Assignment

Updating certification bodies and working with them

The company in which you are employed as a system administrator has significantly expanded the scope of business and, as a result, increased security is required. To provide access to critical sites, you are tasked with implementing the Active Directory Certificate Services role. Your task is to implement a standalone root CA and a subordinate enterprise CA. Implement a standalone root CA on a server called ROOT-CA.

- *The name of the standalone root CA should be: vase_ime. RootCA (e.g., PeterRootCA).*
- *Key length: 4096.*
- *All other settings should remain at the default values.*

Configure New revocation location on ROOT-CA to publish a CRL to ENT-CA, and then create a DNS host record for the ROOT-CA server using the IP address 192.168.100.151. Install and configure a child Enterprise CA on an ENT-CA server. The name of the CA will be vase_ime-IssuingCA (e.g. Peter-IssuingCA). Publish a basic CA certificate through Group Policies.

Create a duplicate of the User certificate template.

Name him by his name (e.g. Peter). Publish this template. Provide the solution in a text document, where you will gradually describe the stages needed to solve the task. Follow the flow of the solution description with appropriate screenshots for each step of the task.

Course: Active Directory Infrastructure

Student: Jovan Ljušić

CONTENT

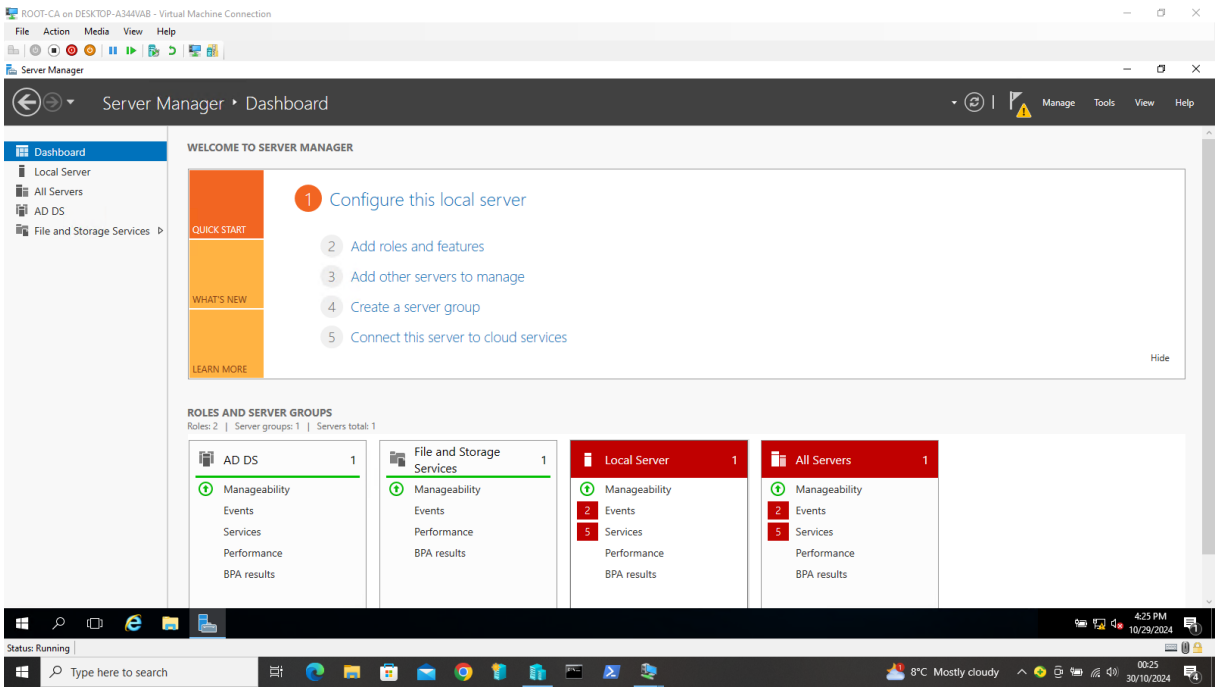
INSTALLING STANDALONE ROOT

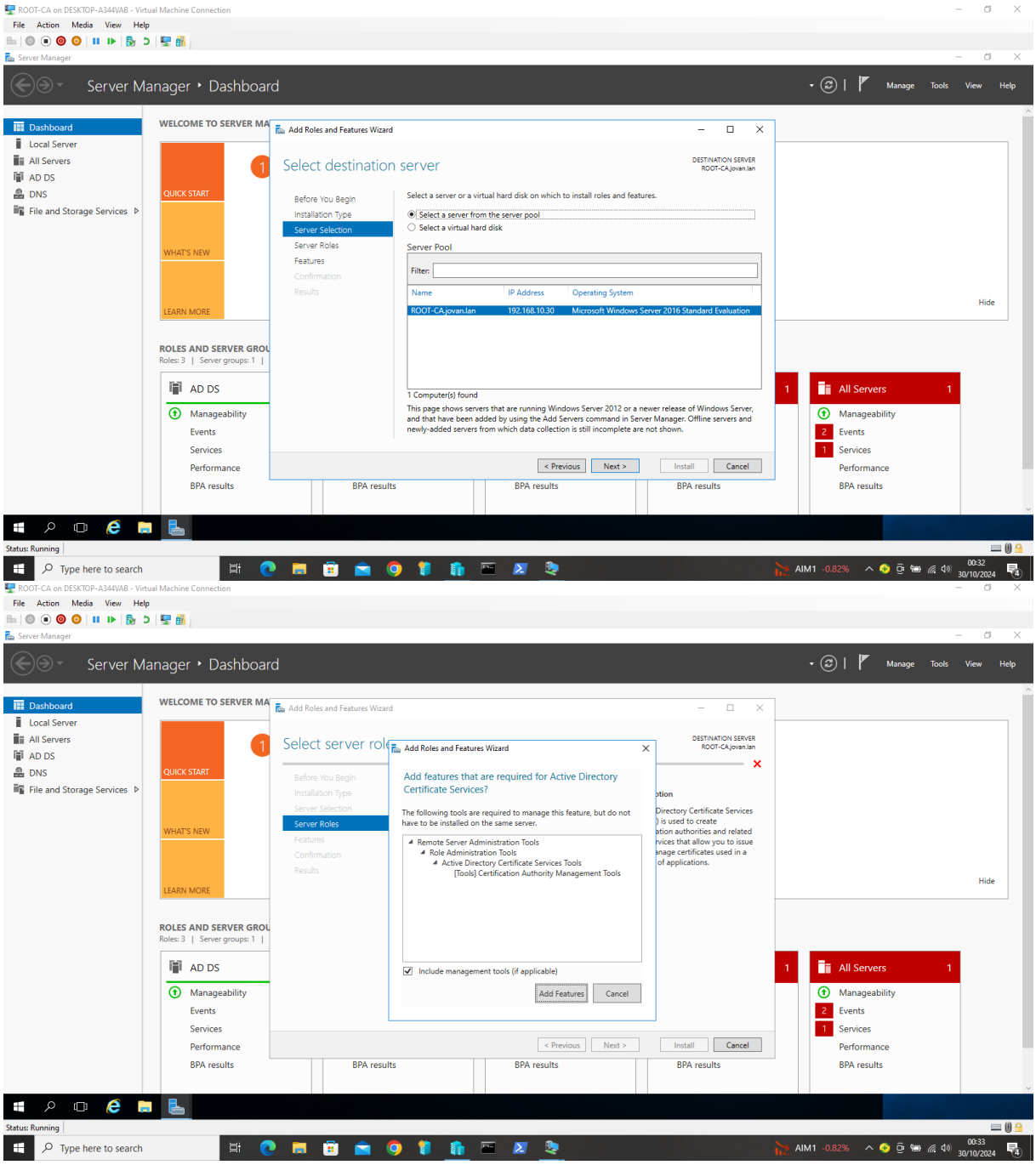
This document presents a step-by-step approach to solving a specific task, outlining the methodology, execution, and expected outcomes. By following the instructions, the reader will gain hands-on experience in applying technical concepts to practical situations, reinforcing both theoretical knowledge and problem-solving abilities.

The structured approach ensures that each step is clearly defined, making the process easy to follow and implement in professional environments.

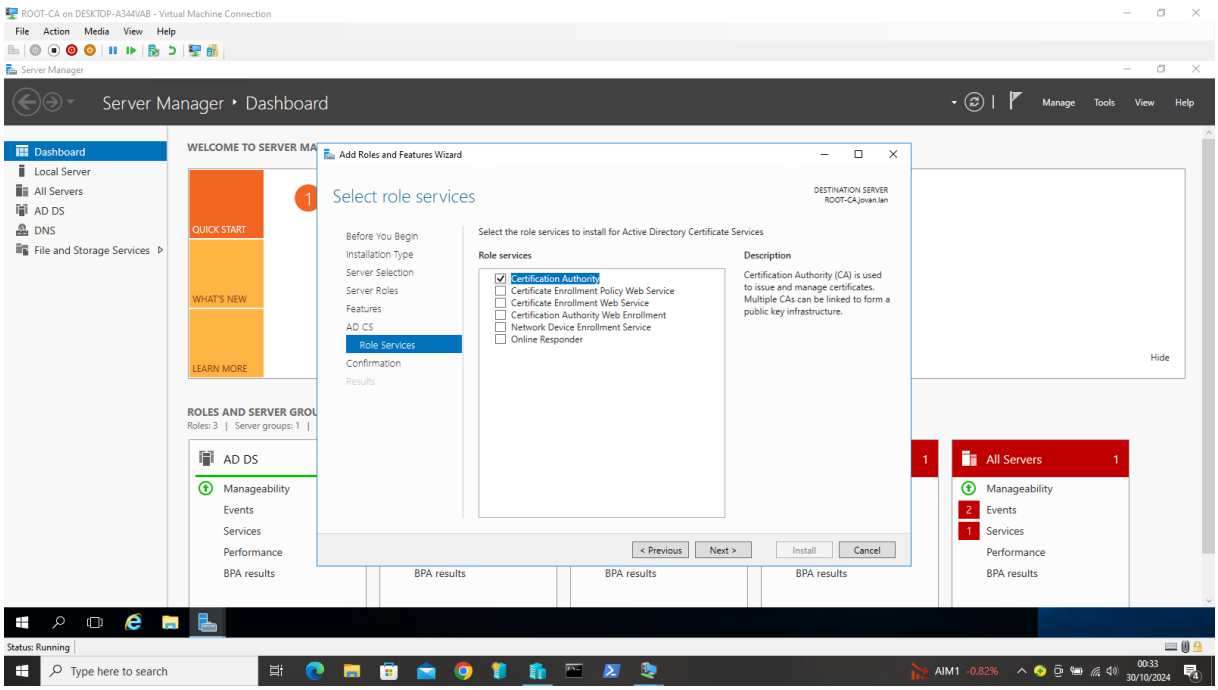
The first step of this task will follow the action that takes place on the ROOT-CA server, the following steps will show the process step by step, with screenshots attached.

1. By running the **Server Manager** on the **ROOT-CA** server.
2. By selecting the **Add roles and features** icon and running the installation wizard.
3. Choice of **Role-based or feature-based installation**.
4. In the role list, select **the Active Directory Certificate Services (AD CS)** field.
5. For the purposes of the task, only the Certification Authority icon is knitted.
6. When the installation is complete, **the Post-deployment Configuration** begins.




ROOT-CA on DESKTOP-A344VAB - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MA
QUICK START
WHAT'S NEW
LEARN MORE
Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
ROOT-CA.jovan.lan
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
ROOT-CA.jovan.lan
192.168.10.30
Microsoft Windows Server 2016 Standard Evaluation
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel
Hide
ROLES AND SERVER GROU
Roles: 3 | Server groups: 1 |
AD DS
Manageability
Events
Services
Performance
BPA results
All Servers
Status: Running
Type here to search
AIM1 -0.82%
00:32
30/10/2024

ROOT-CA on DESKTOP-A344VAB - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
WELCOME TO SERVER MA
QUICK START
WHAT'S NEW
LEARN MORE
Add Roles and Features Wizard
Select server rol
DESTINATION SERVER
ROOT-CA.jovan.lan
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for Active Directory Certificate Services?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
Active Directory Certificate Services Tools
[Tools] Certification Authority Management Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel
Hide
ROLES AND SERVER GROU
Roles: 3 | Server groups: 1 |
AD DS
Manageability
Events
Services
Performance
BPA results
All Servers
Status: Running
Type here to search
AIM1 -0.82%
00:33
30/10/2024



Post-deployment configuration:

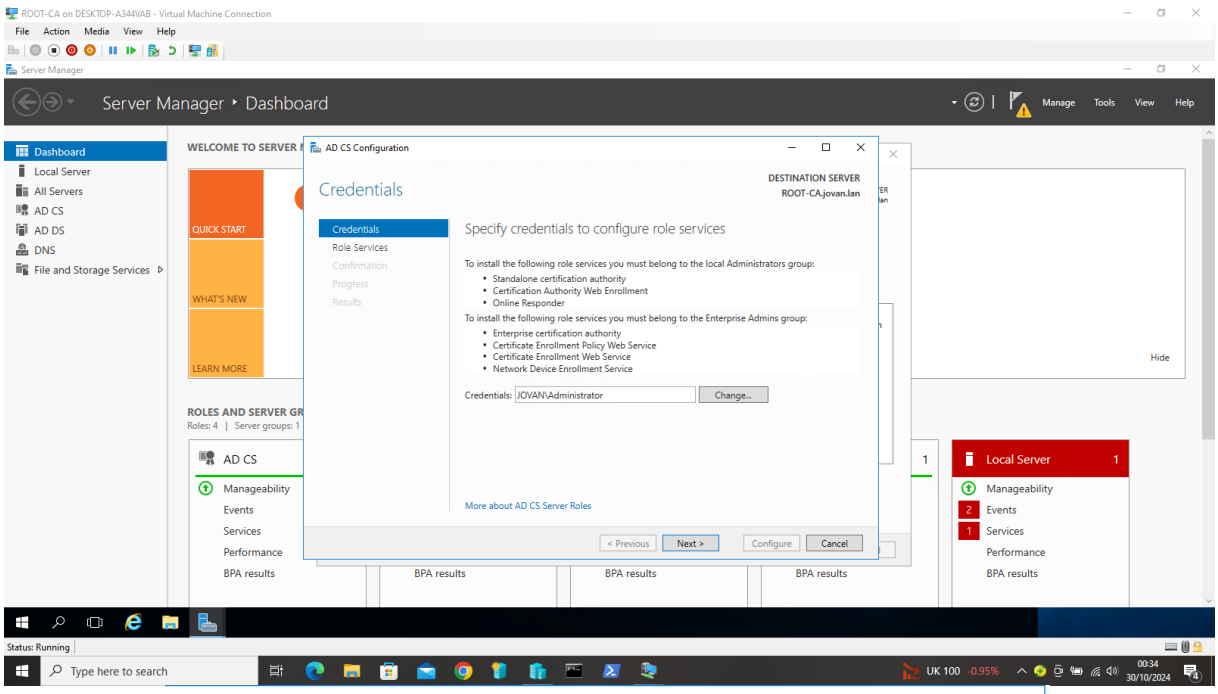
7. In **AD CS Configuration Wizard**, selecting **Standalone CA** and clicking Next.

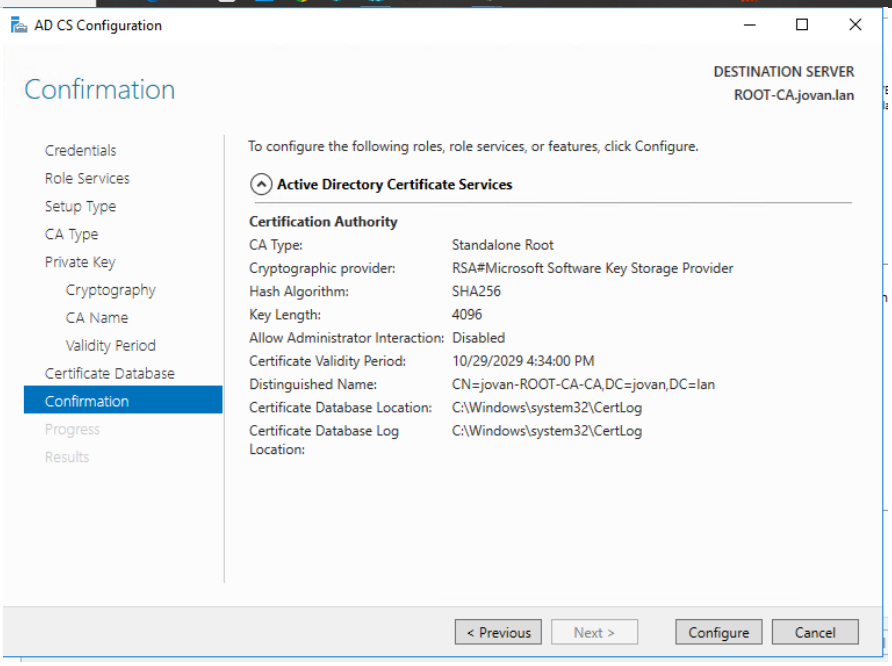
8. Select the **Standalone Root CA icon**.

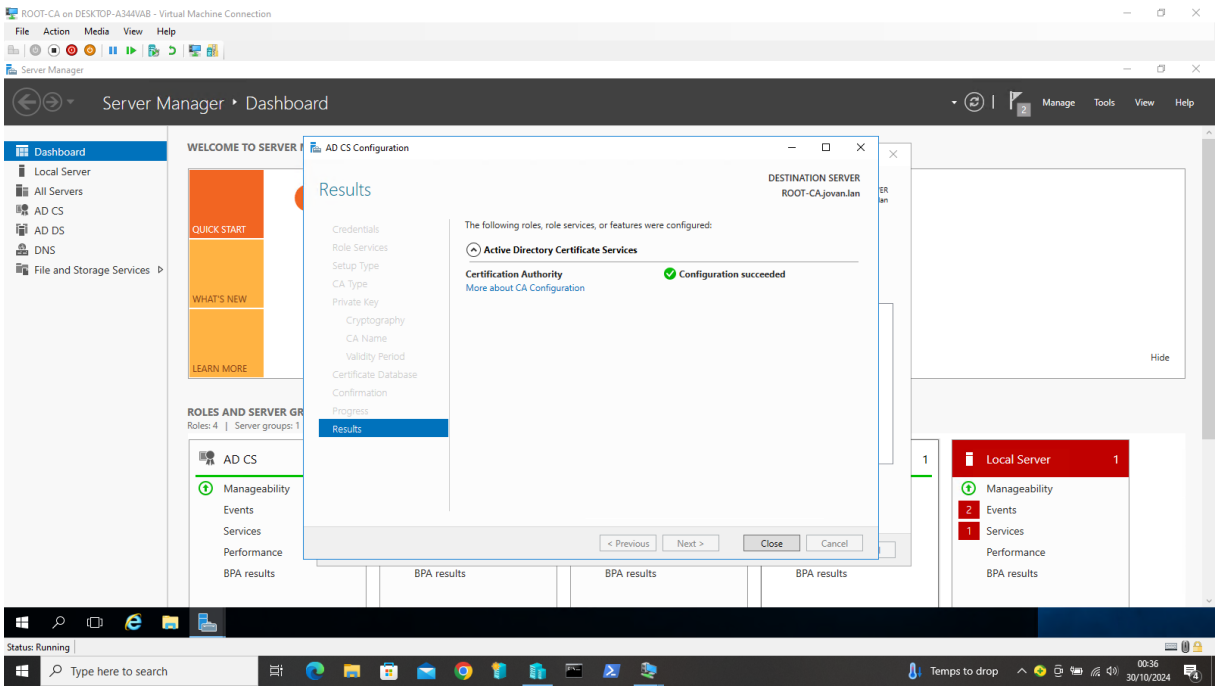
9. The name CA is set according to the task, in this case **john. RootCA.**

10. Set **the Key length** to **4096**.

11. Other settings are left by default.


ROOT-CA on DESKTOP-A344VAB - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
WELCOME TO SERVER
QUICK START
WHAT'S NEW
LEARN MORE
Hide
ROLES AND SERVER GR
Roles: 4 | Server groups: 1
AD CS
Manageability
Events
Services
Performance
BPA results
Local Server 1
Manageability
Events
Services
Performance
BPA results
AD CS Configuration
Credentials
DESTINATION SERVER
ROOT-CA.jovan.lan
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: JOVAN\Administrator
Change...
More about AD CS Server Roles
< Previous
Next >
Configure
Cancel
Status: Running
Type here to search
UK 100 -0.95%
00:34
30/10/2024


AD CS Configuration
Confirmation
DESTINATION SERVER
ROOT-CA.jovan.lan
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results
To configure the following roles, role services, or features, click Configure.
Active Directory Certificate Services
Certification Authority
CA Type: Standalone Root
Cryptographic provider: RSA#Microsoft Software Key Storage Provider
Hash Algorithm: SHA256
Key Length: 4096
Allow Administrator Interaction: Disabled
Certificate Validity Period: 10/29/2029 4:34:00 PM
Distinguished Name: CN=jovan-ROOT-CA-CA,DC=jovan,DC=lan
Certificate Database Location: C:\Windows\system32\CertLog
Certificate Database Log Location: C:\Windows\system32\CertLog
< Previous
Next >
Configure
Cancel



Every detail of this server is recorded in the screenshot. The data is entered as required by the instructions of the task:

- ***The name of the standalone root CA should be: vase_ime. RootCA (e.g., PeterRootCA).***
- ***Key length: 4096.***
- ***All other settings should remain at the default values.***

The following action follows the title of the configuration of the new revocation location, more specifically, **the New Revocation Location**.

CONFIGURE A NEW LOCATION

The first step through this heading follows the action that takes place in the **Certification Authority section** and the action is as follows:

1. By selecting **the Certification Authority** console on the **ROOT-CA** server in the **Tools section**.

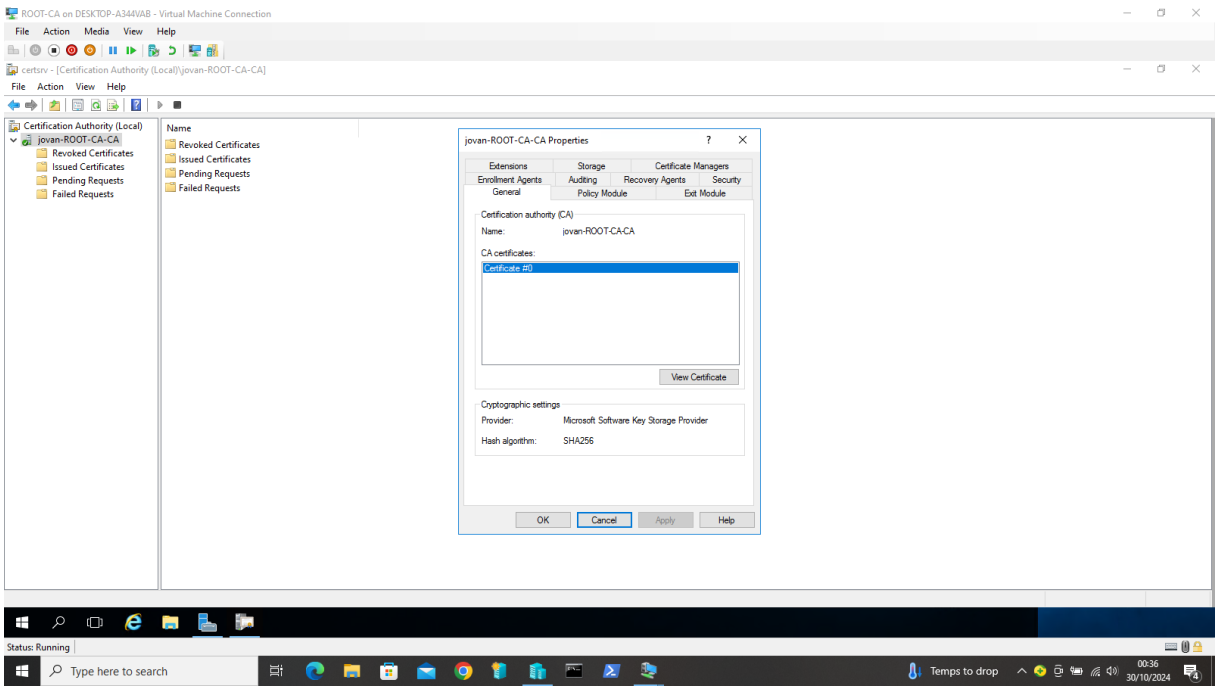
2. Right click on the server (ROOT-CA) **Properties**.

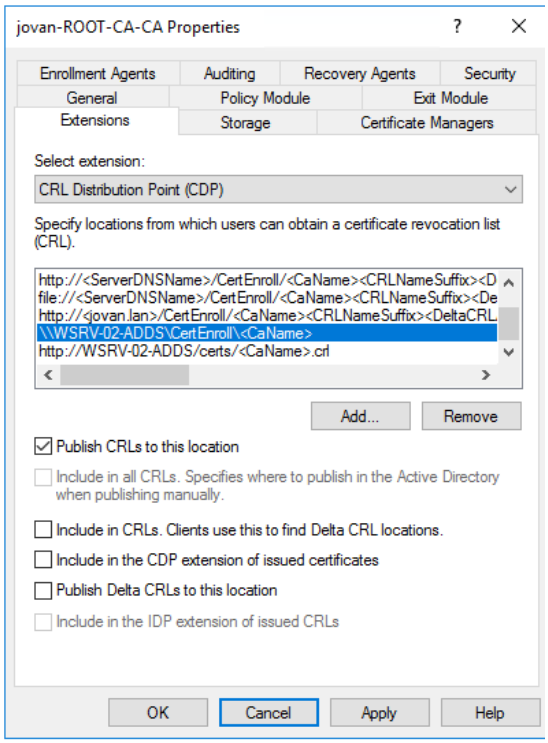
3. Select a segment called **Extensions**.

4. In the **CRL Distribution Points (CDP)** section, click on **Add**.

5. A specific location is set to **WSRV-02-ADDS** where the CRL will be published (in this case the server name mentioned above which also captures the screenshot).

6. Select **the Publish CRL to this location** option and click OK**.**





DNS HOST RECORD

Creating a DNS Host Record for ROOT-CA

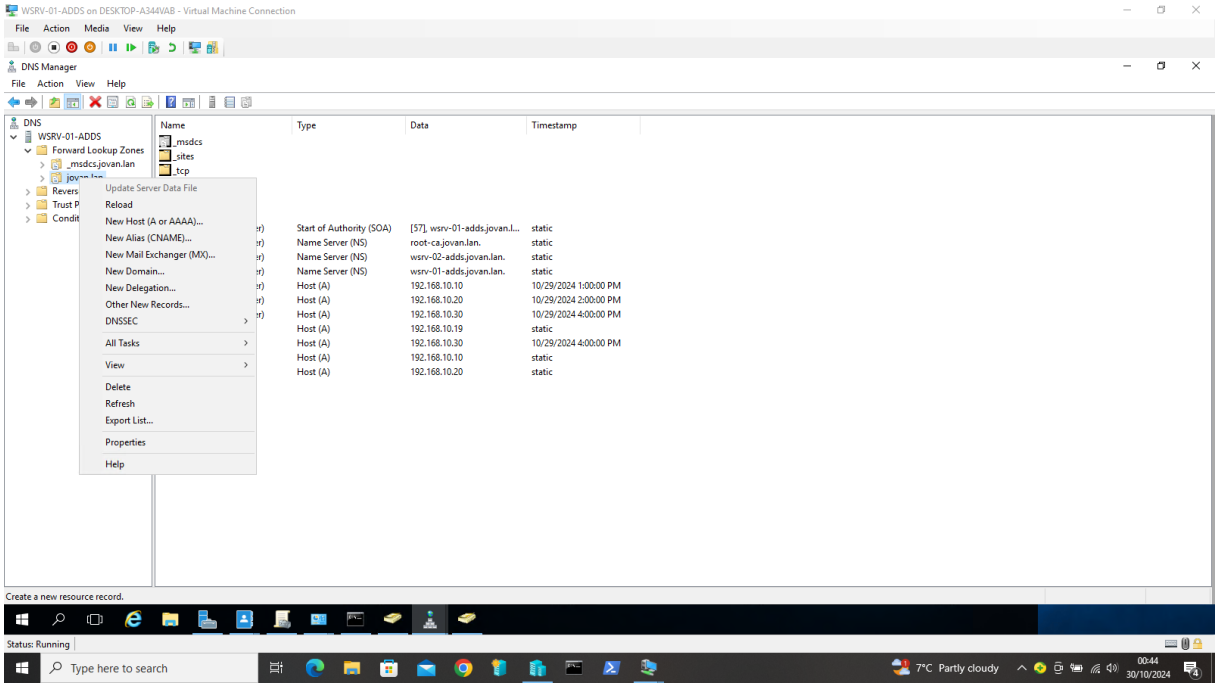
1. By running **DNS Manager**.

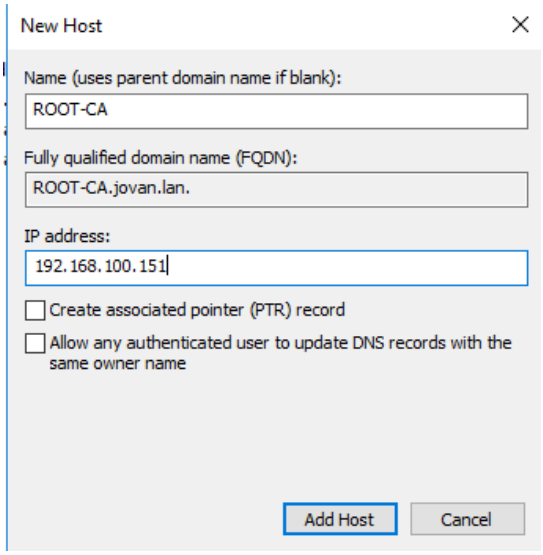
2. In the right panel, right-click on the zone where the domain is located, select **New Host (A or AAAA).**

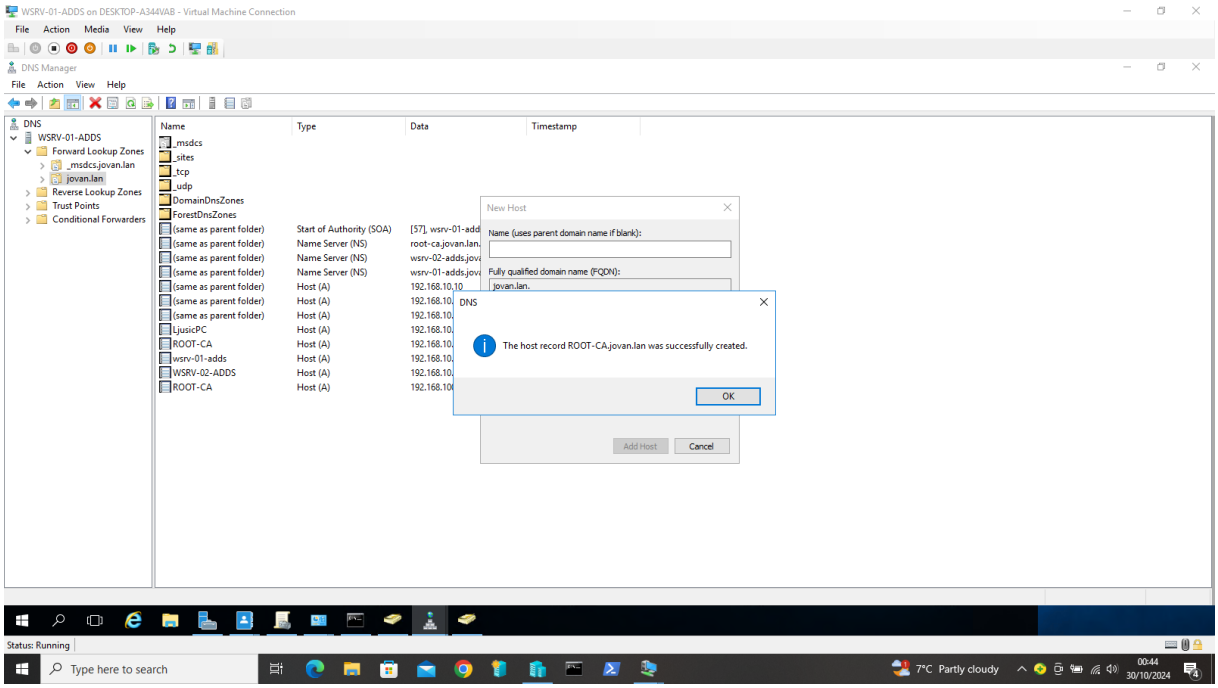
3. Hostname **ROOT-CA.**

4. **IP address** of the ROOT-CA server: **192.168.100.151**.

5. Click on **Add Host** and then **OK.**







INSTALLATION OF ENTERPRISE CA

1. On the **ENT-CA** server, in this case the name **WSRV-02-ADDS** by starting **Server Manager, the** procedure follows a similar action as for the previous server.

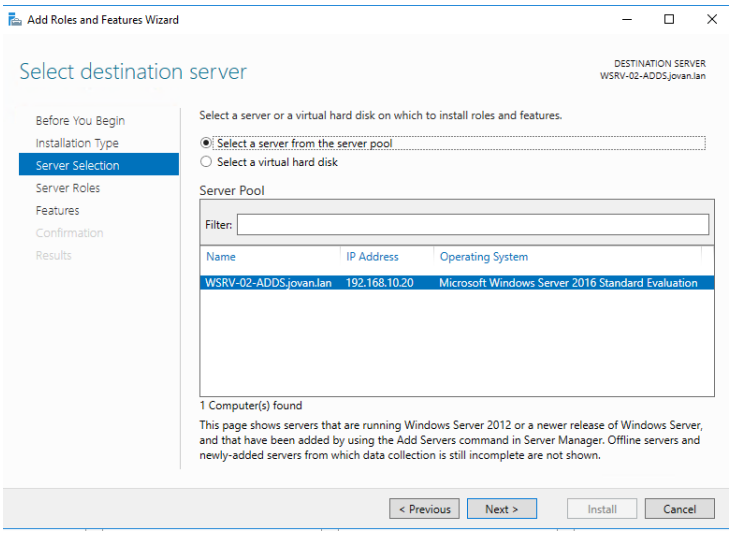
2. By installing **Active Directory Certificate Services (AD CS)** as well as on the ROOT-CA server.

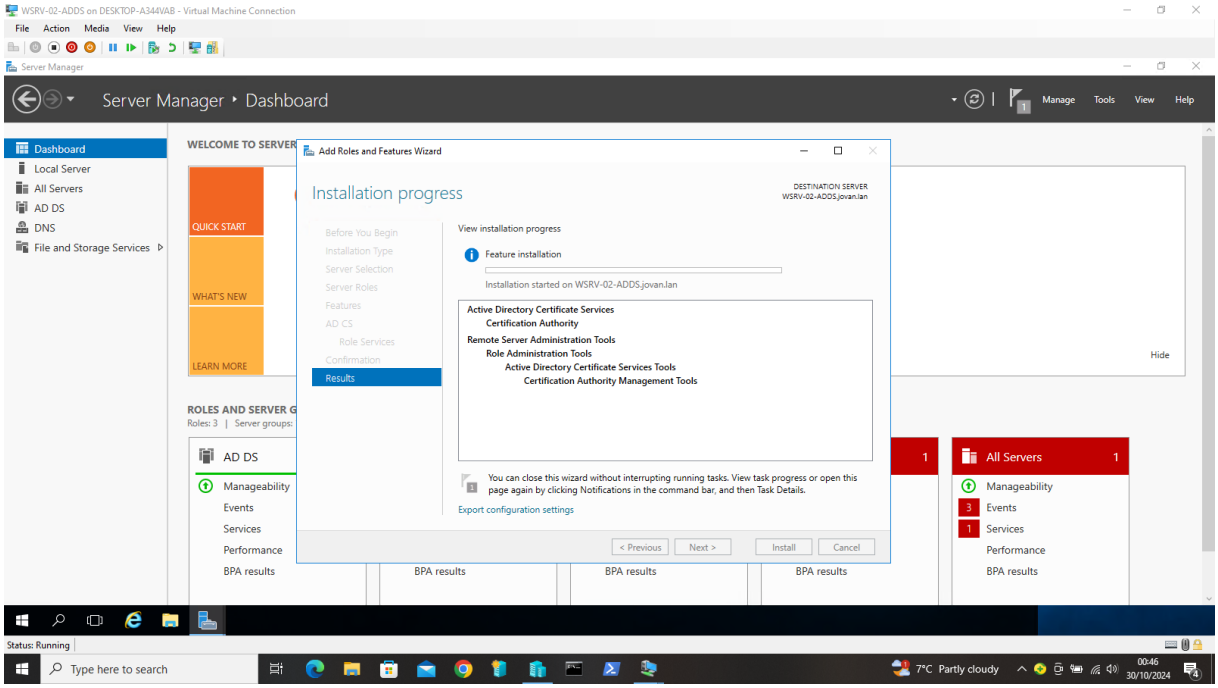
3. After installation, **Post-deployment Configuration**.

4. In this case, **Enterprise CA is selected and** Subordinate CA **is selected as the CA type**.

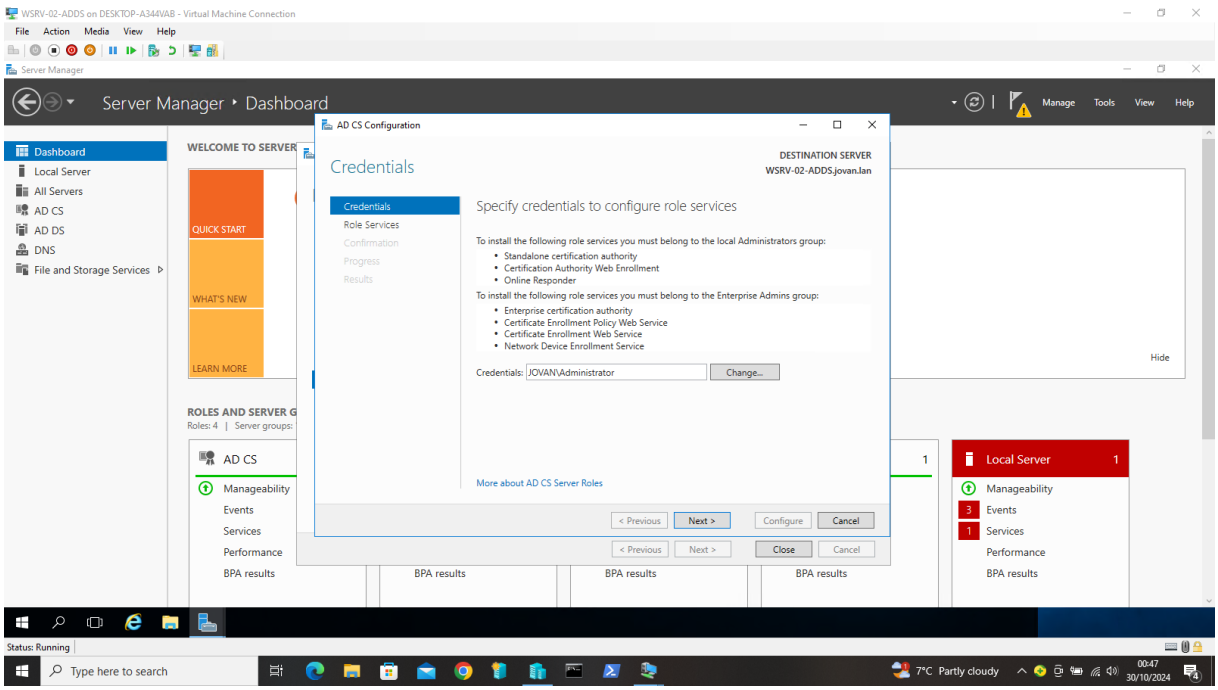
5. The name of the CA, e.g. **john-IssuingCA** (in this case, the default name is john-WSRV-02-ADDS).

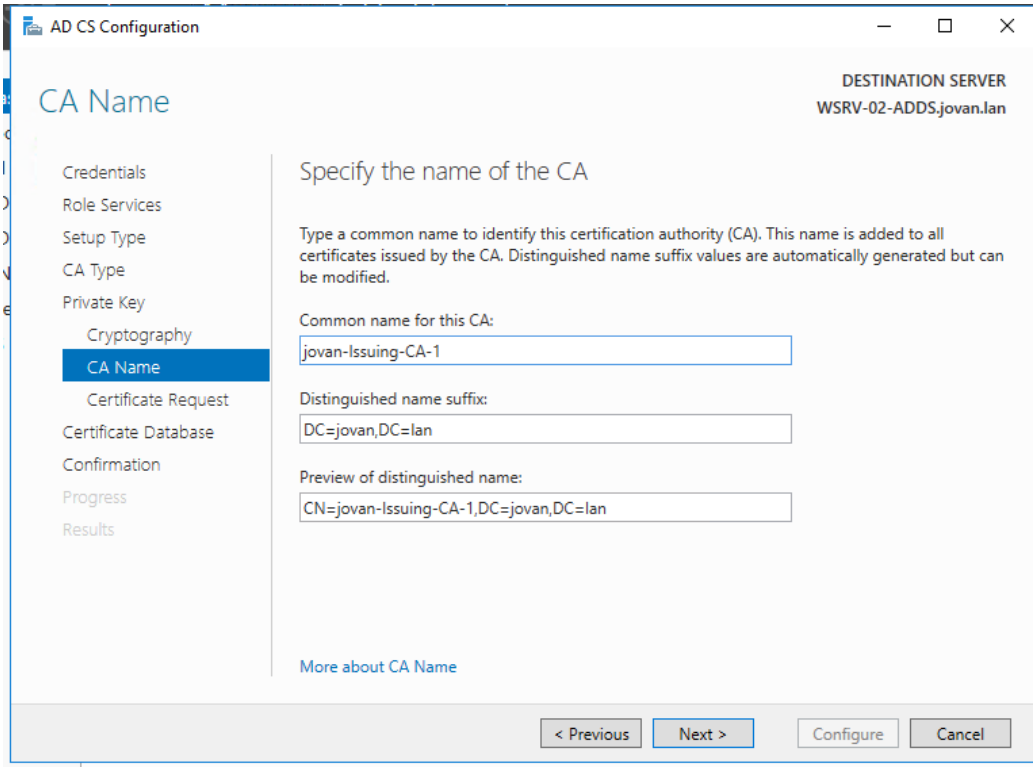
6. Select **ROOT-CA** as the parent CA.

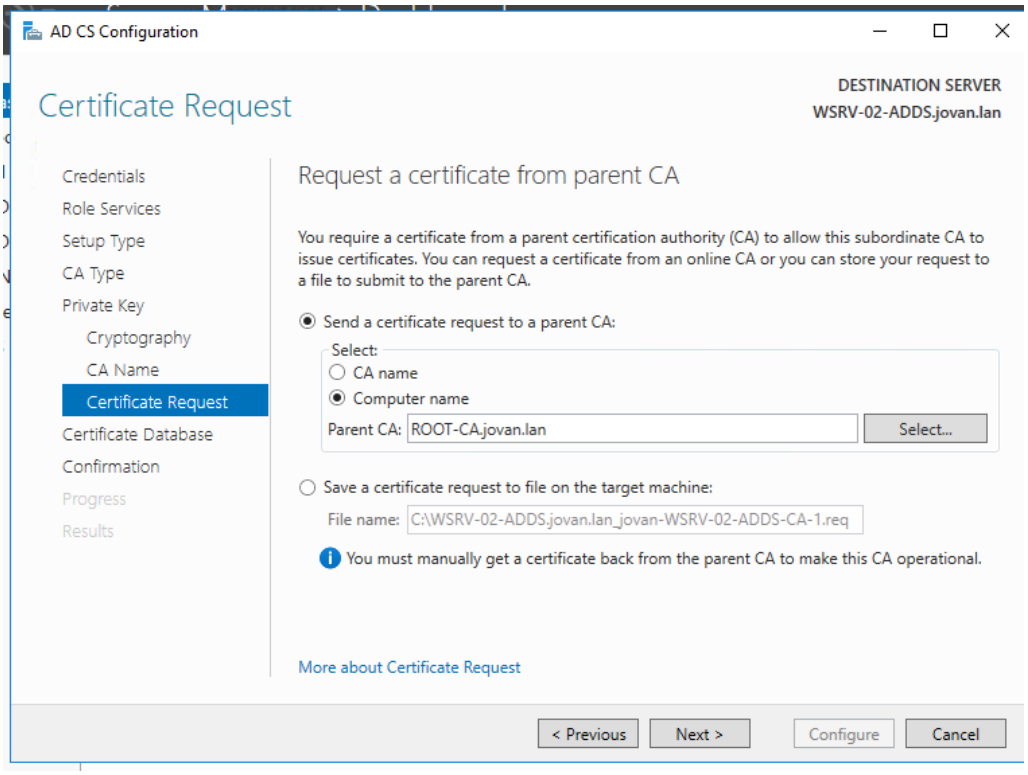


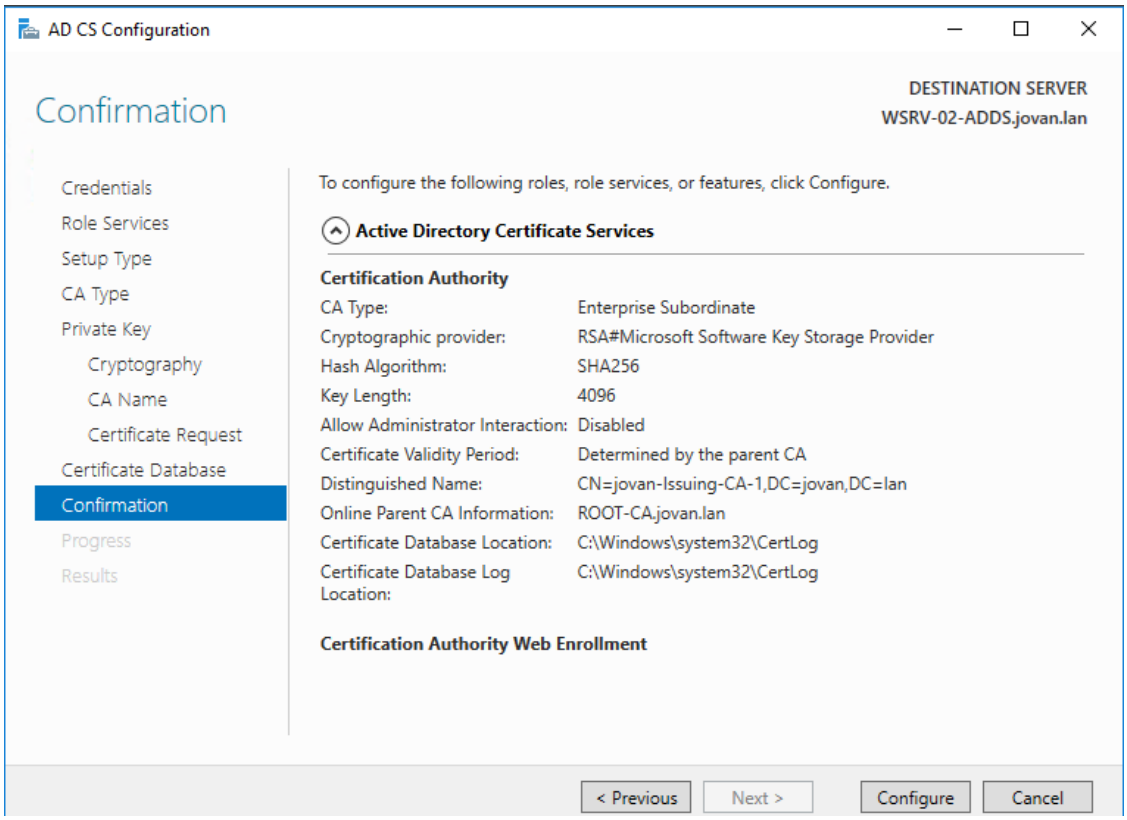


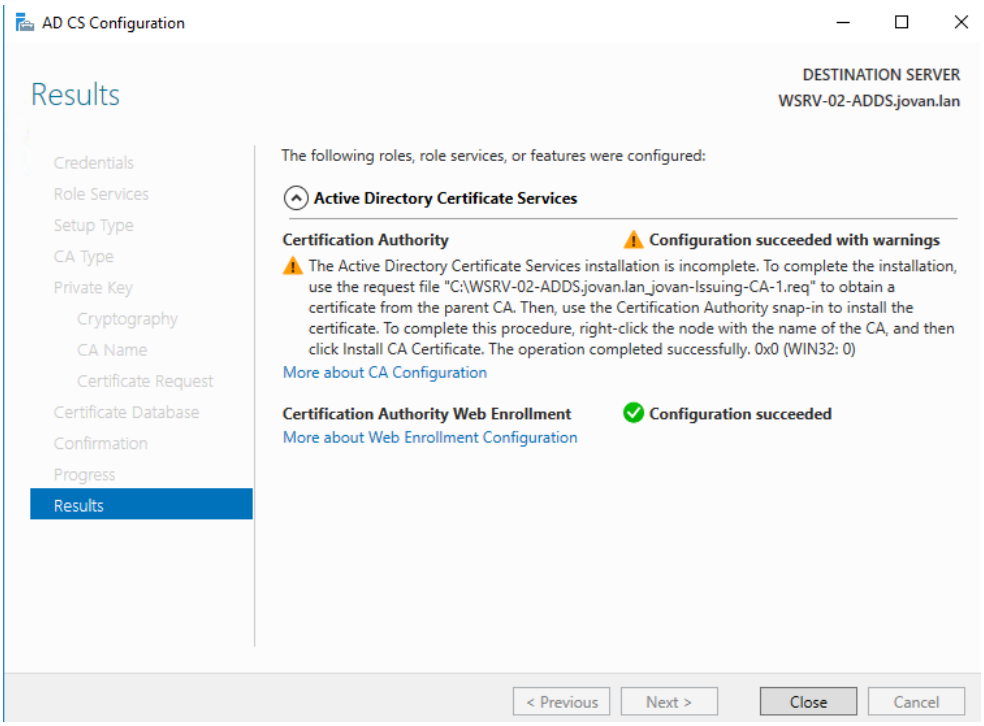
Post-deployment configuration:


WSRV-02-ADDS on DESKTOP-A344VAB - Virtual Machine Connection
File Action Media View Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD CS
AD DS
DNS
File and Storage Services
WELCOME TO SERVER
QUICK START
WHAT'S NEW
LEARN MORE
ROLES AND SERVER G
Roles: 4 | Server groups:
AD CS
Manageability
Events
Services
Performance
BPA results
Local Server 1
Manageability
Events
Services
Performance
BPA results
Hide
AD CS Configuration
Credentials
DESTINATION SERVER
WSRV-02-ADDS.jovan.lan
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: JOVAN\Administrator
Change...
More about AD CS Server Roles
< Previous
Next >
Configure
Cancel
Close
Status: Running
Type here to search
7°C Partly cloudy
00:47
30/10/2024


AD CS Configuration
CA Name
DESTINATION SERVER
WSRV-02-ADDS.jovan.lan
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Certificate Request
Certificate Database
Confirmation
Progress
Results
Specify the name of the CA
Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.
Common name for this CA:
jovan-Issuing-CA-1
Distinguished name suffix:
DC=jovan,DC=lan
Preview of distinguished name:
CN=jovan-Issuing-CA-1,DC=jovan,DC=lan
More about CA Name
< Previous
Next >
Configure
Cancel

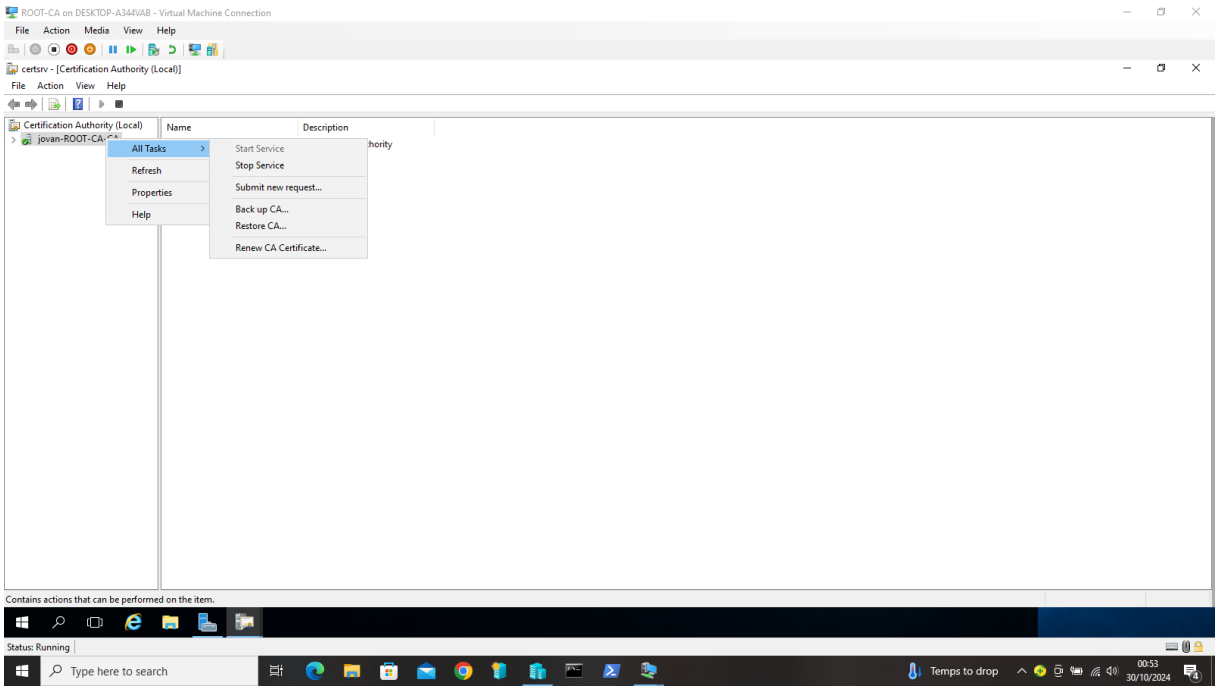

AD CS Configuration
Certificate Request
DESTINATION SERVER
WSRV-02-ADDS.jovan.lan
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Certificate Request
Certificate Database
Confirmation
Progress
Results
Request a certificate from parent CA
You require a certificate from a parent certification authority (CA) to allow this subordinate CA to issue certificates. You can request a certificate from an online CA or you can store your request to a file to submit to the parent CA.
Send a certificate request to a parent CA:
Select:
CA name
Computer name
Parent CA: ROOT-CA.jovan.lan
Select...
Save a certificate request to file on the target machine:
File name: C:\WSRV-02-ADDS.jovan.lan_jovan-WSRV-02-ADDS-CA-1.req
You must manually get a certificate back from the parent CA to make this CA operational.
More about Certificate Request
< Previous
Next >
Configure
Cancel


AD CS Configuration
Confirmation
DESTINATION SERVER
WSRV-02-ADDS.jovan.lan
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Certificate Request
Certificate Database
Confirmation
Progress
Results
To configure the following roles, role services, or features, click Configure.
Active Directory Certificate Services
Certification Authority
CA Type: Enterprise Subordinate
Cryptographic provider: RSA#Microsoft Software Key Storage Provider
Hash Algorithm: SHA256
Key Length: 4096
Allow Administrator Interaction: Disabled
Certificate Validity Period: Determined by the parent CA
Distinguished Name: CN=jovan-Issuing-CA-1,DC=jovan,DC=lan
Online Parent CA Information: ROOT-CA.jovan.lan
Certificate Database Location: C:\Windows\system32\CertLog
Certificate Database Log Location: C:\Windows\system32\CertLog
Certification Authority Web Enrollment
< Previous
Next >
Configure
Cancel



OPTION TO ADD CERTIFICATES MANUALLY

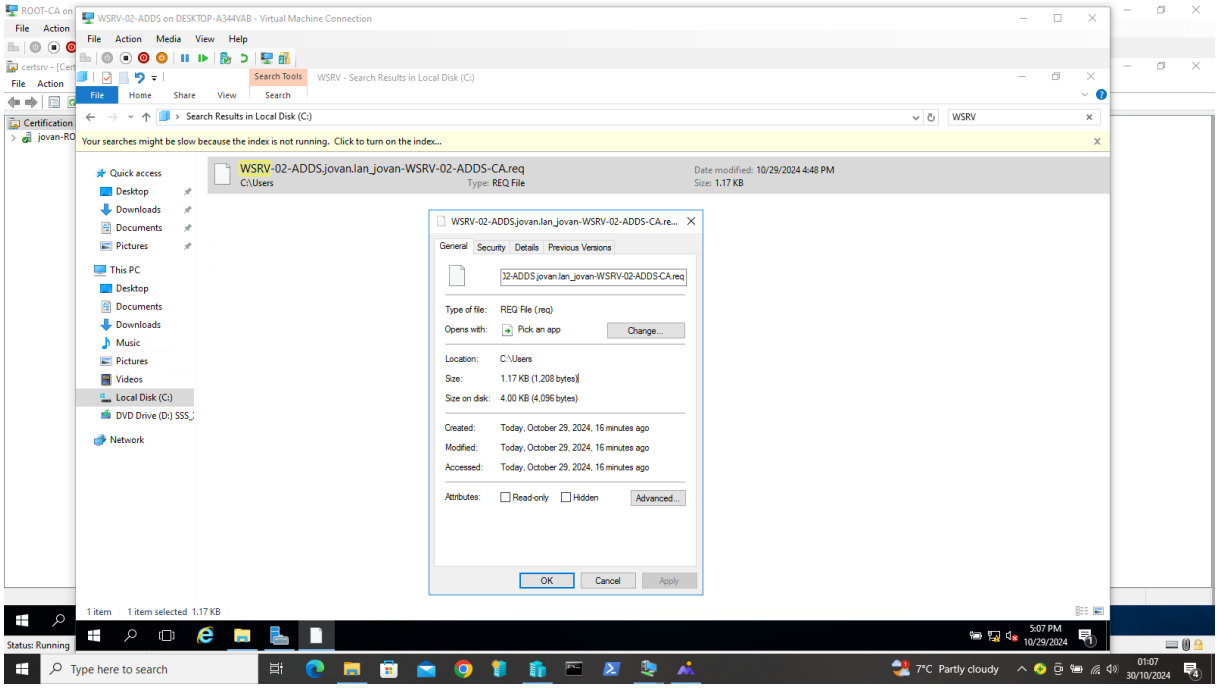
As the screenshot shows, the configuration is successful but there are some caveats, namely that it is necessary to download a certificate from the ROOT-CA server for the installation to be complete. The steps are as follows:

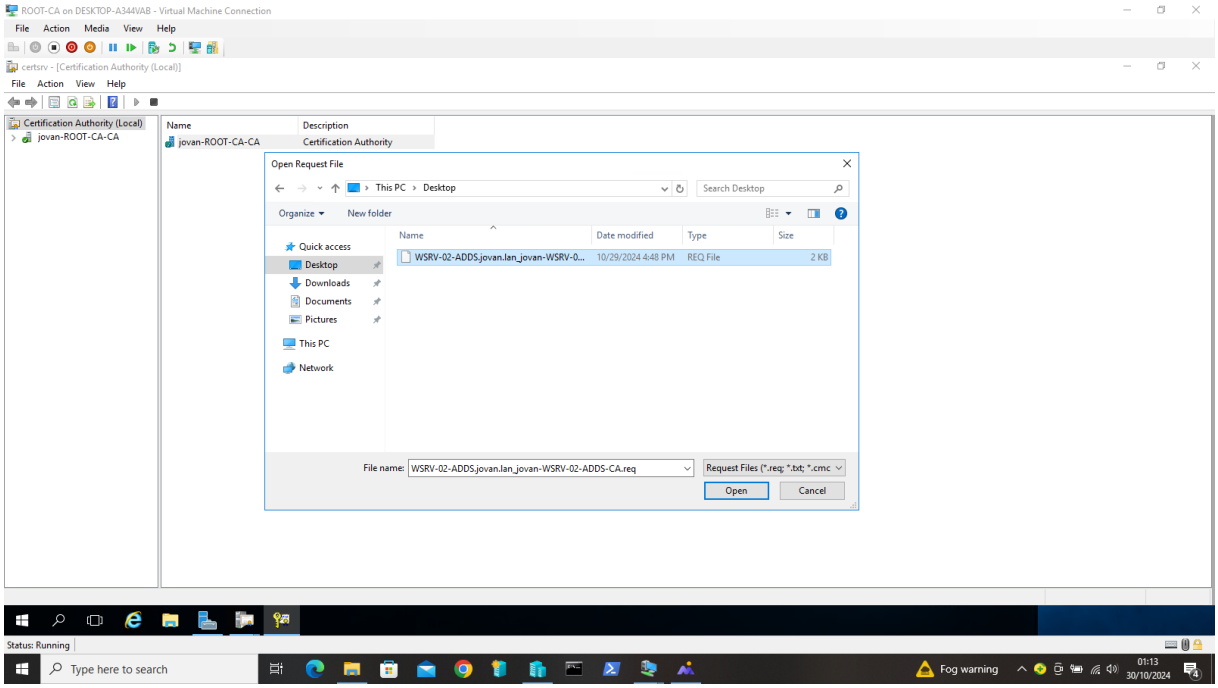


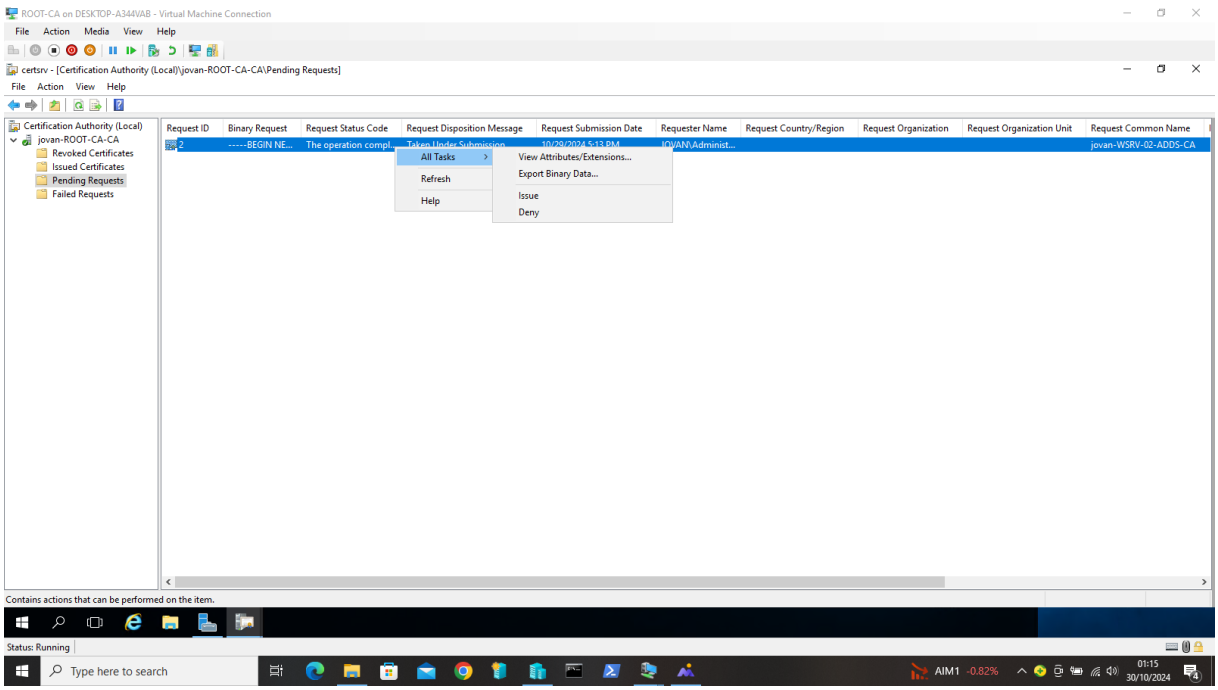
To complete the installation of the Enterprise **CA** and obtain the required certificate from the parent **Standalone Root CA** (ROOT-CA), you need to generate a Certificate Signing Request (CSR) on the Enterprise CA and then manually submit it to the ROOT-CA server for issue. The plot follows the following:

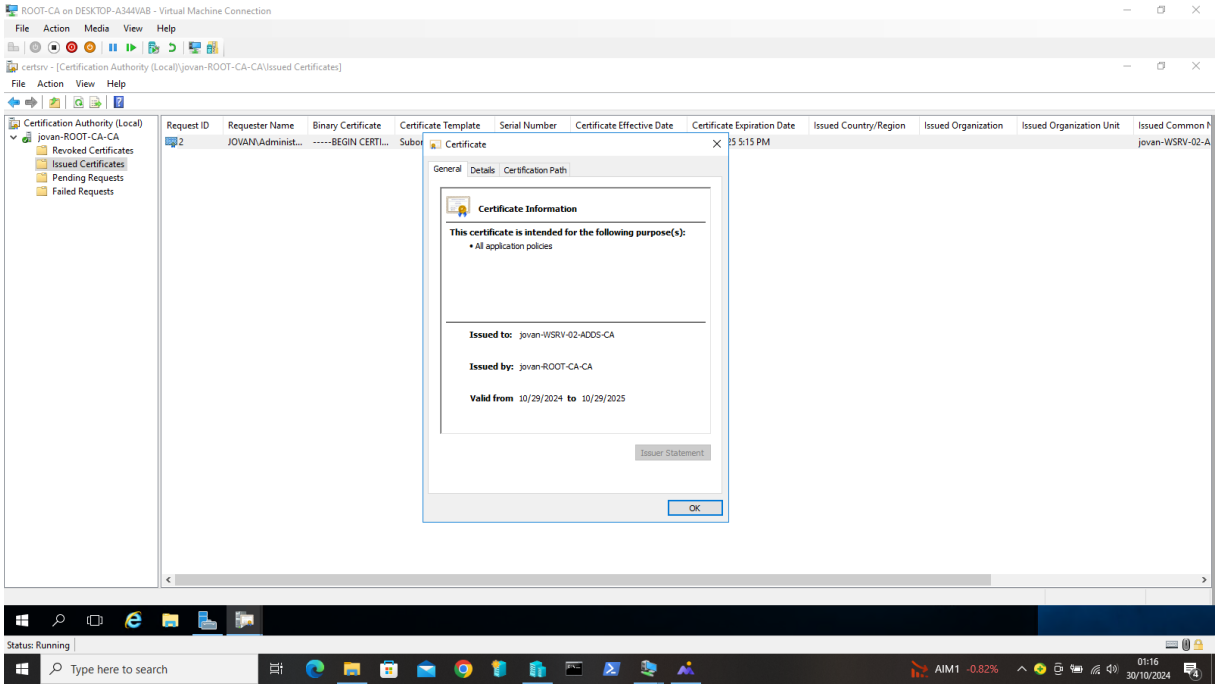
To transfer the CSR file to ROOT-CA:

Copy the **request** file (.req) to the ROOT-CA server, where you will use it to issue certificates.



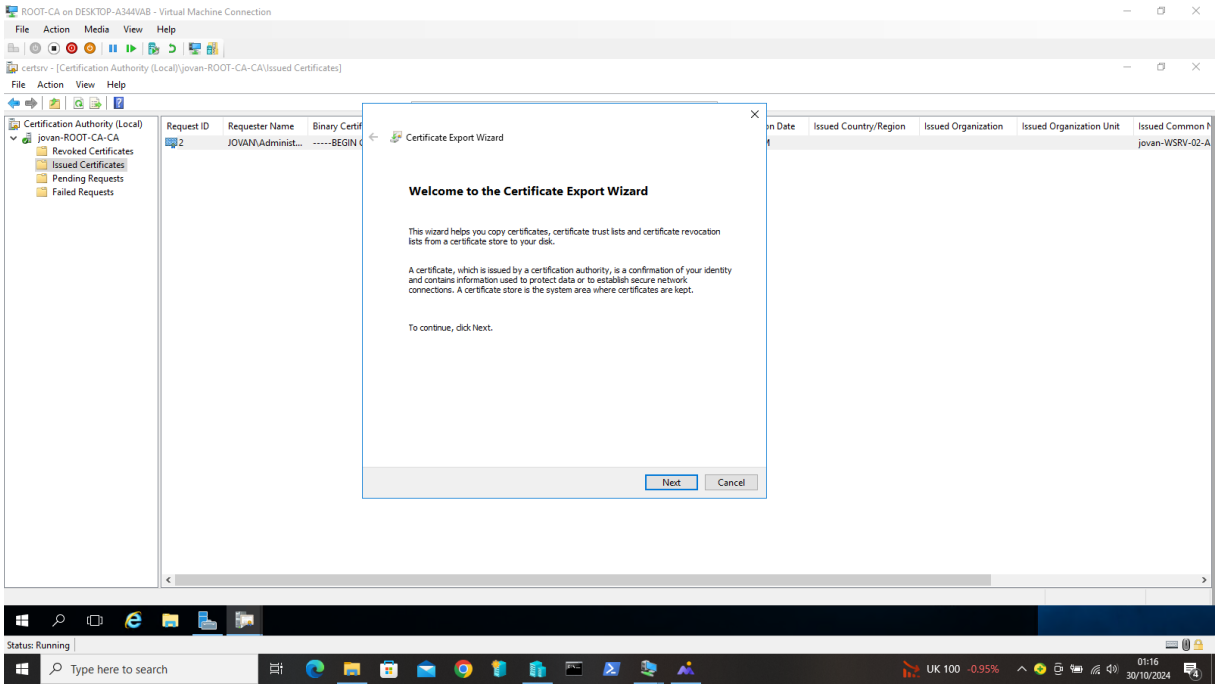


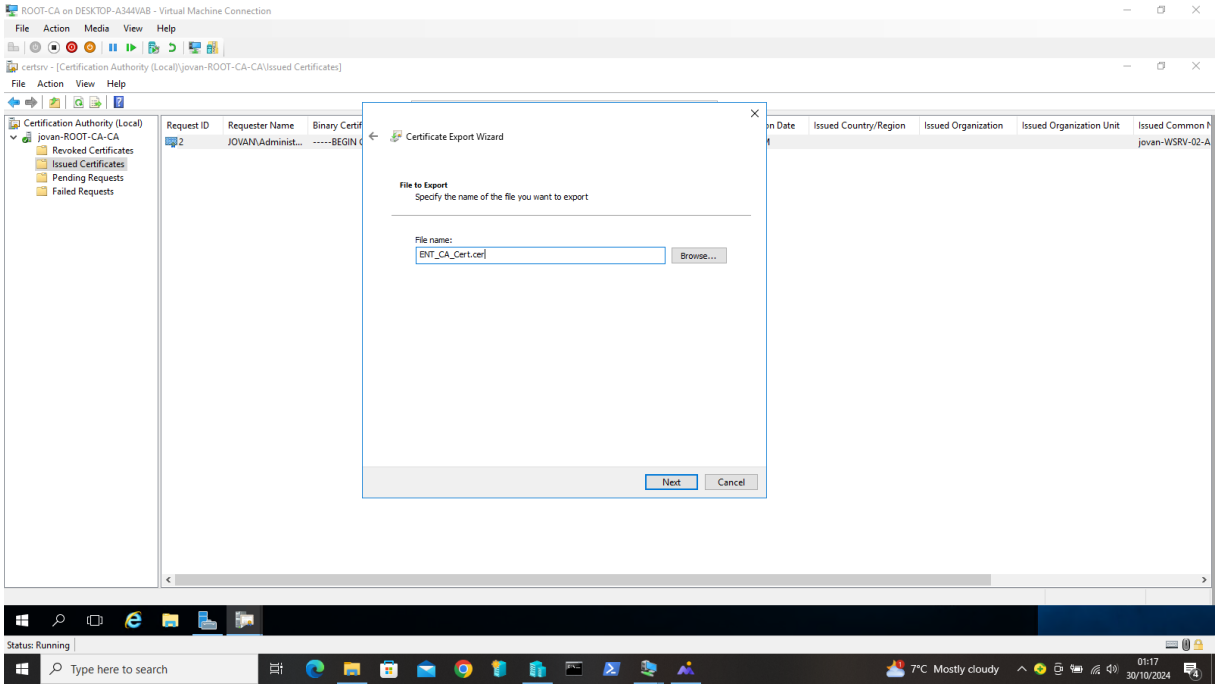


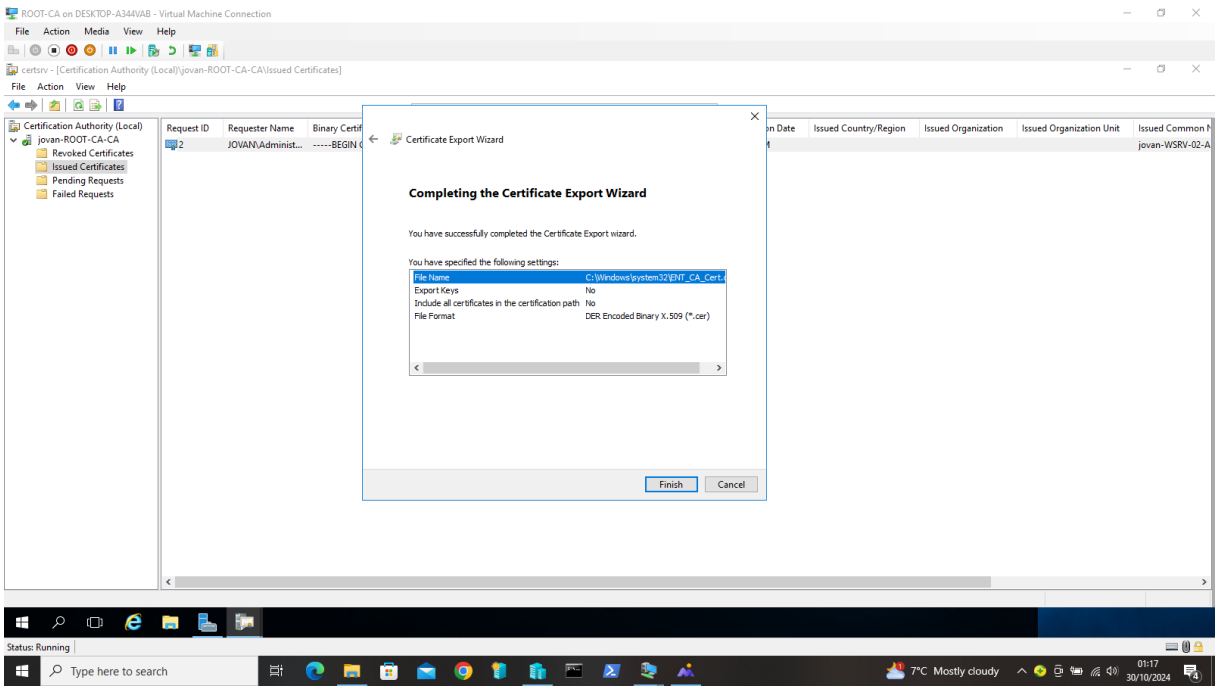


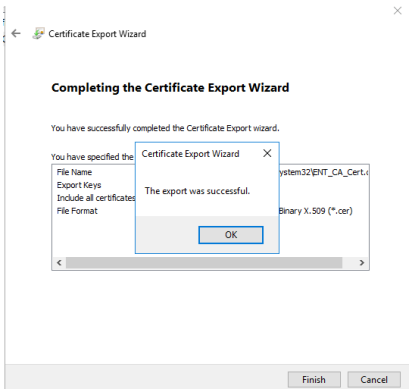
PUBLICATION OF THE BASIC CA CERTIFICATE

In order for a certificate to be published and imported, it is first necessary to export the certificate. The action is as follows:


ROOT-CA on DESKTOP-A344VAB - Virtual Machine Connection
File Action Media View Help
certsrv - [Certification Authority (Local)\jovan-ROOT-CA-CA\Issued Certificates]
File Action View Help
Certification Authority (Local)
jovan-ROOT-CA-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Request ID
Requester Name
Issued Country/Region
Issued Organization
Issued Organization Unit
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.
Next
Cancel
Status: Running
Type here to search
UK 100 -0.95%
01:16
30/10/2024


ROOT-CA on DESKTOP-A344VAB - Virtual Machine Connection
File Action Media View Help
certsrv - [Certification Authority (Local)\jovan-ROOT-CA-CA\Issued Certificates]
File Action View Help
Certification Authority (Local)
jovan-ROOT-CA-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Request ID
Requester Name
Issued Country/Region
Issued Organization
Issued Organization Unit
Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
ENT_CA_Cert.cer
Browse...
Next
Cancel
Status: Running
Type here to search
7°C Mostly cloudy
01:17
30/10/2024





1. By launching **Group Policy Management**.

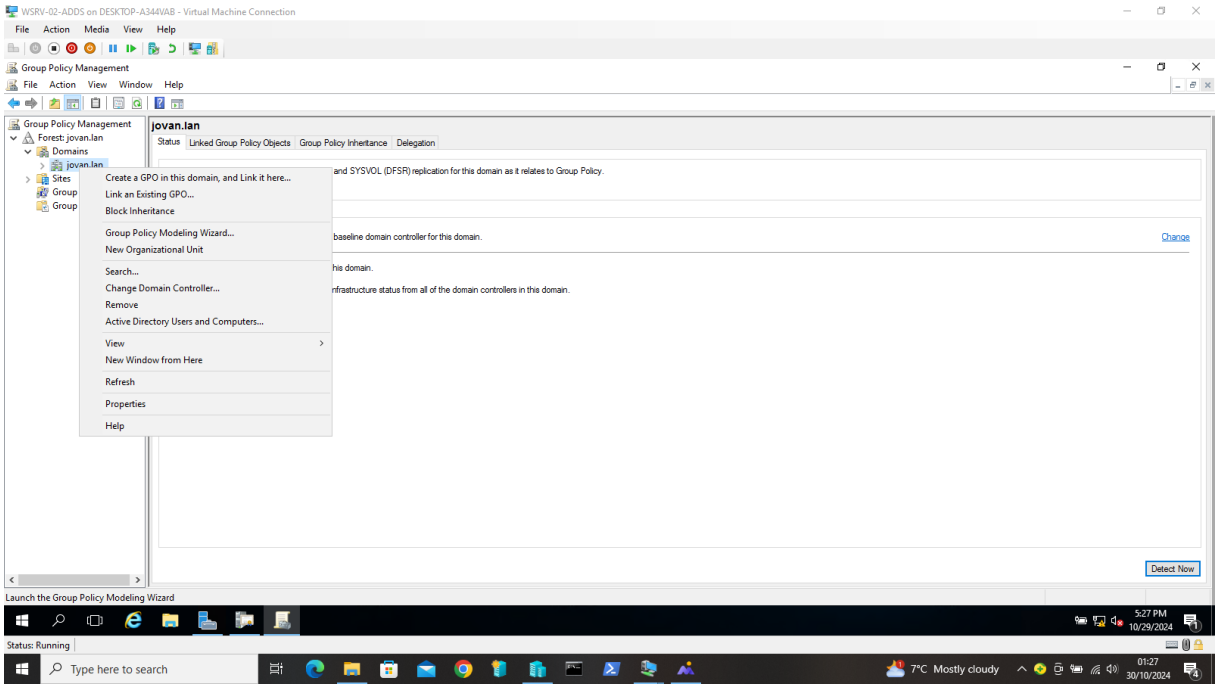
2. By creating a new or using an existing **GPO.**

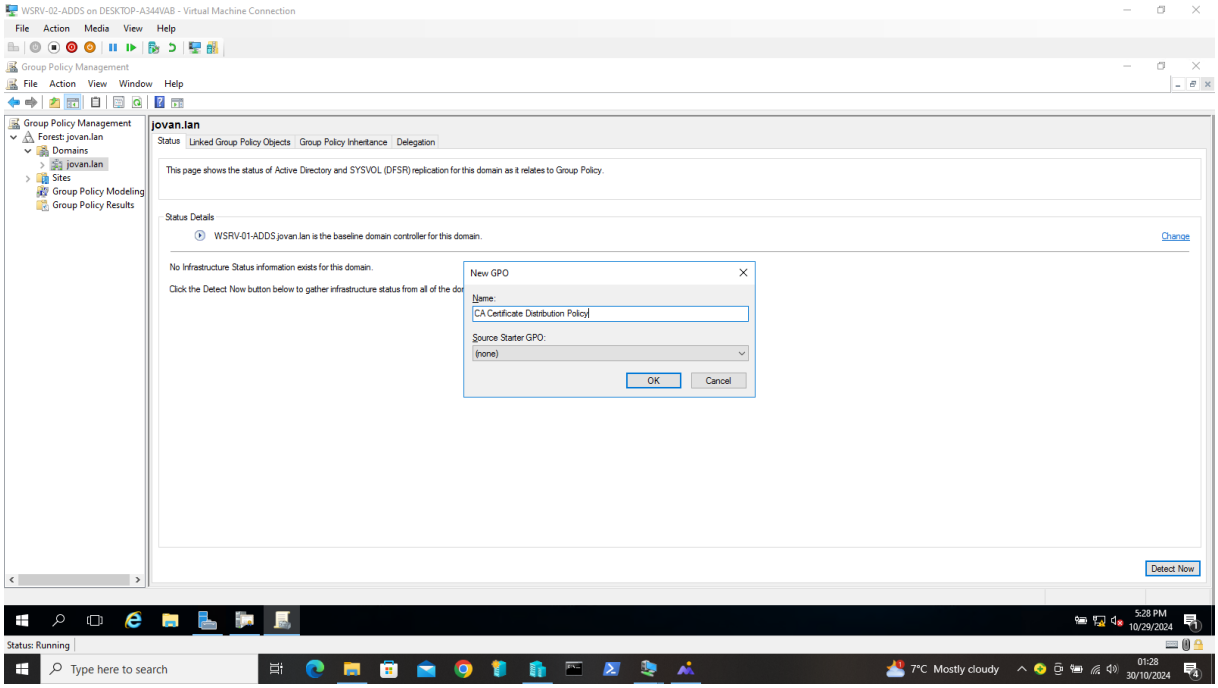
3. In the GPO Editor by running:

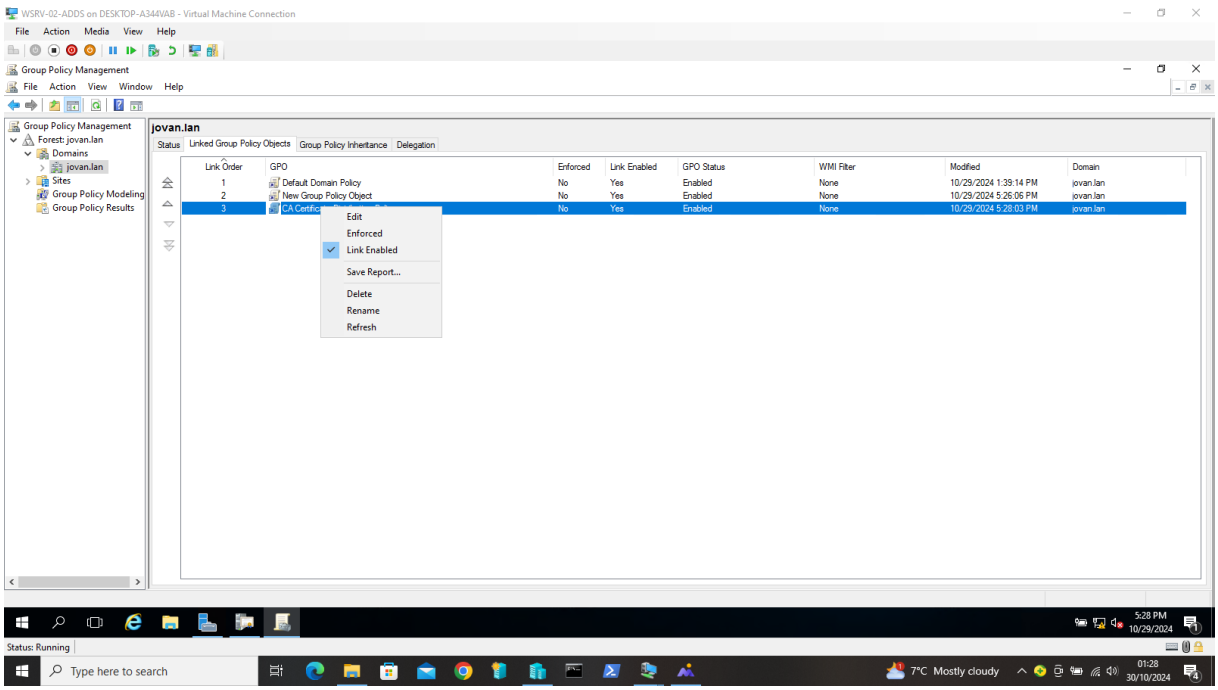
Computer Configuration - Policies - Windows Settings - Security Settings - Public Key Policies.

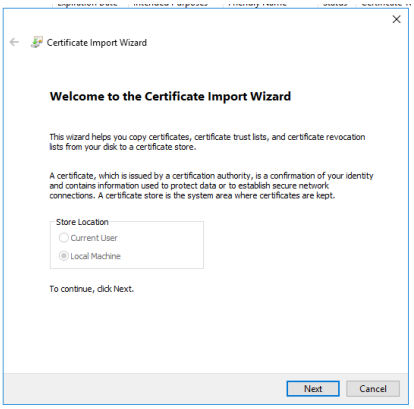
4. Right click on **Trusted Root Certification Authorities** by selecting **Import** and import the basic **CA certificate of the ROOT-CA** server.

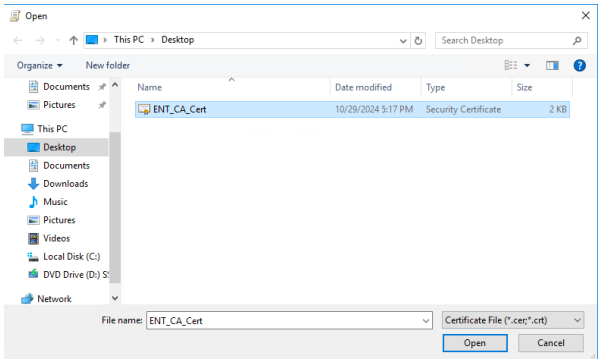
5. Click OK **.**

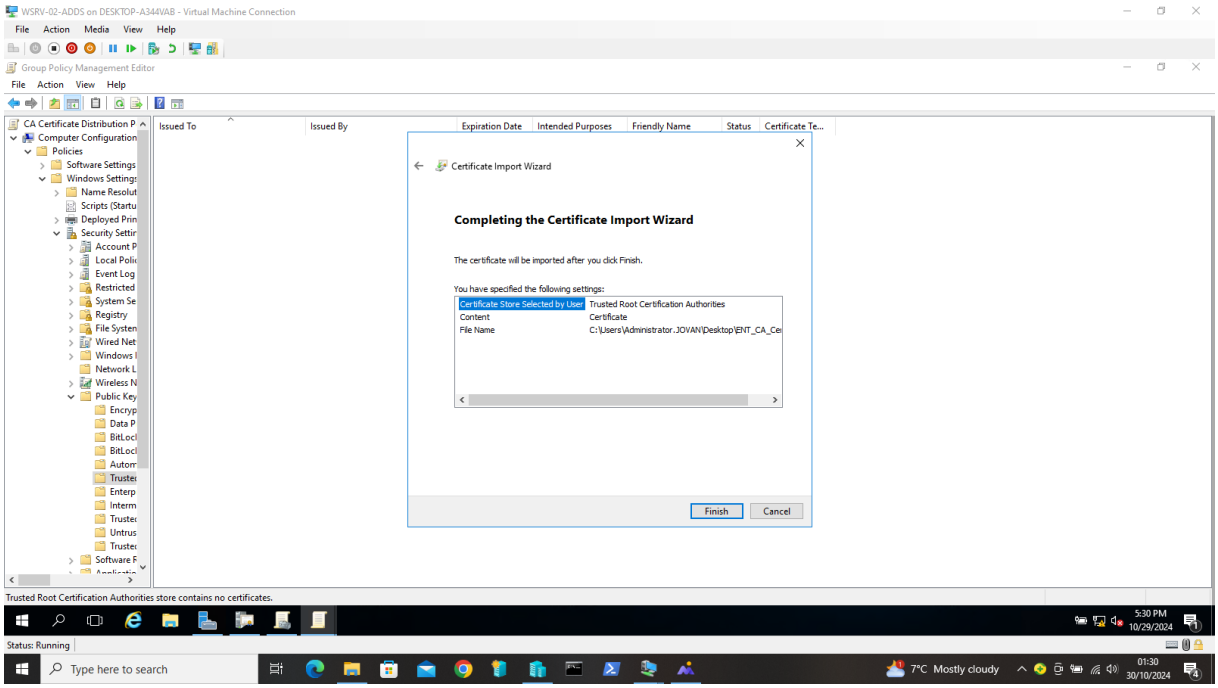

WSRV-02-ADDS on DESKTOP-A344VAB - Virtual Machine Connection
File Action Media View Help
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jovan.lan
Domains
jovan.lan
Sites
Group
Group
jovan.lan
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.
baseline domain controller for this domain.
Change
his domain.
nfrastructure status from all of the domain controllers in this domain.
Create a GPO in this domain, and Link it here...
Link an Existing GPO...
Block Inheritance
Group Policy Modeling Wizard...
New Organizational Unit
Search...
Change Domain Controller...
Remove
Active Directory Users and Computers...
View
New Window from Here
Refresh
Properties
Help
Detect Now
Launch the Group Policy Modeling Wizard
5:27 PM
10/29/2024
Status: Running
Type here to search
7°C Mostly cloudy
01:27
30/10/2024


WSRV-02-ADDS on DESKTOP-A344VAB - Virtual Machine Connection
File Action Media View Help
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jovan.lan
Domains
jovan.lan
Sites
Group Policy Modeling
Group Policy Results
jovan.lan
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
This page shows the status of Active Directory and SYSVOL (DFSR) replication for this domain as it relates to Group Policy.
Status Details
WSRV-01-ADDS.jovan.lan is the baseline domain controller for this domain.
Change
No Infrastructure Status information exists for this domain.
Click the Detect Now button below to gather infrastructure status from all of the dor
New GPO
Name:
CA Certificate Distribution Policy
Source Starter GPO:
(none)
OK
Cancel
Detect Now
5:28 PM
10/29/2024
Status: Running
Type here to search
7°C Mostly cloudy
01:28
30/10/2024


WSRV-02-ADDS on DESKTOP-A344VAB - Virtual Machine Connection
File Action Media View Help
Group Policy Management
File Action View Window Help
Group Policy Management
Forest: jovan.lan
Domains
jovan.lan
Sites
Group Policy Modeling
Group Policy Results
jovan.lan
Status
Linked Group Policy Objects
Group Policy Inheritance
Delegation
Link Order
GPO
Enforced
Link Enabled
GPO Status
WMI Filter
Modified
Domain
1
Default Domain Policy
No
Yes
Enabled
None
10/29/2024 1:39:14 PM
jovan.lan
2
New Group Policy Object
No
Yes
Enabled
None
10/29/2024 5:26:06 PM
jovan.lan
3
No
Yes
Enabled
None
10/29/2024 5:28:03 PM
jovan.lan
Edit
Enforced
Link Enabled
Save Report...
Delete
Rename
Refresh
5:28 PM
10/29/2024
Status: Running
Type here to search
7°C Mostly cloudy
01:28
30/10/2024


Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
Store Location
Current User
Local Machine
To continue, click Next.
Next
Cancel

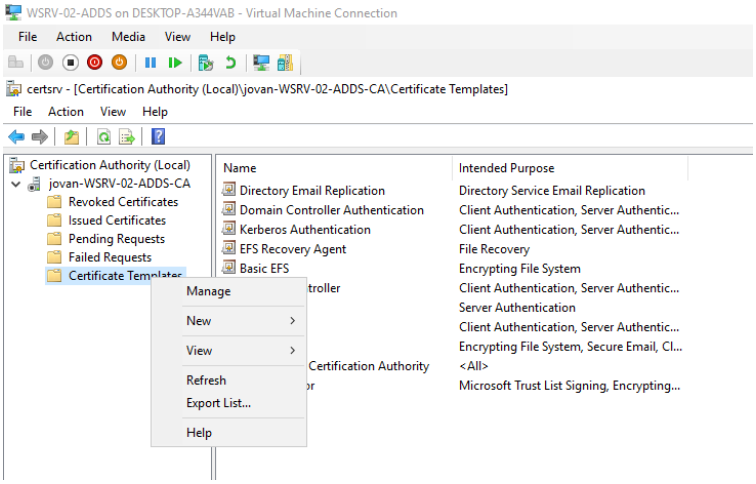

Open
This PC › Desktop
Search Desktop
Organize
New folder
Documents
Pictures
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) S
Network
Name
Date modified
Type
Size
ENT_CA_Cert
10/29/2024 5:17 PM
Security Certificate
2 KB
File name: ENT_CA_Cert
Certificate File (*.cer;*.crt)
Open
Cancel

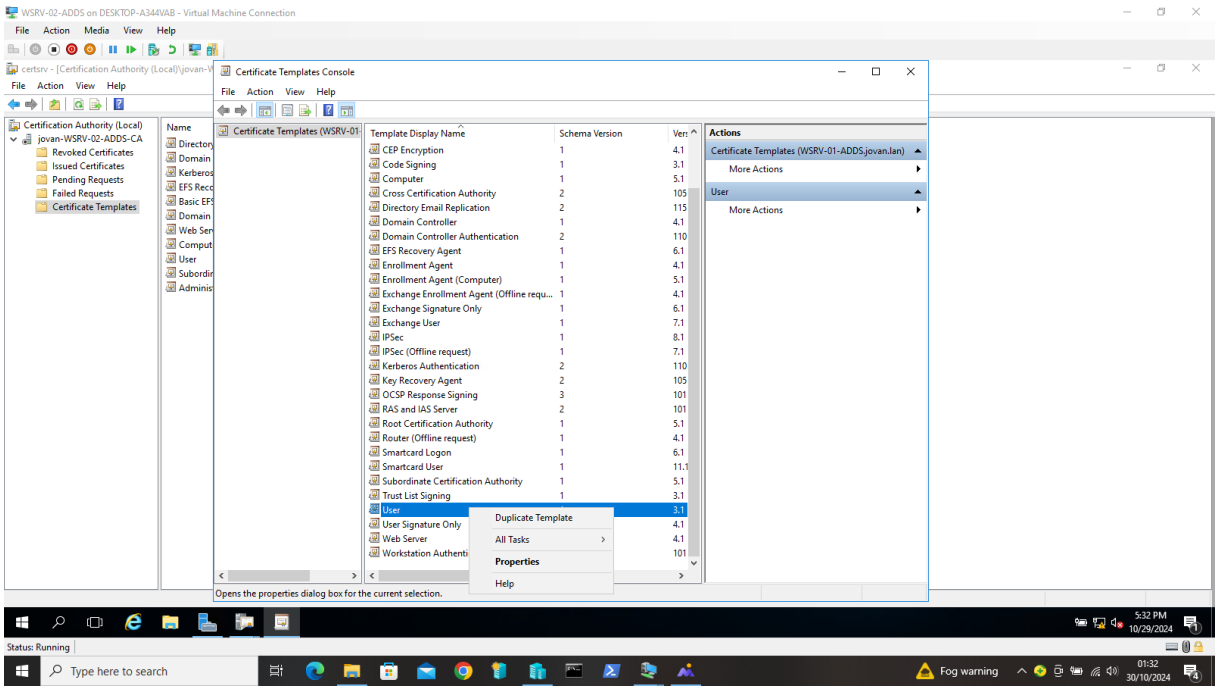


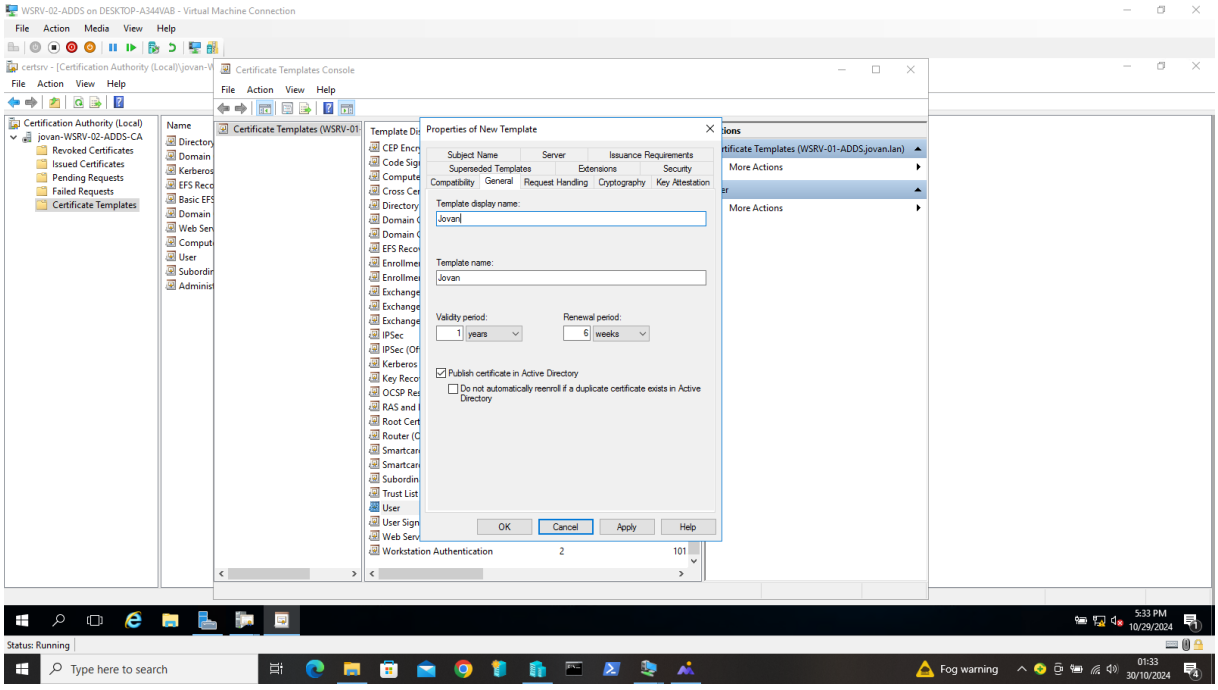
CREATING AND PUBLISHING TEMPLATE CERTIFICATES FOR USERS

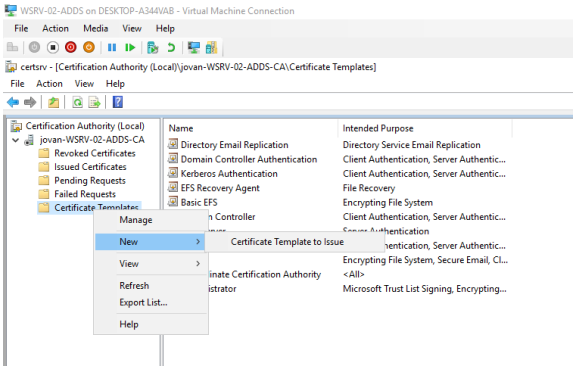
Creating and Publishing Duplicate User Certificates

1. By selecting the **Certification Authority section** on the Enterprise server.
2. In the left pane, expand the **Certificate Templates** and right click **Manage**.
3. By selecting the **User** Template icon, right click on **Duplicate Template**.
4. In the General section, choosing a name, in this case **John.**
5. Click OK**.**
6. Returning to **the Certification Authority**, right click on **Certificate Templates**, select **New -Certificate Template to Issue** and select the created template.


WSRV-02-ADDS on DESKTOP-A344VAB - Virtual Machine Connection
File Action Media View Help
certsrv - [Certification Authority (Local)\jovan-WSRV-02-ADDS-CA\Certificate Templates]
File Action View Help
Certification Authority (Local)
jovan-WSRV-02-ADDS-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Name
Intended Purpose
Directory Email Replication
Directory Service Email Replication
Domain Controller Authentication
Client Authentication, Server Authentic...
Kerberos Authentication
Client Authentication, Server Authentic...
EFS Recovery Agent
File Recovery
Basic EFS
Encrypting File System
Client Authentication, Server Authentic...
Server Authentication
Client Authentication, Server Authentic...
Encrypting File System, Secure Email, Cl...
<All>
Microsoft Trust List Signing, Encrypting...
Manage
New
View
Refresh
Export List...
Help


Certificate Templates Console
File Action View Help
Certificate Templates (WSRV-01-ADDS.jovan.lan)
Template Display Name
Schema Version
CEP Encryption
Code Signing
Computer
Cross Certification Authority
Directory Email Replication
Domain Controller
Domain Controller Authentication
EFS Recovery Agent
Enrollment Agent
Enrollment Agent (Computer)
Exchange Enrollment Agent (Offline requ...
Exchange Signature Only
Exchange User
IPSec
IPSec (Offline request)
Kerberos Authentication
Key Recovery Agent
OCSP Response Signing
RAS and IAS Server
Root Certification Authority
Router (Offline request)
Smartcard Logon
Smartcard User
Subordinate Certification Authority
Trust List Signing
User
User Signature Only
Web Server
Workstation Authenti
Duplicate Template
All Tasks
Properties
Help
Actions
More Actions
Opens the properties dialog box for the current selection.
Status: Running
Type here to search
Fog warning


Properties of New Template
Subject Name
Server
Issuance Requirements
Superseded Templates
Extensions
Security
Compatibility
General
Request Handling
Cryptography
Key Attestation
Template display name:
Jovan
Template name:
Jovan
Validity period:
1
years
Renewal period:
6
weeks
Publish certificate in Active Directory
Do not automatically reenroll if a duplicate certificate exists in Active Directory
OK
Cancel
Apply
Help
Workstation Authentication
2
101
Status: Running
Type here to search
Fog warning


WSRV-02-ADDS on DESKTOP-A344VAB - Virtual Machine Connection
File Action Media View Help
certsrv - [Certification Authority (Local)\jovan-WSRV-02-ADDS-CA\Certificate Templates]
File Action View Help
Certification Authority (Local)
jovan-WSRV-02-ADDS-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Name
Intended Purpose
Directory Email Replication
Directory Service Email Replication
Domain Controller Authentication
Client Authentication, Server Authentic...
Kerberos Authentication
Client Authentication, Server Authentic...
EFS Recovery Agent
File Recovery
Basic EFS
Encrypting File System
Client Authentication, Server Authentic...
Encrypting File System, Secure Email, Cl...
<All>
Microsoft Trust List Signing, Encrypting...
Manage
New
View
Refresh
Export List...
Help
Certificate Template to Issue