Table of Contents

Lab Assignment 3 (Part I)

Task 1 – Deploy an Offline Standalone Root CA on DC207

Objective:

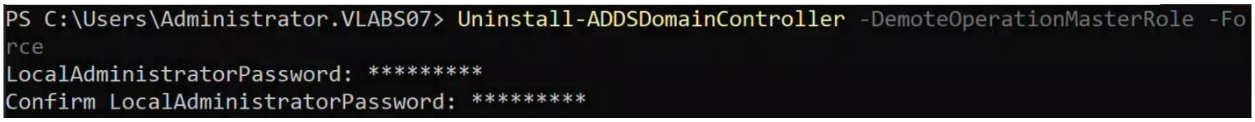
The goal of this task is to create a secure offline Standalone Root Certificate Authority (Root CA).
This Root CA is not part of the domain, and it will issue a certificate to an Enterprise Subordinate CA.
By keeping it offline, we reduce the attack surface and prevent unauthorized certificate issuance.

SYSTEM USED: DC207 (will be renamed to Root07CA)

Step 1 – Demote the Domain Controller

This step removes DC207 from the domain to turn it into an offline standalone server.

```
Uninstall-ADDSDomainController -DemoteOperationMasterRole -Force
```

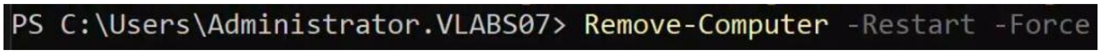


```
PS C:\Users\Administrator.VLABS07> Uninstall-ADDSDomainController -DemoteOperationMasterRole -Fo
rce
LocalAdministratorPassword: *********
Confirm LocalAdministratorPassword: *********
```

Step 2 – Remove the Server from the Domain

After demotion, restart and remove the computer from the domain.

```
Remove-Computer -Restart -Force
```

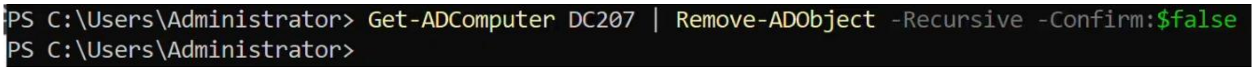


```
PS C:\Users\Administrator.VLABS07> Remove-Computer -Restart -Force
```

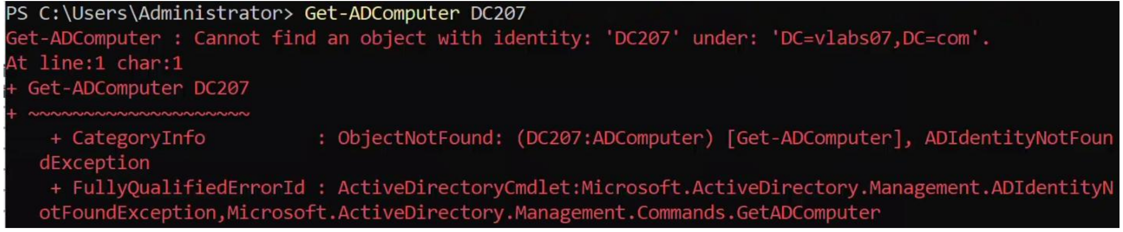
Step 3 – Delete Computer Object from AD (On DC107)

We now clean up the DC207 object from Active Directory.

```
Get-ADComputer DC207 | Remove-ADObject -Recursive -Confirm:$false
```



```
PS C:\Users\Administrator> Get-ADComputer DC207 | Remove-ADObject -Recursive -Confirm:$false
PS C:\Users\Administrator>
```

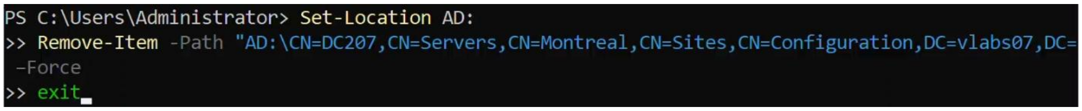


```
PS C:\Users\Administrator> Get-ADComputer DC207
Get-ADComputer : Cannot find an object with identity: 'DC207' under: 'DC=vlabs07,DC=com'.
At line:1 char:1
+ Get-ADComputer DC207
+ ~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (DC207:ADComputer) [Get-ADComputer], ADIdentityNotFoun
   dException
    + FullyQualifiedErrorId : ActiveDirectoryCmdlet:Microsoft.ActiveDirectory.Management.ADIdentityN
   otFoundException,Microsoft.ActiveDirectory.Management.Commands.GetADComputer
```

Step 4 – Remove from AD Sites and Services (On DC107)

This command removes the server from Sites and Services to avoid replication/AD confusion.

```
Set-Location AD:
Remove-Item -Path
"AD:\CN=DC207,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs07,DC=
com" -Force exit
```

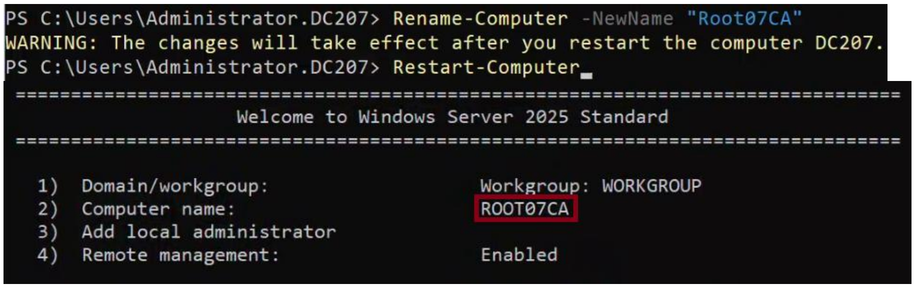


```
PS C:\Users\Administrator> Set-Location AD:
>> Remove-Item -Path "AD:\CN=DC207,CN=Servers,CN=Montreal,CN=Sites,CN=Configuration,DC=vlabs07,DC=
 -Force
>> exit_
```

Step 5 – Rename the Server to Root07CA (On DC207)

We now rename the machine for clarity.

```
Rename-Computer -NewName "Root07CA"
Restart-Computer
```



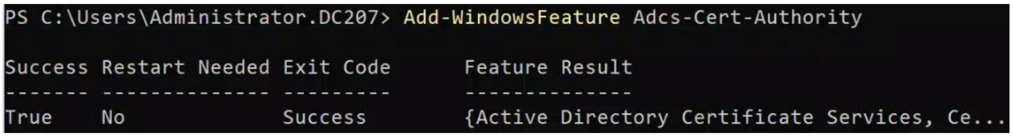
```
PS C:\Users\Administrator.DC207> Rename-Computer -NewName "Root07CA"
WARNING: The changes will take effect after you restart the computer DC207.
PS C:\Users\Administrator.DC207> Restart-Computer_
===============================================================================
                     Welcome to Windows Server 2025 Standard
===============================================================================

  1)  Domain/workgroup:                    Workgroup: WORKGROUP
  2)  Computer name:                       ROOT07CA
  3)  Add local administrator
  4)  Remote management:                   Enabled
```

Step 6 – Install AD CS Role (on Root07CA)

Why this step?
We need to install the Certificate Authority (CA) role so that the server can function as a Standalone Root CA.

```
Add-WindowsFeature Adcs-Cert-Authority
```

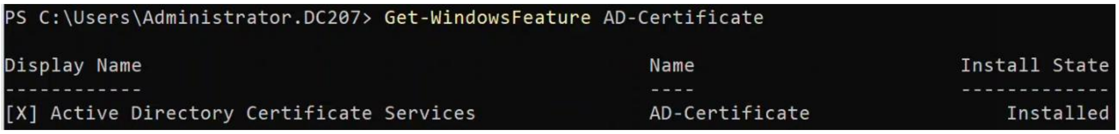
This installs only the certificate services without requiring domain membership.



```
PS C:\Users\Administrator.DC207> Add-WindowsFeature Adcs-Cert-Authority

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

Optional verification:

```
Get-WindowsFeature AD-Certificate
```



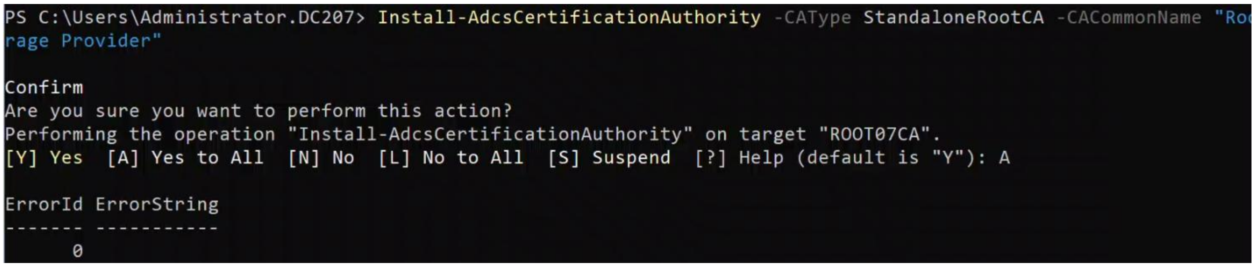
```
PS C:\Users\Administrator.DC207> Get-WindowsFeature AD-Certificate

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

Step 7 – Configure the Standalone Root CA

Why this step?
We now create the actual Root CA on this machine. Since it’s a standalone (offline) CA, we define all settings locally.

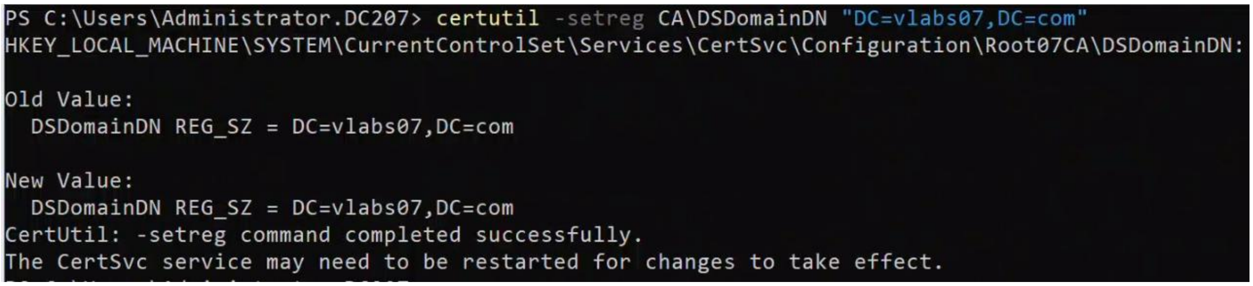
```
Install-AdcsCertificationAuthority `
-CAType StandaloneRootCA `
-CACommonName "Root07CA" `
-KeyLength 4096 `
-HashAlgorithm SHA256 `
-CryptoProviderName "RSA#Microsoft Software Key Storage Provider"
```

Explanation:
- `StandaloneRootCA`: Offline root not integrated with AD
- `CACommonName`: Name shown in certificates
- `KeyLength`: 4096-bit for strong encryption
- `SHA256`: Secure hashing algorithm
- `CryptoProviderName`: Uses Microsoft’s software provider



```
PS C:\Users\Administrator.DC207> Install-AdcsCertificationAuthority -CAType StandaloneRootCA -CACommonName "Ro
rage Provider"

Confirm
Are you sure you want to perform this action?
Performing the operation "Install-AdcsCertificationAuthority" on target "ROOT07CA".
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): A

ErrorId ErrorString
------- -----------
      0
```

When prompted, type 'A' to confirm all.

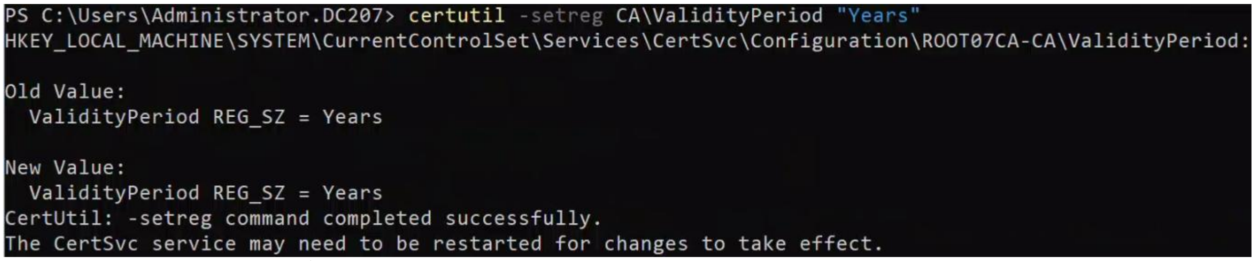


```
PS C:\Users\Administrator.DC207> certutil -setreg CA\DSDomainDN "DC=vlabs07,DC=com"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\Root07CA\DSDomainDN:

Old Value:
  DSDomainDN REG_SZ = DC=vlabs07,DC=com

New Value:
  DSDomainDN REG_SZ = DC=vlabs07,DC=com
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
```

Step 8 – Configure Registry for CA Validity and AD Info

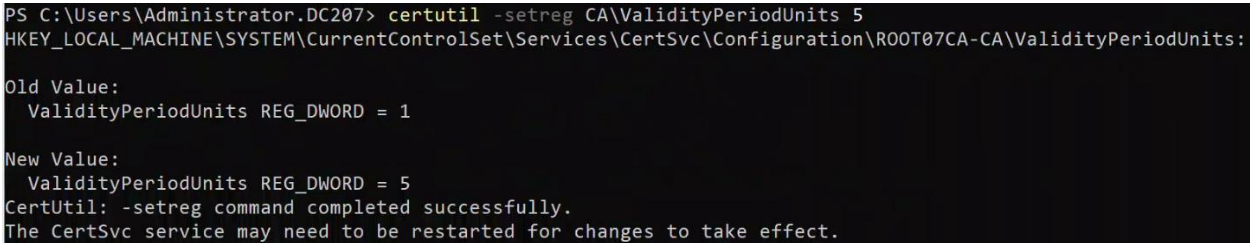
Why this step?
Even though this CA is not domain-joined, we configure it to **embed domain details** in issued certificates (for trust).
We also set certificate validity to 5 years (common for Root CAs).

```
certutil -setreg CA\ValidityPeriod "Years"
```



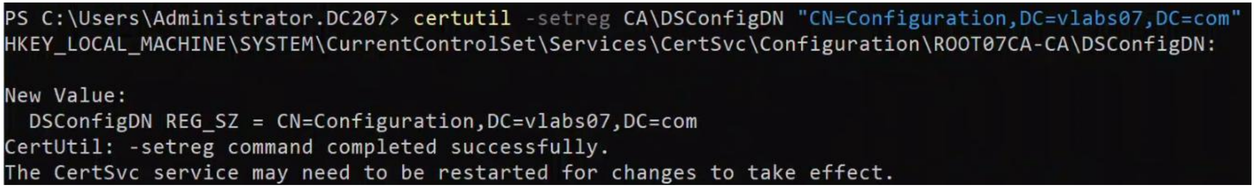
```
PS C:\Users\Administrator.DC207> certutil -setreg CA\ValidityPeriod "Years"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\ROOT07CA-CA\ValidityPeriod:

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.
```

```
certutil -setreg CA\ValidityPeriodUnits 5
```



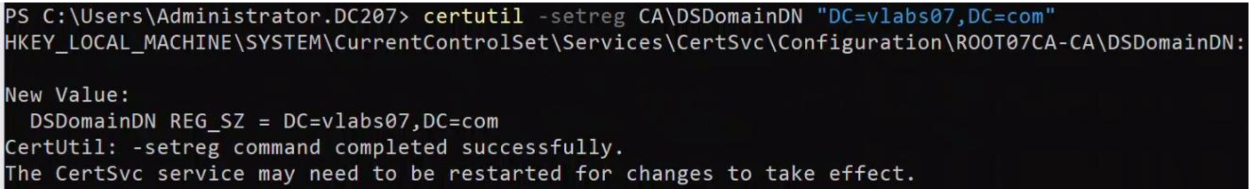
```
PS C:\Users\Administrator.DC207> certutil -setreg CA\ValidityPeriodUnits 5
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\ROOT07CA-CA\ValidityPeriodUnits:

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.
```

```
certutil -setreg CA\DSConfigDN "CN=Configuration,DC=vlabs07,DC=com"
```



```
PS C:\Users\Administrator.DC207> certutil -setreg CA\DSConfigDN "CN=Configuration,DC=vlabs07,DC=com"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\ROOT07CA-CA\DSConfigDN:

New Value:
  DSConfigDN REG_SZ = CN=Configuration,DC=vlabs07,DC=com
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
```

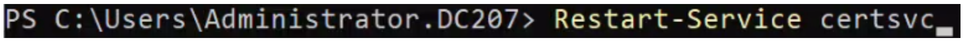
```
certutil -setreg CA\DSDomainDN "DC=vlabs07,DC=com"
```



```
PS C:\Users\Administrator.DC207> certutil -setreg CA\DSDomainDN "DC=vlabs07,DC=com"
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\ROOT07CA-CA\DSDomainDN:

New Value:
  DSDomainDN REG_SZ = DC=vlabs07,DC=com
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
```

Restart the Certificate Services:

```
Restart-Service certsvc
```



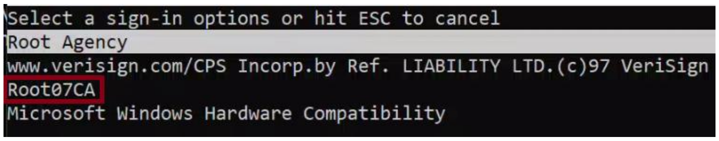
```
PS C:\Users\Administrator.DC207> Restart-Service certsvc_
```

Step 9 – View Root CA Certificate (Optional)

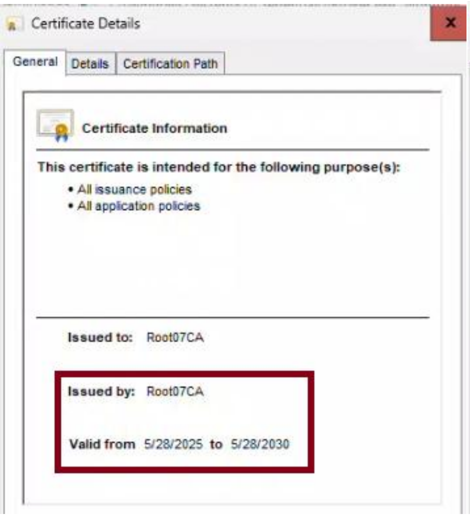
Why this step?
This lets you visually confirm that the Root CA has created its own certificate.

```
certutil -viewstore CA
```

You should see the self-signed Root07CA certificate.



```
Select a sign-in options or hit ESC to cancel
Root Agency
www.verisign.com/CPS Incorp.by Ref. LIABILITY LTD.(c)97 VeriSign
Root07CA
Microsoft Windows Hardware Compatibility
```



Certificate Details

General | Details | Certification Path

Certificate Information

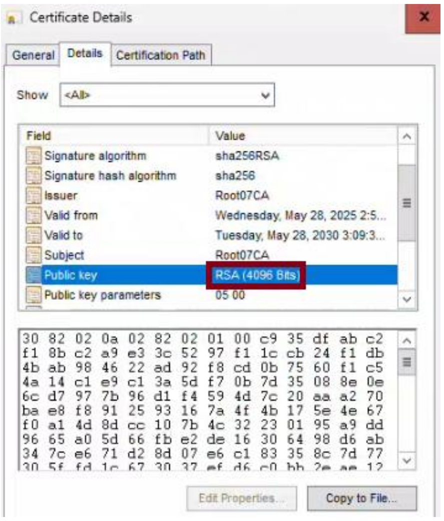
This certificate is intended for the following purpose(s):

- All issuance policies
- All application policies

Issued to: Root07CA

Issued by: Root07CA

Valid from 5/28/2025 to 5/28/2030



Certificate Details

General | Details | Certification Path

Show <All>

Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Root07CA
Valid from	Wednesday, May 28, 2025 2:5...
Valid to	Tuesday, May 28, 2030 3:09:3...
Subject	Root07CA
Public key	RSA (4096 Bits)
Public key parameters	05 00

```
30 82 02 0a 02 82 02 01 00 c9 35 df ab c2
f1 8b c2 a9 e3 3c 52 97 f1 1c cb 24 f1 db
4b ab 98 46 22 ad 92 f8 cd 0b 75 60 f1 c5
4a 14 c1 e9 c1 3a 5d f7 0b 7d 35 08 8e 0e
6c d7 97 7b 96 d1 f4 59 4d 7c 20 aa a2 70
ba e8 f8 91 25 93 16 7a 4f 4b 17 5e 4e 67
f0 a1 4d 8d cc 10 7b 4c 32 23 01 95 a9 dd
96 65 a0 5d 66 fb e2 de 16 30 64 98 d6 ab
34 7c e6 71 d2 8d 07 e6 c1 83 35 8c 7d 77
30 5f fd 1c 67 30 37 ef d6 c0 bb 2e ae 12
```

Step 10 – Modify CDP and AIA from DC107

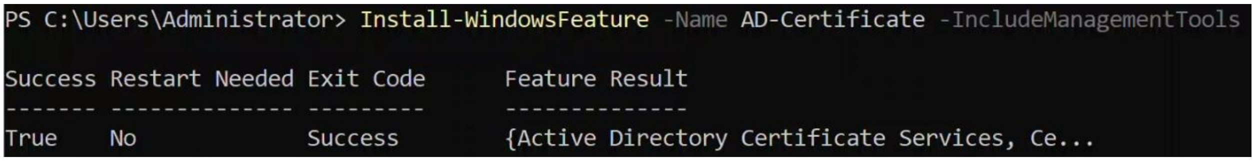
Why this step?

Clients need to know where to download the Root CA certificate (AIA) and where to check certificate revocation (CDP).

Since Root07CA is offline, DC107 will serve these files using HTTP. We will remotely configure the Root CA from DC107.

On DC107, install the CA tools if they are not already installed:

```
Install-WindowsFeature -Name AD-Certificate -IncludeManagementTools
```



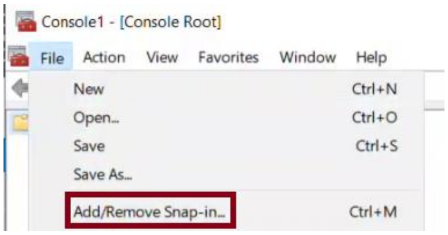
```
PS C:\Users\Administrator> Install-WindowsFeature -Name AD-Certificate -IncludeManagementTools

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

Open MMC:

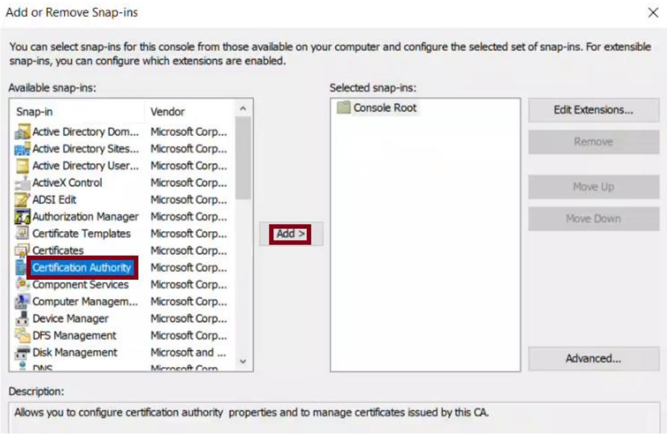
- Press Windows + R, type mmc, and press Enter

Add the Certification Authority snap-in:

- In MMC, go to File > Add/Remove Snap-in



- Select Certification Authority and click Add
- Choose "Another computer"
- Type 192.168.7.2 (IP of Root07CA)
- Click Finish, then OK



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:

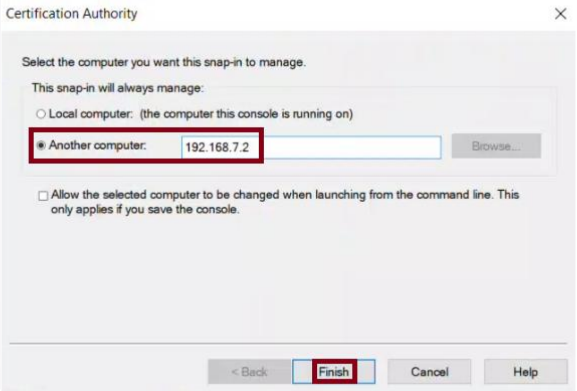
Snap-in	Vendor
Active Directory Dom...	Microsoft Corp...
Active Directory Sites...	Microsoft Corp...
Active Directory User...	Microsoft Corp...
ActiveX Control	Microsoft Corp...
ADSI Edit	Microsoft Corp...
Authorization Manager	Microsoft Corp...
Certificate Templates	Microsoft Corp...
Certificates	Microsoft Corp...
Certification Authority	Microsoft Corp...
Component Services	Microsoft Corp...
Computer Managem...	Microsoft Corp...
Device Manager	Microsoft Corp...
DFS Management	Microsoft Corp...
Disk Management	Microsoft and ...
DNS	Microsoft Corp...

Selected snap-ins:

Console Root

Description:

Allows you to configure certification authority properties and to manage certificates issued by this CA.



Certification Authority

Select the computer you want this snap-in to manage.

This snap-in will always manage:

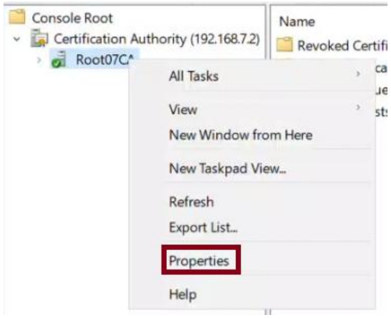
○ Local computer: (the computer this console is running on)

● Another computer: 192.168.7.2

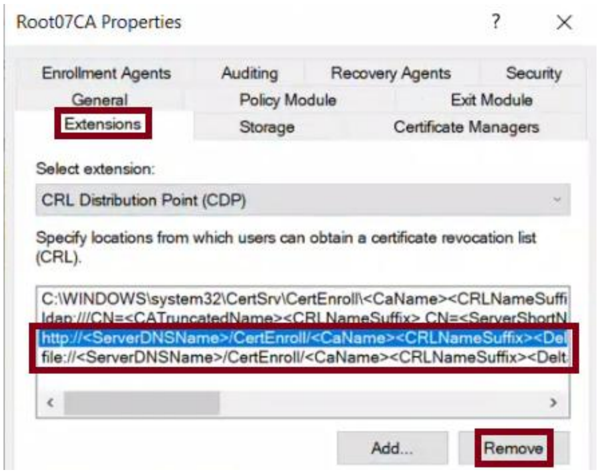
□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

In the left pane of MMC:

- Expand Certification Authority (192.168.7.2) > Root07CA
- Right-click Root07CA and choose Properties
- Click the Extensions tab



Modify CDP entries:
- In the "Select extension" drop-down, choose "CRL Distribution Point (CDP)"
- Remove entries for HTTP and FILE (highlight each and click Remove)



Root07CA Properties

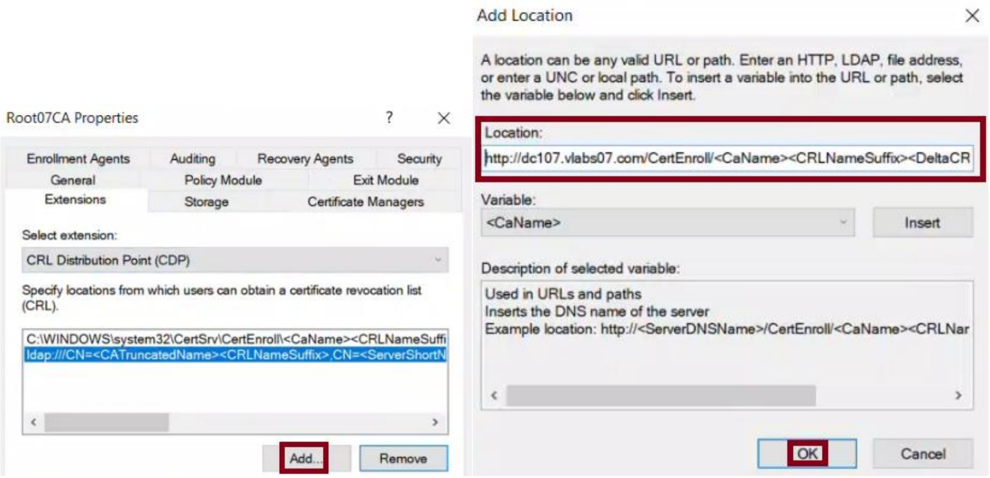
Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

```
C:\WINDOWS\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffi
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortN
http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><Del
file://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><Delt
```

- Click Add and enter the following URL:
http://dc107.vlabs07.com/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl



Select extension:
CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

C:\WINDOWS\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffi
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortN

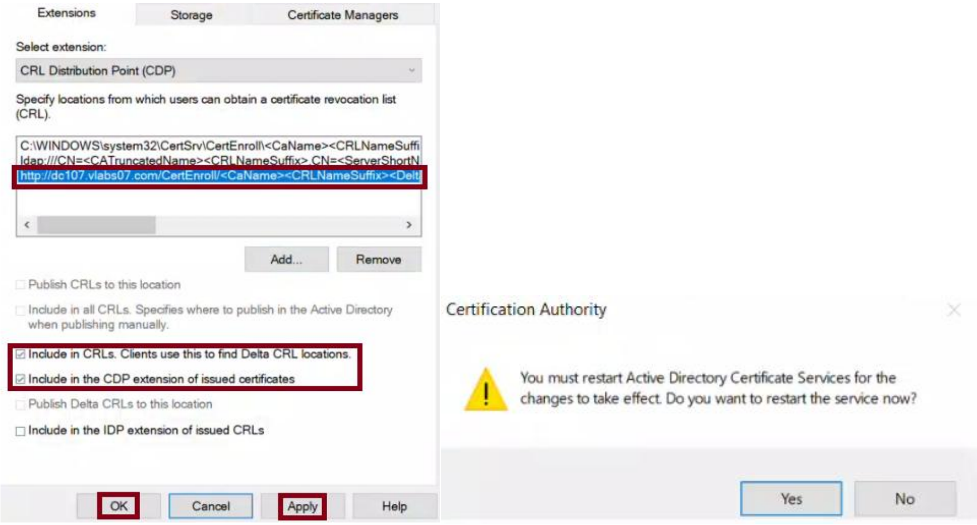
A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

Location:
http://dc107.vlabs07.com/CertEnroll/<CaName><CRLNameSuffix><DeltaCR

Variable:
<CaName>

Description of selected variable:
Used in URLs and paths
Inserts the DNS name of the server
Example location: http://<ServerDNSName>/CertEnroll/<CaName><CRLNar

- Check these options for the new entry:
  - Include in CRLs. Clients use this to find Delta CRL locations
  - Include in the CDP extension of issued certificates



Select extension:
CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

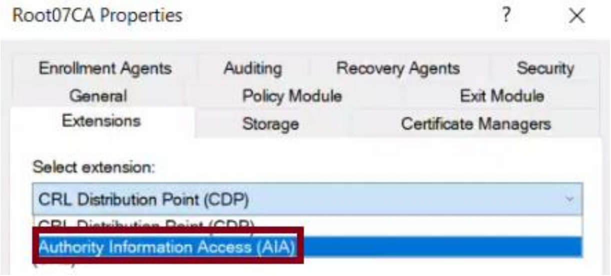
C:\WINDOWS\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffi
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortN
http://dc107.vlabs07.com/CertEnroll/<CaName><CRLNameSuffix><Delt

□ Publish CRLs to this location
□ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.
☑ Include in CRLs. Clients use this to find Delta CRL locations.
☑ Include in the CDP extension of issued certificates
□ Publish Delta CRLs to this location
□ Include in the IDP extension of issued CRLs

You must restart Active Directory Certificate Services for the changes to take effect. Do you want to restart the service now?

Modify AIA entries:

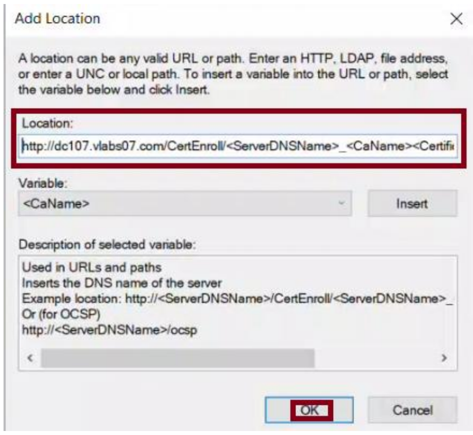
- In the "Select extension" drop-down, choose "Authority Information Access (AIA)"



Select extension:
CRL Distribution Point (CDP)
CRL Distribution Point (CDP)
Authority Information Access (AIA)

- Remove entries for HTTP and FILE (highlight each and click Remove)
- Click Add and enter this URL:

http://dc107.vlabs07.com/CertEnroll/<ServerDNSName>_<CaName><CertificateName>.crt



Add Location

A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.

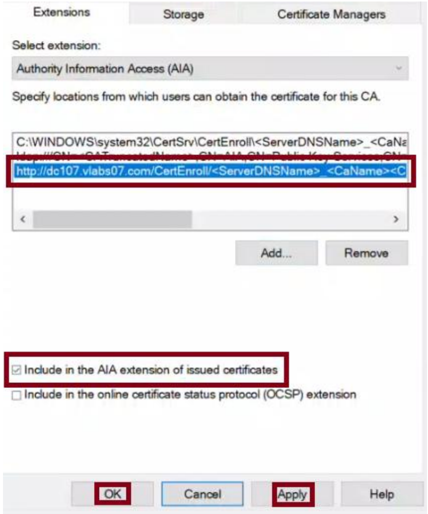
Location:
http://dc107.vlabs07.com/CertEnroll/<ServerDNSName>_<CaName><Certifi

Variable:
<CaName>

Description of selected variable:
Used in URLs and paths
Inserts the DNS name of the server
Example location: http://<ServerDNSName>/CertEnroll/<ServerDNSName>_
Or (for OCSP)
http://<ServerDNSName>/ocsp

- Check this option for the new entry:
- Include in the AIA extension of issued certificates

Click Apply, then OK



Select extension:
Authority Information Access (AIA)

Specify locations from which users can obtain the certificate for this CA.

C:\WINDOWS\system32\CertSrv\CertEnroll\<ServerDNSName>_<CaNa
ldap:///CN=<CATruncatedName>,CN=AIA,CN=Public Key Services,CN=
http://dc107.vlabs07.com/CertEnroll/<ServerDNSName>_<CaName><C

☑ Include in the AIA extension of issued certificates
☐ Include in the online certificate status protocol (OCSP) extension

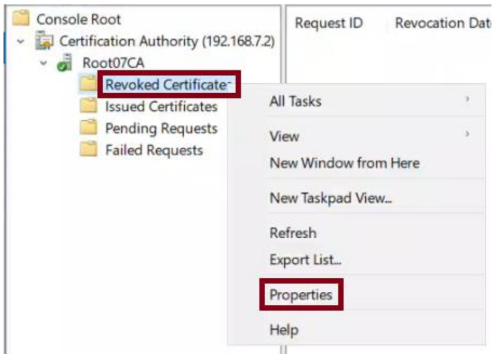
The CA service on Root07CA will restart automatically to apply the new settings

What this achieves:
These settings embed HTTP links into issued certificates. When a client checks a certificate, it will contact DC107 to download the Root CA cert or check for revocation info. This is essential for a working PKI structure with an offline Root CA.

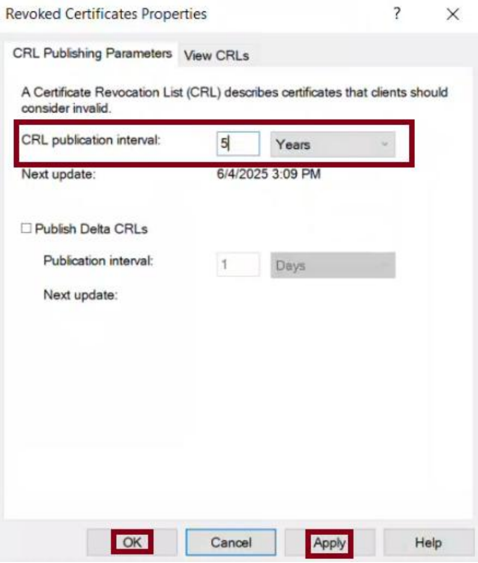
Step 11 - Set CRL Publication Interval to 5 Years

Why this step?
Since the Root CA is offline, it wont be available to republish CRLs frequently. A long publication interval (5 years) is recommended.

• Still in MMC on DC107:
- Go to **Revoked Certificates** > Right-click > **Properties**



- Set the CRL publication interval to **5 years**
- Click OK to apply.


Revoked Certificates Properties

CRL Publishing Parameters | View CRLs

A Certificate Revocation List (CRL) describes certificates that clients should consider invalid.

CRL publication interval: 5 Years

Next update: 6/4/2025 3:09 PM

□ Publish Delta CRLs

Publication interval: 1 Days

Next update:

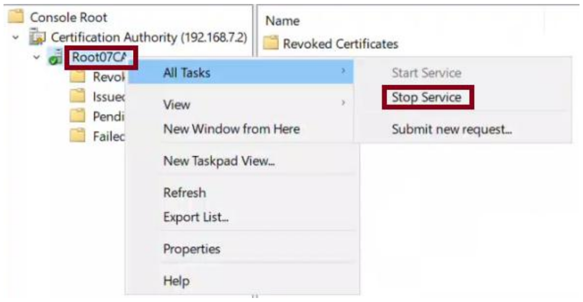
OK Cancel Apply Help

Step 12 - Restart the Root CA Service from MMC (as per course slides)

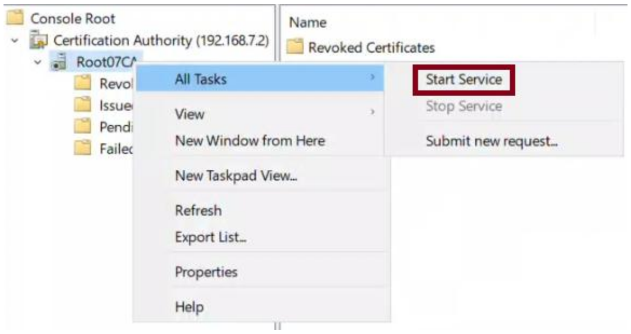
Why this step?
After modifying the CDP and AIA locations, the changes won't take effect until the Certificate Authority (CA) service is restarted.
Instead of rebooting the whole server, we follow the slides and restart the CA service from the MMC console.

On DC107 in the MMC snap-in (already connected to 192.168.7.2):

- In the left pane, right-click on Root07CA
- Go to All Tasks > Stop Service



- Wait a few seconds
- Then go back to All Tasks > Start Service



This applies all CDP and AIA changes without restarting the entire machine.

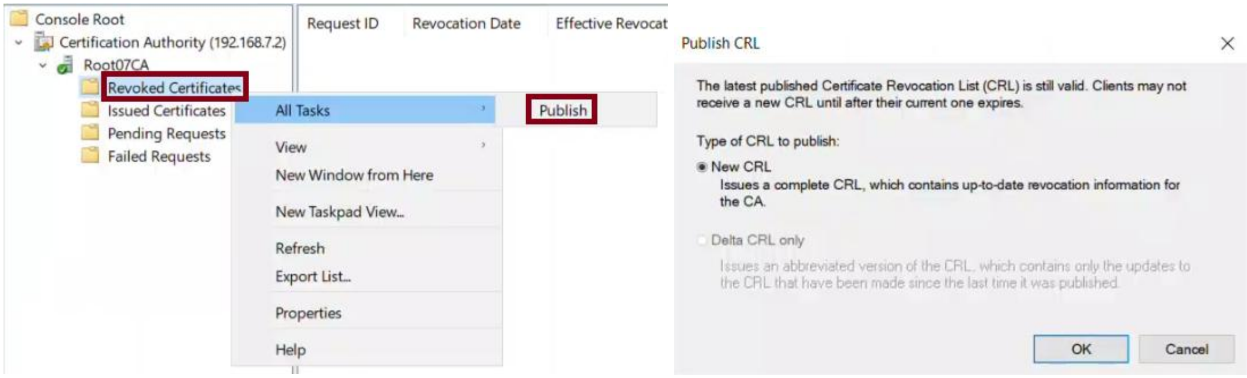
Step 13 - Publish the CRL from MMC

Why this step?
Now that the Root CA has been configured and restarted, we must publish its first Certificate Revocation List (CRL).
This CRL is a critical file that clients use to check if any issued certificates have been revoked.

We do this manually through the GUI

What we do (on DC107 through MMC):

- In the left pane, expand Certification Authority (192.168.7.2)
- Right-click on "Revoked Certificates"
- Go to "All Tasks" > "Publish"



The latest published Certificate Revocation List (CRL) is still valid. Clients may not receive a new CRL until after their current one expires.

Type of CRL to publish:

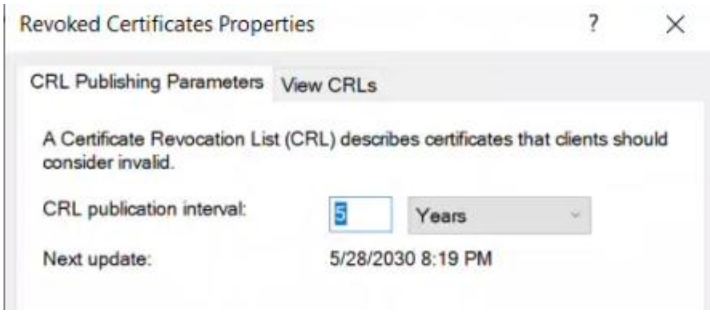
● New CRL
Issues a complete CRL, which contains up-to-date revocation information for the CA.

○ Delta CRL only
Issues an abbreviated version of the CRL, which contains only the updates to the CRL that have been made since the last time it was published.

- In the popup window, make sure "New CRL" is selected
- Click OK to publish the CRL

This will create the .crl file inside:
C:\Windows\System32\CertSrv\CertEnroll

The file includes up-to-date information (even though no certificates are revoked yet), and will be referenced by clients and subordinate CAs to validate trust.



A Certificate Revocation List (CRL) describes certificates that clients should consider invalid.

CRL publication interval: 5 Years

Next update: 5/28/2030 8:19 PM

After publishing, continue with copying the CRL and certificate in Step 14.

Step 14 – Copy Root CA Certificate, CRL, and Private Key to DC107

Why this step?
Now that the Root CA has generated its certificate and CRL, and published it properly, we must copy:

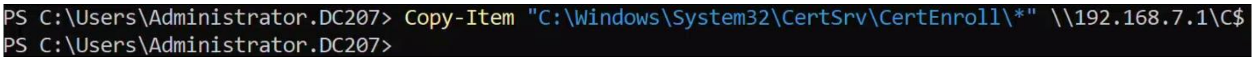
- The Root CA certificate (.crt)
- The CRL (.crl)
- The private key and config (as backup)

We copy these files to DC107 so the Subordinate CA can access them and also back them up for safekeeping.

What we do (on Root07CA = DC207):

Copy the certificate and CRL to DC107:

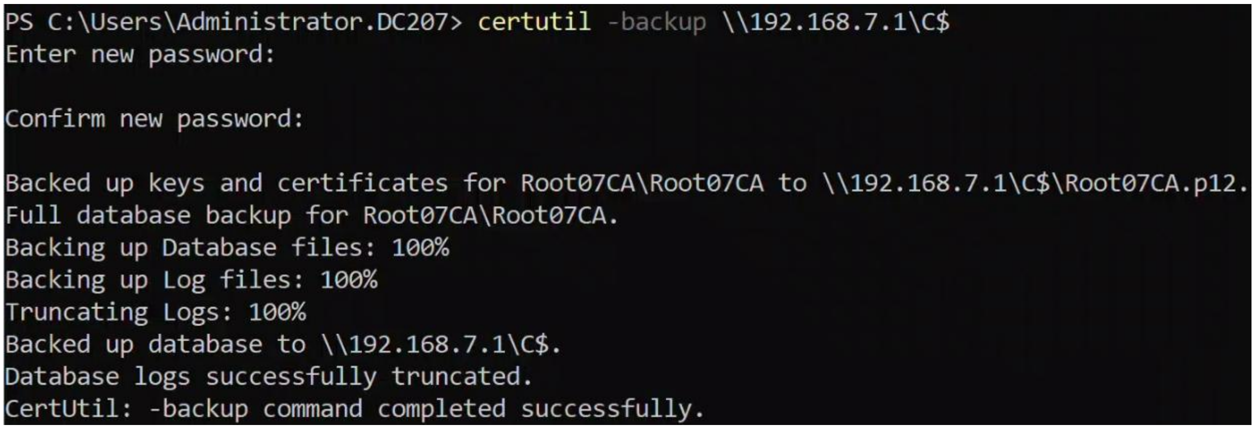
```
Copy-Item "C:\Windows\System32\CertSrv\CertEnroll\*" \\192.168.7.1\C$
```



```
PS C:\Users\Administrator.DC207> Copy-Item "C:\Windows\System32\CertSrv\CertEnroll\*" \\192.168.7.1\C$
PS C:\Users\Administrator.DC207>
```

Back up the CAs private key and configuration:

```
certutil -backup \\192.168.7.1\C$
```



```
PS C:\Users\Administrator.DC207> certutil -backup \\192.168.7.1\C$
Enter new password:

Confirm new password:

Backed up keys and certificates for Root07CA\Root07CA to \\192.168.7.1\C$\Root07CA.p12.
Full database backup for Root07CA\Root07CA.
Backing up Database files: 100%
Backing up Log files: 100%
Truncating Logs: 100%
Backed up database to \\192.168.7.1\C$.
Database logs successfully truncated.
CertUtil: -backup command completed successfully.
```

You will be asked to create a password to protect the private key during the backup.
This backup typically generates:

- A .p12 or .pfx file (contains the private key)
- The Root CA certificate (.crt)
- The CRL (.crl)

Recommendation:
After verifying the files are on DC107 (C:\), you should also copy the private key (.p12) to a USB key and store it offline securely.

This ensures that if the Root CA is ever lost or corrupted, you can restore it from this backup.

At this point, Root07CA is fully set up and ready to issue a certificate to the Subordinate CA.

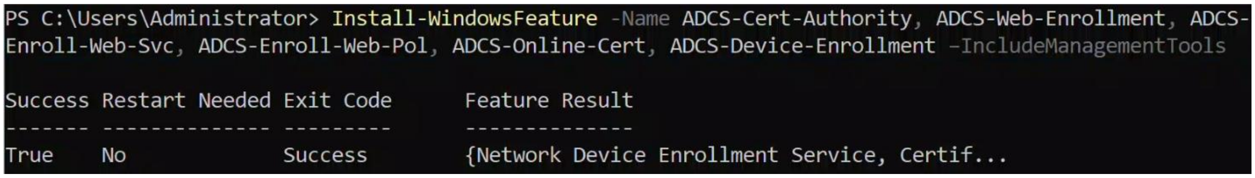
Task 2 – Deploy an Enterprise Subordinate CA on DC107

Step 1 – Install Active Directory Certificate Services with All Features

Why this step?
Before configuring the Subordinate CA, we must install the Certificate Services role and all related features required for enrollment, policy, and web services. These components enable domain-integrated certificate requests and responses.

Run the following command on DC107:

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

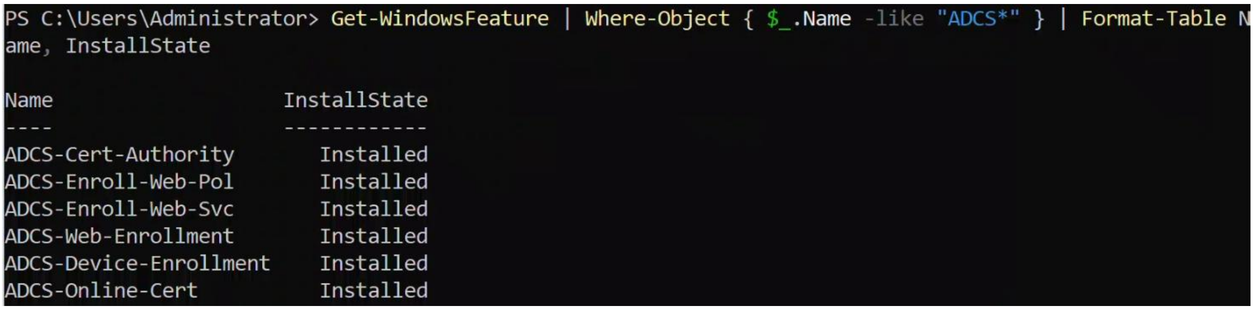


```
PS C:\Users\Administrator> Install-WindowsFeature -Name ADCS-Cert-Authority, ADCS-Web-Enrollment, ADCS-
Enroll-Web-Svc, ADCS-Enroll-Web-Pol, ADCS-Online-Cert, ADCS-Device-Enrollment -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Network Device Enrollment Service, Certif...
```

Explanation:
- ADCS-Cert-Authority: The core Certificate Authority role
- ADCS-Web-Enrollment: Web interface to request and issue certificates
- ADCS-Enroll-Web-Svc: Web service for certificate enrollment
- ADCS-Enroll-Web-Pol: Web policy service
- ADCS-Online-Cert: Online Responder role for revocation checking
- ADCS-Device-Enrollment: Used for enrolling non-domain-joined devices

After installation, verify that all AD CS components are installed:

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



```
PS C:\Users\Administrator> Get-WindowsFeature | Where-Object { $_.Name -like "ADCS*" } | Format-Table N
ame, InstallState

Name                      InstallState
----                      ------------
ADCS-Cert-Authority          Installed
ADCS-Enroll-Web-Pol          Installed
ADCS-Enroll-Web-Svc          Installed
ADCS-Web-Enrollment          Installed
ADCS-Device-Enrollment       Installed
ADCS-Online-Cert             Installed
```

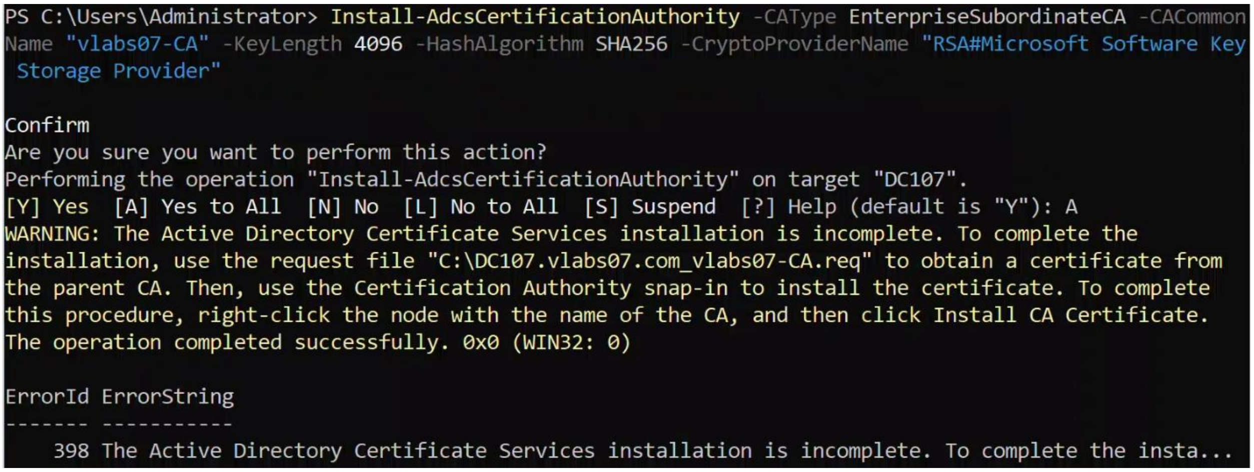
What this achieves:
This installs and prepares all required CA roles on DC107 before we configure the server as an Enterprise Subordinate CA.

Step 2 – Configure the Enterprise Subordinate CA

Why this step?
We are setting up DC107 as an Enterprise Subordinate Certificate Authority.
This server will issue certificates in the domain, but must first be authorized by the offline Root CA.
This step creates the initial certificate request that must be signed by the Root CA.

What we do:
Run the following command on DC107 (your DC1XX server):

```
Install-AdcsCertificationAuthority `
-CAType EnterpriseSubordinateCA `
-CACommonName "vlabs07-CA" `
-KeyLength 4096 `
-HashAlgorithm SHA256 `
-CryptoProviderName "RSA#Microsoft Software Key Storage Provider"
```



```
PS C:\Users\Administrator> Install-AdcsCertificationAuthority -CAType EnterpriseSubordinateCA -CACommon
Name "vlabs07-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 "DC107".
[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:\DC107.vlabs07.com_vlabs07-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 insta...
```

Explanation:
- CAType: EnterpriseSubordinateCA means this CA is domain-integrated but subordinate to a Root CA
- CACommonName: This will appear as the name on the Subordinate CA certificate (vlabs07-CA)
- KeyLength: 4096-bit for strong security
- HashAlgorithm: SHA256 is the industry standard secure hashing algorithm
- CryptoProviderName: Uses Microsoft's RSA provider to generate private/public key pairs

During the process, type A (for "Yes to All") when prompted.

What happens after:
After executing the command, the system will generate a warning message like this:

WARNING: The Active Directory Certificate Services installation is incomplete.

To complete the installation, use the request file
"C:\DC107.vlabs07.com_vlabs07-CA.req"
to obtain a certificate from the parent CA (Root07CA).

This is normal — it means the request was generated successfully.

In Step 3, we'll copy this `.req` file to Root07CA, sign it, and return the signed certificate to complete the Subordinate CA setup.

Step 3 – Submit the Subordinate CA Request and Complete the Installation

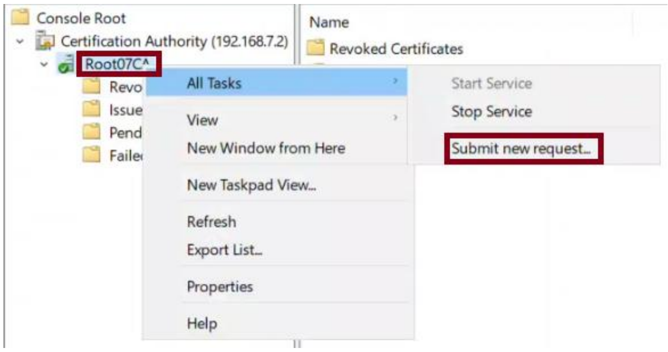
Why this step?
After running the setup command in Step 2 on DC107, a certificate request (.req) was created.
In this step, we use the MMC snap-in on DC107 to connect to Root07CA remotely, submit the request, issue the certificate, and bring it back to DC107 to complete the Subordinate CA installation.

Part A – Submit the Request via MMC from DC107

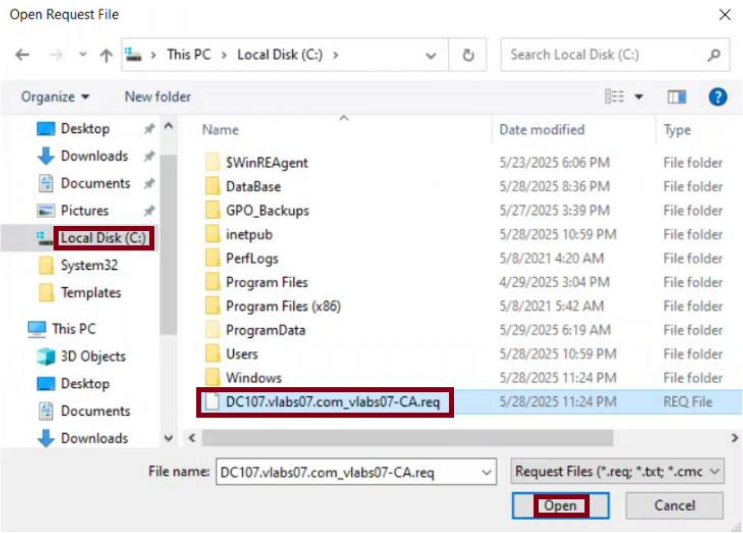
1. On DC107, open the MMC console:
   - Press Windows + R → type mmc → press Enter

2. Add the Certification Authority snap-in:
   - File → Add/Remove Snap-in
   - Select Certification Authority → Add
   - Choose "Another computer" and enter 192.168.7.2 (IP of Root07CA)
   - Click Finish, then OK

3. In MMC:
   - Expand the connected Root07CA
   - Right-click on Root07CA → All Tasks → Submit new request...



- Browse to:
  C:\DC107.vlabs07.com_vlabs07-CA.req
- Select and click Open

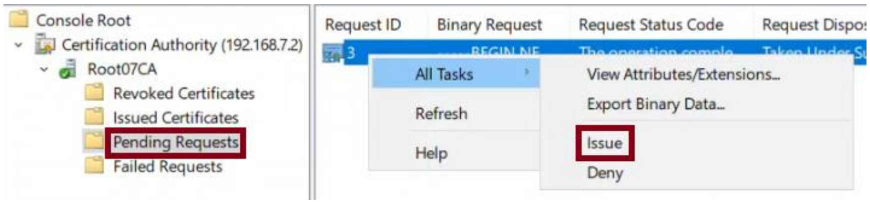


Name	Date modified	Type
$WinREAgent	5/23/2025 6:06 PM	File folder
DataBase	5/28/2025 8:36 PM	File folder
GPO_Backups	5/27/2025 3:39 PM	File folder
inetpub	5/28/2025 10:59 PM	File folder
PerfLogs	5/8/2021 4:20 AM	File folder
Program Files	4/29/2025 3:04 PM	File folder
Program Files (x86)	5/8/2021 5:42 AM	File folder
ProgramData	5/29/2025 6:19 AM	File folder
Users	5/28/2025 10:59 PM	File folder
Windows	5/28/2025 11:24 PM	File folder
DC107.vlabs07.com_vlabs07-CA.req	5/28/2025 11:24 PM	REQ File

File name: DC107.vlabs07.com_vlabs07-CA.req

Request Files (*.req; *.txt; *.cmc

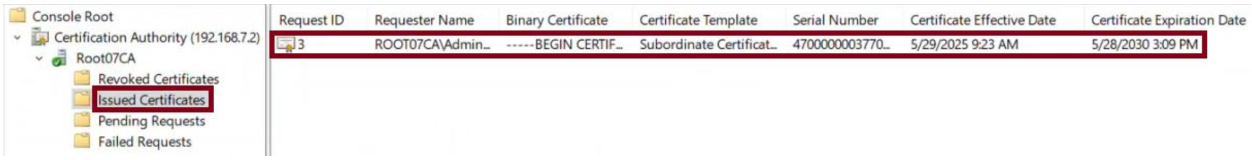
4. Wait a few seconds, then go to “Pending Requests”
   - Right-click the new request → All Tasks → Issue



Request ID	Binary Request	Request Status Code	Request Dispo:
3	-----BEGIN NE	The operation comple	Taken Under Su

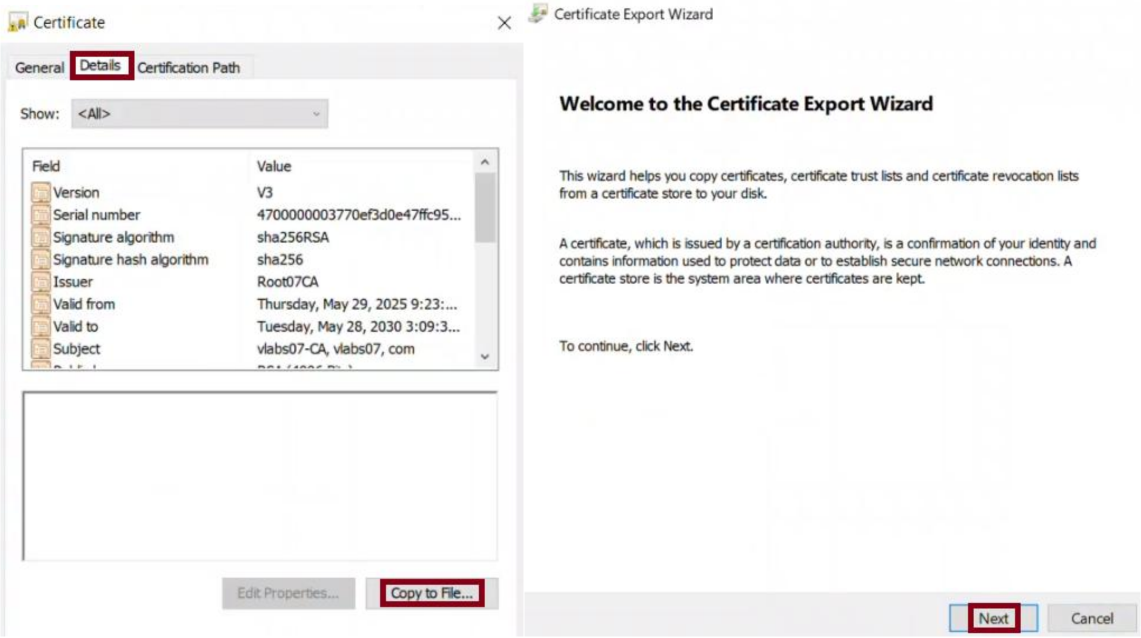
Part B – Export the Issued Certificate in PKCS7 Format

1. Go to “Issued Certificates”
   - Double-click the newly issued certificate



Request ID	Requester Name	Binary Certificate	Certificate Template	Serial Number	Certificate Effective Date	Certificate Expiration Date
3	ROOT07CA\Admin...	-----BEGIN CERTIF...	Subordinate Certificat...	4700000003770...	5/29/2025 9:23 AM	5/28/2030 3:09 PM

- Go to the "Details" tab → Click "Copy to File..."



Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	4700000003770ef3d0e47ffc95...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Root07CA
Valid from	Thursday, May 29, 2025 9:23:...
Valid to	Tuesday, May 28, 2030 3:09:3...
Subject	vlabs07-CA, vlabs07, com

Certificate Export Wizard

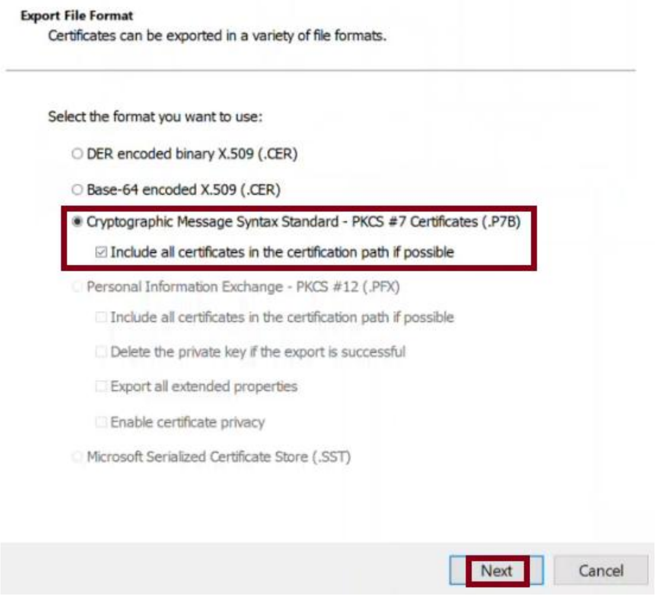
Welcome to the Certificate Export Wizard

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.

2. In the wizard:
   - Choose: Cryptographic Message Syntax Standard - PKCS 7 (.P7B)
   - Check: “Include all certificates in the certification path if possible”



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

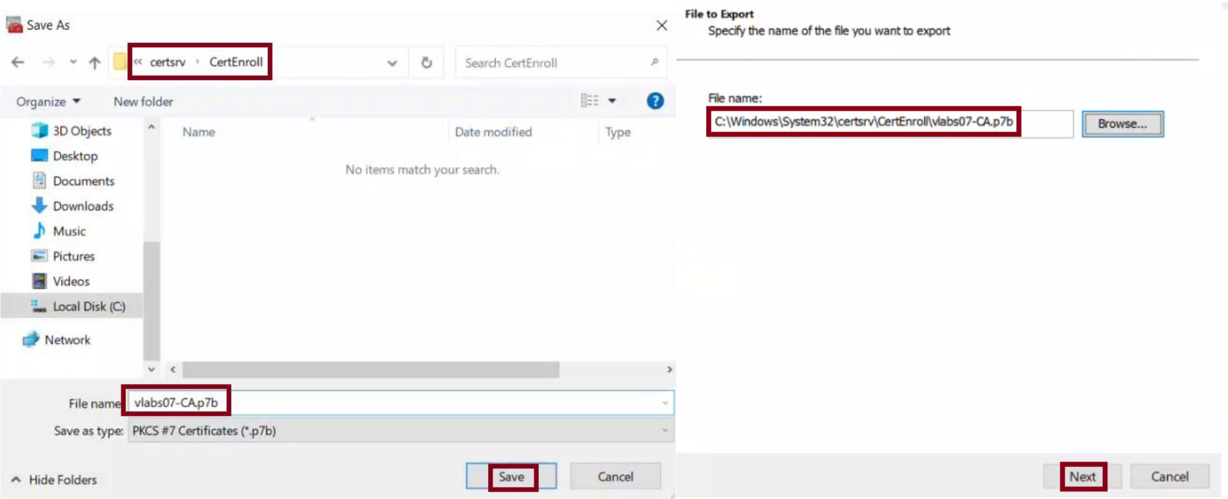
 □ Delete the private key if the export is successful

 □ Export all extended properties

 □ Enable certificate privacy

○ Microsoft Serialized Certificate Store (.SST)

- Save it to:
  C:\Windows\System32\certsrv\CertEnroll\vlabs07-CA.p7b



File name: vlabs07-CA.p7b

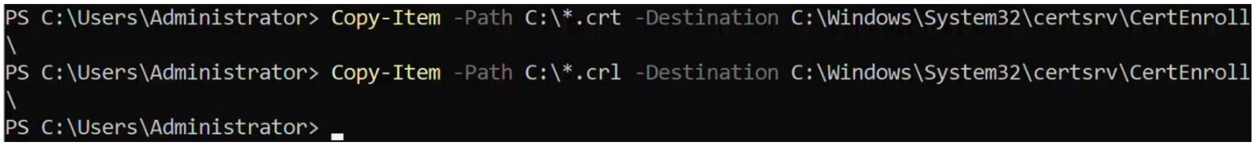
Save as type: PKCS #7 Certificates (*.p7b)

File name: C:\Windows\System32\certsrv\CertEnroll\vlabs07-CA.p7b

3. Copy the .p7b file to DC107's local directory (optional if done locally)

Also make sure the Root CA certificate and CRL are available on DC107:

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



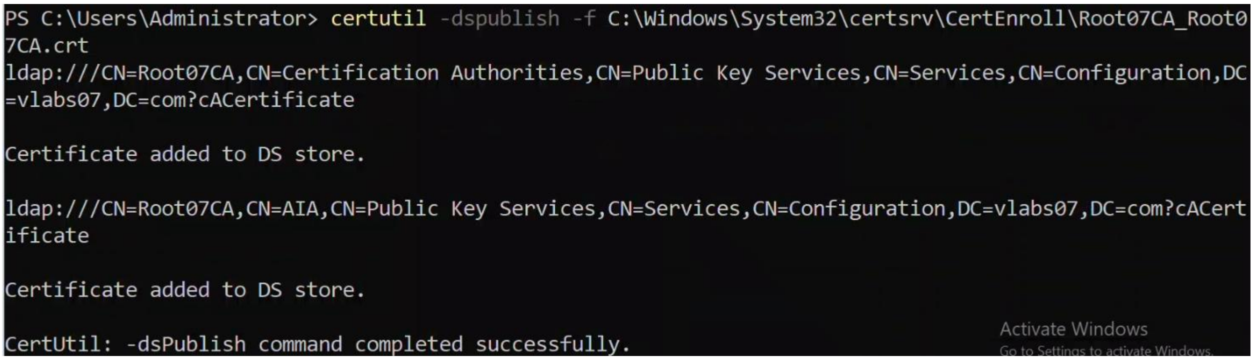
```
PS C:\Users\Administrator> Copy-Item -Path C:\*.crt -Destination C:\Windows\System32\certsrv\CertEnroll
\
PS C:\Users\Administrator> Copy-Item -Path C:\*.crl -Destination C:\Windows\System32\certsrv\CertEnroll
\
PS C:\Users\Administrator> _
```

Part C – Publish and Install on DC107

Why this step?
We are now finalizing the Subordinate CA setup by:
- Publishing the Root CA certificate and CRL to Active Directory
- Installing the trust chain locally (Root CA cert and CRL)
- Installing the signed Subordinate CA certificate
- Starting the CA service

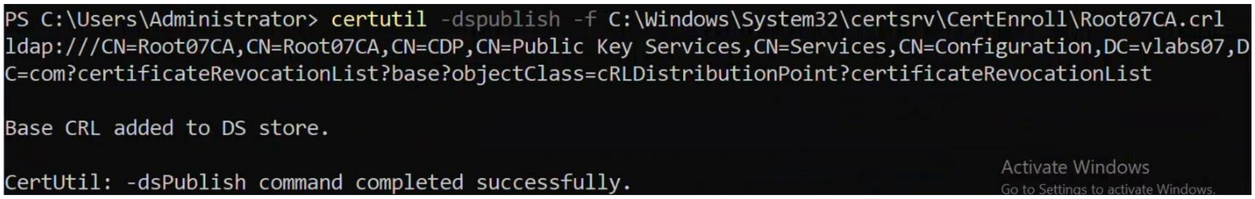
1. Publish the Root CA certificate and CRL to Active Directory:

```
certutil -dspublish -f
C:\Windows\System32\certsrv\CertEnroll\Root07CA_Root07CA.crt
```



```
PS C:\Users\Administrator> certutil -dspublish -f C:\Windows\System32\certsrv\CertEnroll\Root07CA_Root0
7CA.crt
ldap:///CN=Root07CA,CN=Certification Authorities,CN=Public Key Services,CN=Services,CN=Configuration,DC
=vlabs07,DC=com?cACertificate

Certificate added to DS store.

ldap:///CN=Root07CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=vlabs07,DC=com?cACert
ificate

Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.
```

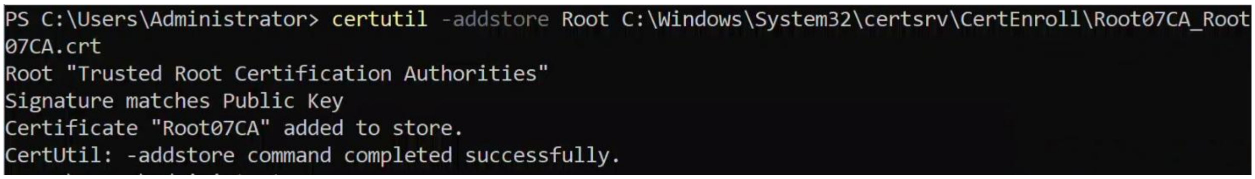
```
certutil -dspublish -f C:\Windows\System32\certsrv\CertEnroll\Root07CA.crl
```



```
PS C:\Users\Administrator> certutil -dspublish -f C:\Windows\System32\certsrv\CertEnroll\Root07CA.crl
ldap:///CN=Root07CA,CN=Root07CA,CN=CDP,CN=Public Key Services,CN=Services,CN=Configuration,DC=vlabs07,D
C=com?certificateRevocationList?base?objectClass=cRLDistributionPoint?certificateRevocationList

Base CRL added to DS store.

CertUtil: -dsPublish command completed successfully.
```

2. Install the Root CA certificate (adds to Trusted Root Certification Authorities):

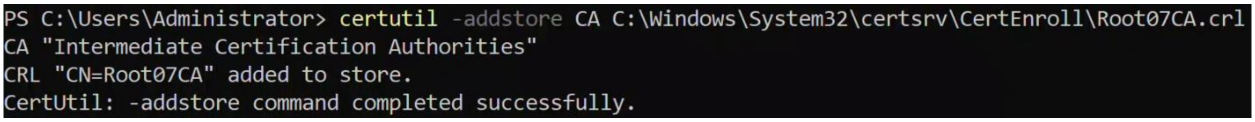
```
certutil -addstore Root
C:\Windows\System32\certsrv\CertEnroll\Root07CA_Root07CA.crt
```



```
PS C:\Users\Administrator> certutil -addstore Root C:\Windows\System32\certsrv\CertEnroll\Root07CA_Root
07CA.crt
Root "Trusted Root Certification Authorities"
Signature matches Public Key
Certificate "Root07CA" added to store.
CertUtil: -addstore command completed successfully.
```

3. Install the Root CA CRL (Certificate Revocation List):

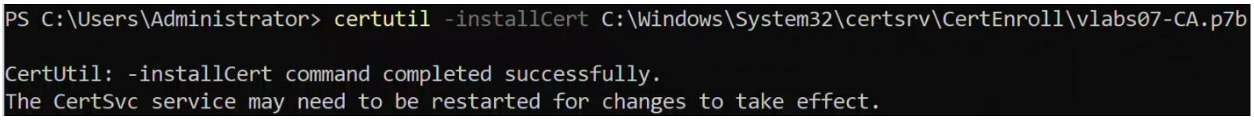
```
certutil -addstore CA C:\Windows\System32\certsrv\CertEnroll\Root07CA.crl
```



```
PS C:\Users\Administrator> certutil -addstore CA C:\Windows\System32\certsrv\CertEnroll\Root07CA.crl
CA "Intermediate Certification Authorities"
CRL "CN=Root07CA" added to store.
CertUtil: -addstore command completed successfully.
```

4. Install the signed Subordinate CA certificate (PKCS 7 chain):

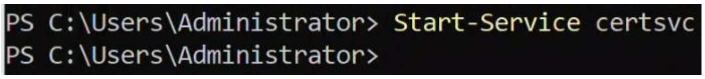
```
certutil -installCert C:\Windows\System32\certsrv\CertEnroll\vlabs07-CA.p7b
```



```
PS C:\Users\Administrator> certutil -installCert C:\Windows\System32\certsrv\CertEnroll\vlabs07-CA.p7b

CertUtil: -installCert command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
```

5. Start the CA service:

```
Start-Service certsvc
```



```
PS C:\Users\Administrator> Start-Service certsvc
PS C:\Users\Administrator>
```

The Enterprise Subordinate CA is now active and trusted. It can issue certificates within the domain under the Root CA hierarchy.

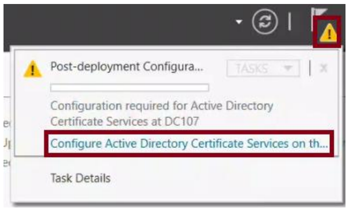
Step 4 – Configure AD CS Additional Roles on DC107

Why this step?
To enable modern and flexible certificate services in a Windows environment, we need to configure additional AD CS roles. These include:

Web-based Enrollment & Policy Services (CES and CEP): For certificate requests over HTTP
Web Enrollment: GUI for requesting certificates
Online Responder: Responds to revocation status requests (OCSP)
NDES: For enrolling network devices like routers or switches

Part D – Configure AD CS Additional Roles
Performed on: DC107

1. Launch Post-Deployment Configuration Wizard:
- Open Server Manager
- Click the yellow flag near Manage
- Select Configure Active Directory Certificate Services on the destination server

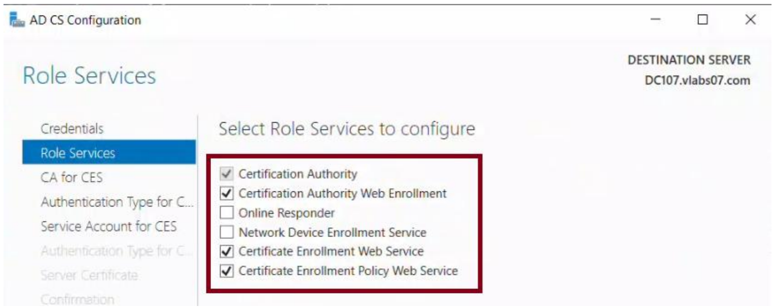


Post-deployment Configura...

Configuration required for Active Directory Certificate Services at DC107

Configure Active Directory Certificate Services on th...

2. Select Role Services to Configure:
- Check the following boxes in Role Services:
  - Certification Authority
  - Certification Authority Web Enrollment
  - Certificate Enrollment Web Service (CES)
  - Certificate Enrollment Policy Web Service (CEP)



AD CS Configuration

Role Services

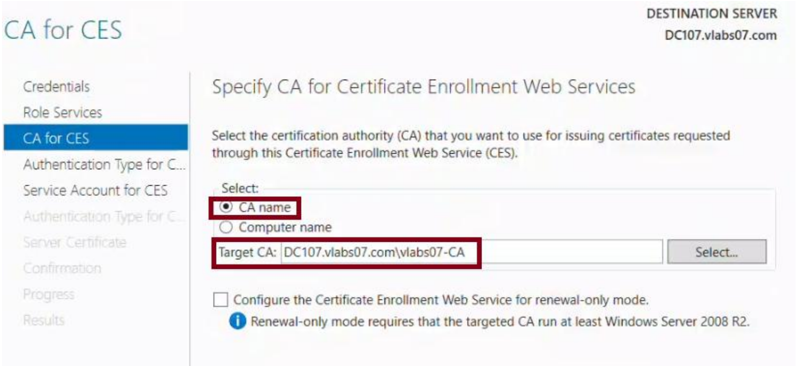
DESTINATION SERVER
DC107.vlabs07.com

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

3. Specify CA for CES:

- Choose CA name
- Select DC107.vlabs07.com\vlabs07-CA



CA for CES

DESTINATION SERVER
DC107.vlabs07.com

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

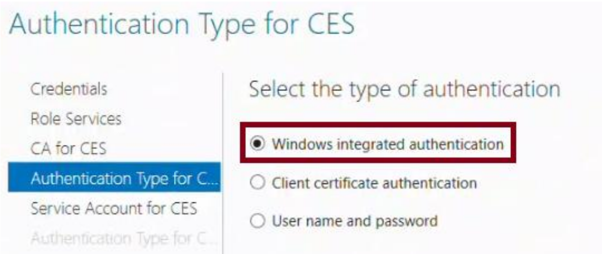
Target CA: DC107.vlabs07.com\vlabs07-CA

□ 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.

4. Authentication Type for CES:

- Select Windows Integrated Authentication



Authentication Type for CES

Select the type of authentication

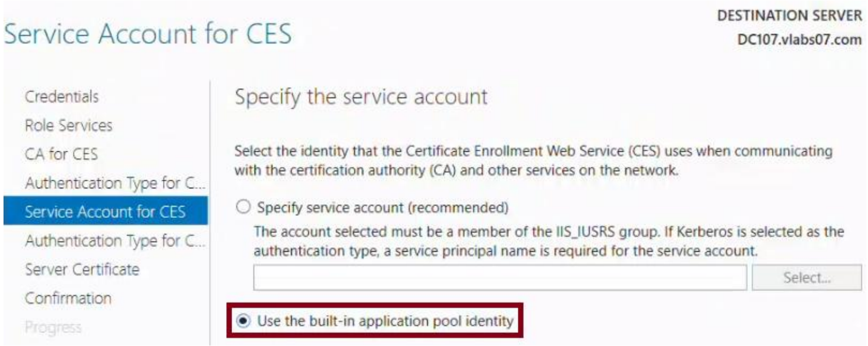
● Windows integrated authentication

○ Client certificate authentication

○ User name and password

5. Service Account for CES:

- Select Use the built-in application pool identity



Service Account for CES

DESTINATION SERVER
DC107.vlabs07.com

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.

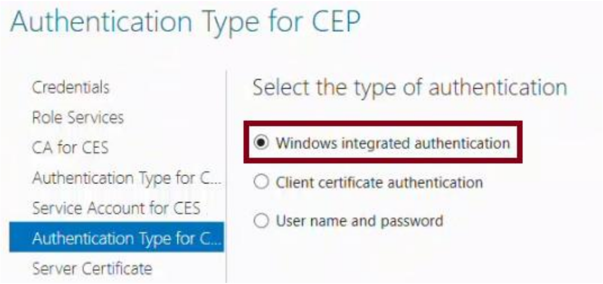
○ Specify service account (recommended)

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.

● Use the built-in application pool identity

6. Authentication Type for CEP:

- Select Windows Integrated Authentication



Authentication Type for CEP

Select the type of authentication

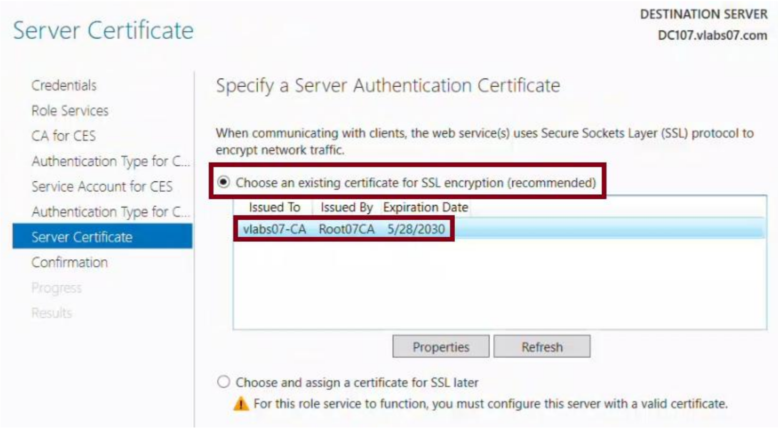
● Windows integrated authentication

○ Client certificate authentication

○ User name and password

7. Server Certificate:

- Choose an existing certificate (issued to vlabs07-CA by Root07CA)



Server Certificate

DESTINATION SERVER
DC107.vlabs07.com

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)

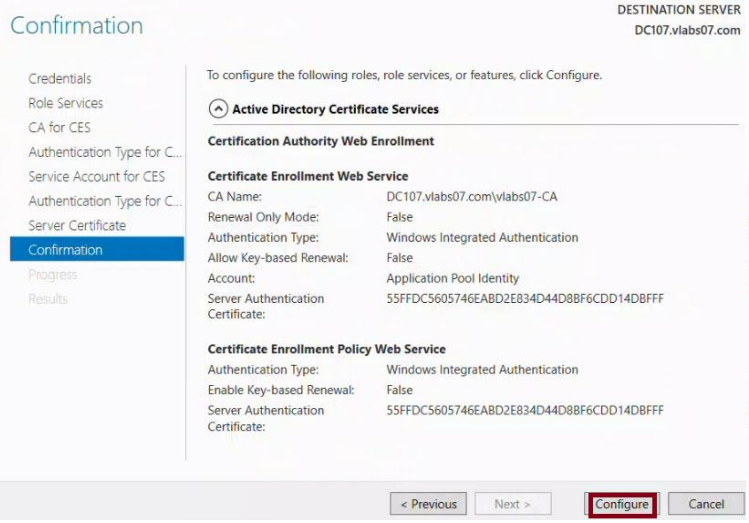
Issued To	Issued By	Expiration Date
vlabs07-CA	Root07CA	5/28/2030

○ Choose and assign a certificate for SSL later

⚠ For this role service to function, you must configure this server with a valid certificate.

8. Confirm Settings and Configure:

- Review the summary
- Click Configure



Confirmation

DESTINATION SERVER
DC107.vlabs07.com

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

Active Directory Certificate Services

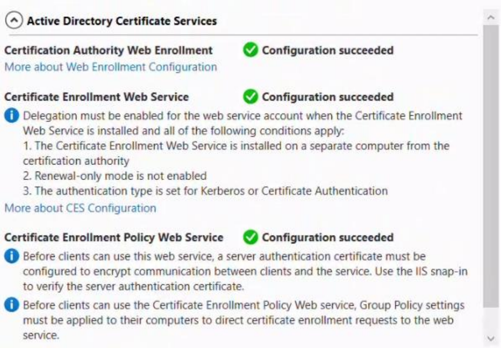
Certification Authority Web Enrollment

Certificate Enrollment Web Service

CA Name:	DC107.vlabs07.com\vlabs07-CA
Renewal Only Mode:	False
Authentication Type:	Windows Integrated Authentication
Allow Key-based Renewal:	False
Account:	Application Pool Identity
Server Authentication Certificate:	55FFDC5605746EABD2E834D44D8BF6CDD14DBFFF

Certificate Enrollment Policy Web Service

Authentication Type:	Windows Integrated Authentication
Enable Key-based Renewal:	False
Server Authentication Certificate:	55FFDC5605746EABD2E834D44D8BF6CDD14DBFFF



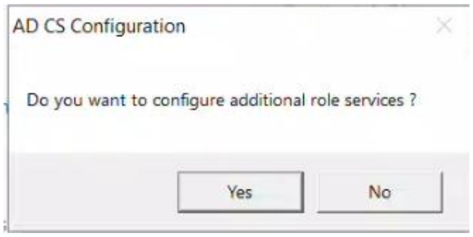
Active Directory Certificate Services

Certification Authority Web Enrollment ✓ Configuration succeeded
More about Web Enrollment Configuration

Certificate Enrollment Web Service ✓ Configuration succeeded
ⓘ Delegation must be enabled for the web service account when the Certificate Enrollment Web Service is installed and all of the following conditions apply:
1. The Certificate Enrollment Web Service is installed on a separate computer from the certification authority
2. Renewal-only mode is not enabled
3. The authentication type is set for Kerberos or Certificate Authentication
More about CES Configuration

Certificate Enrollment Policy Web Service ✓ Configuration succeeded
ⓘ Before clients can use this web service, a server authentication certificate must be configured to encrypt communication between clients and the service. Use the IIS snap-in to verify the server authentication certificate.
ⓘ Before clients can use the Certificate Enrollment Policy Web service, Group Policy settings must be applied to their computers to direct certificate enrollment requests to the web service.

Additional Step - Configure NDES

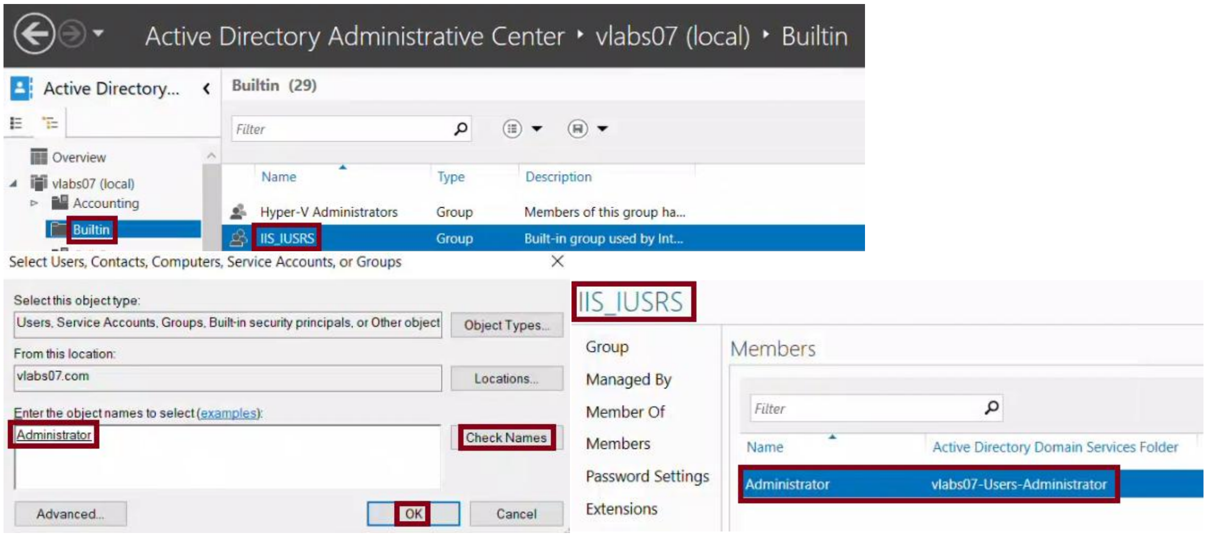


AD CS Configuration

Do you want to configure additional role services ?

9. Add Administrator to IIS_IUSRS group:

- On DC107, open Active Directory Administrative Center
- Navigate to Builtin → IIS_IUSRS → Add Member
- Add the Administrator account



Active Directory Administrative Center ‣ vlabs07 (local) ‣ Builtin

Builtin (29)

Name	Type	Description
Hyper-V Administrators	Group	Members of this group ha...
IIS_IUSRS	Group	Built-in group used by Int...

Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type: Users, Service Accounts, Groups, Built-in security principals, or Other object

From this location: vlabs07.com

Enter the object names to select (examples): Administrator

IIS_IUSRS — Members

Name	Active Directory Domain Services Folder
Administrator	vlabs07-Users-Administrator

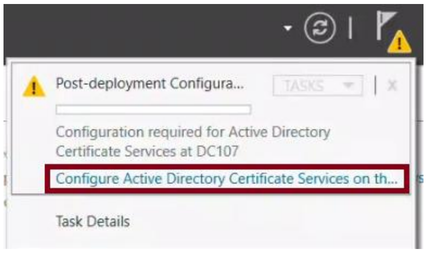
10 – NDES Role Wizard: Pre-Configuration Screens

The wizard displays several key configuration screens. These help ensure credentials and role selections are correct.

Screens observed during configuration:

AD CS Configuration Prompt

- Prompt: "Do you want to configure additional role services?"
- Response: Clicked "Yes"



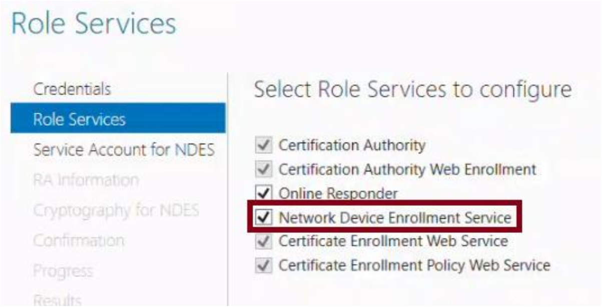
Post-deployment Configura...

Configuration required for Active Directory Certificate Services at DC107

Configure Active Directory Certificate Services on th...

Role Services Selection

- Verified that only the following were selected:
  - Certification Authority
  - Certification Authority Web Enrollment
  - Certificate Enrollment Web Service
  - Certificate Enrollment Policy Web Service
  - Network Device Enrollment Service
  - Clicked "Next"

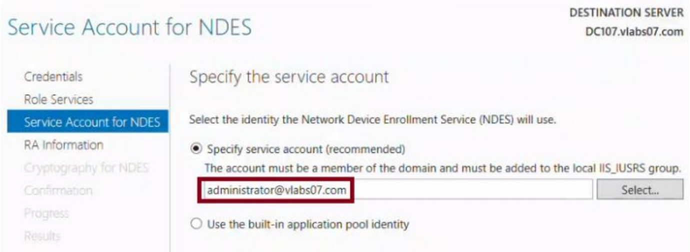


Select Role Services to configure

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

Credential Selection Screen

- Confirmed: VLABS07\Administrator is selected
- Proceeded by clicking "Next"



Specify the service account

Select the identity the Network Device Enrollment Service (NDES) will use.

● Specify service account (recommended)

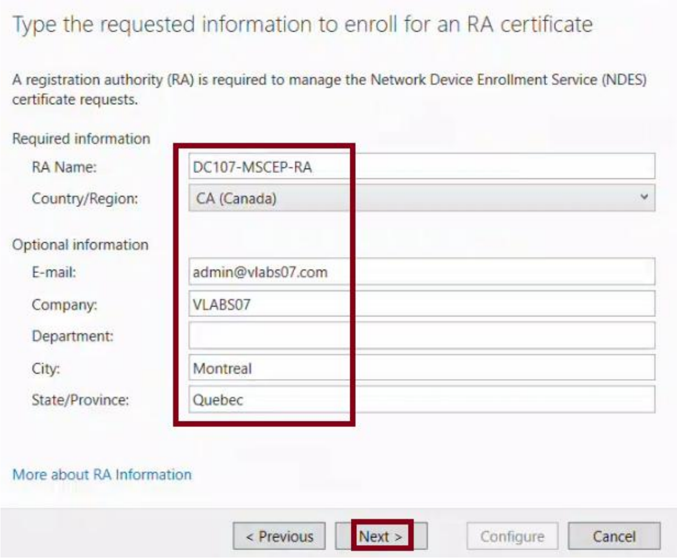
The account must be a member of the domain and must be added to the local IIS_IUSRS group.

administrator@vlabs07.com

○ Use the built-in application pool identity

10.5 NDES Configuration (in the wizard):

- RA Name: DC107-MSCEP-RA
- Country: CA (Canada)
- Email: admin@vlabs07.com
- Company: VLABS07
- Department: IT (optional)
- City: Montreal
- State: Quebec



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: DC107-MSCEP-RA

Country/Region: CA (Canada)

Optional information

E-mail: admin@vlabs07.com

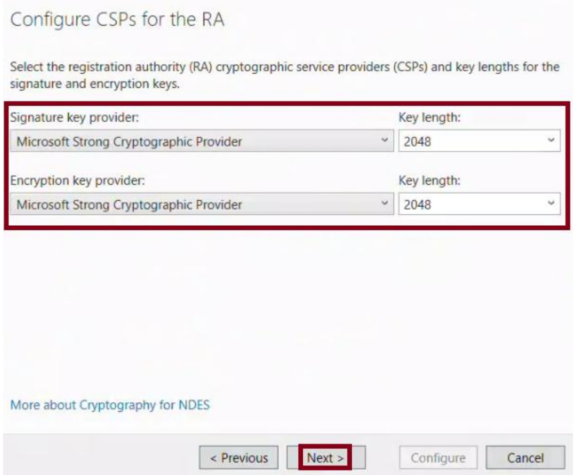
Company: VLABS07

Department:

City: Montreal

State/Province: Quebec

```
11. NDES Cryptographic Settings:
- Signature key provider: Microsoft Strong Cryptographic Provider
- Key length: 2048
- Encryption key provider: Microsoft Strong Cryptographic Provider
- Key length: 2048
```



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

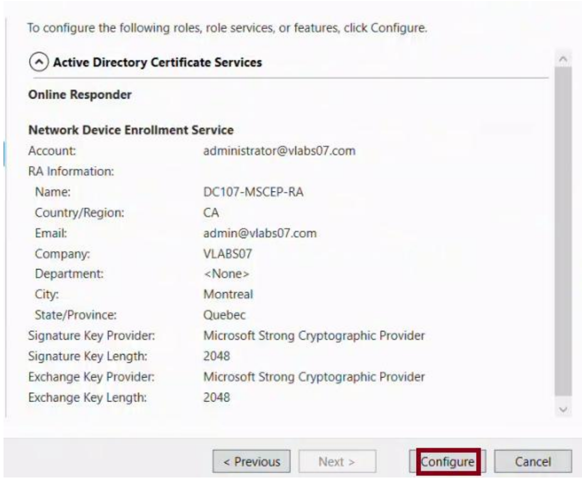
Key length: 2048

Encryption key provider: Microsoft Strong Cryptographic Provider

Key length: 2048

More about Cryptography for NDES

```
12. Final Confirmation:
- Click Configure
- Wait for the success message
```



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

Active Directory Certificate Services

Online Responder

Network Device Enrollment Service

Account: administrator@vlabs07.com

RA Information:

Name: DC107-MSCEP-RA

Country/Region: CA

Email: admin@vlabs07.com

Company: VLABS07

Department: <None>

City: Montreal

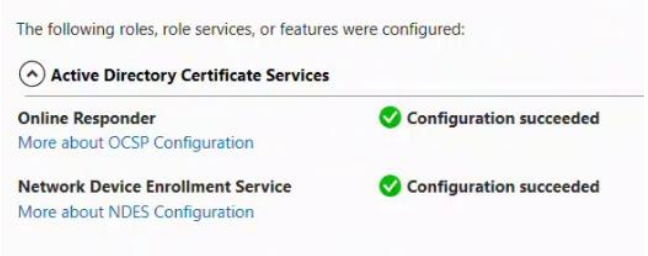
State/Province: Quebec

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 were configured:

Active Directory Certificate Services

Online Responder ✓ Configuration succeeded

More about OCSP Configuration

Network Device Enrollment Service ✓ Configuration succeeded

More about NDES Configuration

```
Result:
All AD CS web and network services are now active. DC107 can handle:
- HTTP-based enrollment and revocation status
- Network device certificate requests
- Web-based certificate requests by users and administrators
```

Step 5 – Secure the Root CA and Take It Offline

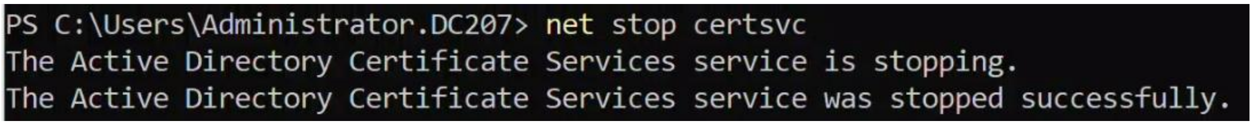
Why this step?
Now that the Subordinate CA (on DC107) is fully deployed and functional, the Root CA (Root07CA) should be taken offline to enhance security. Keeping it offline protects its private key and minimizes exposure to attacks.

Stop Certificate Services and Shut Down Root07CA

We will now stop the Root CA service and shut down the server.

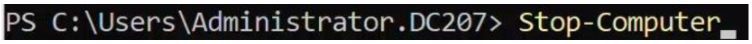
Run the following commands on Root07CA:

```
net stop certsvc
```



```
PS C:\Users\Administrator.DC207> net stop certsvc
The Active Directory Certificate Services service is stopping.
The Active Directory Certificate Services service was stopped successfully.
```

```
Stop-Computer
```



```
PS C:\Users\Administrator.DC207> Stop-Computer
```

This stops the Active Directory Certificate Services and powers down the offline Root CA, completing the secure PKI setup.

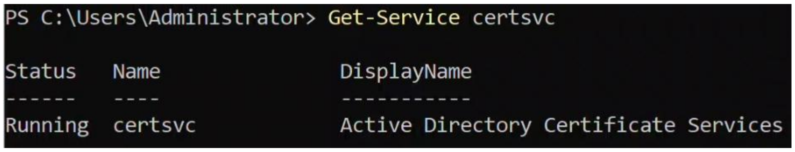
Step 6 – Verify the Enterprise Subordinate CA

Why this step?
After completing the subordinate CA setup and taking the Root CA offline, its essential to verify that DC107 (vlabs07-CA) can correctly issue certificates and that the services are functioning as intended.

Confirm CA is Running on DC107

Run the following command on DC107 to confirm the CA service is active:

```
Get-Service certsvc
```



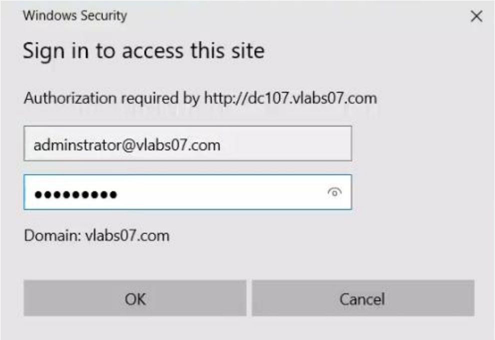
```
PS C:\Users\Administrator> Get-Service certsvc

Status   Name               DisplayName
------   ----               -----------
Running  certsvc            Active Directory Certificate Services
```

You should see the status as Running.

Access Web Enrollment Portal

Open a web browser on DC107 or any domain-joined machine and go to:

http://dc107.vlabs07.com/certsrv



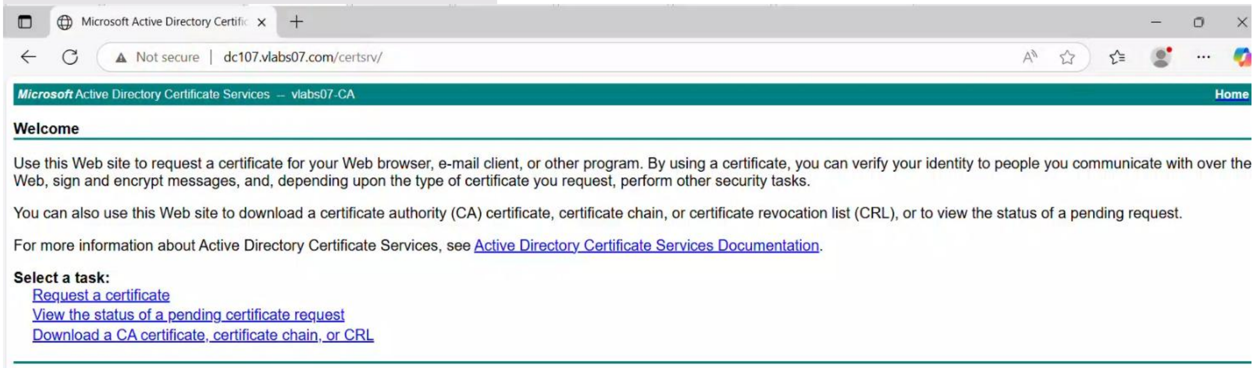
Sign in to access this site

Authorization required by http://dc107.vlabs07.com

adminstrator@vlabs07.com

●●●●●●●●●

Domain: vlabs07.com



Microsoft Active Directory Certific
Not secure
dc107.vlabs07.com/certsrv/
Microsoft Active Directory Certificate Services -- vlabs07-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

You should see the Microsoft Active Directory Certificate Services web interface. **If** you see the Welcome page with enrollment options, then the service is correctly installed and responding.