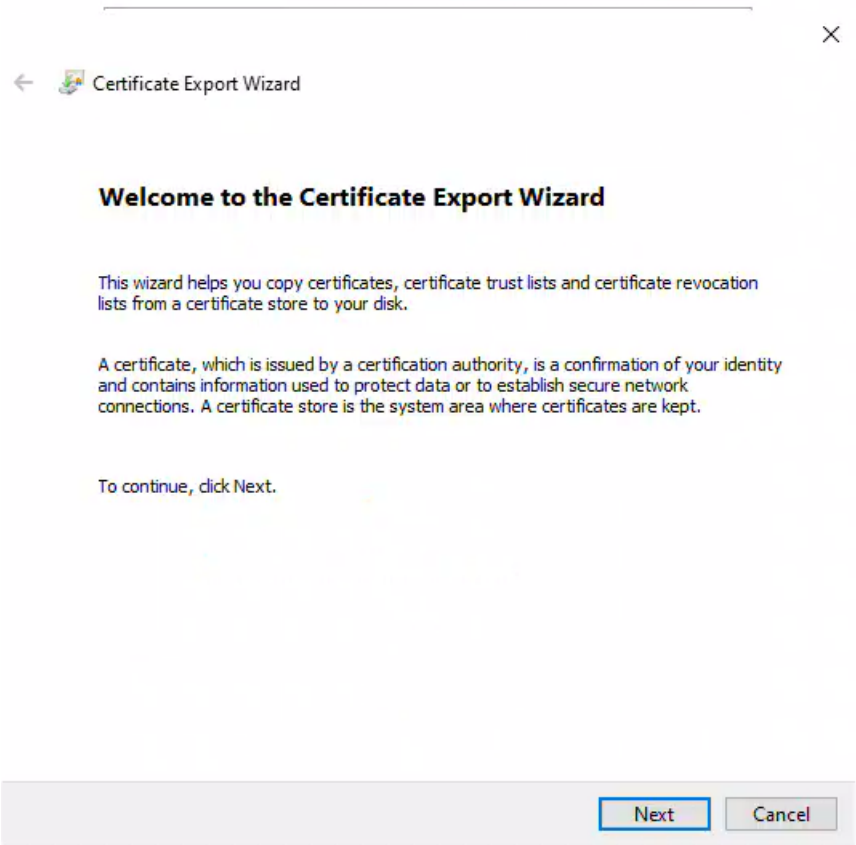
f) The certificate is now under Issued Certificates.



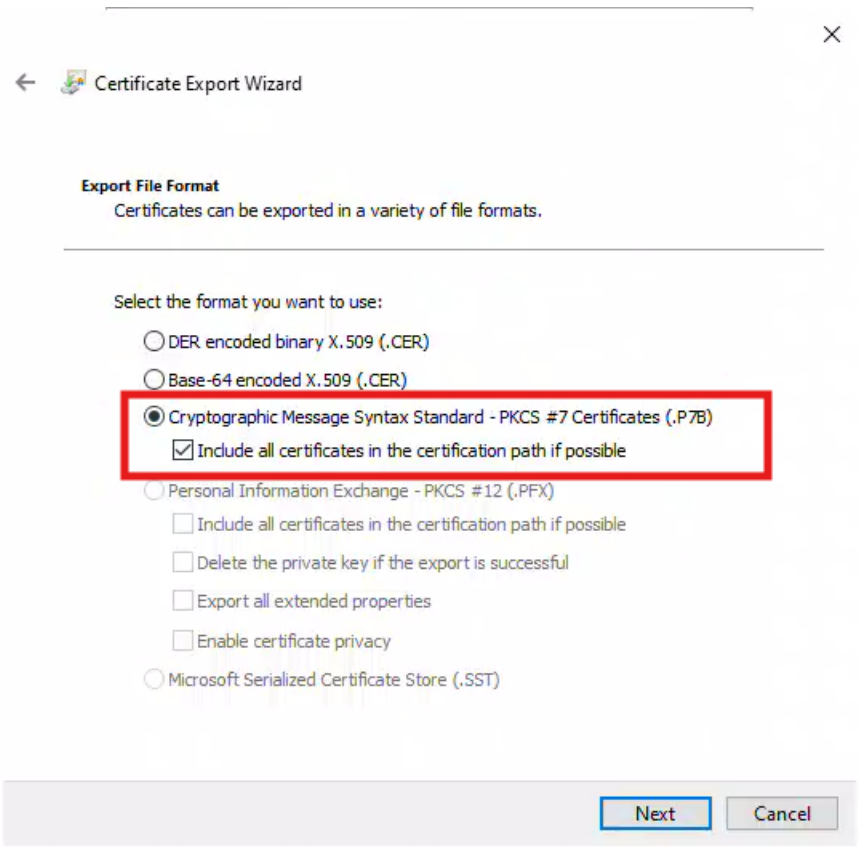
g) Double click on the issued certificate, navigate to Details tab and click Copy to File…



h) Certificate Export Wizard appears Click on Next

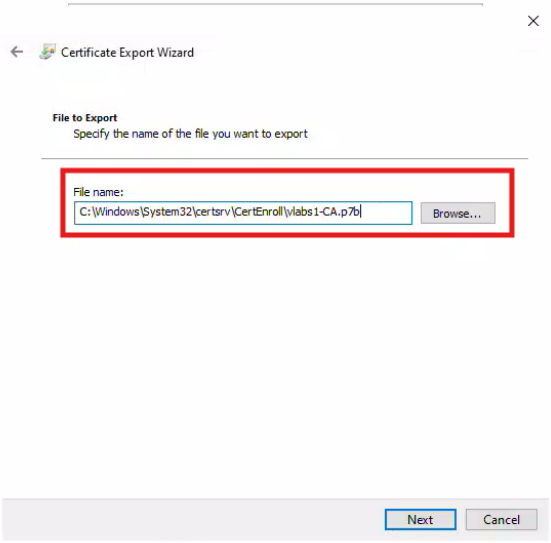


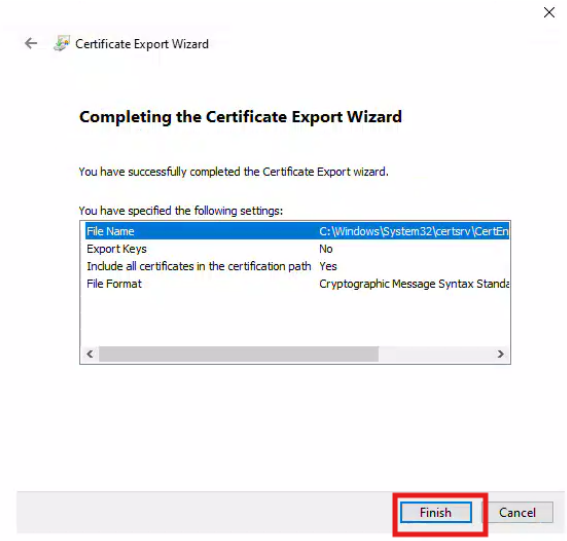
i) Select the **Cryptographie Message Syntax Standard -PKCS #7** type and select Include all certificates in the certification path



j) Save the file under:

C:\Windows\System32\certsrv\CertEnroll\vlabs1-CA.p7b





k) The Entreprise Subordinate CA Server certificate is now copied to your certificate Enroll folder.

Copy also the RootCA certificate and CRL to the Entreprise Subordinate CA certificate Enroll folder:

Copy-Item -Path C:*.crt -Destination C:\Windows\System32\certsrv\CertEnroll
Copy-Item -Path C:*.crl -Destination C:\Windows\System32\certsrv\CertEnroll

```
PS C:\Users\Administrator> Copy-Item -Path C:\*.crt -Destination C:\Windows\System32\certsrv\CertEnroll\
PS C:\Users\Administrator> Copy-Item -Path C:\*.crl -Destination C:\Windows\System32\certsrv\CertEnroll\
PS C:\Users\Administrator> _
```

Execute the following commands to Publish the Certificate and CRL to AD:
certutil -dspublish -f C:\Windows\System32\certsrv\CertEnroll\RootCA_RootCA.crt
certutil -dspublish -f C:\Windows\System32\certsrv\CertEnroll\RootCA.crl

```
PS C:\Users\Administrator> #Execute the following commands to Publish the Certificate and CRL to AD:
PS C:\Users\Administrator> certutil -dspublish -f C:\Windows\System32\certsrv\CertEnroll\RootCA_RootCA.crt
ldap:///CN=RootCA,CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC=vlabs1,DC=com?cACertificate

Certificate added to DS store.

ldap:///CN=RootCA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=vlabs1,DC=com?cACertificate

Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.
PS C:\Users\Administrator> certutil -dspublish -f C:\Windows\System32\certsrv\CertEnroll\RootCA.crl
ldap:///CN=RootCA,CN=RootCA,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=vlabs1,DC=com?certificateRevocationList?base?objectClass=cRLDistributionPoint?certificateRevocationList

Base CRL added to DS store.

CertUtil: -dsPublish command completed successfully.
PS C:\Users\Administrator>
```

Execute the following command to install the Root CA certificate:
certutil -addstore Root C:\Windows\System32\certsrv\CertEnroll\RootCA_RootCA.crt

```
PS C:\Users\Administrator> #Execute the following command to install  the Root CA certificate:
PS C:\Users\Administrator> certutil -addstore Root C:\Windows\System32\certsrv\CertEnroll\RootCA_RootCA.crt
Root "Trusted Root Certification Authorities"
Signature matches Public Key
Certificate "RootCA" added to store.
CertUtil: -addstore command completed successfully.
PS C:\Users\Administrator>
```

Execute the following command to install the Root CA CRL:
certutil -addstore CA C:\Windows\System32\certsrv\CertEnroll\RootCA.crl

```
PS C:\Users\Administrator> certutil -addstore CA C:\Windows\System32\certsrv\CertEnroll\RootCA.crl
CA "Intermediate Certification Authorities"
CRL "CN=RootCA" added to store.
CertUtil: -addstore command completed successfully.
PS C:\Users\Administrator>
```

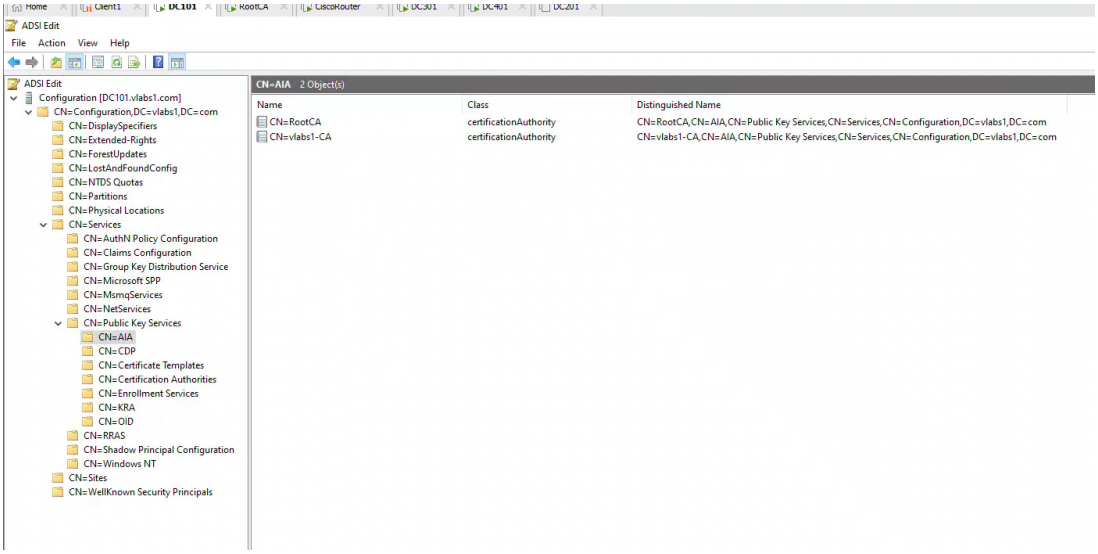
Execute the following command to install the Subordinate CA Certificate:
certutil -installCert C:\Windows\System32\certsrv\CertEnroll\vlabs1-CA.p7b

```
PS C:\Users\Administrator> certutil -installCert C:\Windows\System32\certsrv\CertEnroll\vlabs1-CA.p7b
CertUtil: -installCert command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
PS C:\Users\Administrator>
```

Start the CA service on the Subordinate CA Certificate:
Start-Service certsvc

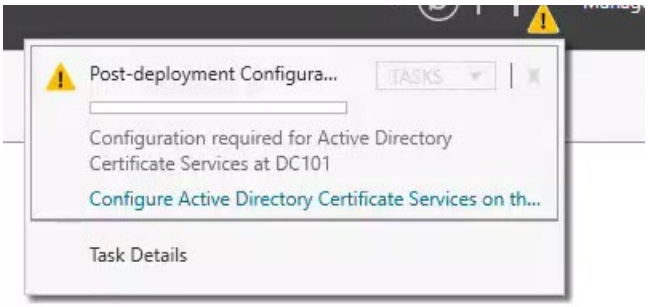
```
PS C:\Users\Administrator> #Start the CA service on the Subordinate CA Certificate:
PS C:\Users\Administrator> Start-Service certsvc
PS C:\Users\Administrator>
```

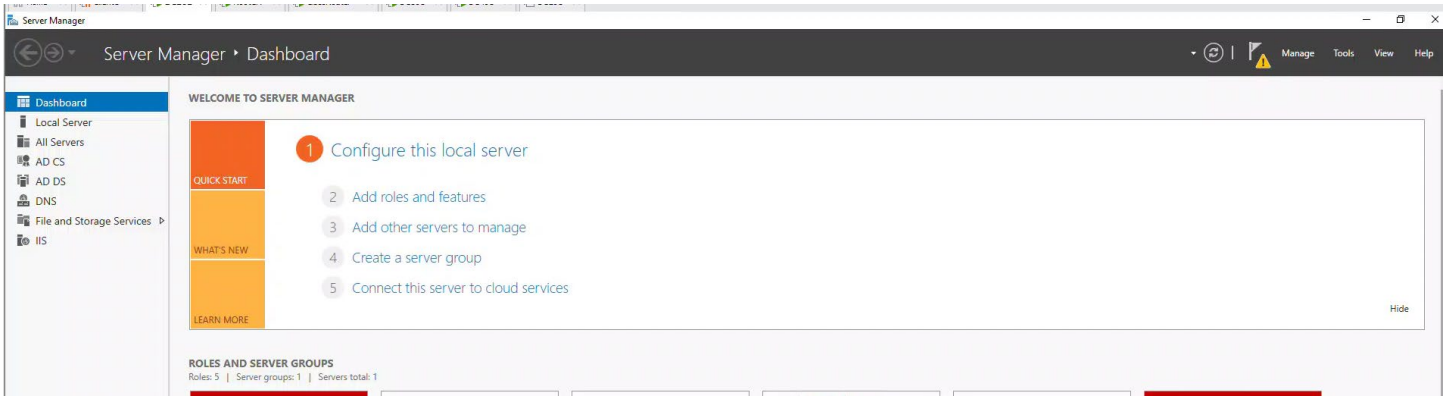
Verify with ADSI Edit

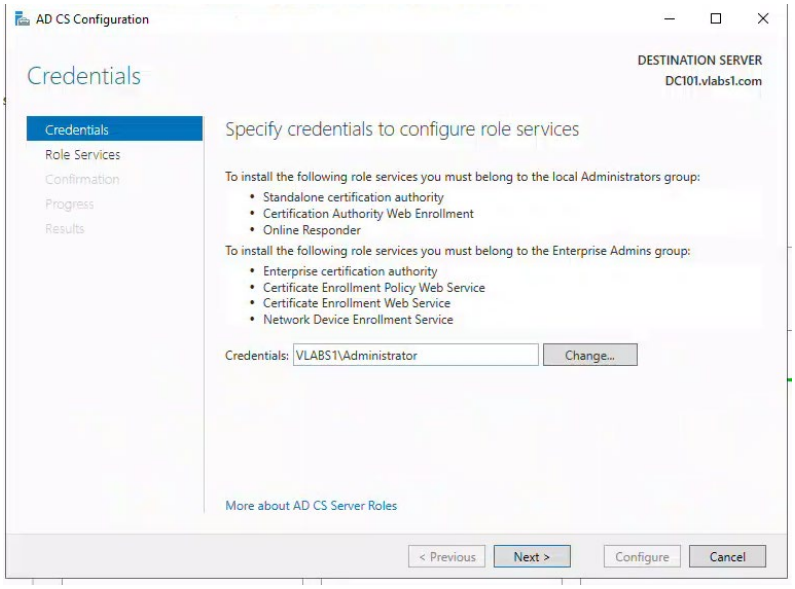


4.3 Configure AD CS other roles on DC101.

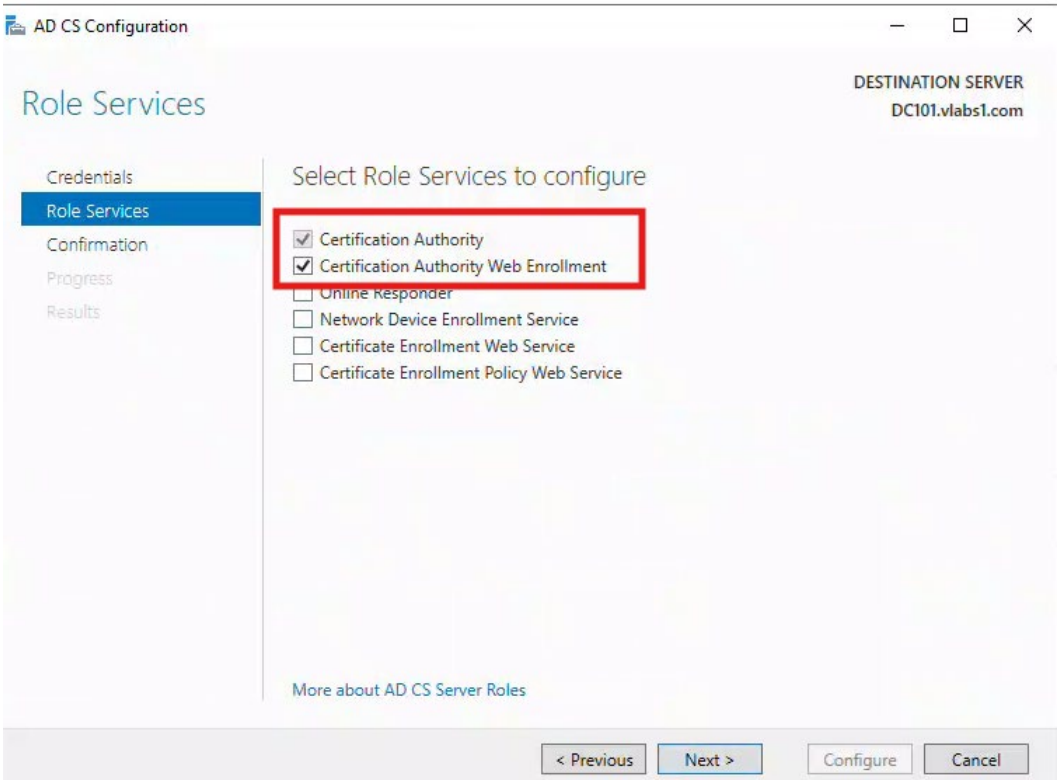
Open server manager
See there is a warning

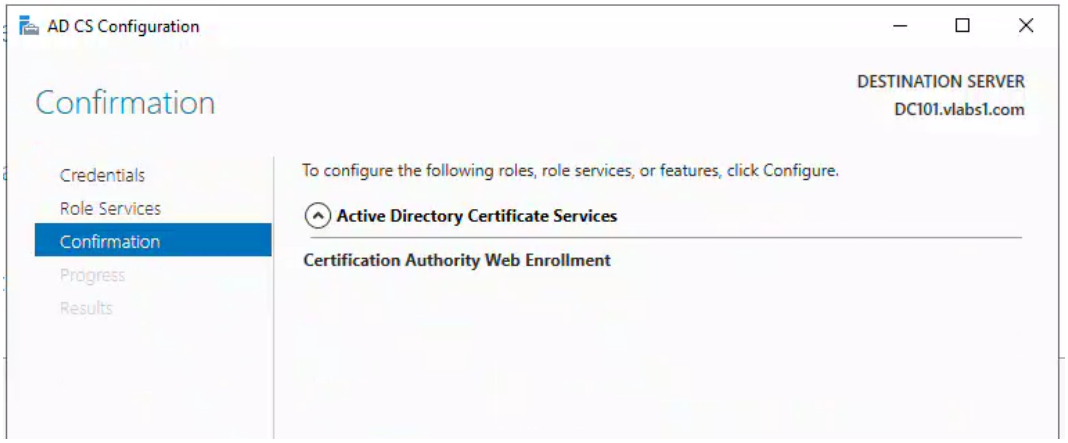


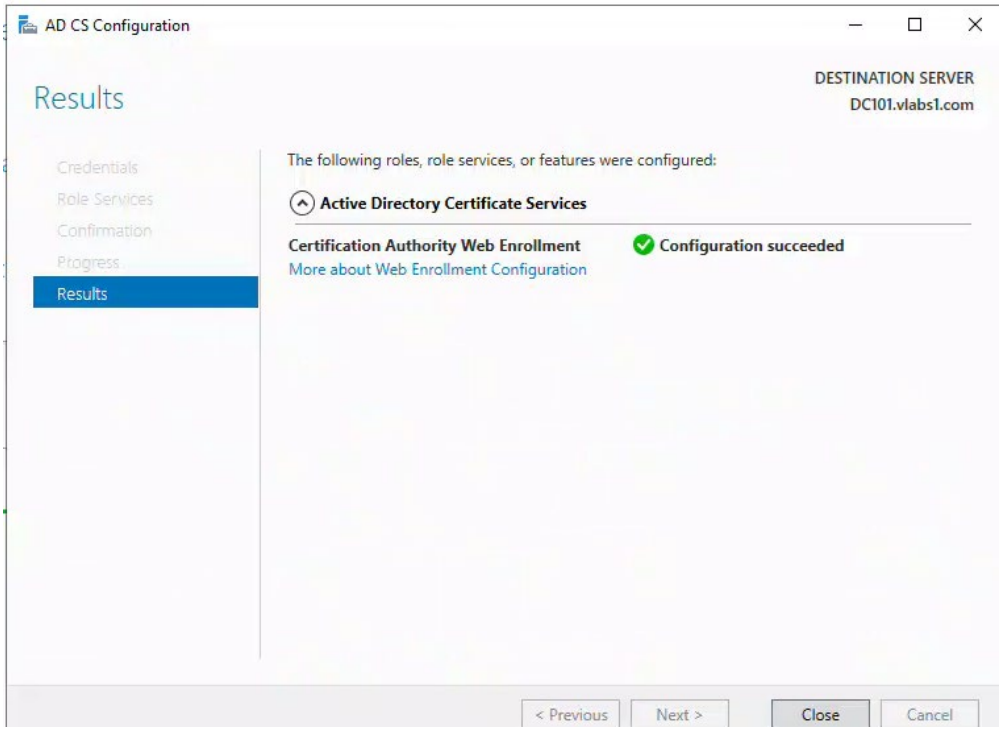


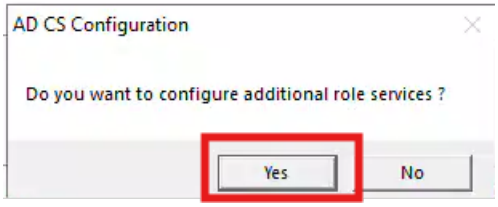


4.3.1 Certification authority and Certificatation Authority Web Enrollment

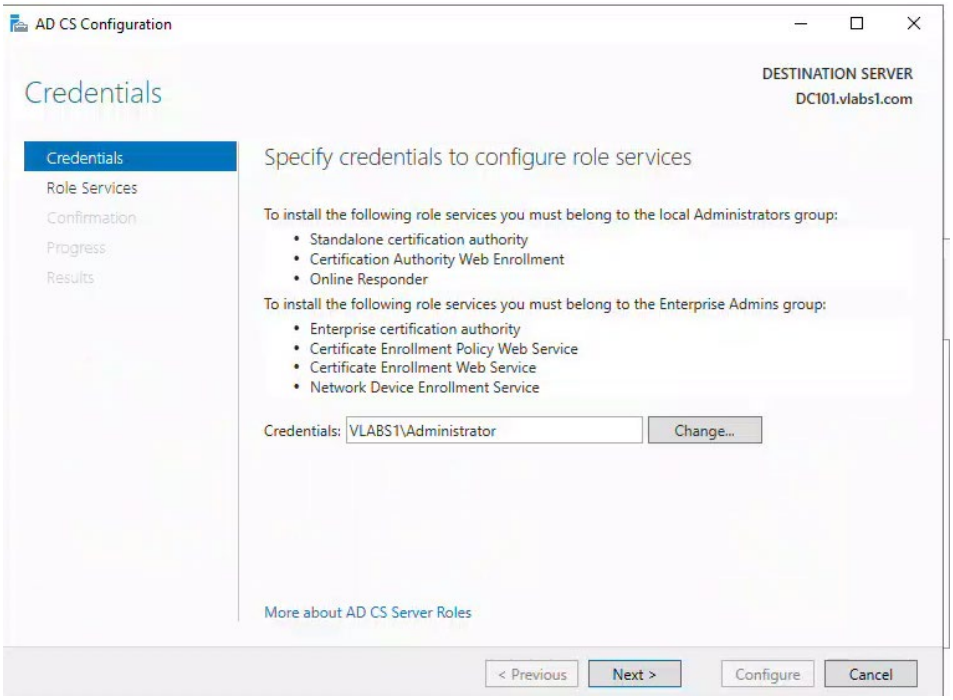


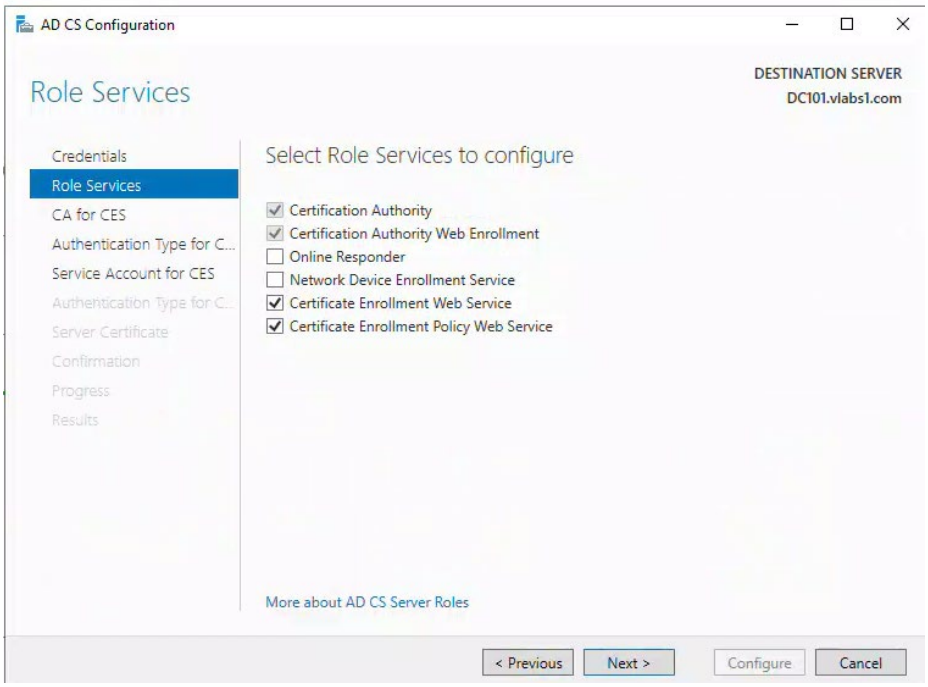


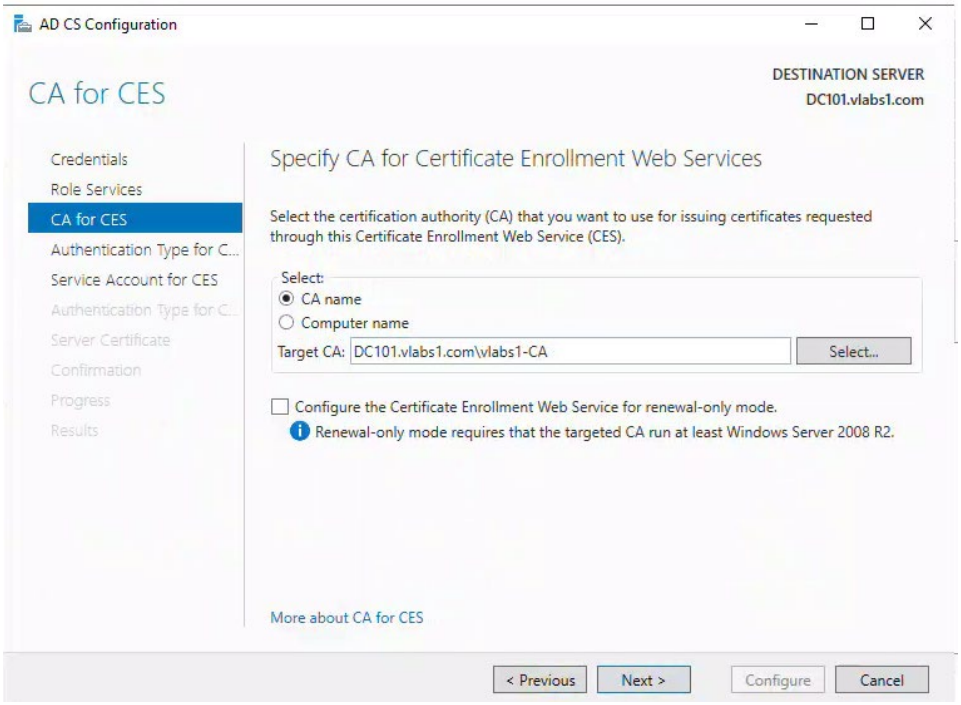


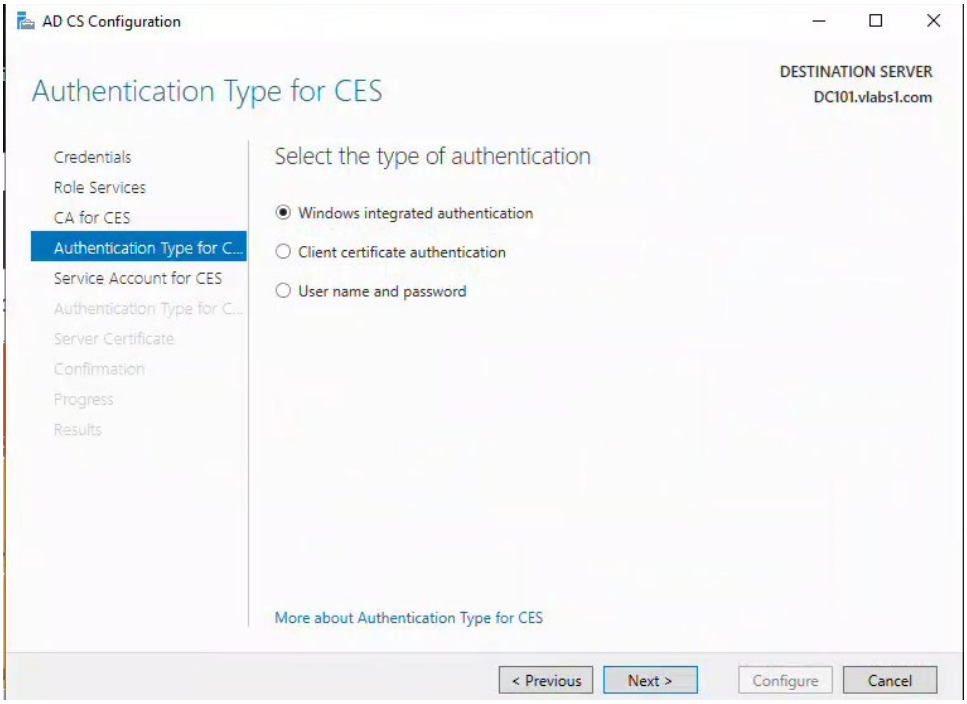


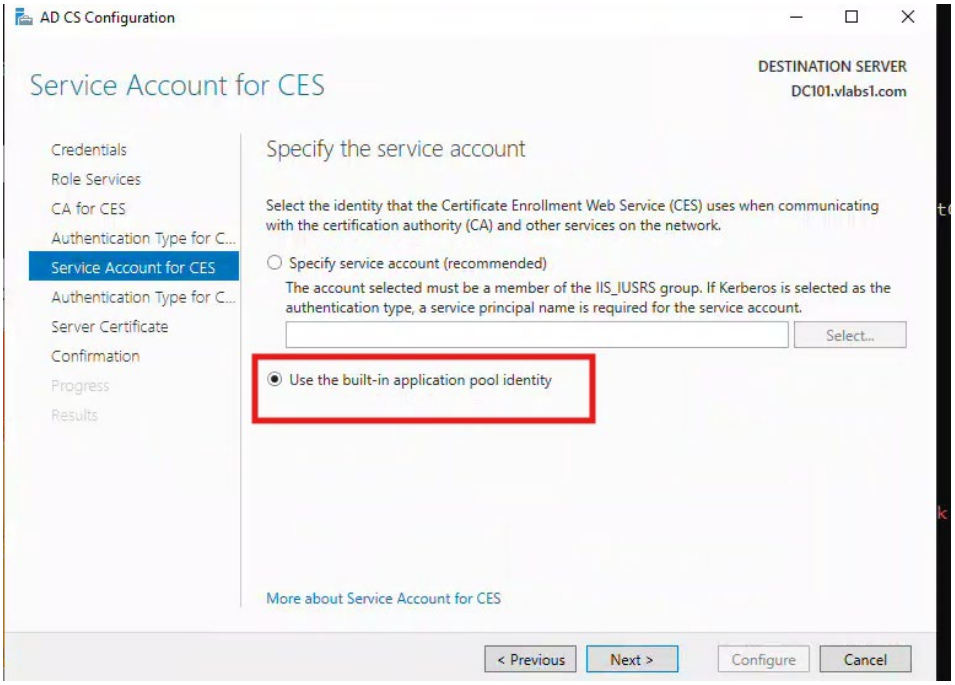
4.3.2 Certificate Enrollment Web Service (CES) and Certificate Enrollment Policy Web Service (CEP)

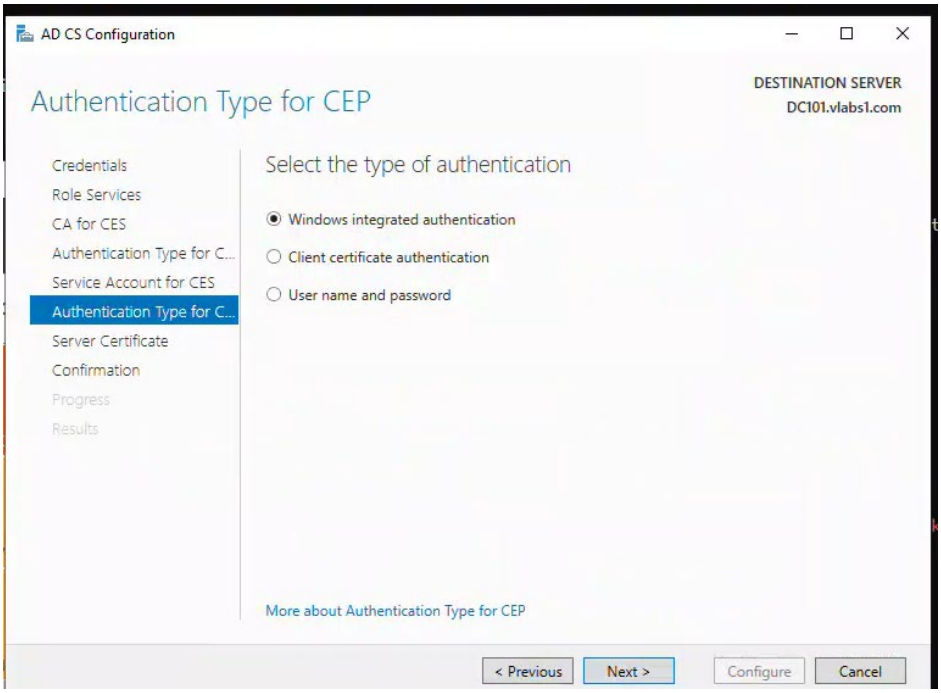

AD CS Configuration
Credentials
DESTINATION SERVER
DC101.vlabs1.com
Credentials
Role Services
Confirmation
Progress
Results
Specify credentials to configure role services
To install the following role services you must belong to the local Administrators group:
• Standalone certification authority
• Certification 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: VLABS1\Administrator
Change...
More about AD CS Server Roles
< Previous
Next >
Configure
Cancel

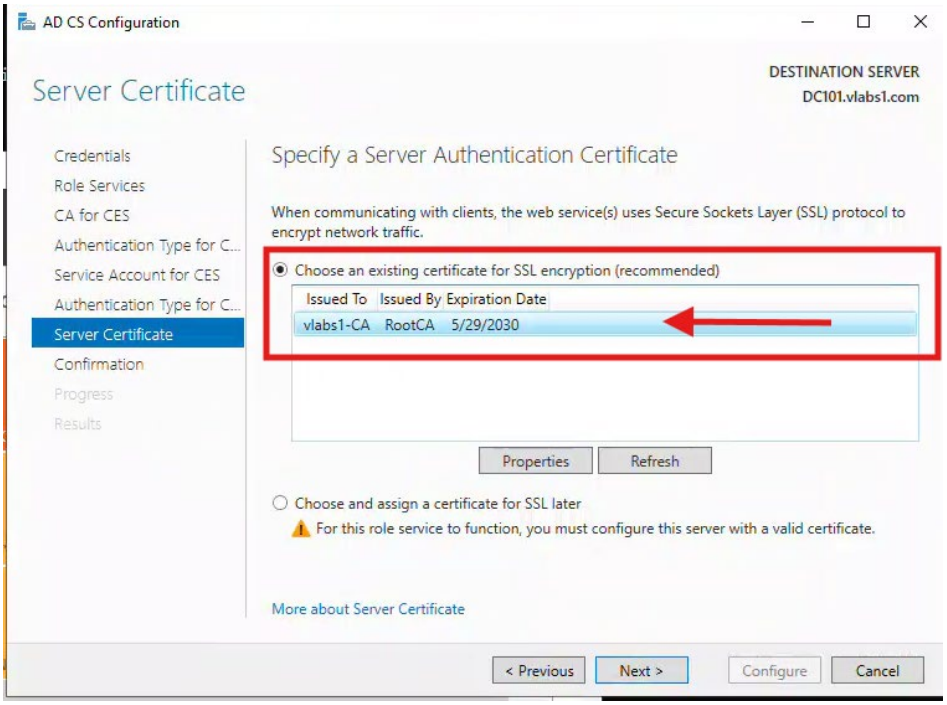

AD CS Configuration
Role Services
DESTINATION SERVER
DC101.vlabs1.com
Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results
Select Role Services to configure
Certification Authority
Certification Authority Web Enrollment
Online Responder
Network Device Enrollment Service
Certificate Enrollment Web Service
Certificate Enrollment Policy Web Service
More about AD CS Server Roles
< Previous
Next >
Configure
Cancel

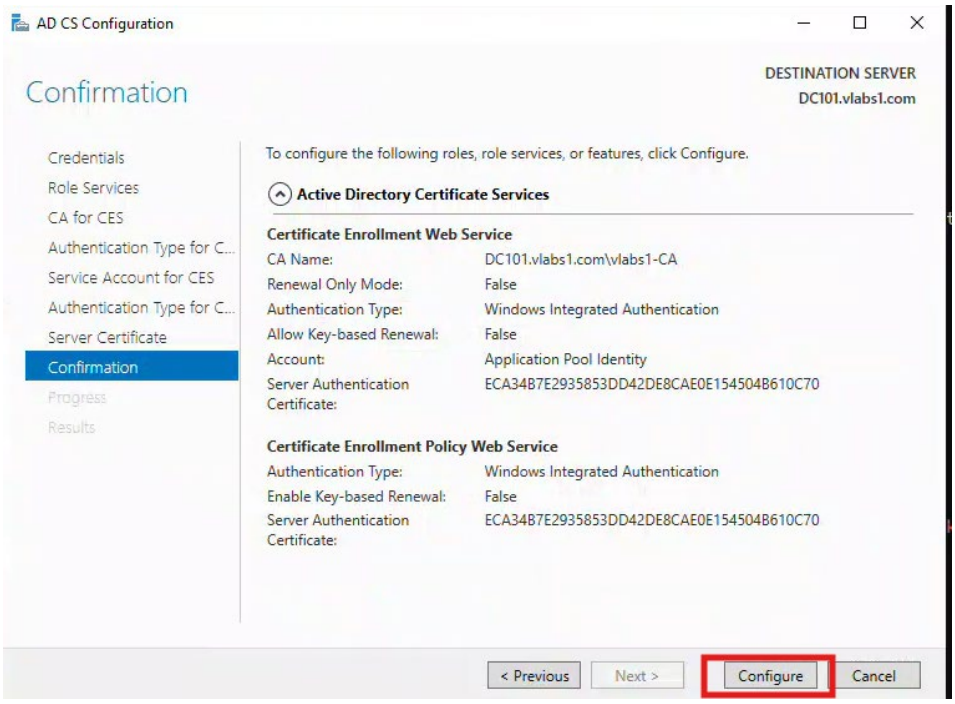

AD CS Configuration
CA for CES
DESTINATION SERVER
DC101.vlabs1.com
Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results
Specify CA for Certificate Enrollment Web Services
Select the certification authority (CA) that you want to use for issuing certificates requested through this Certificate Enrollment Web Service (CES).
Select:
CA name
Computer name
Target CA: DC101.vlabs1.com\vlabs1-CA
Select...
Configure the Certificate Enrollment Web Service for renewal-only mode.
Renewal-only mode requires that the targeted CA run at least Windows Server 2008 R2.
More about CA for CES
< Previous
Next >
Configure
Cancel

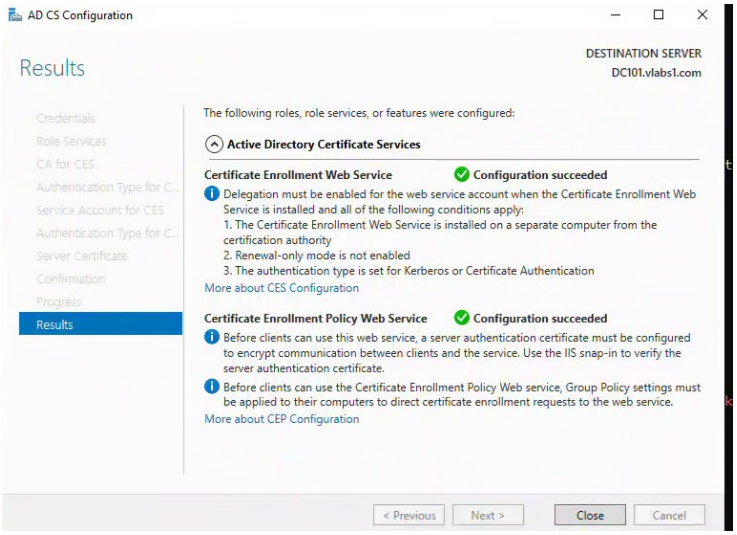

AD CS Configuration
Authentication Type for CES
DESTINATION SERVER
DC101.vlabs1.com
Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results
Select the type of authentication
Windows integrated authentication
Client certificate authentication
User name and password
More about Authentication Type for CES
< Previous
Next >
Configure
Cancel

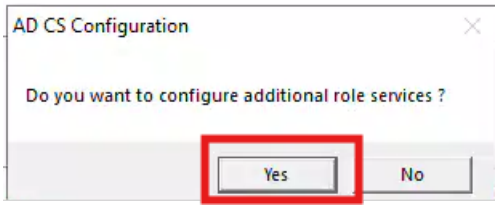

AD CS Configuration
Service Account for CES
DESTINATION SERVER
DC101.vlabs1.com
Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results
Specify the service account
Select the identity that the Certificate Enrollment Web Service (CES) uses when communicating with the certification authority (CA) and other services on the network.
Specify service account (recommended)
The account selected must be a member of the IIS_IUSRS group. If Kerberos is selected as the authentication type, a service principal name is required for the service account.
Select...
Use the built-in application pool identity
More about Service Account for CES
< Previous
Next >
Configure
Cancel


AD CS Configuration
Authentication Type for CEP
DESTINATION SERVER
DC101.vlabs1.com
Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results
Select the type of authentication
Windows integrated authentication
Client certificate authentication
User name and password
More about Authentication Type for CEP
< Previous
Next >
Configure
Cancel


AD CS Configuration
Server Certificate
DESTINATION SERVER
DC101.vlabs1.com
Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results
Specify a Server Authentication Certificate
When communicating with clients, the web service(s) uses Secure Sockets Layer (SSL) protocol to encrypt network traffic.
Choose an existing certificate for SSL encryption (recommended)
Issued To Issued By Expiration Date
vlabs1-CA RootCA 5/29/2030
Properties
Refresh
Choose and assign a certificate for SSL later
For this role service to function, you must configure this server with a valid certificate.
More about Server Certificate
< Previous
Next >
Configure
Cancel

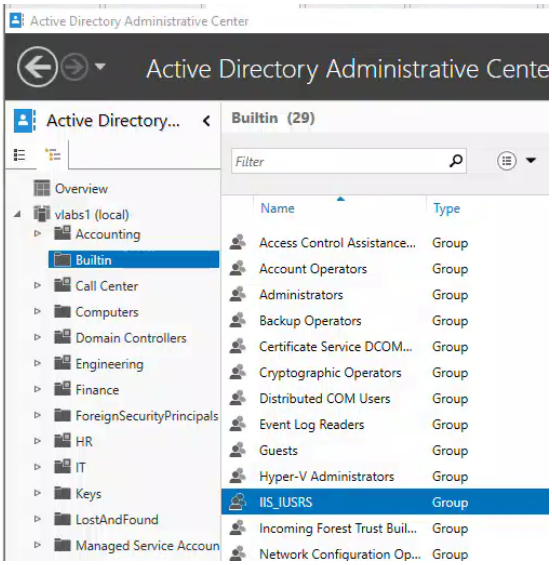

AD CS Configuration
Confirmation
DESTINATION SERVER
DC101.vlabs1.com
Credentials
Role Services
CA for CES
Authentication Type for C...
Service Account for CES
Authentication Type for C...
Server Certificate
Confirmation
Progress
Results
To configure the following roles, role services, or features, click Configure.
Active Directory Certificate Services
Certificate Enrollment Web Service
CA Name: DC101.vlabs1.com\vlabs1-CA
Renewal Only Mode: False
Authentication Type: Windows Integrated Authentication
Allow Key-based Renewal: False
Account: Application Pool Identity
Server Authentication Certificate: ECA34B7E2935853DD42DE8CAE0E154504B610C70
Certificate Enrollment Policy Web Service
Authentication Type: Windows Integrated Authentication
Enable Key-based Renewal: False
Server Authentication Certificate: ECA34B7E2935853DD42DE8CAE0E154504B610C70
< Previous
Next >
Configure
Cancel

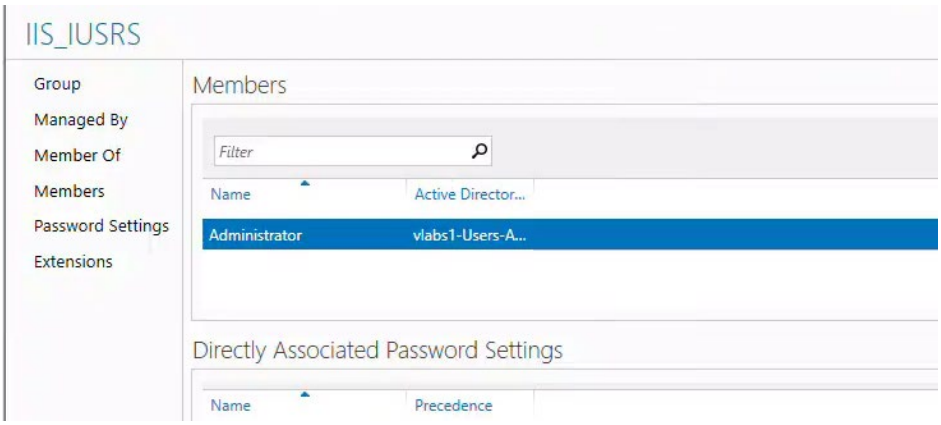


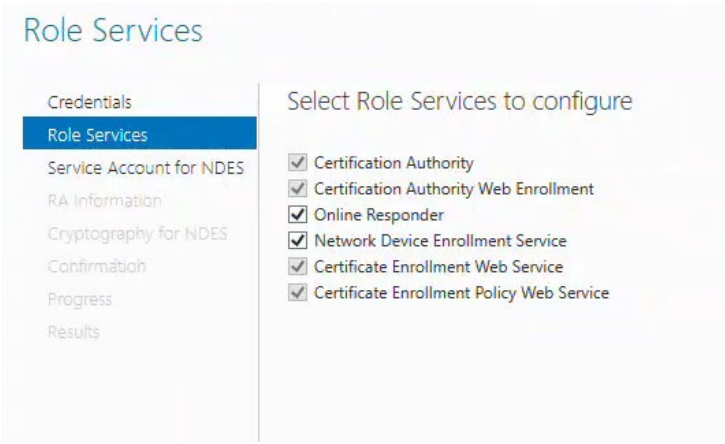


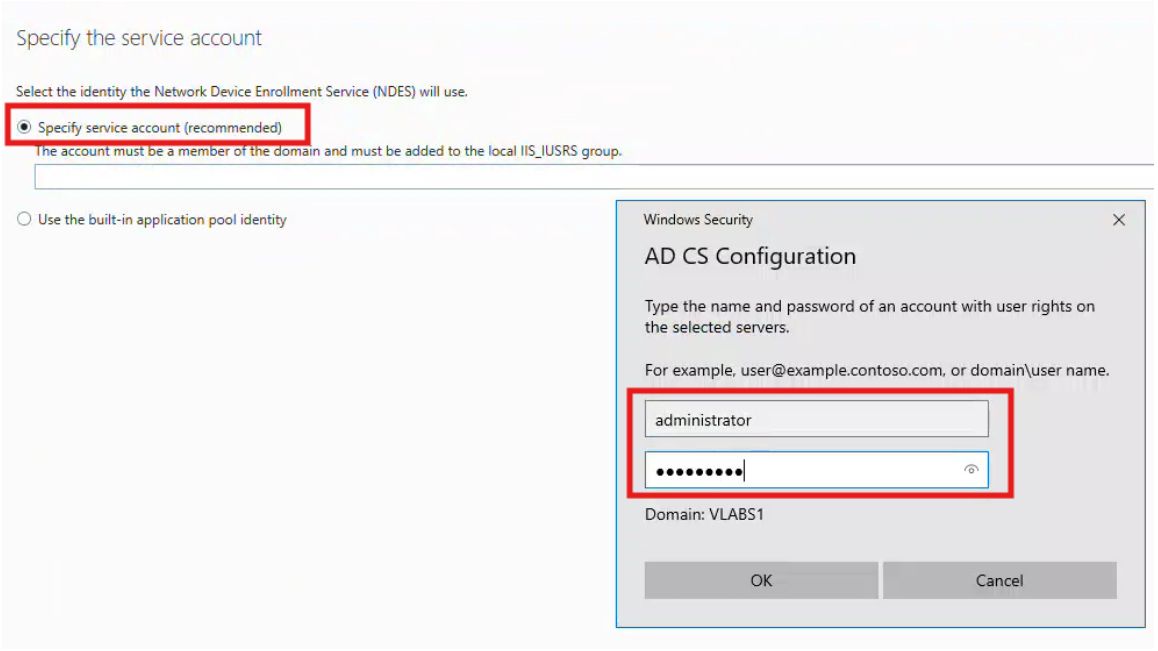
4.3.3 Network Device Enrollment Service & Online responder

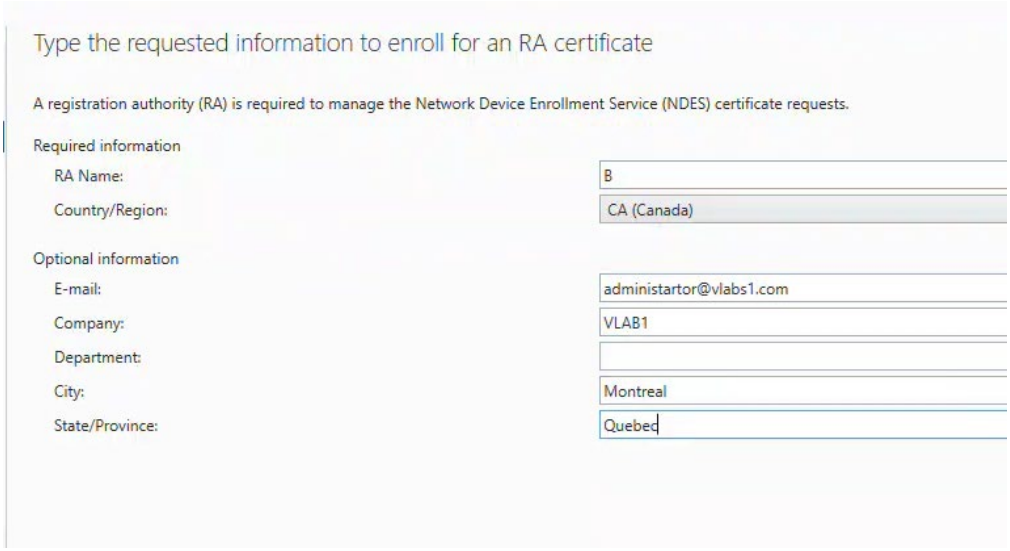
First, add the administrator account to the IIS_IUSRS group.

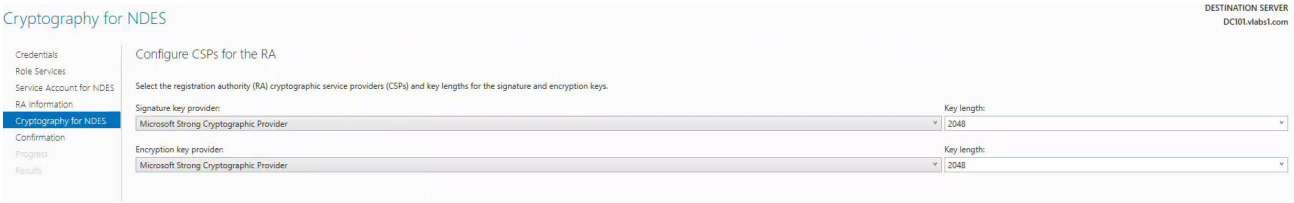


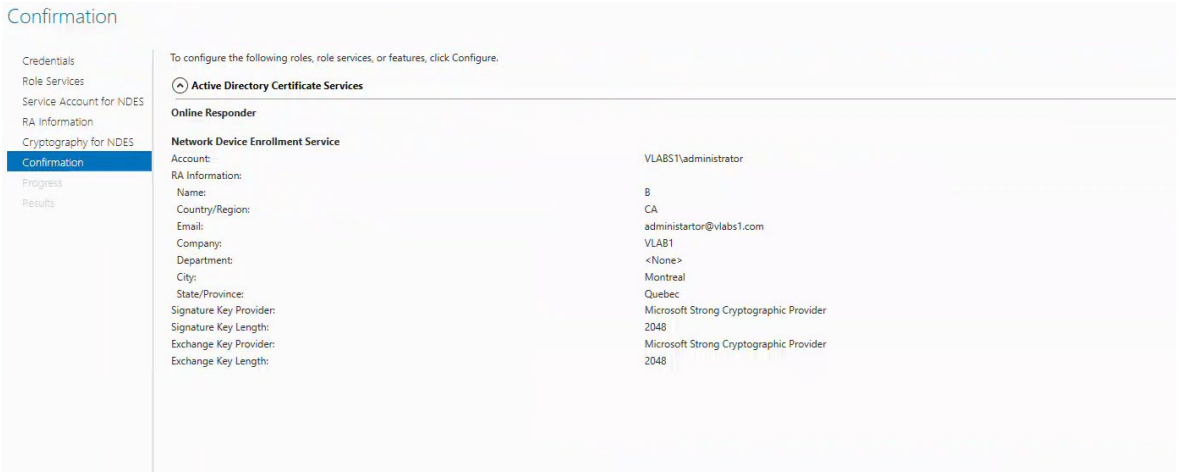

IIS_IUSRS
Group
Managed By
Member Of
Members
Password Settings
Extensions
Members
Filter
Name
Active Director...
Administrator
vlabs1-Users-A...
Directly Associated Password Settings
Name
Precedence

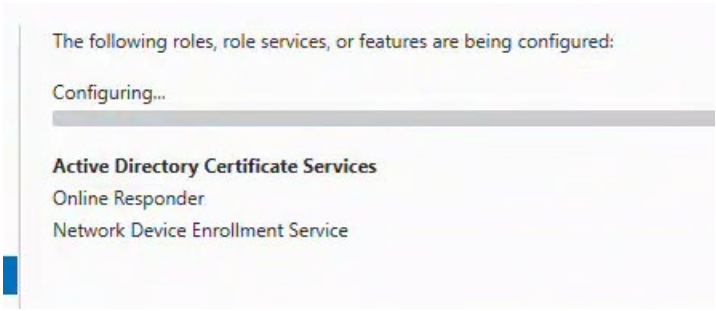

Role Services
Credentials
Role Services
Service Account for NDES
RA Information
Cryptography for NDES
Confirmation
Progress
Results
Select Role Services to configure
Certification Authority
Certification Authority Web Enrollment
Online Responder
Network Device Enrollment Service
Certificate Enrollment Web Service
Certificate Enrollment Policy Web Service

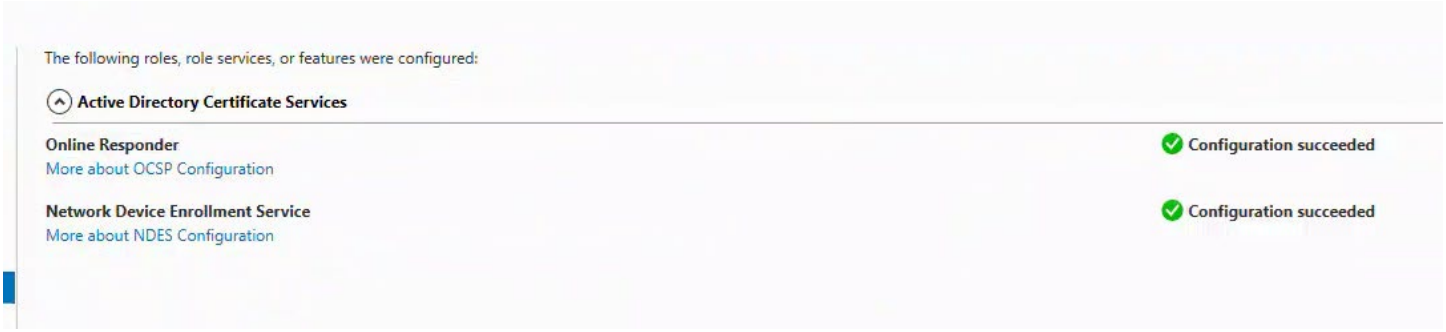

Specify the service account
Select the identity the Network Device Enrollment Service (NDES) will use.
Specify service account (recommended)
The account must be a member of the domain and must be added to the local IIS_IUSRS group.
Use the built-in application pool identity
Windows Security
AD CS Configuration
Type the name and password of an account with user rights on the selected servers.
For example, user@example.contoso.com, or domain\user name.
administrator
Domain: VLABS1
OK
Cancel


Type the requested information to enroll for an RA certificate
A registration authority (RA) is required to manage the Network Device Enrollment Service (NDES) certificate requests.
Required information
RA Name:
B
Country/Region:
CA (Canada)
Optional information
E-mail:
administartor@vlabs1.com
Company:
VLAB1
Department:
City:
Montreal
State/Province:
Quebec


Cryptography for NDES
DESTINATION SERVER
DC101.vlabs1.com
Credentials
Role Services
Service Account for NDES
RA Information
Cryptography for NDES
Confirmation
Progress
Results
Configure CSPs for the RA
Select the registration authority (RA) cryptographic service providers (CSPs) and key lengths for the signature and encryption keys.
Signature key provider:
Microsoft Strong Cryptographic Provider
Key length:
2048
Encryption key provider:
Microsoft Strong Cryptographic Provider
Key length:
2048

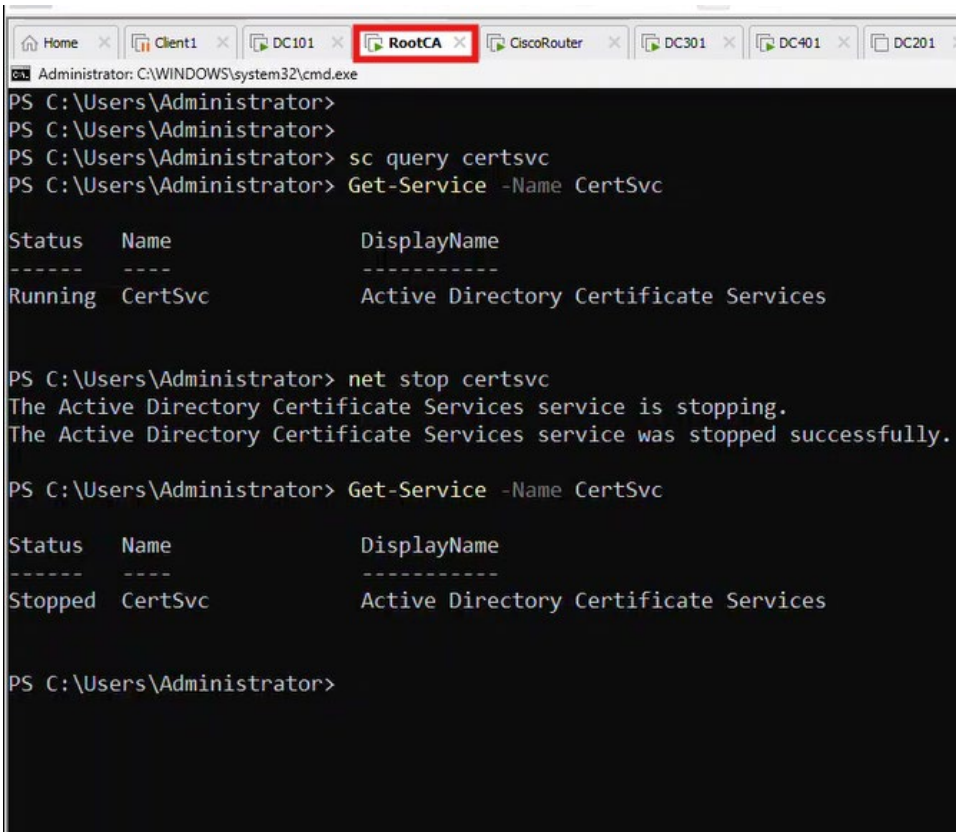

Confirmation
Credentials
Role Services
Service Account for NDES
RA Information
Cryptography for NDES
Confirmation
Progress
Results
To configure the following roles, role services, or features, click Configure.
Active Directory Certificate Services
Online Responder
Network Device Enrollment Service
Account: VLABS1\administrator
RA Information:
Name: B
Country/Region: CA
Email: administartor@vlabs1.com
Company: VLAB1
Department: <None>
City: Montreal
State/Province: Quebec
Signature Key Provider: Microsoft Strong Cryptographic Provider
Signature Key Length: 2048
Exchange Key Provider: Microsoft Strong Cryptographic Provider
Exchange Key Length: 2048


The following roles, role services, or features are being configured:
Configuring...
Active Directory Certificate Services
Online Responder
Network Device Enrollment Service

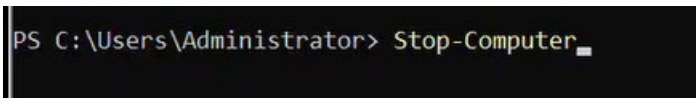


4.4 Secure Root CA and take it offline.

Once setup is complete, take the Root CA offline to protect it from attacks:
Go to the RootCAserver (Standalone):
net stop certsvc



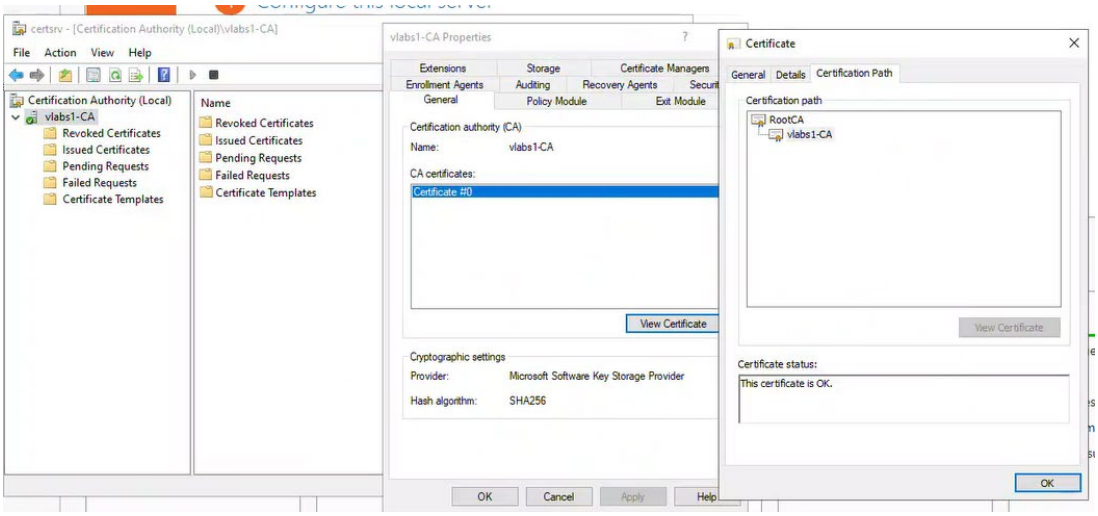
Stop-Computer

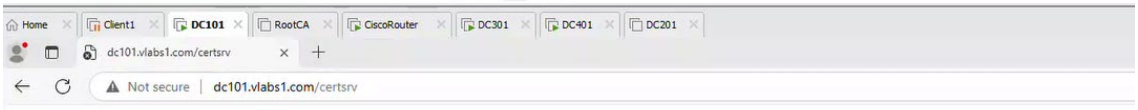


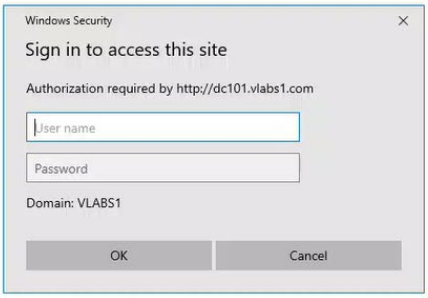
Stops Certificate Services.
Shuts down the Root CA to keep it offline for security.

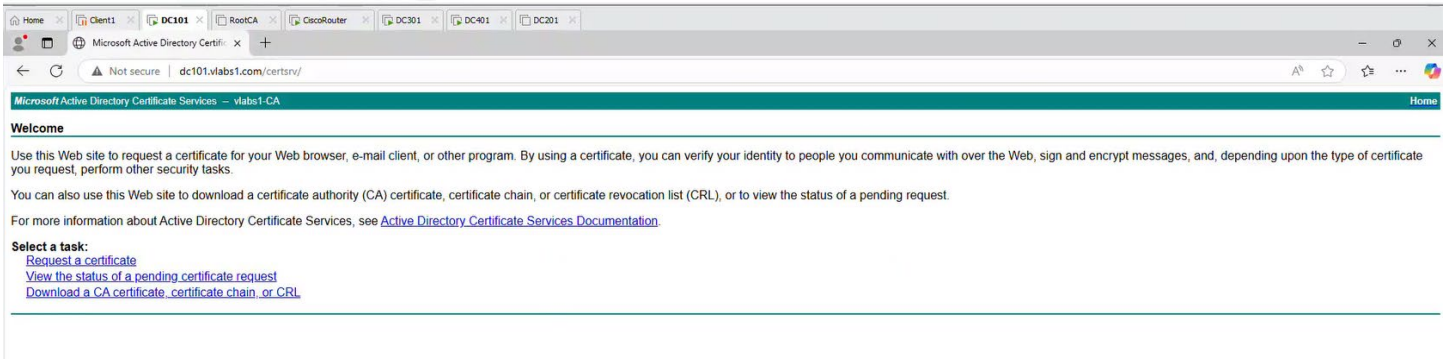
4.5 Verify that Enterprise Subordinate CA is working fine.

Now the Entreprise Subordinate CA Server is ready to issue new certificates








Home
Client1
DC101
RootCA
CiscoRouter
DC301
DC401
DC201
Microsoft Active Directory Certifi
Not secure
dc101.vlabs1.com/certsrv/
Microsoft Active Directory Certificate Services -- vlabs1-CA
Home
Welcome
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.
Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL