Active Directory with Windows Server 2016

Contents

1. Purpose

The purpose of this project is to familiarize ourselves with user Active Directory role of Windows Server 2016. Our main objectives are to create users, apply user rights, create security groups along with templates for them, create organizational units and then apply group policies via Group Policy Objects (GPO) to map network drives and set certain Internet Explorer settings for our fictional company: Wissen Şirket. This is the hierarchy of the company that we will be using:

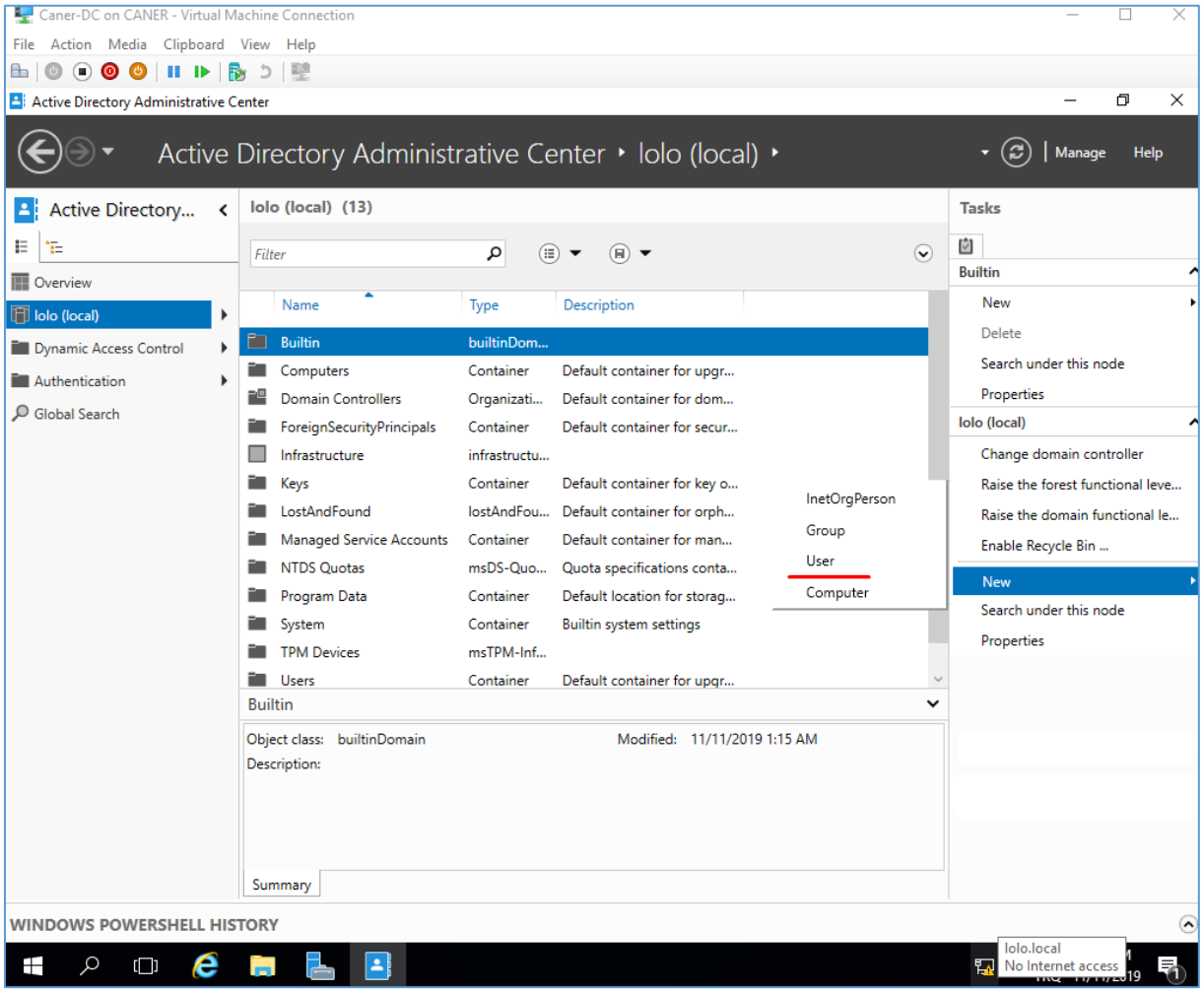
	IT	HR
Manager	Avşar	Esra
Team Leader	Umut	Ertan
Employee	Caner	Mehmet

In the second part of this project, we shall be using certificates for an extra layer of security. The topology we will be using is with 3 servers; LON-DC1 is the Domain Controller of our domain “cert.local”, LON-SRV1 is the Subordinate Enterprise Certificate Authority which will be circulating the certificate and CA-SRV1 is the Standalone Root Certificate Authority (CA) that originally publishes the certificate. Our aim is to test how certificates work and implement increased security.

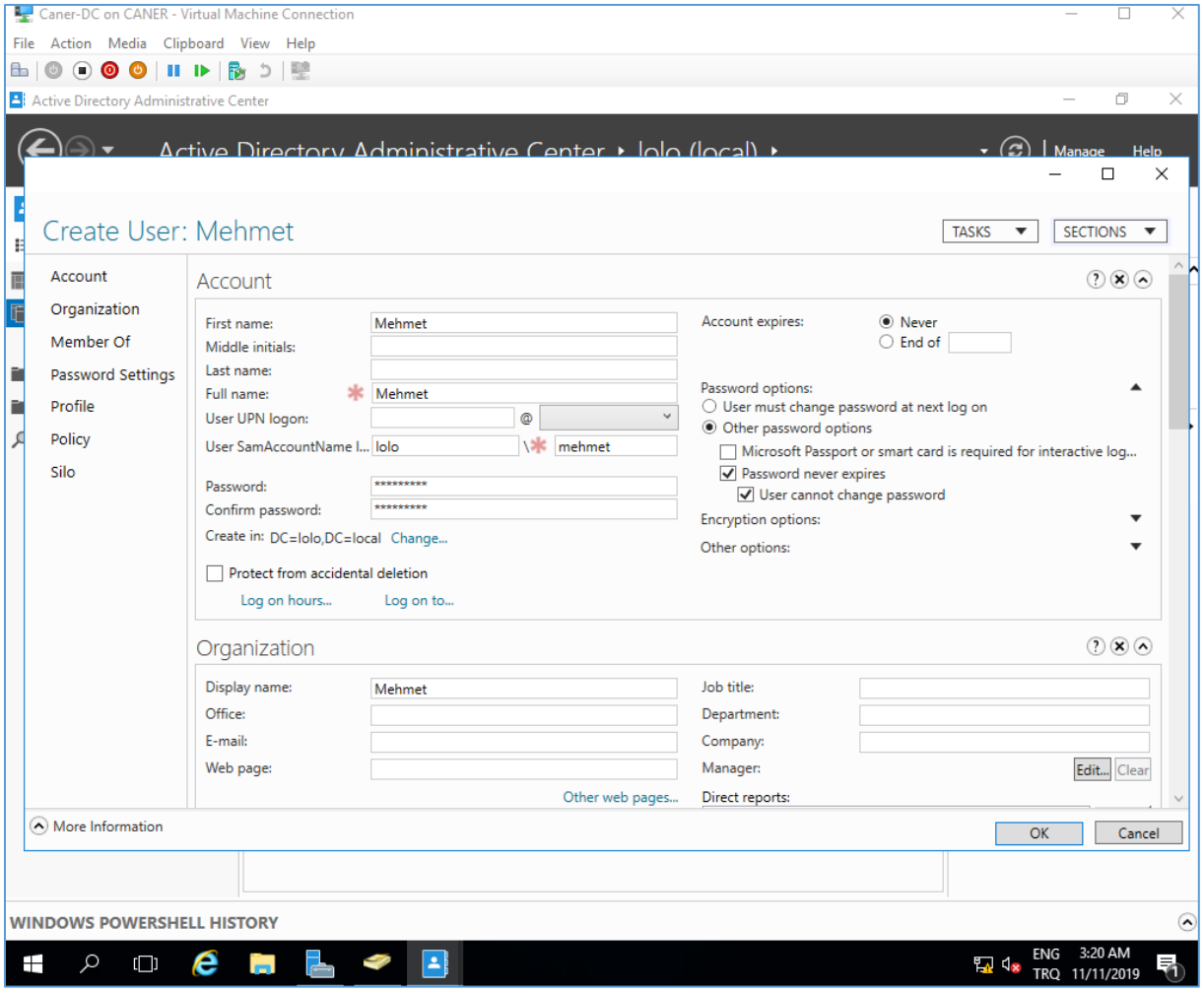
2. Procedure

I. Active Directory and Group Policy Objects (GPO)

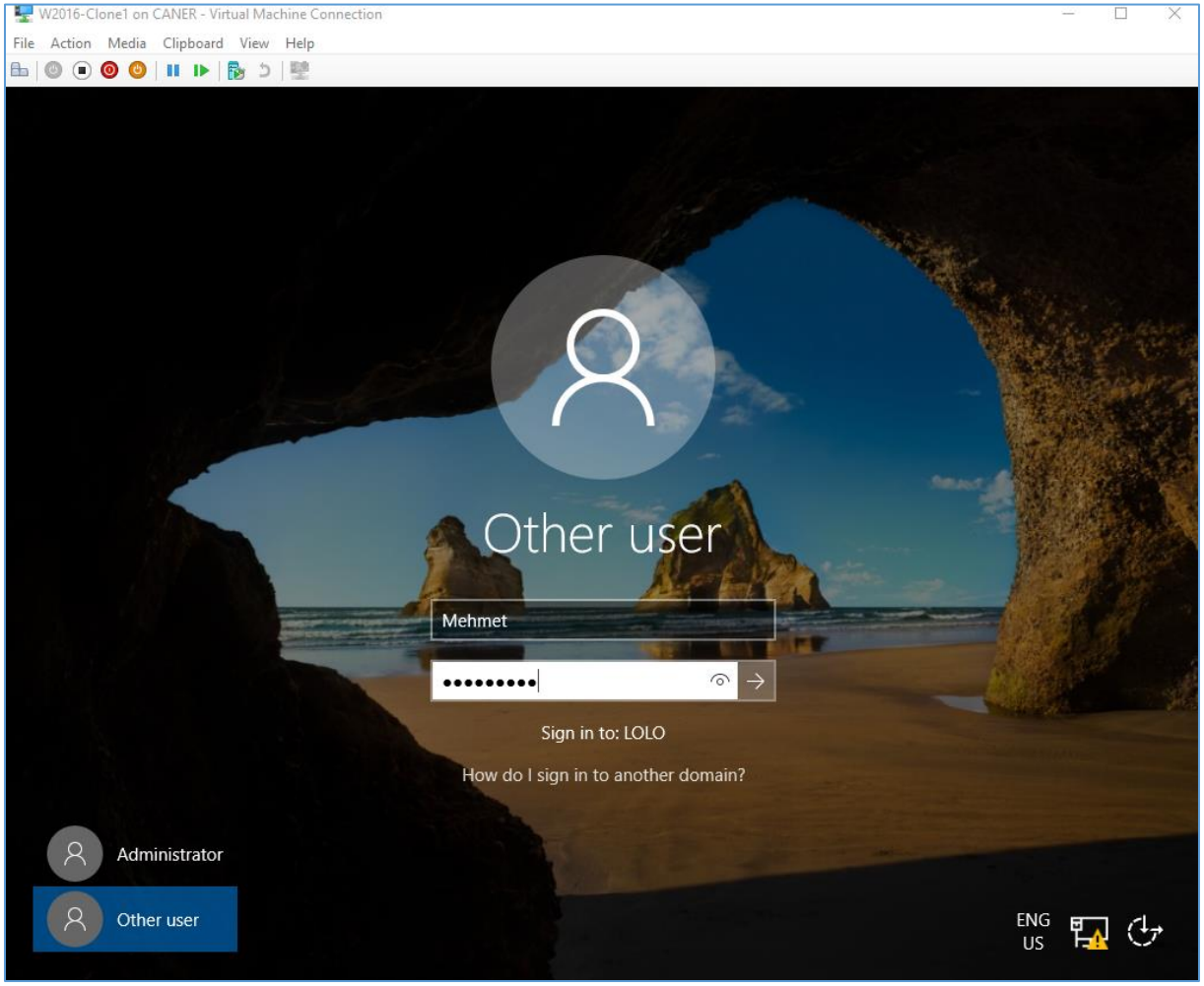
We start with an already established Active Directory domain. Ours is “lolo.local”. You can refer to Report 3: Windows Server 2016-High Availability for the creation of a new domain in active directory. At the Domain Controller, we create new users via clicking on New and selecting User under Active Directory Administrative Center.



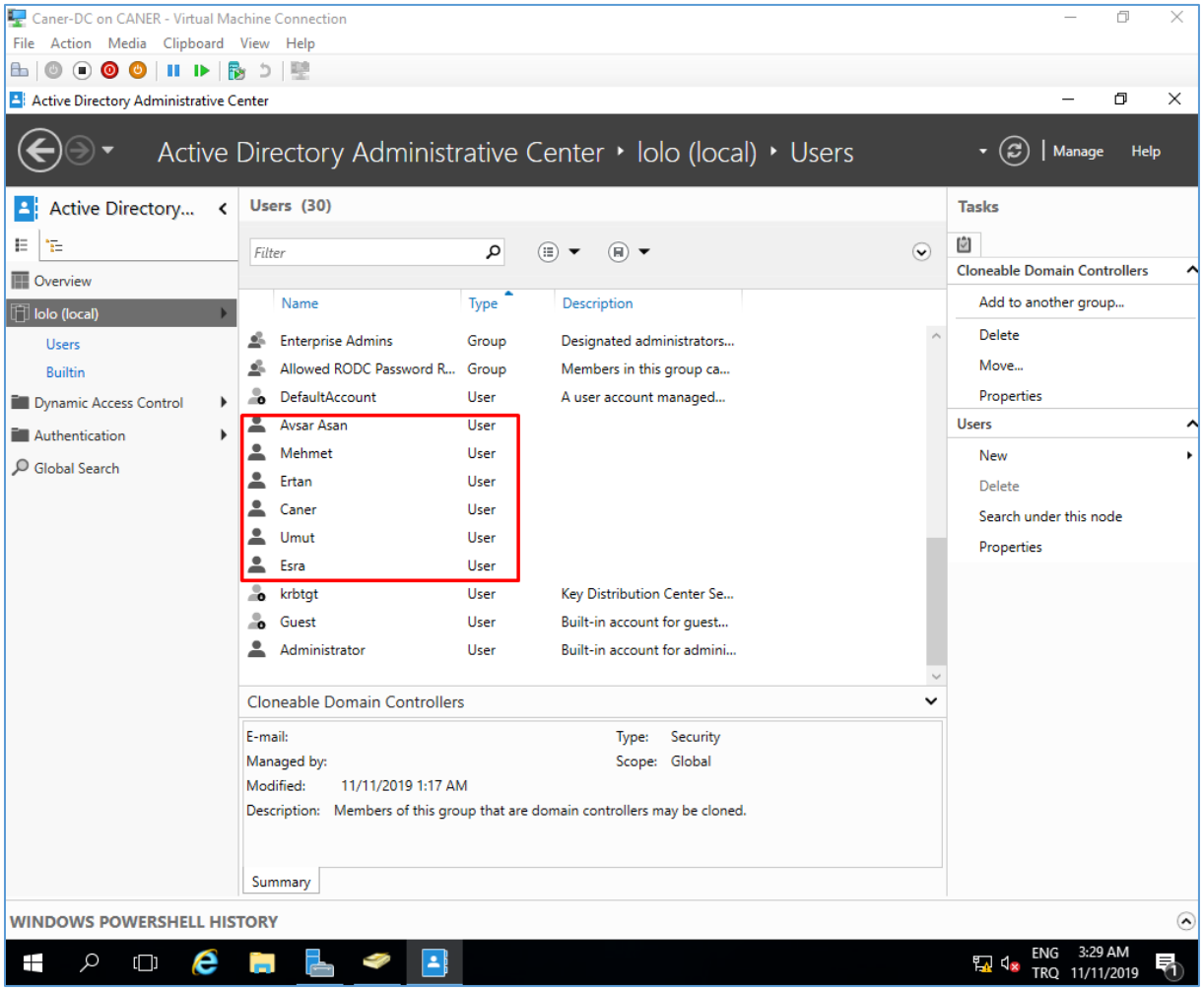
We enter the relevant information, password and setting for the new user.



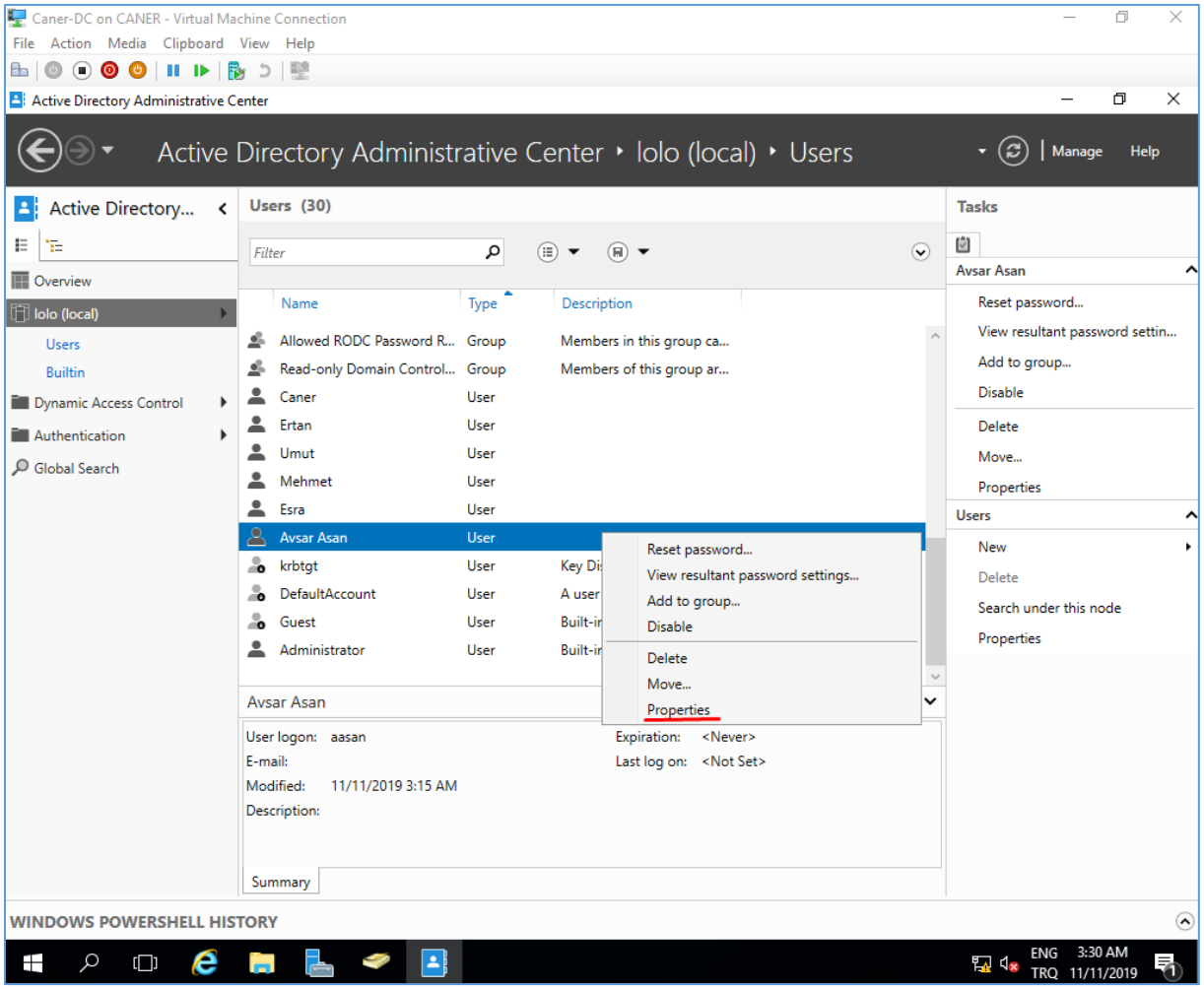
Then, we switch to the other PC in our domain, lolo.local, and log in using the credentials of the new User we have just created.



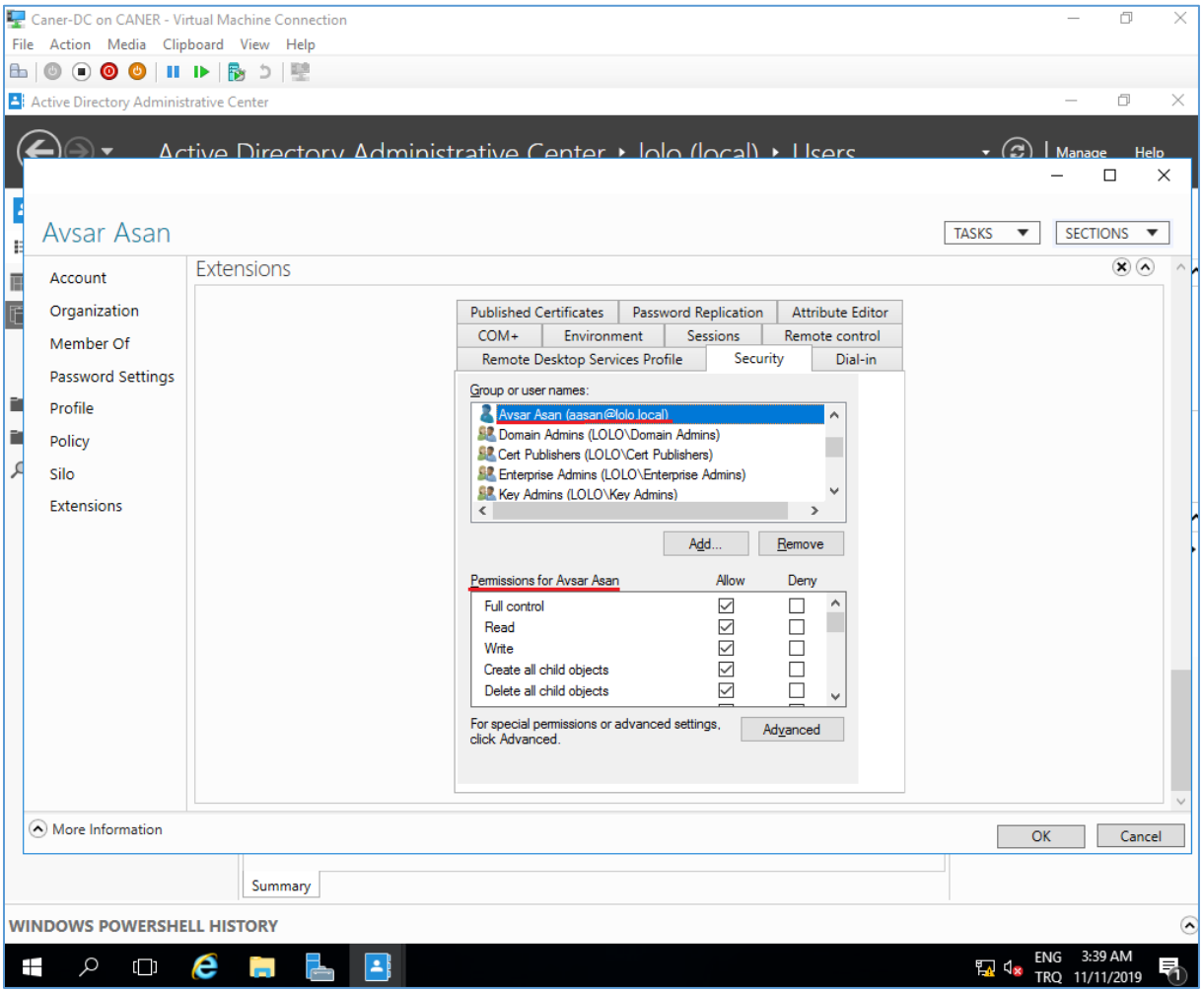
We create all the Users we will be needing.



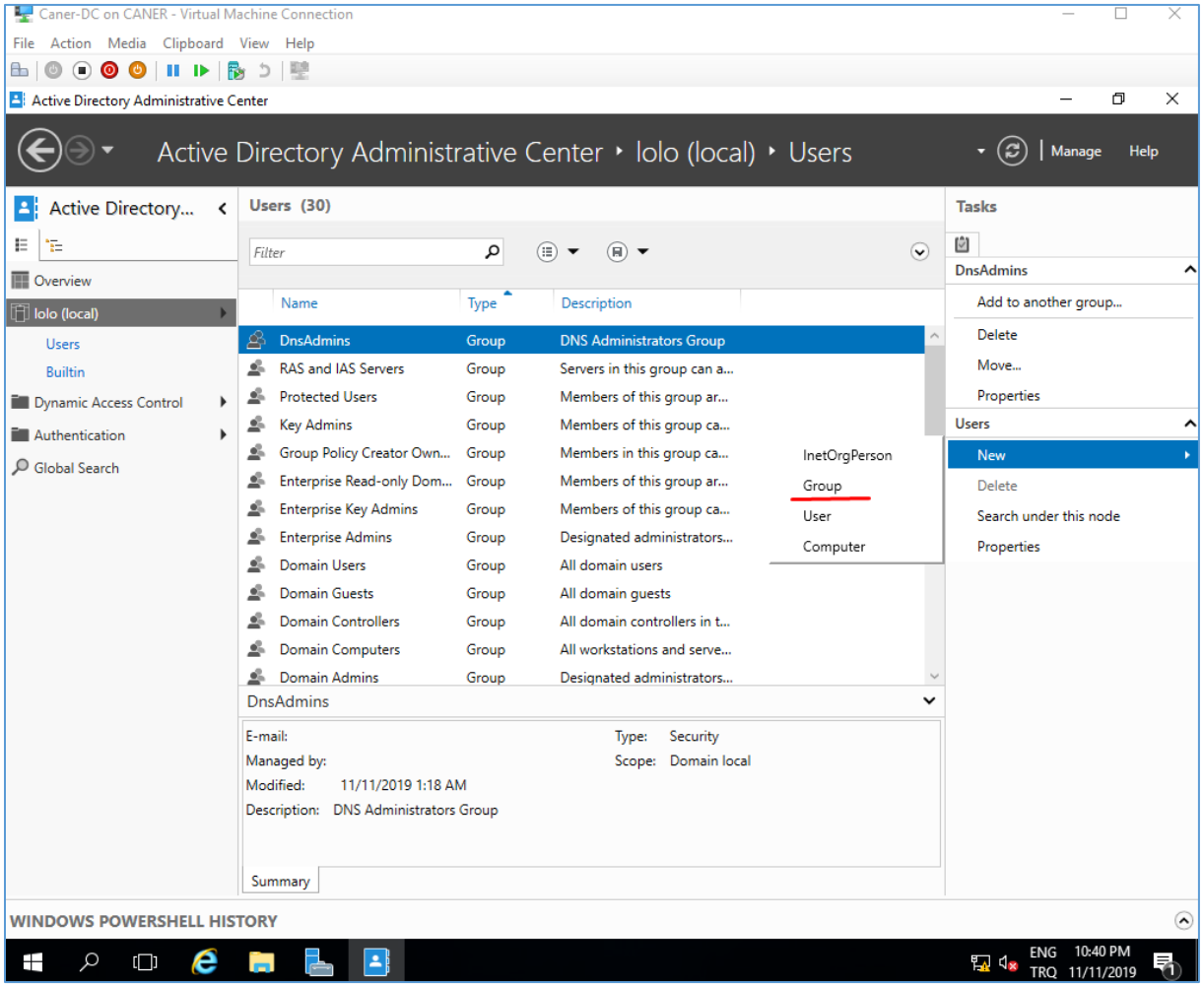
To apply user rights, we need to get to the user's properties.



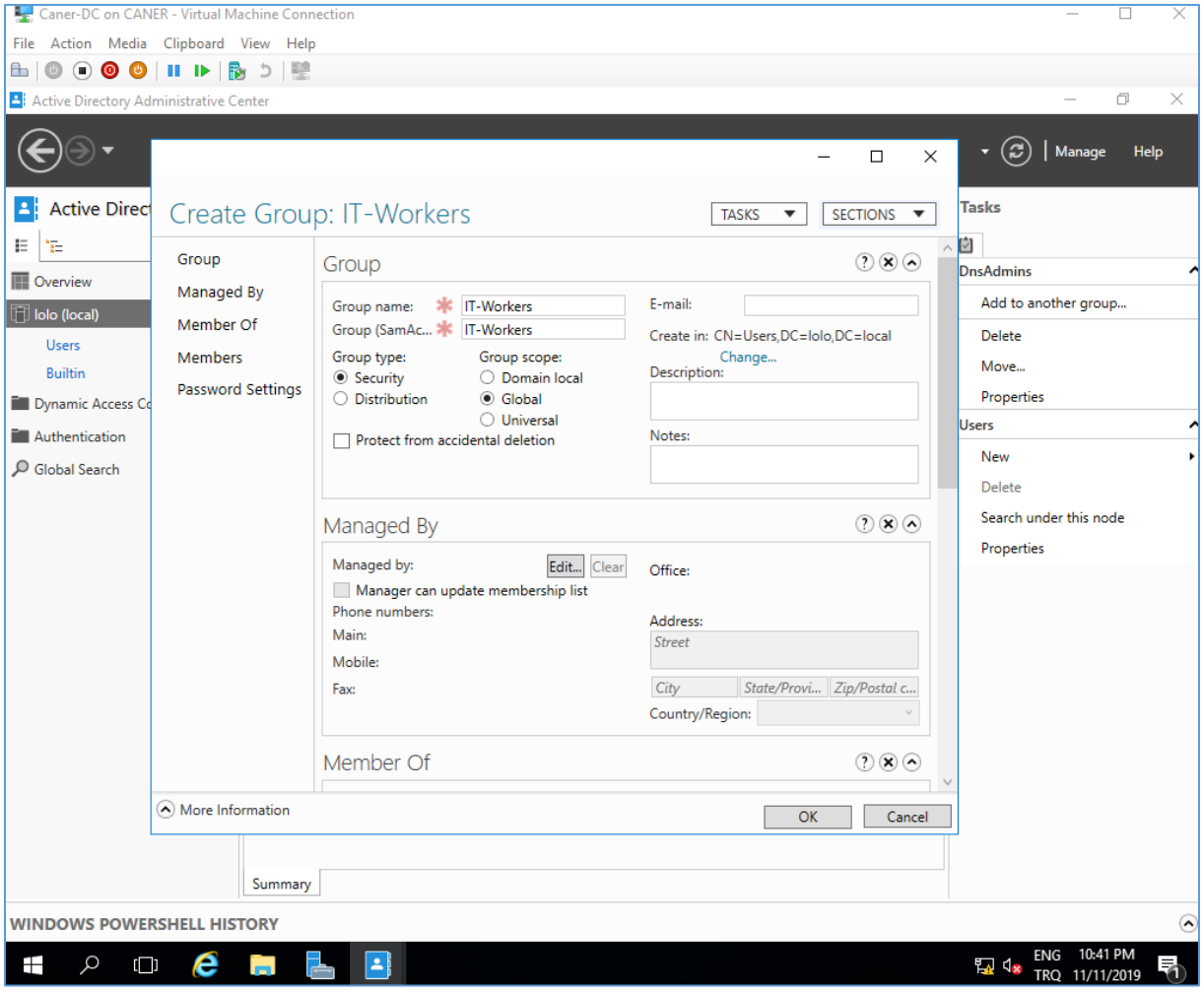
At the bottom of the page we get to Extensions and select Security. If we see the user's name, then we select it at the top; or else, we add the user we want to apply rights for and then select it. Then, at the bottom box we can see Permissions for the User or Group that we selected and we can apply rights to them. As you can see, Avşar Asan has full control.



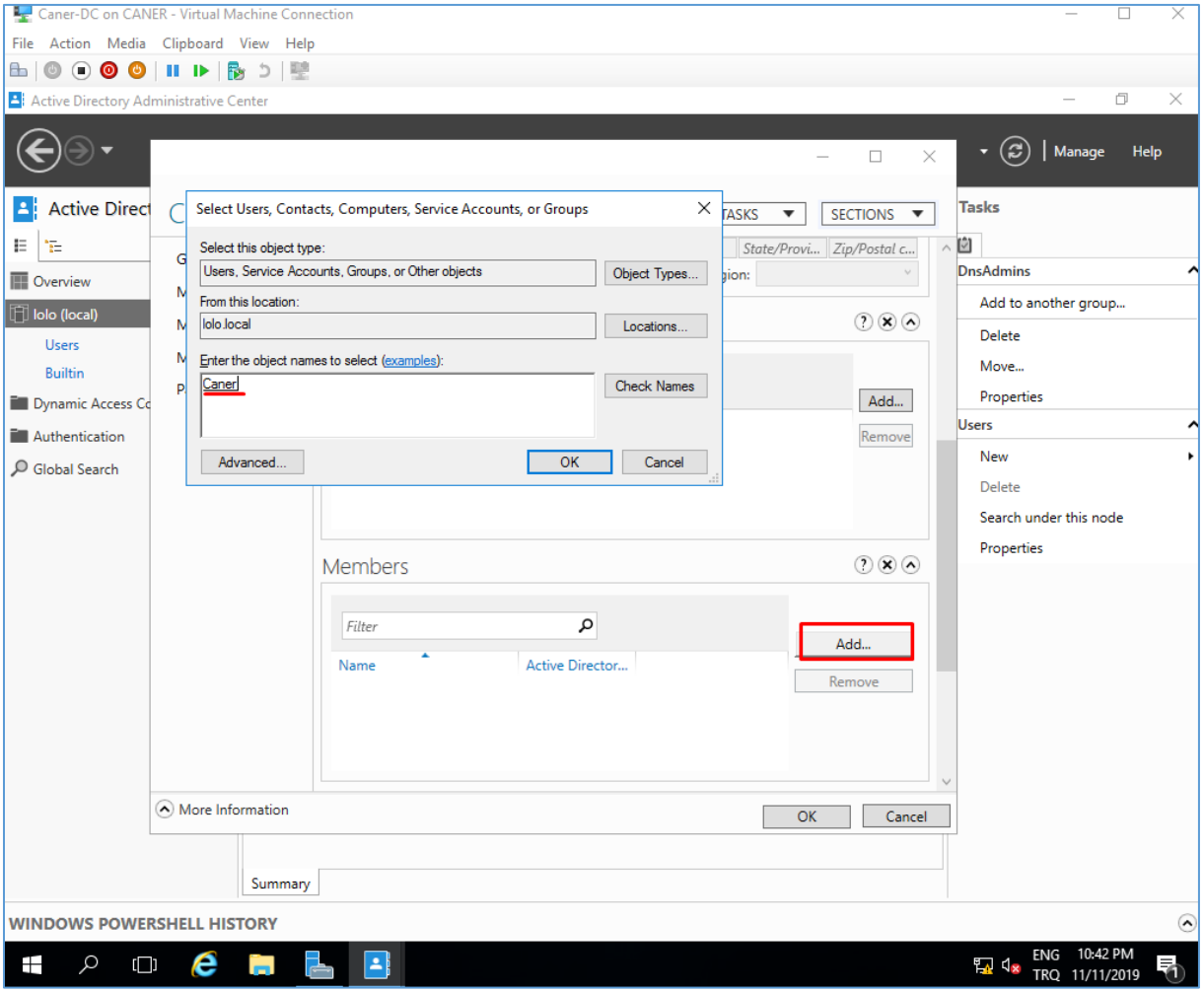
We shall then create a Group in our domain.



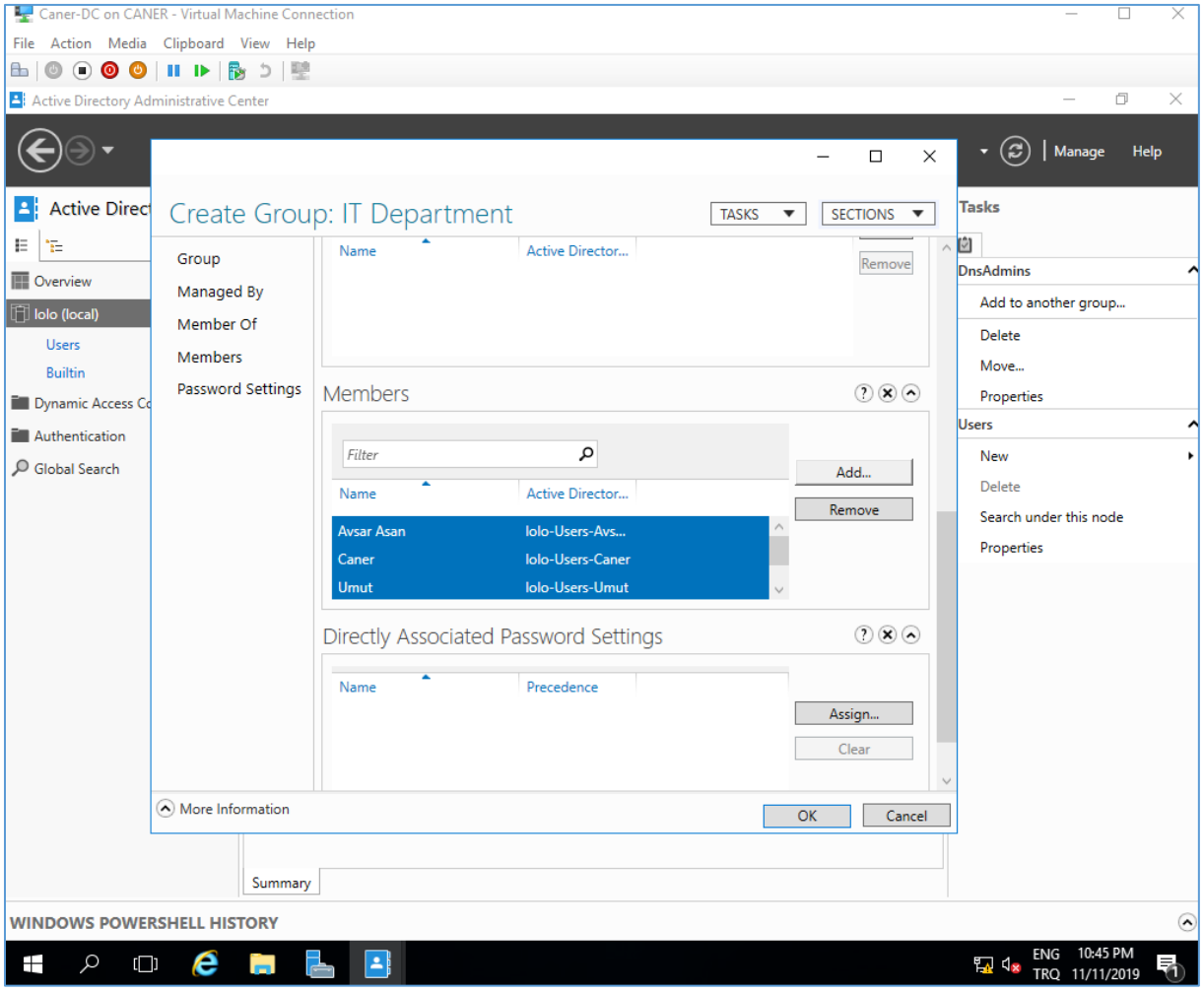
Similarly, to creating a User we enter relevant information and settings.



Then, under Members of our new Group, IT-Workers, we select Add our employees.

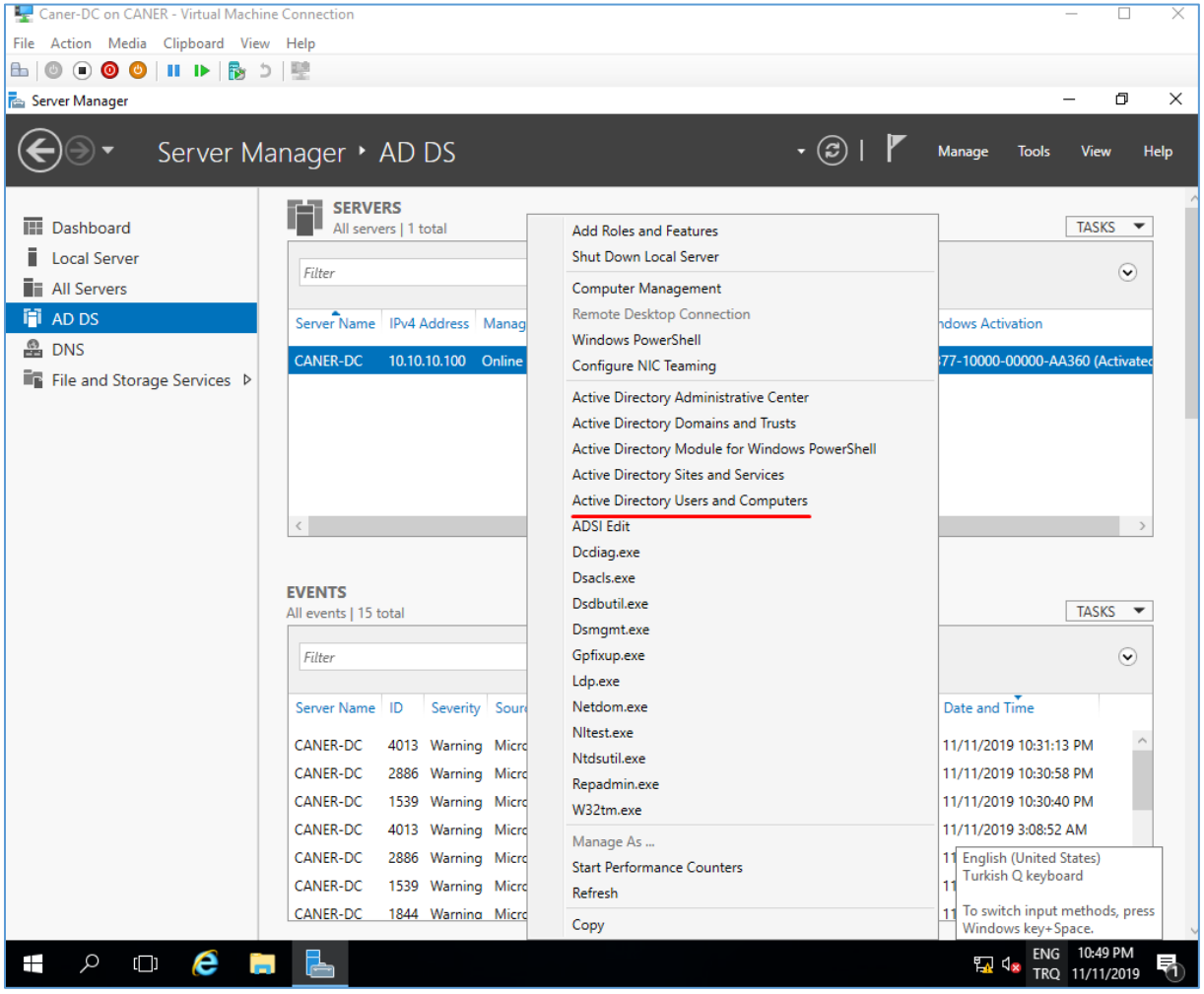


Our IT Crew is ready.

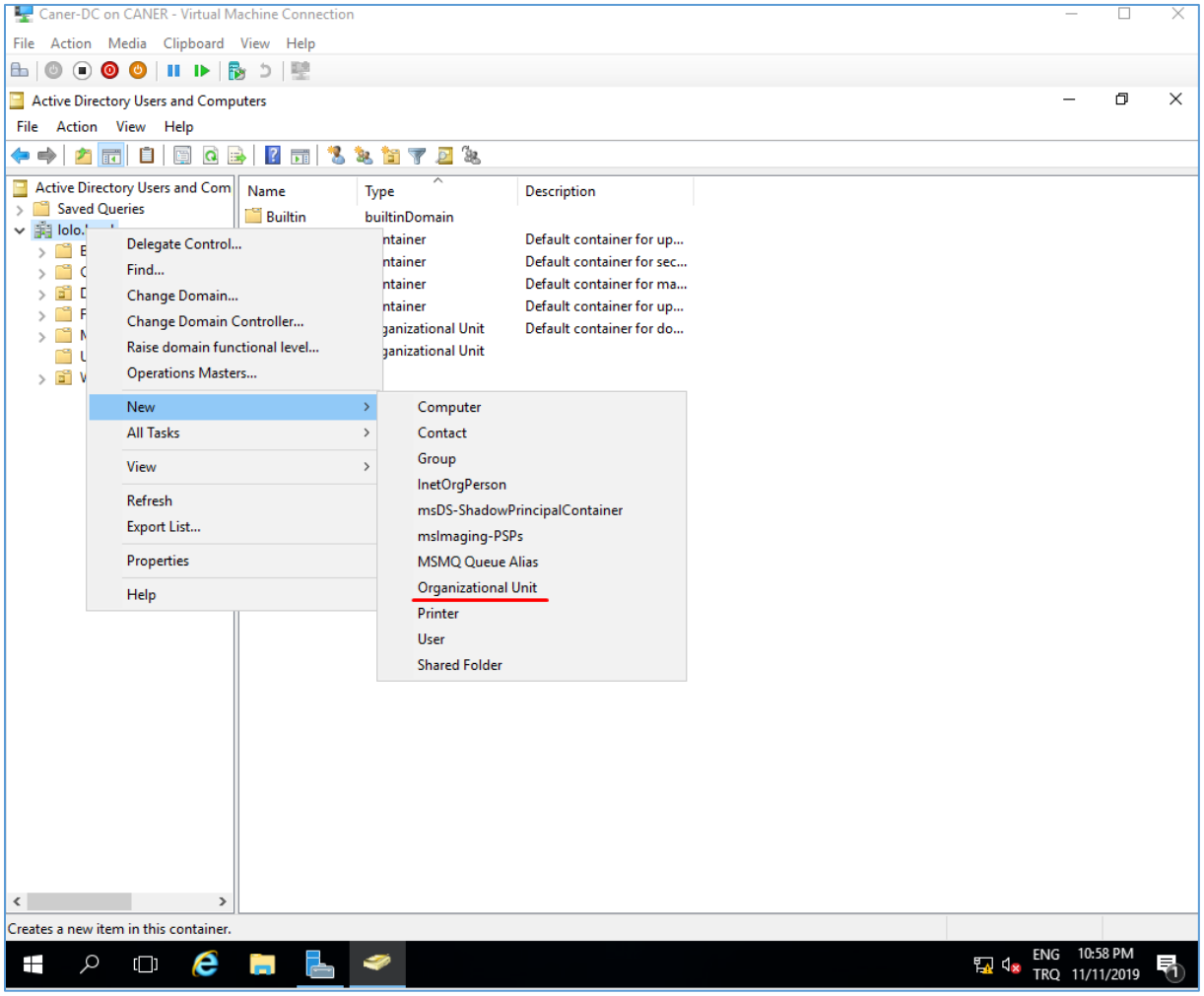


20.11.2019

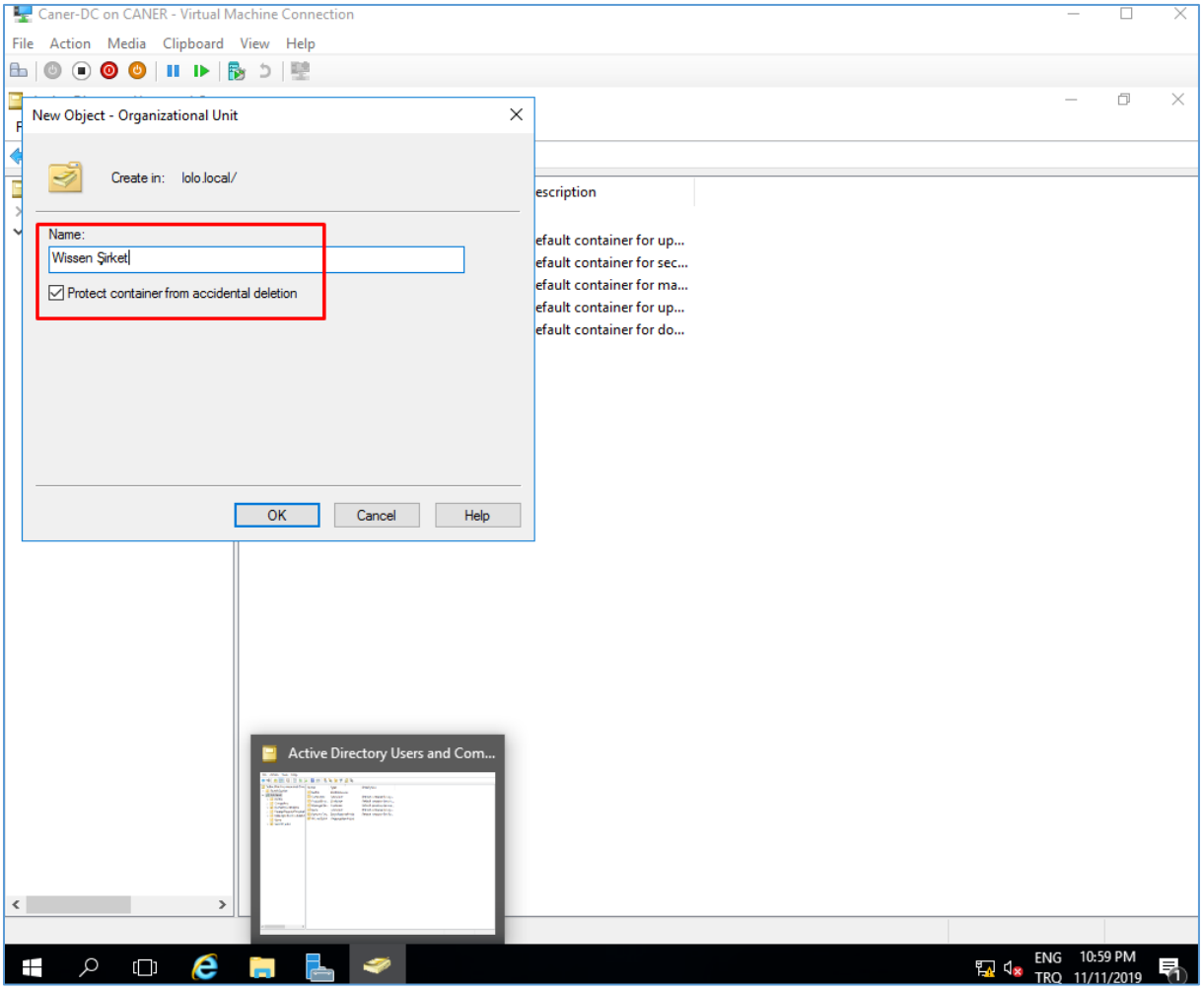
We proceed to Active Directory Users and Computers since we want to create an Organizational Unit.



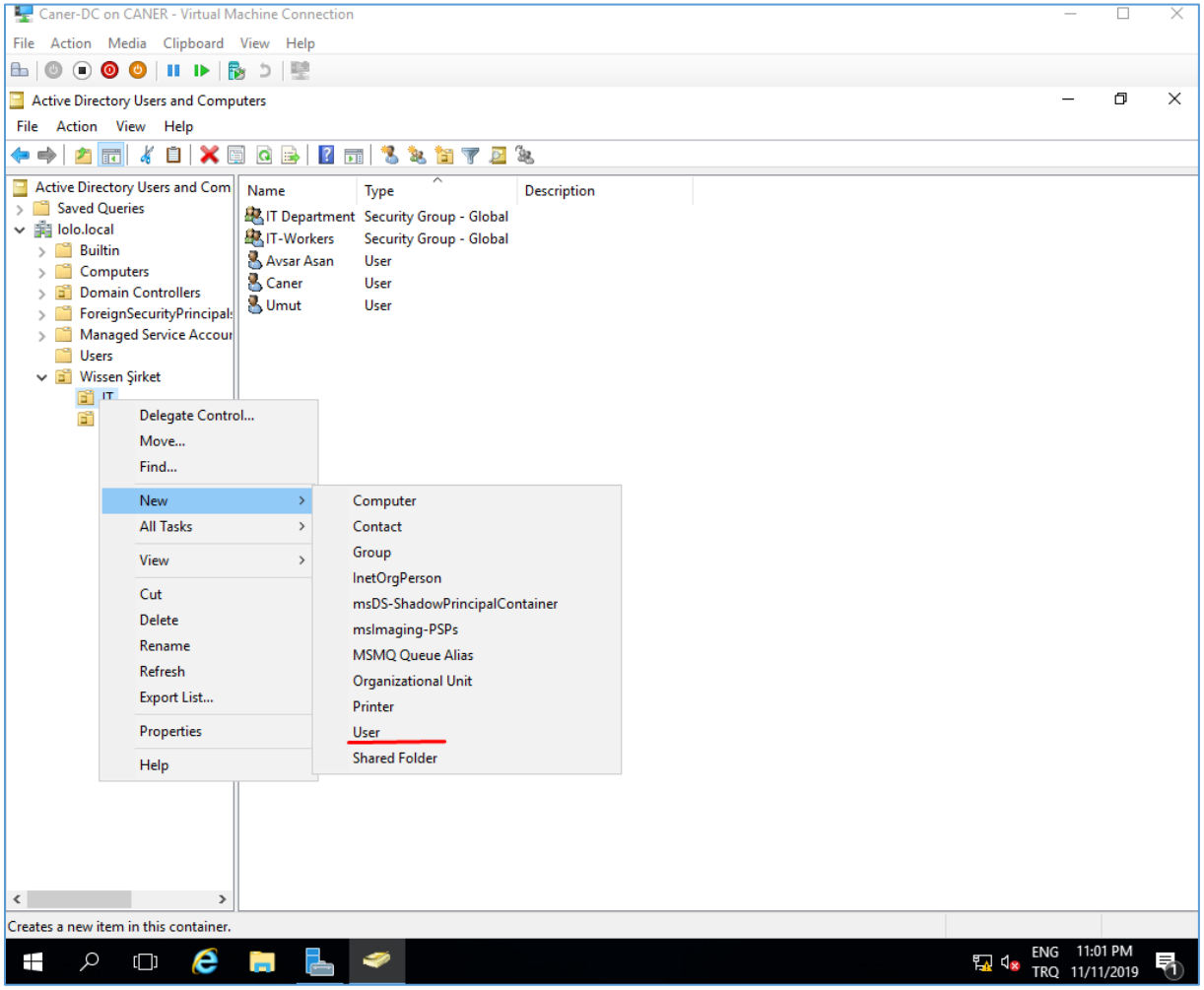
Under lolo.local domain we right click and select New -> Organizational Unit.



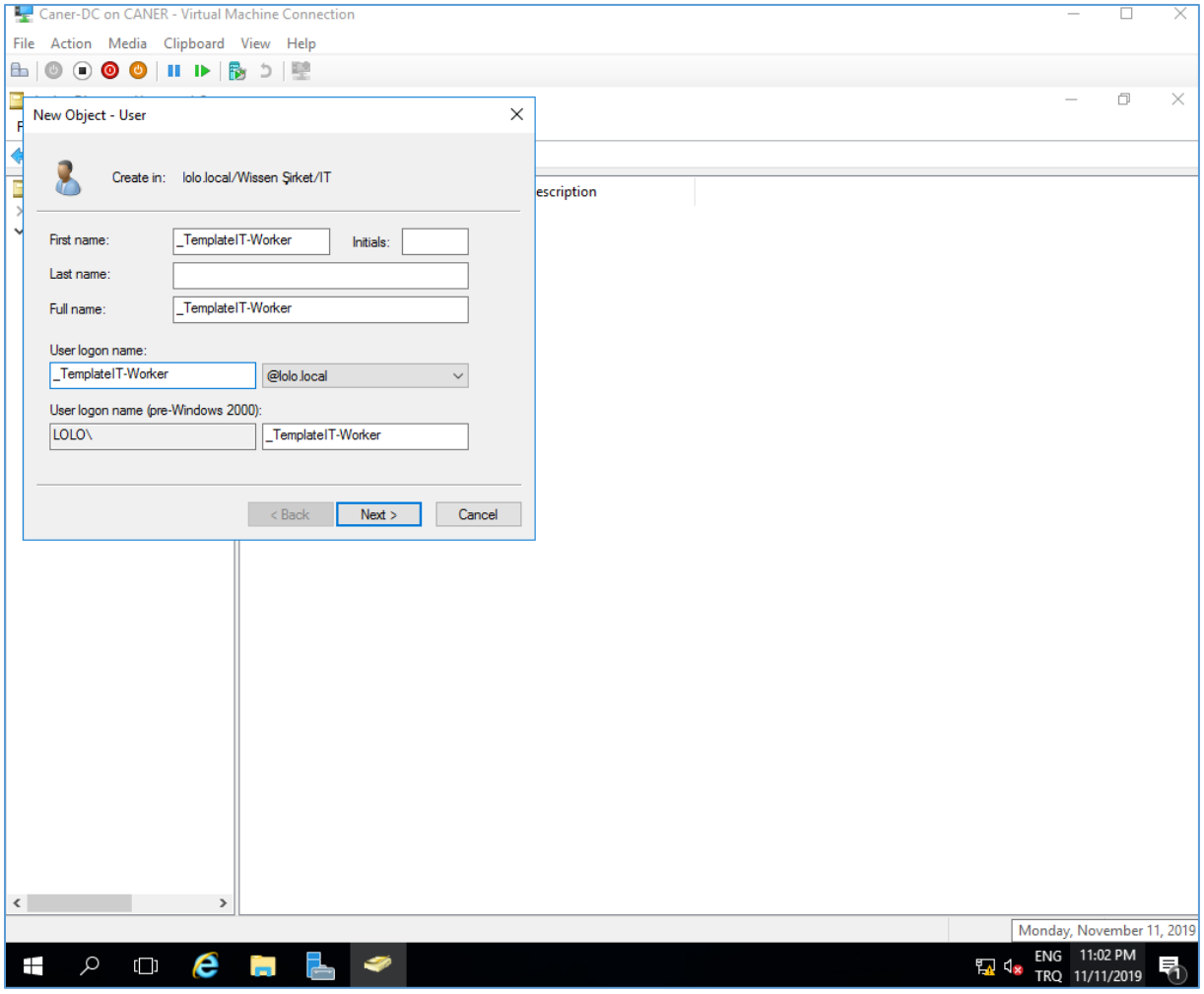
We name our Organizational Unit.



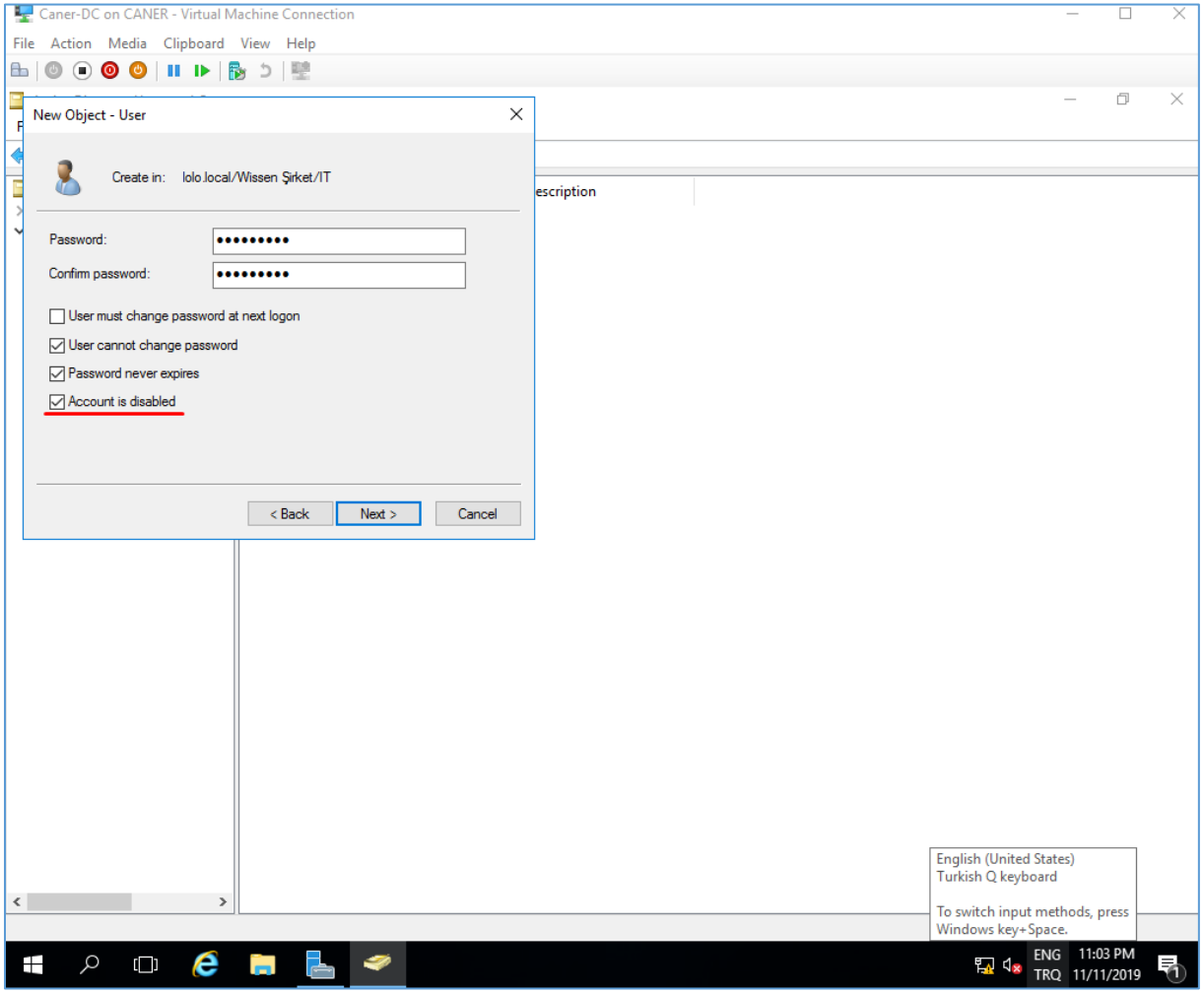
Now that we have Groups and Organizational Units, we want to create a template for our group. We get to create a new User.



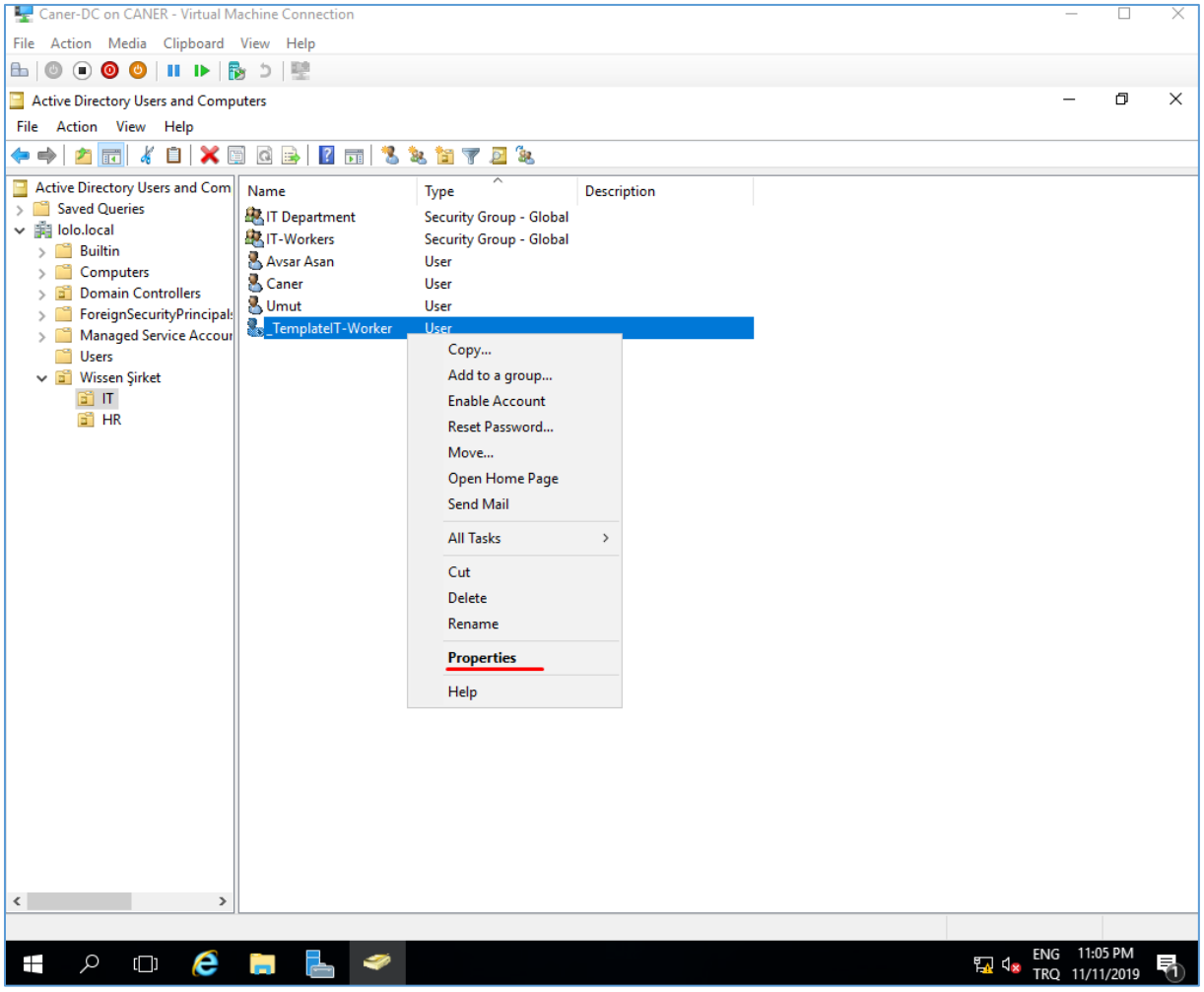
We name the template accordingly.



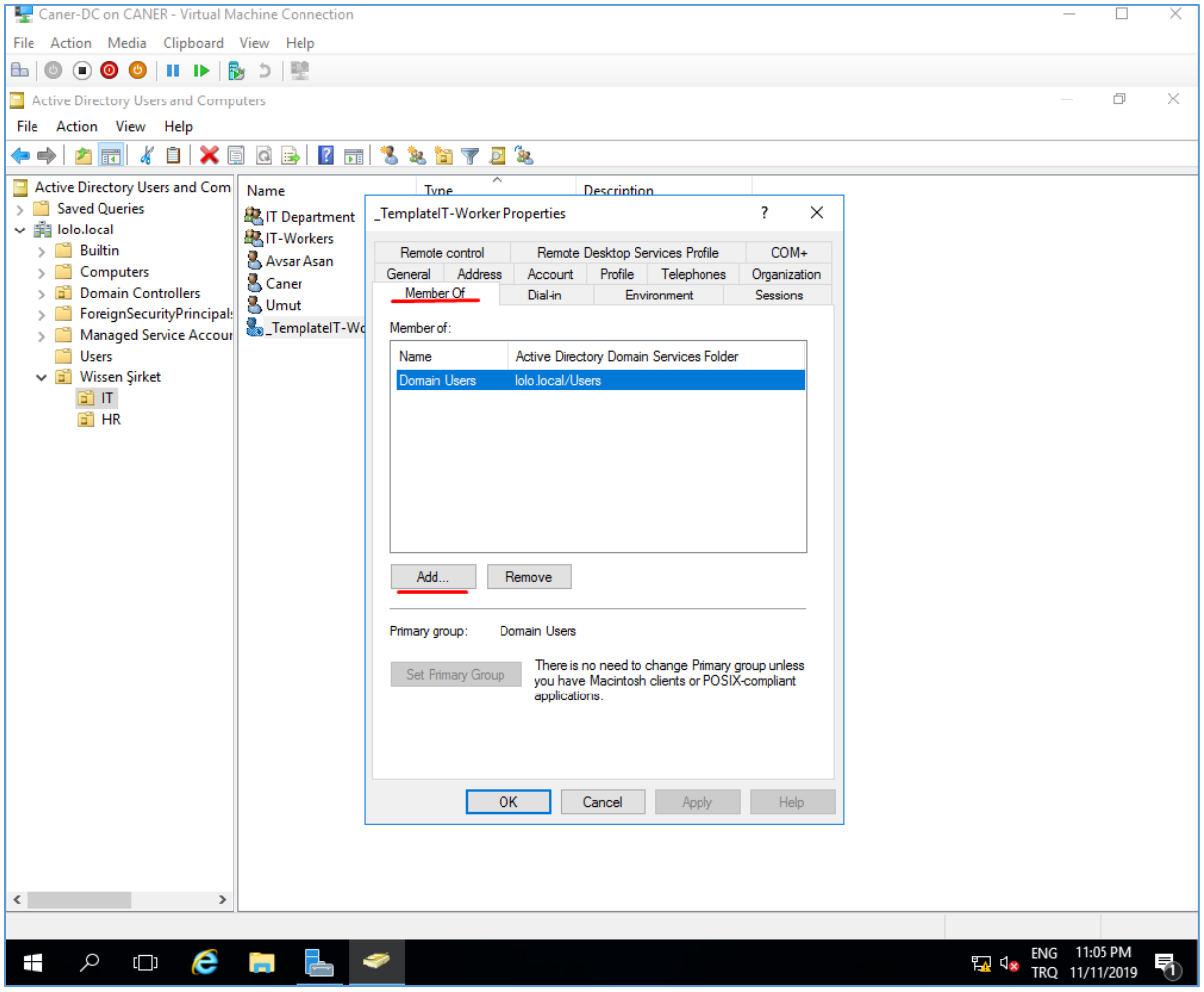
We assign the password and depending on your preference you can keep the account active or not. I prefer to make the templates inactive.



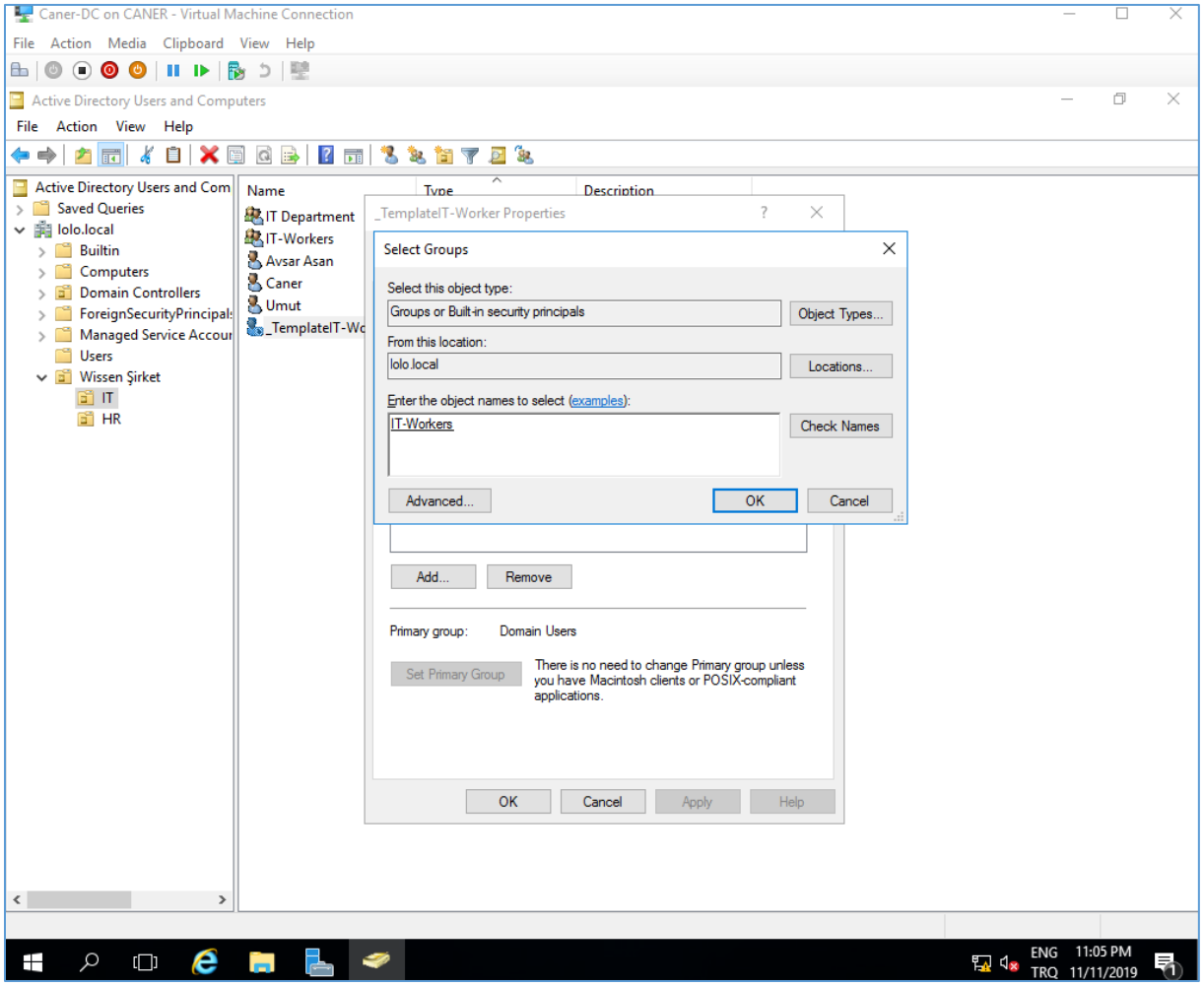
We then get to the properties of the Template.



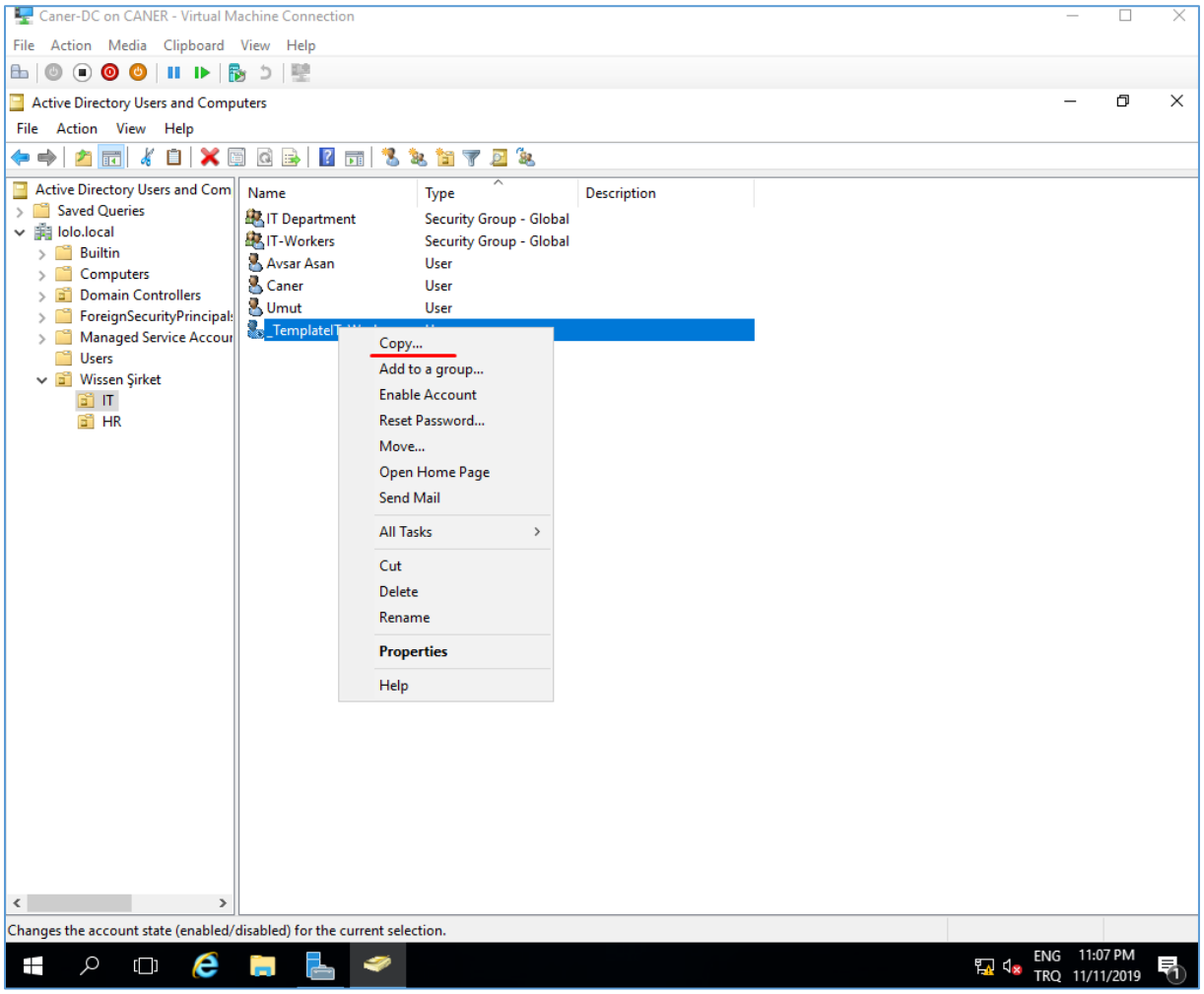
Under “Members Of” we select the Group that we are making this Template for.



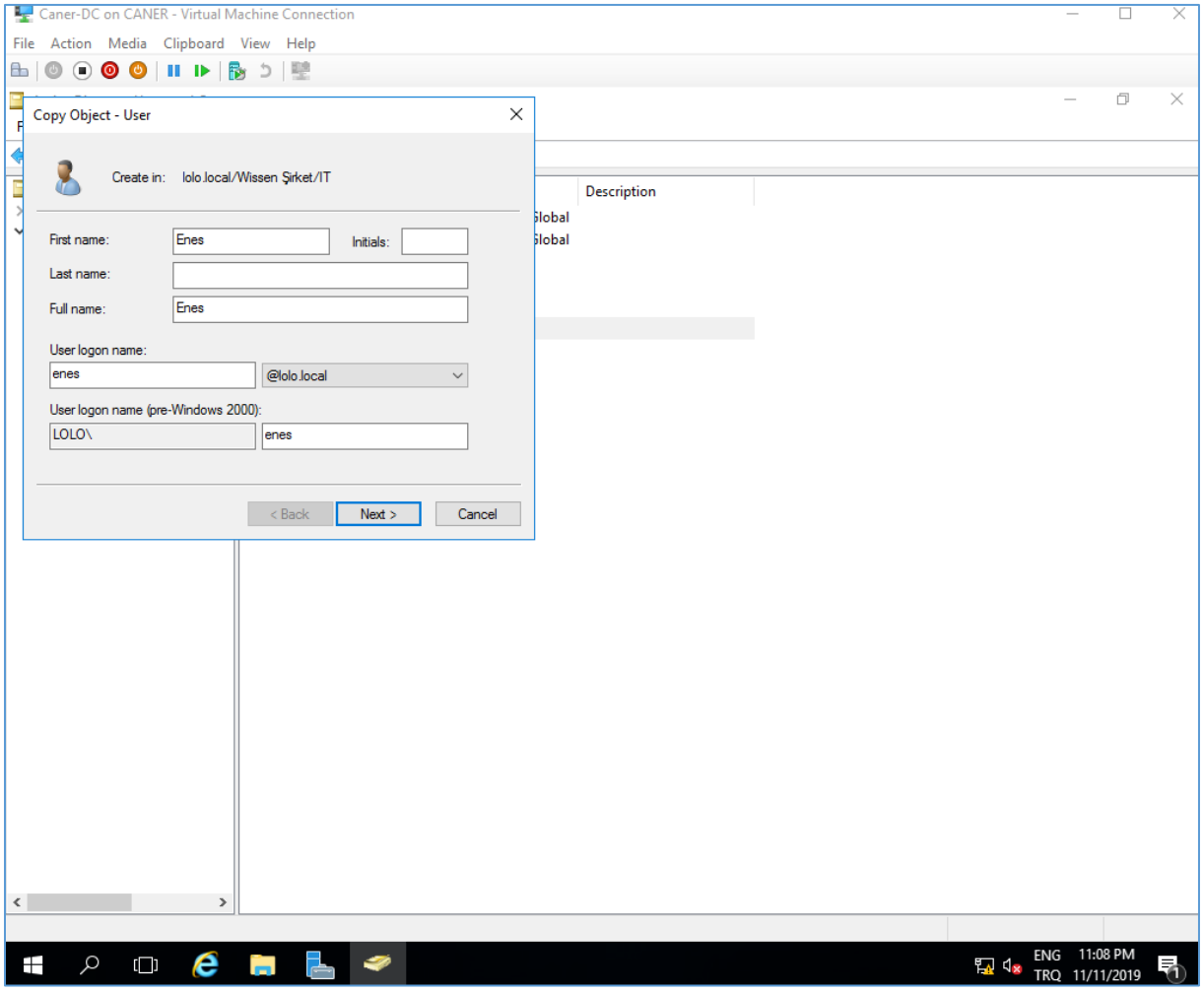
This specific Template is for new hires in IT Department.



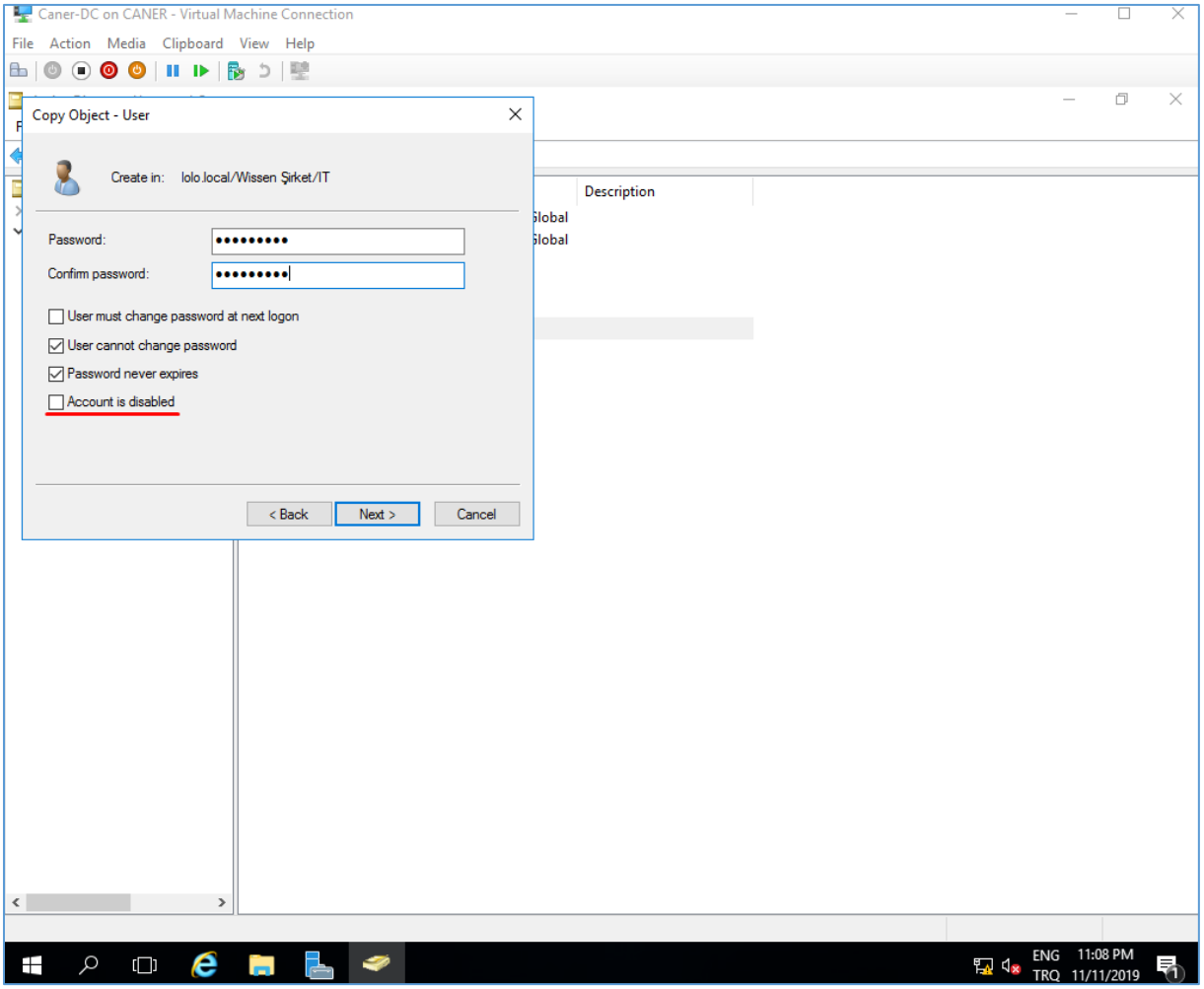
Now, let’s say we have a new employee at IT, to create a new account for them with all the correct rights to access and generic information for the IT department. We simply copy the Template.



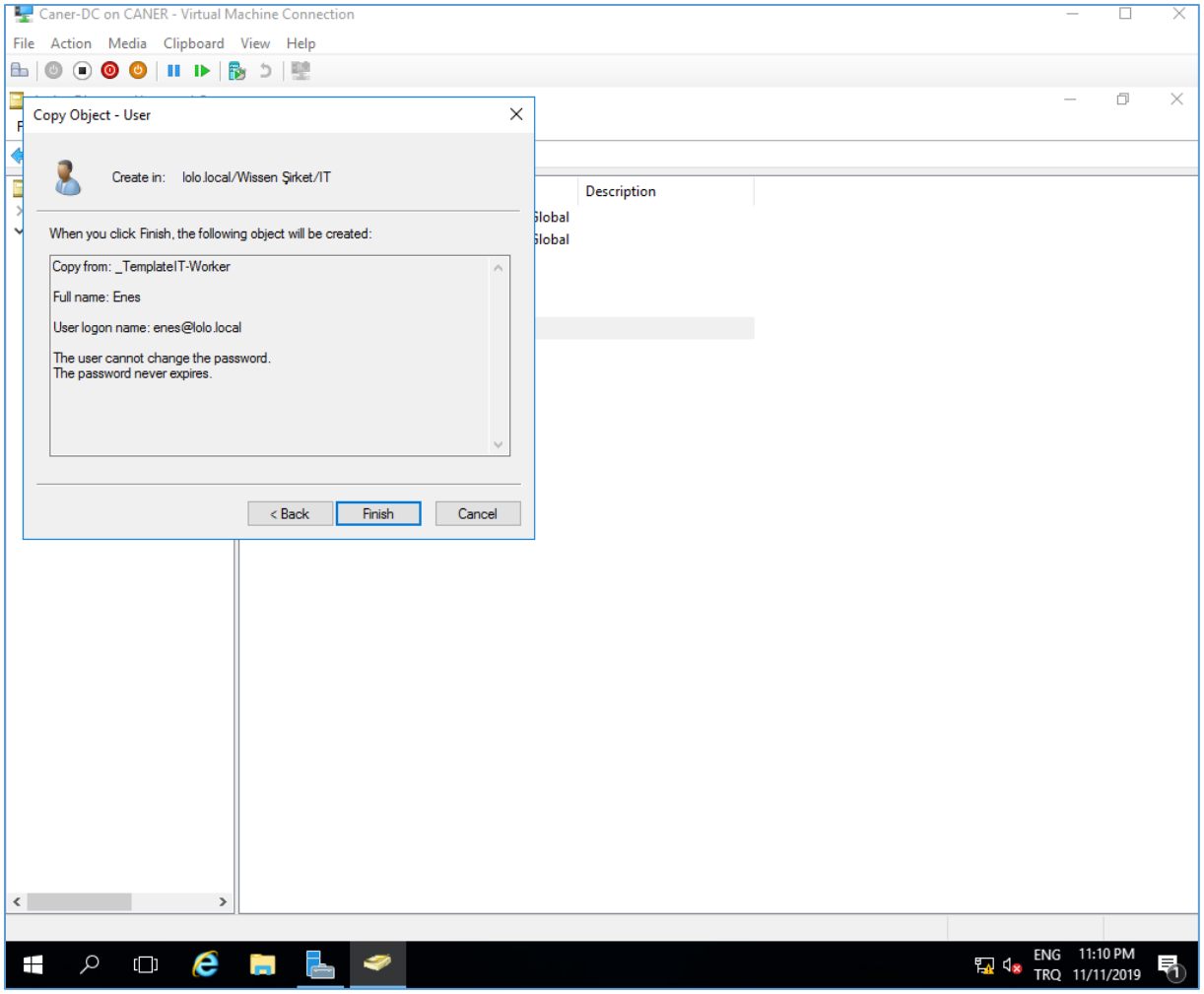
Change the name and log in information.



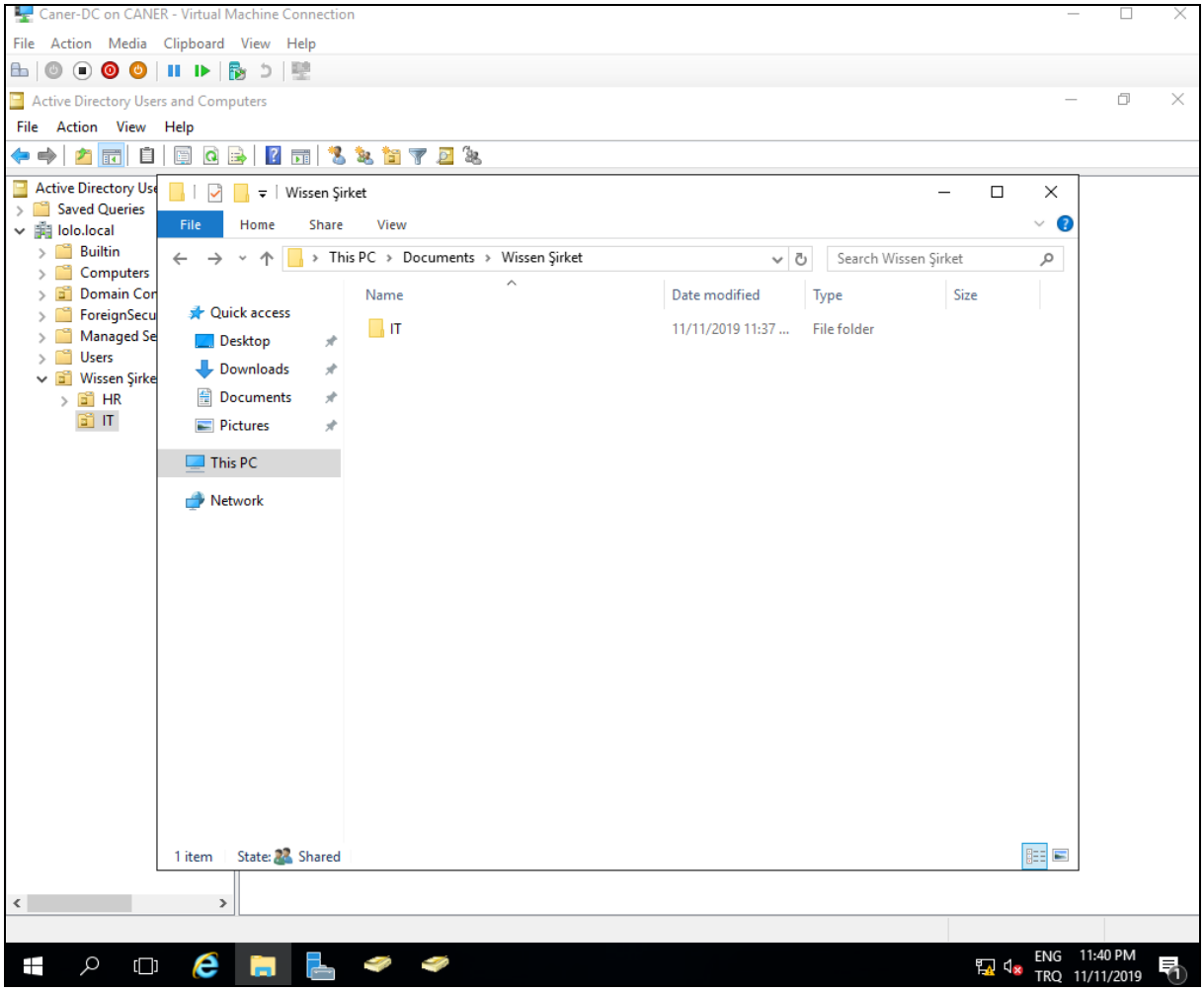
Enable the account since the Template itself is disabled.



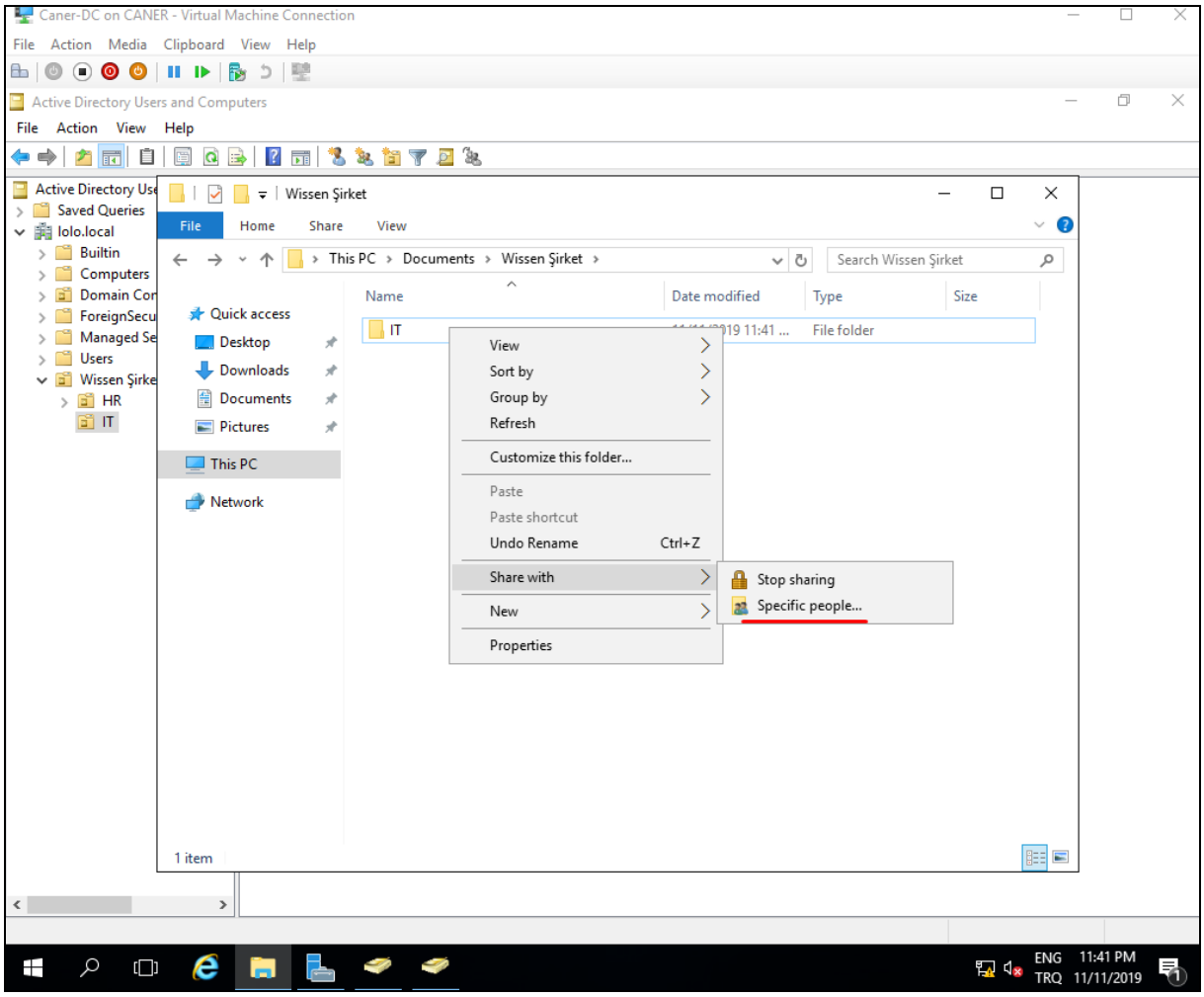
When we finish the process and we have the account for the new employee Enes ready to go.



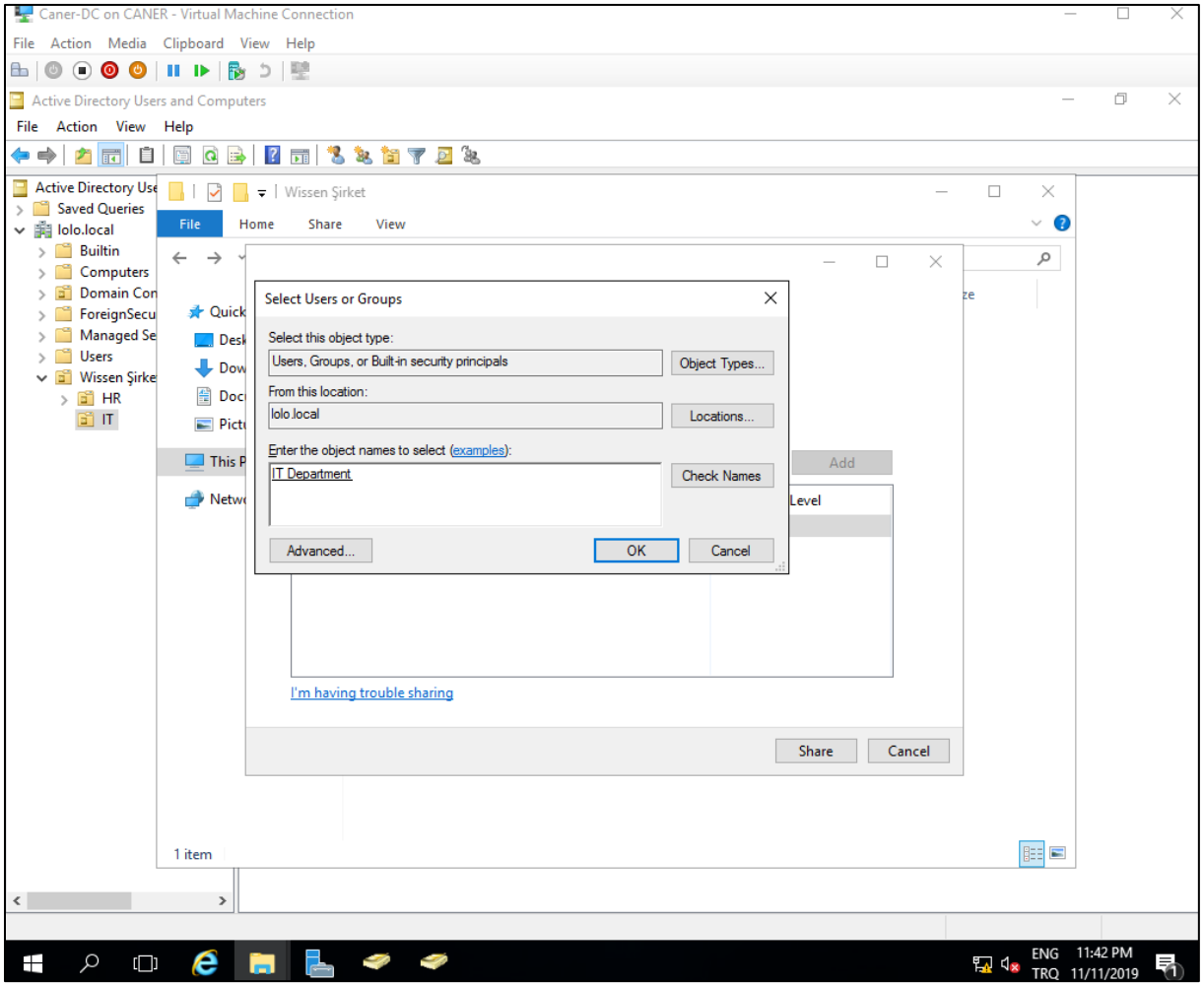
Now let’s investigate how Shared Folders and access rights work. Firstly, let’s create a folder only the IT department should access.



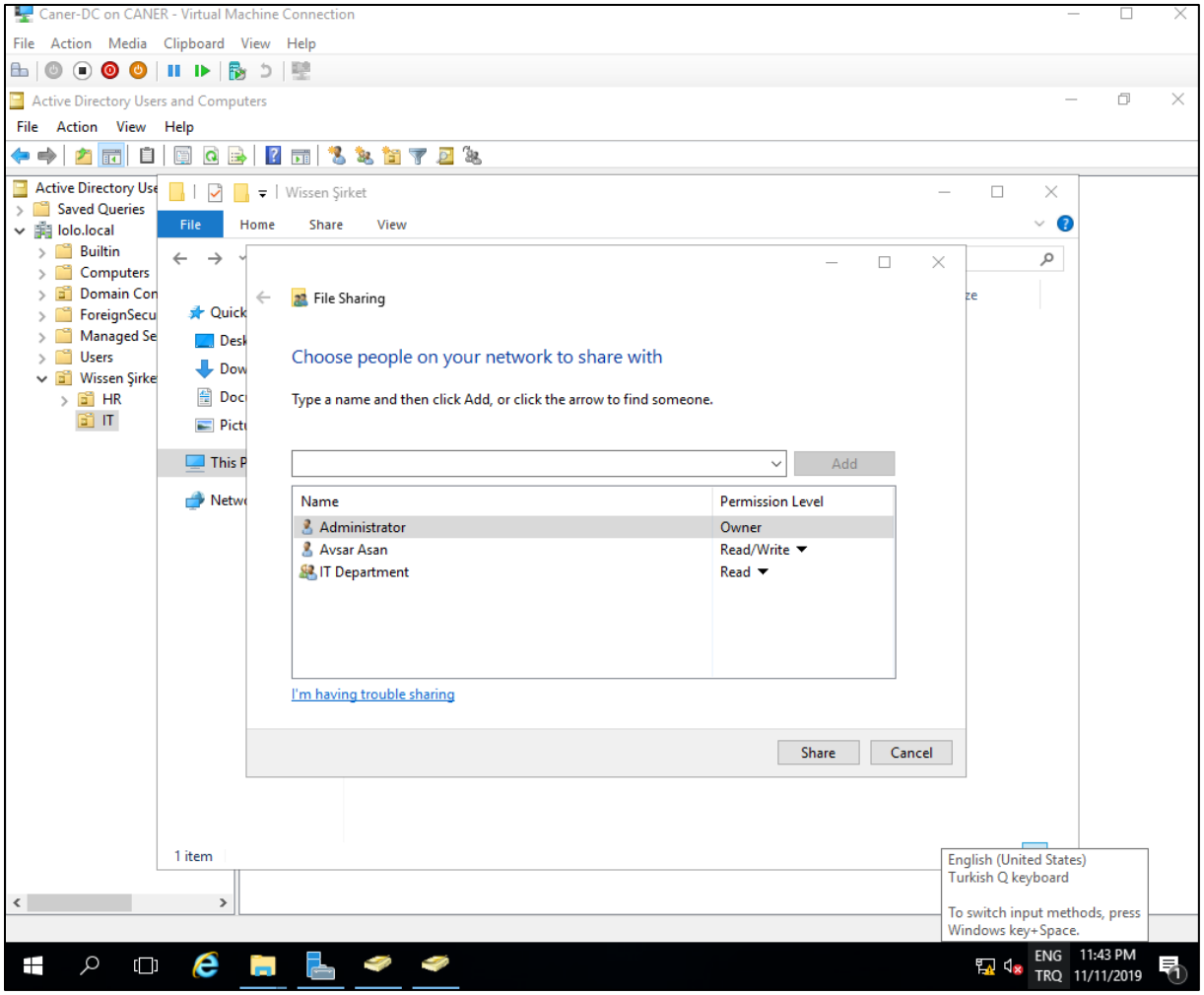
We share the folder with specific people.



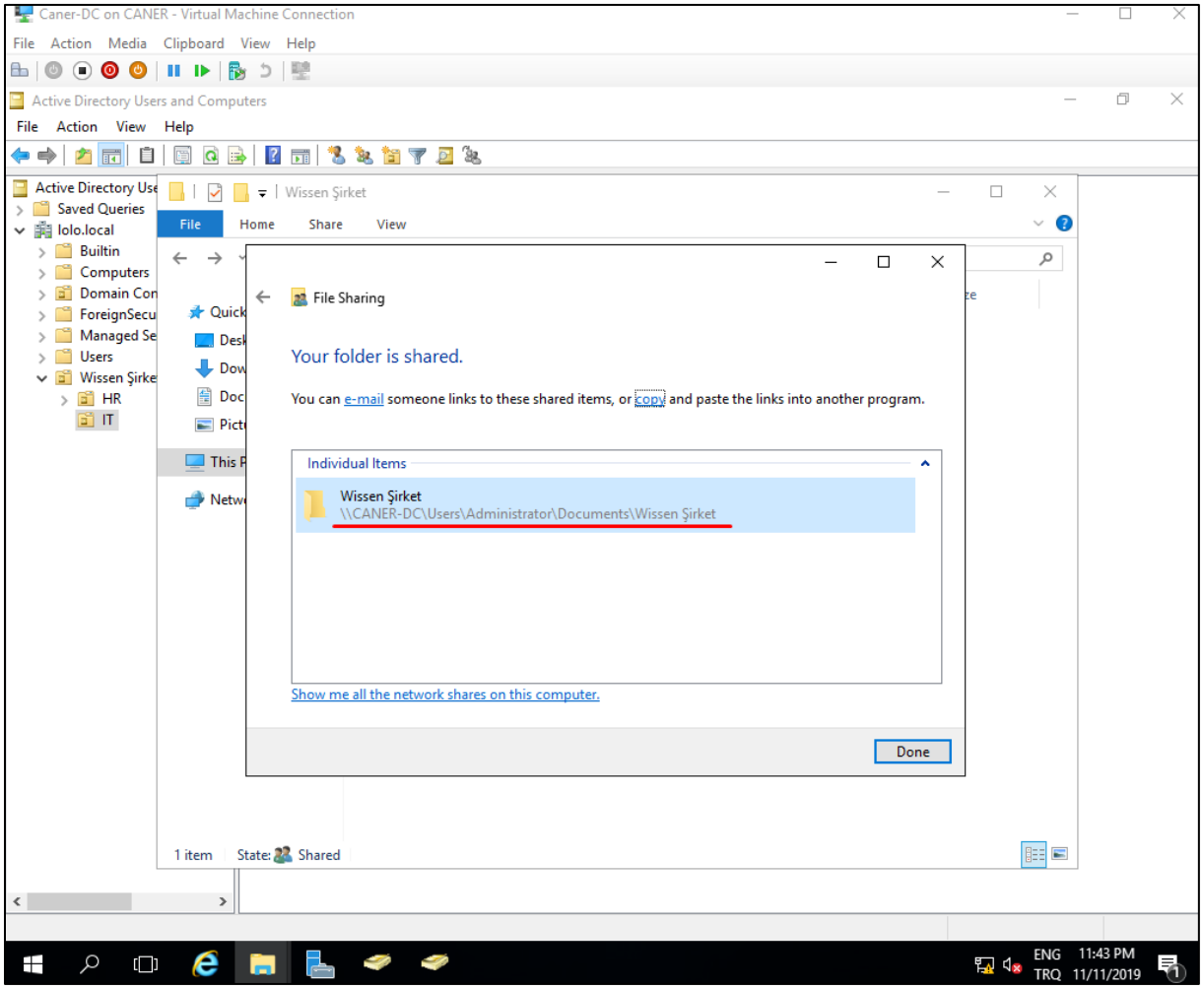
We choose only the IT department to see the document.



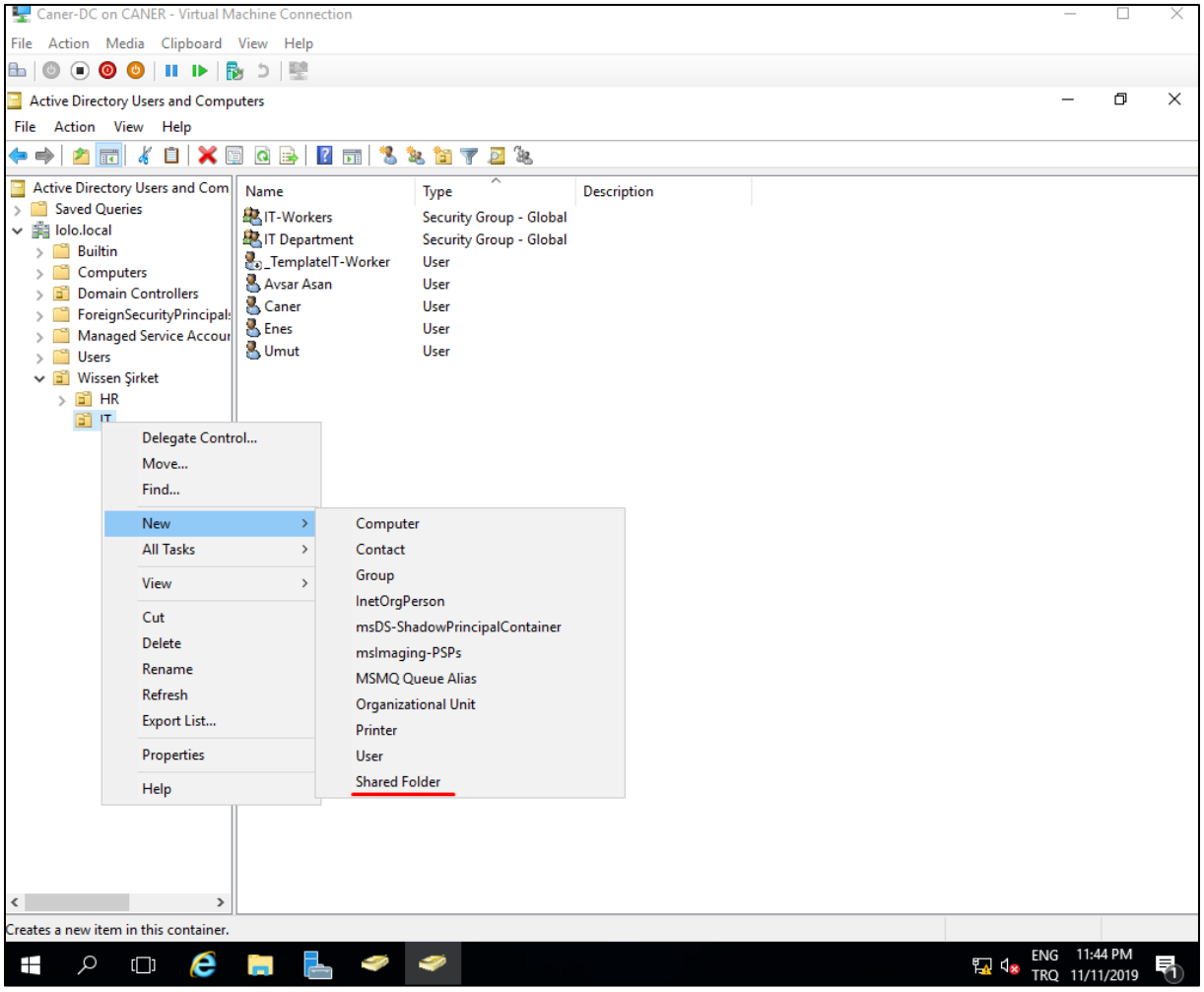
Then, we assign rights to the folder here as well on who can write and only read the files.



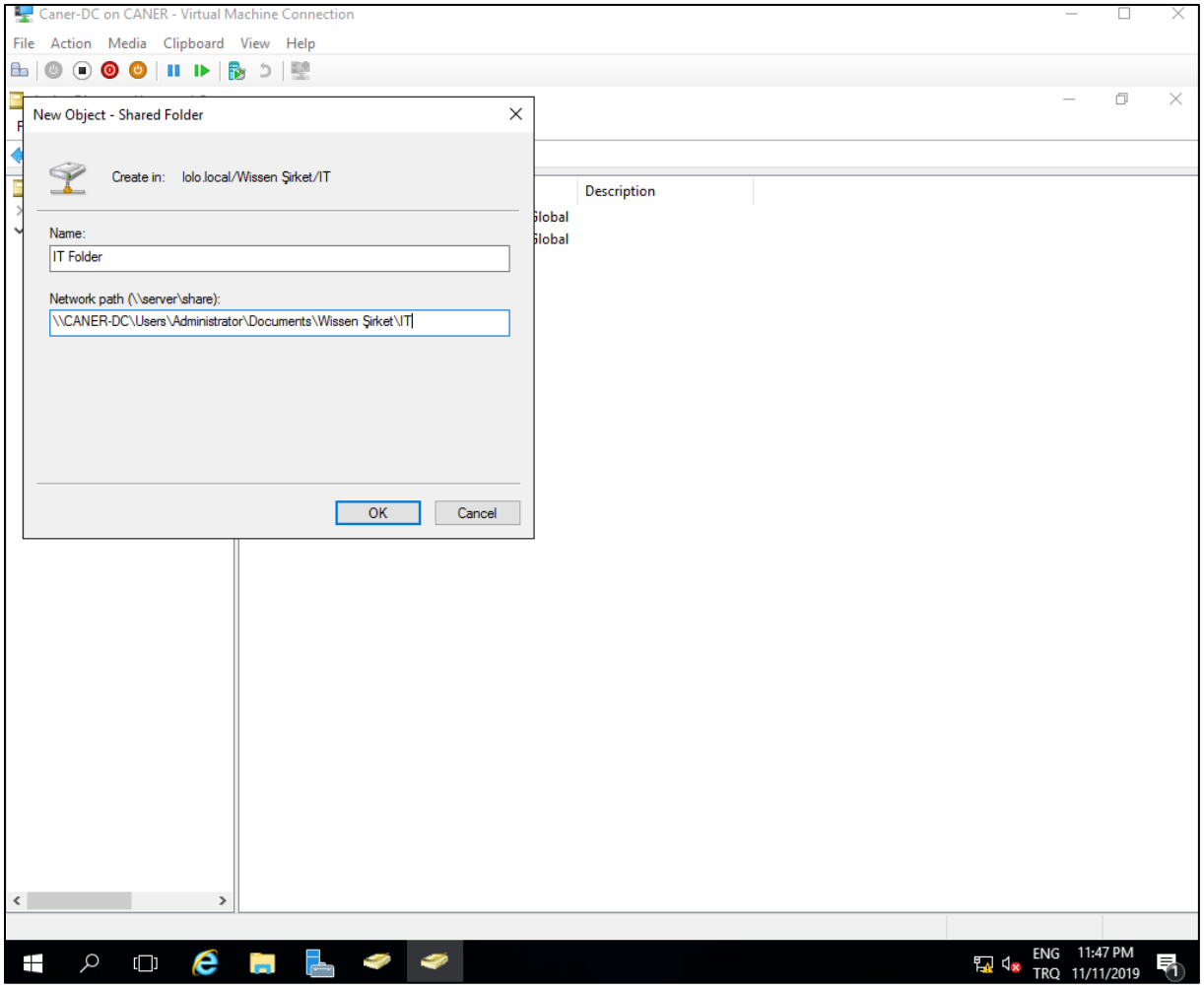
We start the sharing process and keep note on the path in case we need it later.



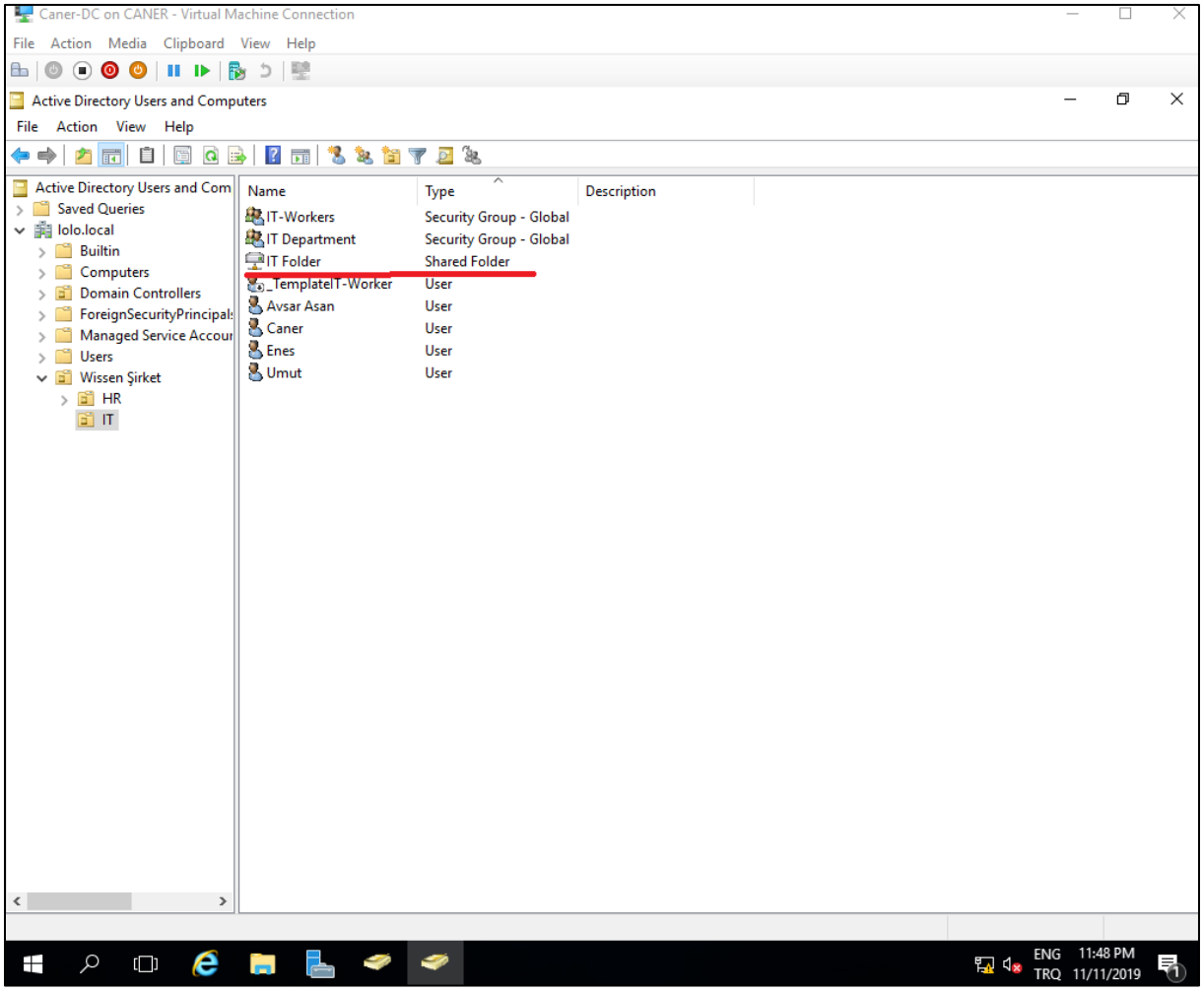
We create a shared folder in the Organizational Unit of IT Department as well.



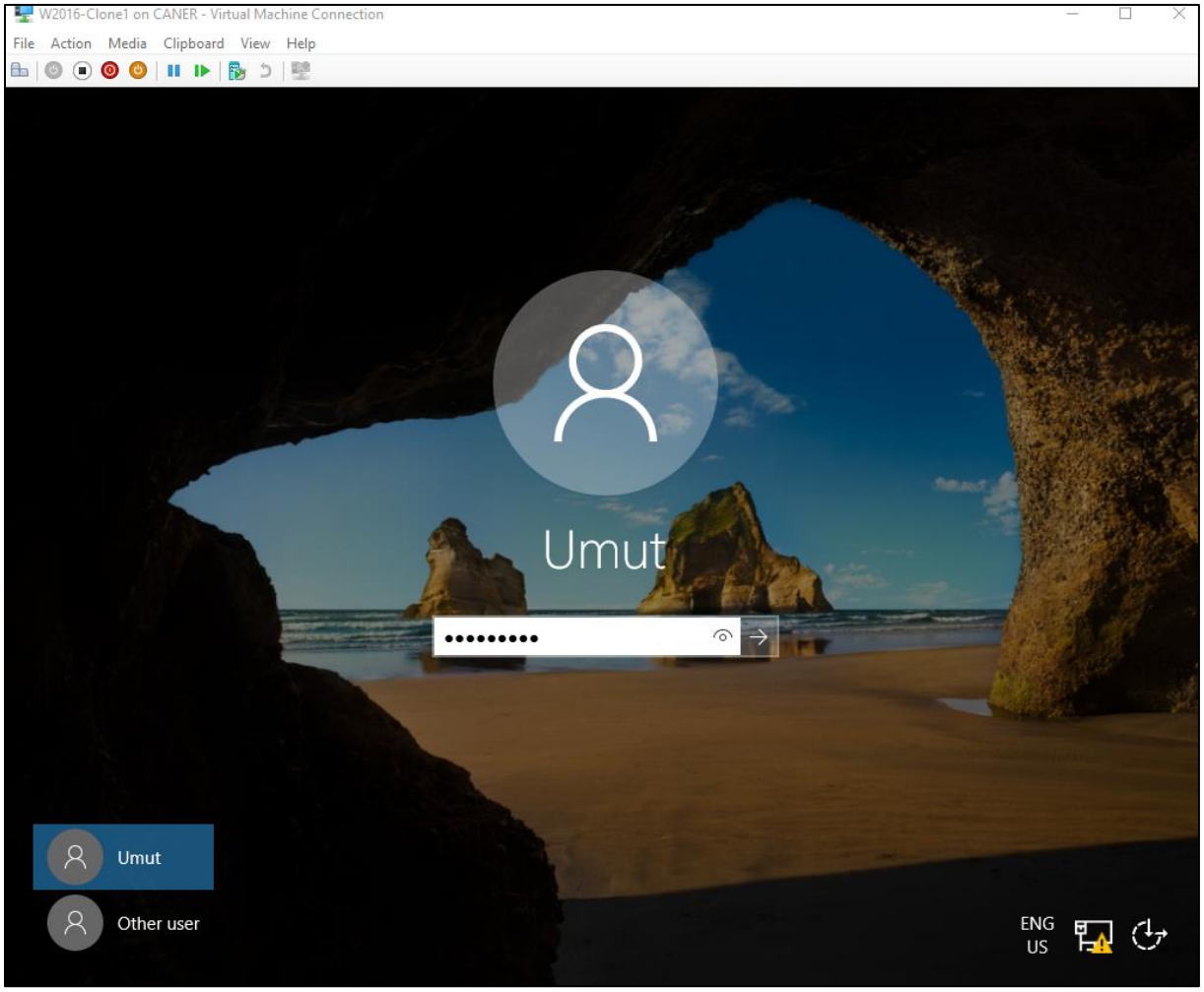
And use the path from the previously shared folder.



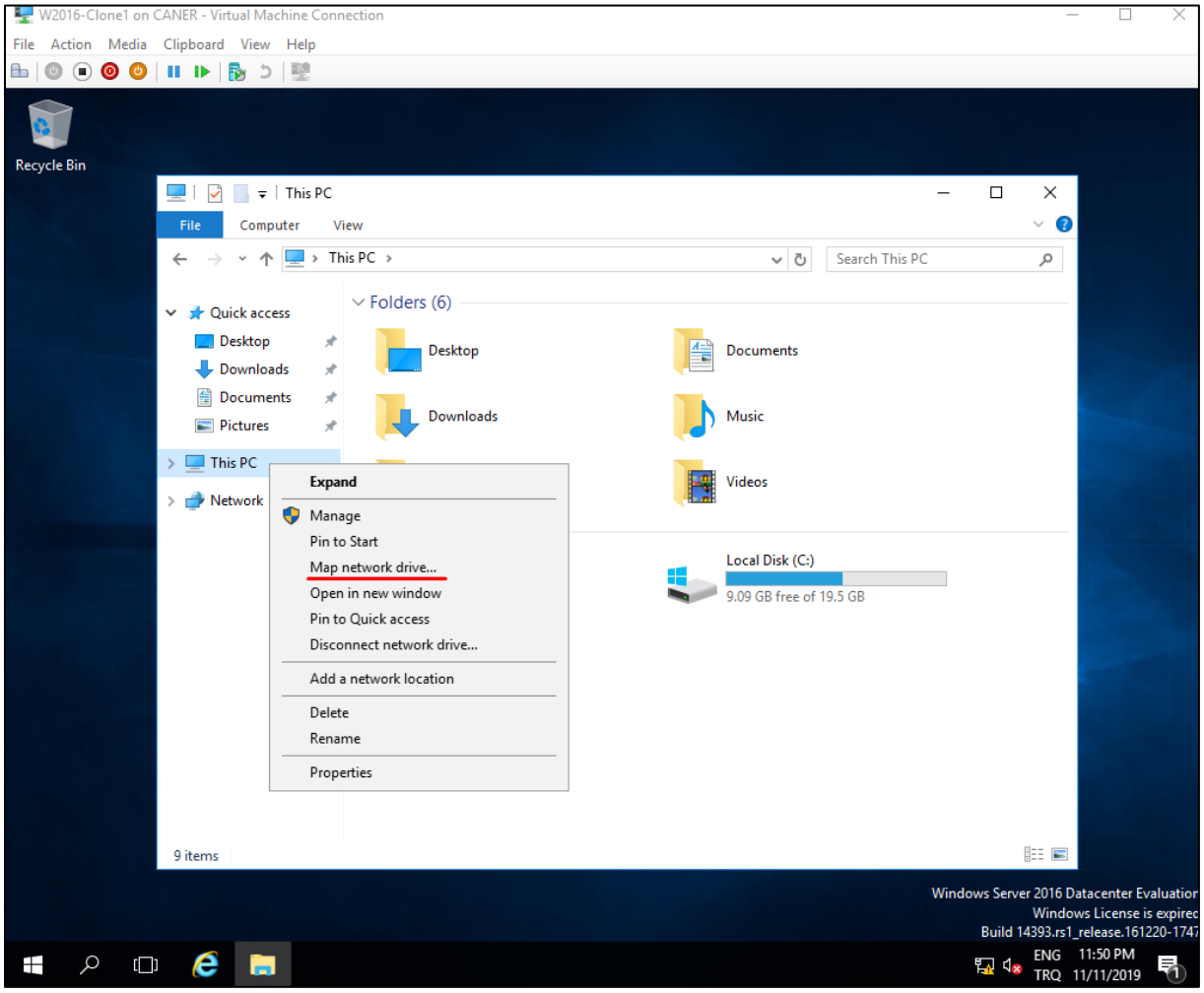
Our folder is ready.



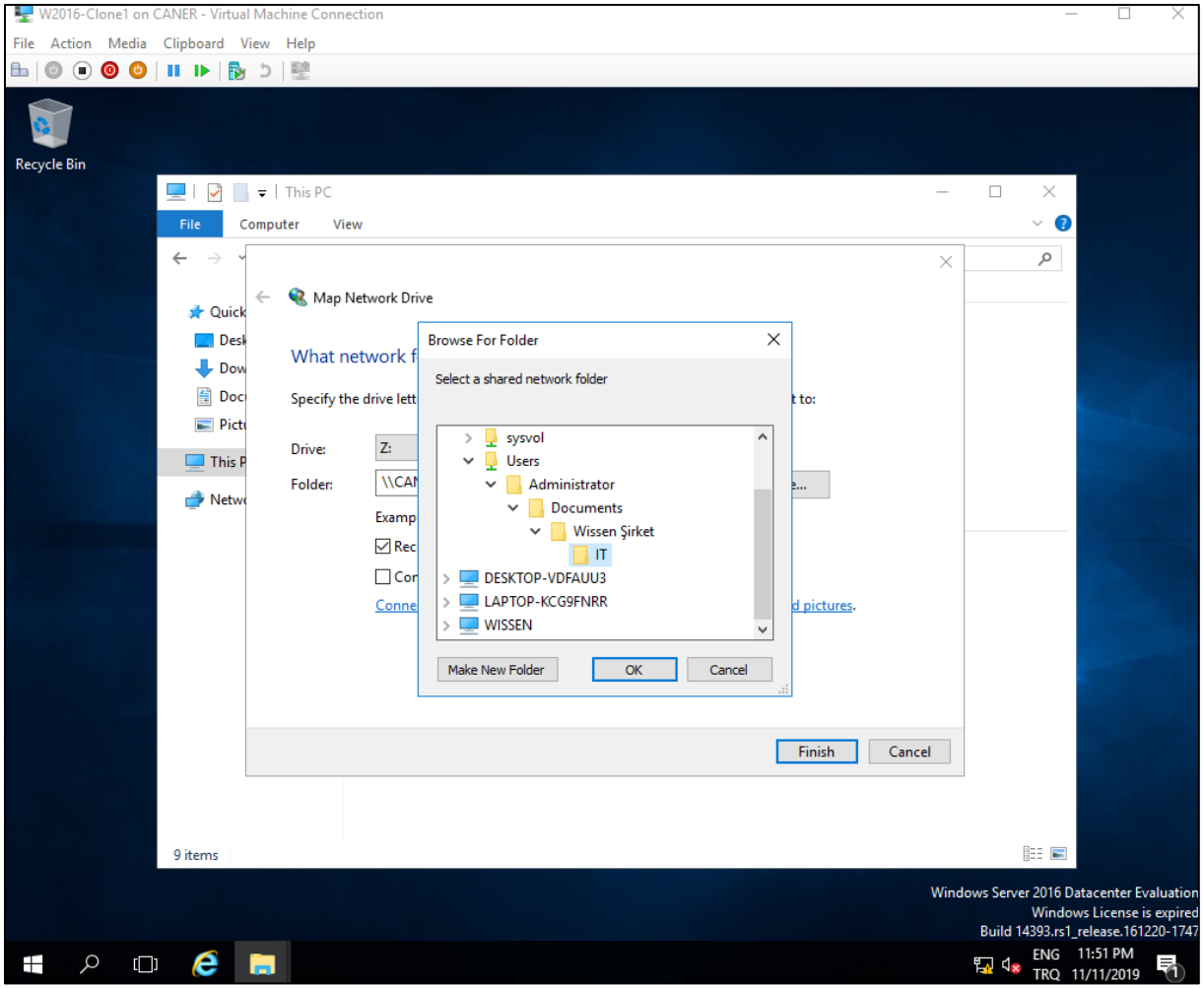
Now, let’s test our sharing process. We login as Umut who is the team leader in IT.



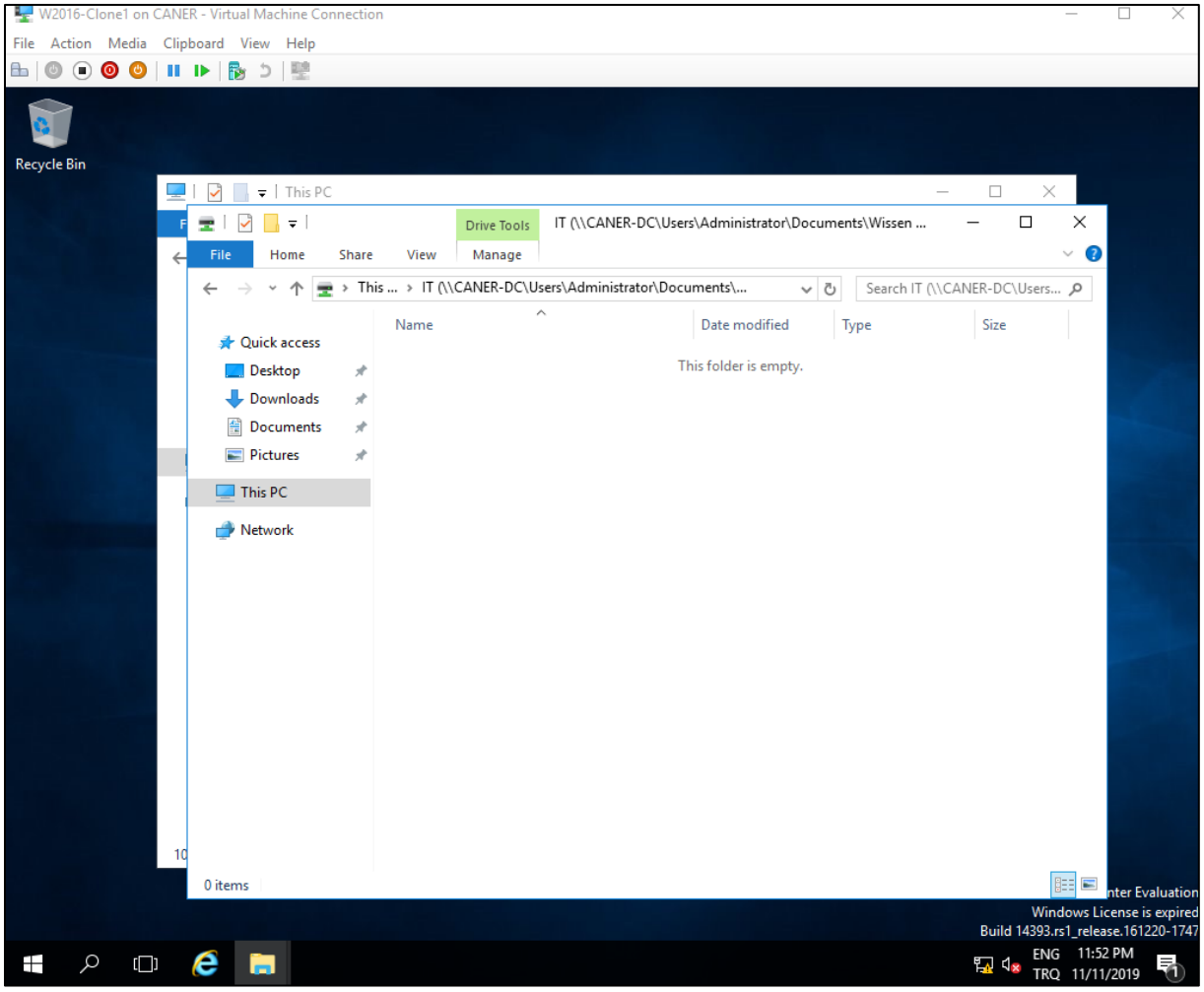
We do the usual Map Drive Network process which you can learn more about from the second report which is on Windows 2016 Storage.



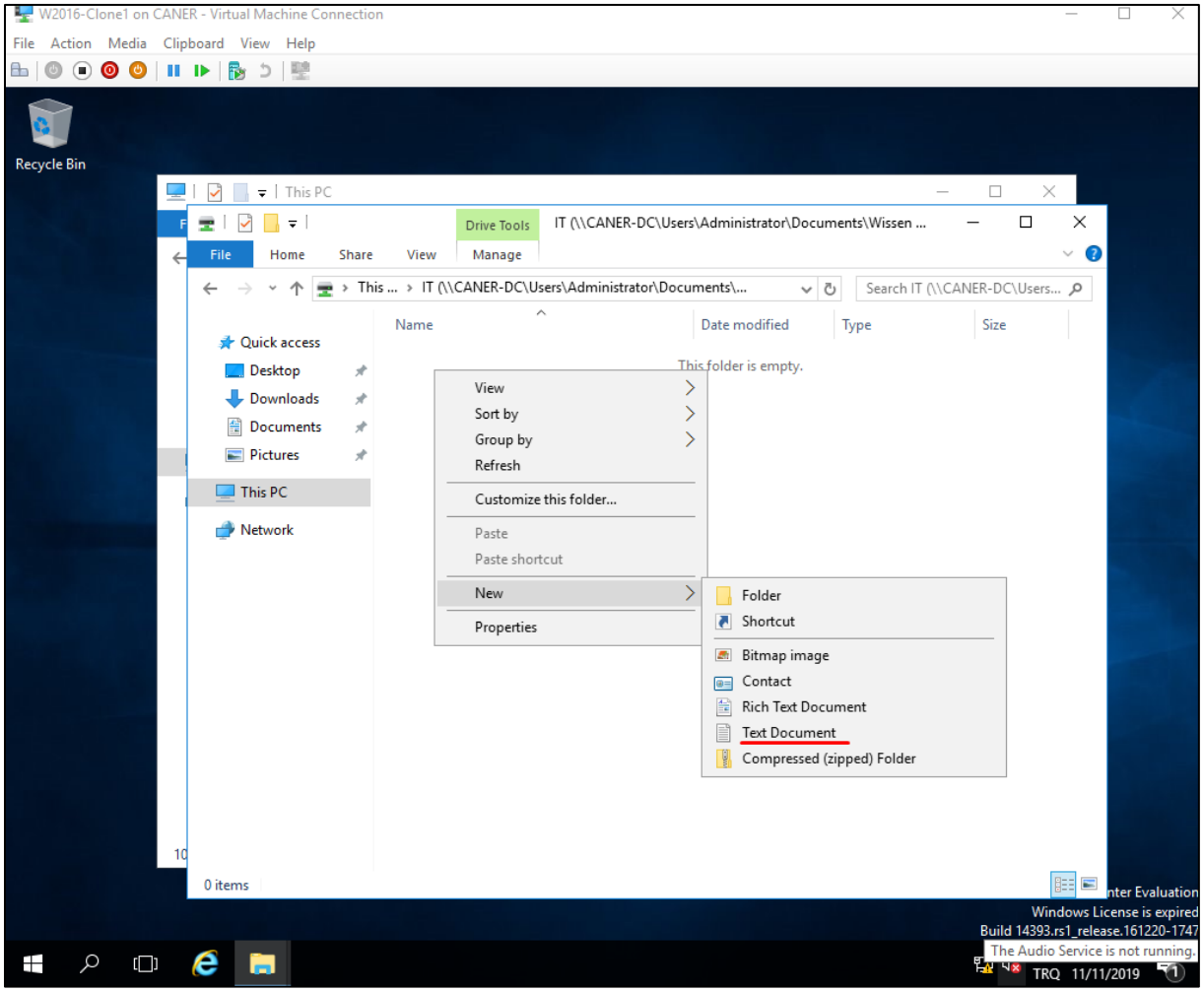
We can easily see the folder we created after following the path.



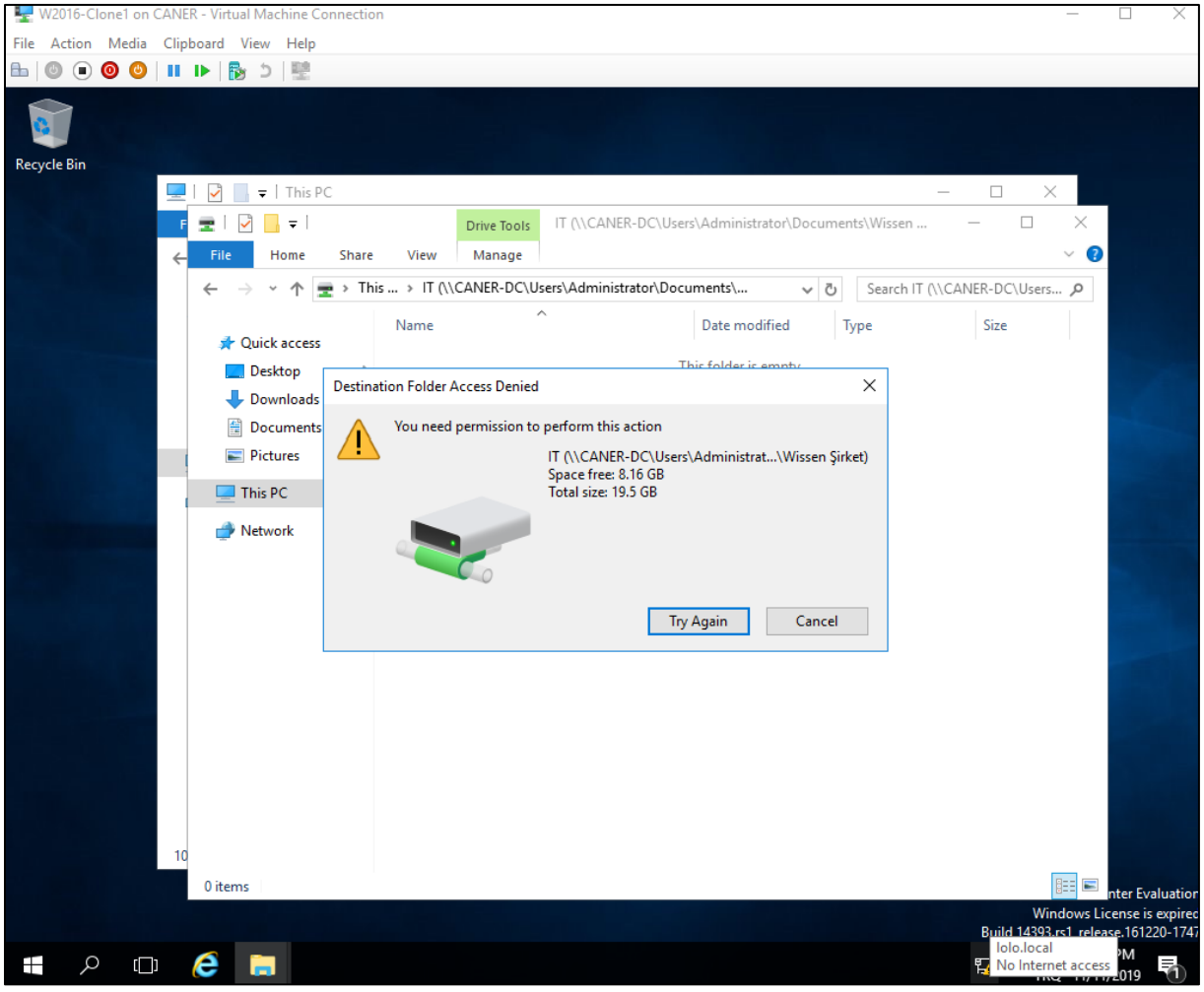
Folder is accessed.



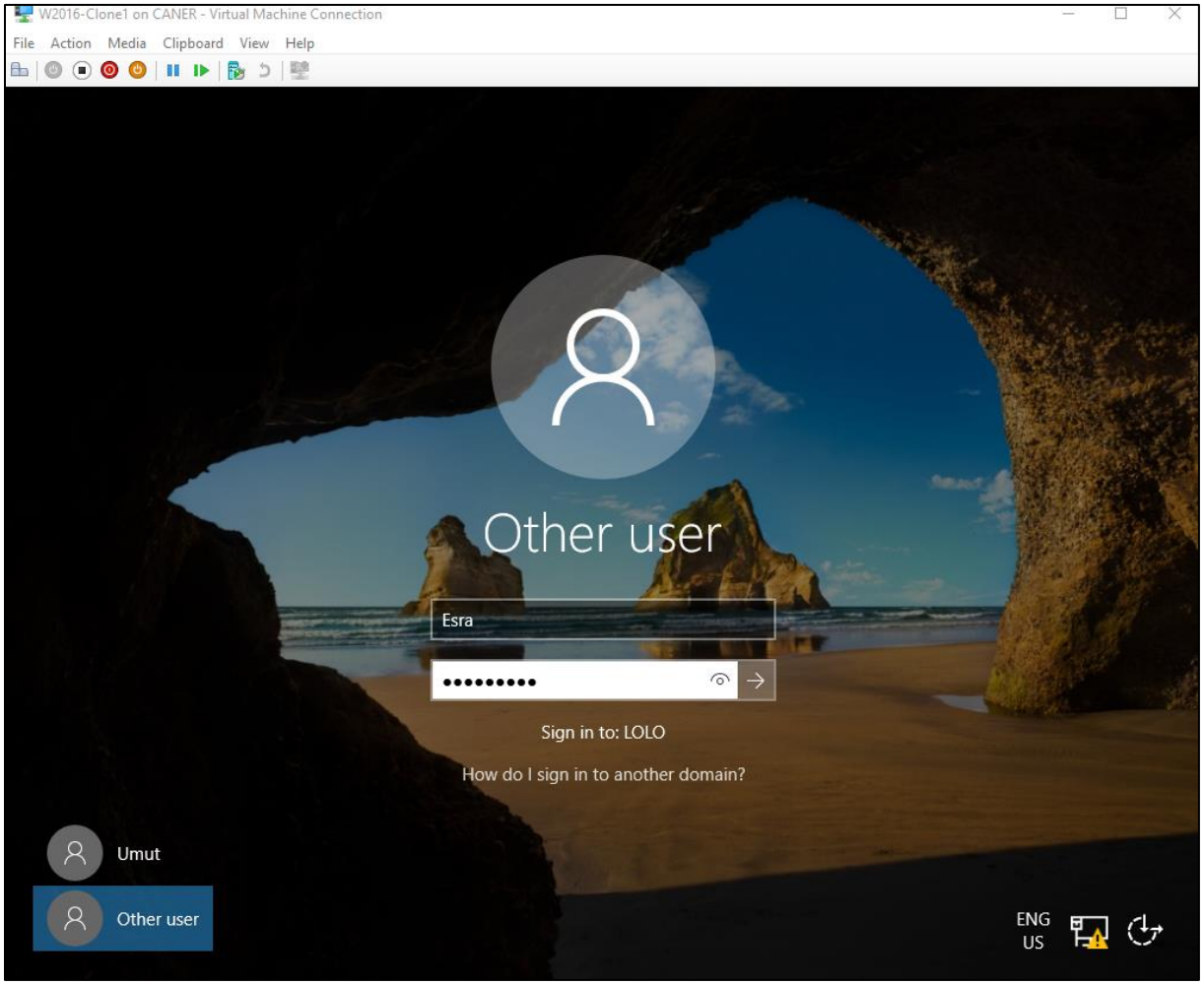
When Umut tries to create a new file on the folder,...



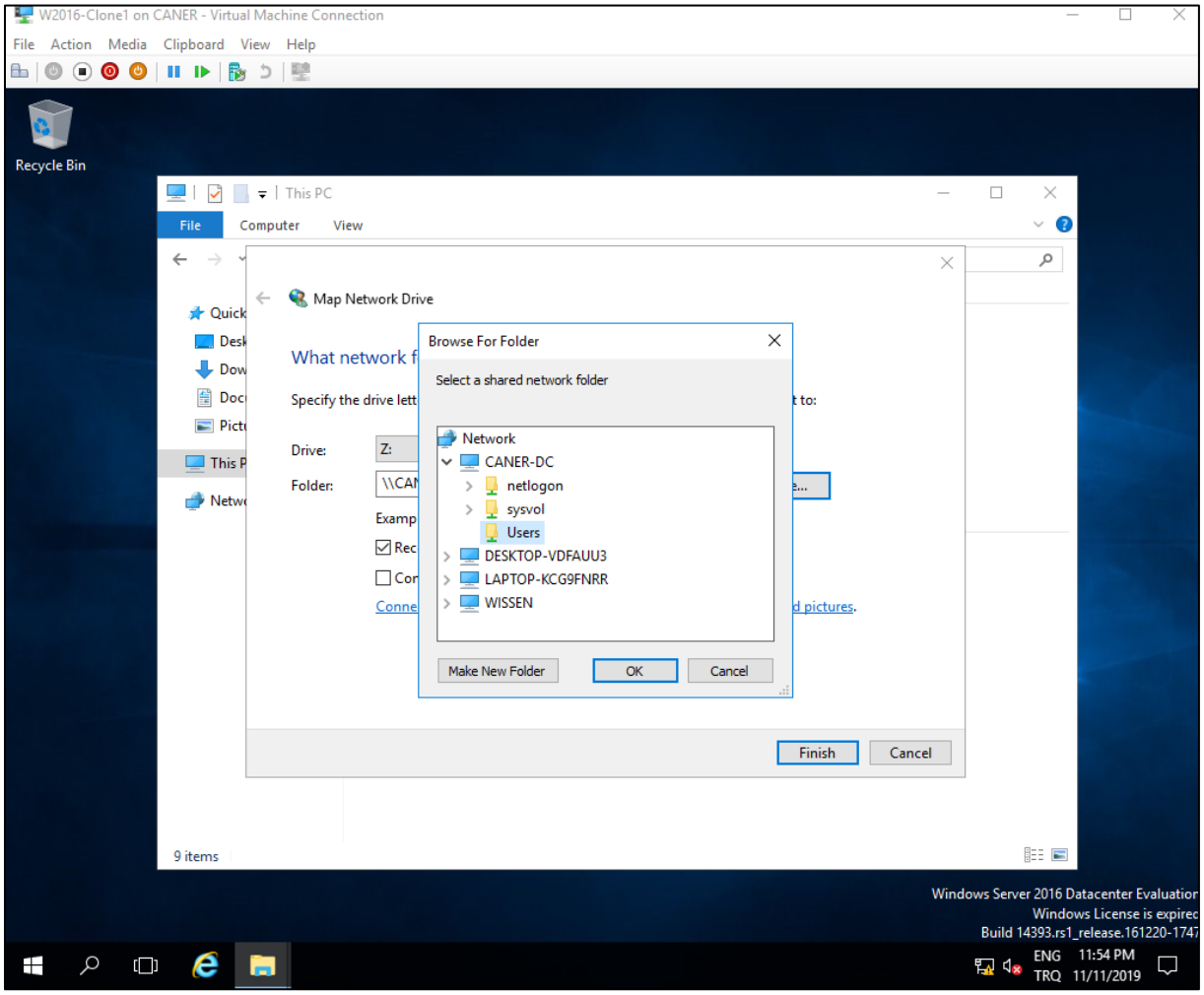
... he cannot since only Avşar Asan has the right to write on this shared folder.



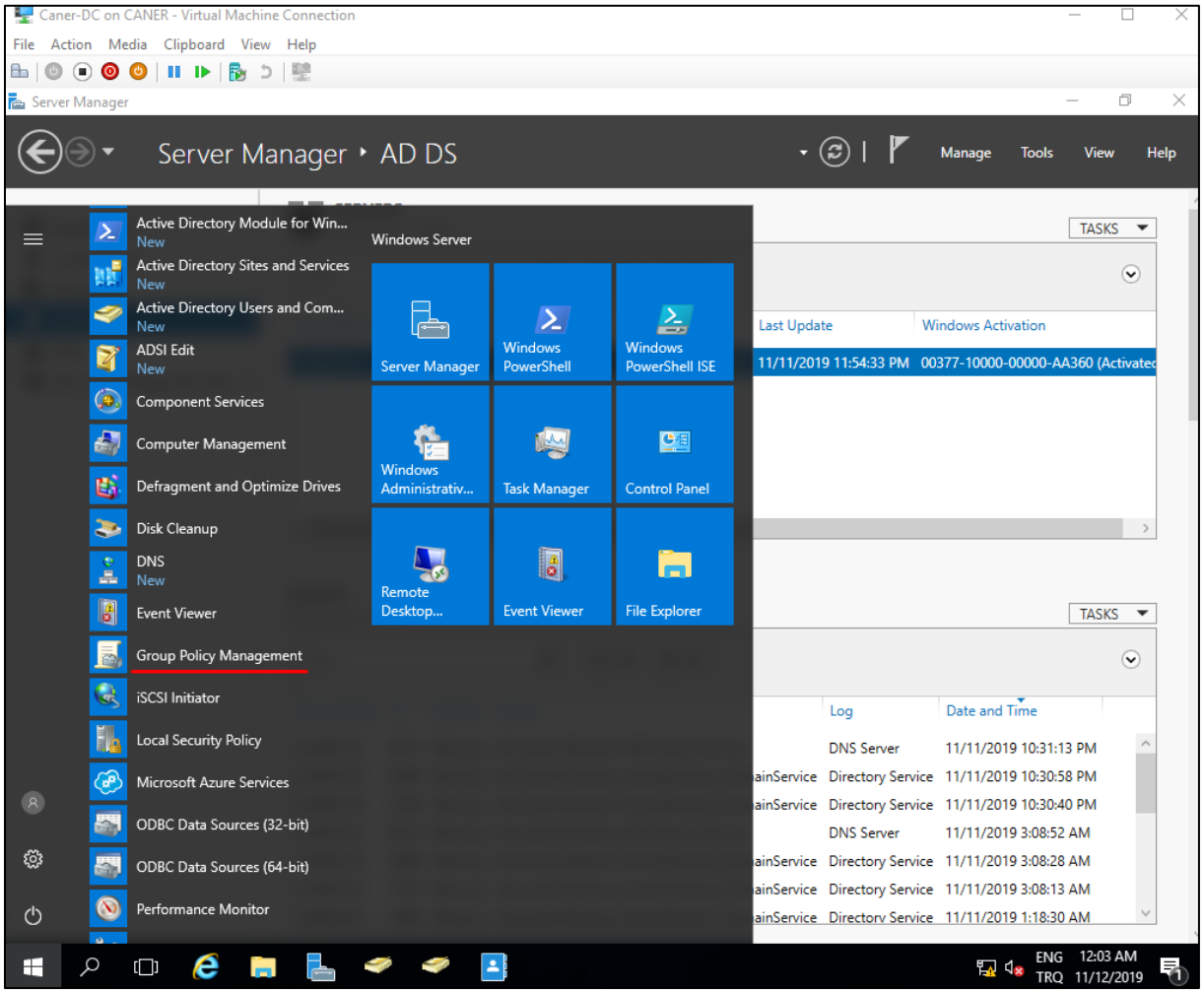
Now let’s test the access of HR Department with the Manager Esra’s account.



When we map the network drive with the previous path, we can see that she cannot even see the folder.



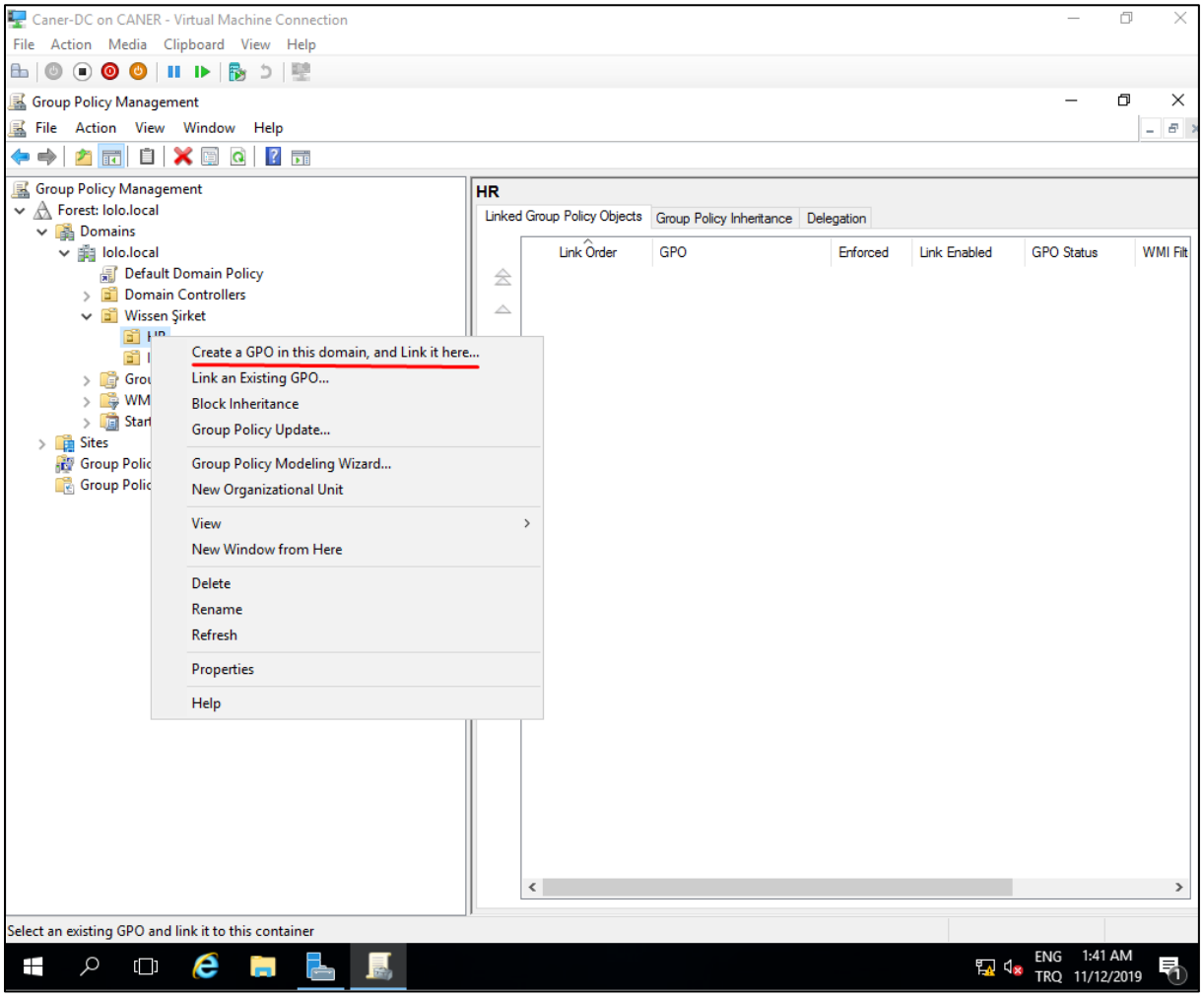
Note that this process was tolerable with a few users; however, image having 200 employees that you need to map the shared drive correctly. That'd be quite tedious. Fortunately, in Active Directory we can use Group Policy Objects and share the drives and folder automatically. Under Windows Administrative Tools we select Group Policy Management.



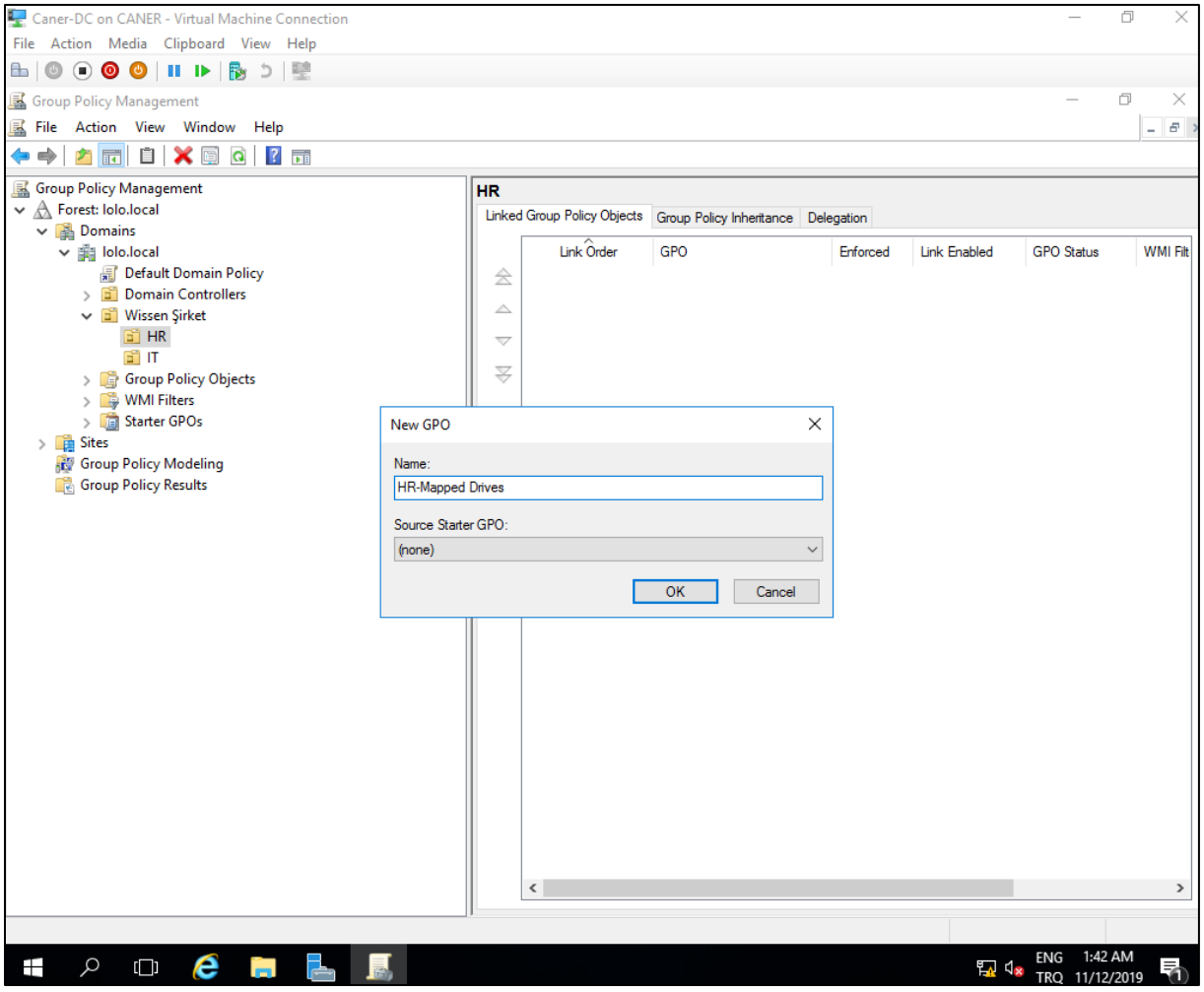
20.11.2019

We added a new disk for the HR Department's mapped drive but we assume we don't have to use an empty physical drive. In case, we can create volumes out of virtual disks via Storage Pools if we definitely need distinct physical drive for policies. What we must do for certain is to share the drive or the folder since it will be necessary later.

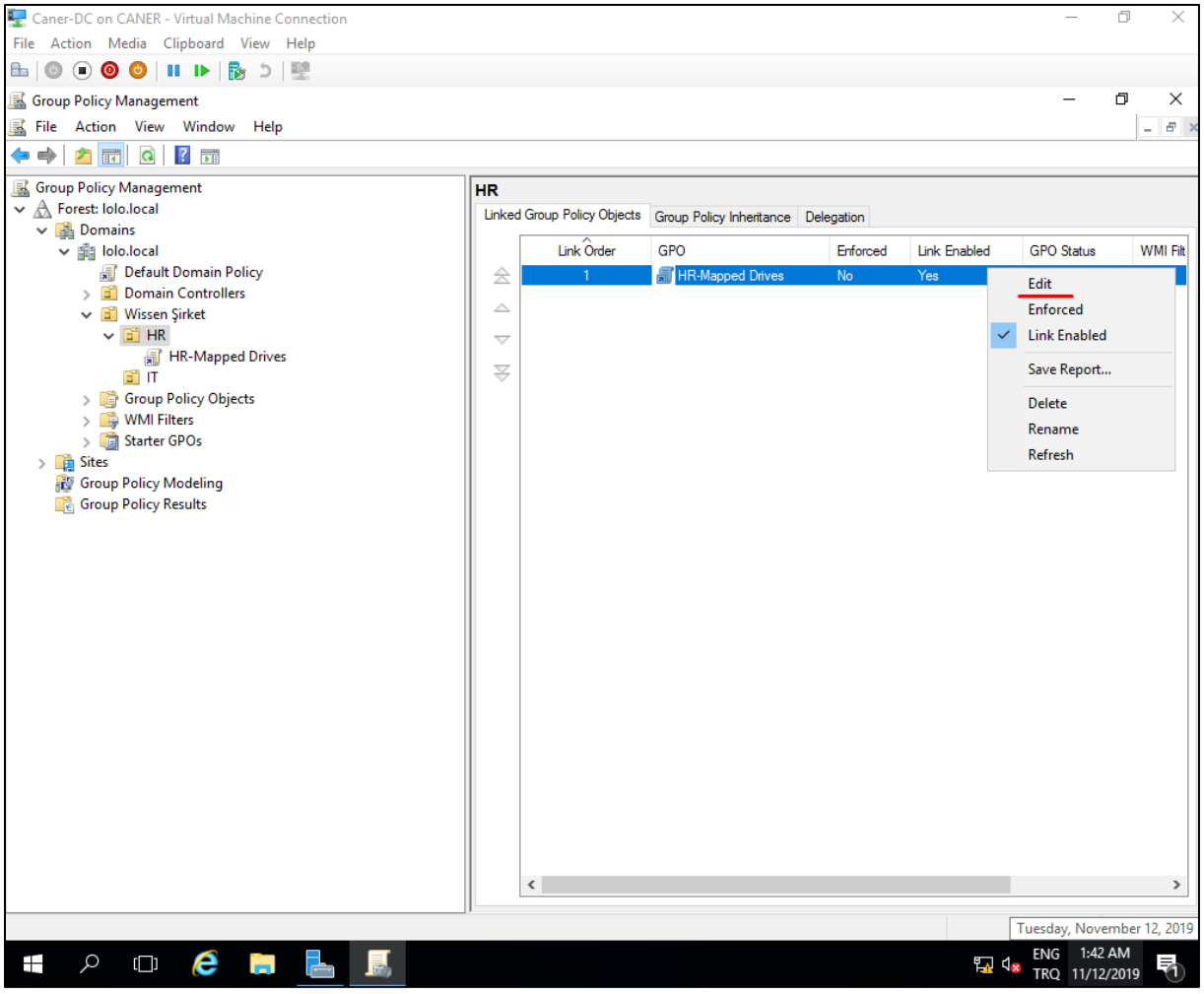
We select our domain lolo.local and locate the Organiztional Unit under which we want to create our Group Policy Object. GPOs affect only the Organizational Unit in which they are located. Since we want our HR Drive to be mapped only to the HR people, that's where we are putting our GPO. We right click the Organizational Unit and select Create a GPO in this domain and link it here.



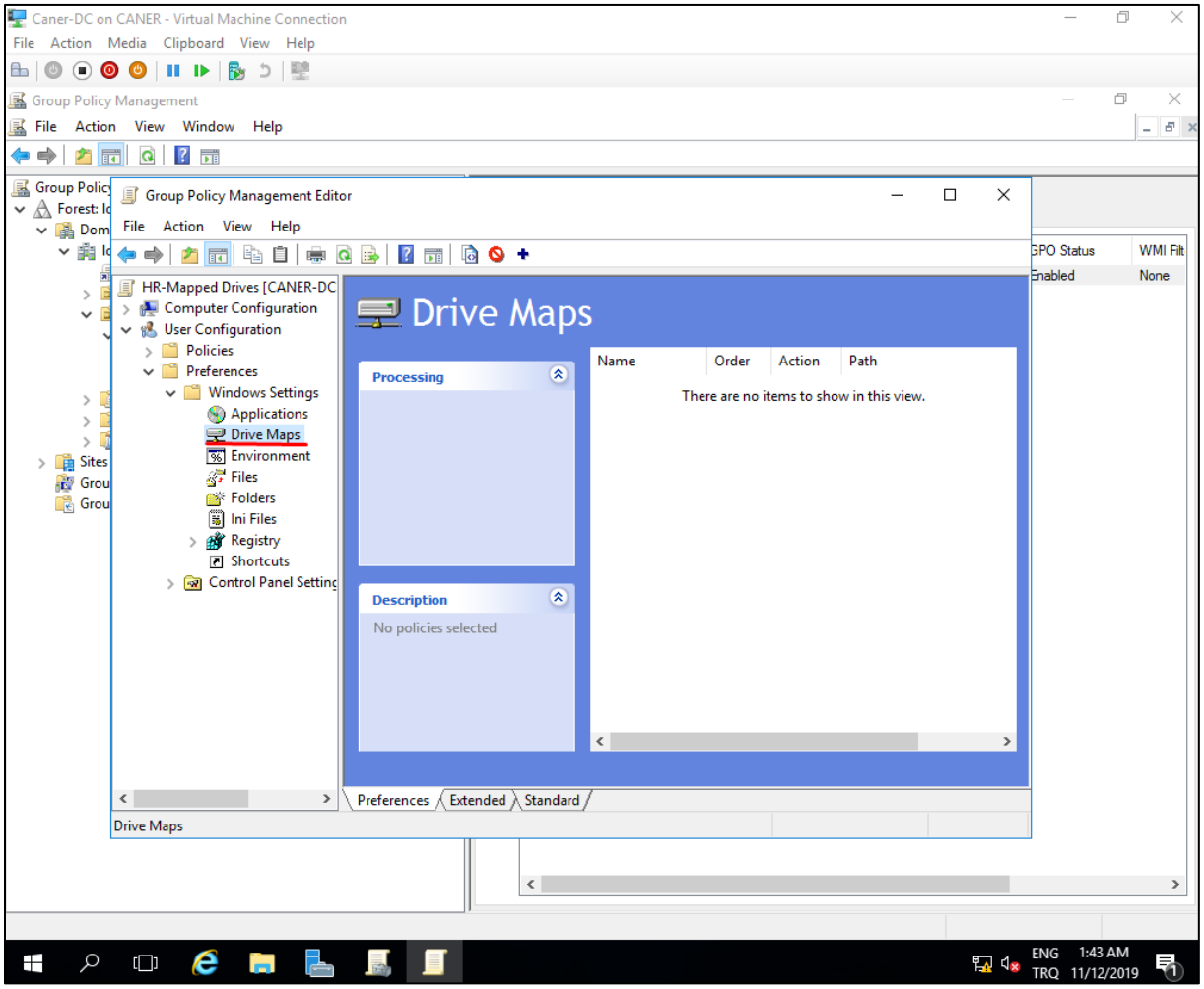
We name the GPO.



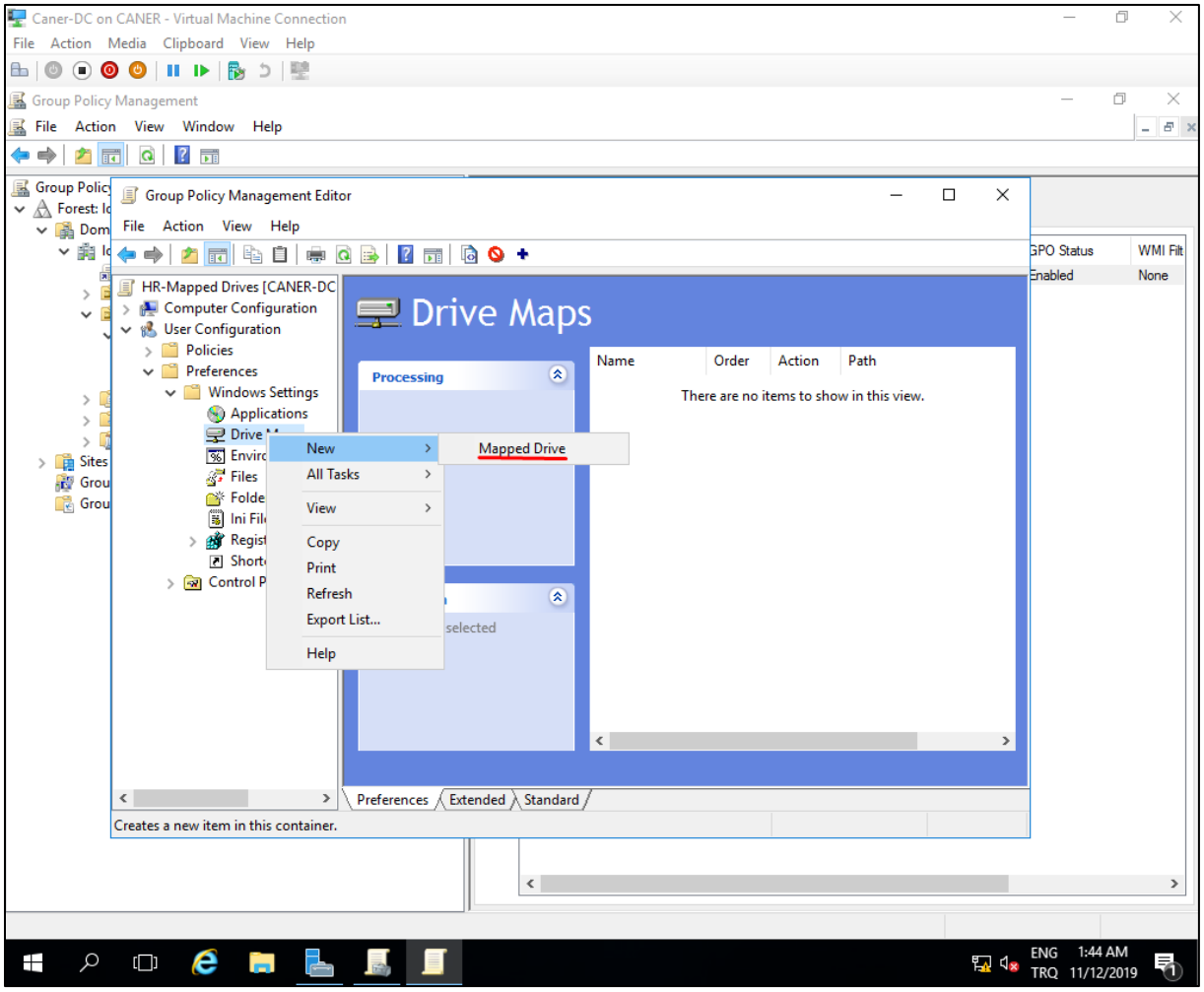
We then edit the GPO.



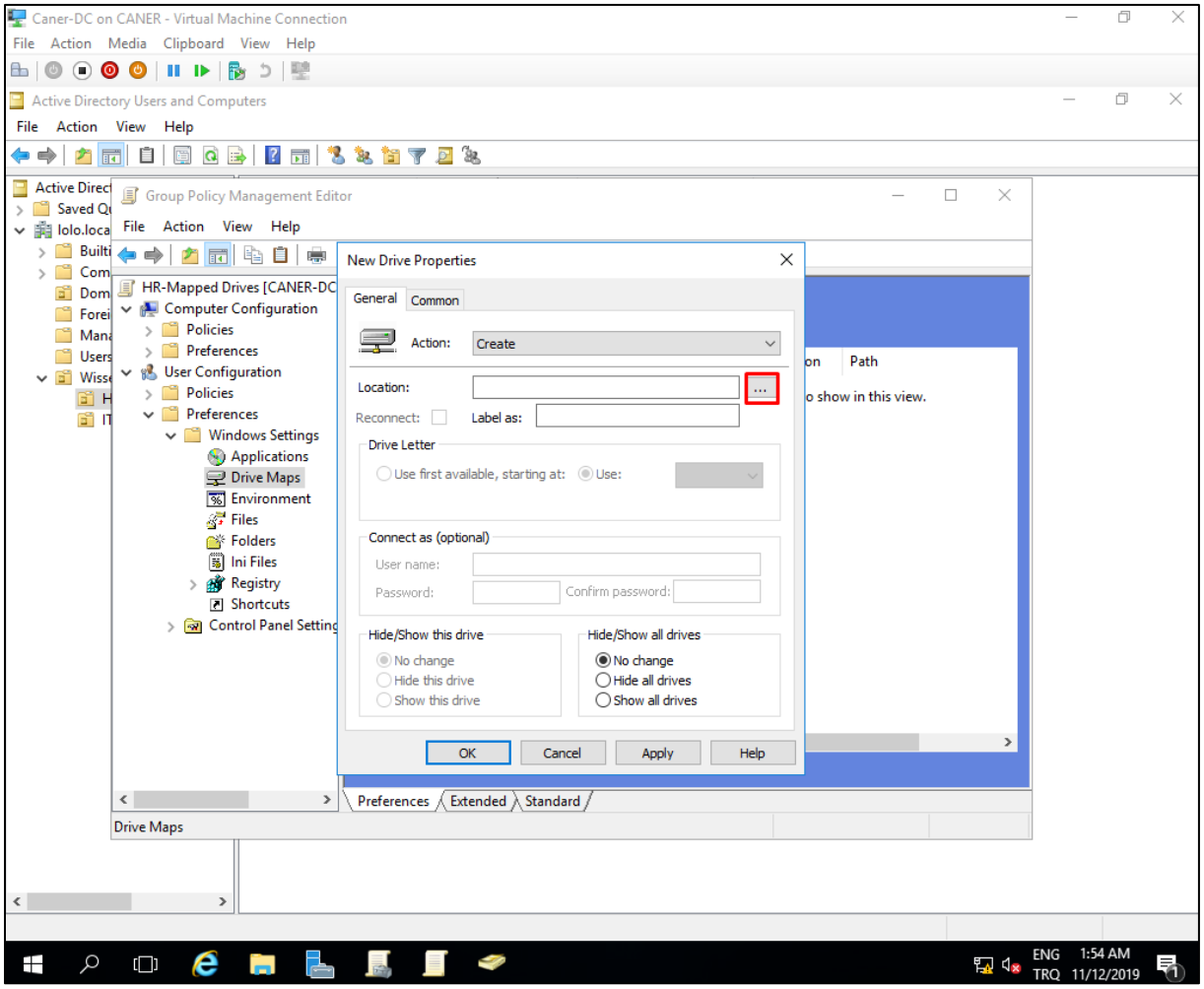
Under User Configuration, Preferences, Windows Settings we select Drive Maps.



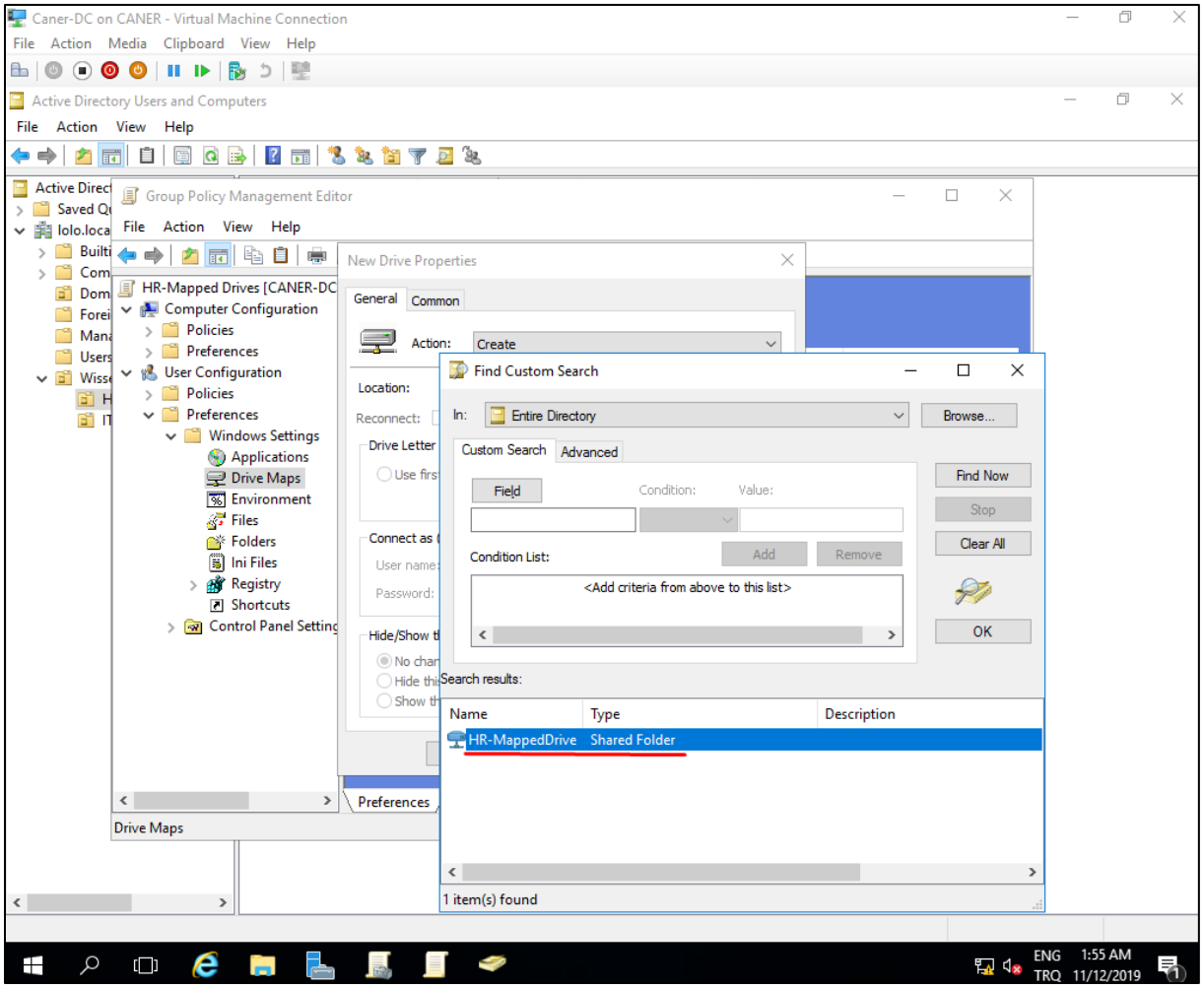
We right click and create a New Mapped Drive.



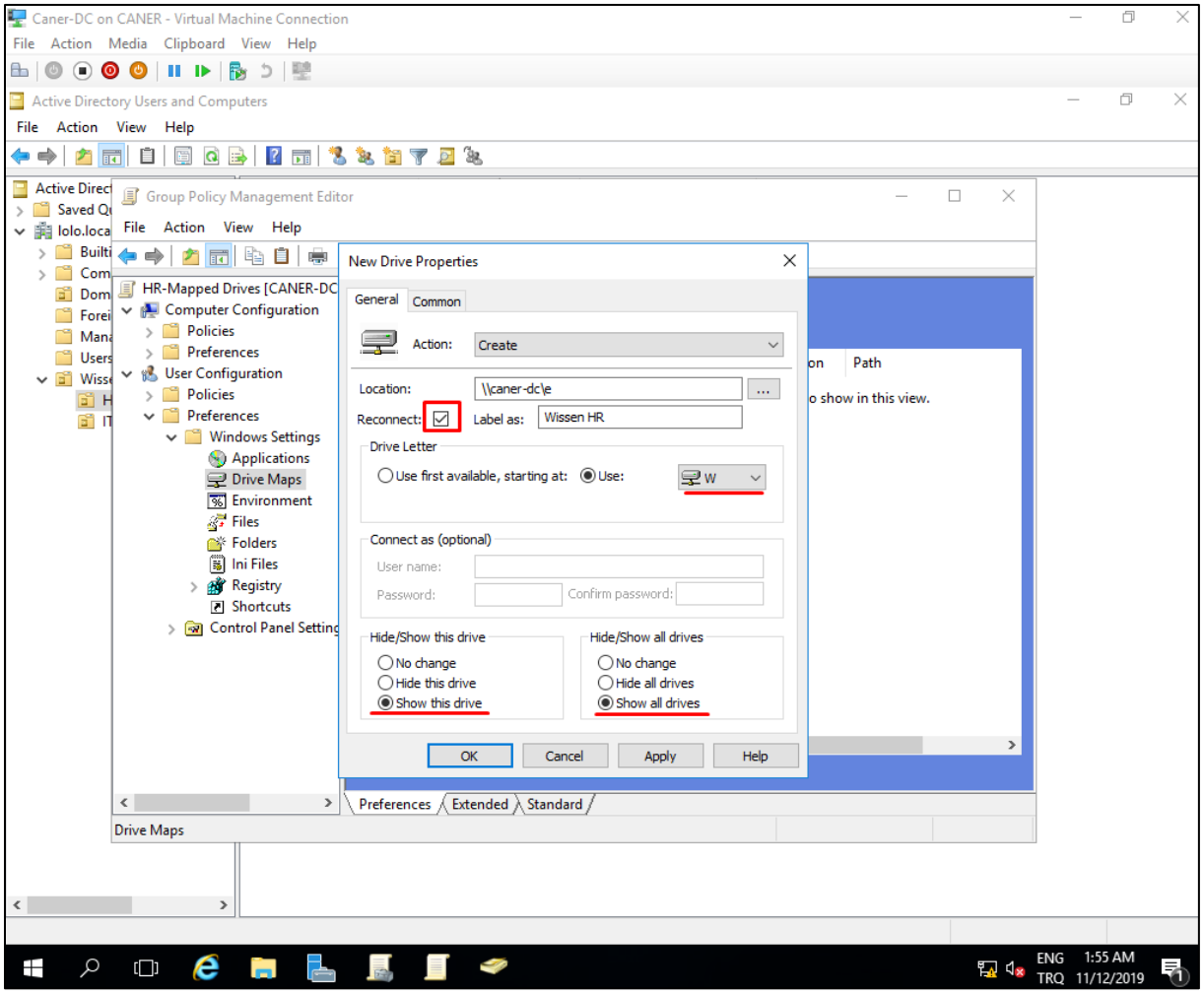
We find the location of the drive (or folder) we want mapped.



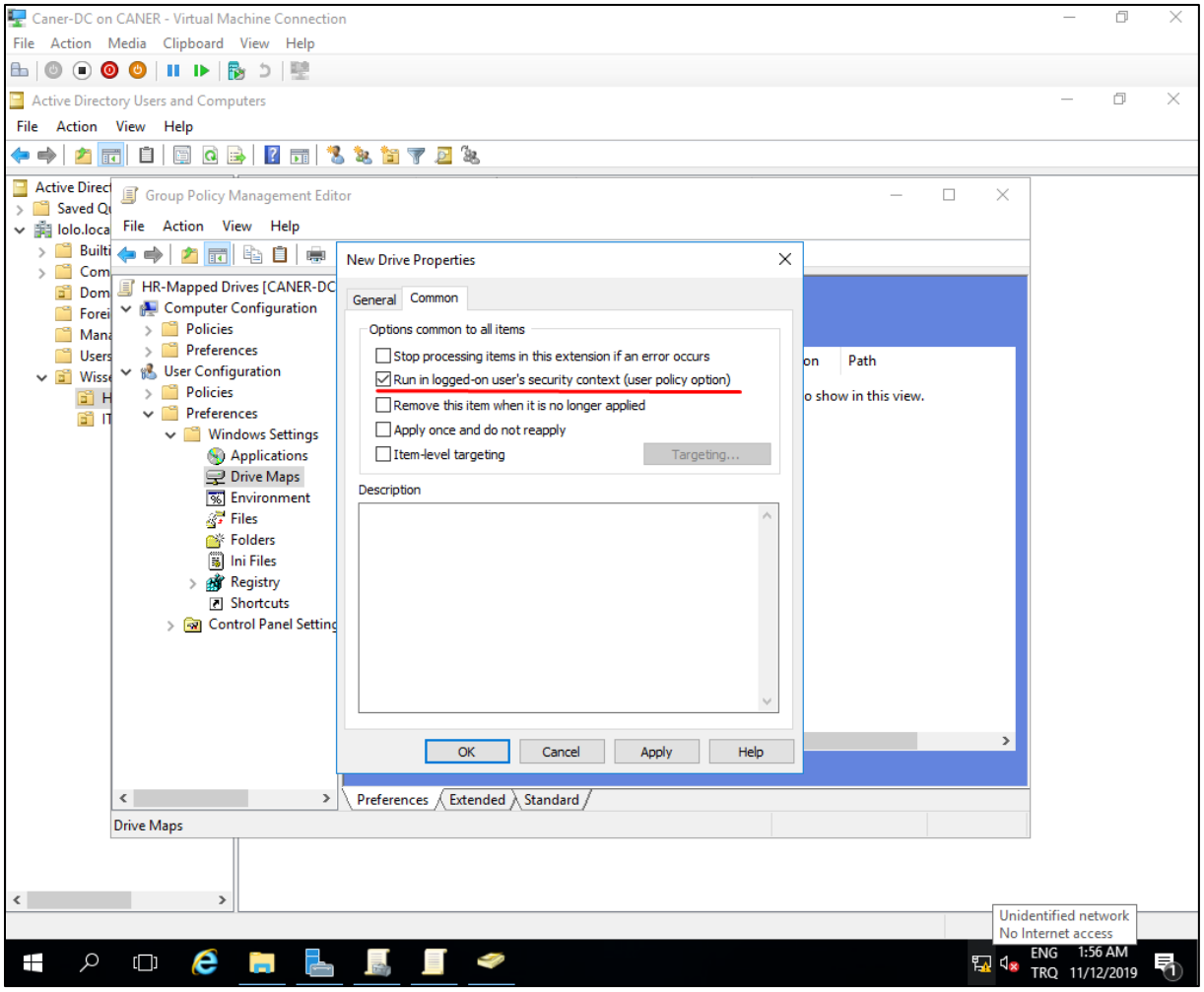
Since we shared our drive (or folder) previously, we see it here and select it.



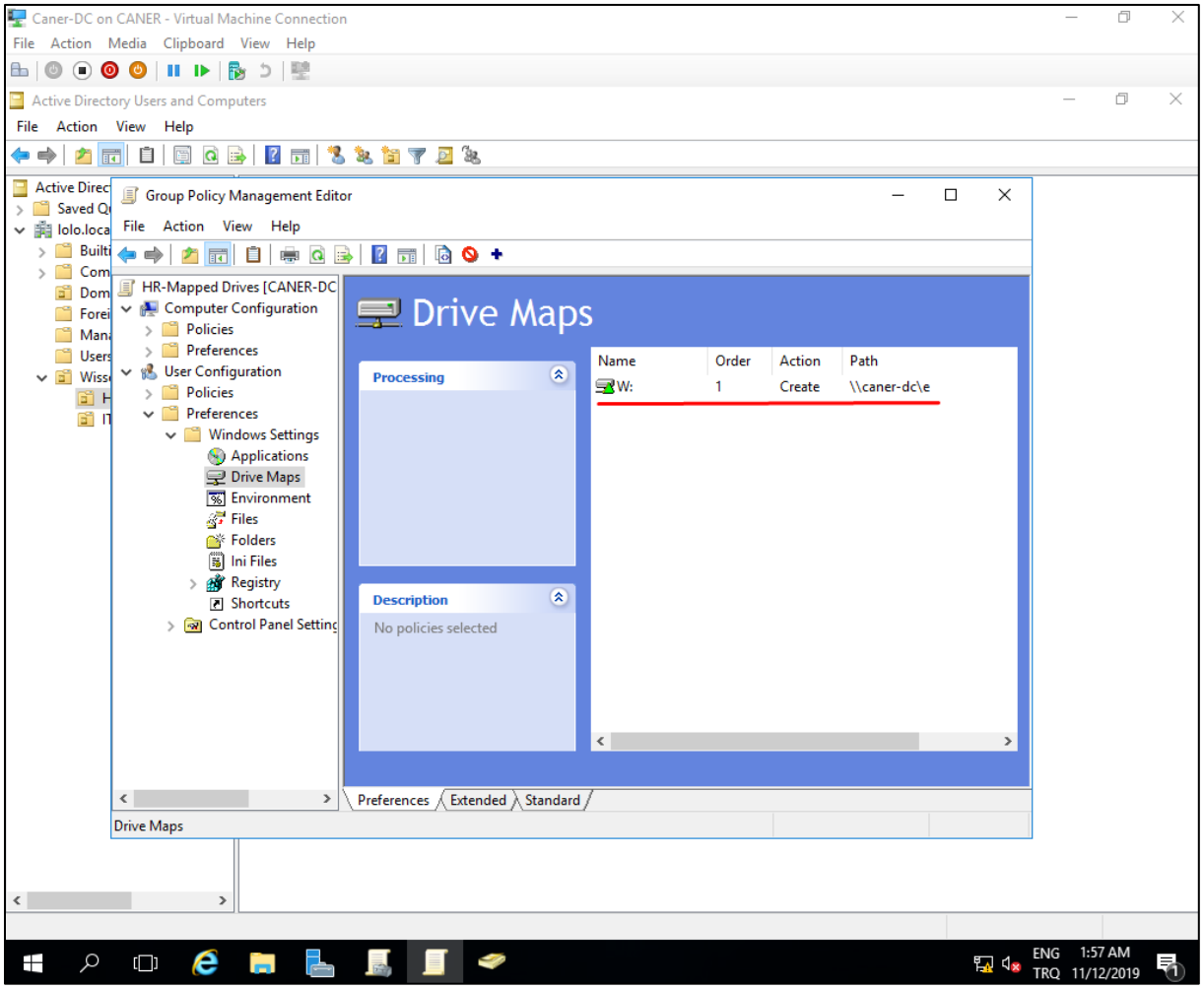
We assign a drive letter and label it appropriately and then select the following setting.



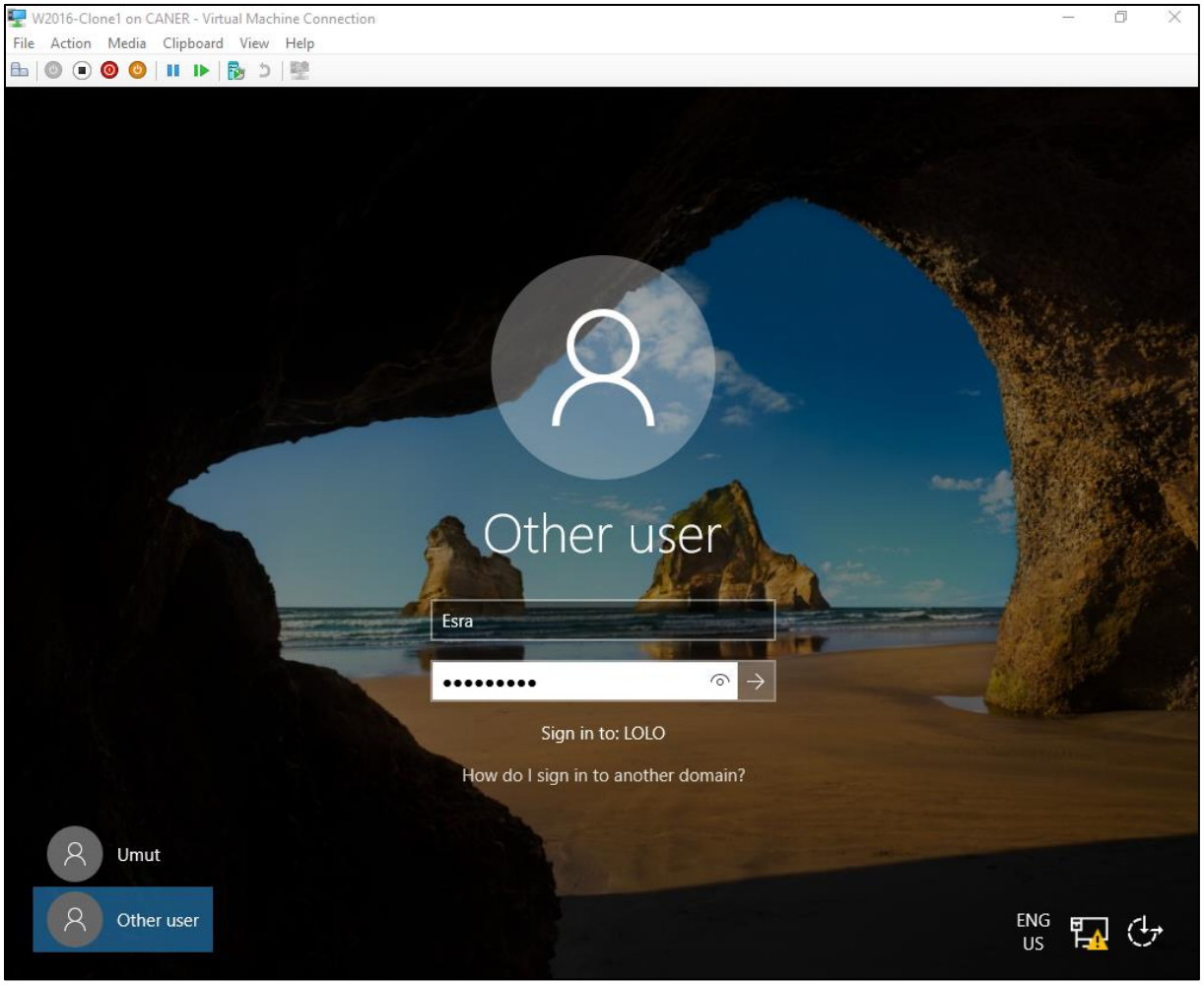
On the next screen we select Run in logged-on user's security context.



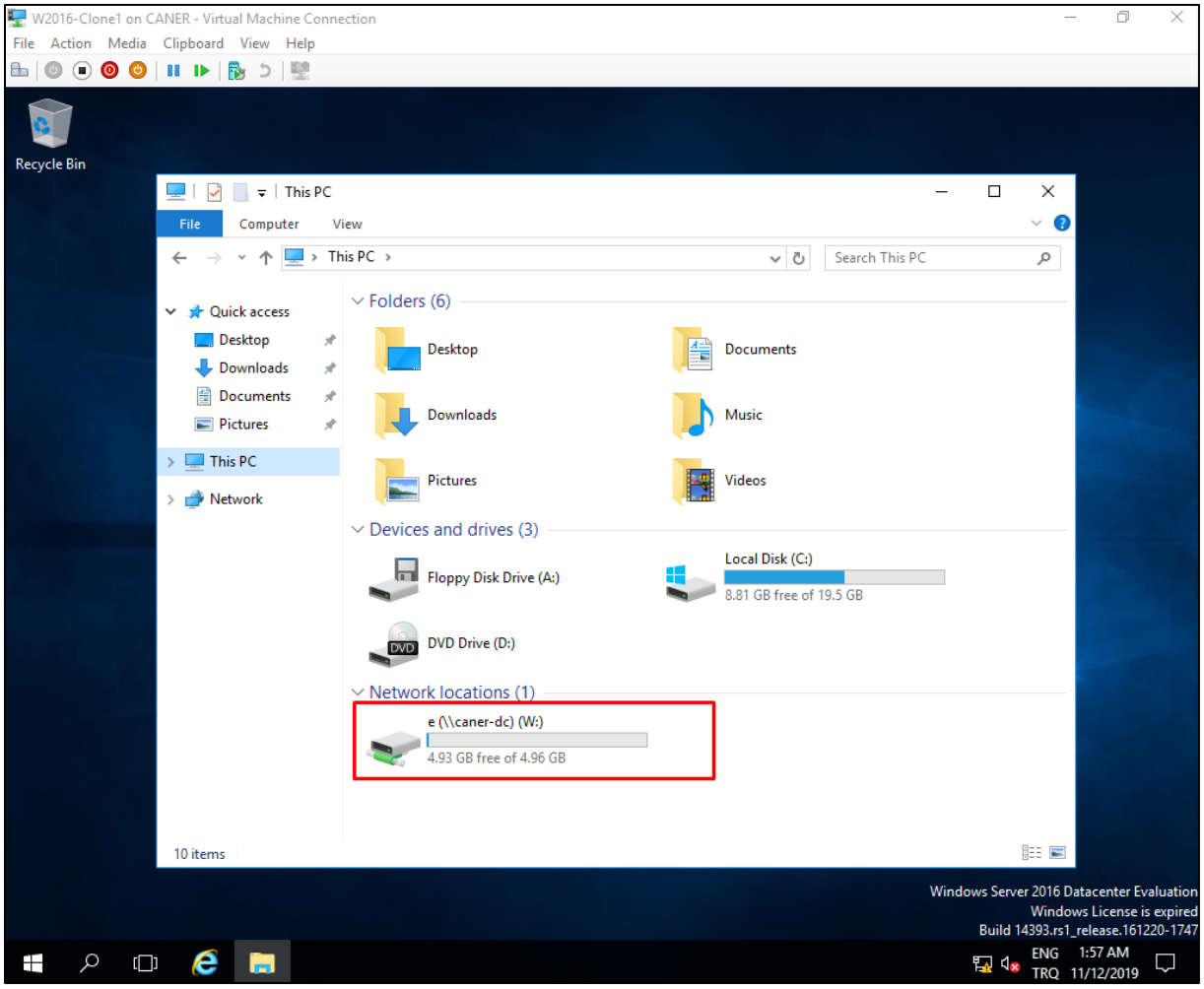
Then the map is visible with the action “Create” which we selected from the previous menu.



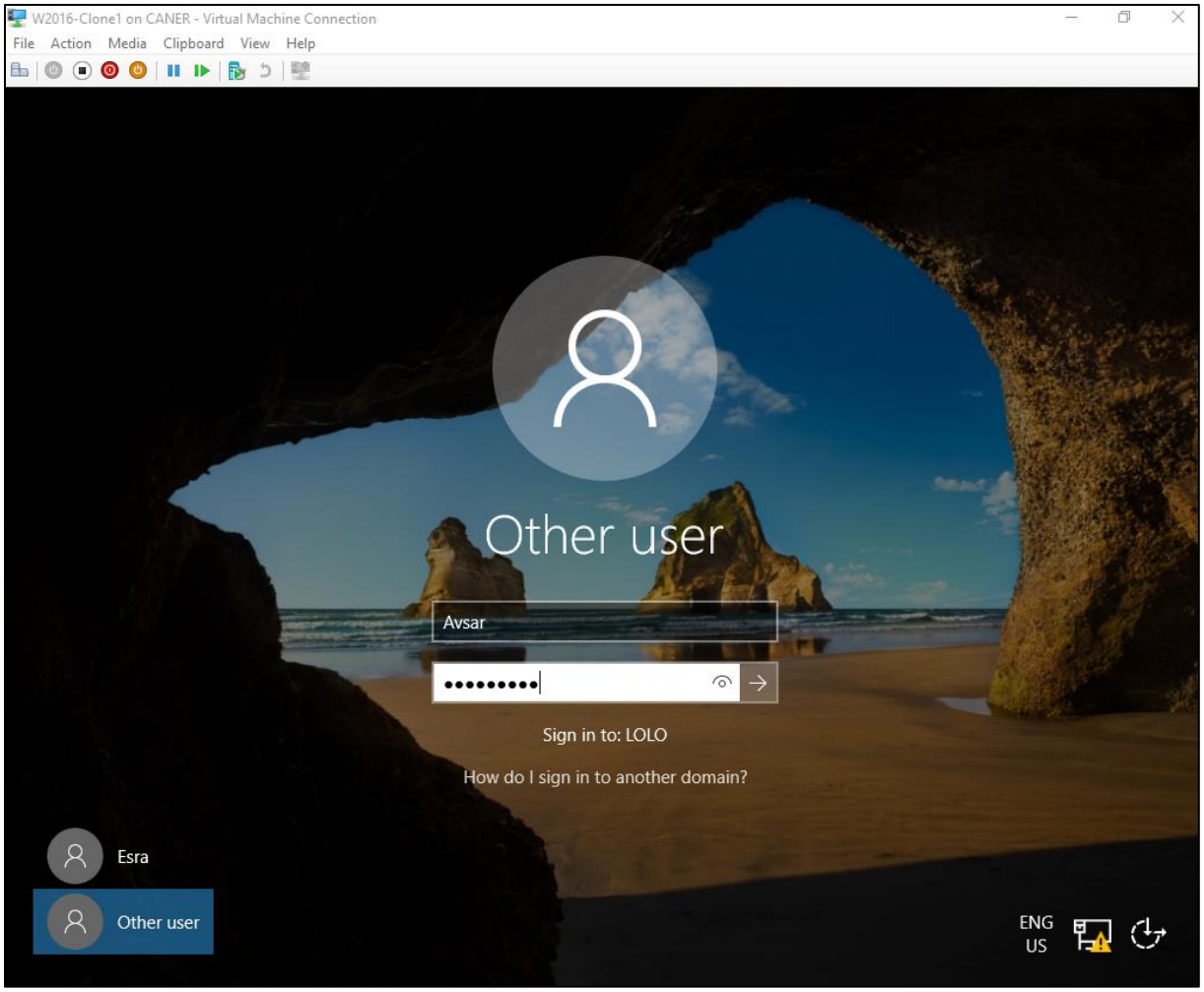
We log in as the head of HR, Esra.



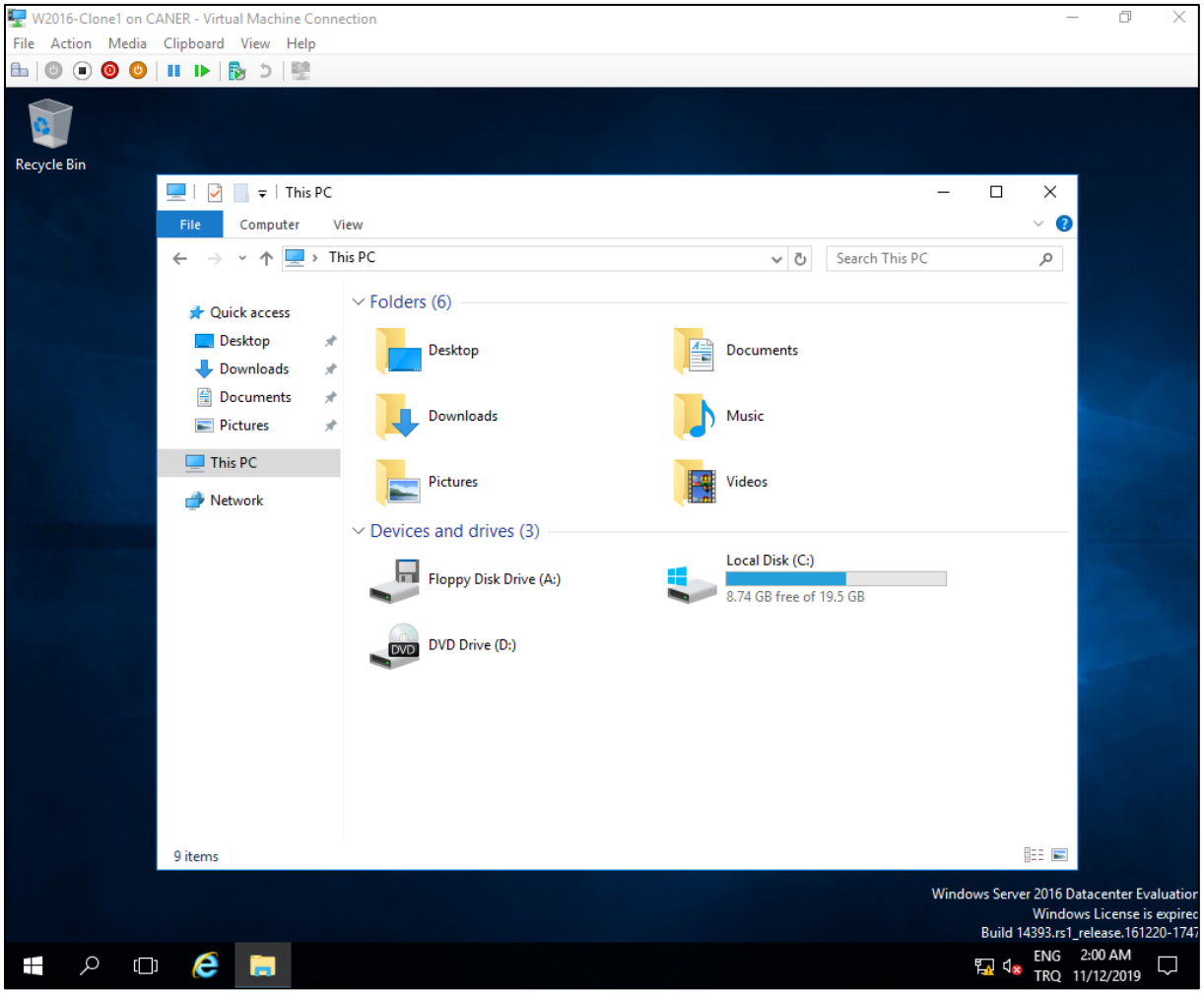
We can see that the drive is automatically visible without any effort.



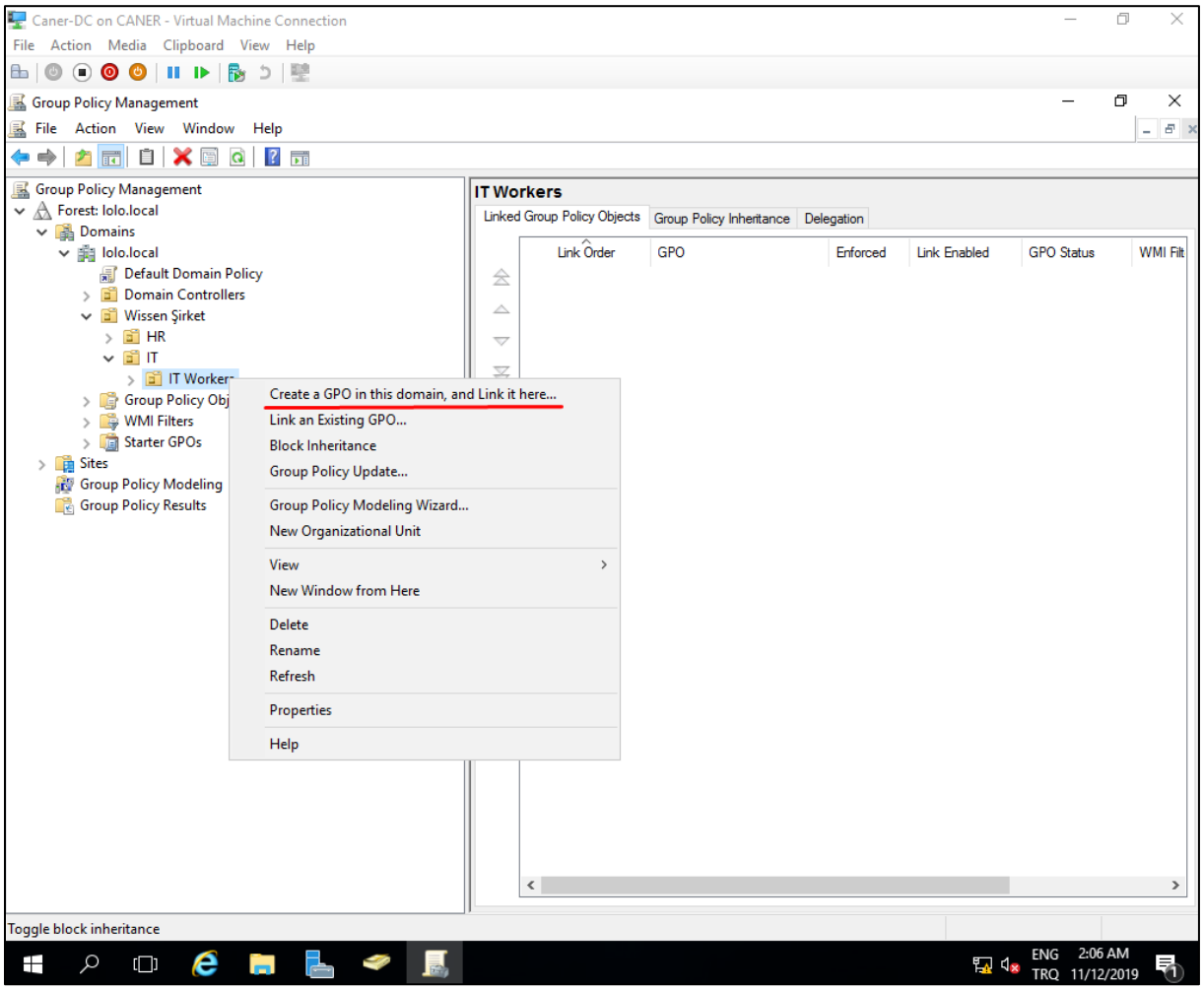
Let’s check whether people from outside of HR can access the drive.



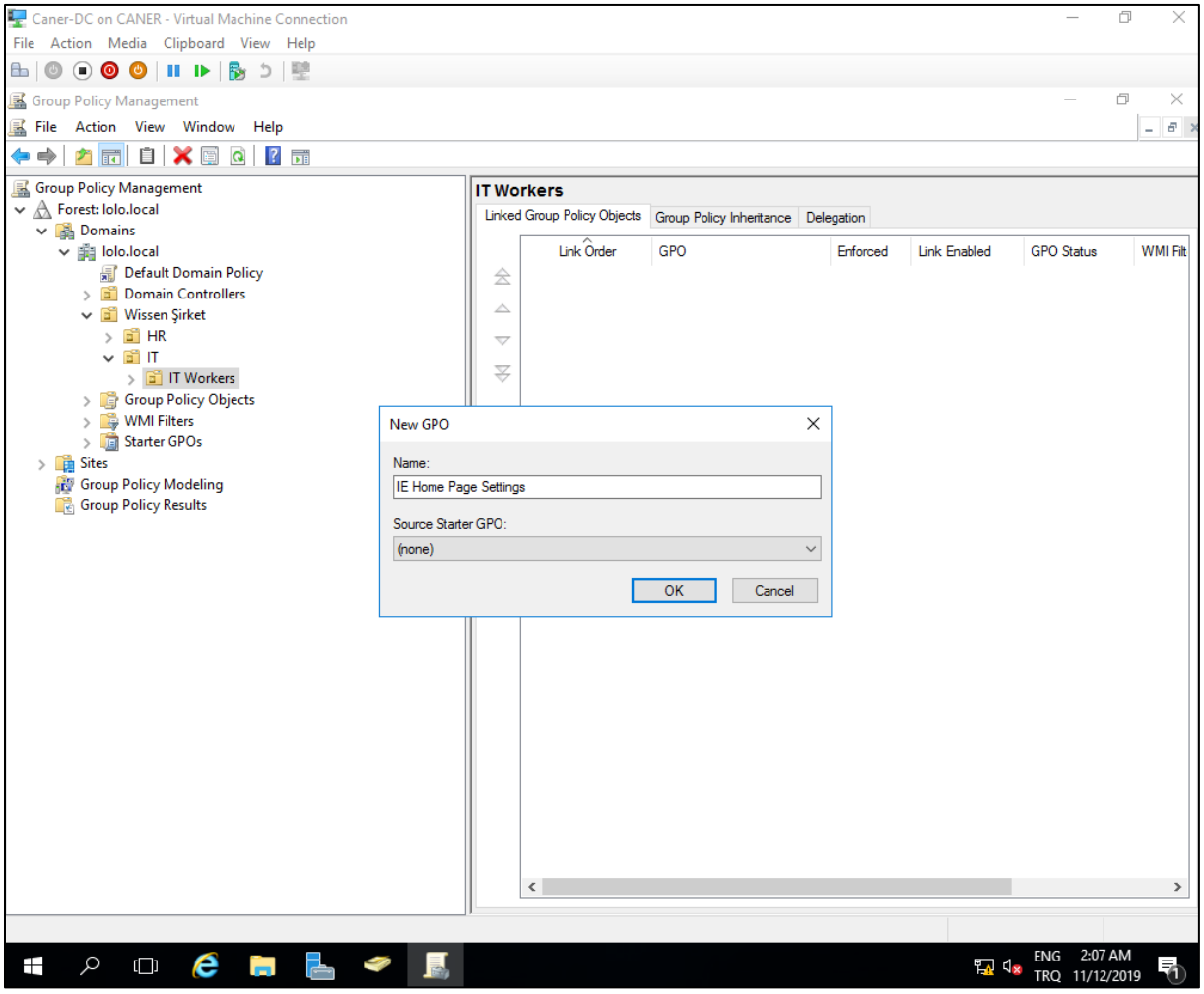
Even the manager of IT cannot see the drive shared for HR.



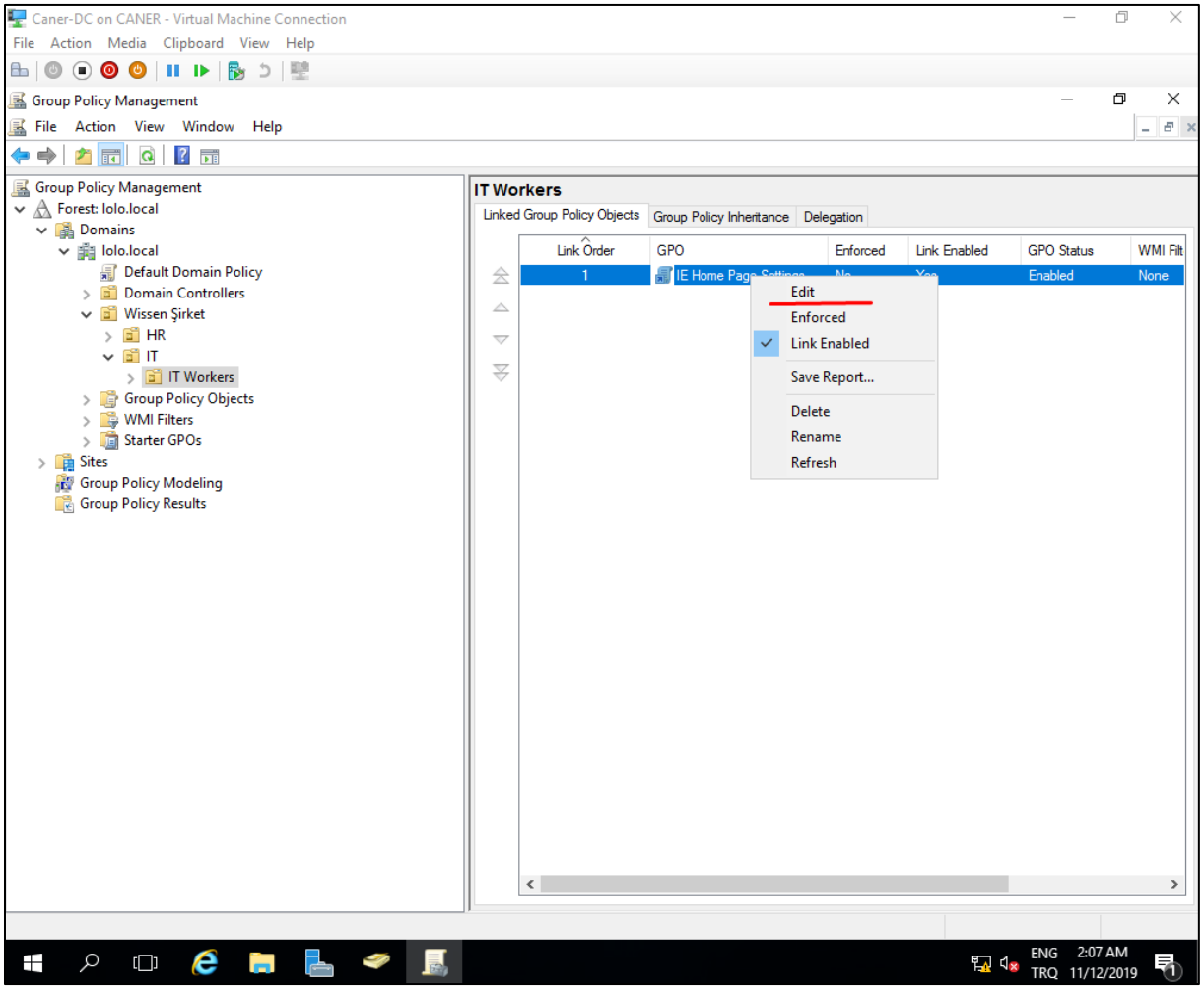
Now, let's administer Internet Explorer settings using another GPO. We want to block IT Workers' right to changing the home page of IE and set the page to a specific website. Firstly, we create a GPO under the Organizational Unit of IT Workers.



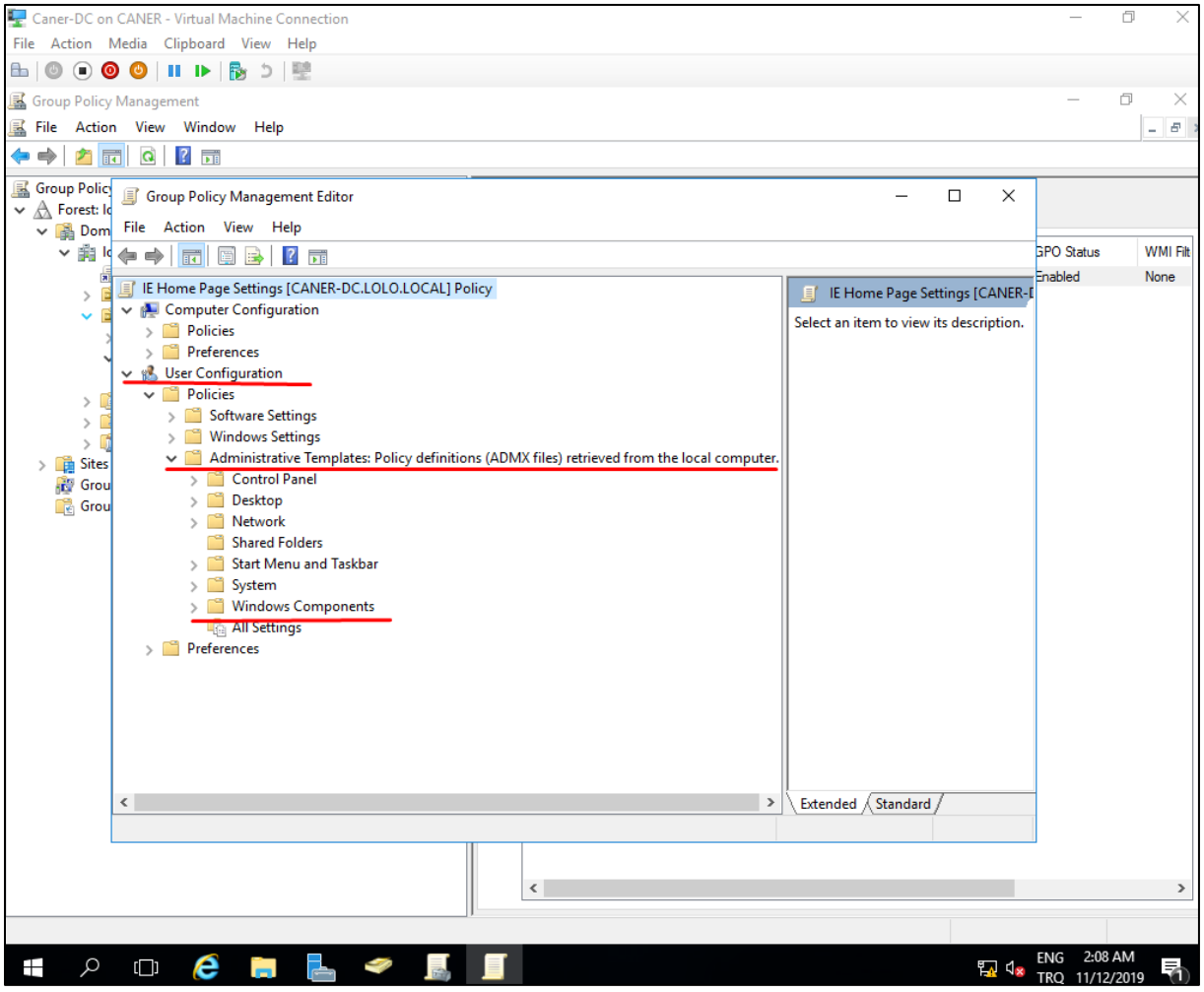
We name the GPO.



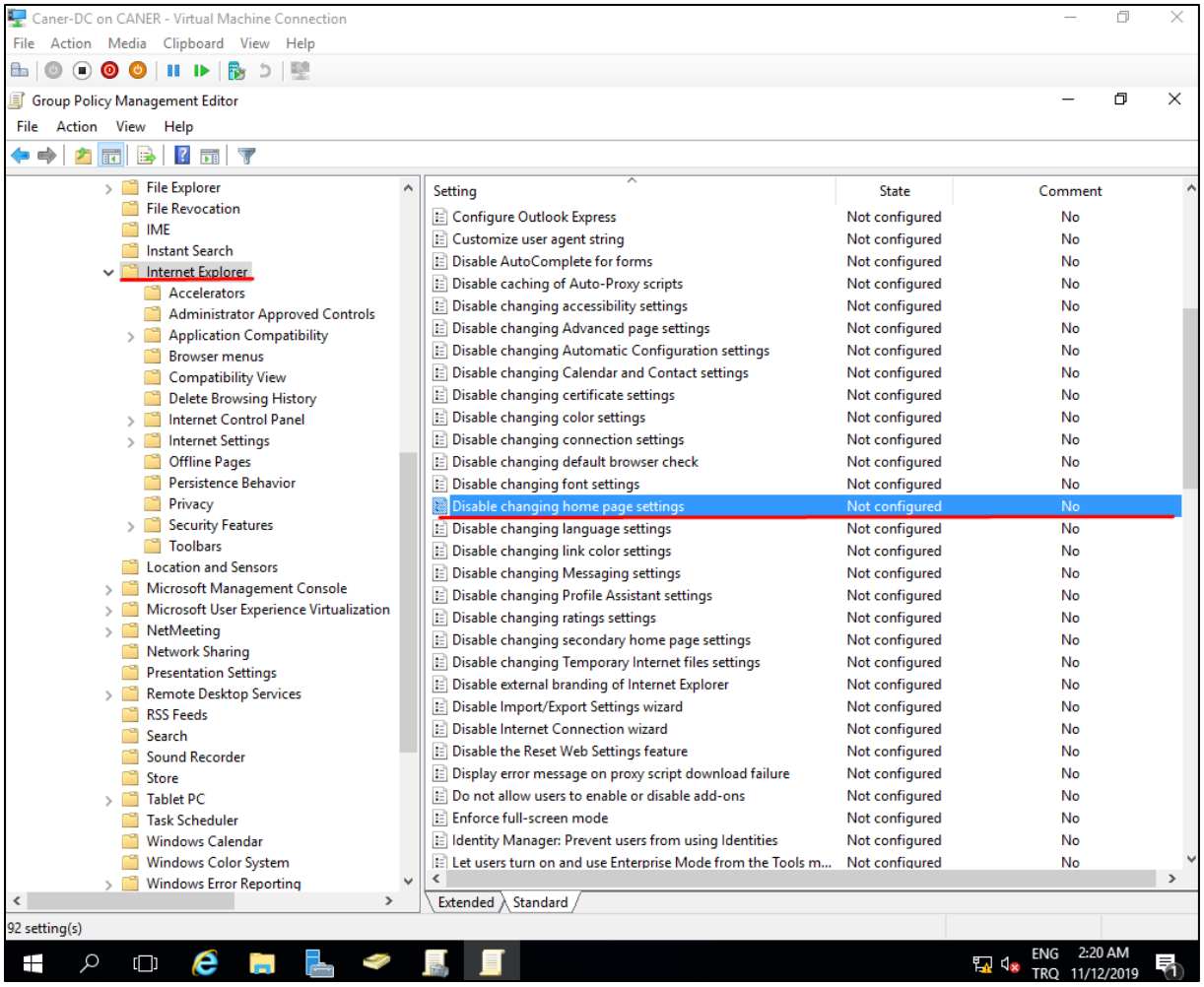
Edit the GPO again.



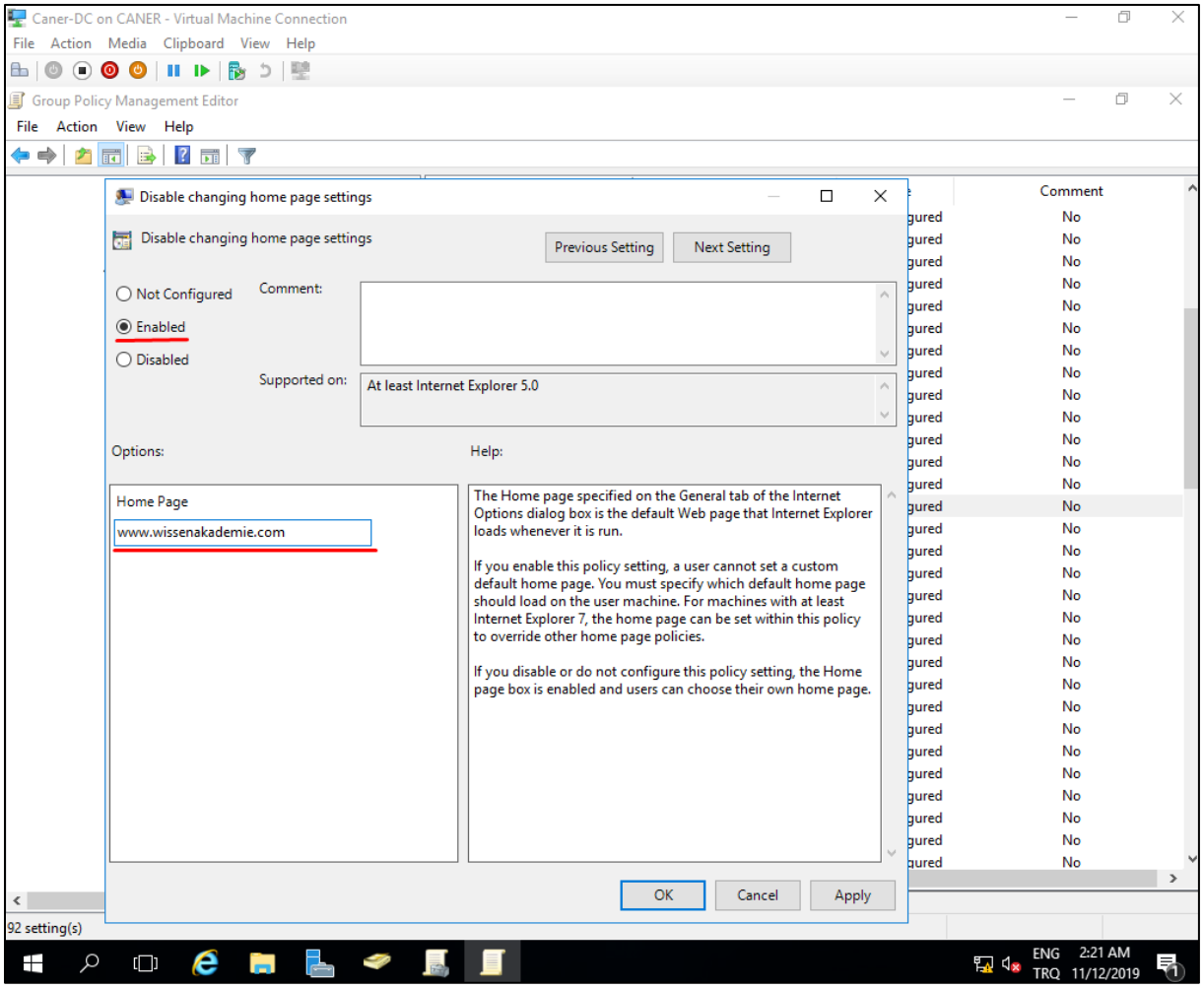
Under User Configuration, Administrative Templates, Windows Components...



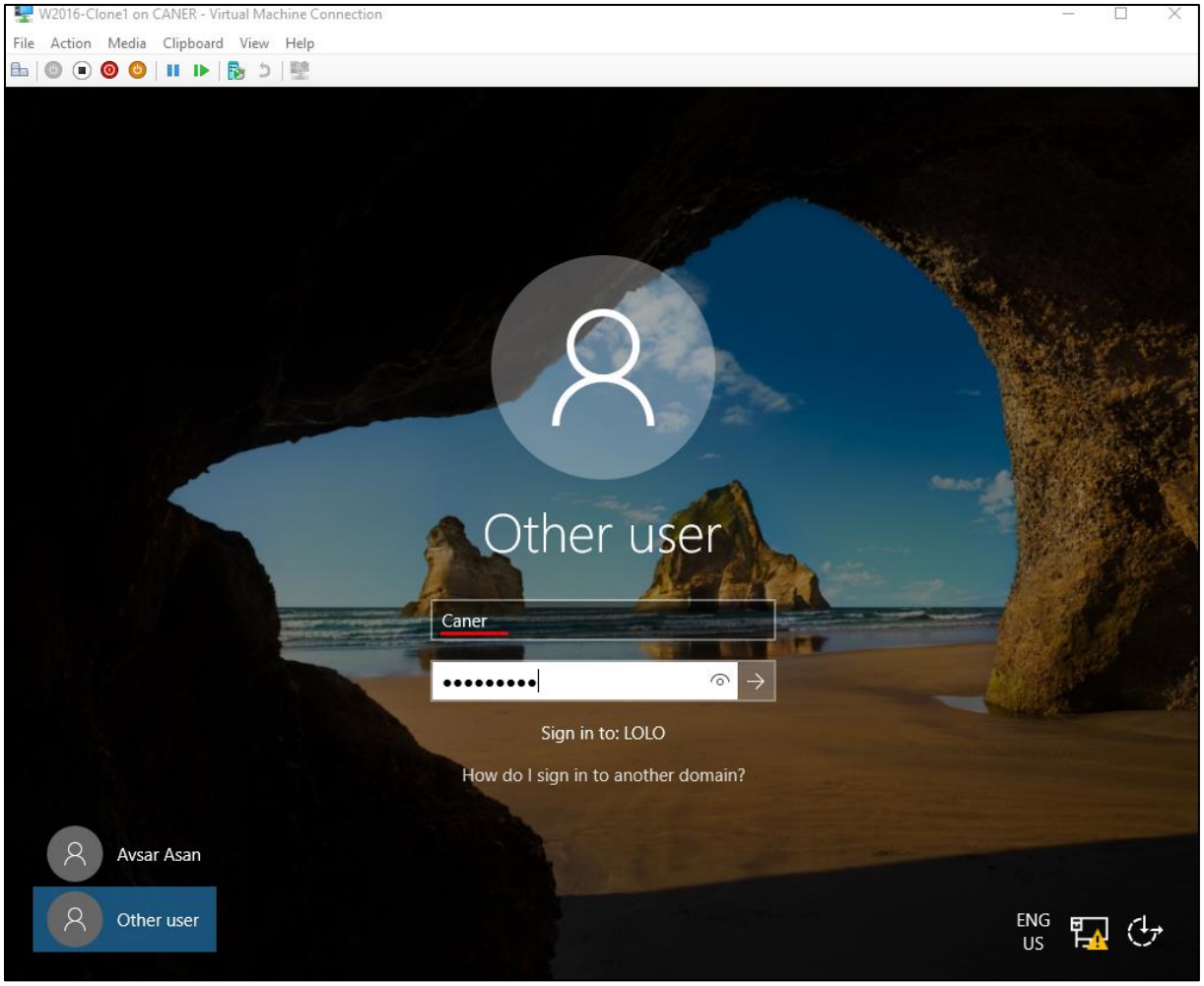
...there is IE with policy: “Disable changing home page setting”.



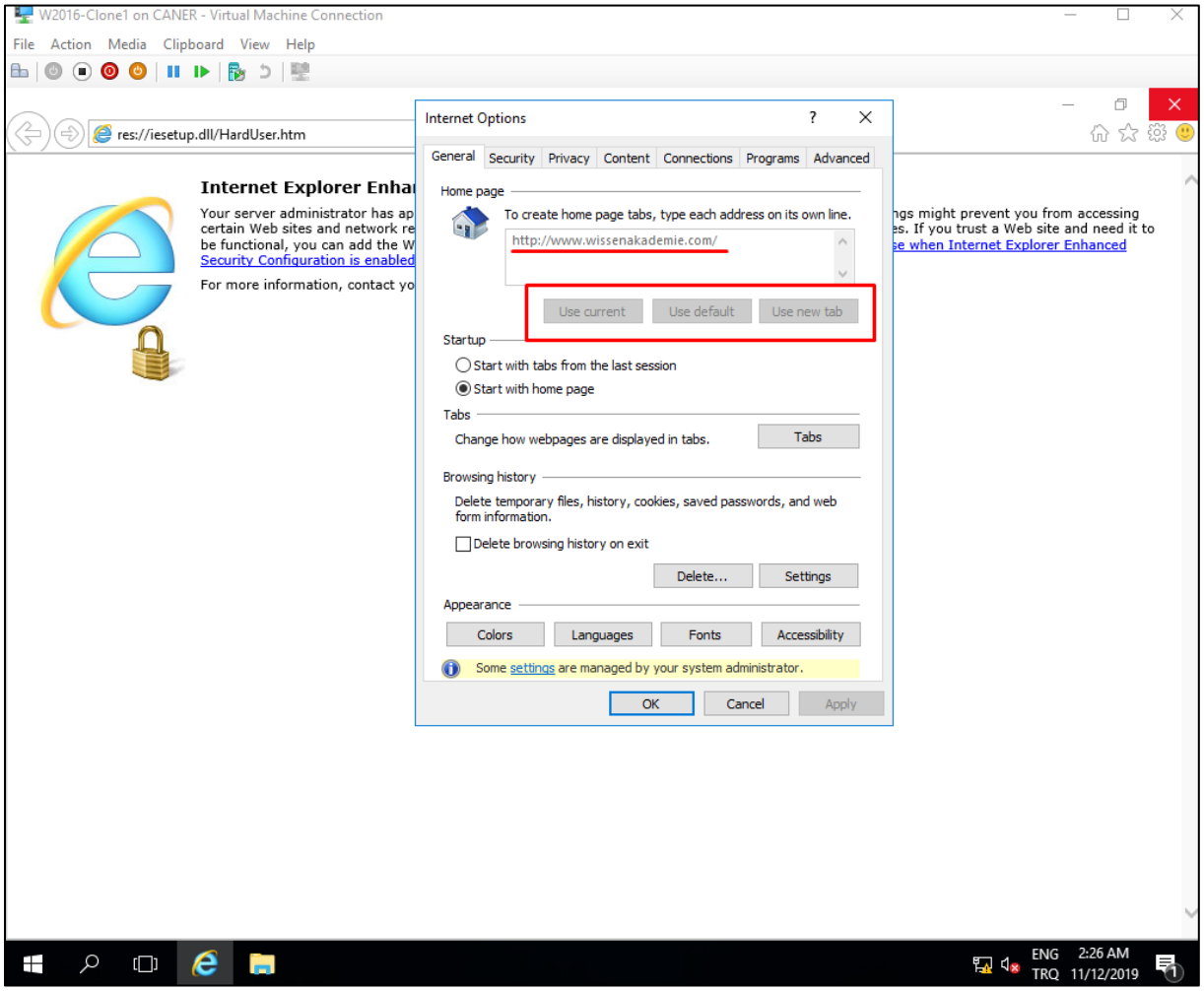
We Enable it and set the home webpage.



To test the policy implementation we login as Caner.



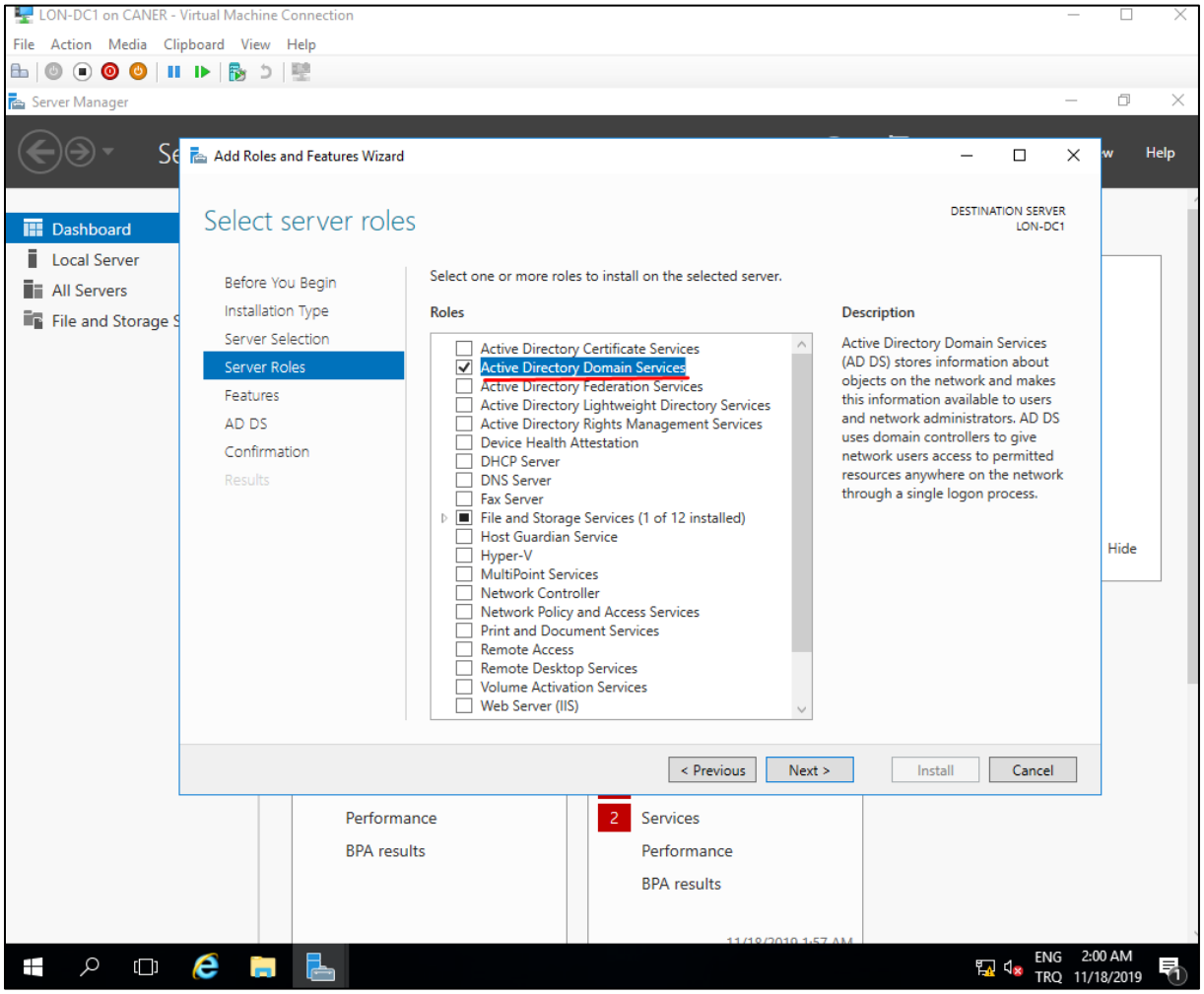
As you can see, the homepage is exactly as we set and the options to change the homepage are greyed out.



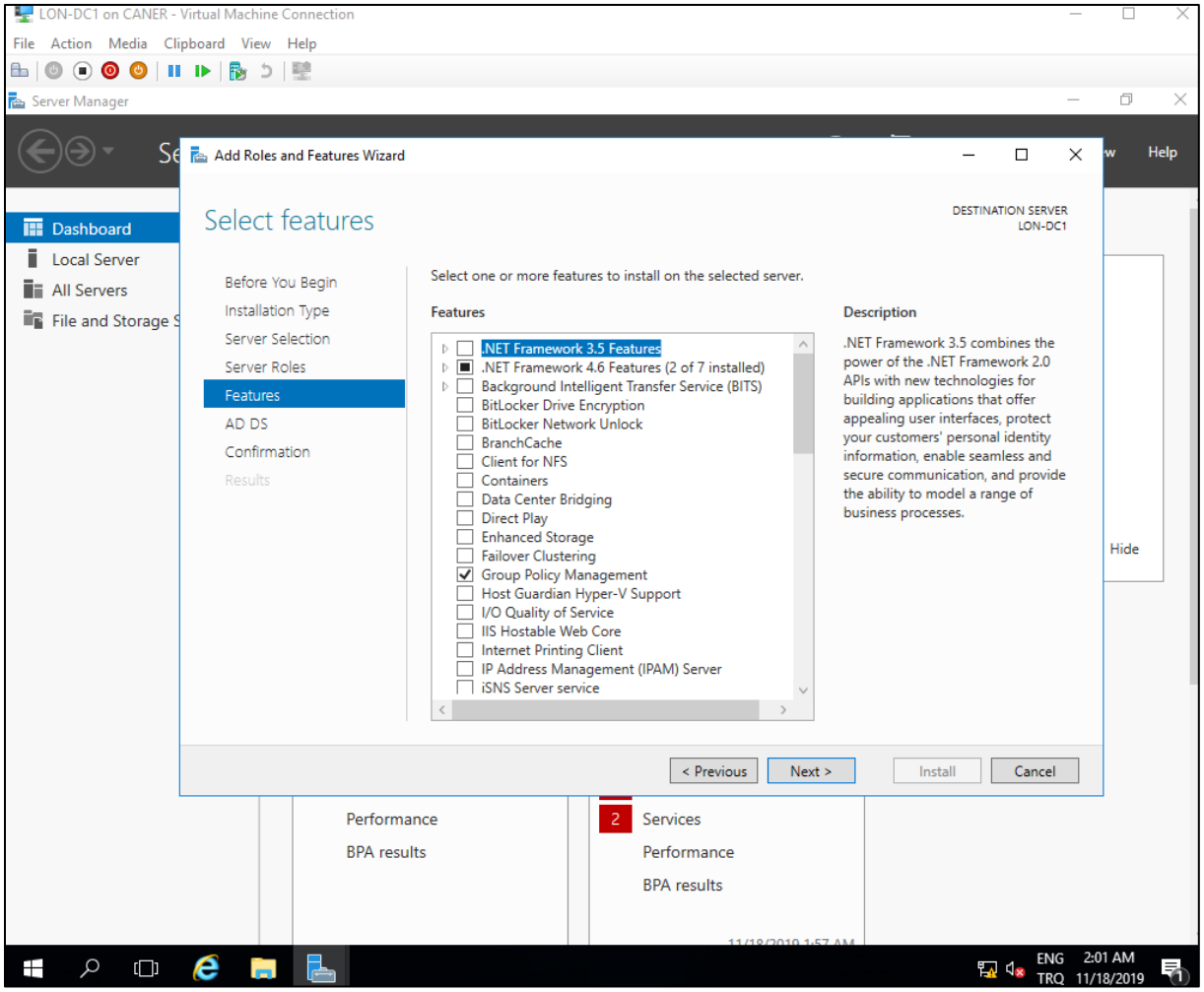
II. Certificate Services

In this part of the project we have 3 server PCs which use Windows Server 2016 and one client PC which uses Windows 10. LON-DC1 is the Domain Controller (DC) for our domain “cert.local”. CA-SRV1 is NOT a part of this domain and hence not included in the Active Directory. It is the Standalone Root Certificate Authority which will be original source of our certificates. Since CA-SRV1 is not in the domain “cert.local” and hence cannot distribute the certificates, we need an Enterprise Subordinate Certificate Authority in the domain. LON-SRV1 is that server so it’s a Certificate Authority (CA) and a member in the domain.

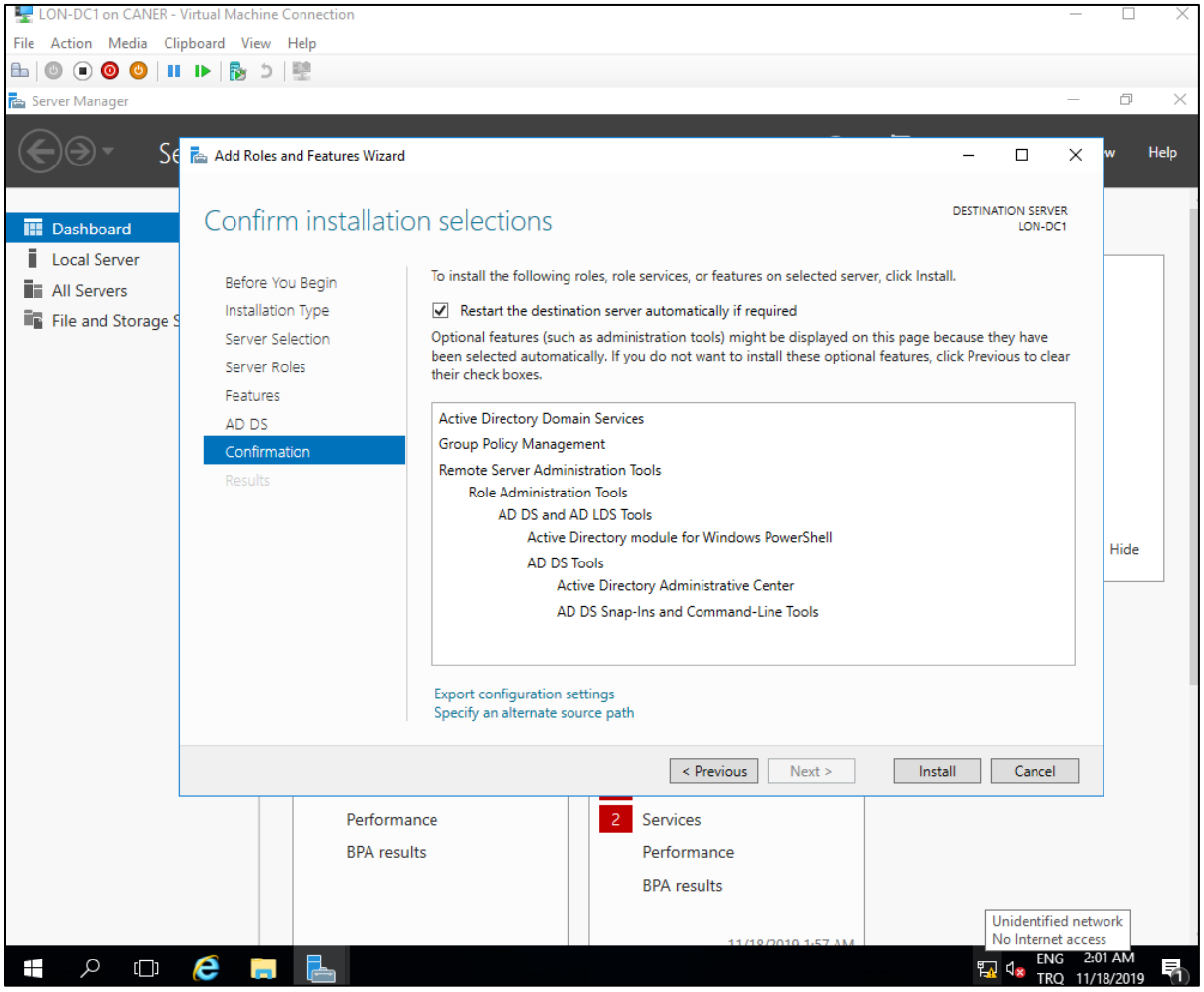
We need a new domain so we start with adding the Active Directory Role on the DC…



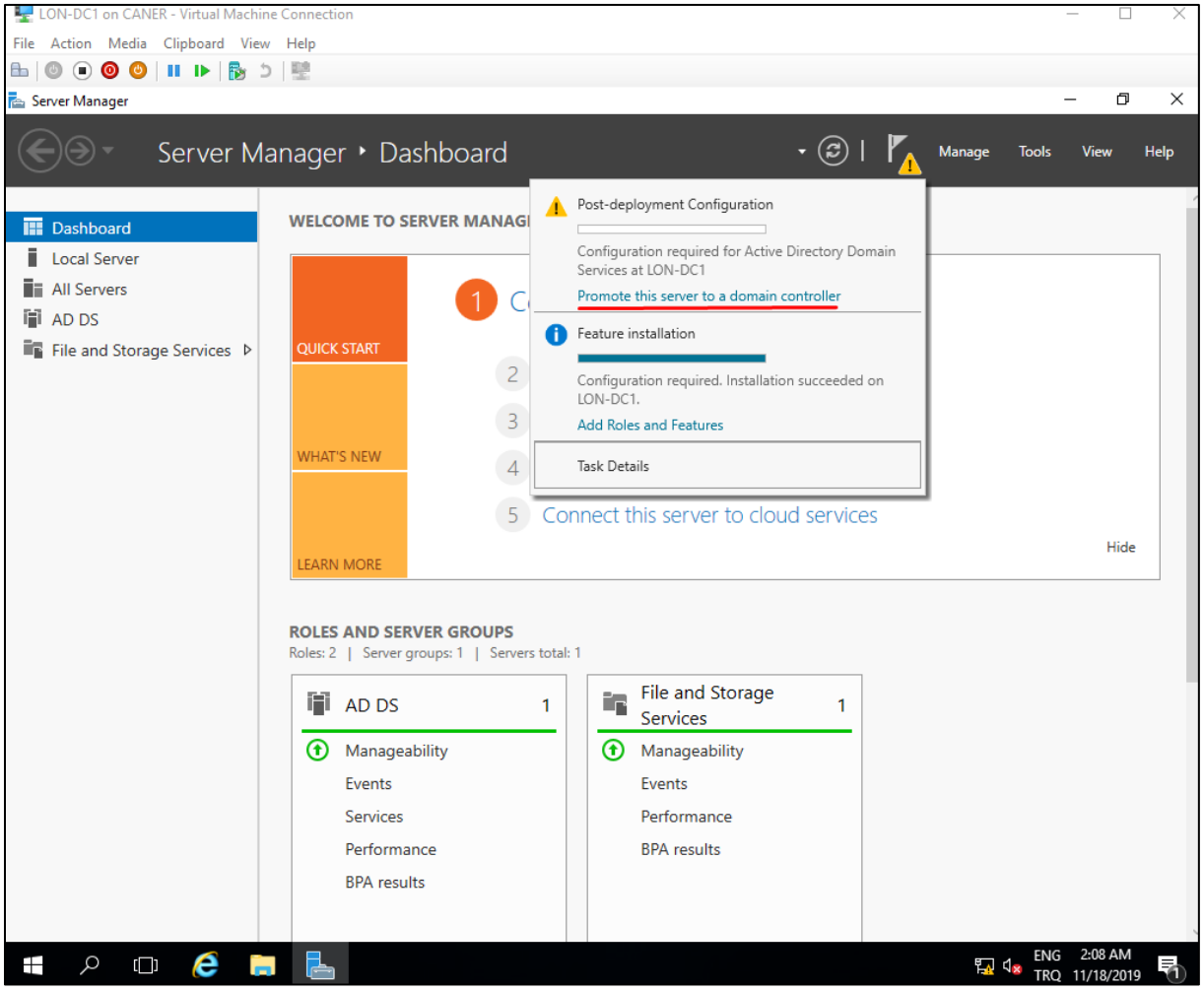
…and no additional features.



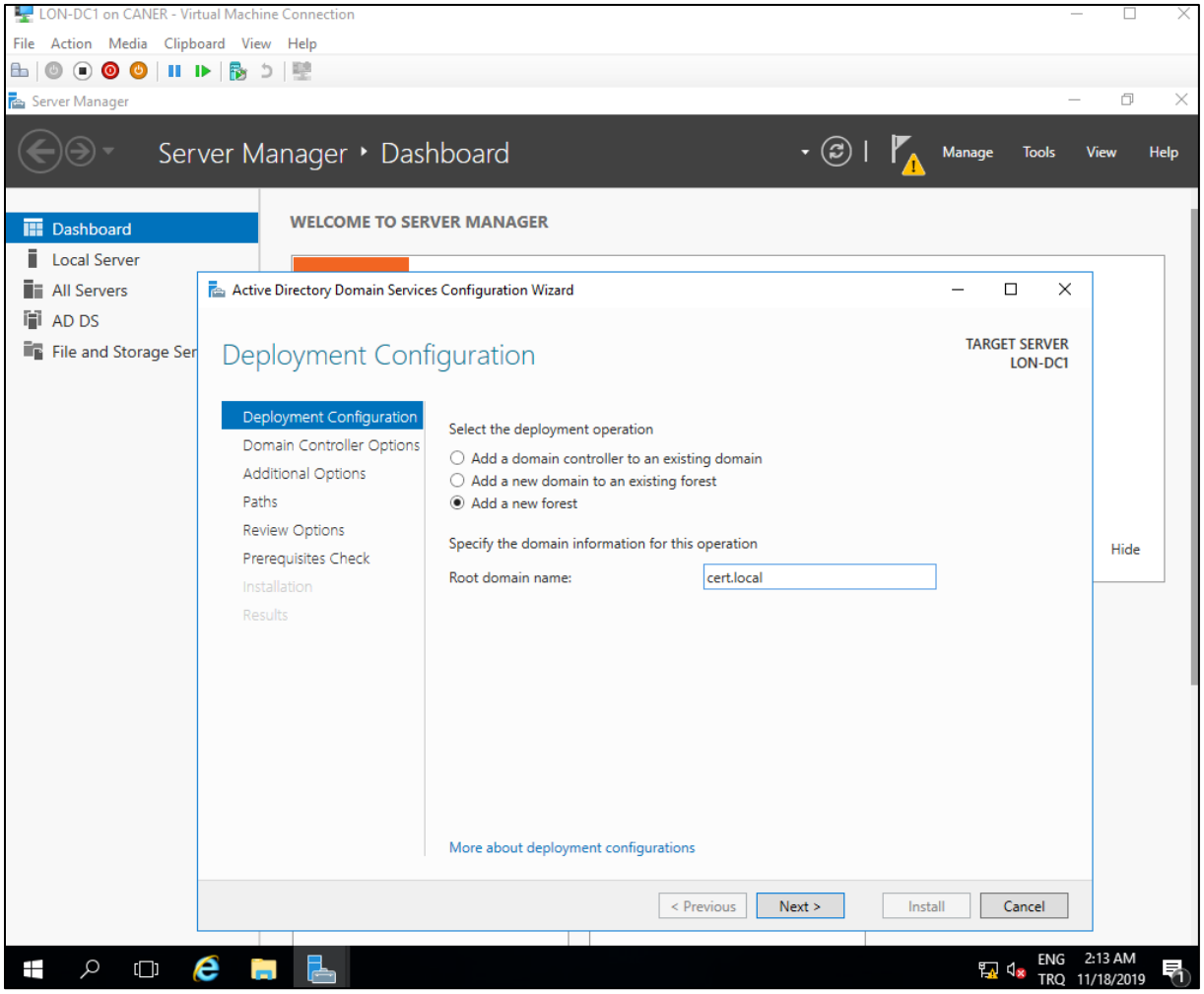
We proceed.


LON-DC1 on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Server Manager
Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
LON-DC1
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD DS
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Active Directory Domain Services
Group Policy Management
Remote Server Administration Tools
Role Administration Tools
AD DS and AD LDS Tools
Active Directory module for Windows PowerShell
AD DS Tools
Active Directory Administrative Center
AD DS Snap-Ins and Command-Line Tools
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel
Dashboard
Local Server
All Servers
File and Storage S
Performance
BPA results
2
Services
Performance
BPA results
Hide
Unidentified network
No Internet access
ENG
TRQ
2:01 AM
11/18/2019

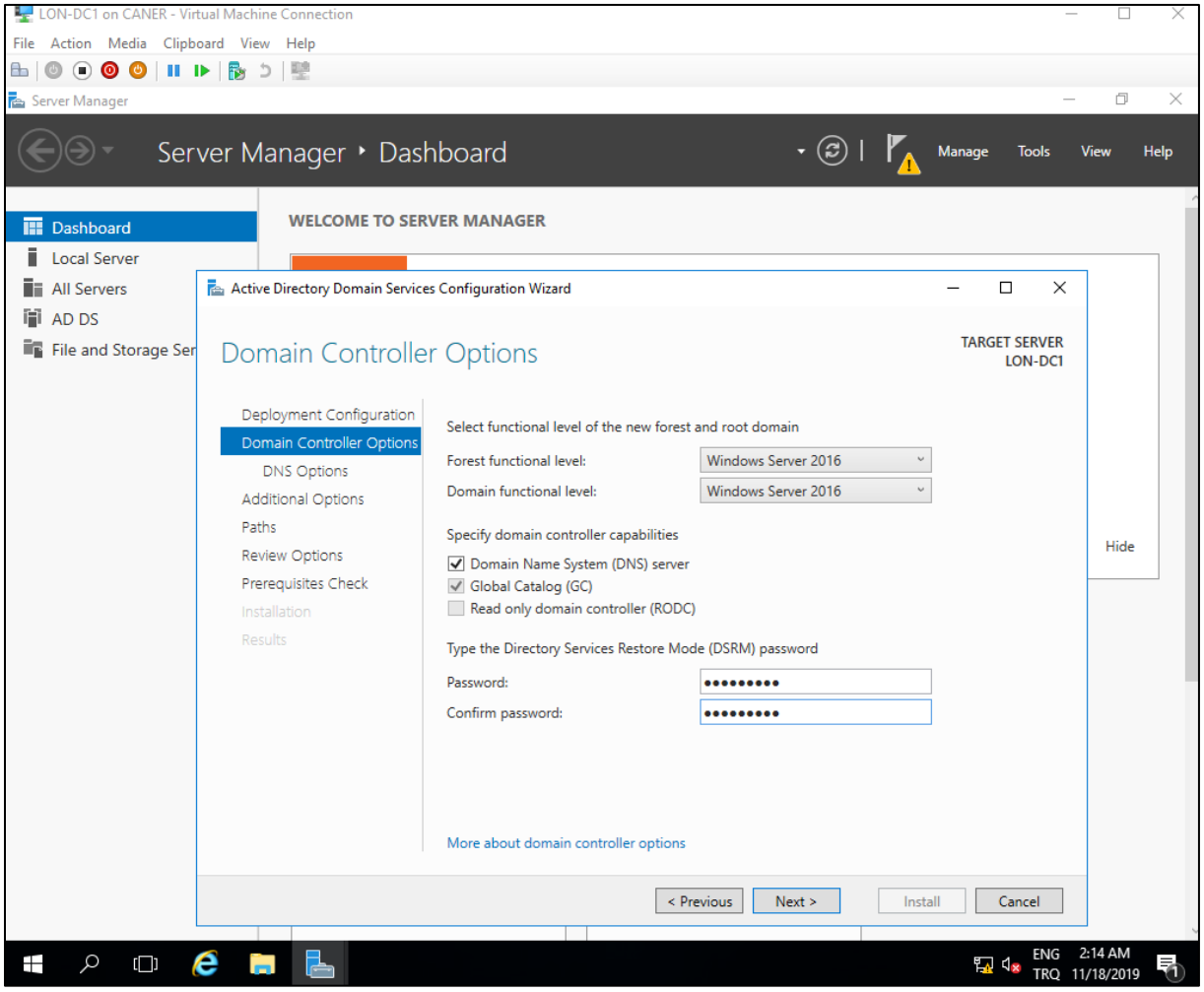
Promote LON-DC1 to Domain Controller.



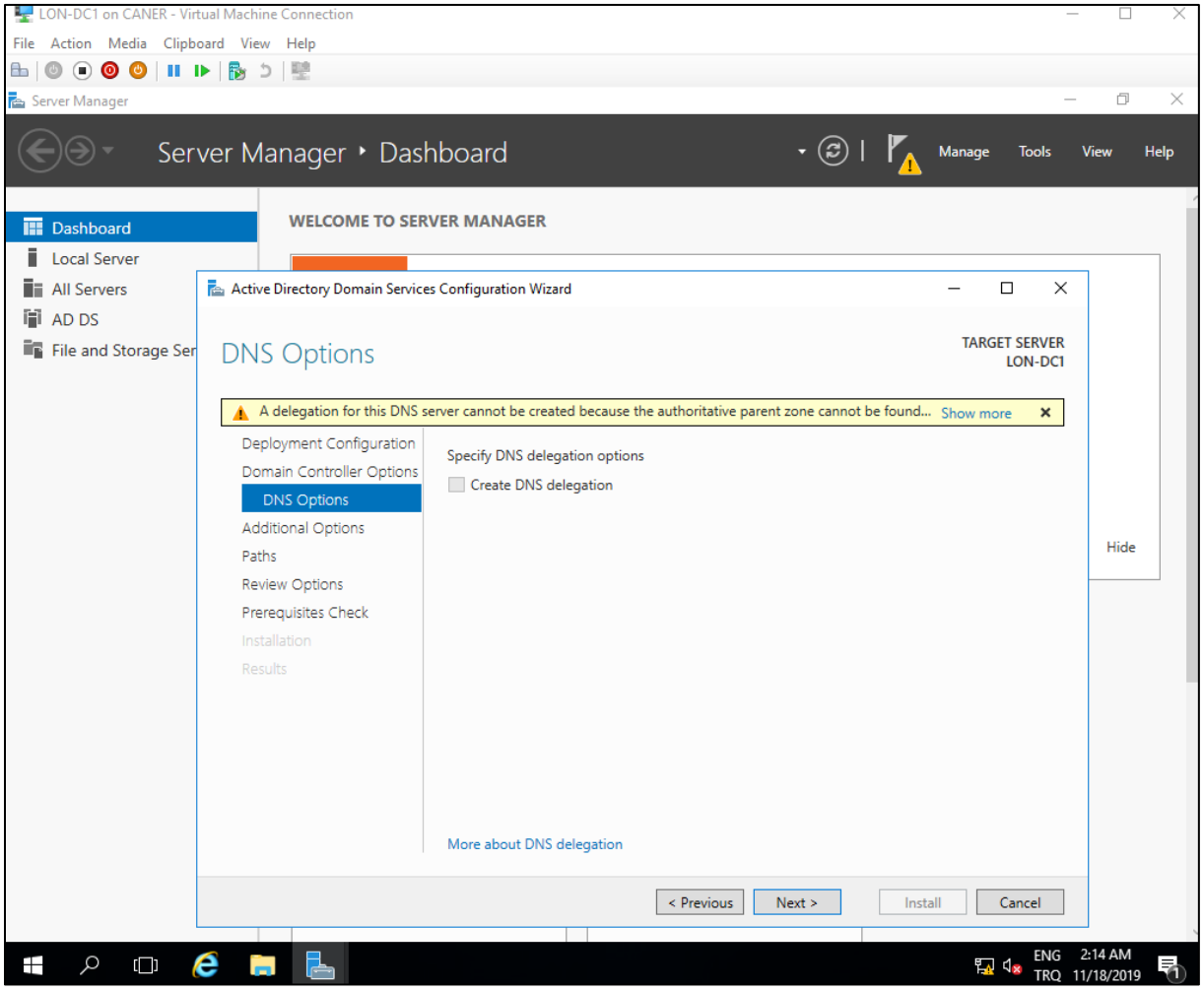
Creating a new forest for our new domain “cert.local”



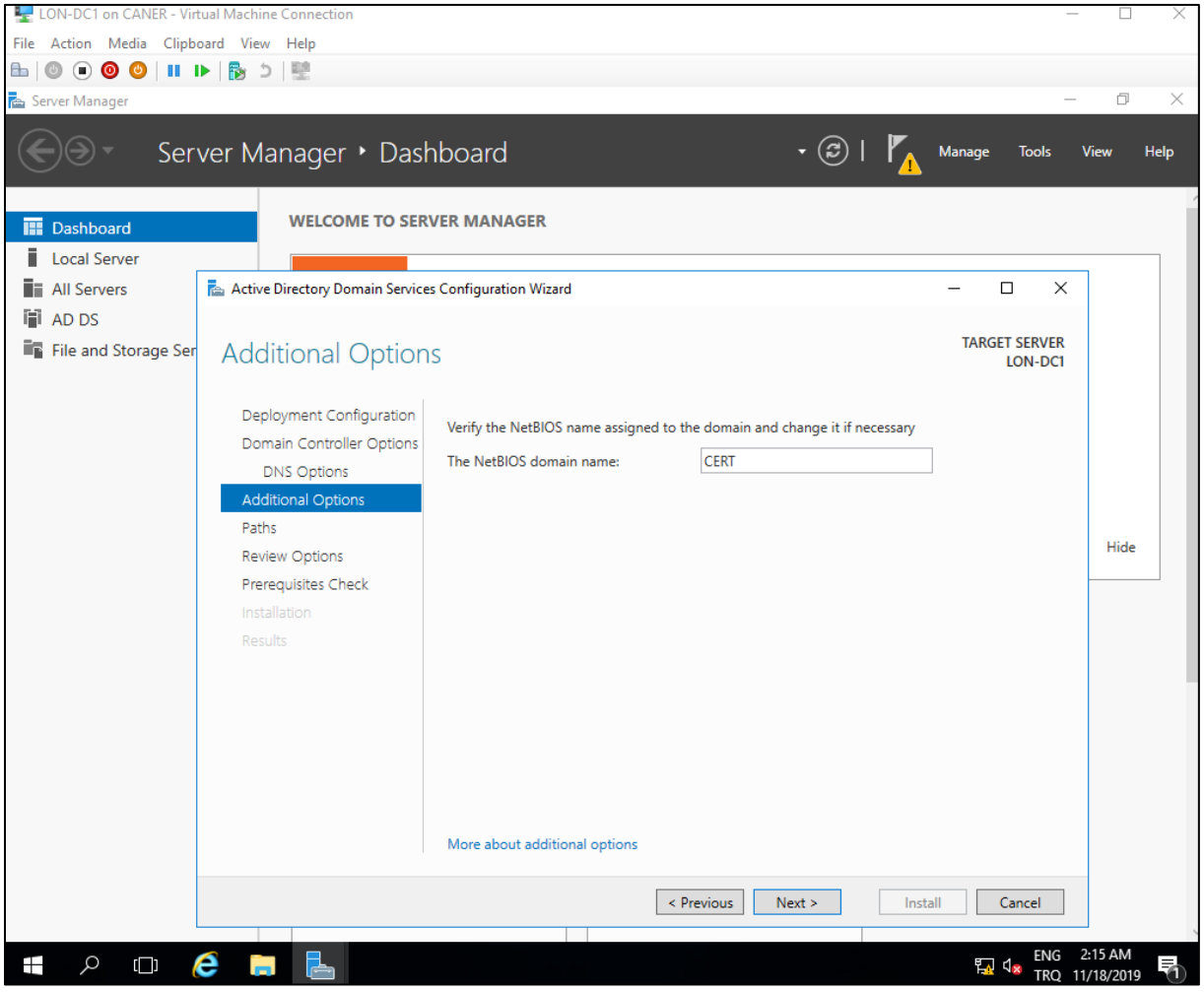
We assign a password to join the domain.



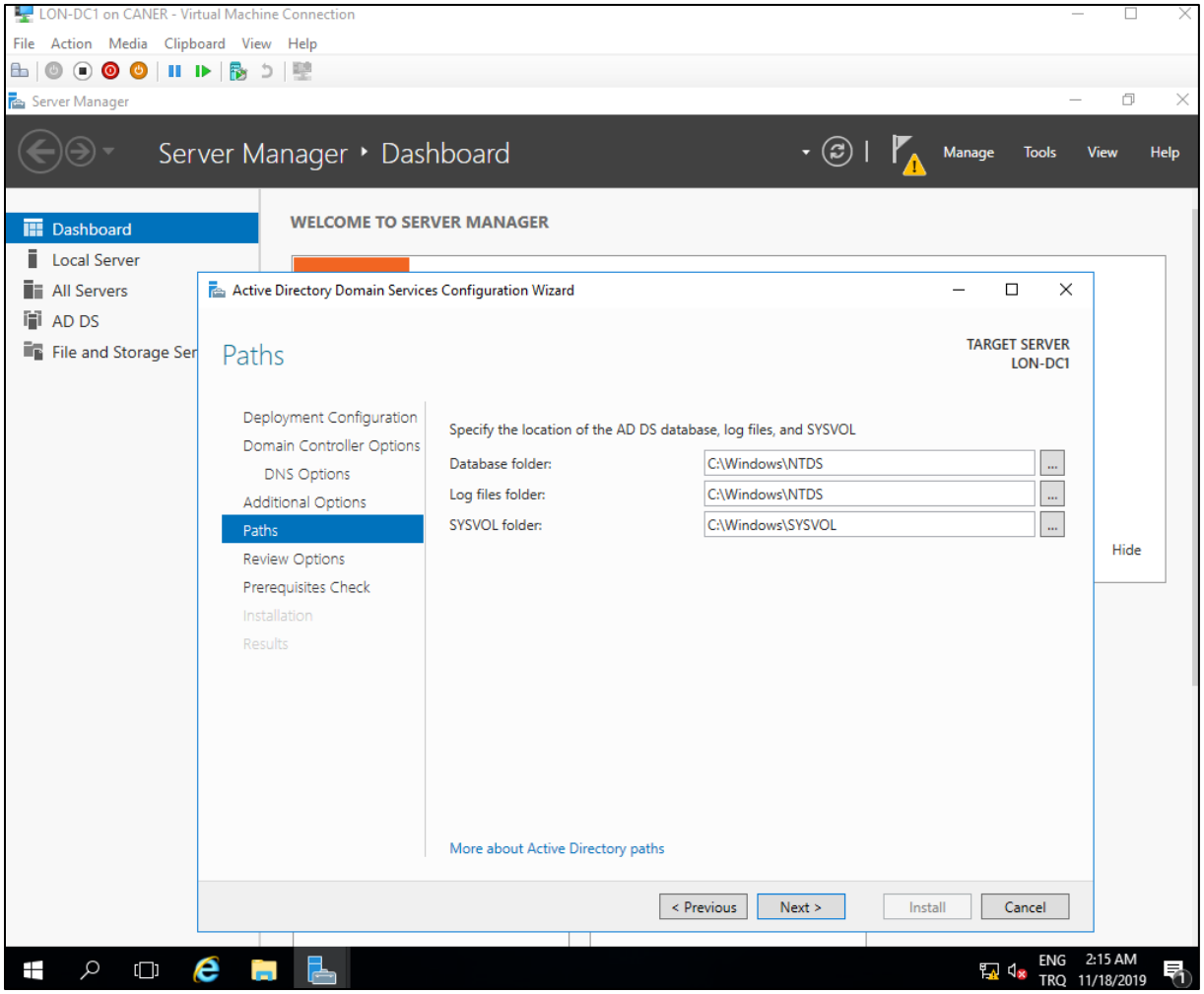
Since this is the root domain we cannot have a DNS delegation.



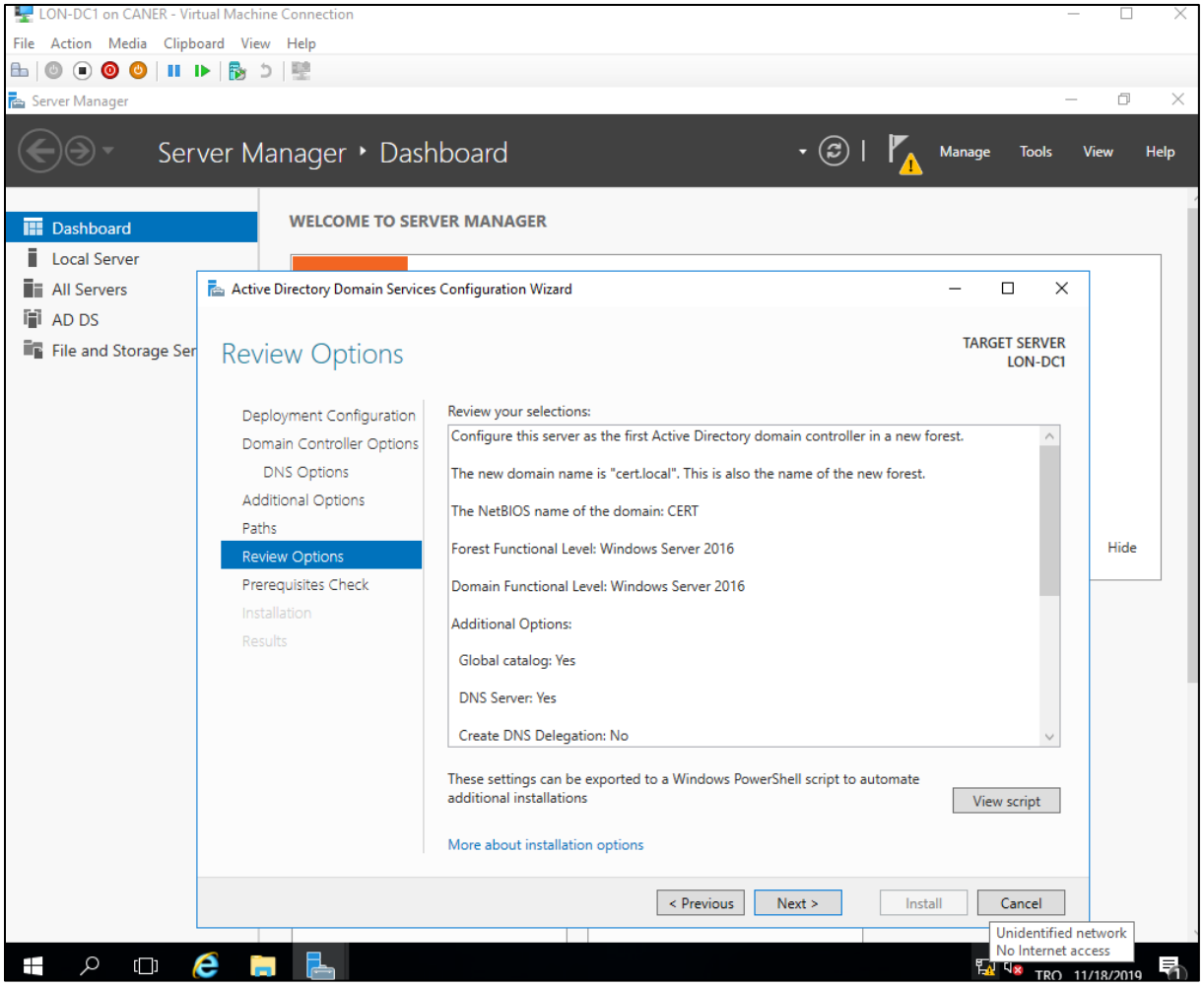
This name is automatically assigned to the domain.



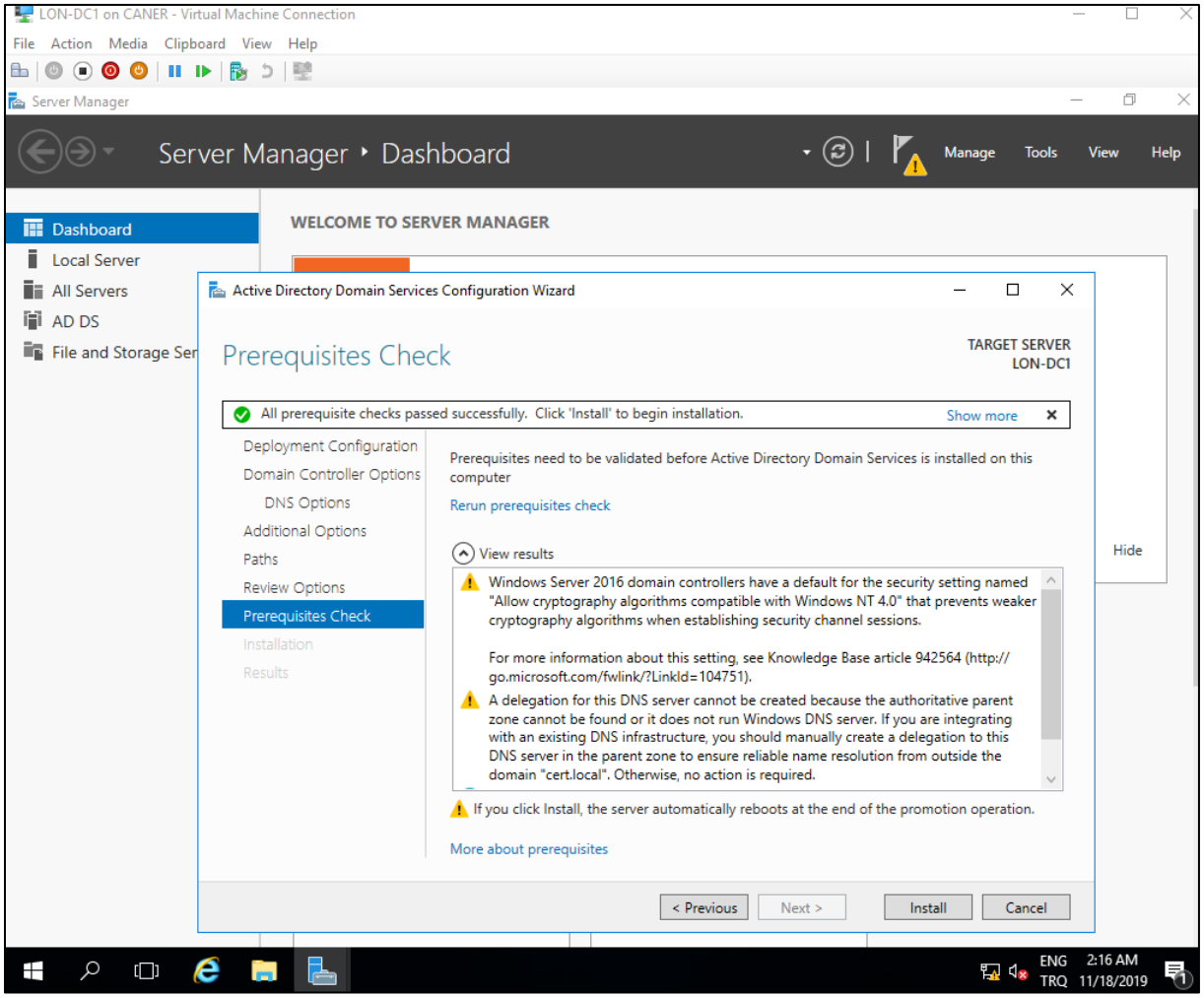
We proceed.


LON-DC1 on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Server Manager
Server Manager • Dashboard
Manage Tools View Help
Dashboard
Local Server
All Servers
AD DS
File and Storage Ser
WELCOME TO SERVER MANAGER
Active Directory Domain Services Configuration Wizard
Paths
TARGET SERVER
LON-DC1
Deployment Configuration
Domain Controller Options
DNS Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Specify the location of the AD DS database, log files, and SYSVOL
Database folder:
C:\Windows\NTDS
Log files folder:
C:\Windows\NTDS
SYSVOL folder:
C:\Windows\SYSVOL
Hide
More about Active Directory paths
< Previous
Next >
Install
Cancel
ENG
TRQ
2:15 AM
11/18/2019

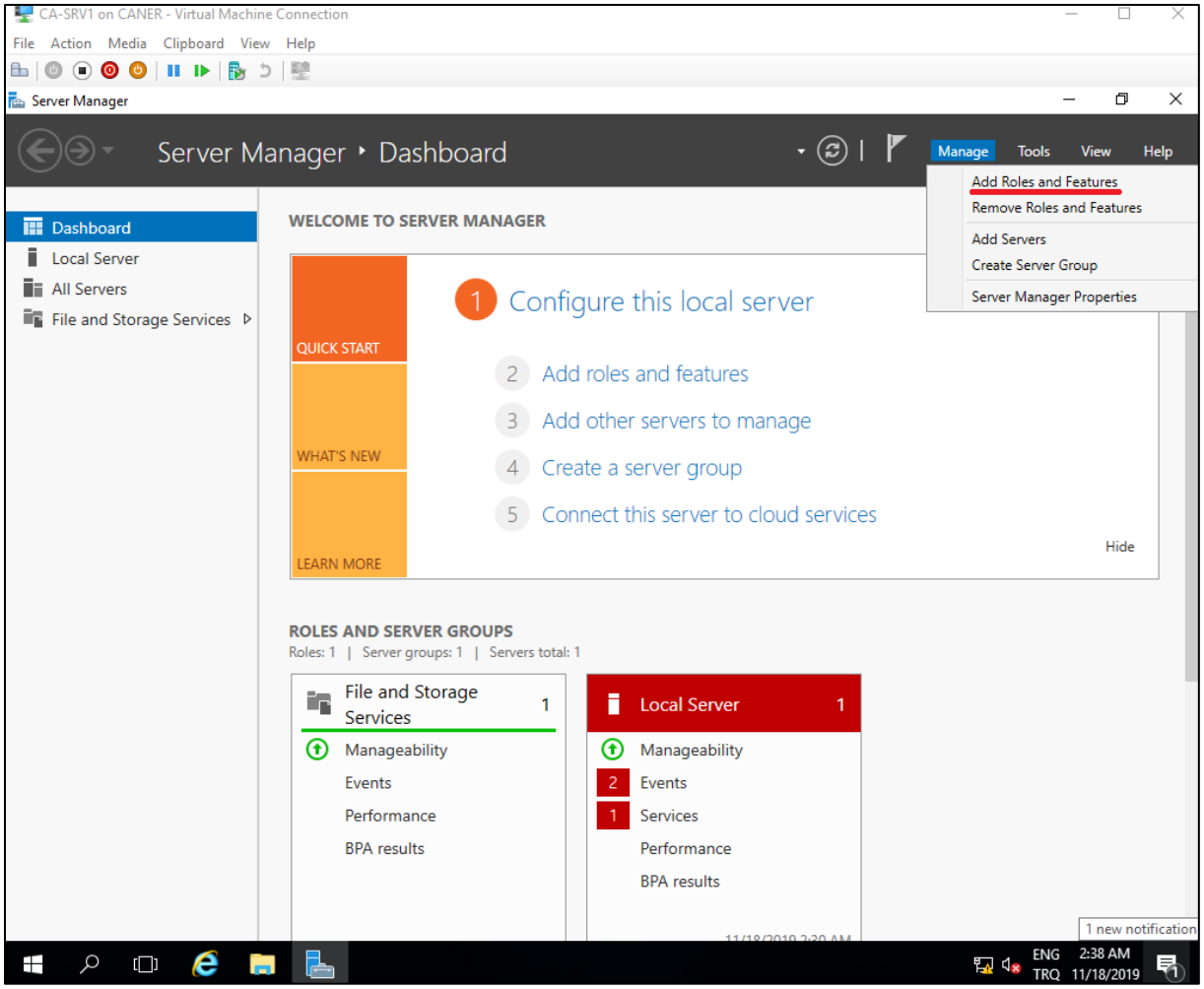
We simply click on Next again.



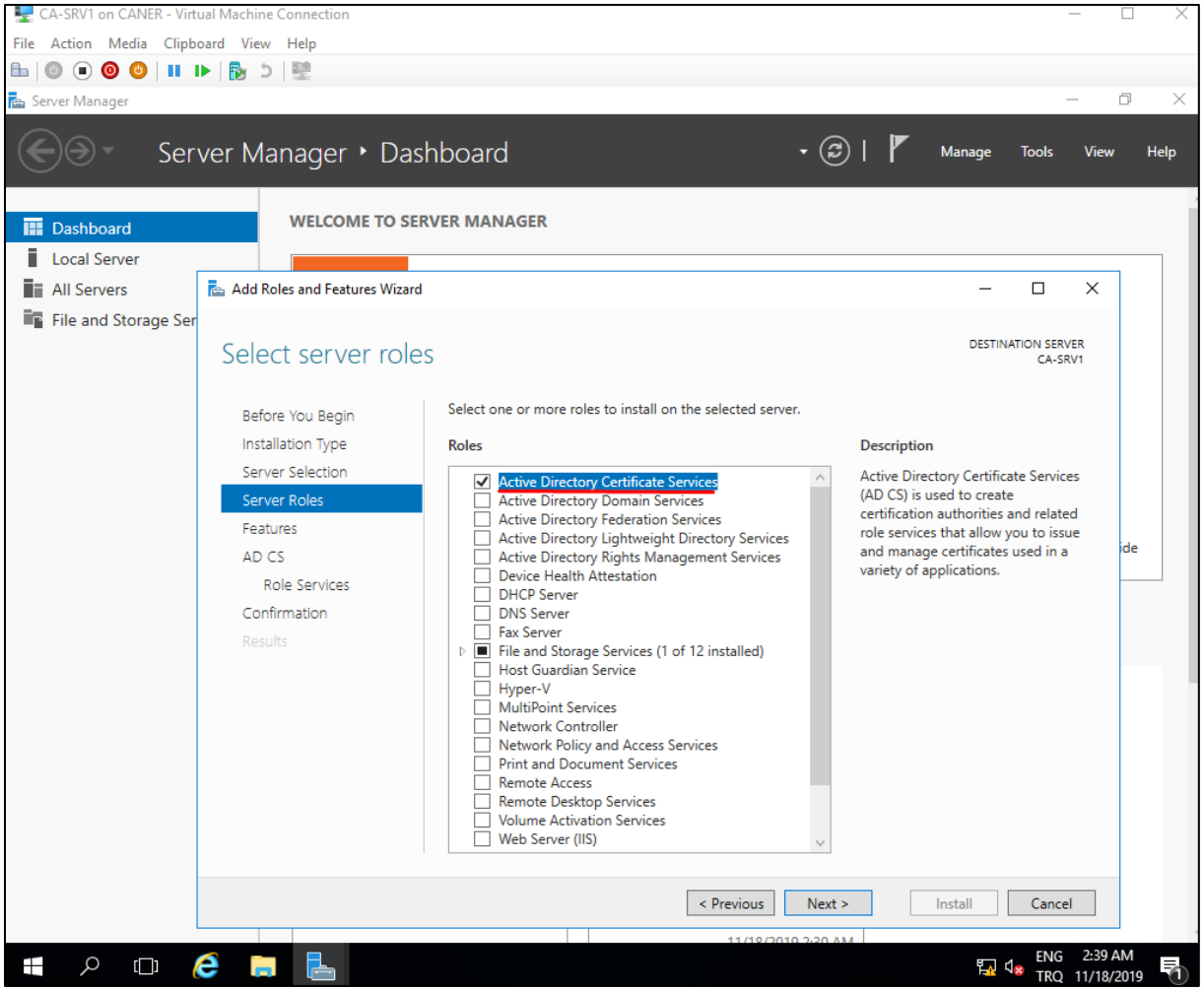
We finish promoting LON-DC1 to Domain Controller.



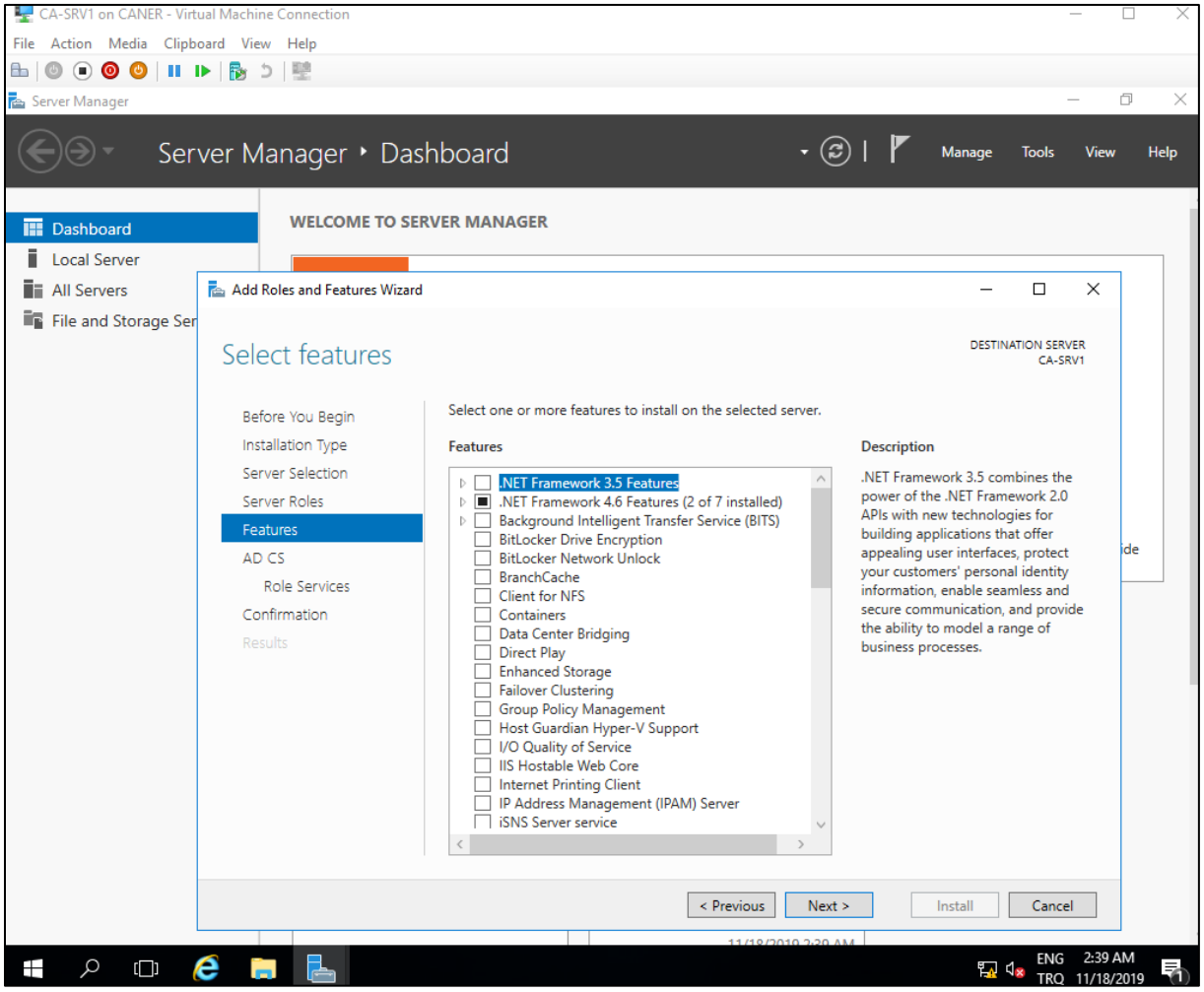
Then, we move on to CA-SRV1 and add a new role.



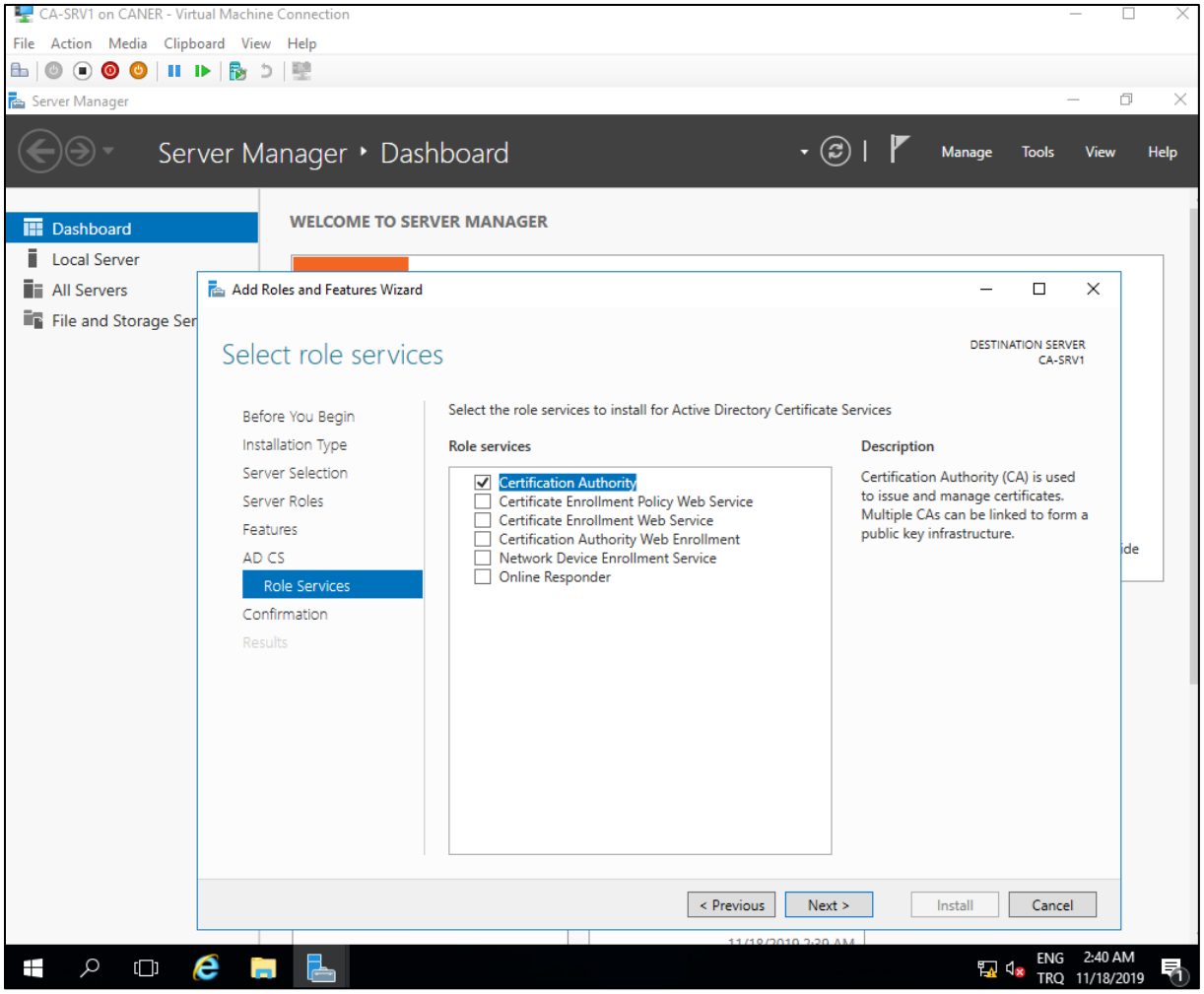
The new role is Active Directory Certificate Services.



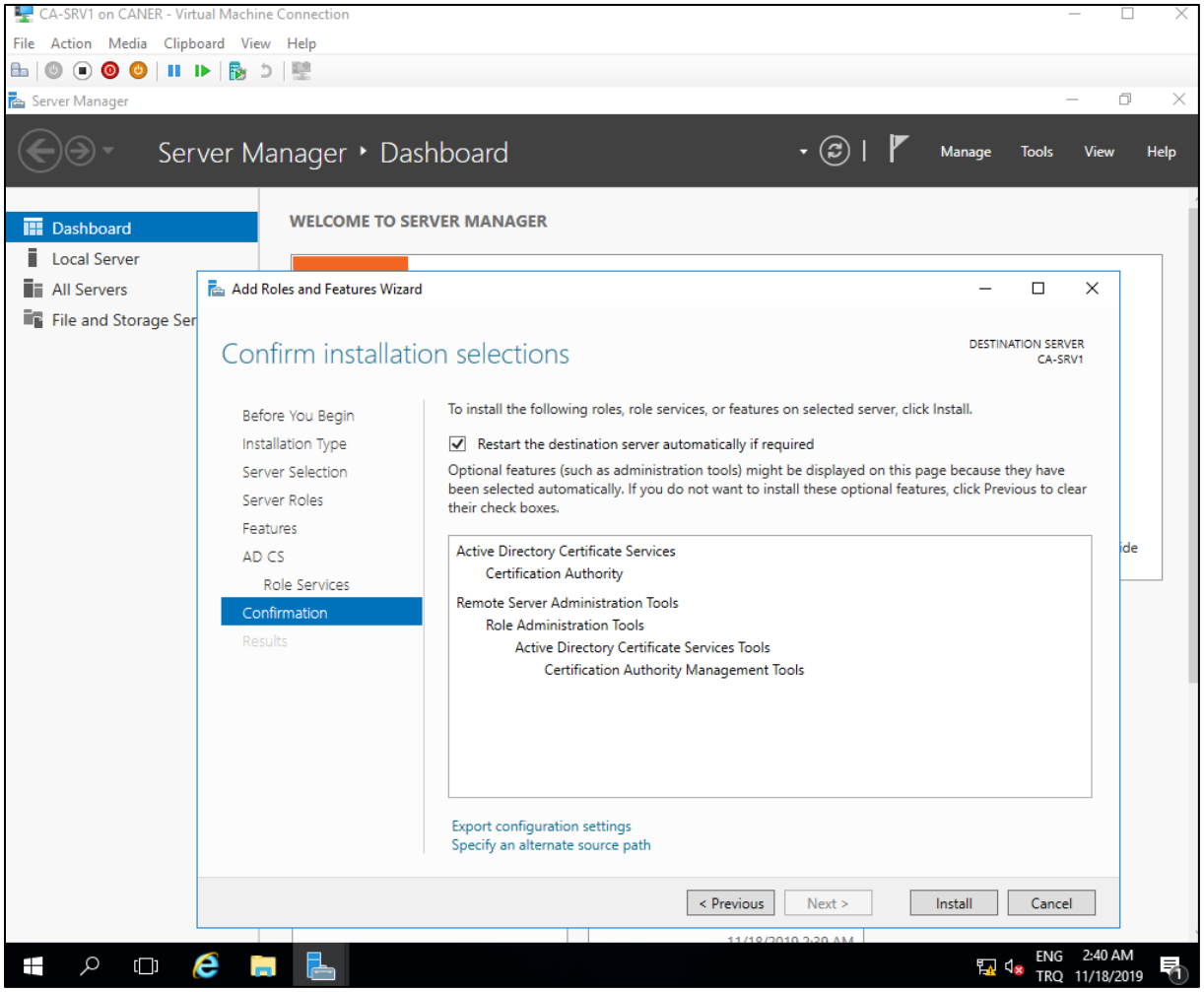
And we add no features.



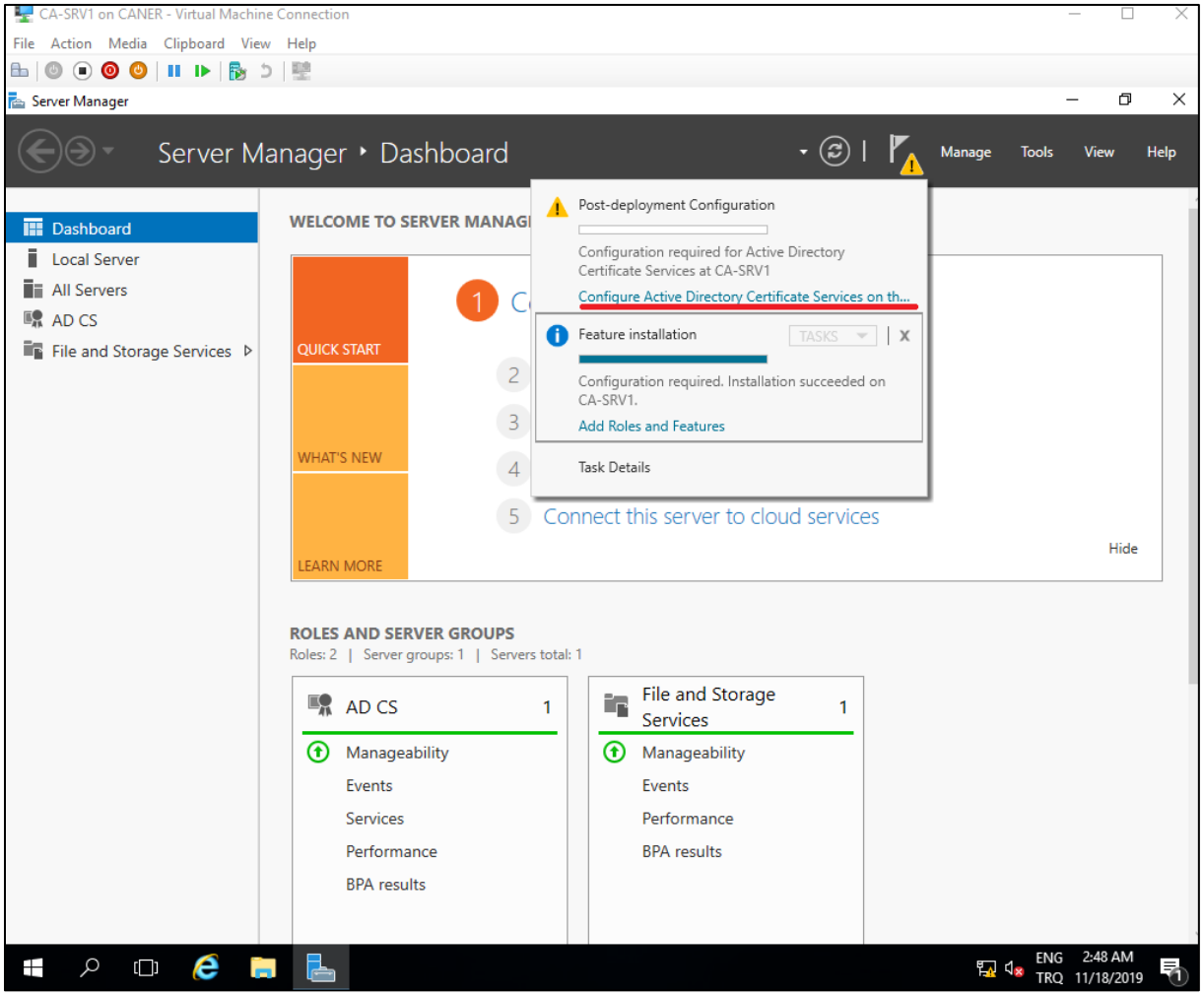
The Certificate Service Role we need to add is Certificate Authority.



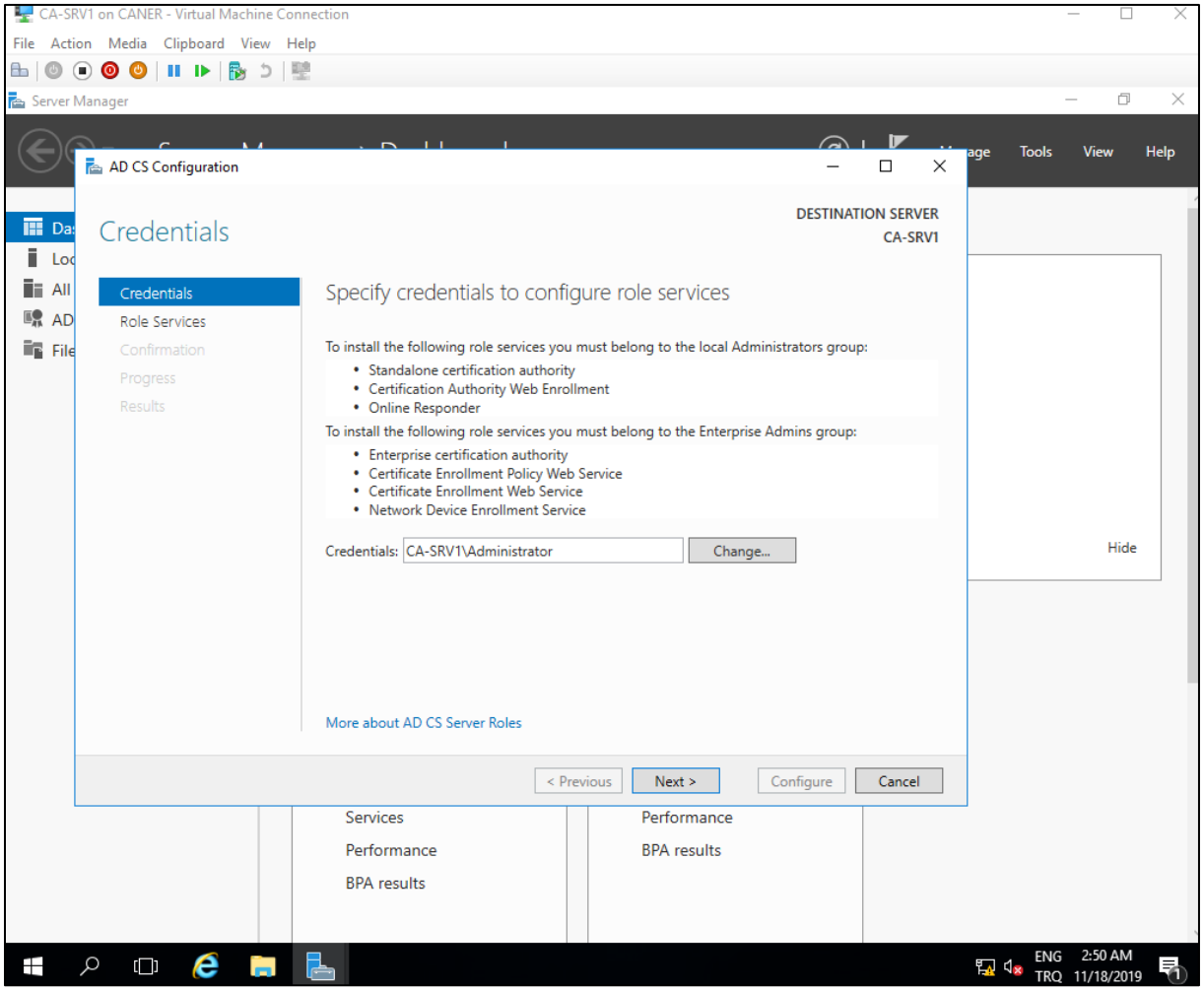
We finalize this process.



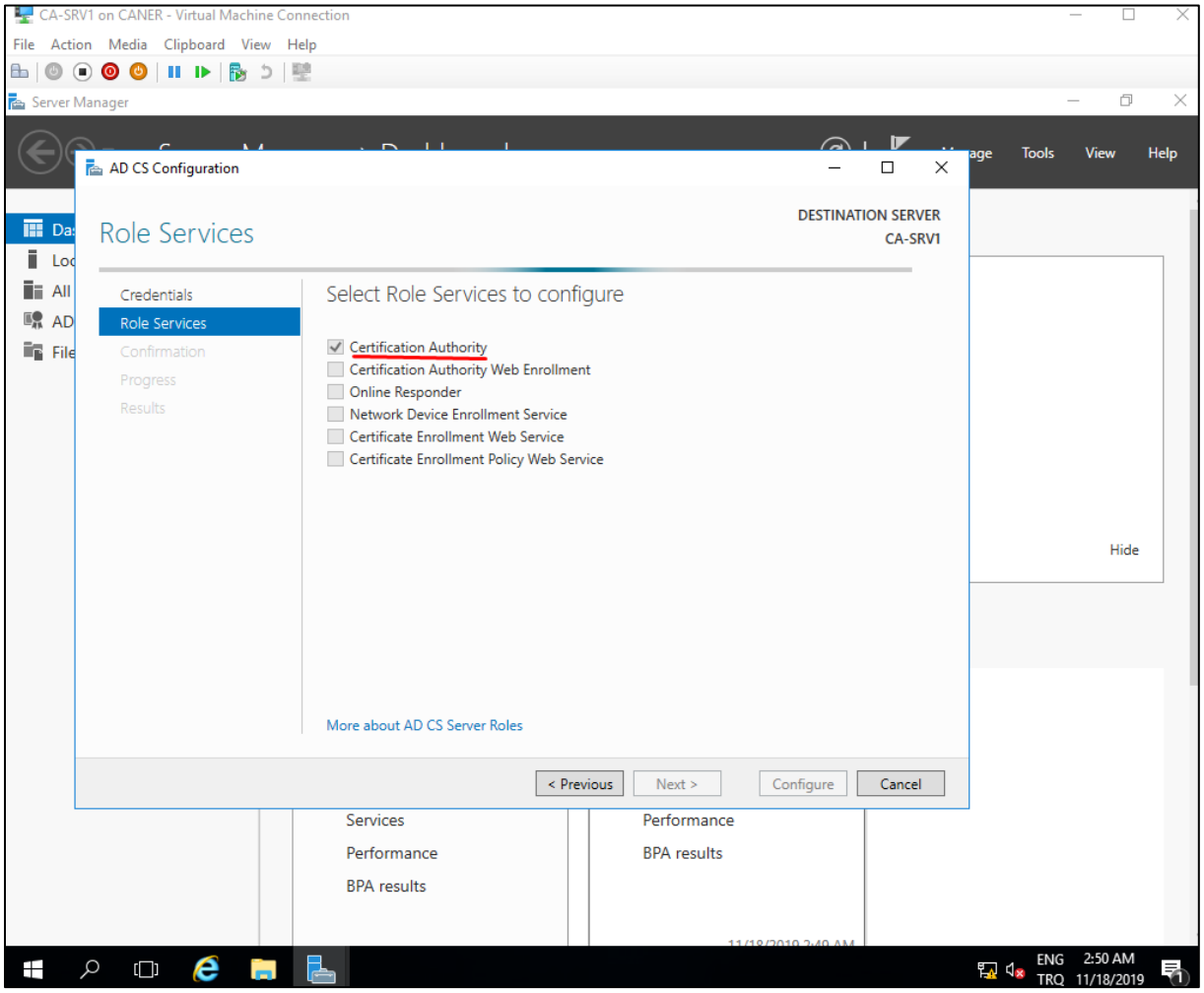
We start the configuration of the CA on CA-SRV1.



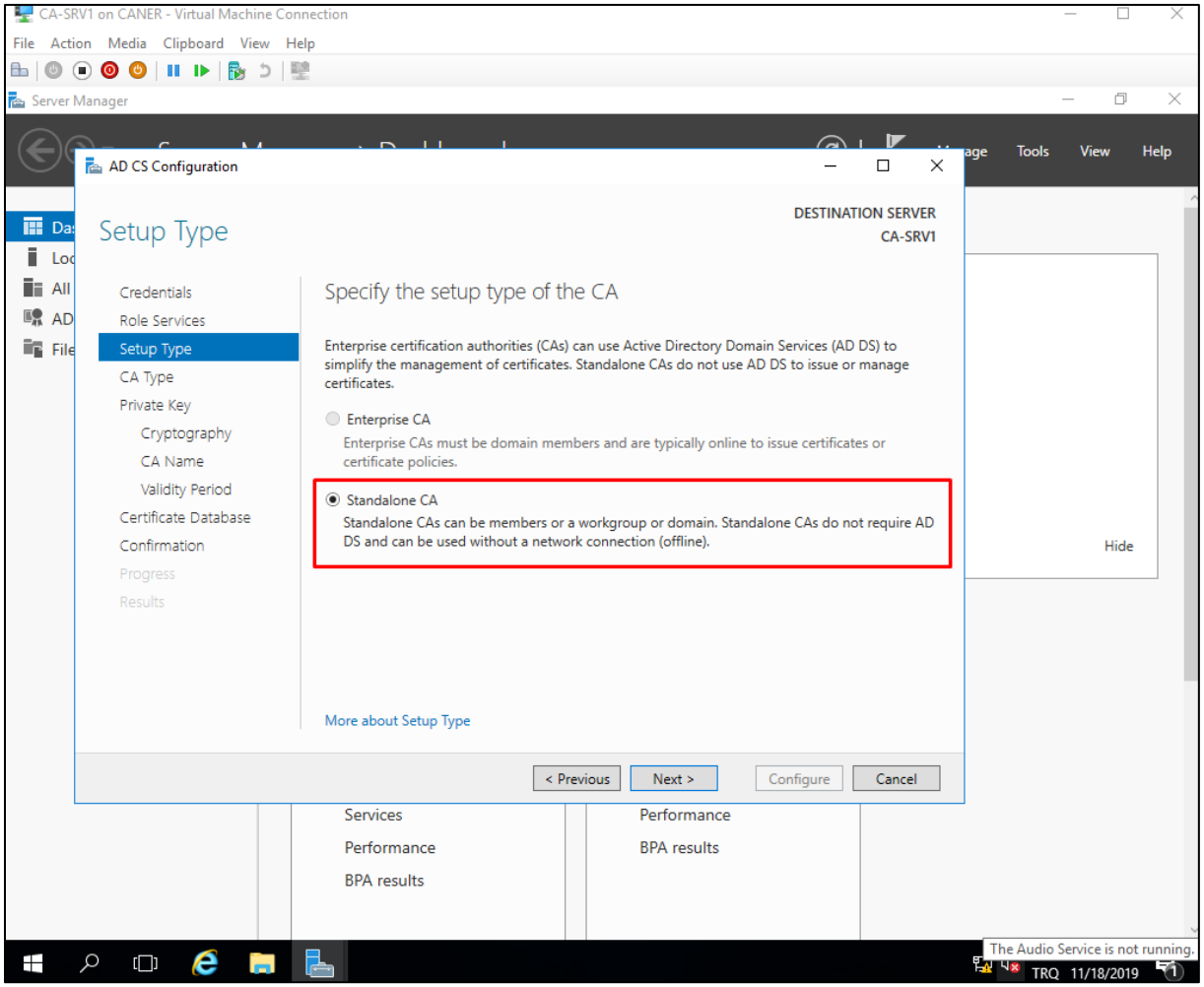
The credentials are assigned automatically.



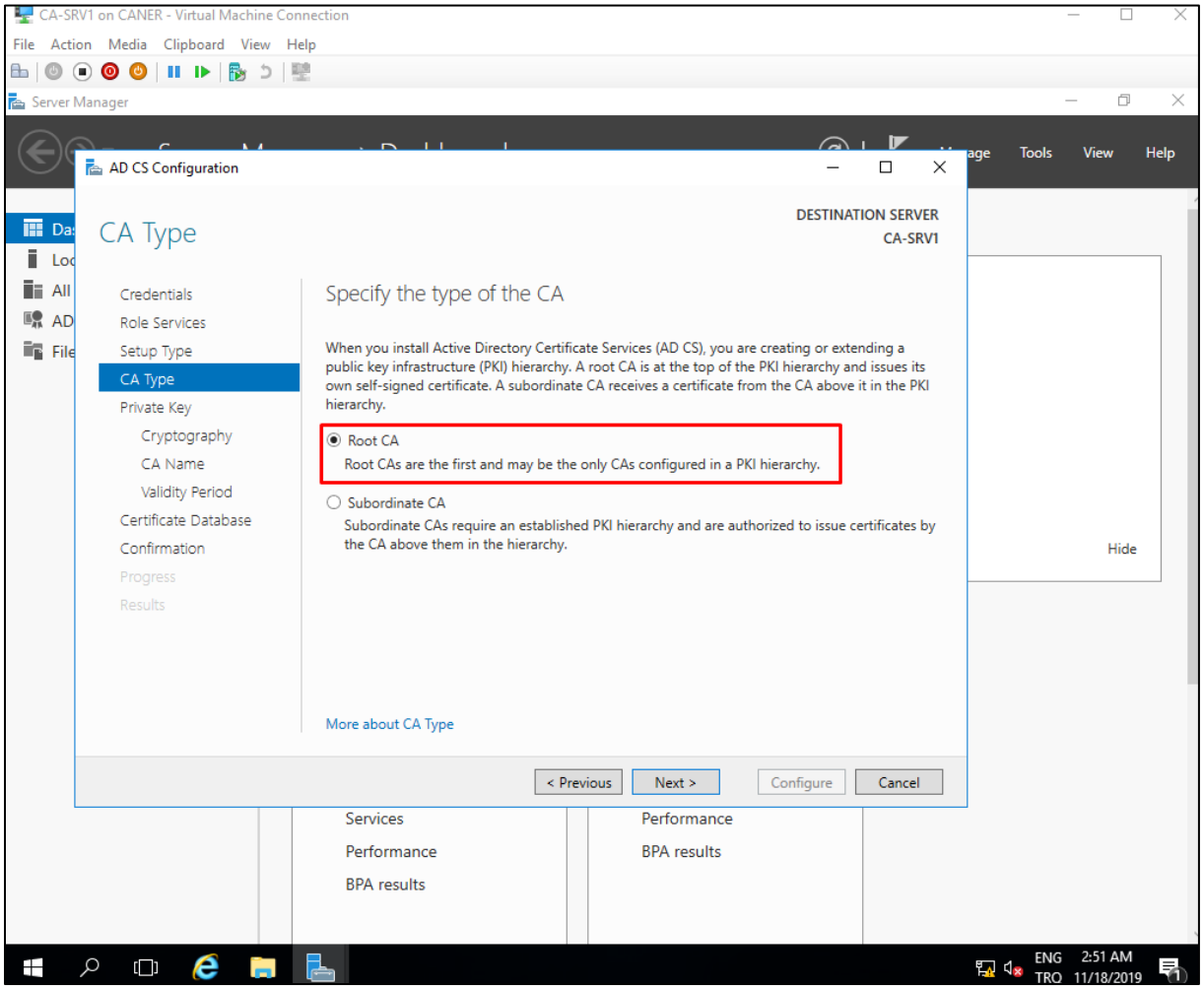
We select Certification Authority. Note that all other options are grayed out since we didn't add the other roles.



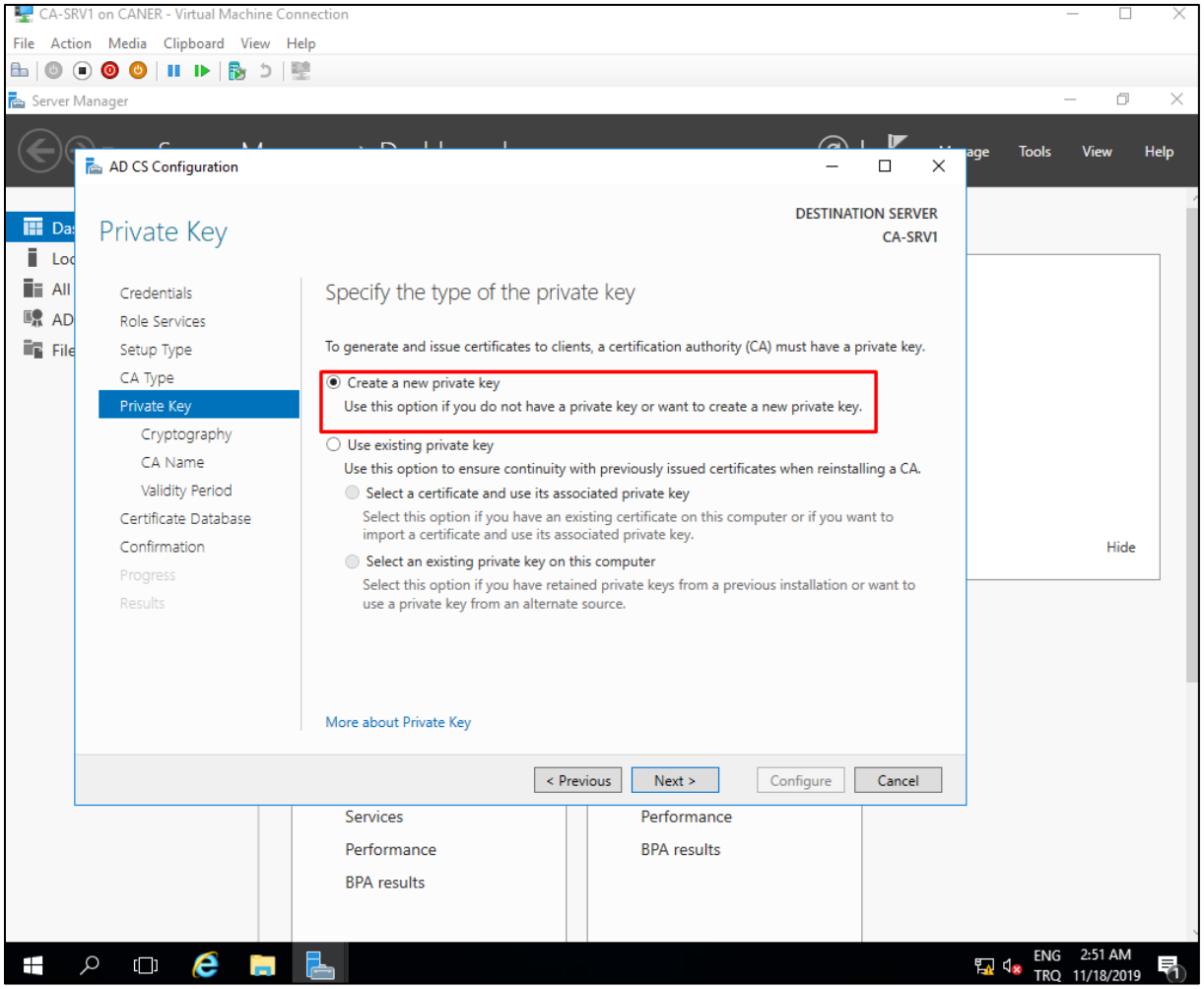
We select Standalone CA. As CA-SRV1 isn't in the domain, Enterprise option is grayed out.



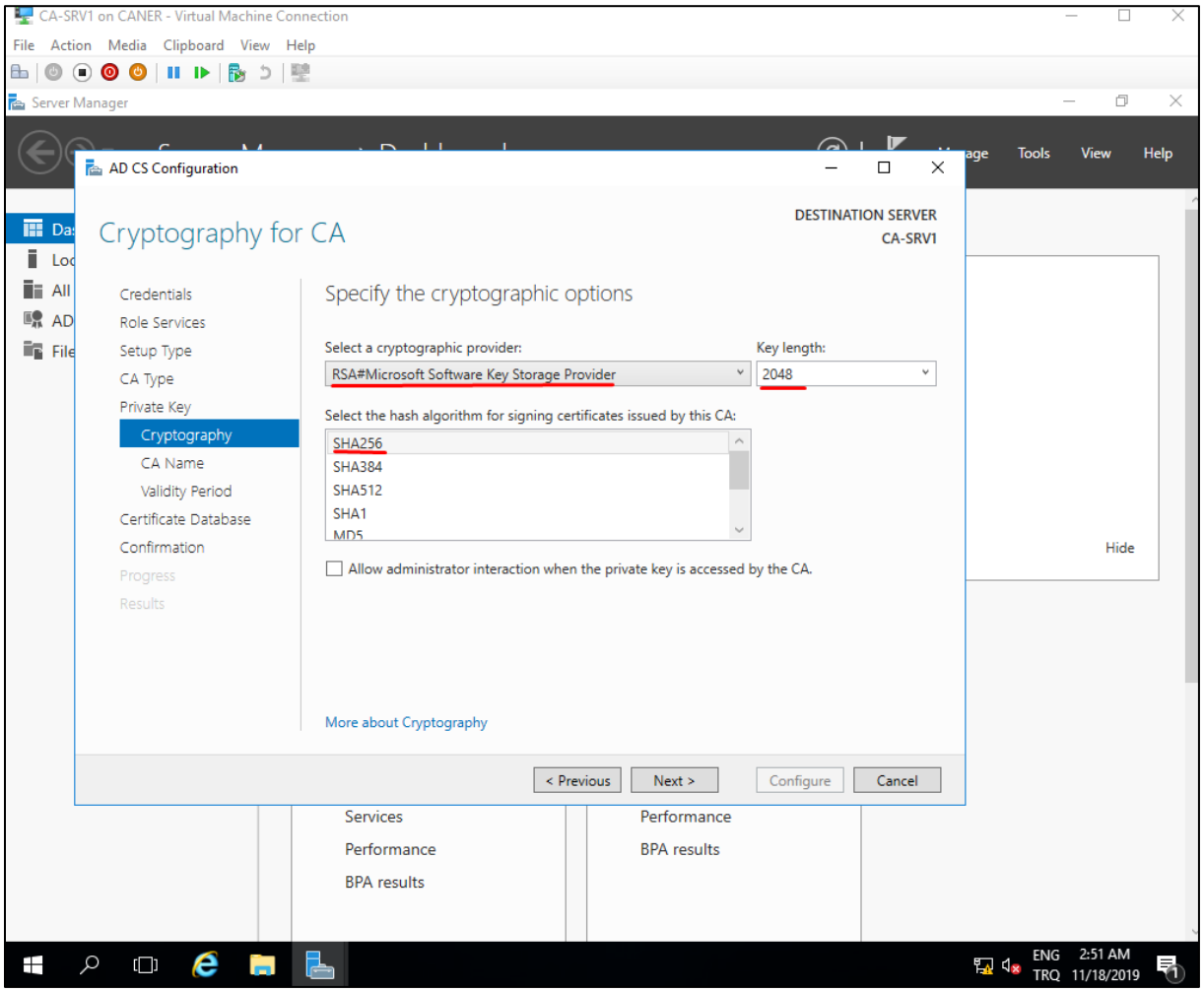
We select Root CA as we will be creating the certificates with this server. Subordinate CA would mean we simply distribute certificates created by another server which is the Root CA.



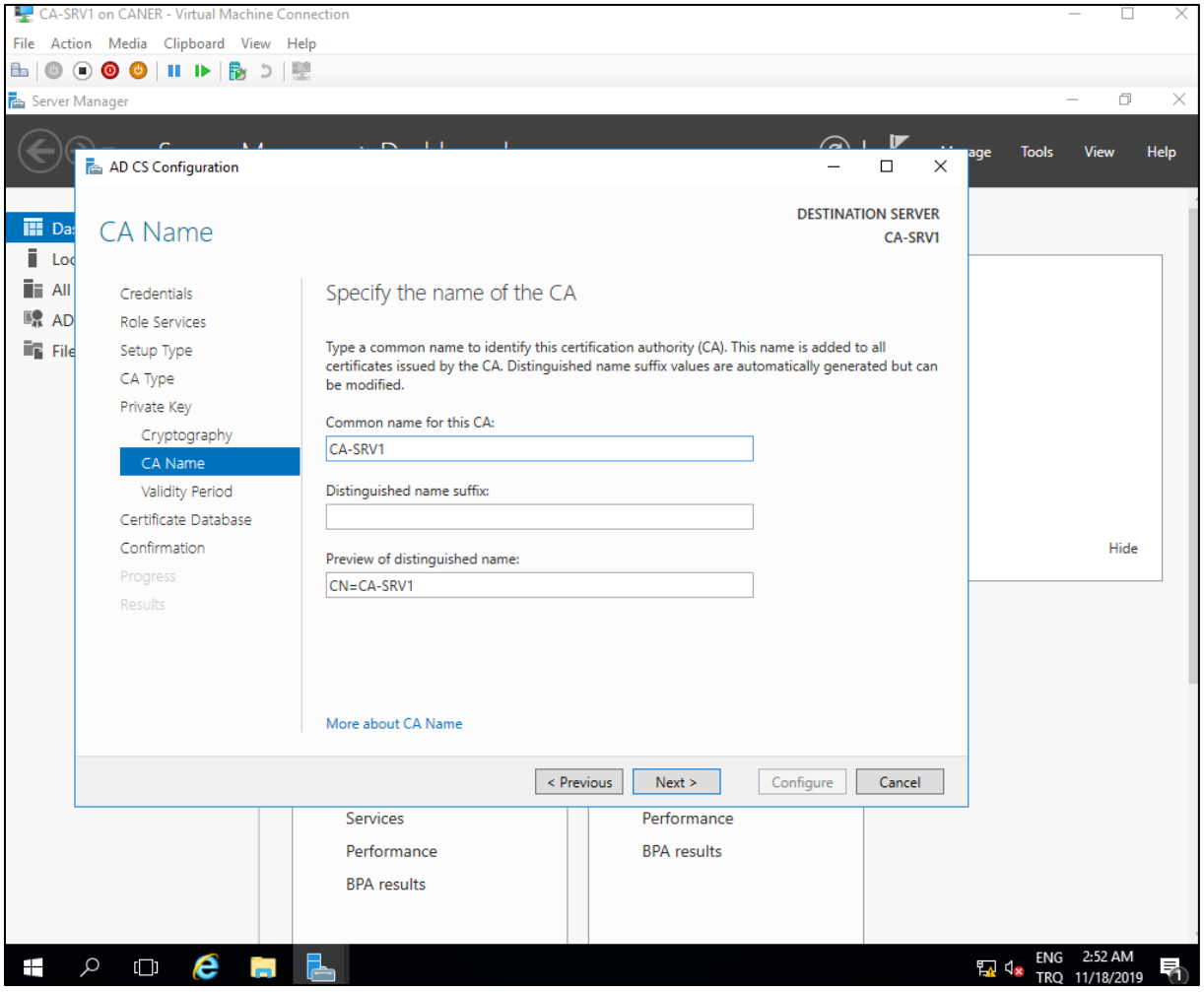
We create a new private key.



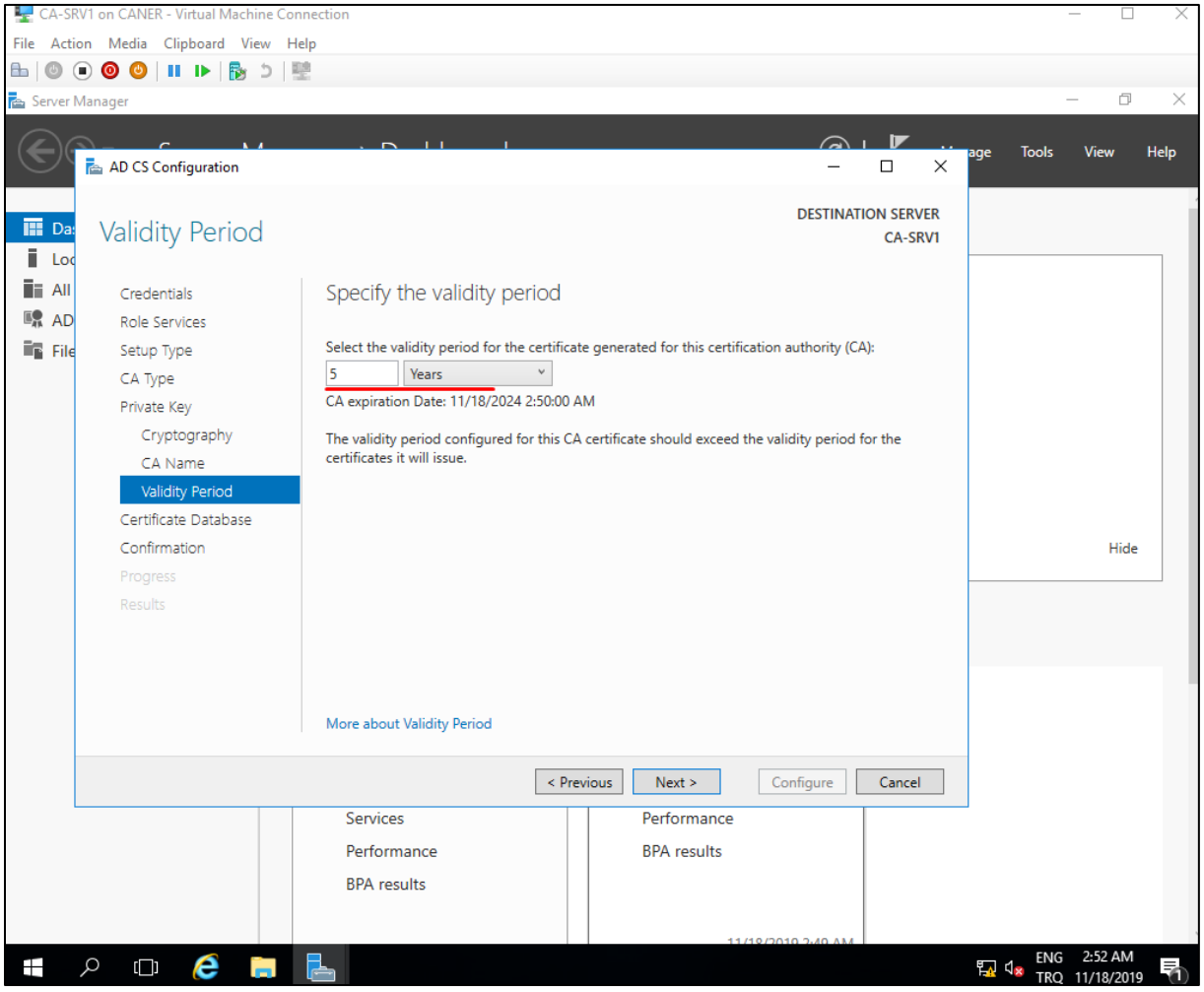
The recommended settings for the cryptography of CA are key length of 4096, but 2048 is sufficient; hash algorithm of SHA256 and cryptographic provider of RSA#Microsoft Software Key Storage Provider.



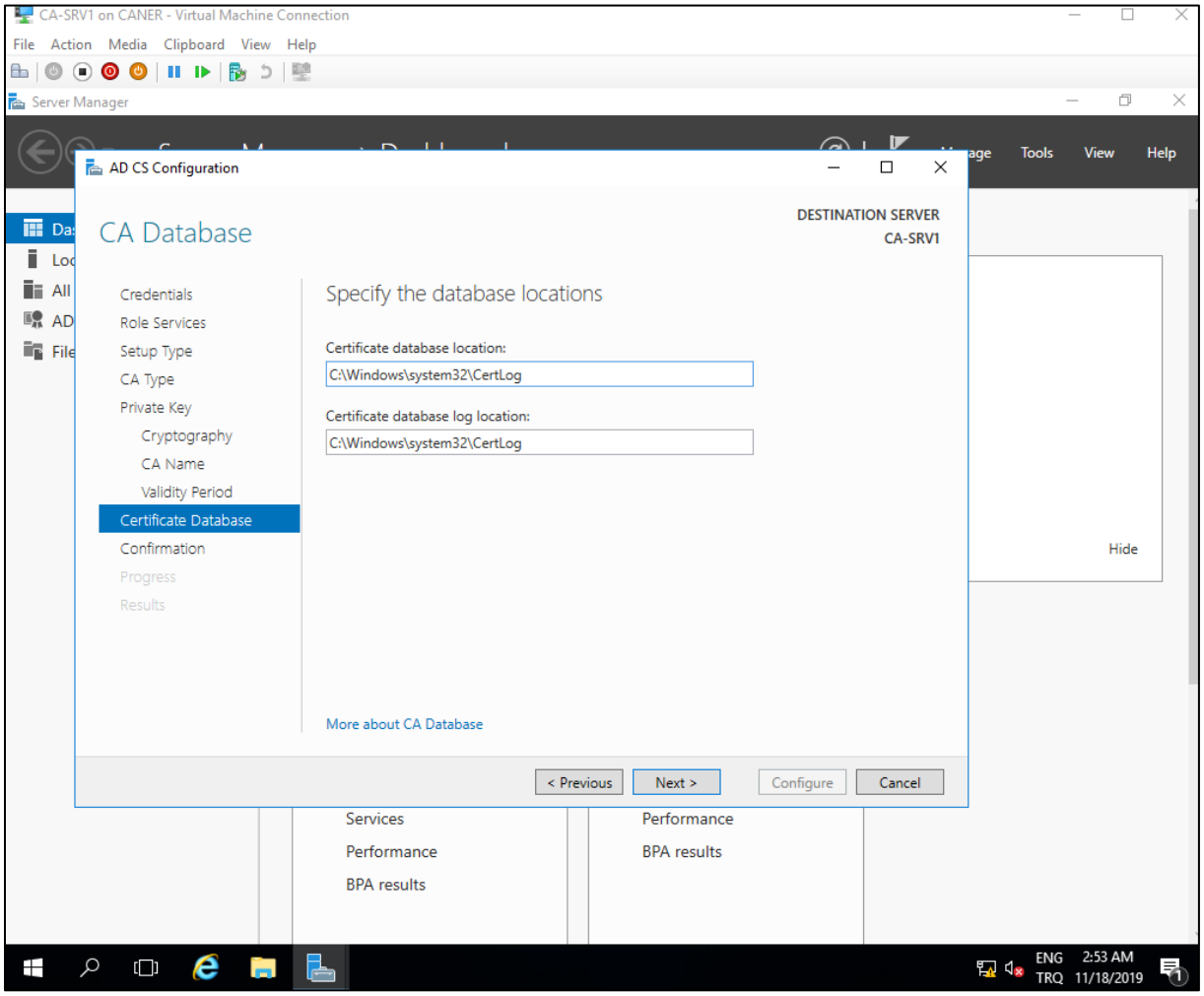
We proceed with the automatic naming schemes.



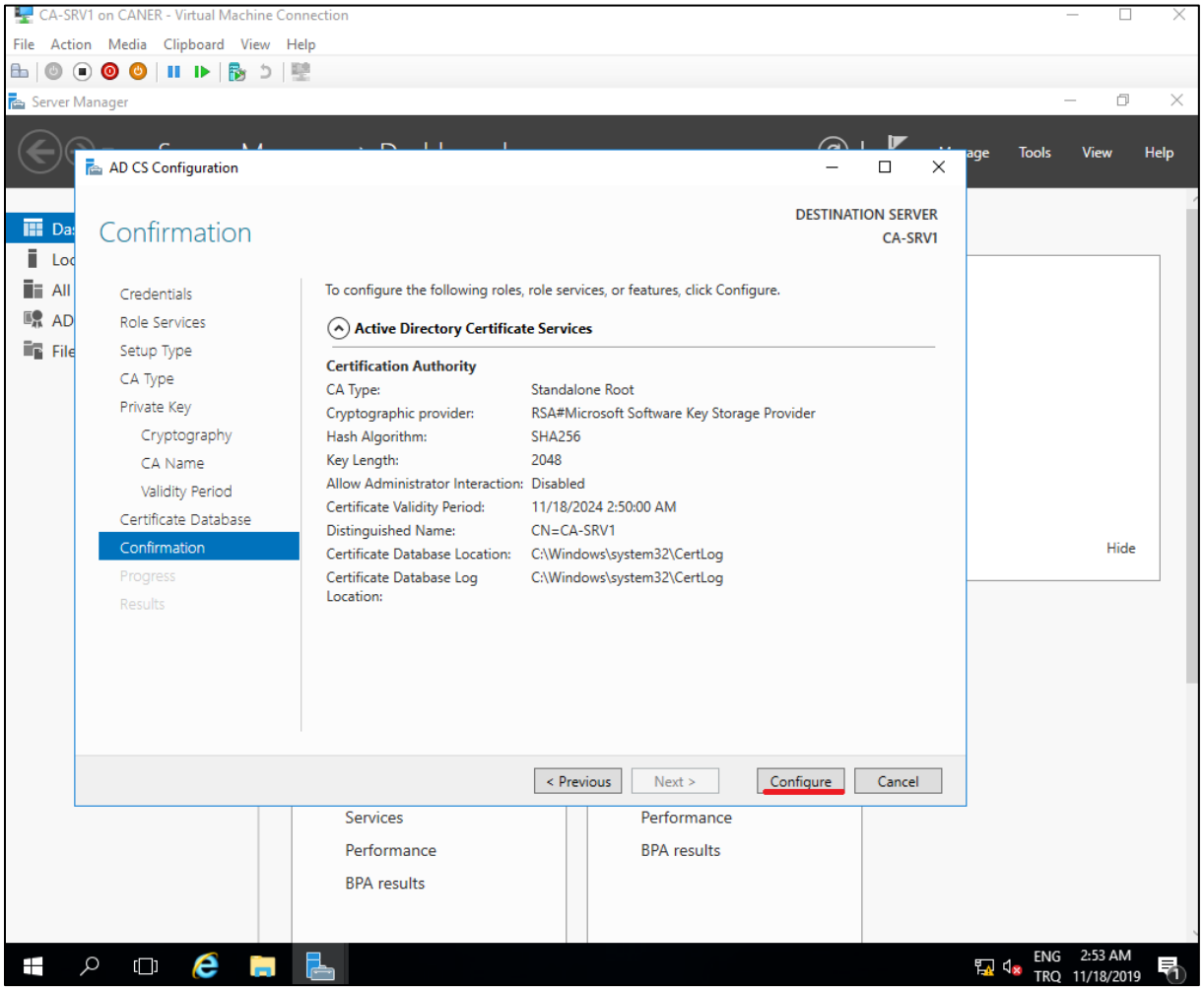
We choose how long we want the certificate to be valid.



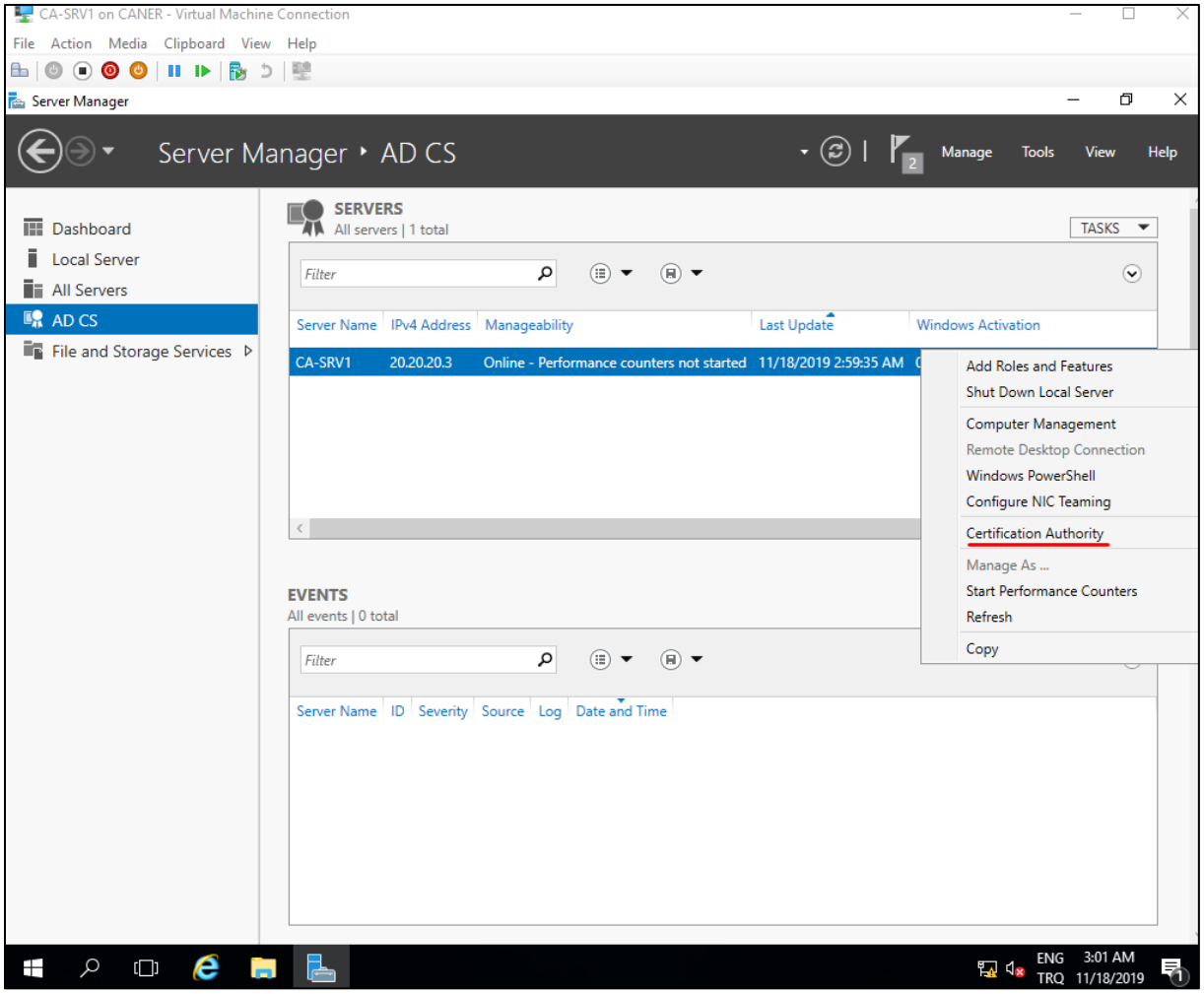
We recommend not changing the default storage paths as it would complicate the troubleshooting in case of an error later.



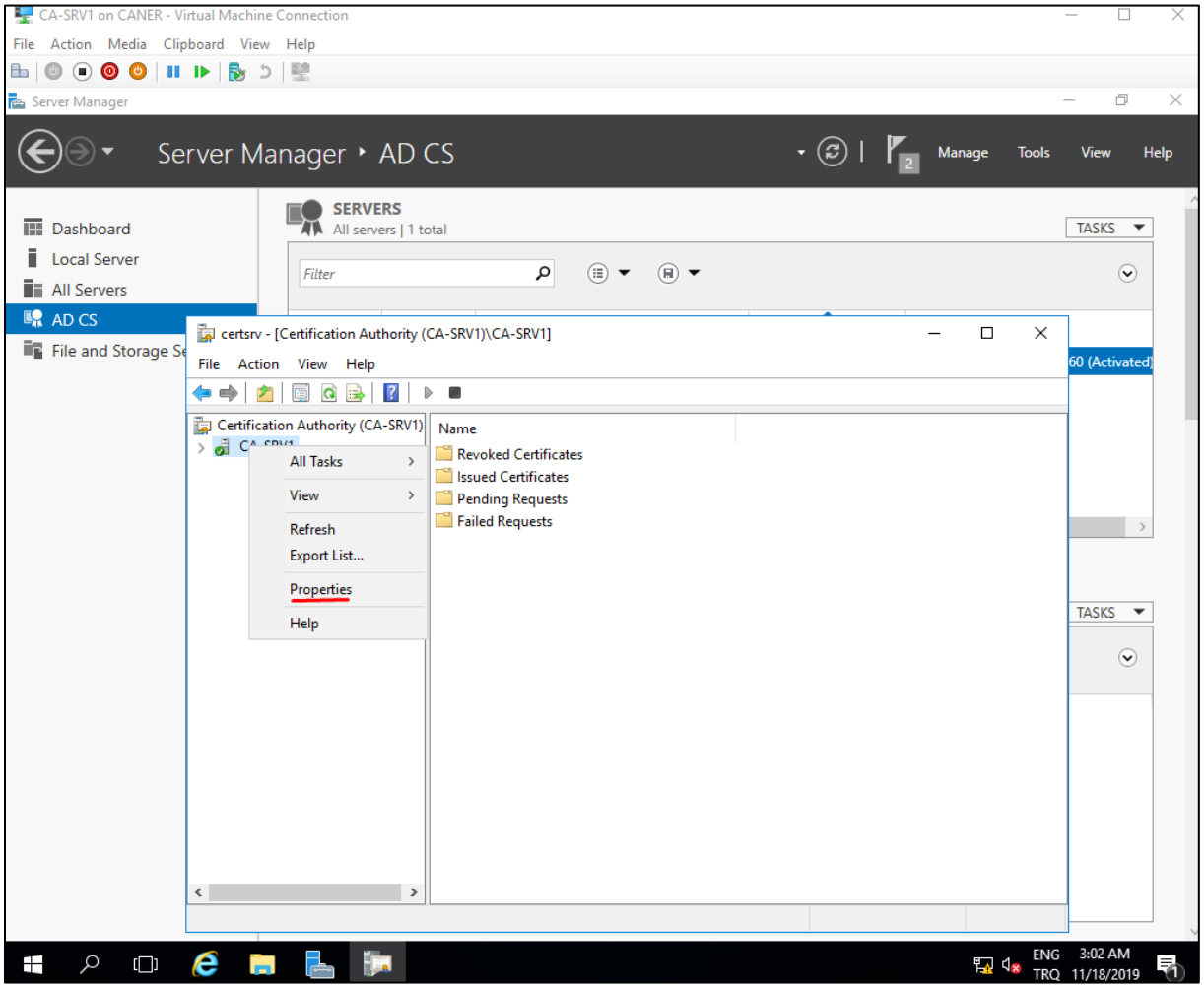
After we’re done with choosing the relevant options and see a summary. We configure the certificate finally.



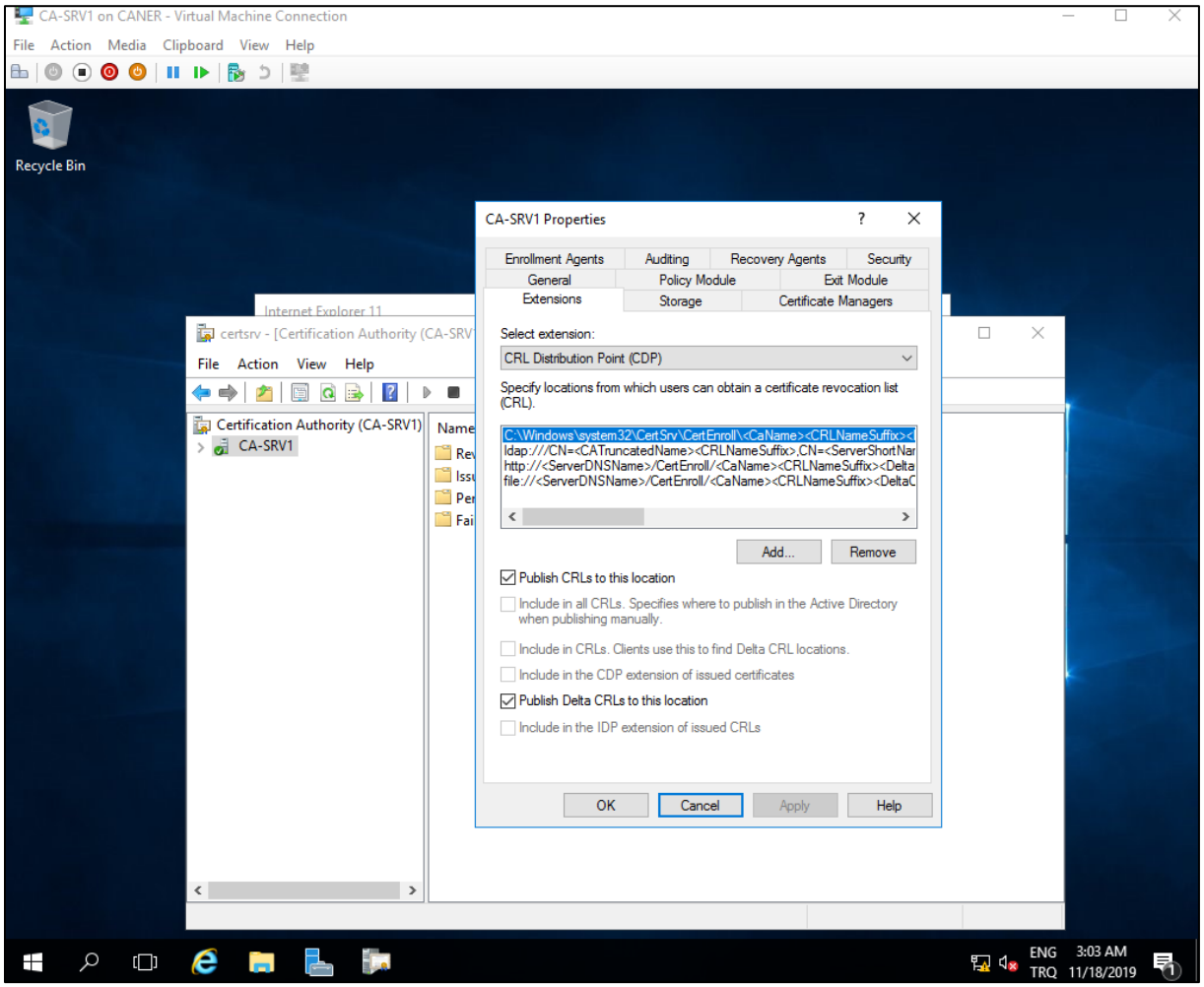
We right click at the AD CS page and pick Certification Authority.



We right click on the credentials of the server which is simply the name of CA-SRV1 and click on Properties.



We get to extensions and can see a few locations such as the file location path for the newly published CRLs and Delta CRLs. We then need to add new locations for the CRL Distribution Point (CDP).

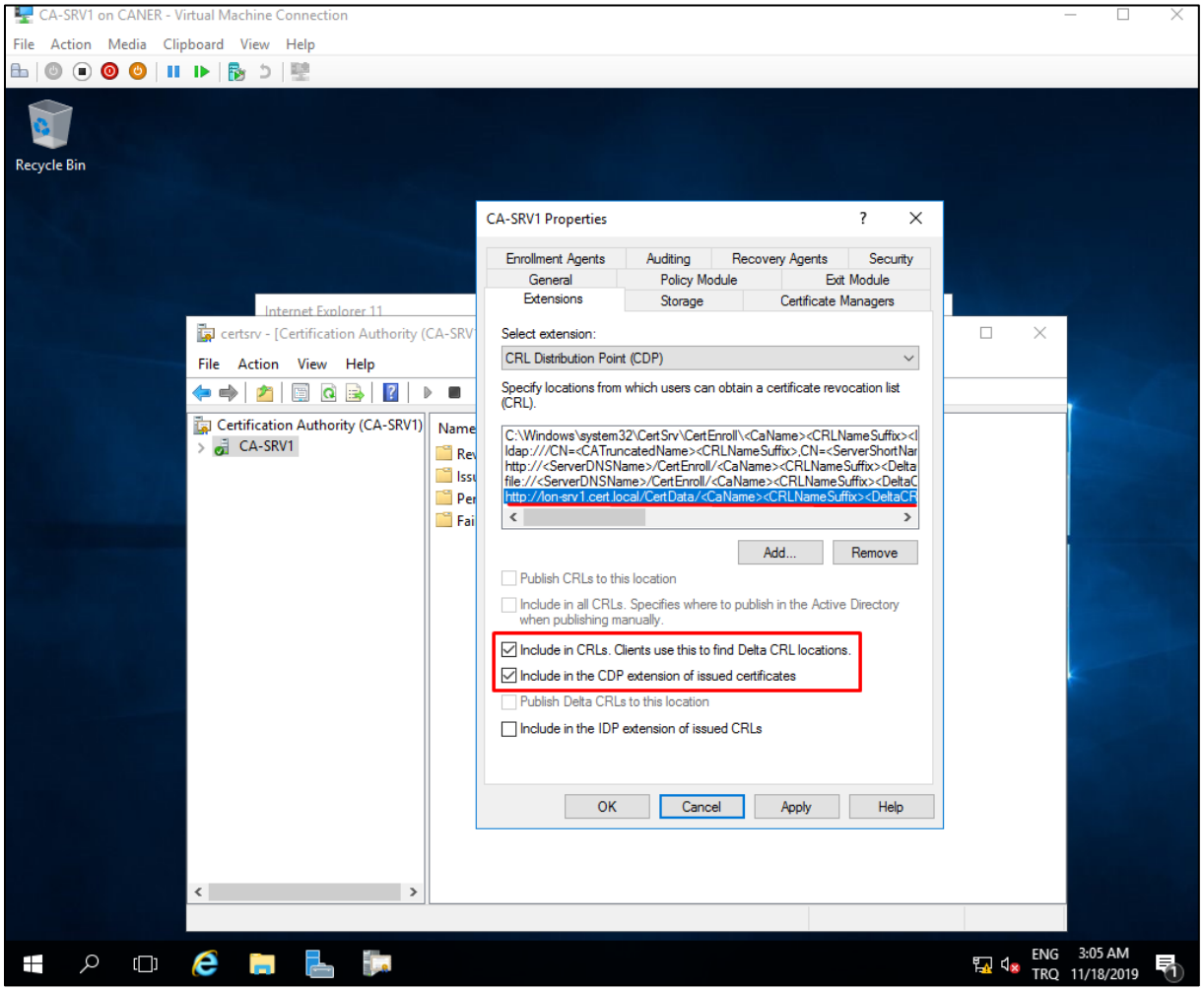


We need to add http://&&&NAMEOFTHESTANDALONE-CA.DOMAIN&&&

/CertData/<Ca-Name><CRLNameSuffix><DeltaCRLAllowed>.crl

So we added:

http://lon-srv1.cert.local/CertData/<Ca-Name><CRLNameSuffix><DeltaCRLAllowed>.crl

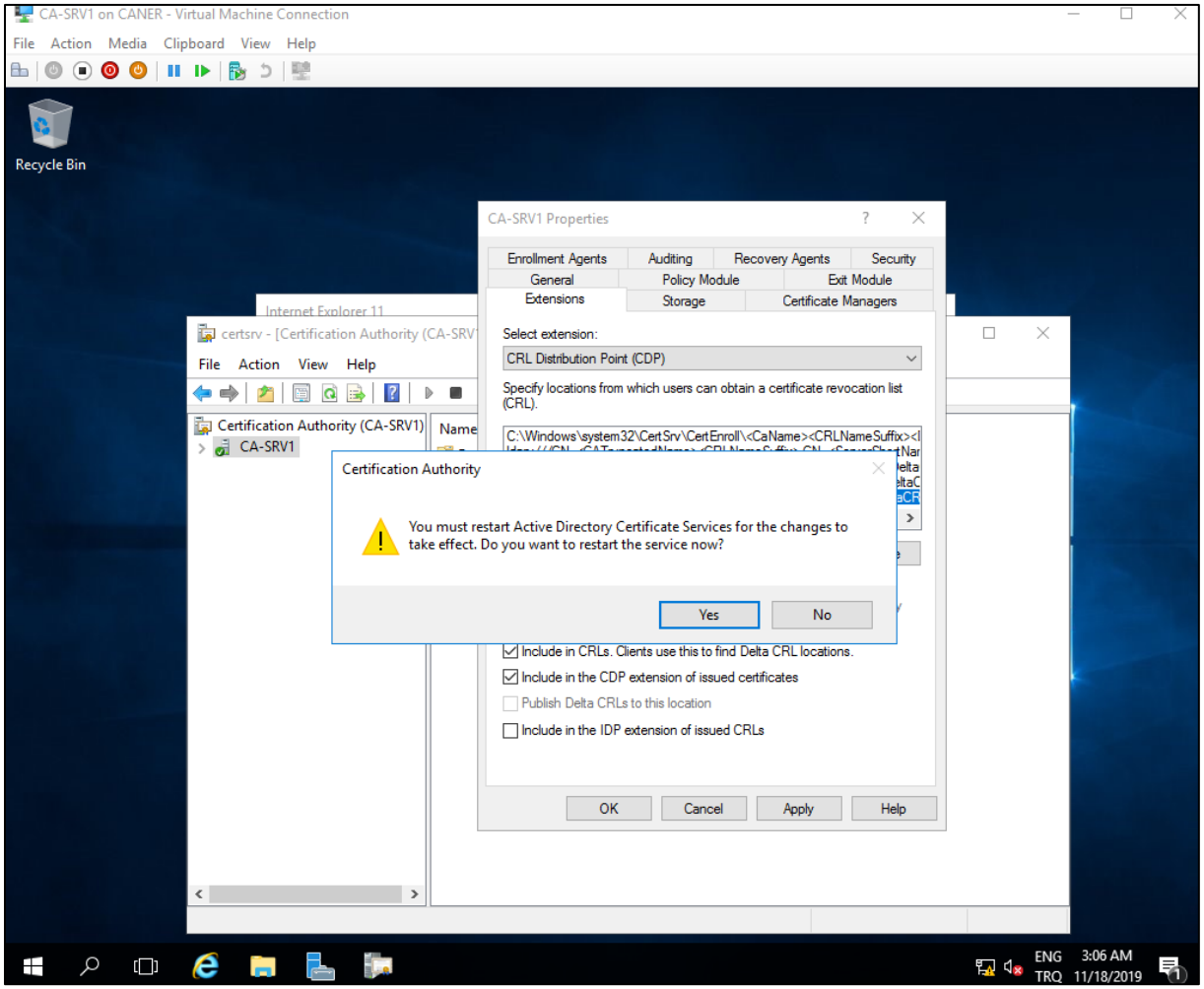


Note that we select the following option:

“Include in CRLs. Clients use this to find Delta CRL locations.” and

“Include in the CDP extension of issued certificates.”

This initiates a restart.



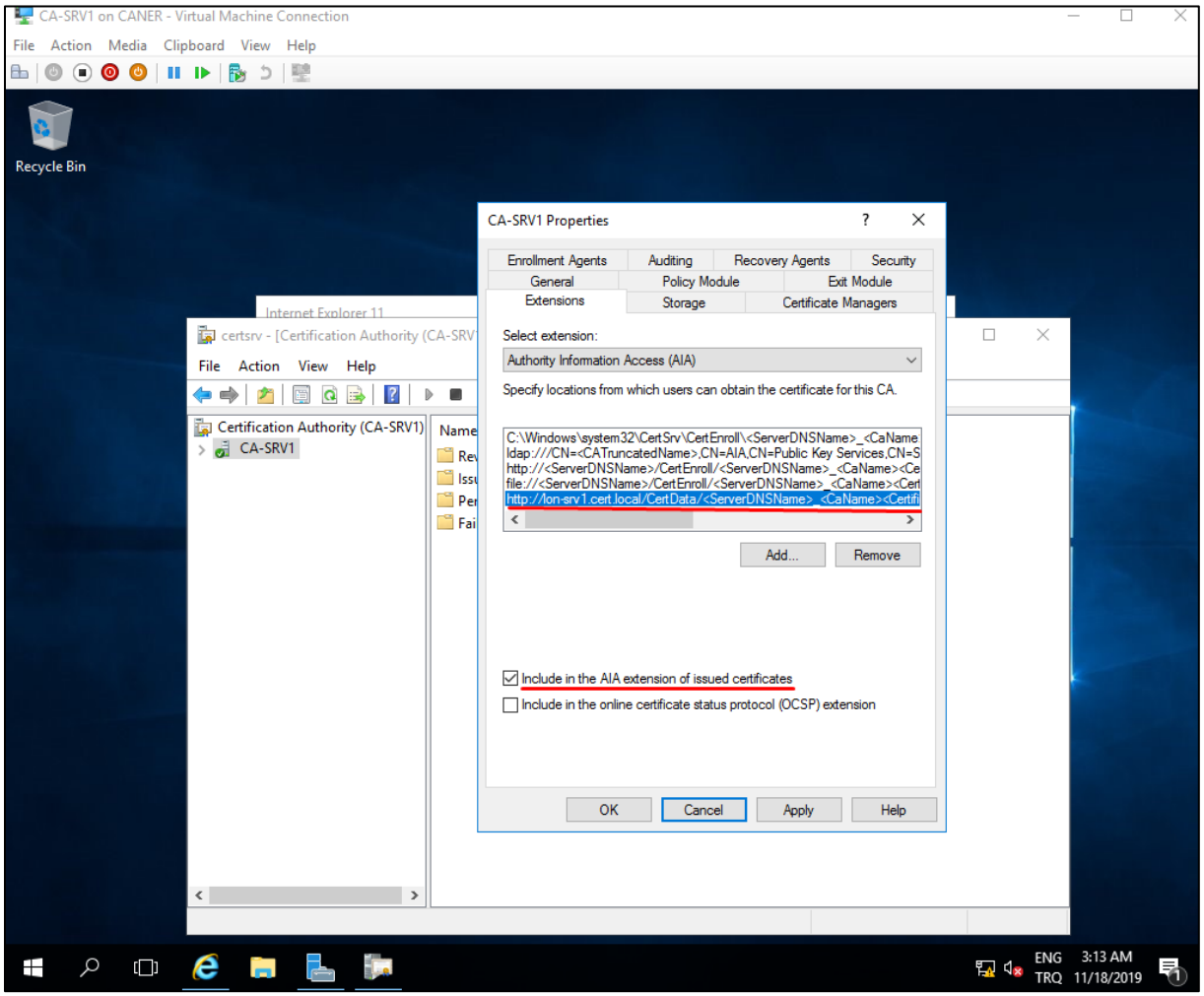
We then need to add new locations for Authority Information Access (AIA).

We need to add http://&&&NAMEOFTHESTANDALONE-CA.DOMAIN&&&

/CertData/<ServerDNSName>_<CaName><CertificateName>.crt

So we added:

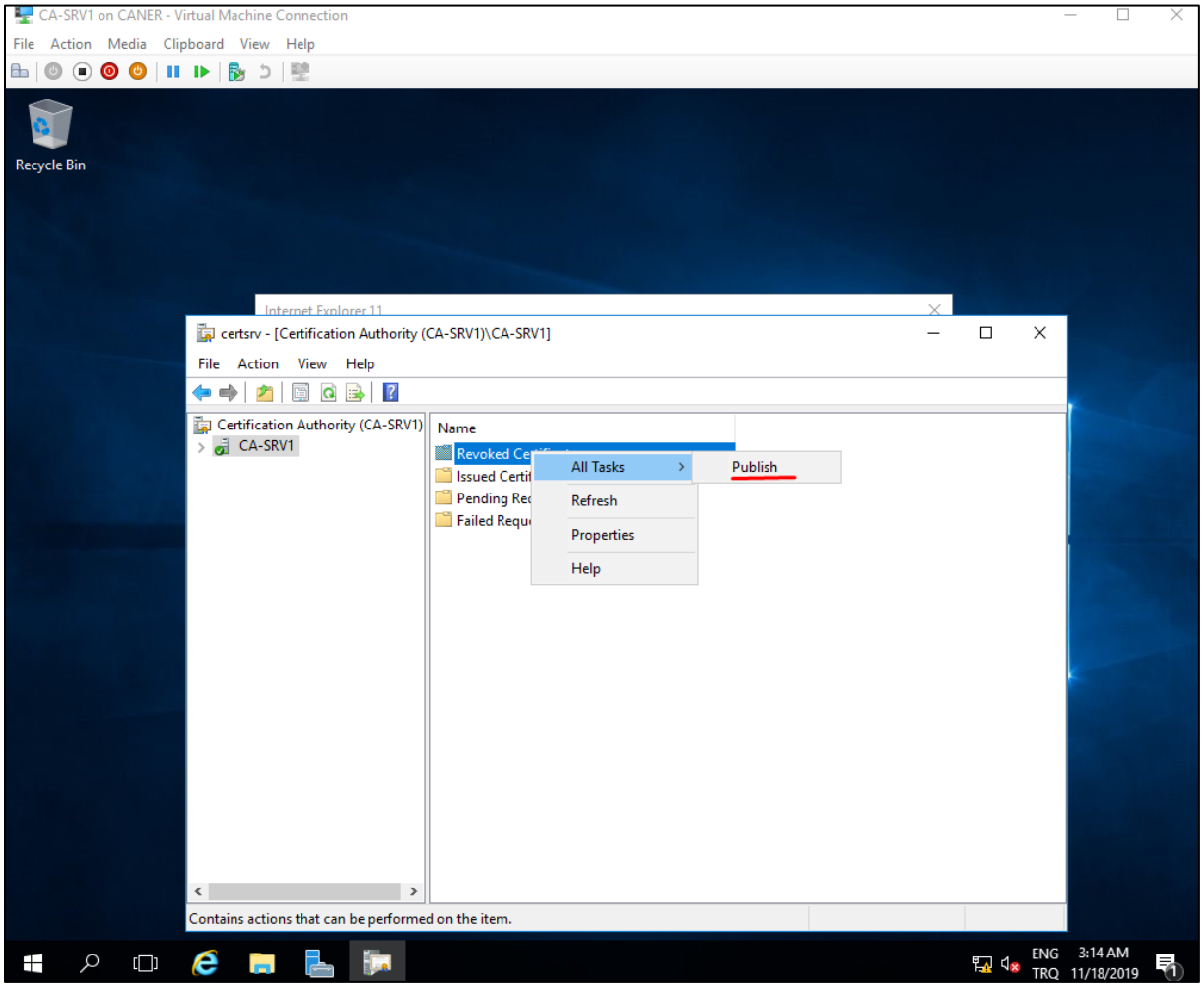
http://lon-srv1.cert.local/CertData/<ServerDNSName>_<CaName><CertificateName>.crt



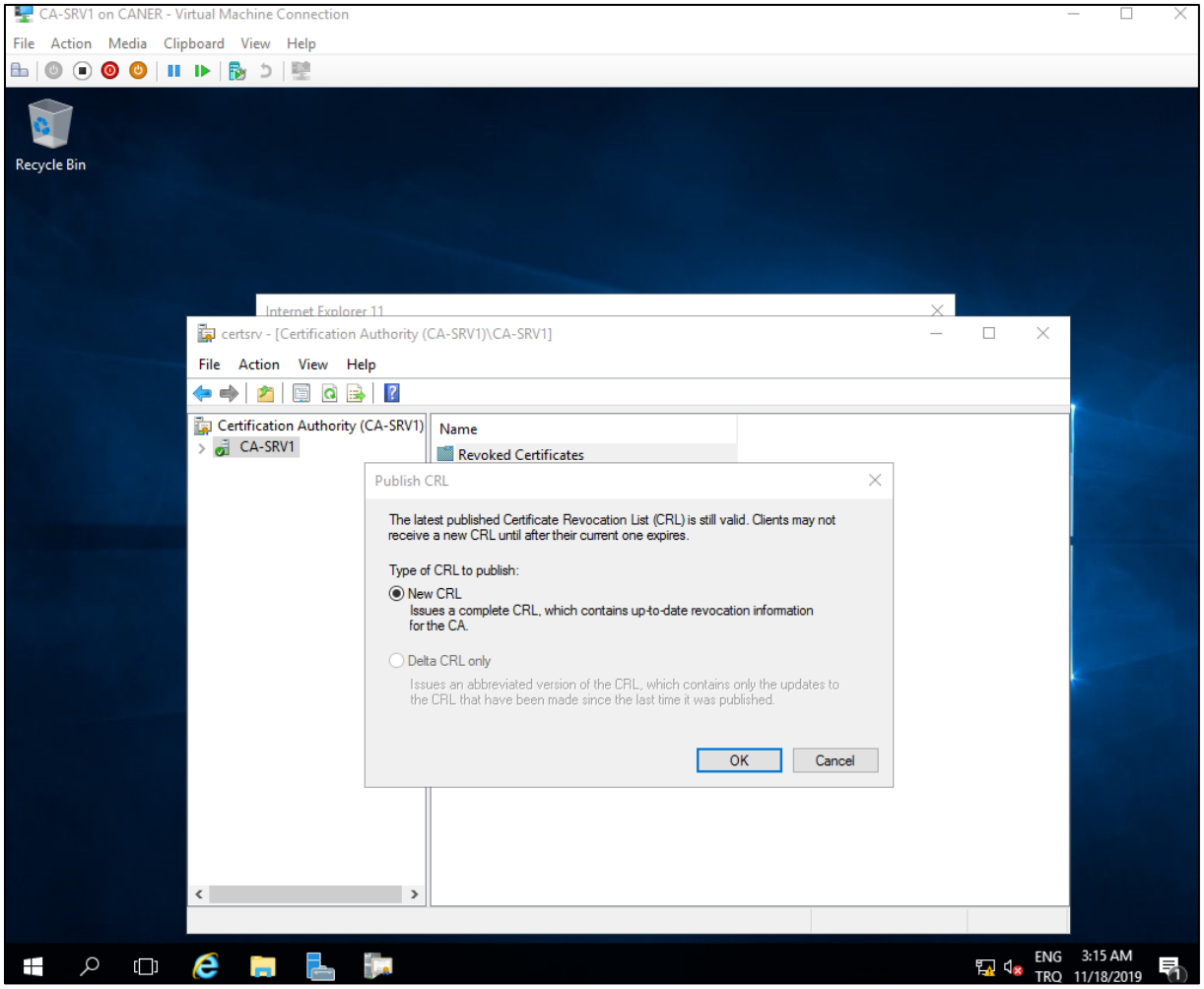
Note that we need to select:

“Include in the AIA extension of issued certificates.”

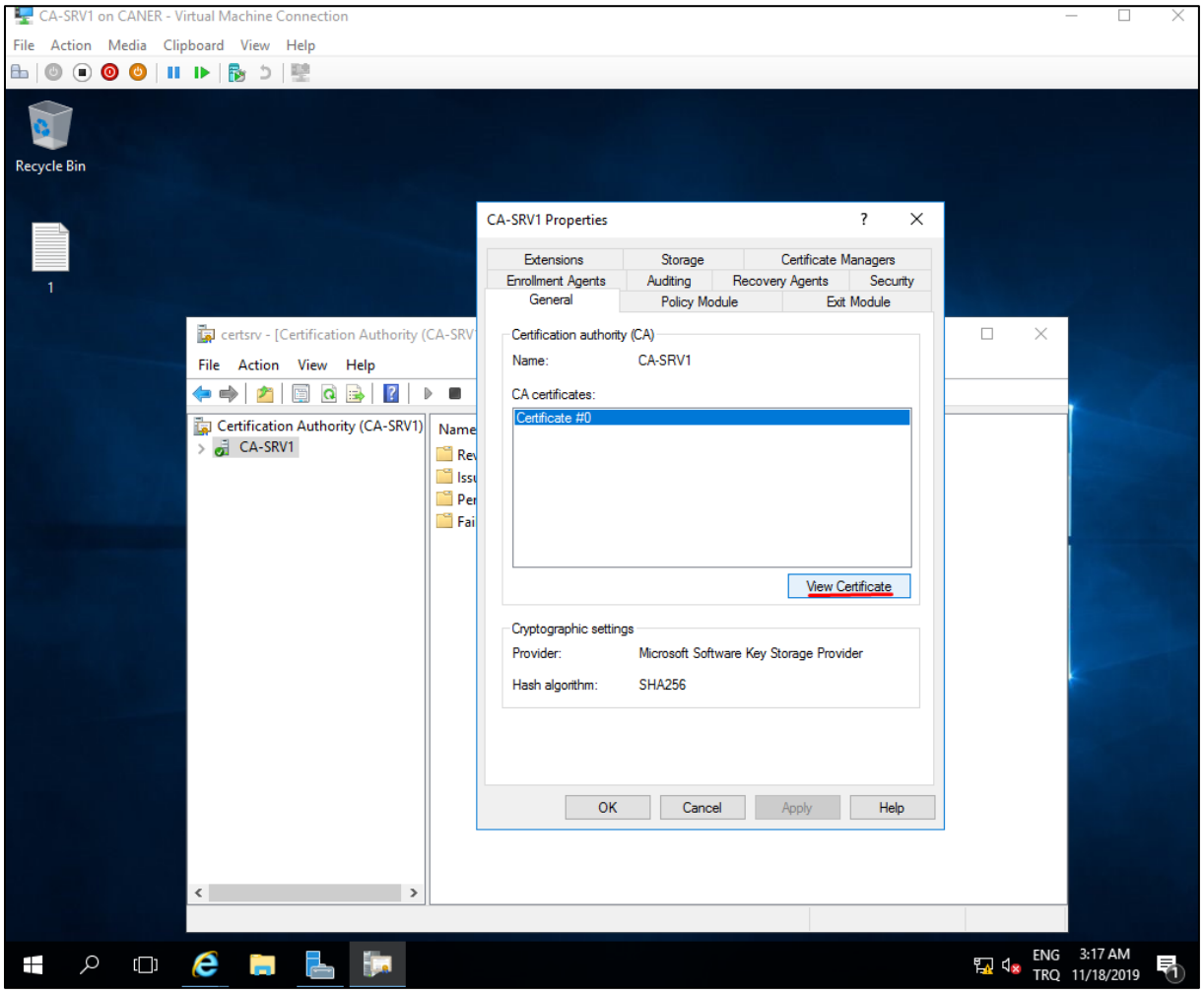
We then publish the certificate by going to the Certificate Authority and right clicking to get to “Publish” among “All Tasks”.



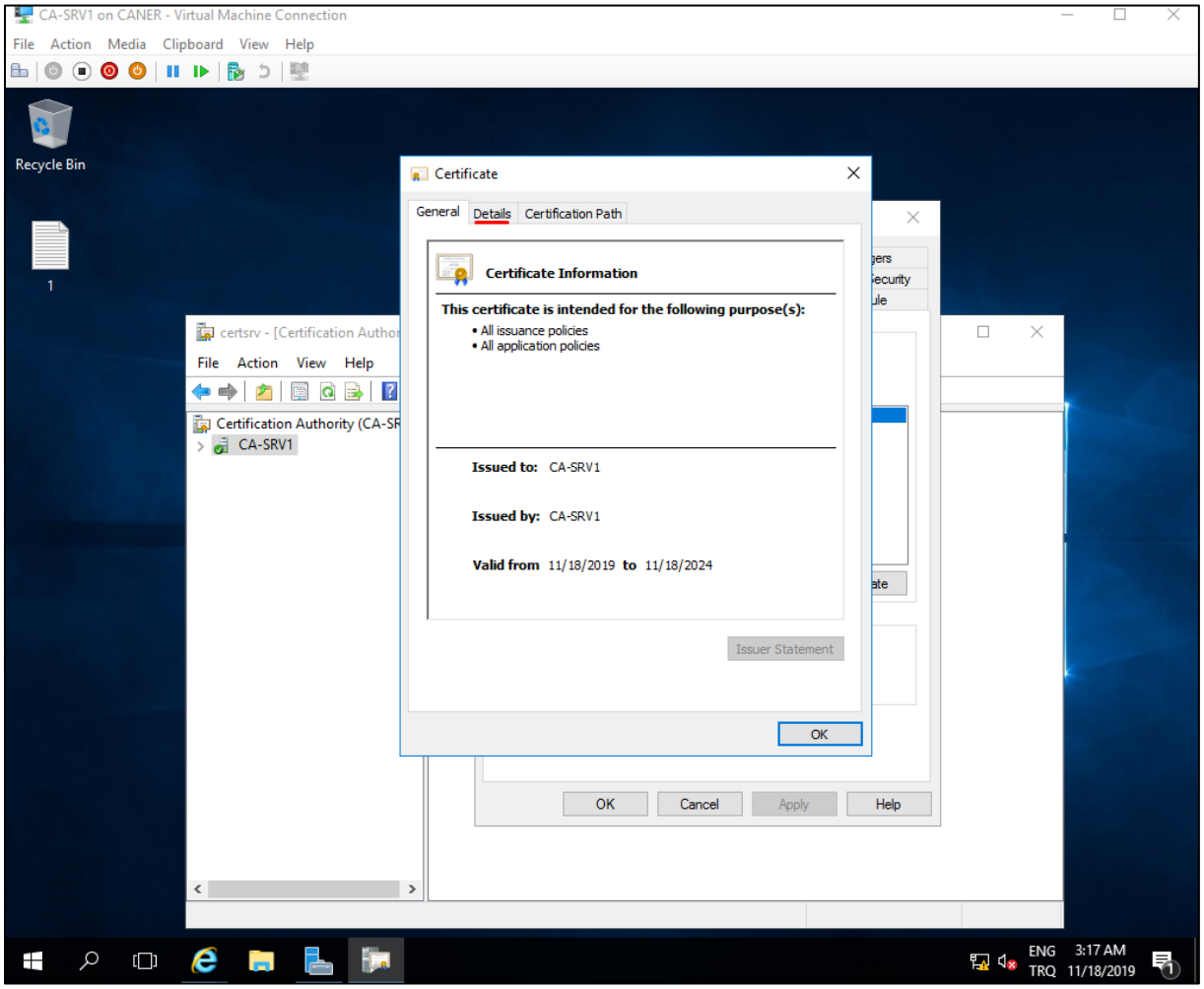
This initiates the Publish CRL Wizard. We choose New CRL obviously.



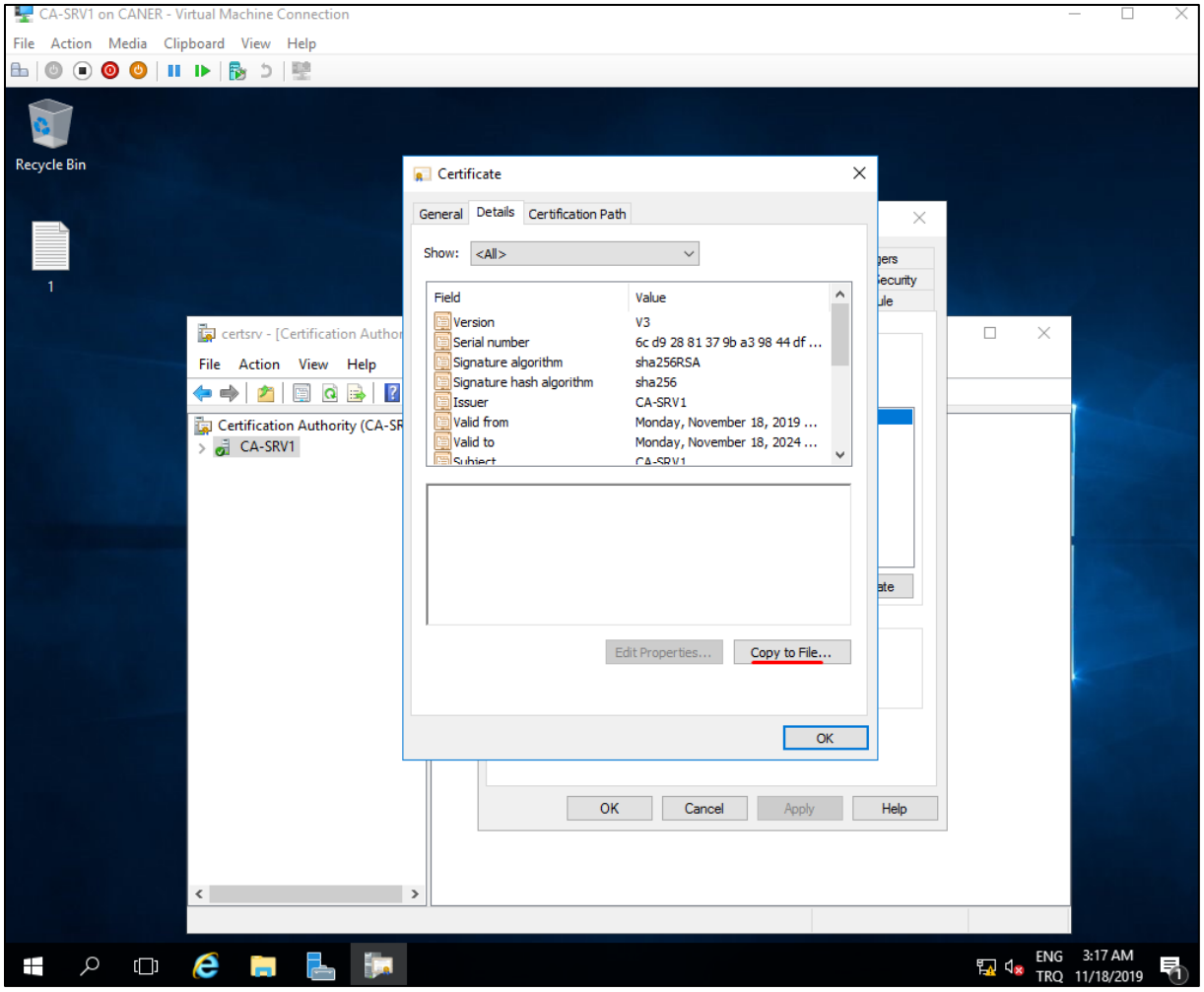
This publishes the certificate. Then, we can find it by right clicking on Certificate Authority to get to the Properties of the CA. In which we can find the new certificate under “General” tab. We click on View Certificate.



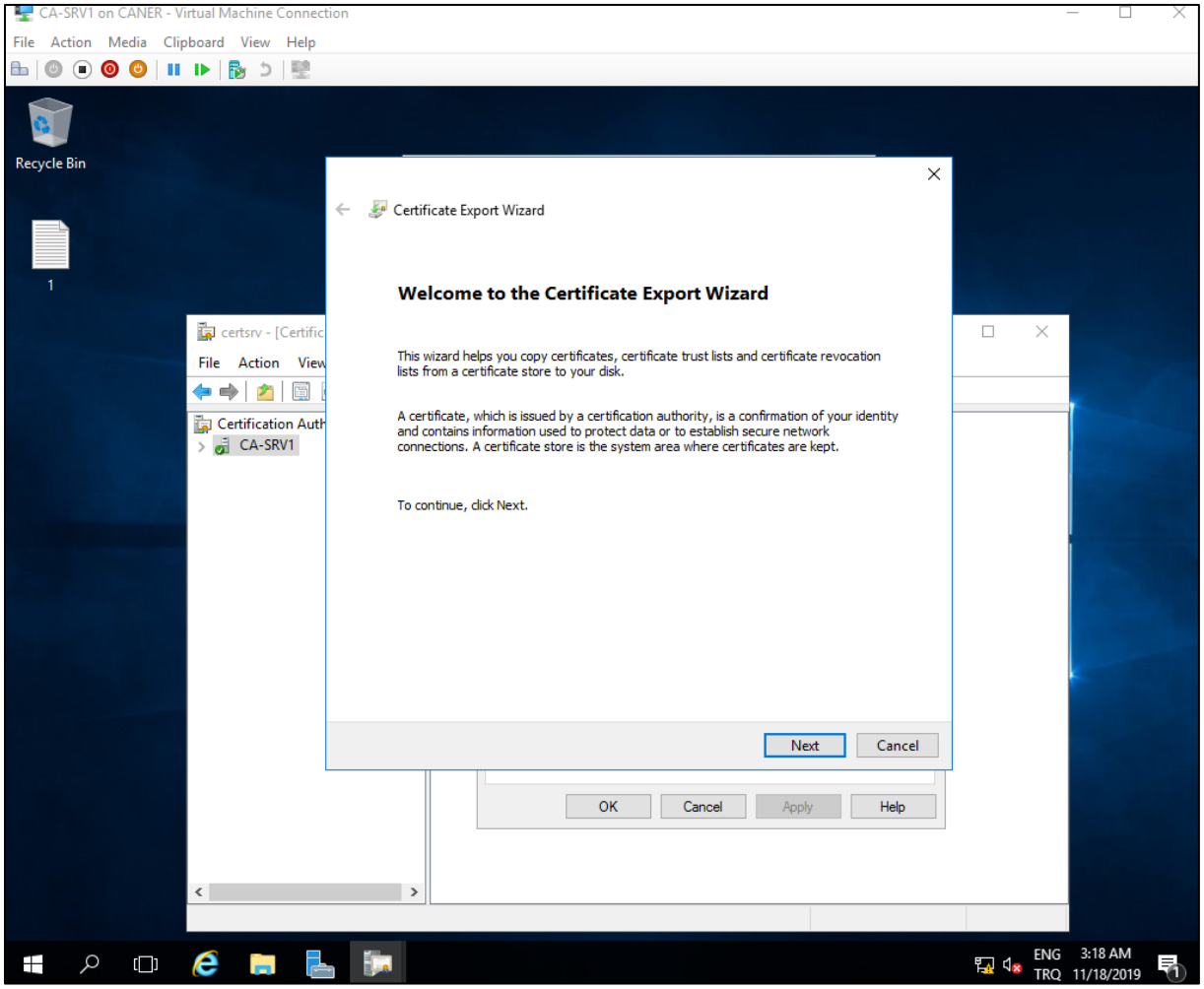
To export this certificate from the Standalone CA we need the file of the certificate. Hemce, we get to the Details tab on the certificate so that…



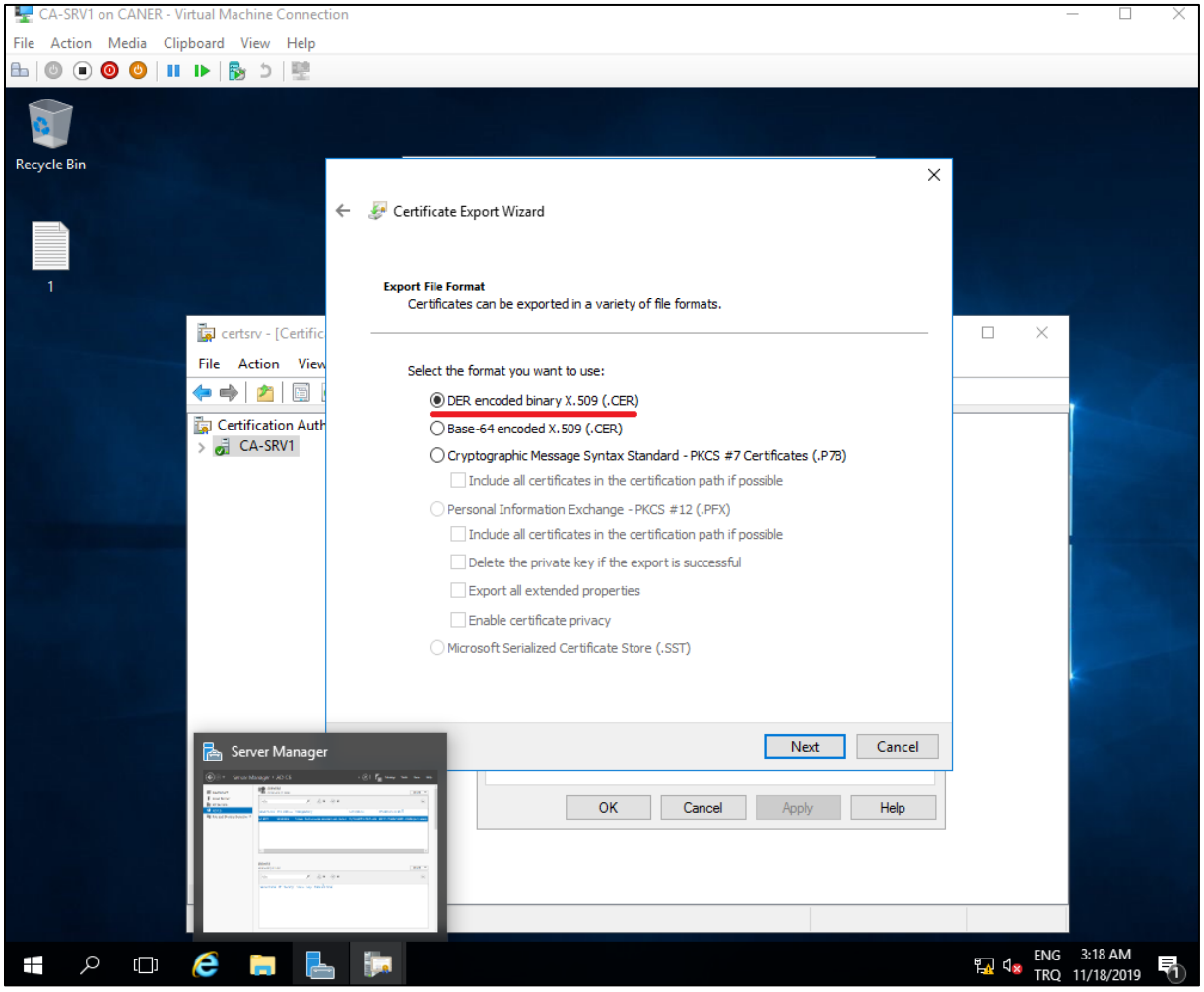
…we can Copy to File the certificate.



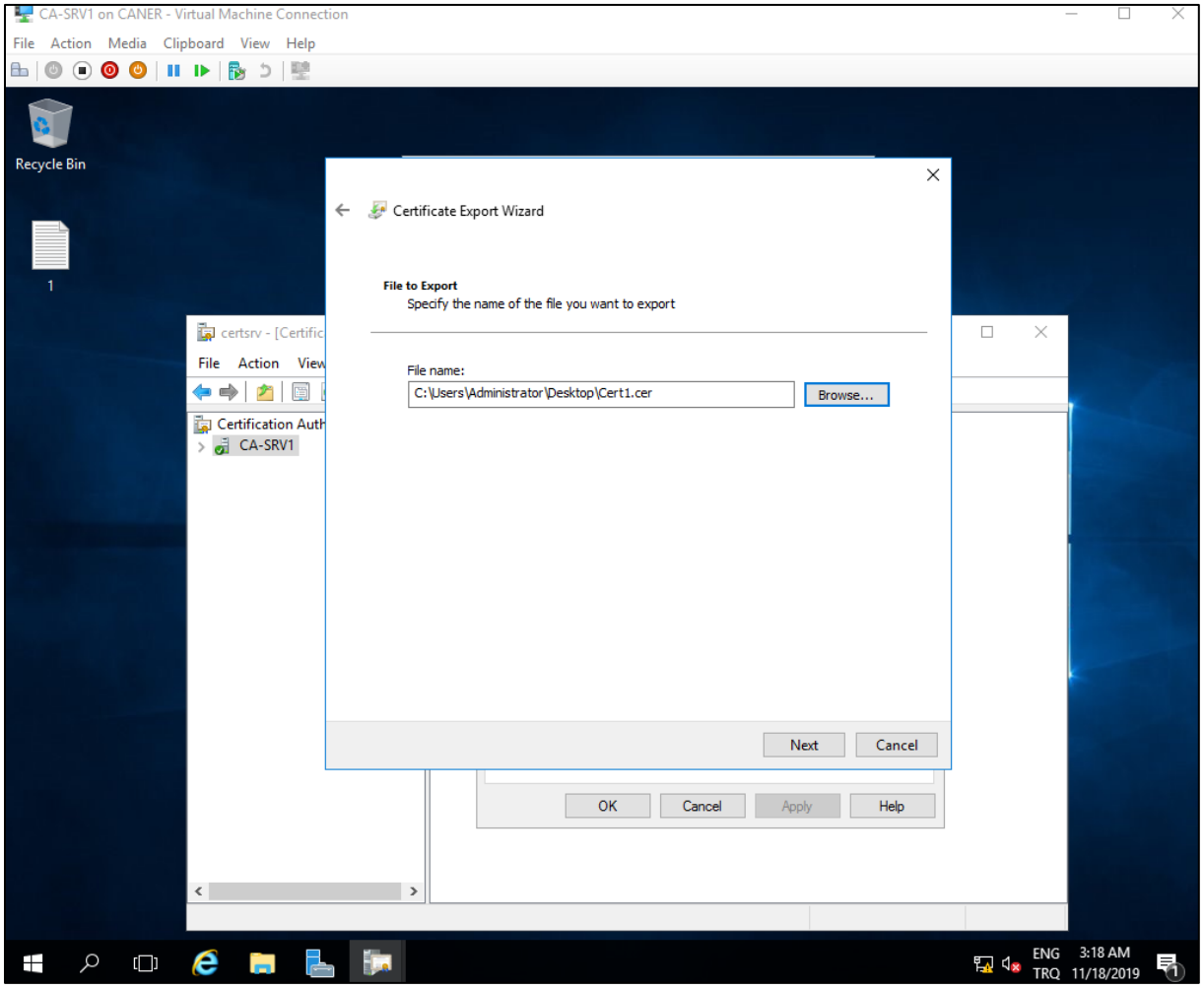
This initiates the Export Certificate Wizard.



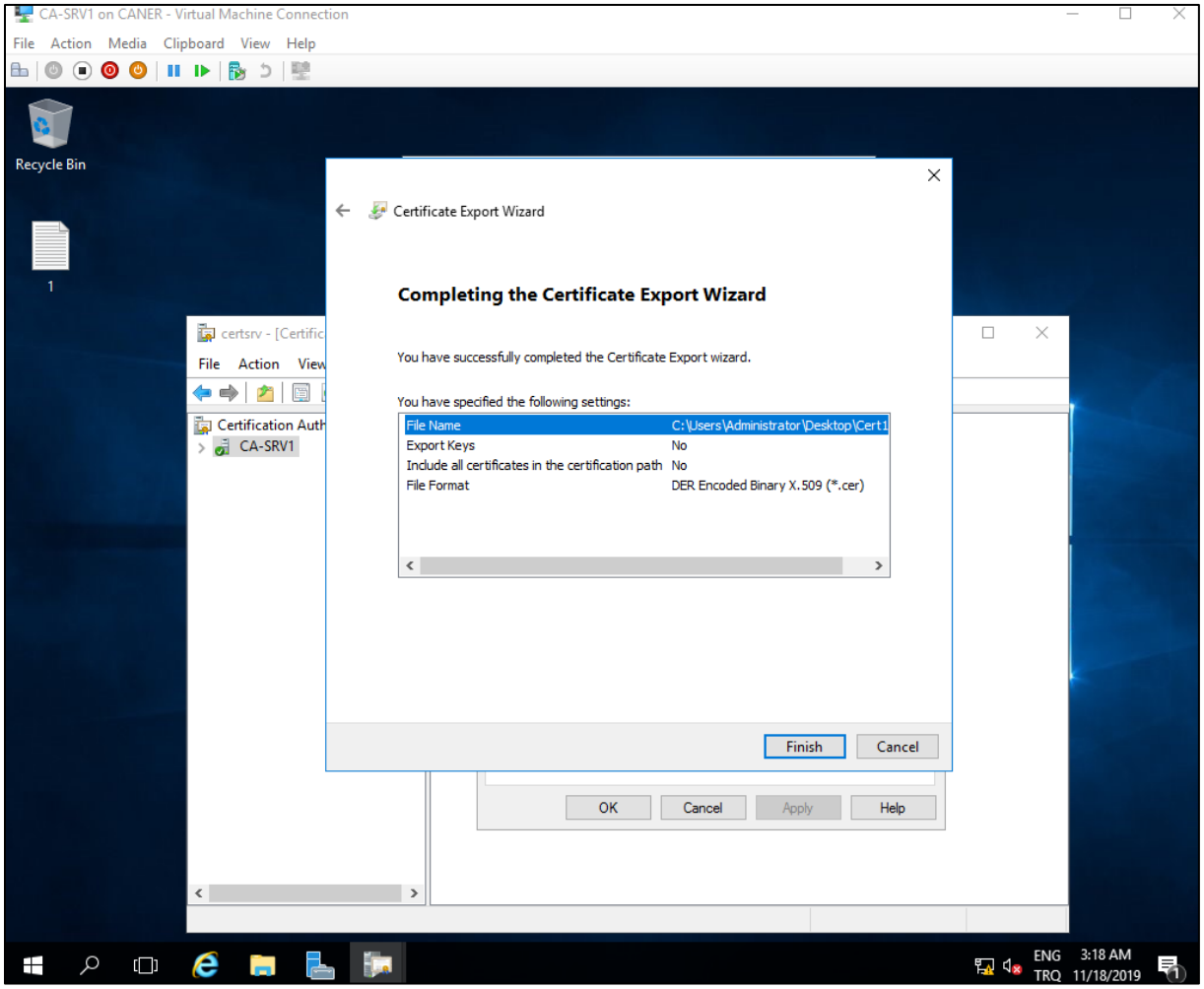
We choose the default setting.



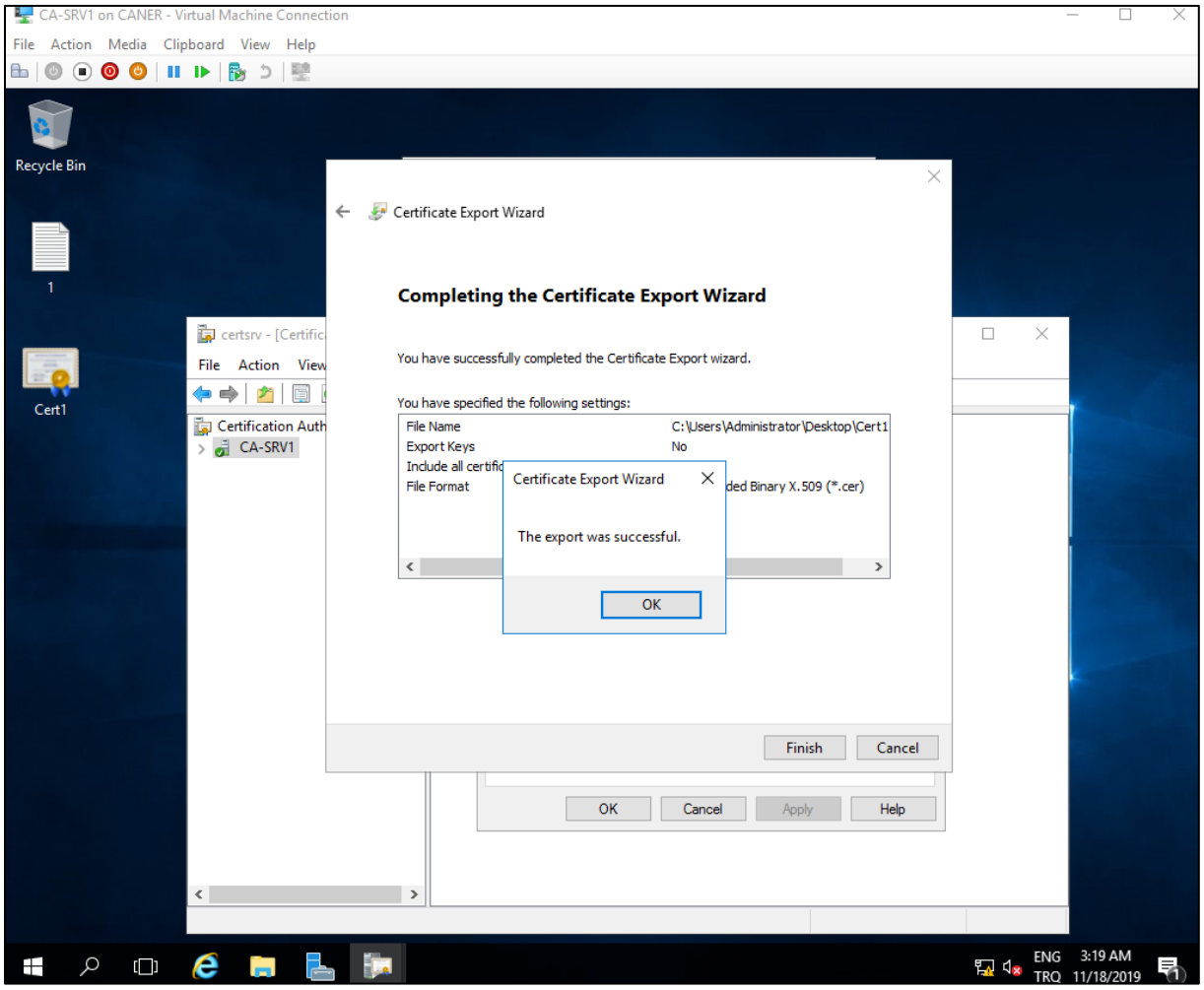
We chose Desktop for easy retrieval of the certificate but any path is possible.



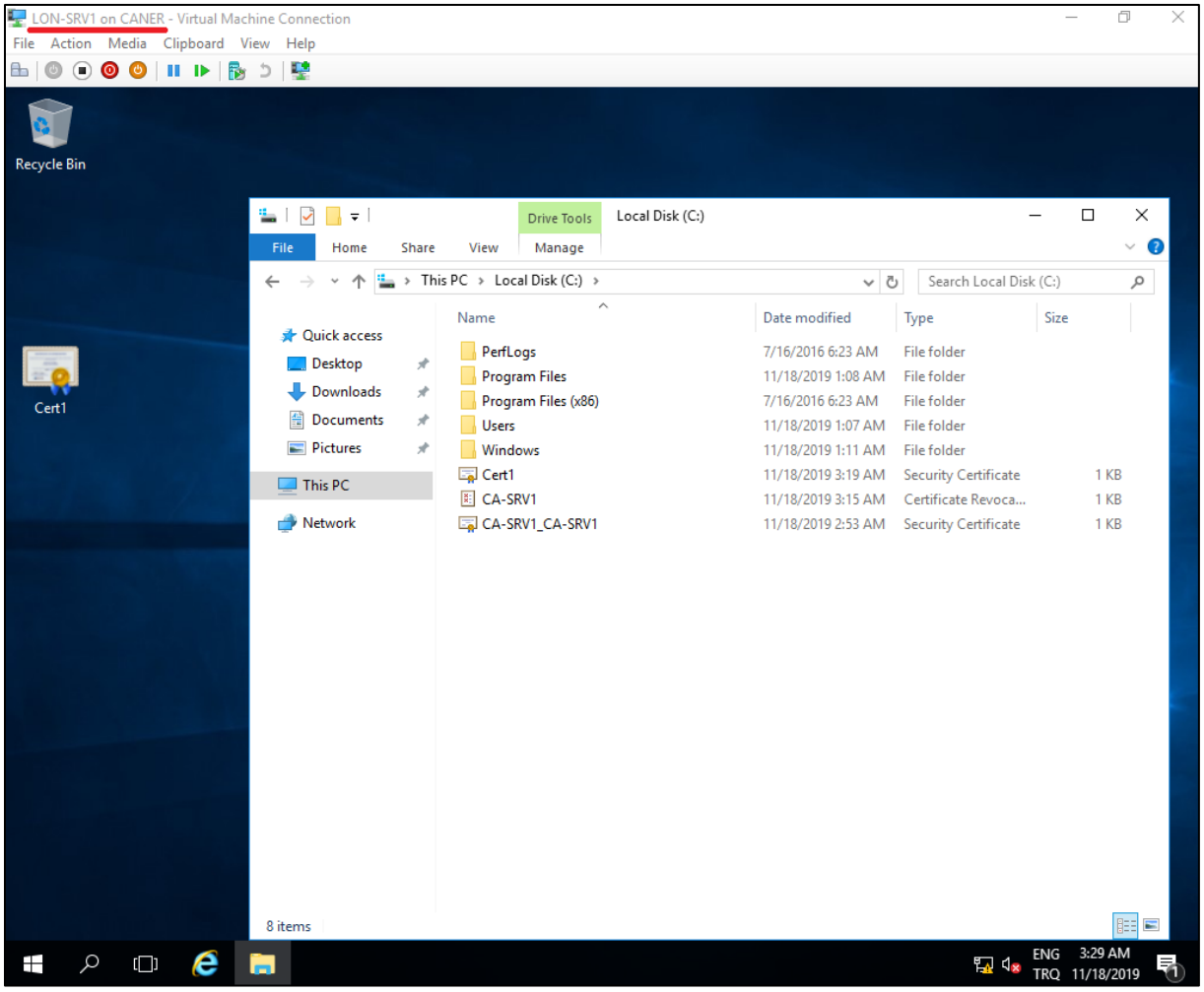
We get a summary of our picks and…



… we complete exporting the certificate.

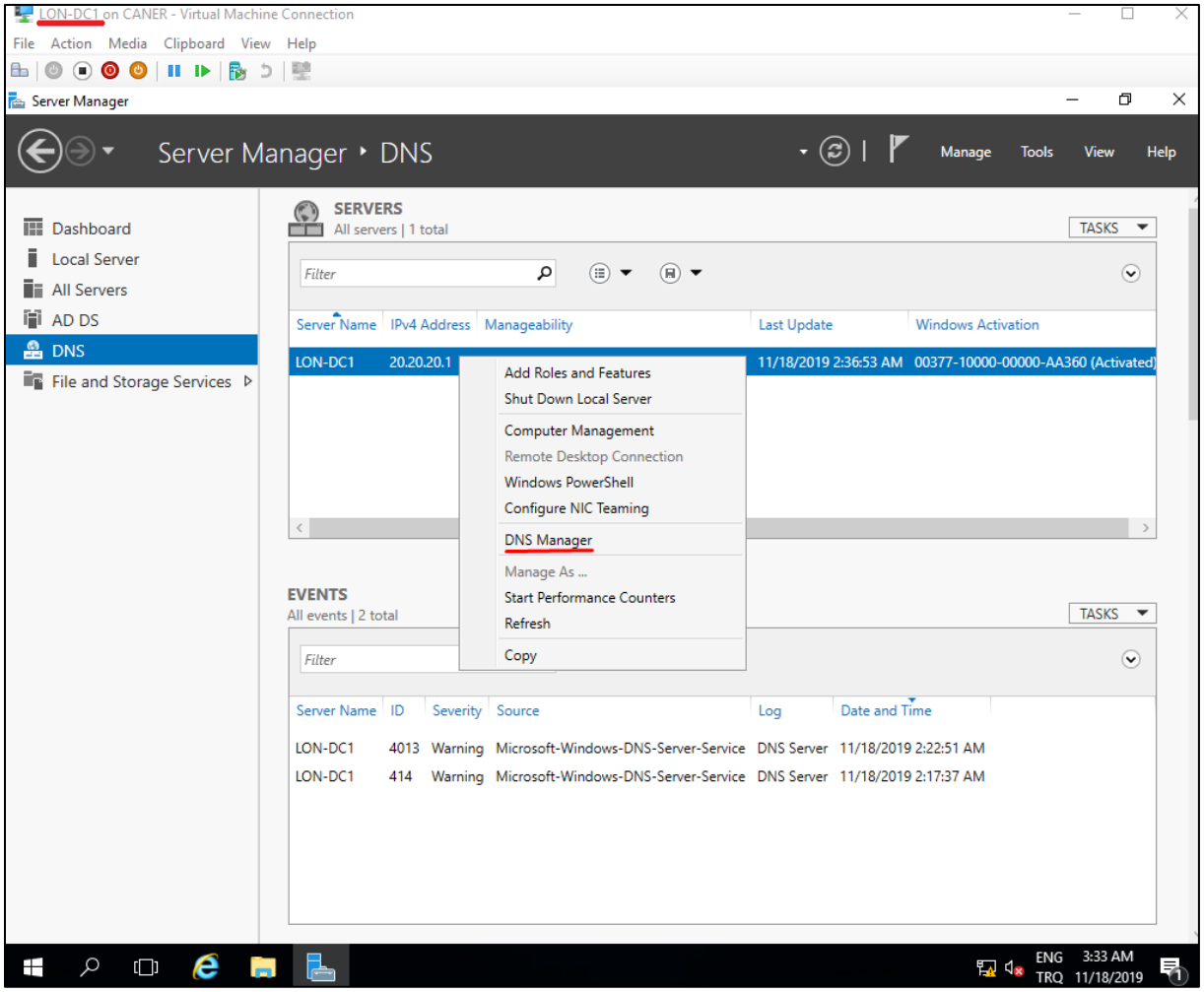


We manually copy the certificate and the relevant files to the Standalone CA.

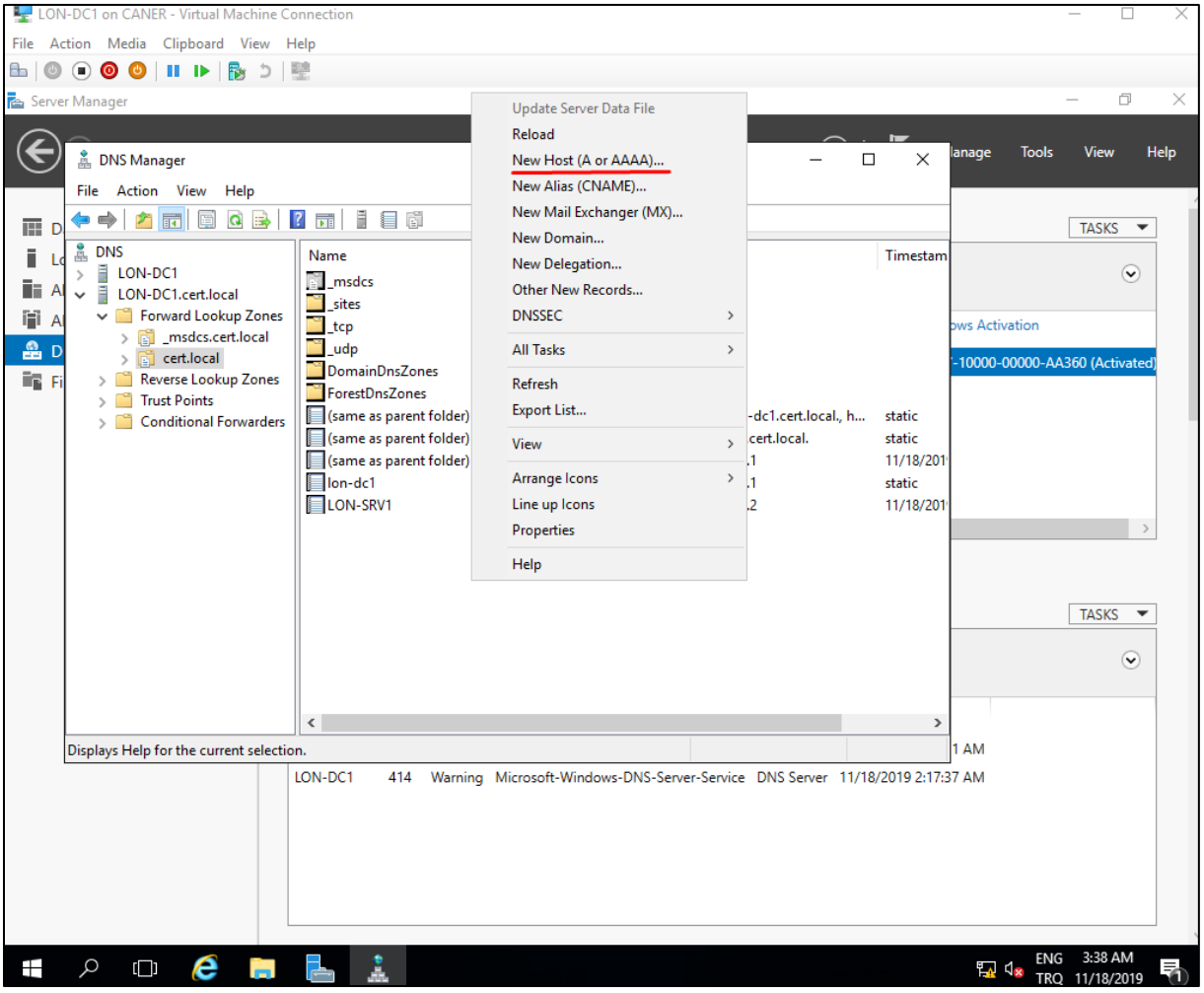


Now all we need to do before being able to turn the Standalone CA off is to enter it on the DNS list on Forward Lookup Zone.

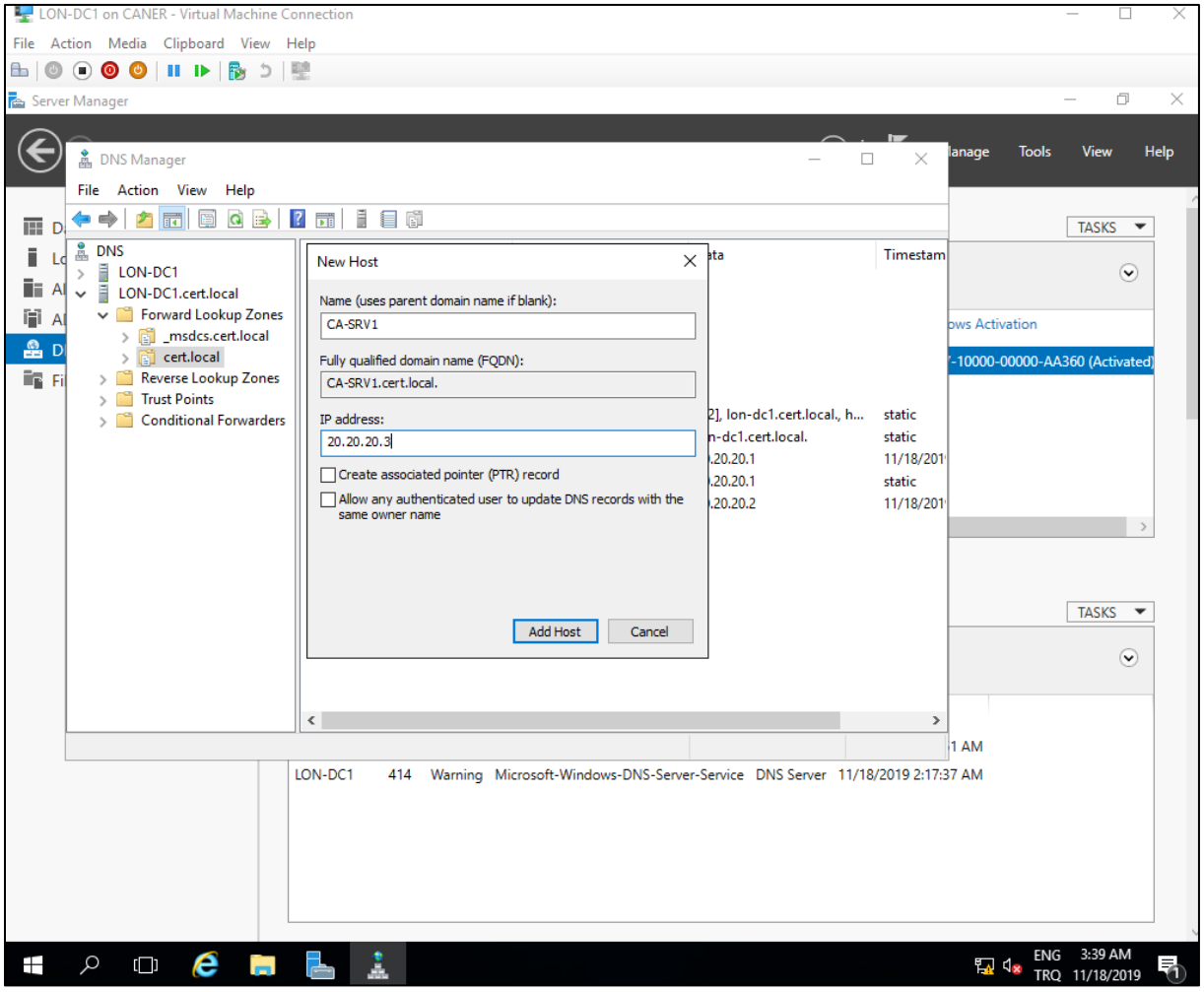
To add the Standalone CA to the DNS list we need to get to the DNS manager on the DC.



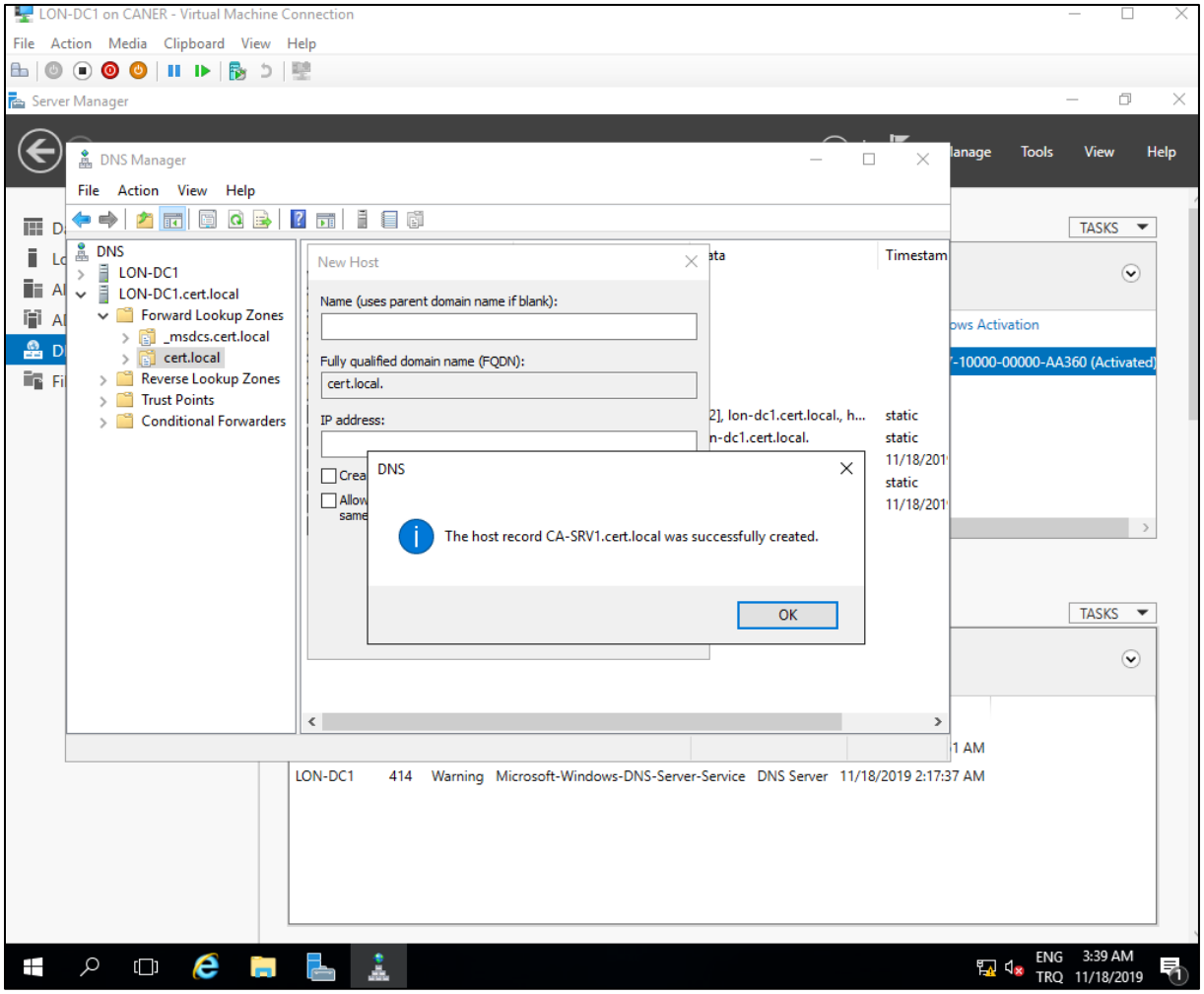
We get to the Forward Lookup Zones and add a New Host



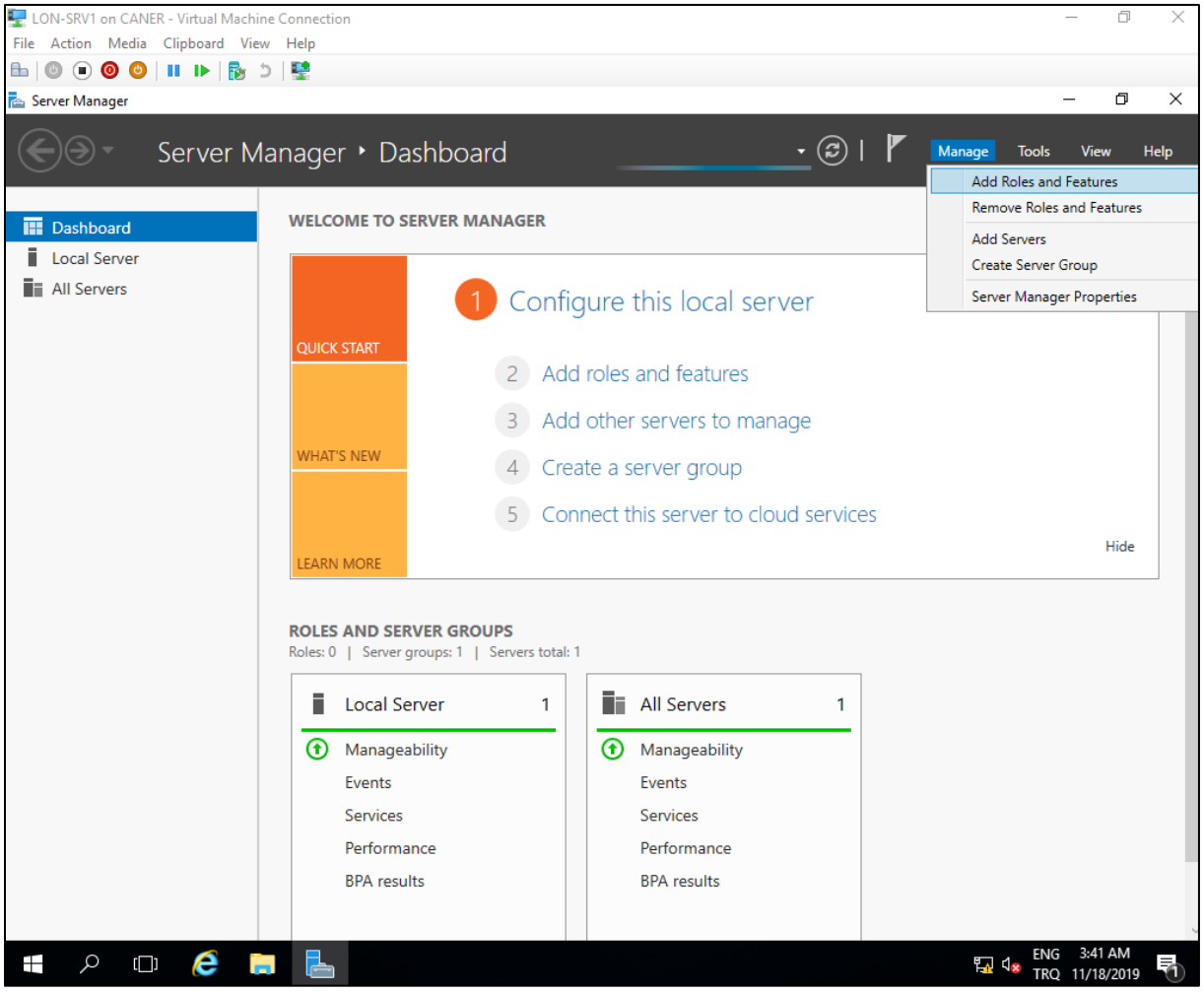
We enter CA-SRV1's name and IP address and …



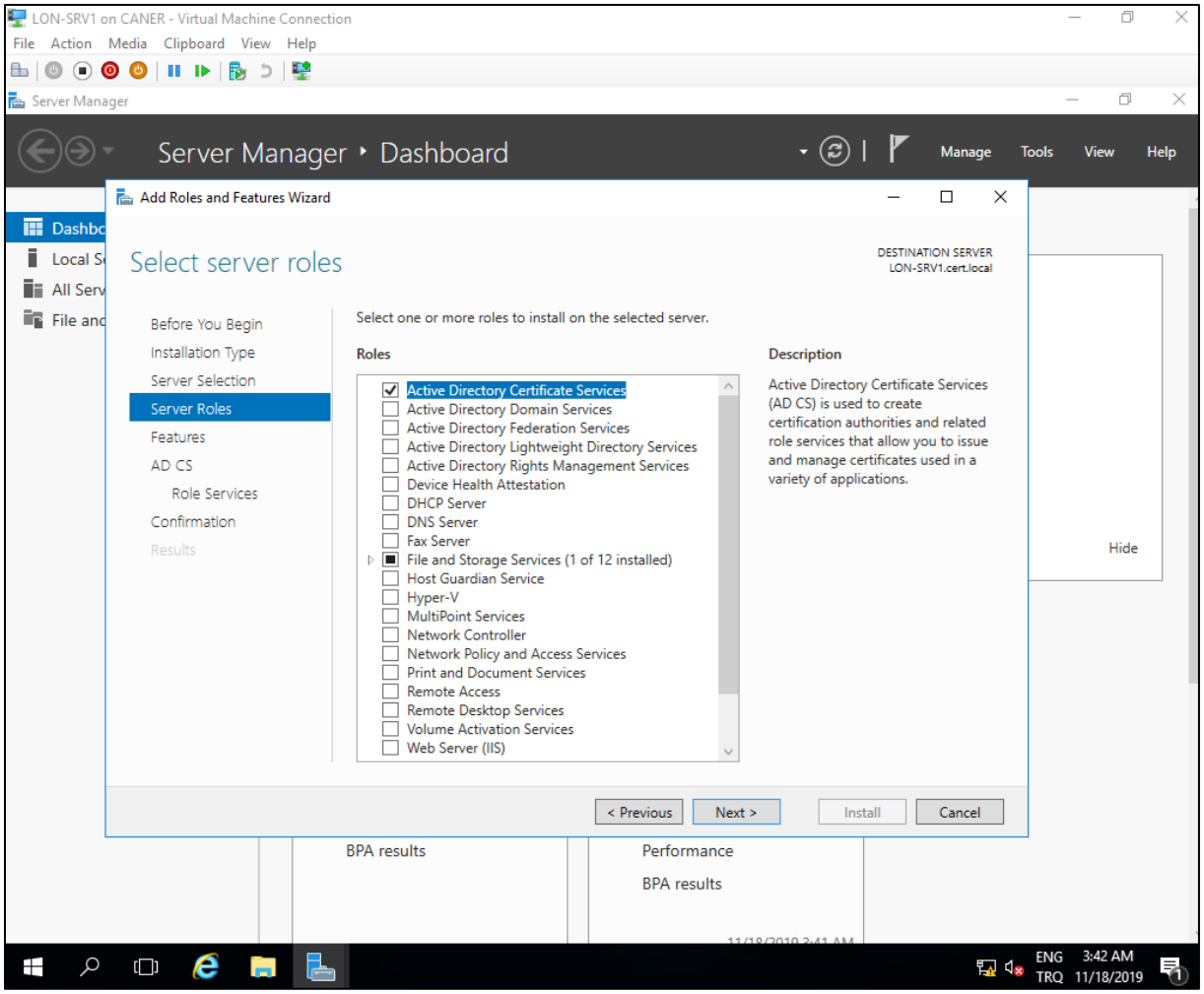
… add it to the DNS list.



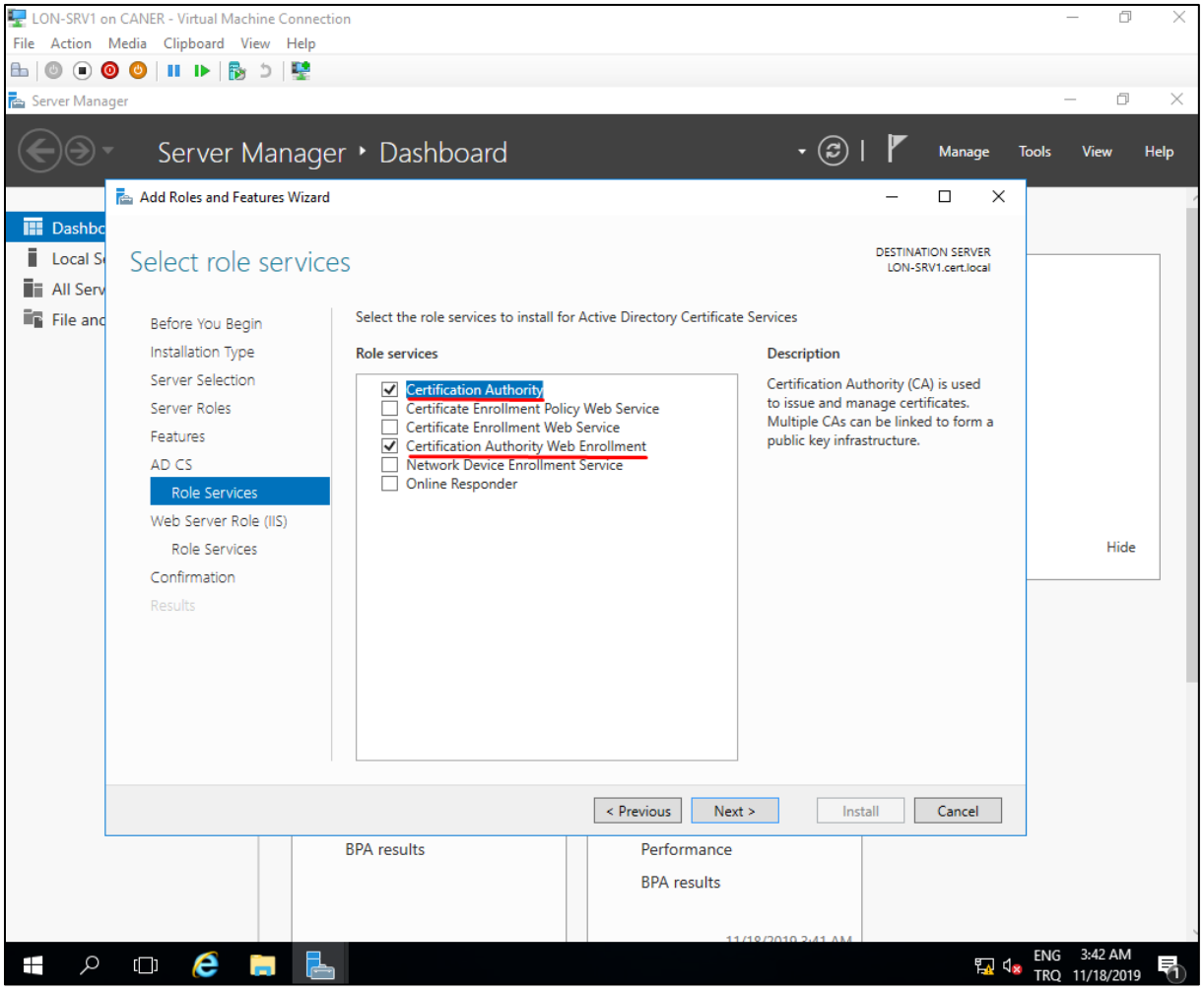
Now we can start to set LON-SRV1 as the Enterprise CA.



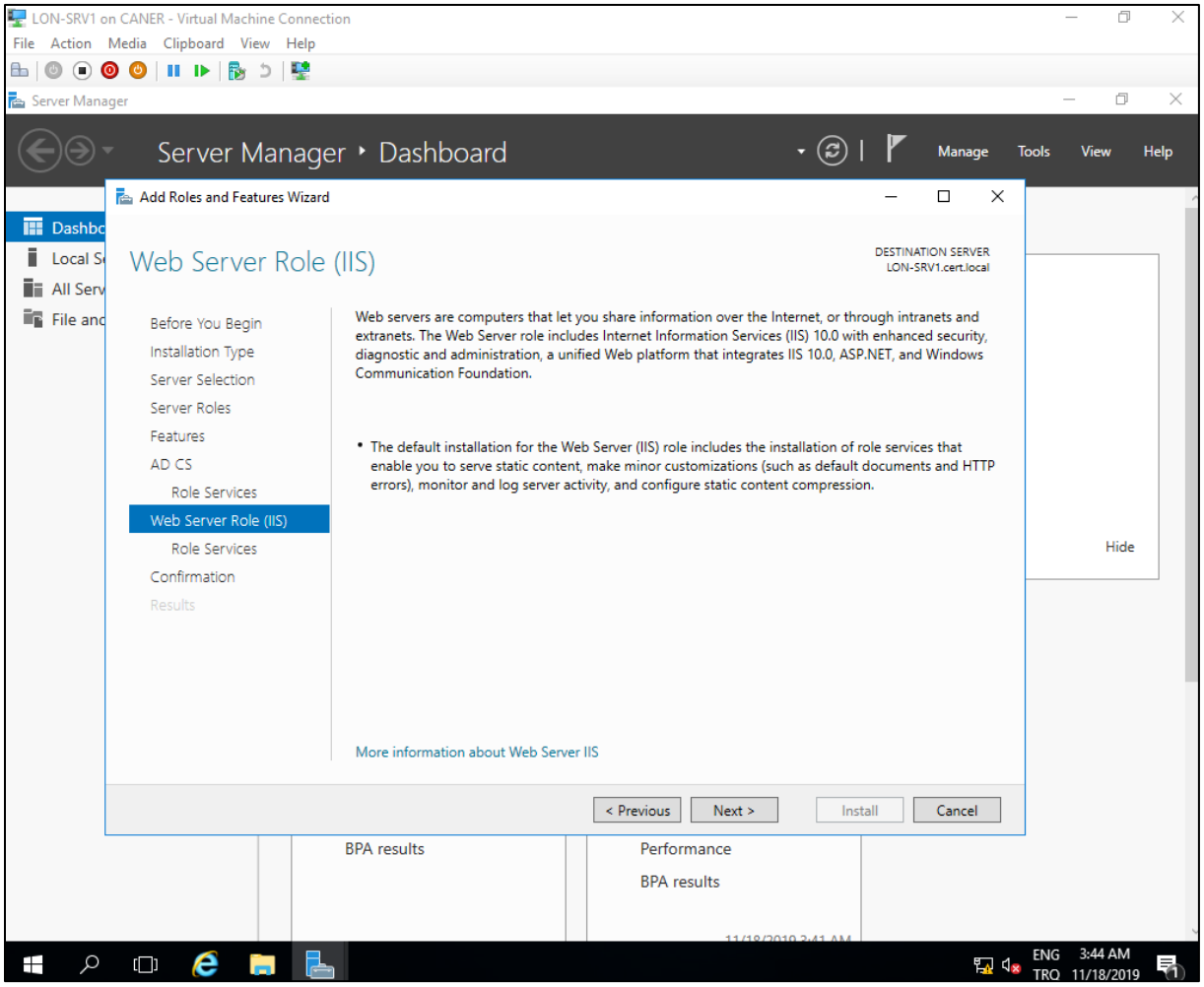
We need Active Directory Certificate Services obviously.



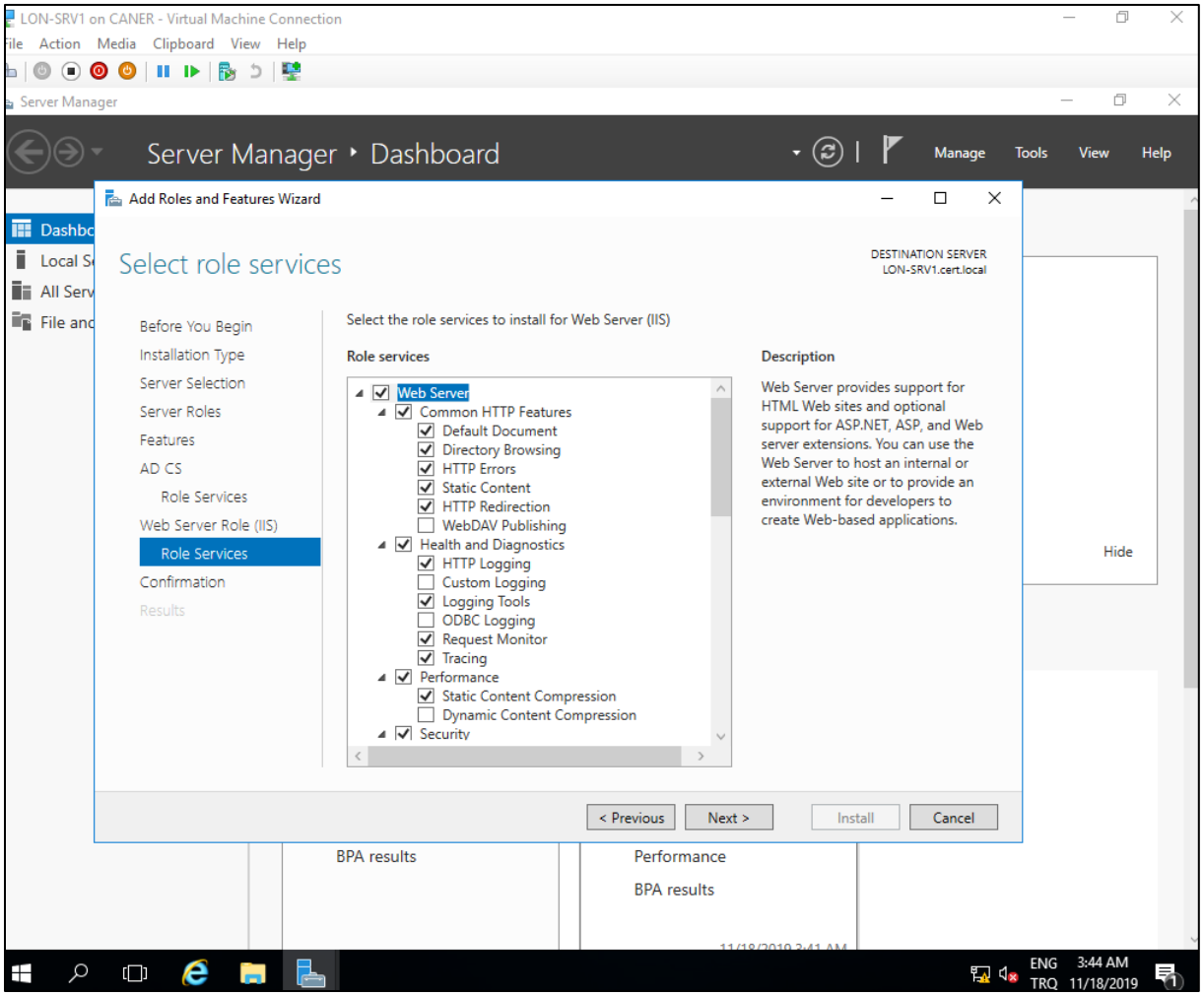
We select both Certification Authority and Certification Authority Web Enrollment.



We proceed.

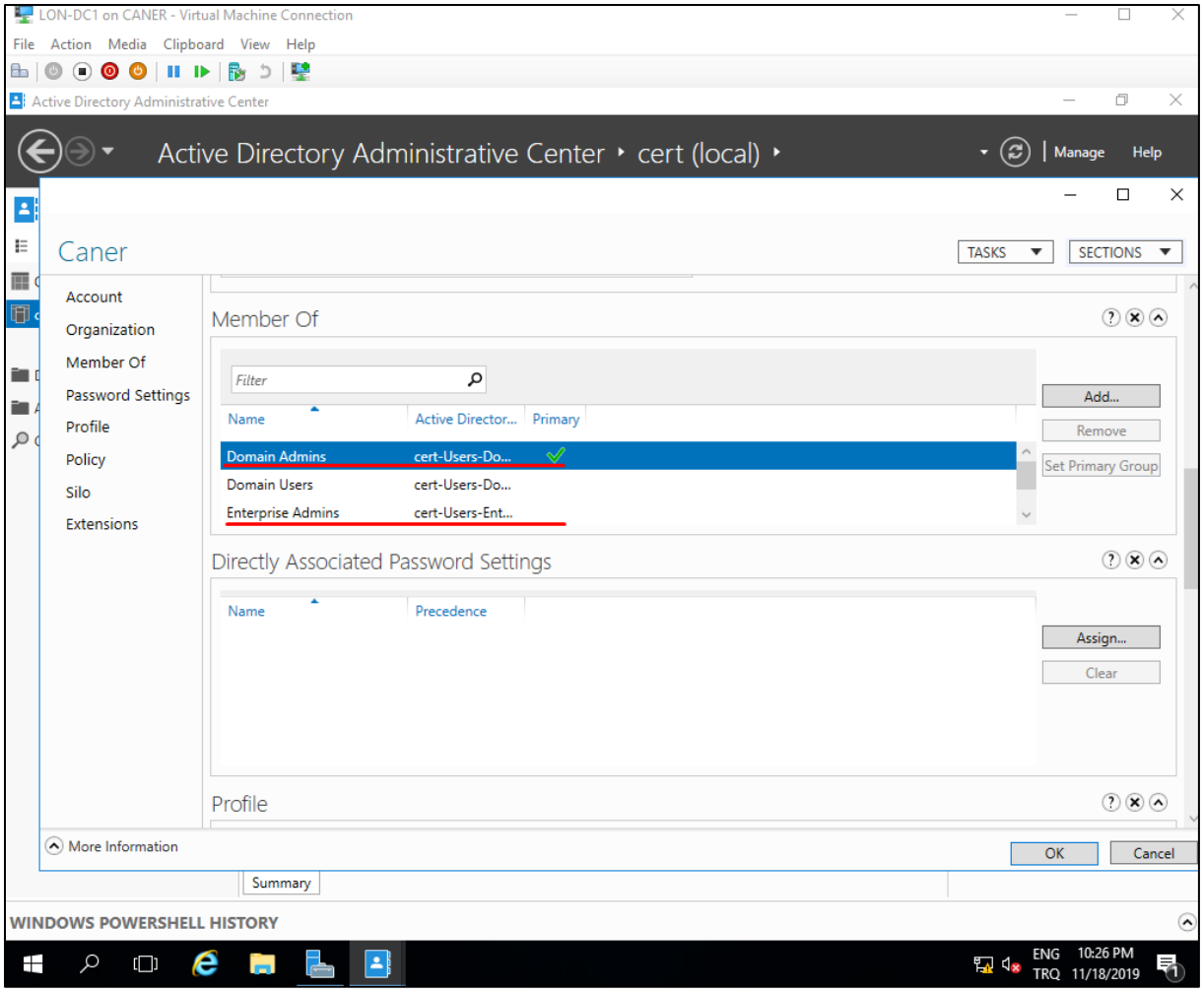

LON-SRV1 on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Server Manager
Server Manager ‣ Dashboard
Manage Tools View Help
Add Roles and Features Wizard
Web Server Role (IIS)
DESTINATION SERVER
LON-SRV1.cert.local
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
Web servers are computers that let you share information over the Internet, or through intranets and extranets. The Web Server role includes Internet Information Services (IIS) 10.0 with enhanced security, diagnostic and administration, a unified Web platform that integrates IIS 10.0, ASP.NET, and Windows Communication Foundation.
The default installation for the Web Server (IIS) role includes the installation of role services that enable you to serve static content, make minor customizations (such as default documents and HTTP errors), monitor and log server activity, and configure static content compression.
More information about Web Server IIS
< Previous
Next >
Install
Cancel
Hide
BPA results
Performance
BPA results
ENG
TRQ
3:44 AM
11/18/2019

Since we chose CA Web Enrollment, a bunch of various features are preselected.



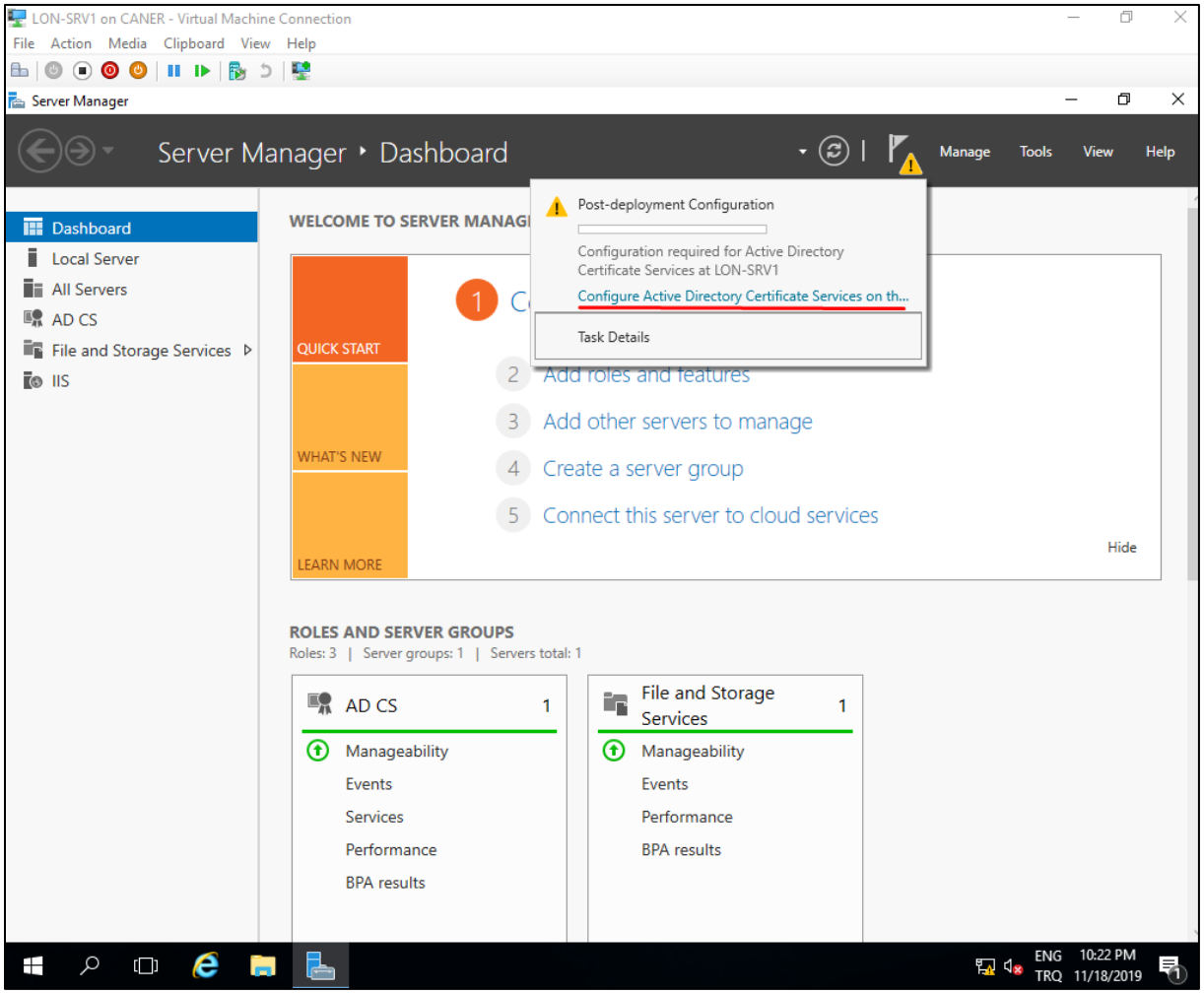
Then, the installation finishes.

Note that, before this point nothing we have done required an explicit use of Active Directory features. However, now we want to create an Enterprise Subordinate CA. For it to be able to be Enterprise, we have to create a user that is both Domain and Enterprise Admin. The administrator account on LON-SRV1 wouldn't work of course because that is a local administrator. For this CA to be Enterprise we need it to distribute the certificate over the entire domain, only an AD User with specific rights can accomplish this task.

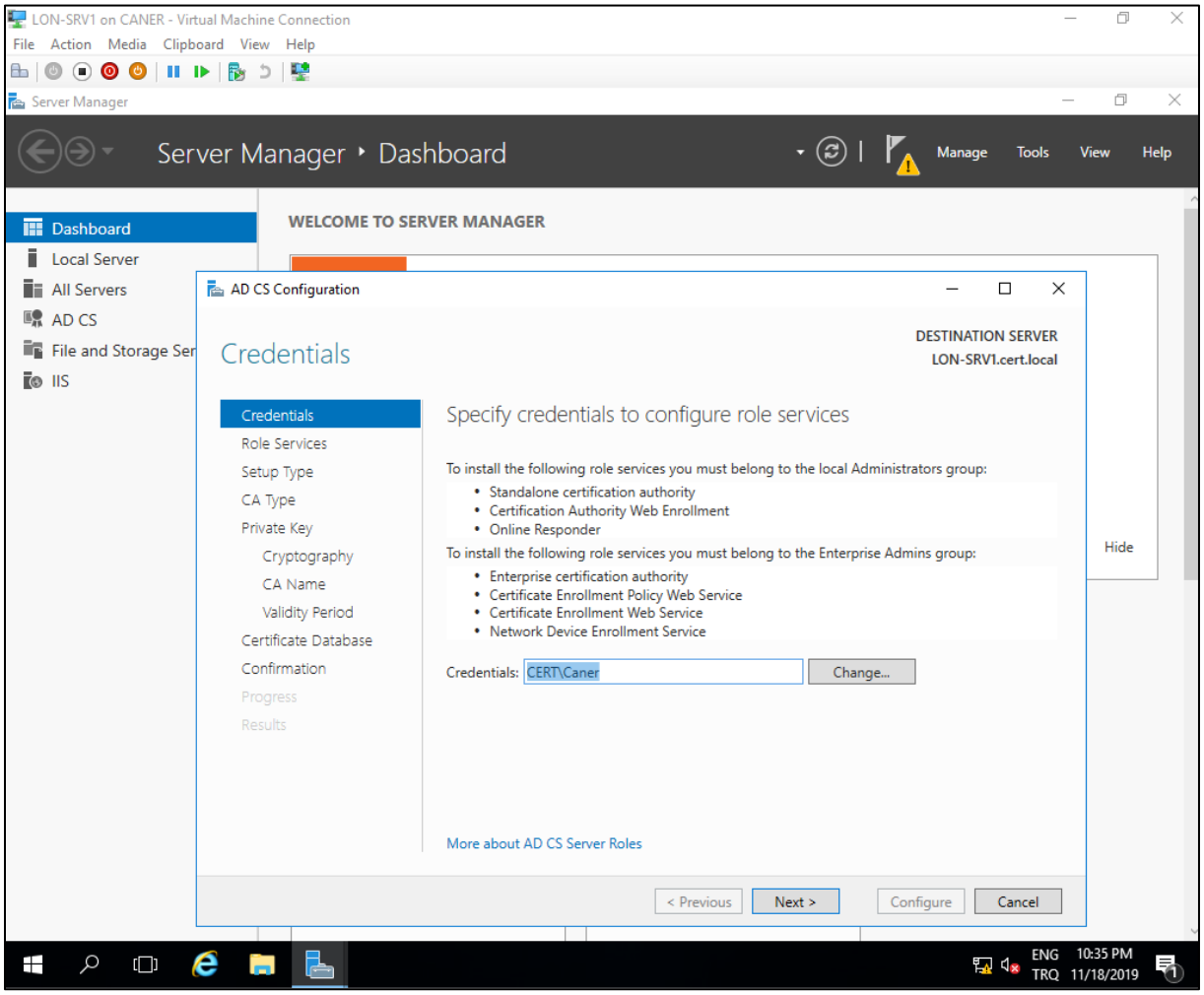


New User Caner is both Domain and Enterprise Admin.

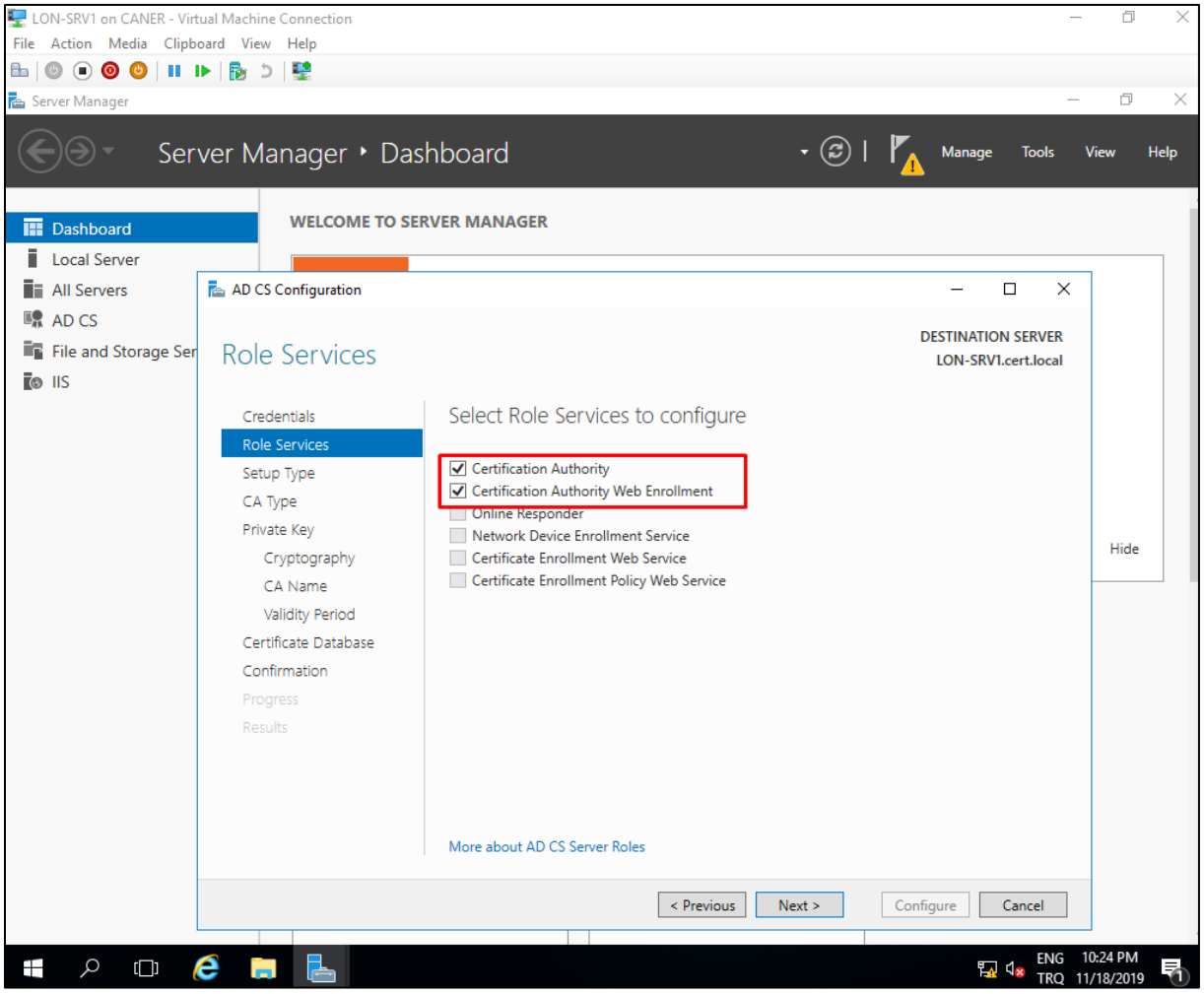
We login to LON-SRV1 with Caner and start the configuration.



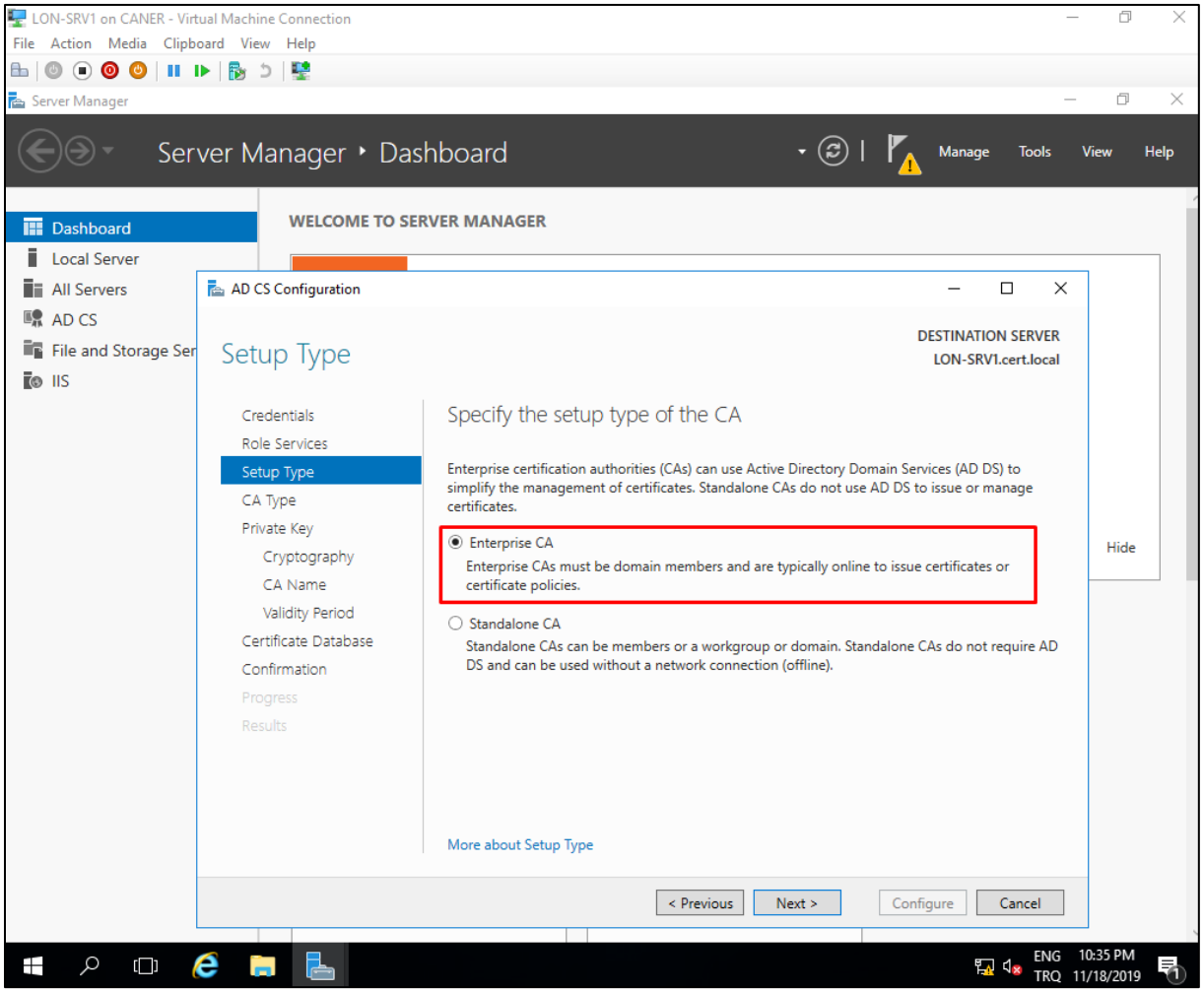
This wizard is exactly the same one that we used on CA-SRV1 to set it up as the Standalone Root CA.



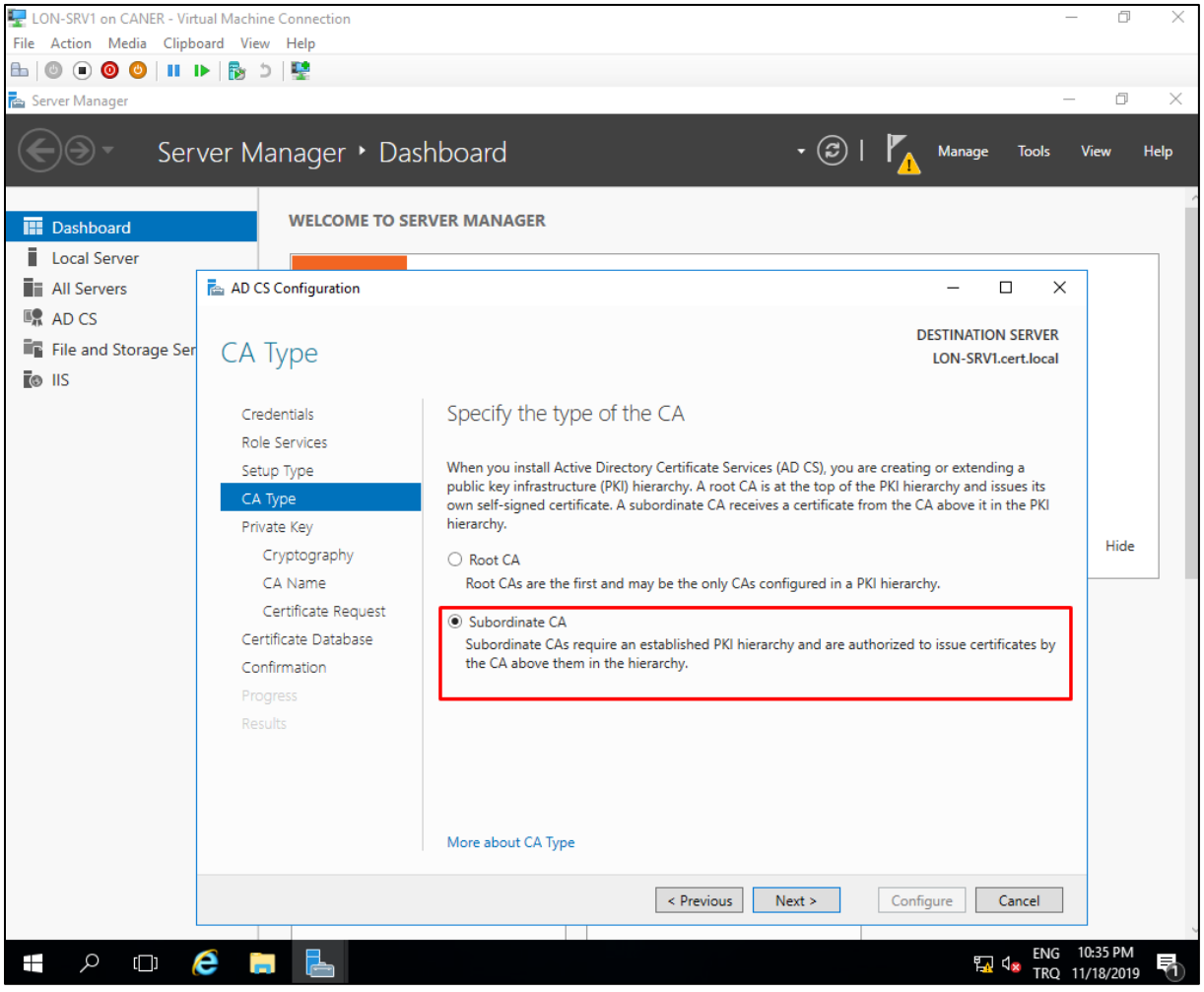
We choose both roles.



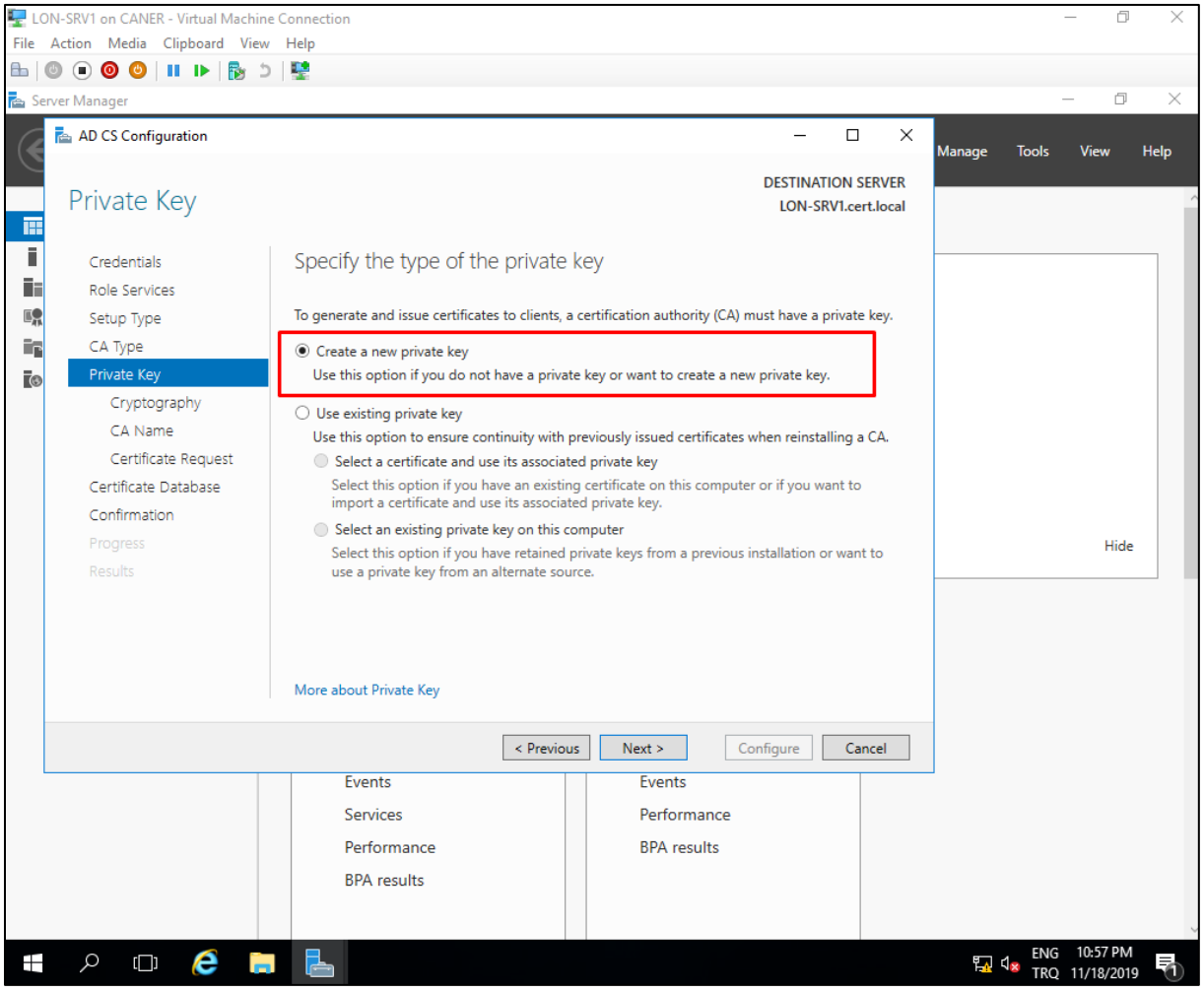
We choose Enterprise CA.



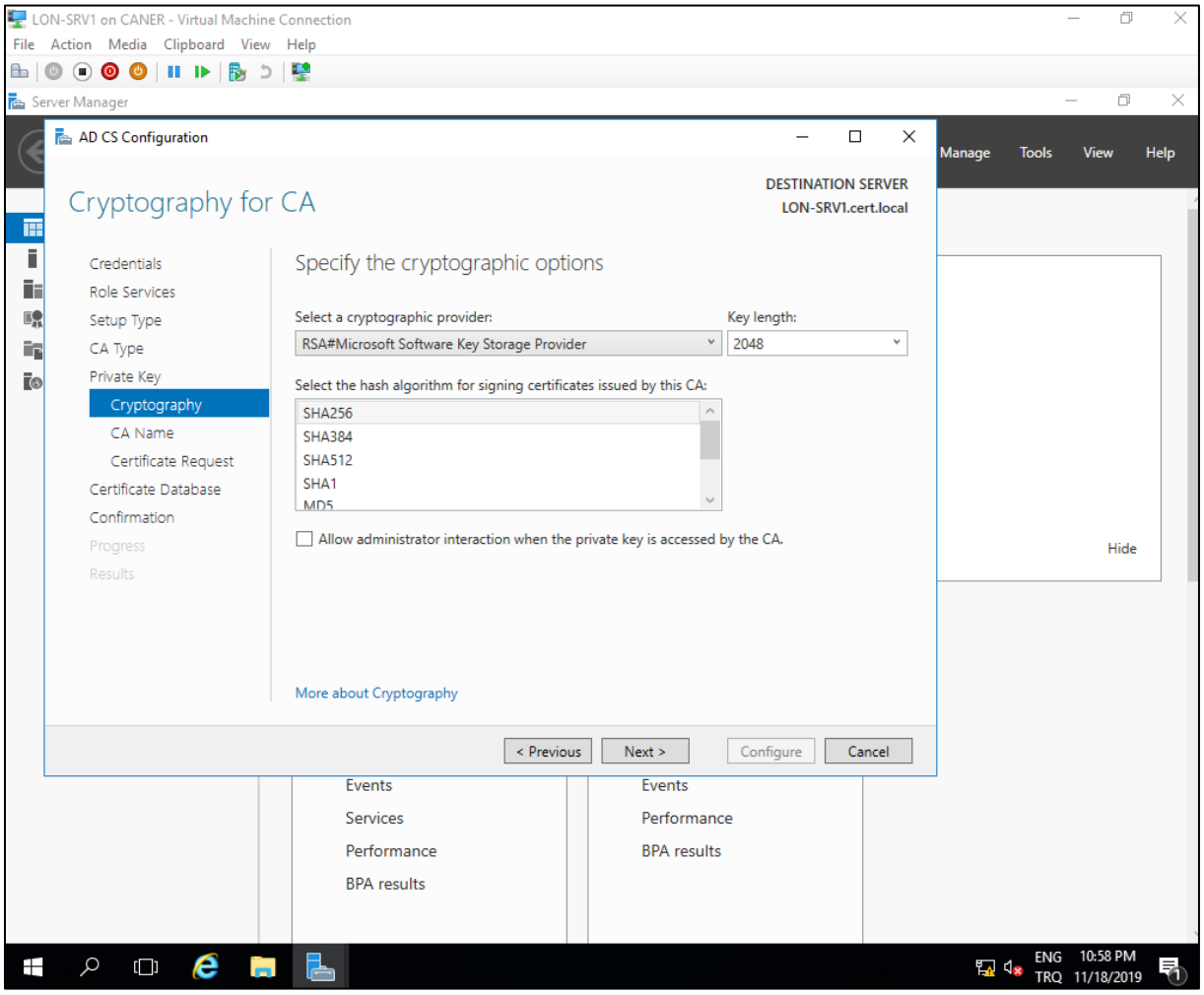
Then, we select Subordinate obviously.



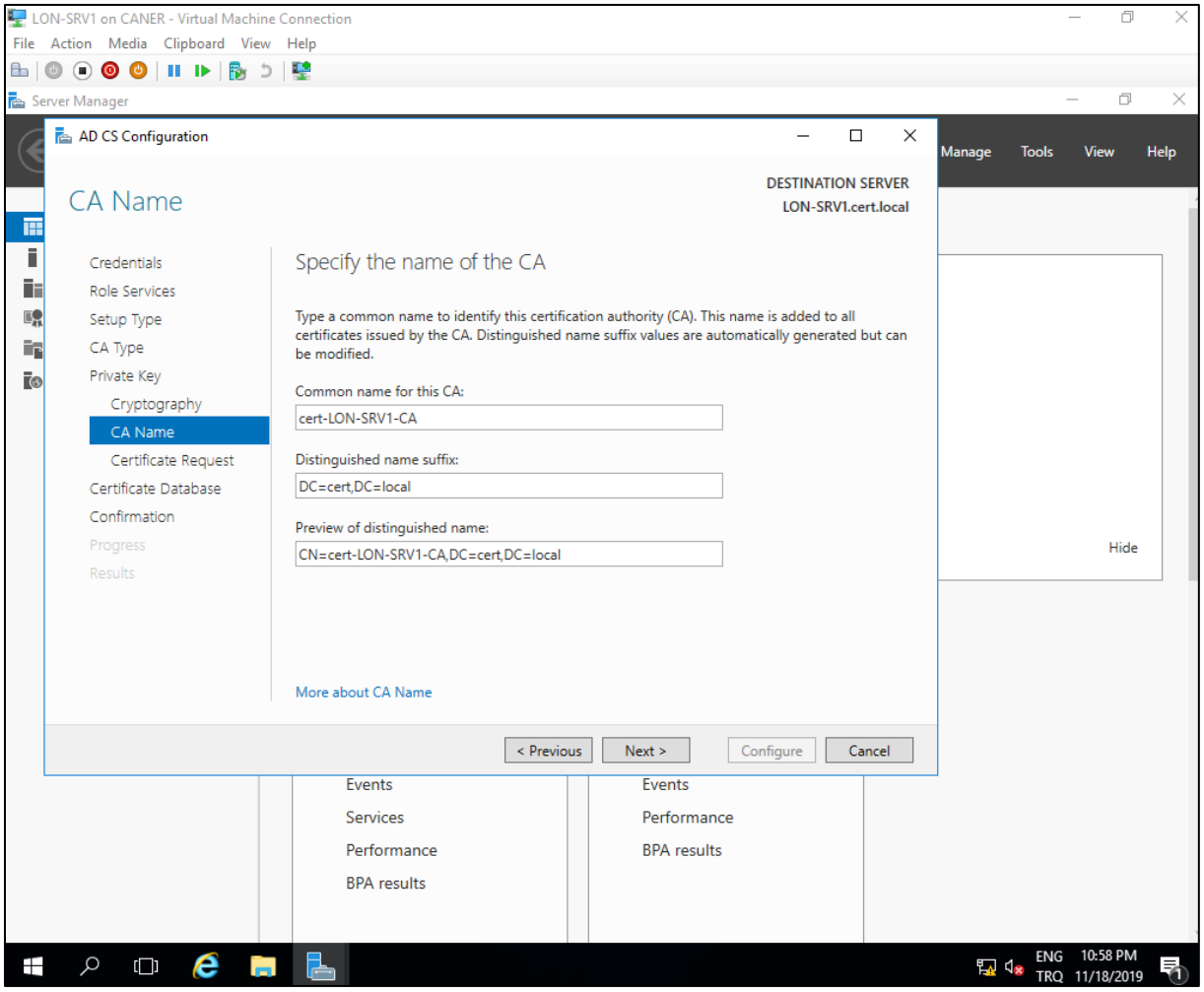
Then, we proceed by creating a new private key.



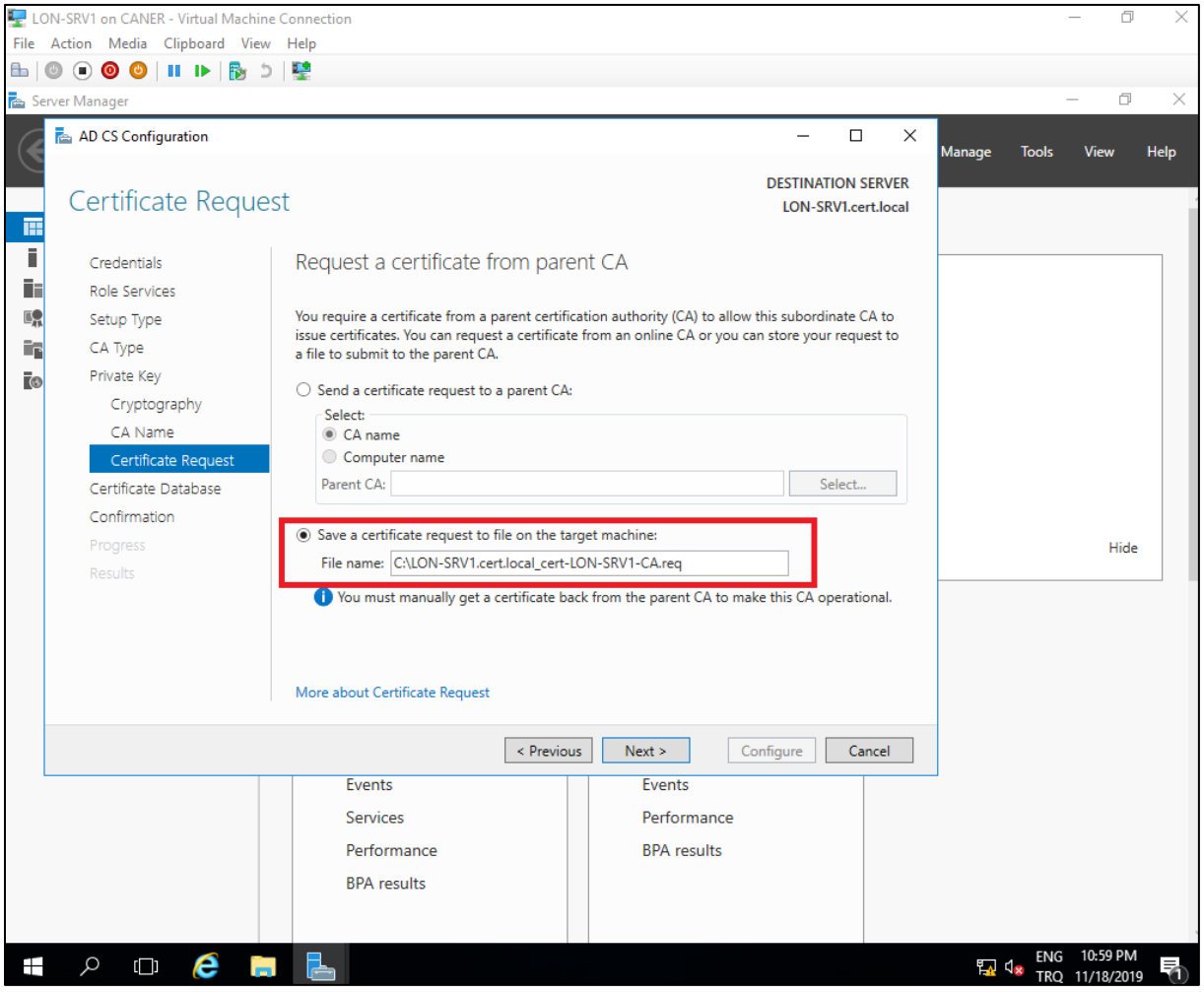
We selected the same specialties for this key as the Standalone CA's but we're not sure if that matters. Otherwise we could have simply requested the previous key.



We did not alter any of the choices here either.

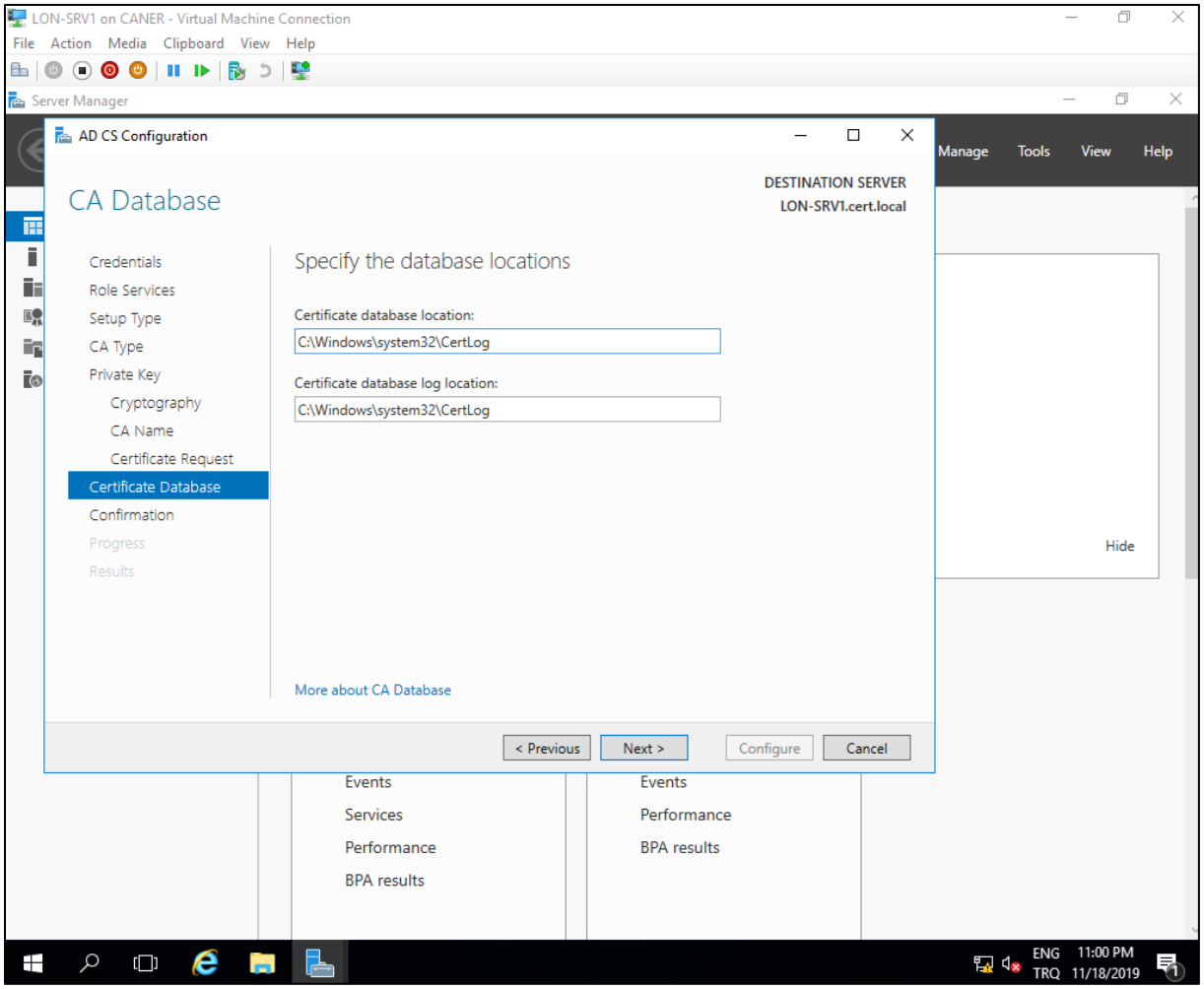


We then choose to create a new request file on disk.

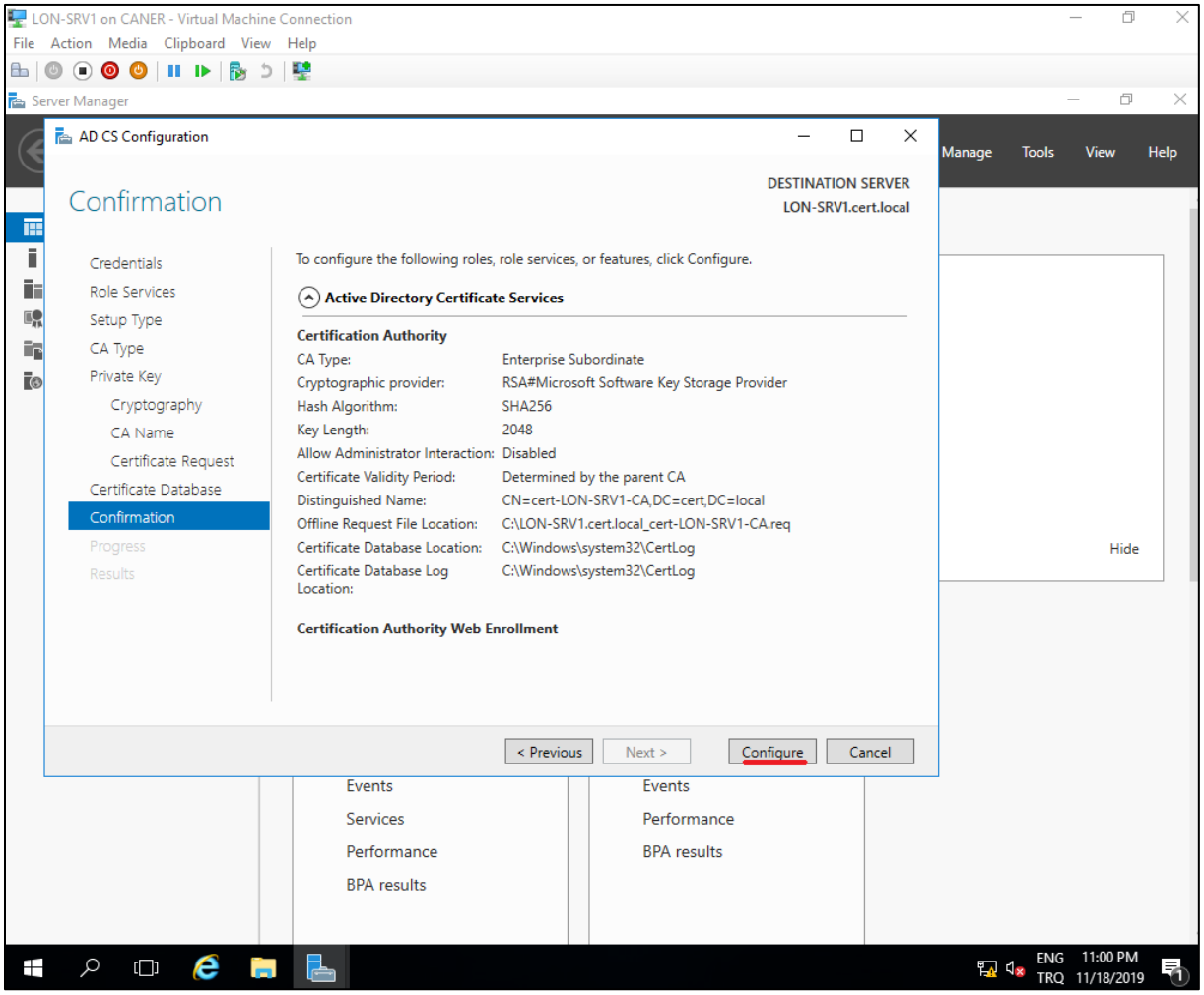


We need to manually transport this request file to the Standalone Root CA and generate the replying certificate later.

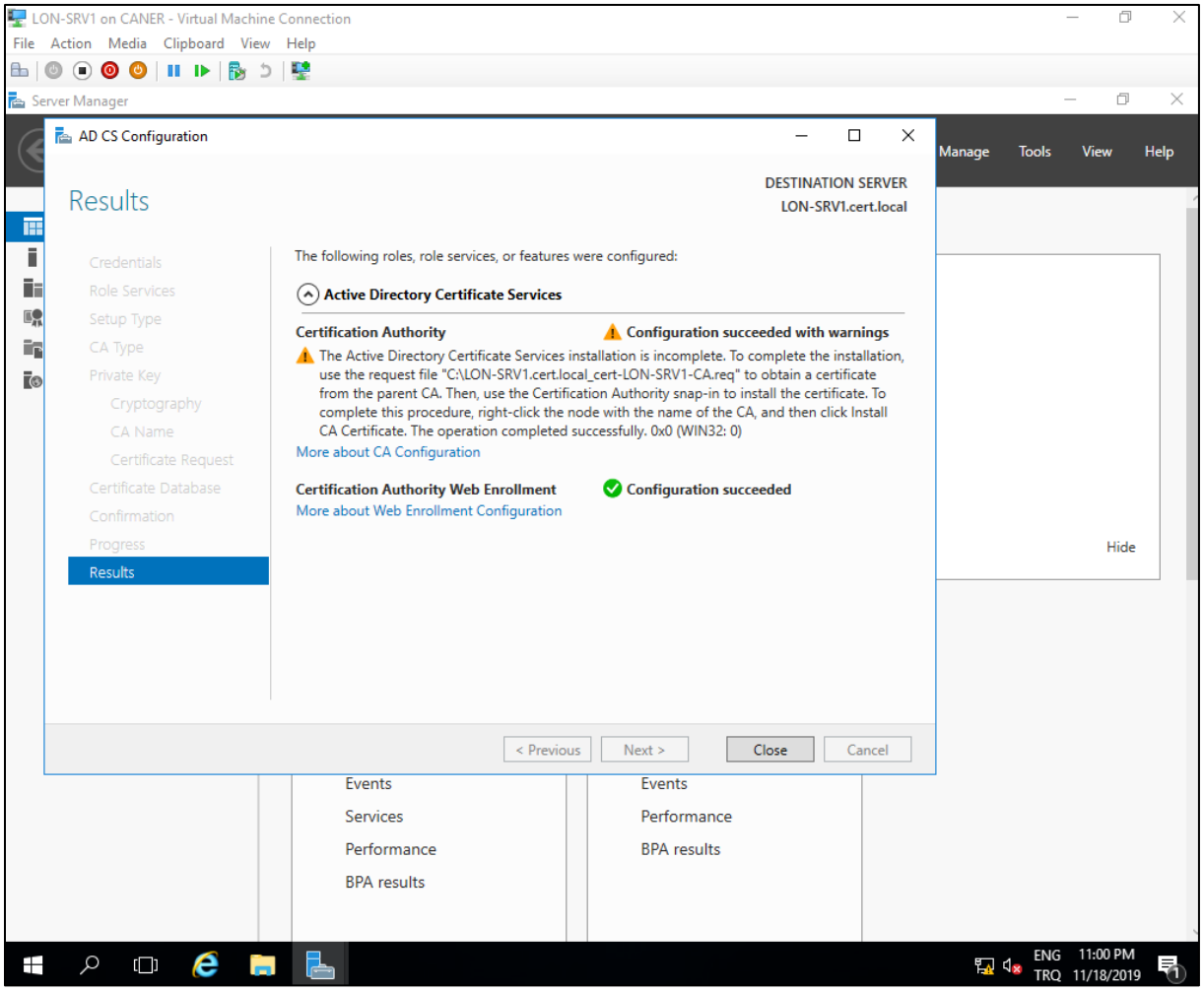
We proceed with the default selections.



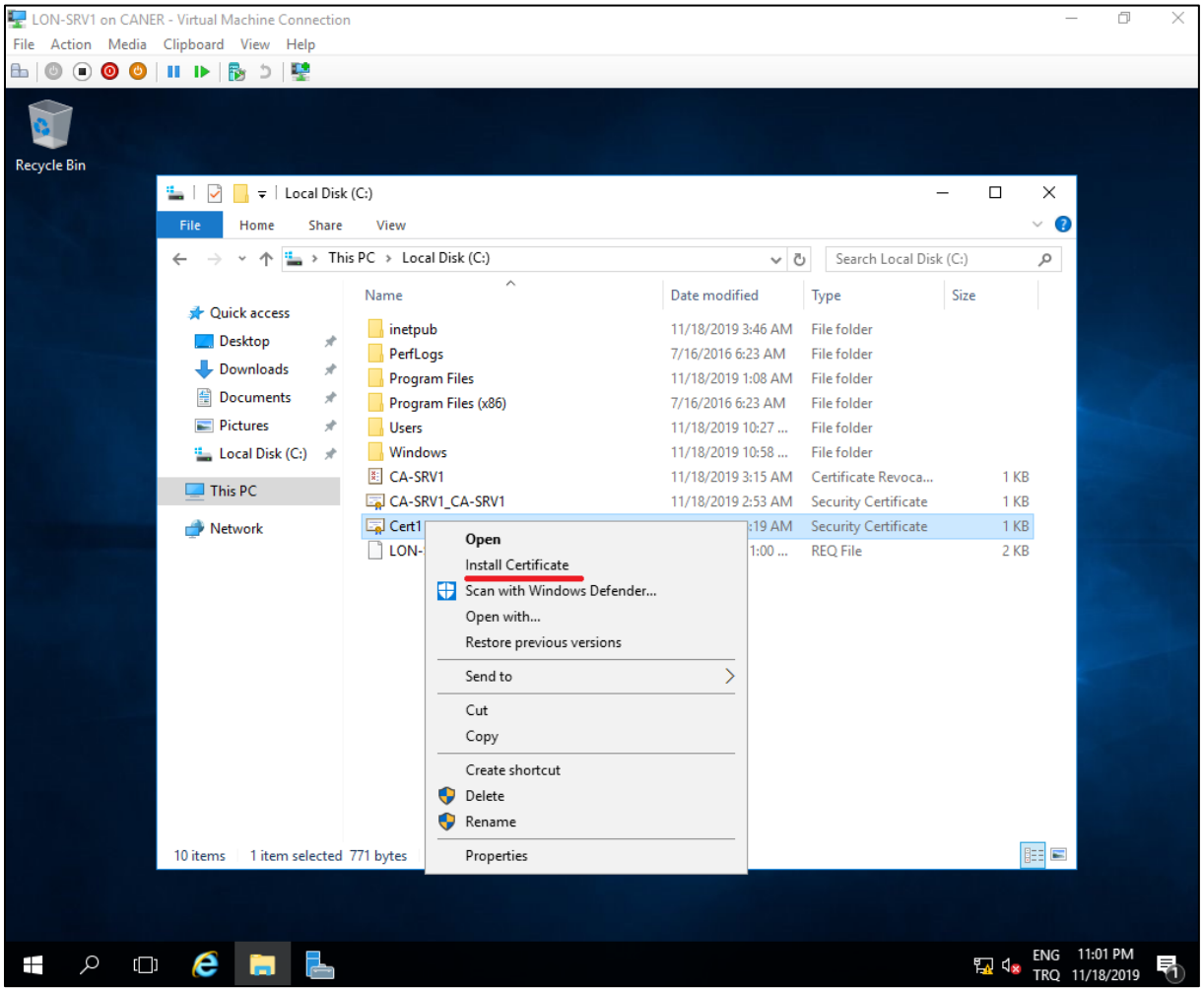
After we see the summary, we finish the configuration.



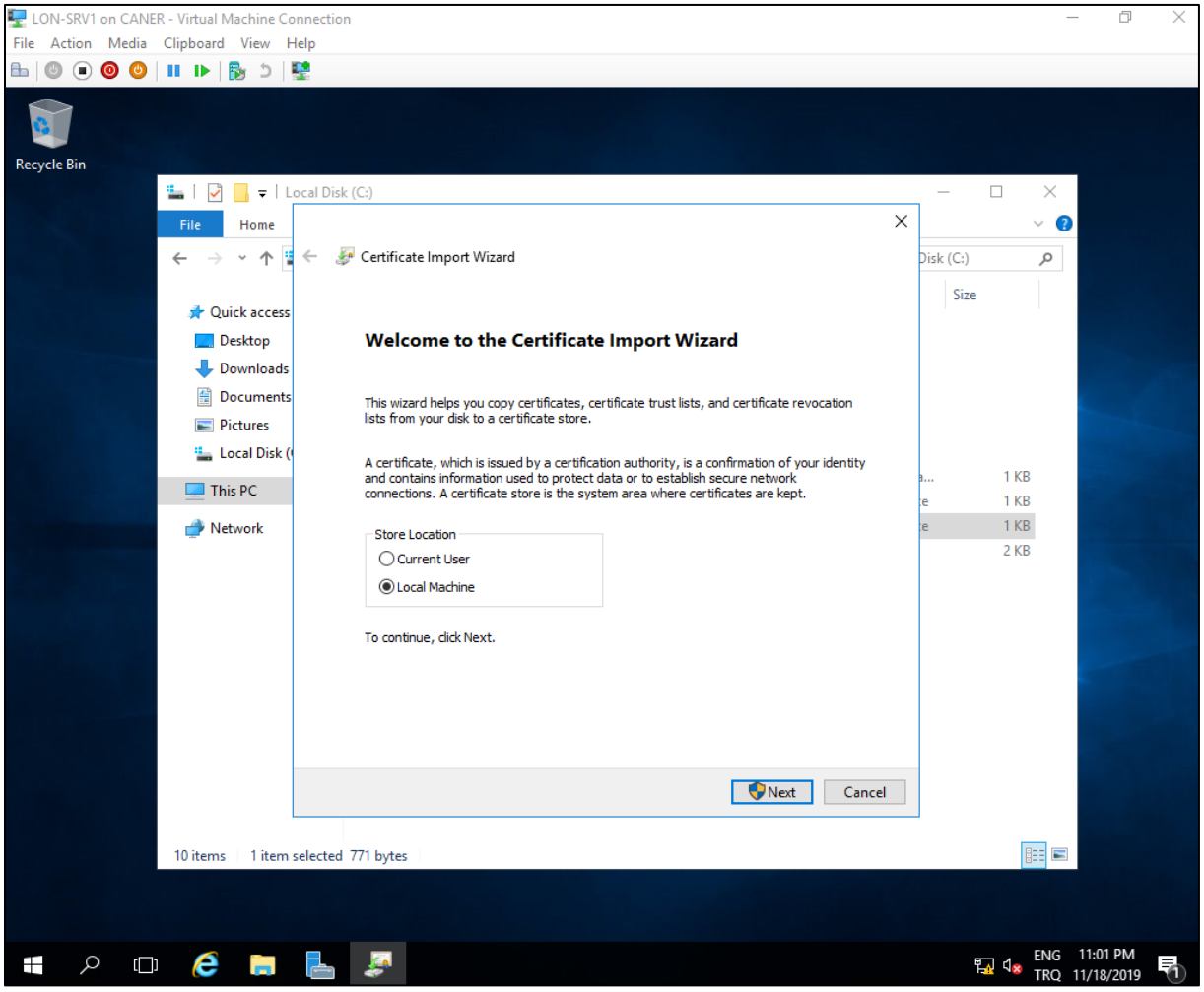
...


LON-SRV1 on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Server Manager
AD CS Configuration
Results
DESTINATION SERVER
LON-SRV1.cert.local
Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Certificate Request
Certificate Database
Confirmation
Progress
Results
The following roles, role services, or features were configured:
Active Directory Certificate Services
Certification Authority
Configuration succeeded with warnings
The Active Directory Certificate Services installation is incomplete. To complete the installation, use the request file "C:\LON-SRV1.cert.local_cert-LON-SRV1-CA.req" to obtain a certificate from the parent CA. Then, use the Certification Authority snap-in to install the certificate. To complete this procedure, right-click the node with the name of the CA, and then click Install CA Certificate. The operation completed successfully. 0x0 (WIN32: 0)
More about CA Configuration
Certification Authority Web Enrollment
Configuration succeeded
More about Web Enrollment Configuration
< Previous
Next >
Close
Cancel
Manage Tools View Help
Hide
Events
Services
Performance
BPA results
Events
Performance
BPA results
ENG
TRQ
11:00 PM
11/18/2019

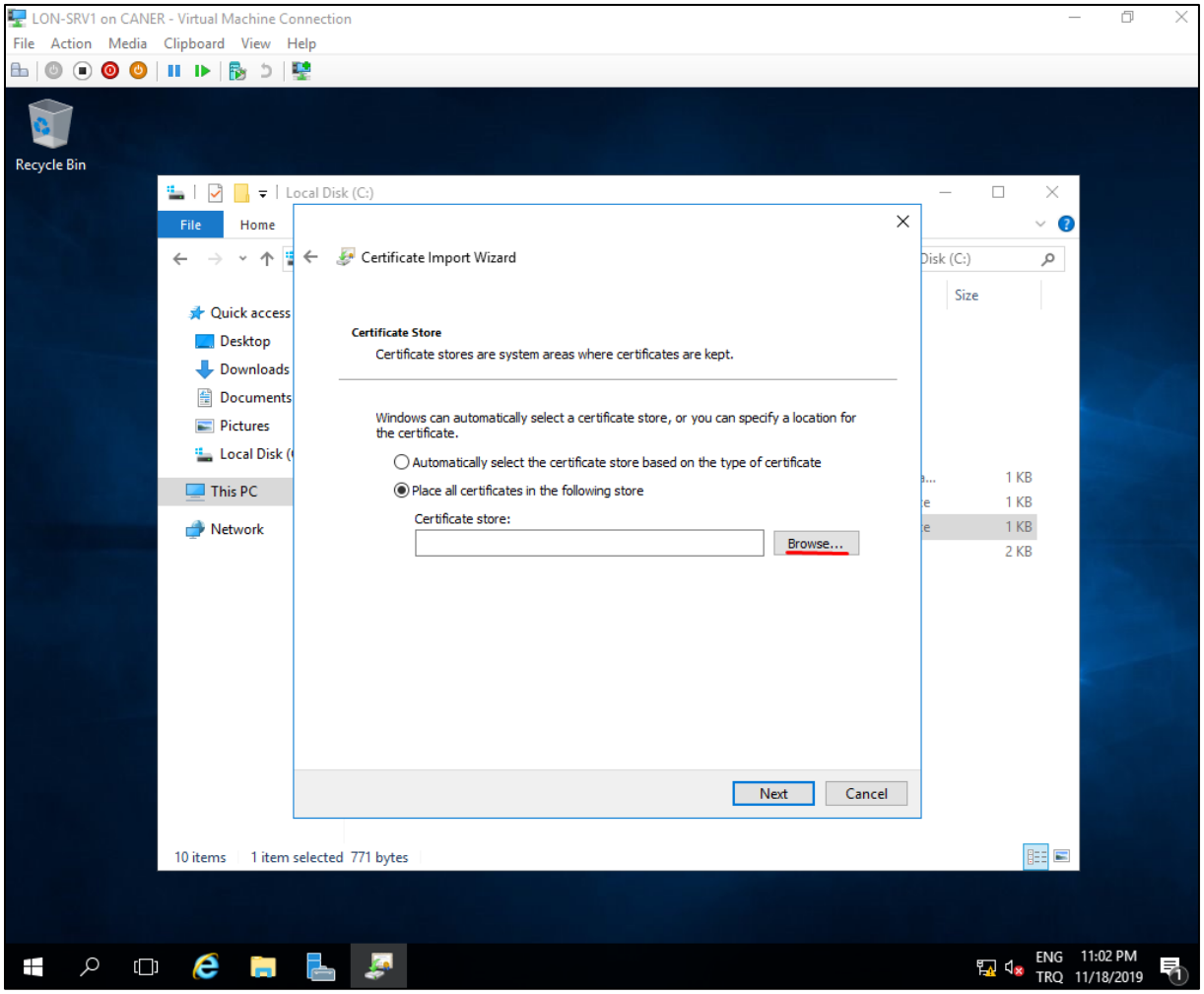
Now we need to install the certificate that CA-SRV1 created to the Trusted Root Certification Authority store. We begin with right clicking on the certificate.



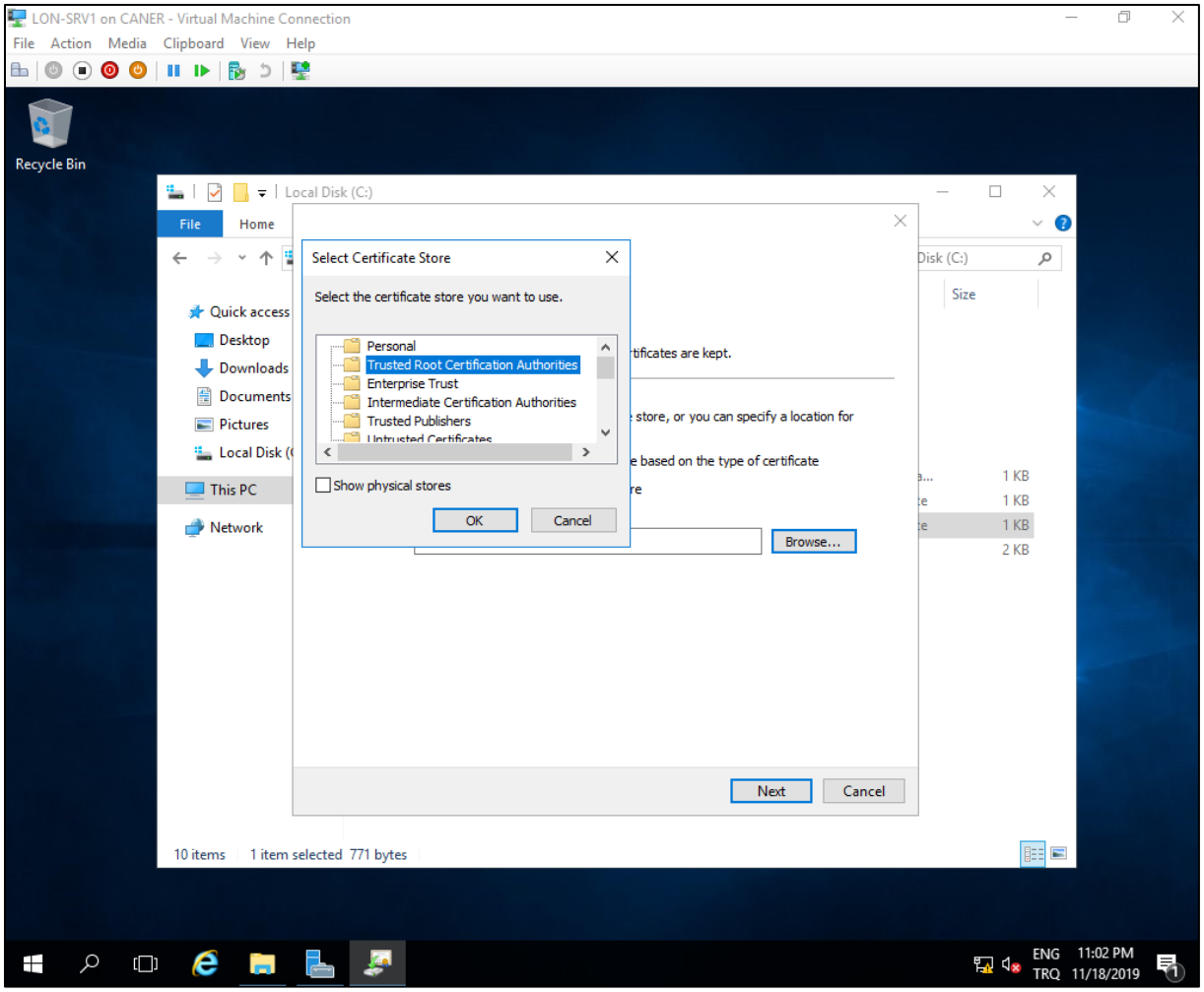
We choose local machine.



We browse…

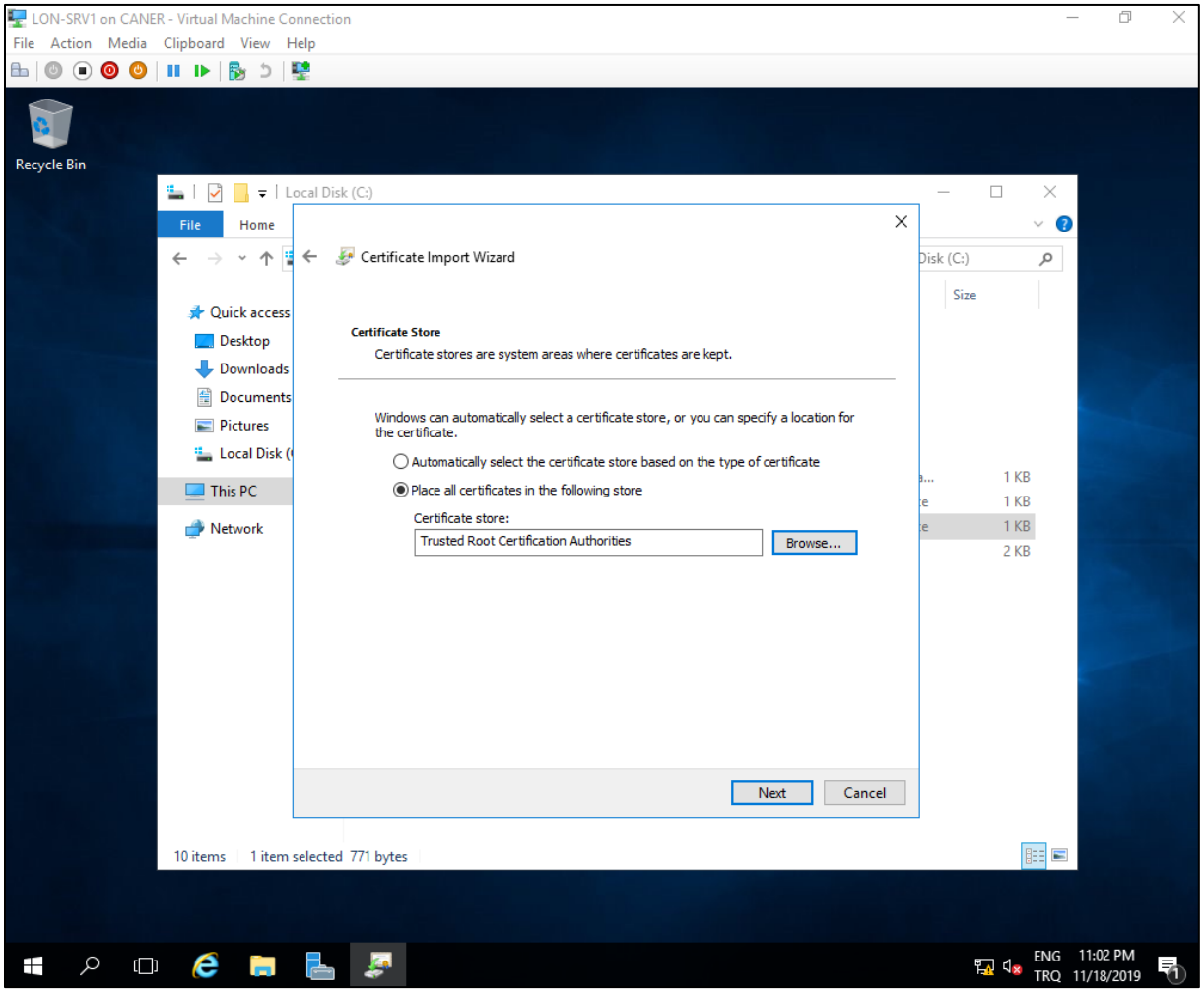

LON-SRV1 on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Local Disk (C:)
File Home
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
Next
Cancel
10 items
1 item selected 771 bytes
ENG
TRQ
11:02 PM
11/18/2019

…to find Trusted Root Certification Authorities.

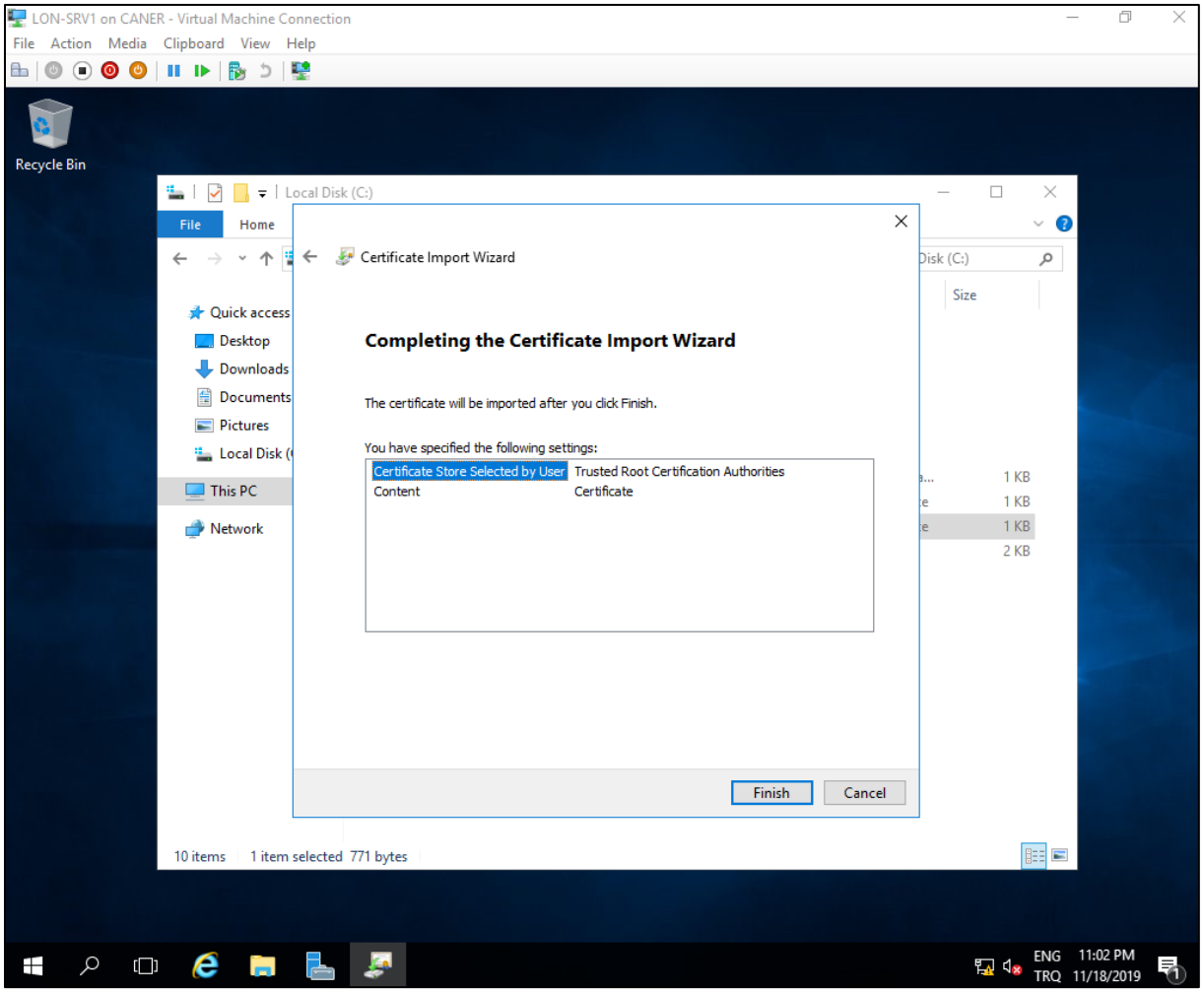


20.11.2019

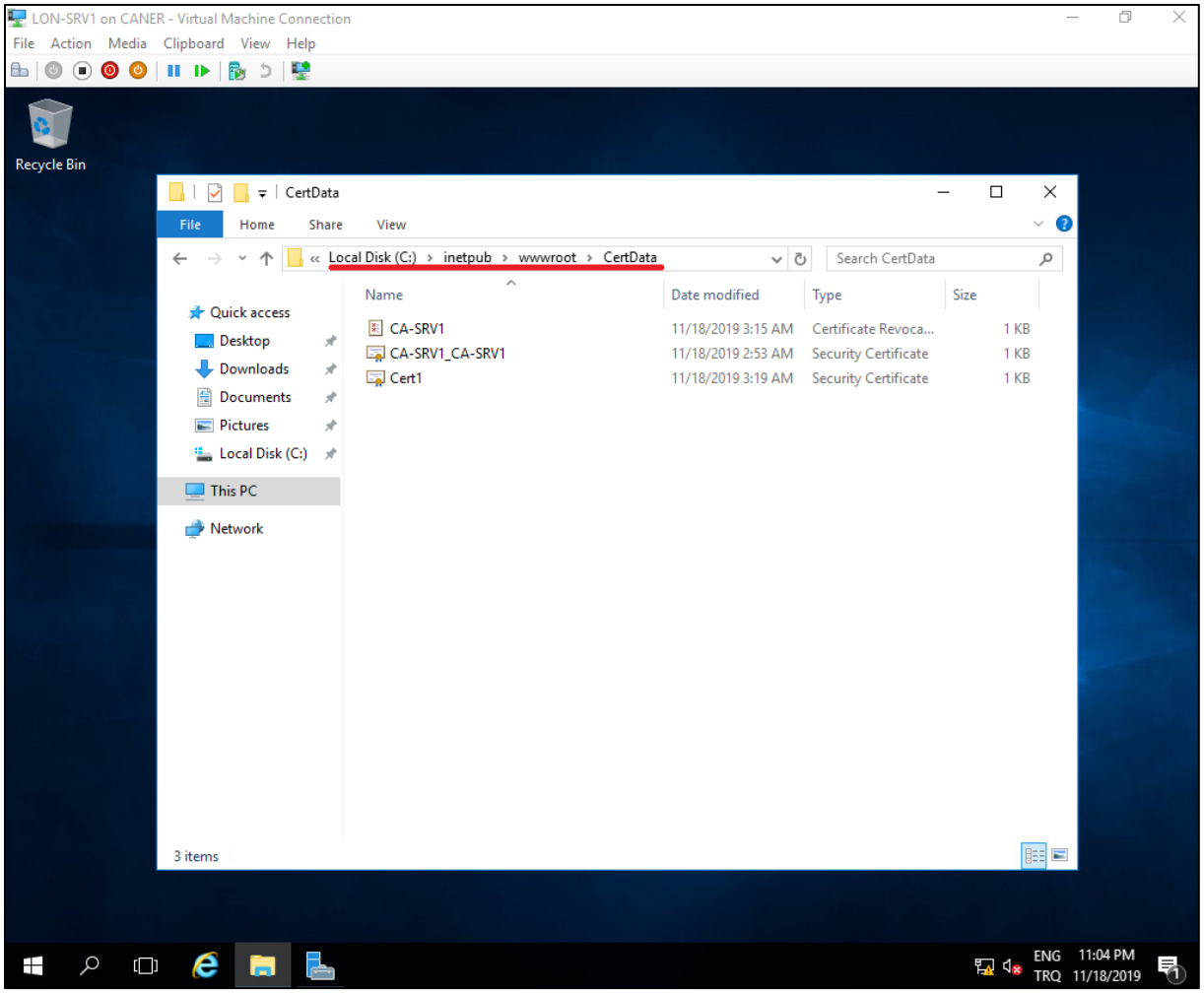
...


LON-SRV1 on CANER - Virtual Machine Connection
File Action Media Clipboard View Help
Recycle Bin
Local Disk (C:)
File Home
Quick access
Desktop
Downloads
Documents
Pictures
Local Disk (
This PC
Network
Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Trusted Root Certification Authorities
Browse...
Next
Cancel
10 items
1 item selected 771 bytes
Size
1 KB
1 KB
1 KB
2 KB
ENG
TRQ
11:02 PM
11/18/2019

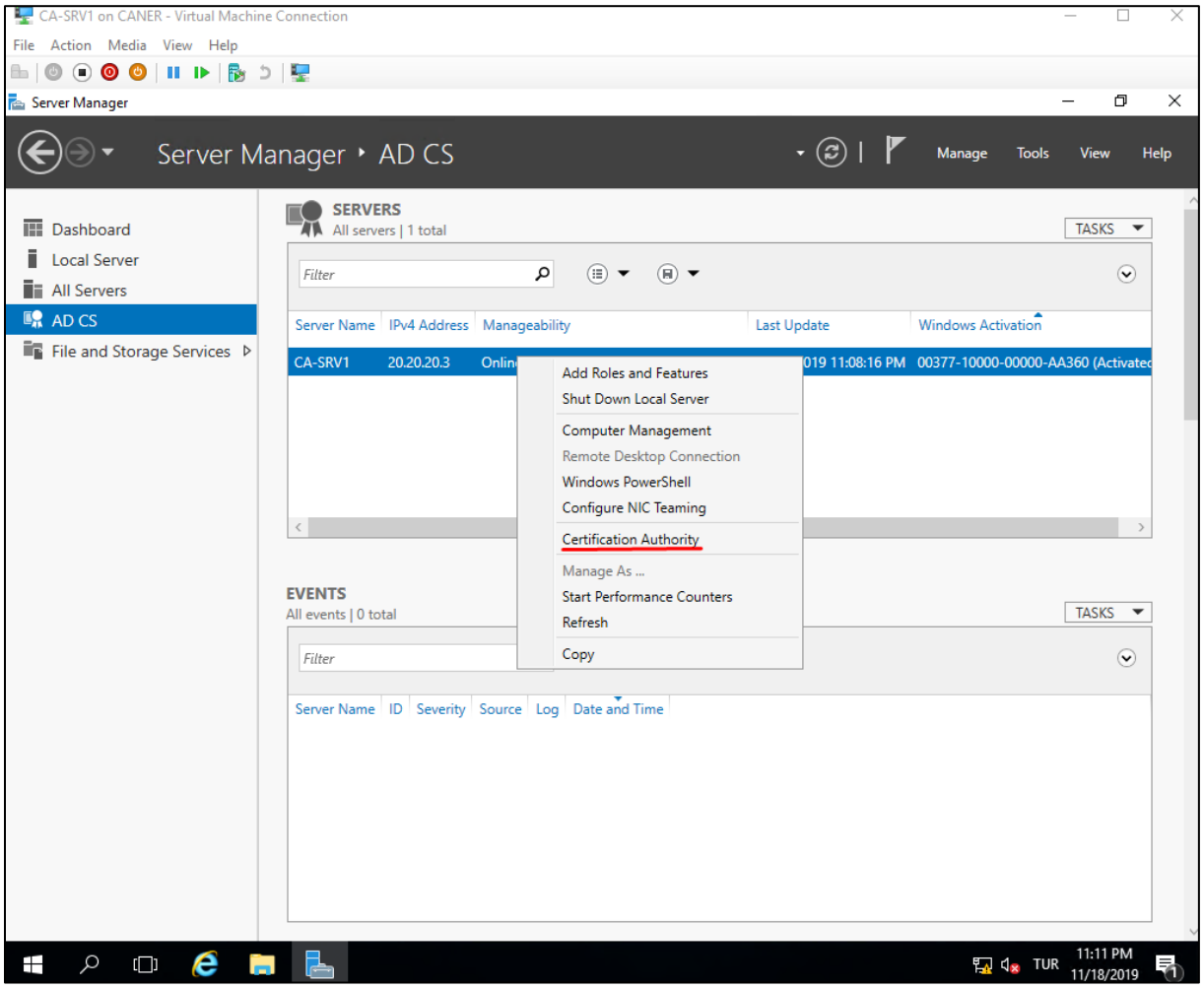
We finish this process.



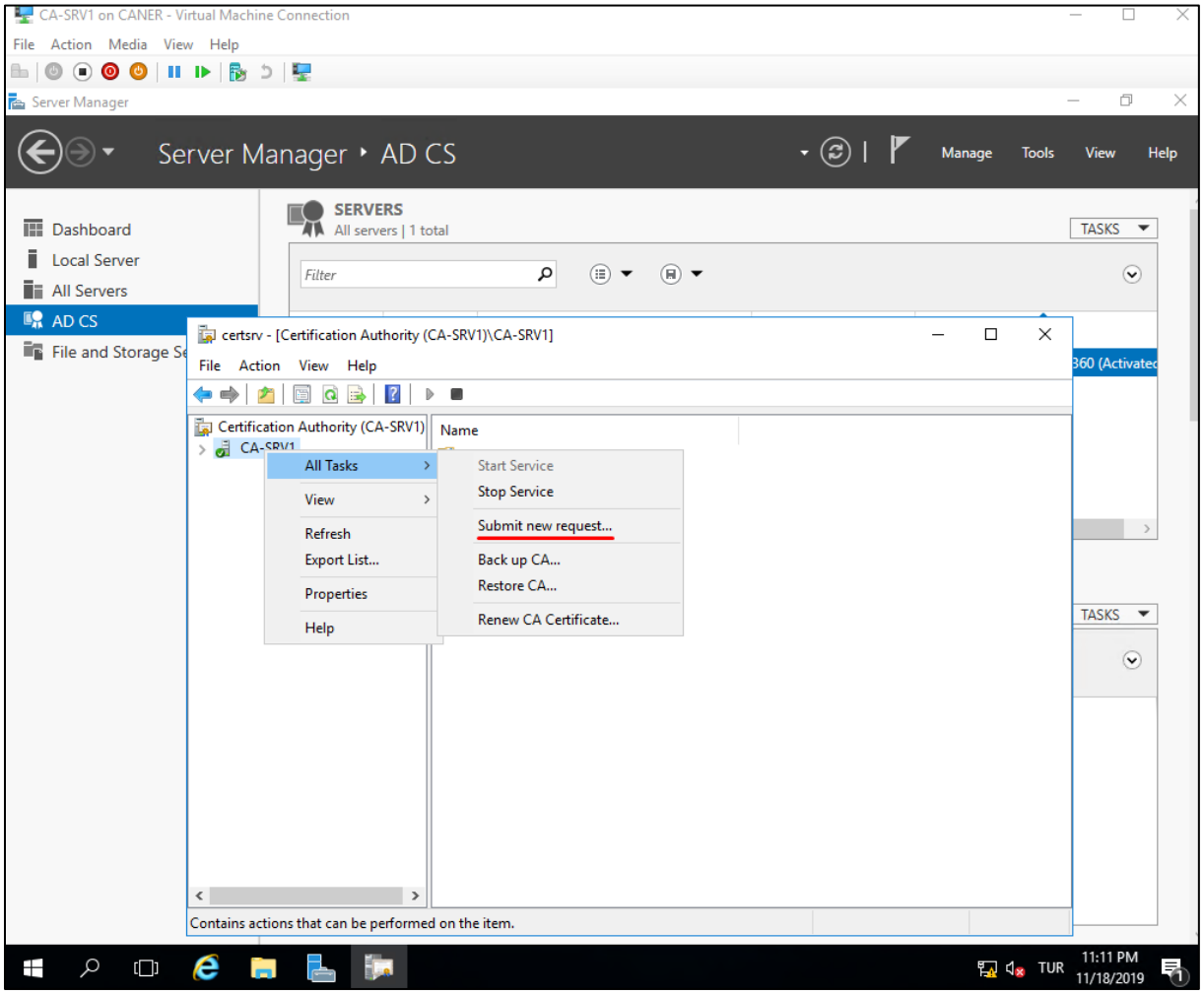
Then, we copy the ".crl" and ".crt" files to C:\inetpub\wwwroot\CertData



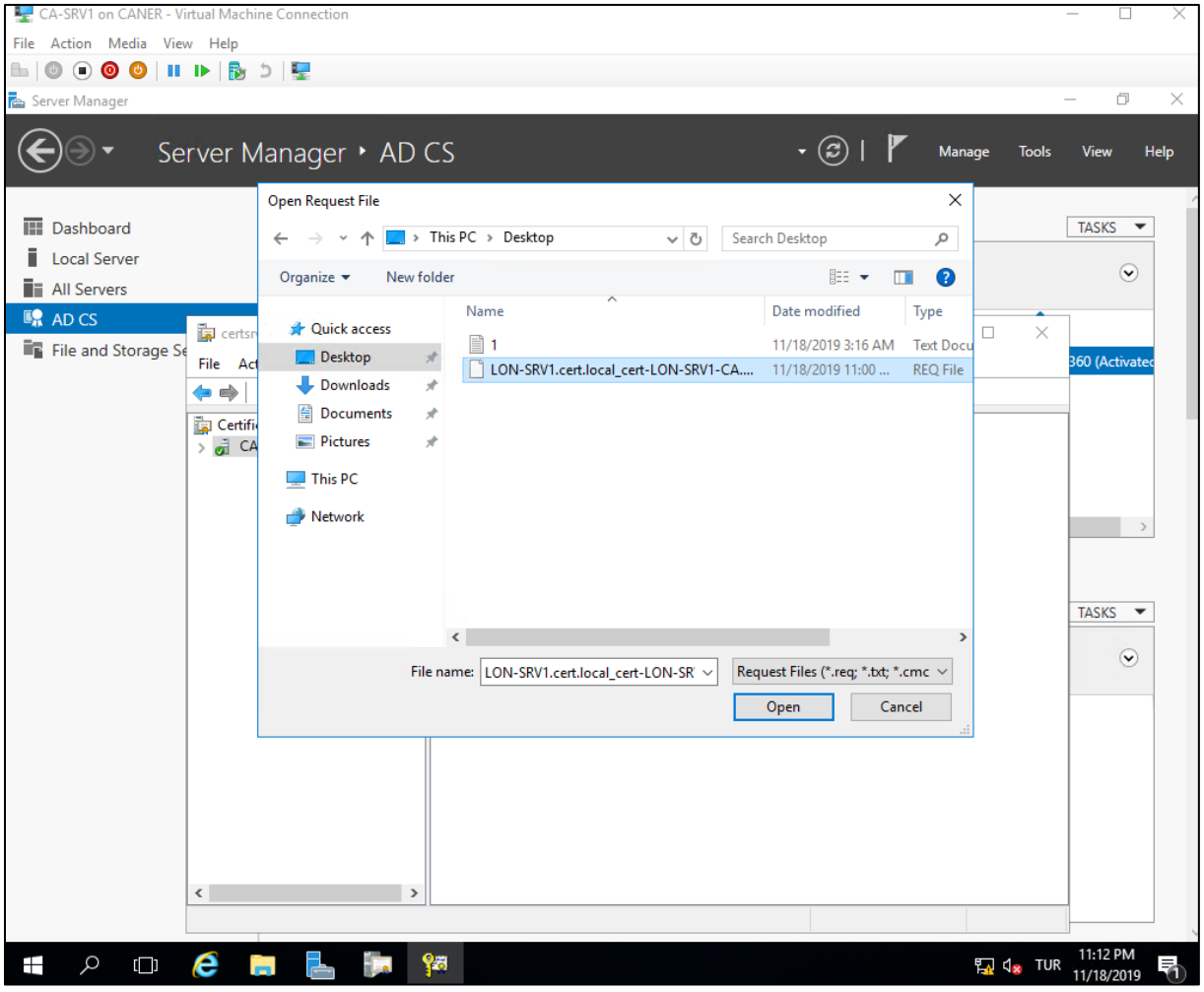
Then, we need to copy the request file from LON-SRV1 to CA-SRV1 and submit a new request for the certificate. For this, after transferring the file we get to Certification Authority on the Standalone Root CA which is CA-SRV1 for our topology.



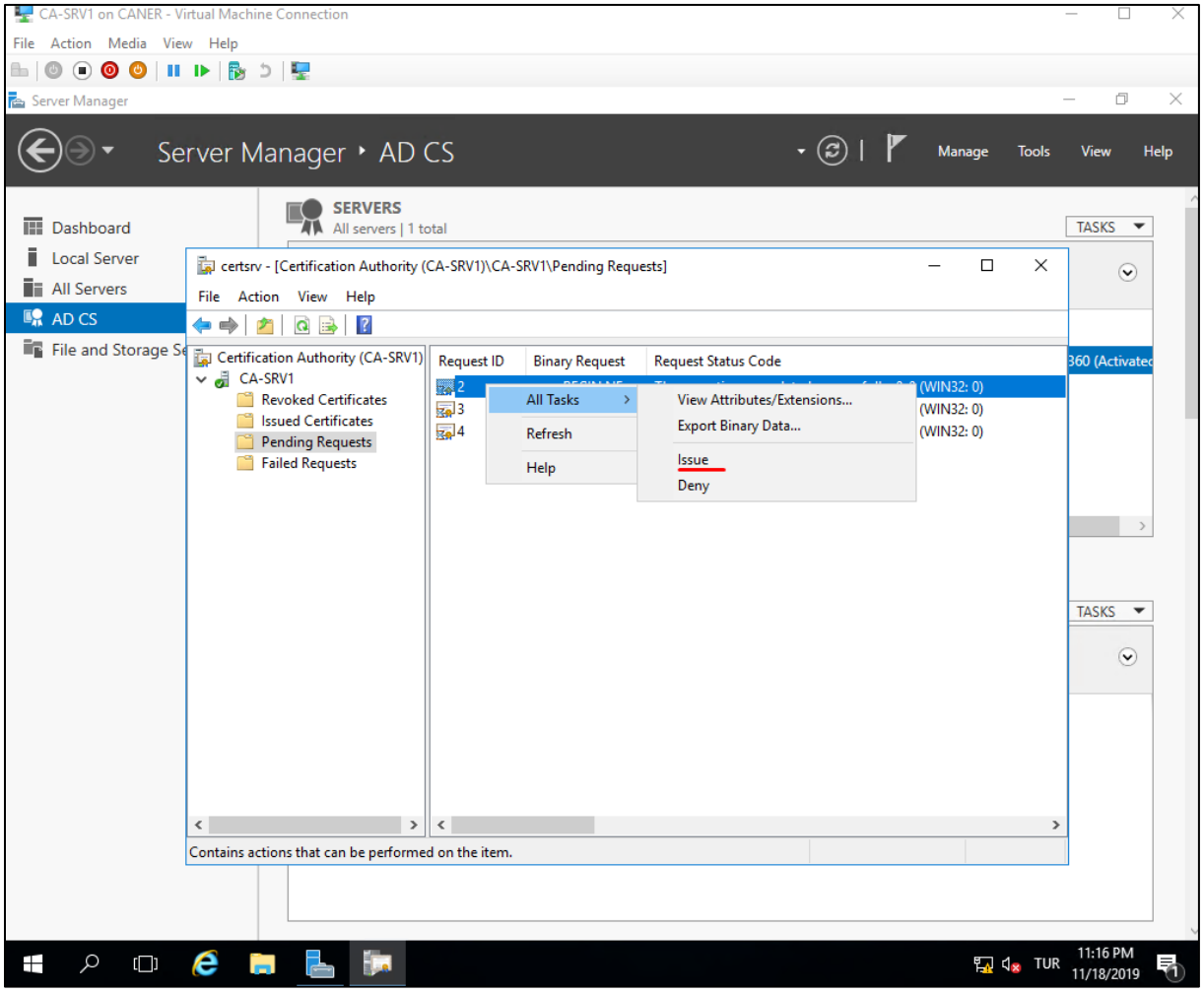
We submit a new request form via right-clicking, choosing All Tasks and then Submit new request…



We locate the .req file that we copied over from LON-SRV1.

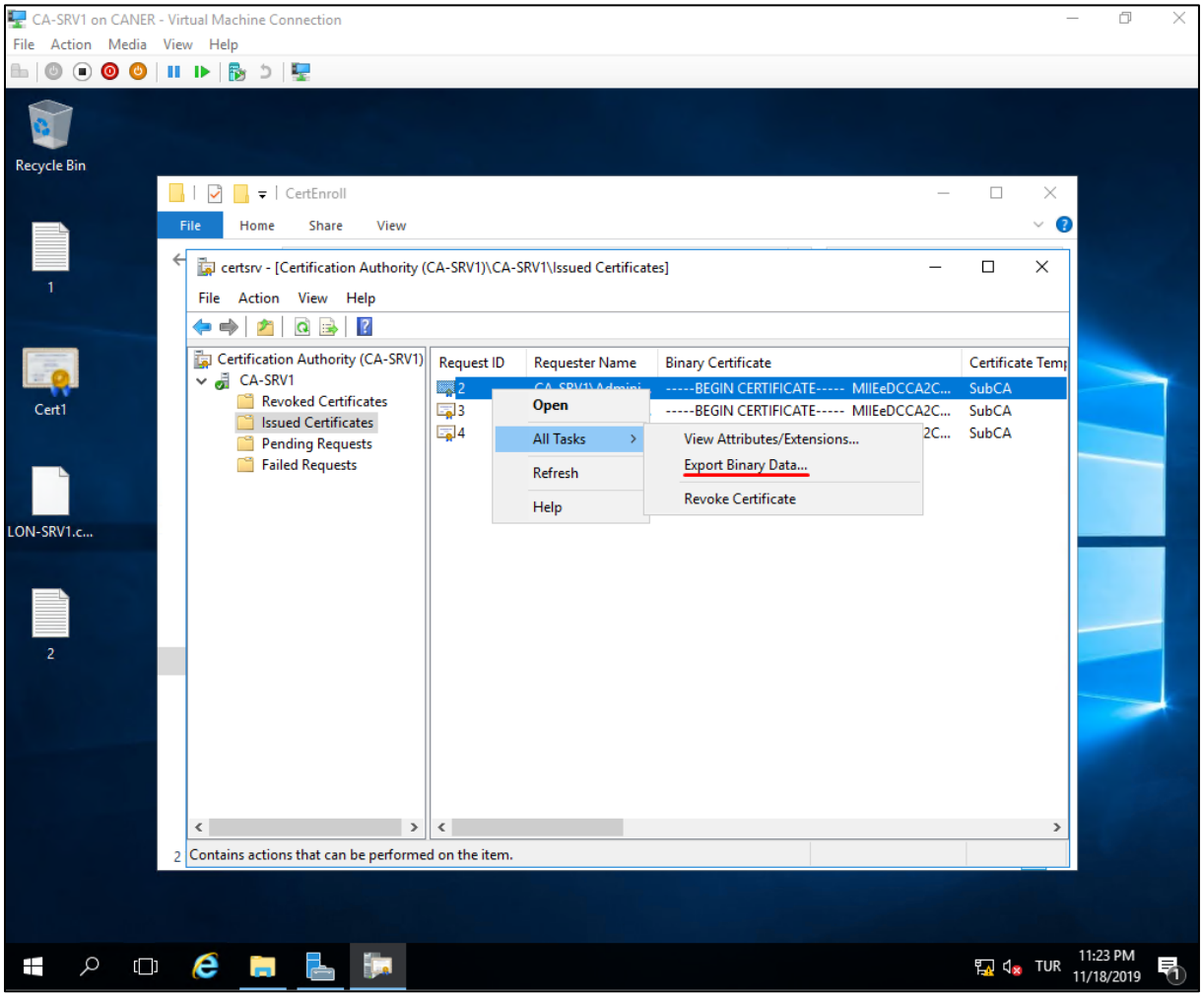


This creates a pending request for the certificate. We right-click to issue the certificate.



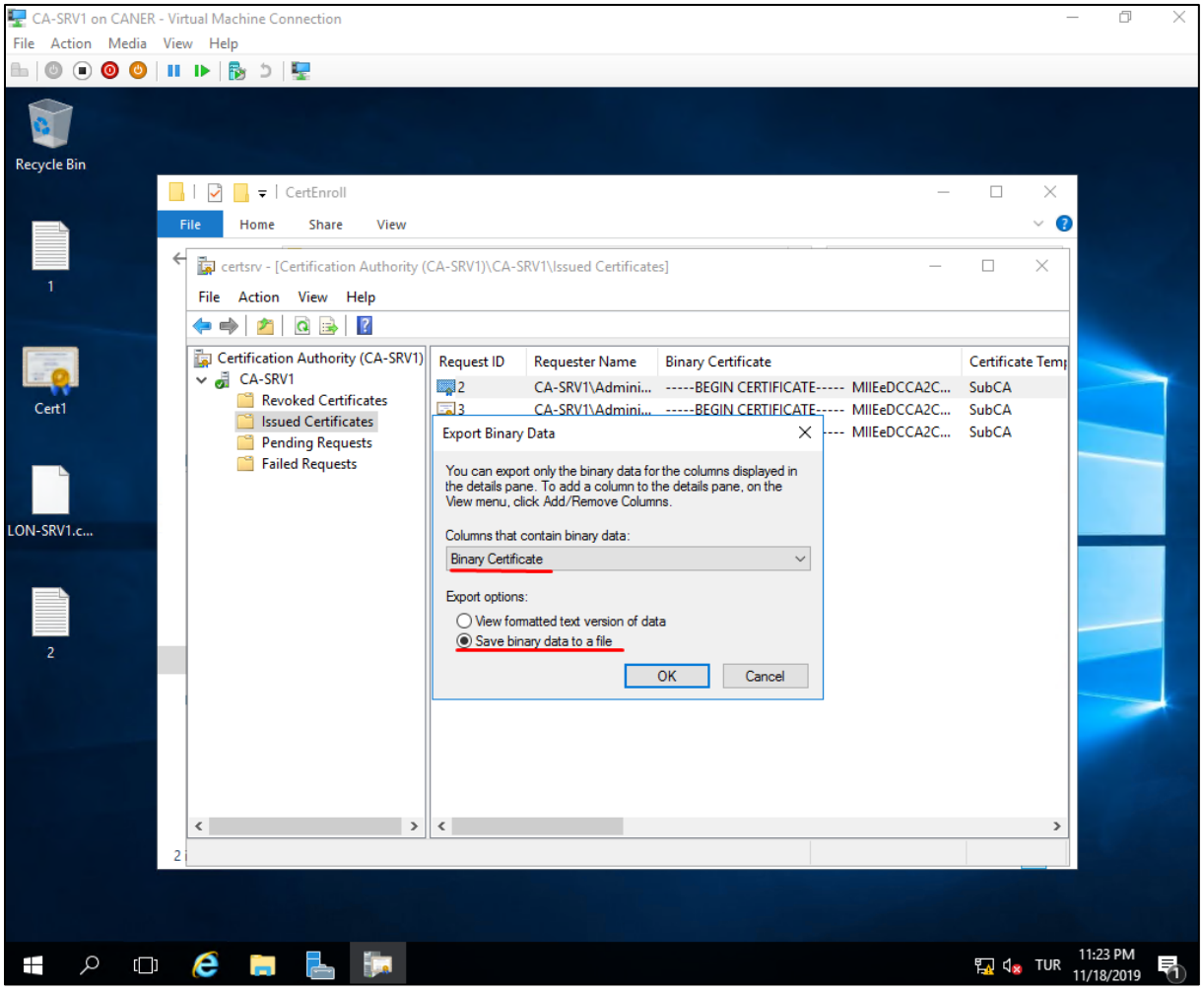
We need to export this freshly issued certificate in .p7b format and copy it to the Enterprise Subordinate CA, which is LON-SRV1, in this case. Note that probably how I have done this was erroneous. Probably, choosing “Copy to File…” from the Details tab of the properties of the certificate would have been a better way to do this. However, here is how I have actually done it in this project.

We right-click and choose Export Binary and Data…

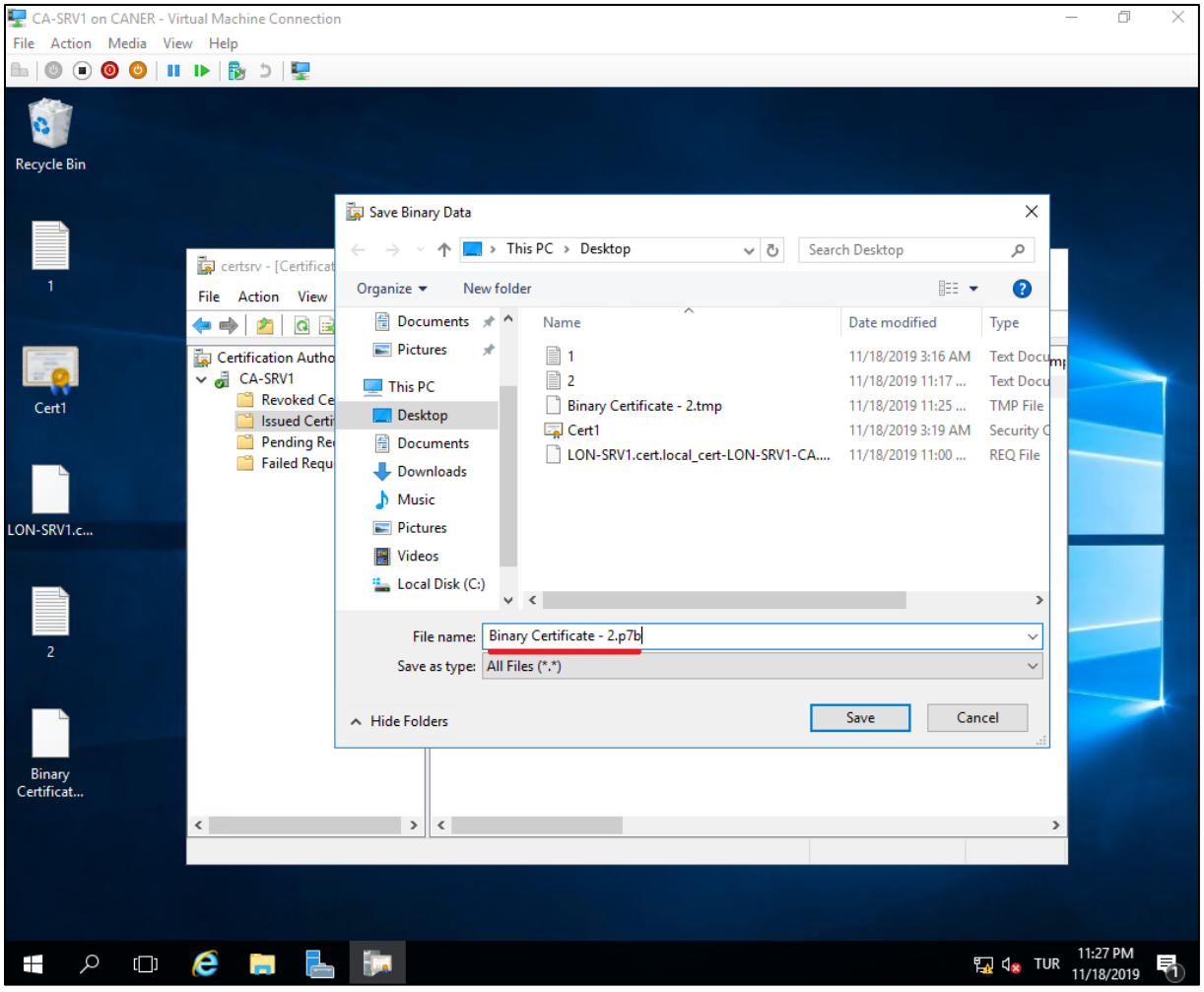


Note that we selected the certificate from the Issued Certificates folder this time.

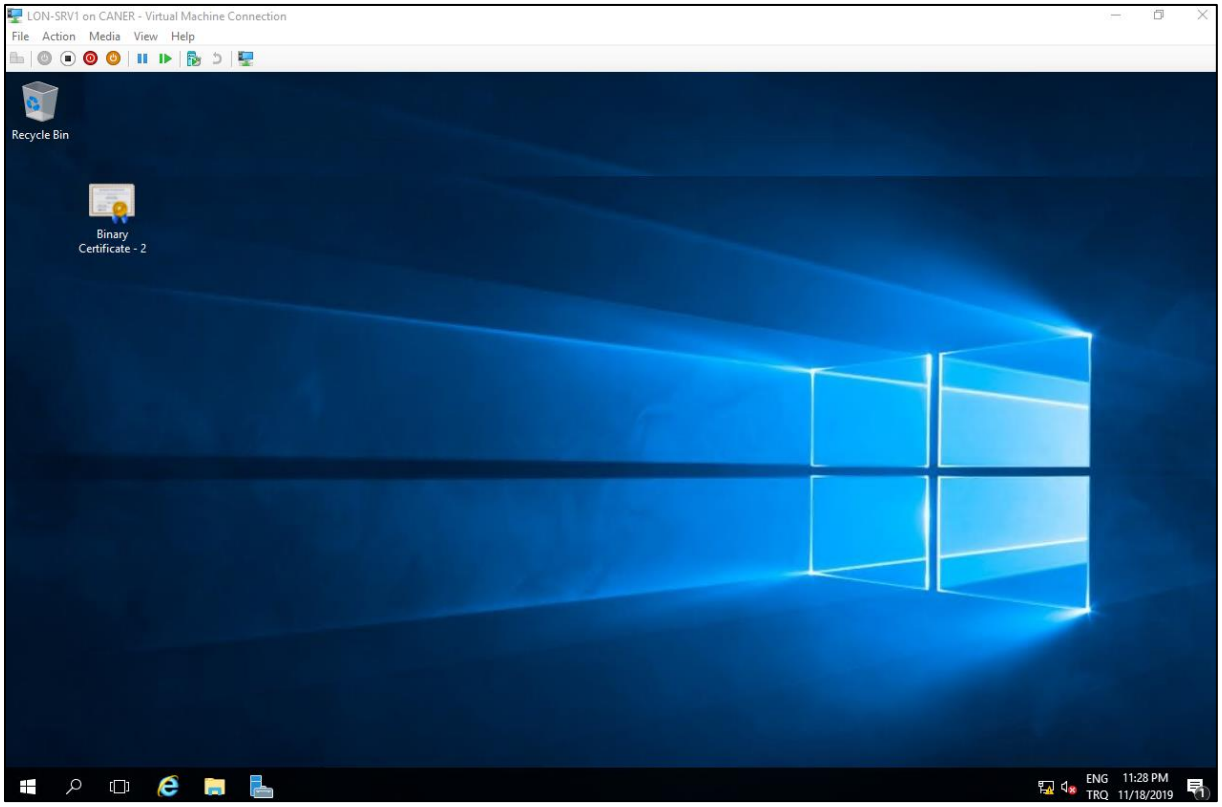
We choose “Binary Certificate” and “Save binary file to file…”



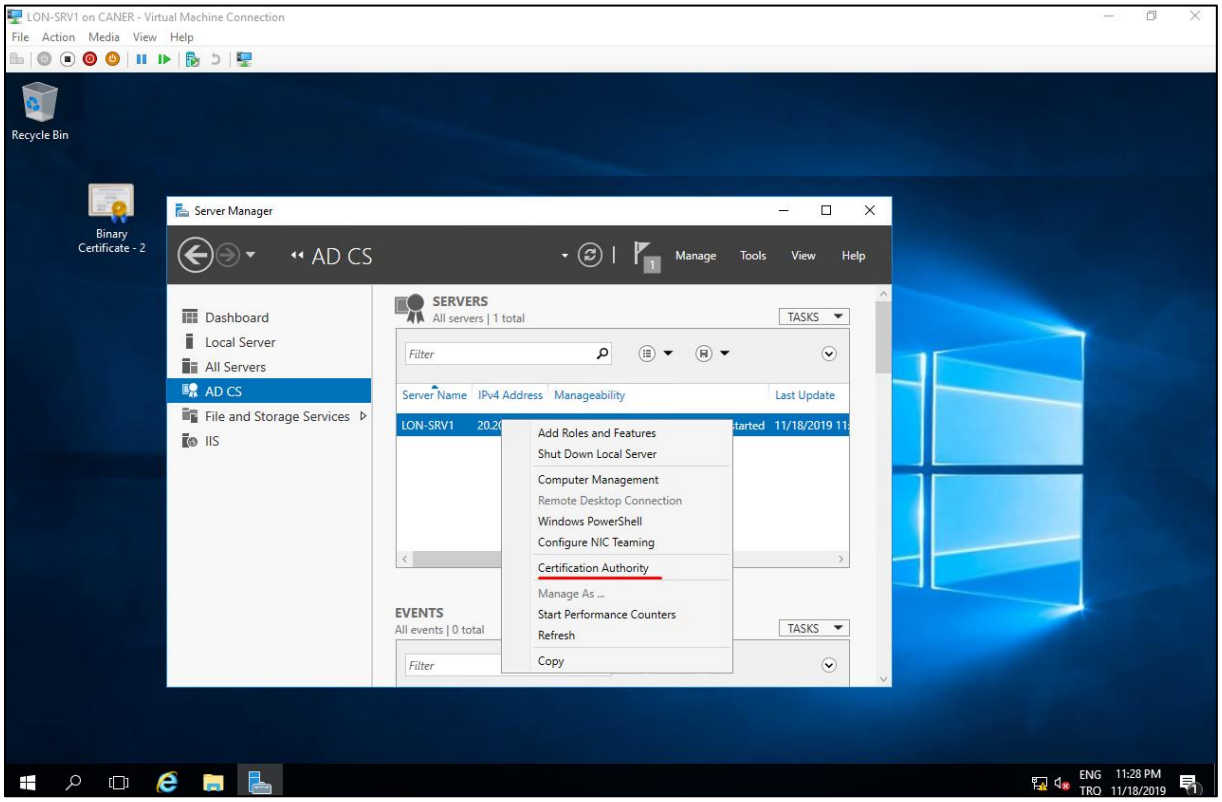
We manually add .p7b as the extension to the file and save.



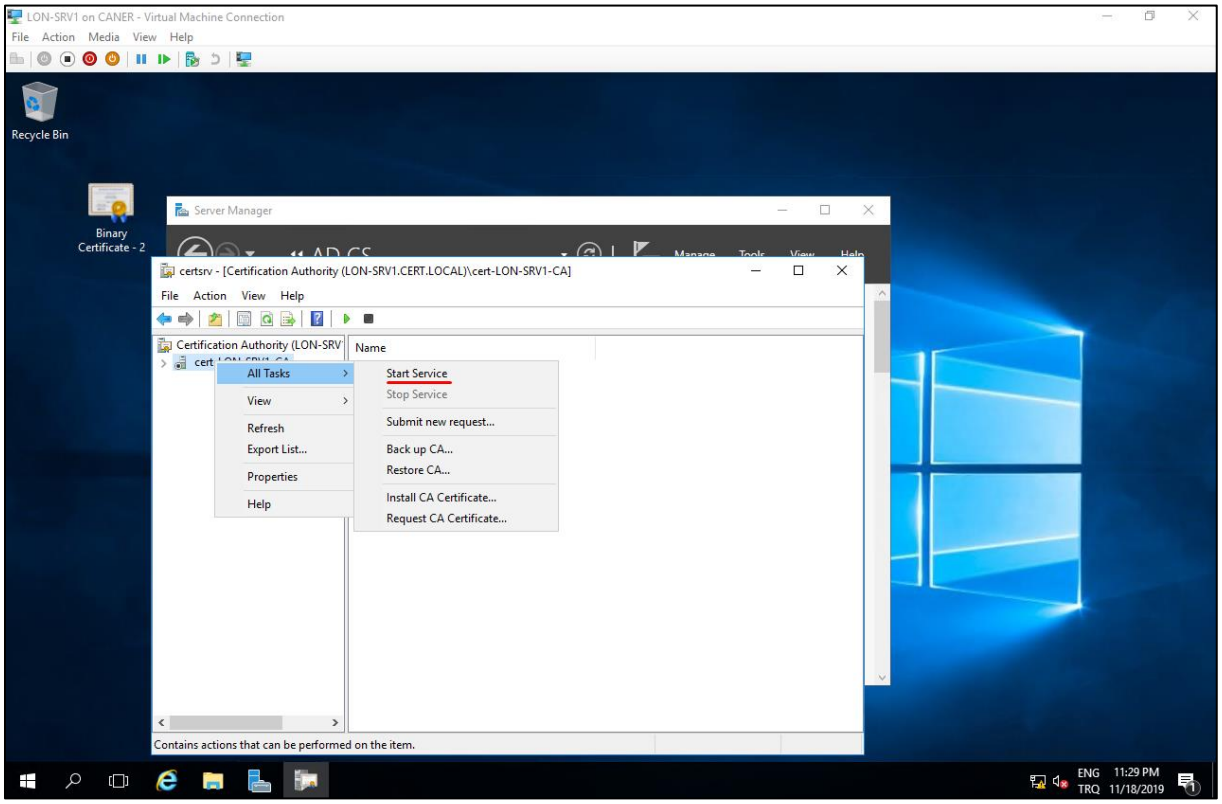
It looks just like a regular certificate but the extension is different.



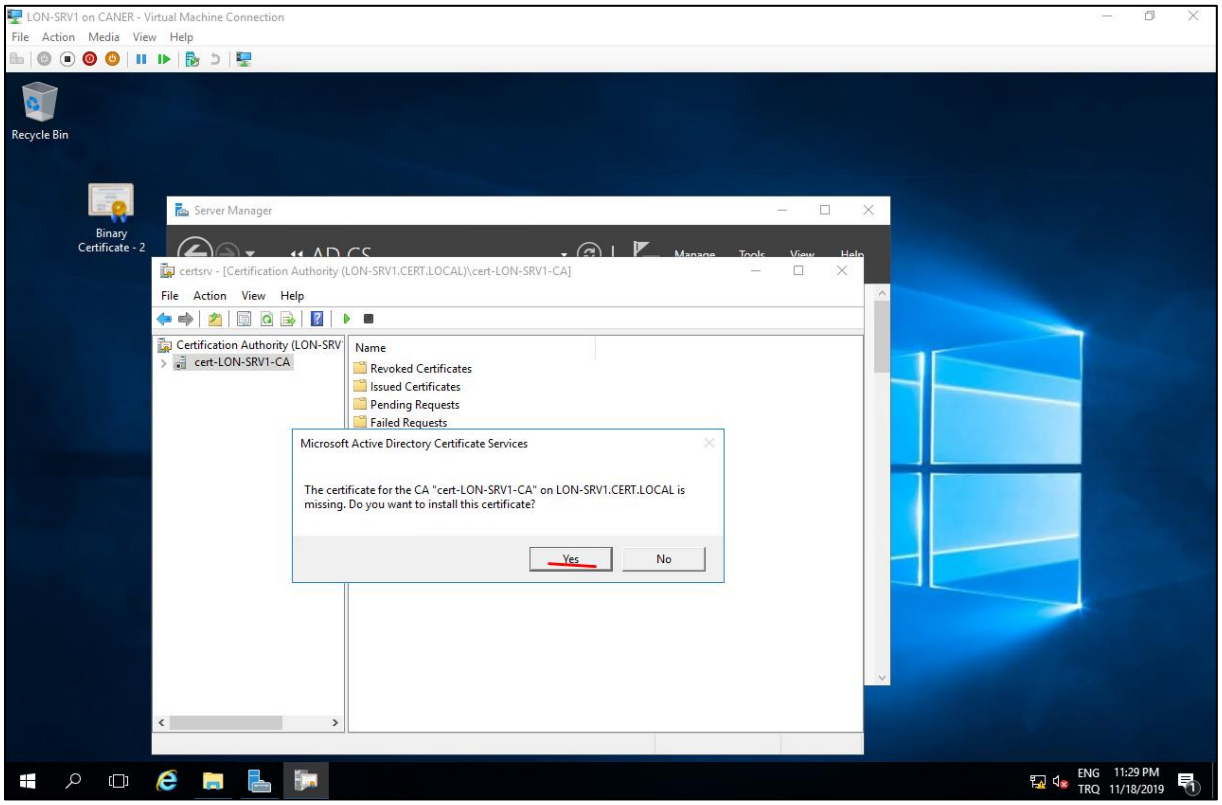
Now we copy this .p7b file to the Subordinate CA, which is LON-SRV1, manually and open up Certification Authority.



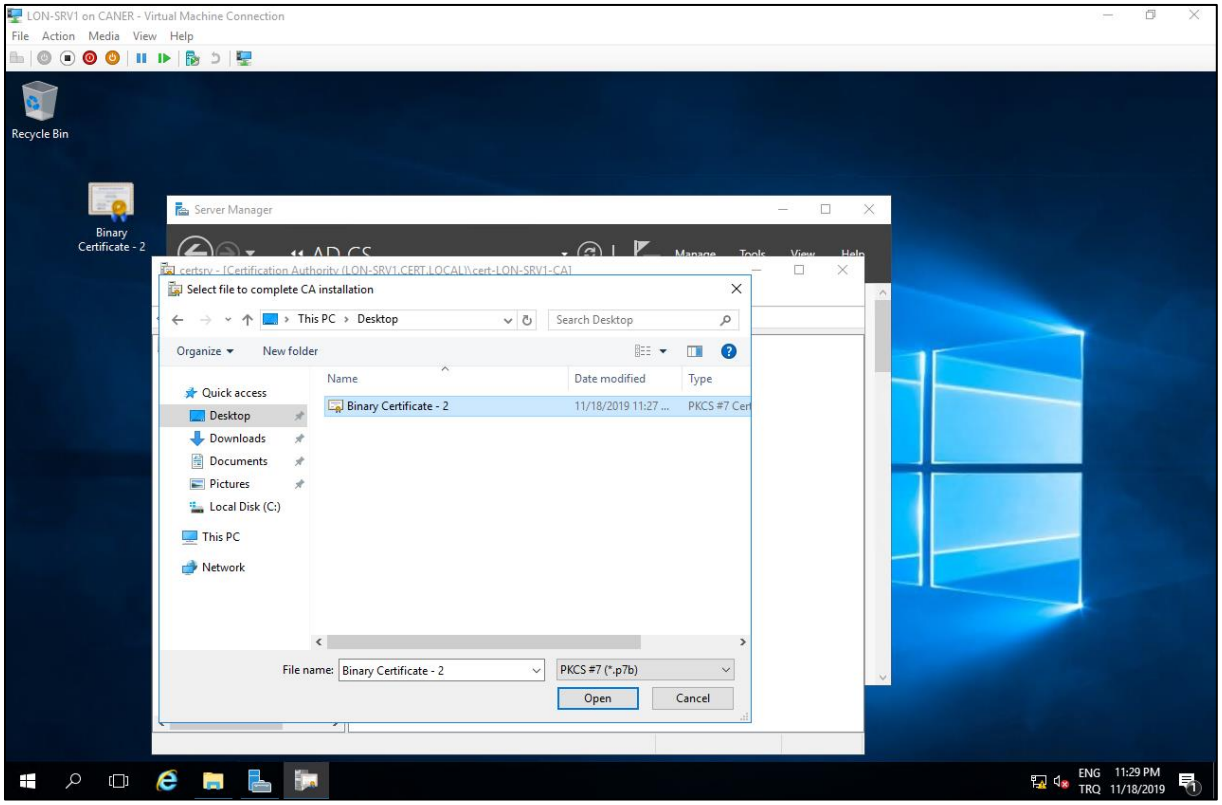
Now, we get to start distributing the certificate and we need the .p7b file to start the Certification Authority on the Subordinate CA.



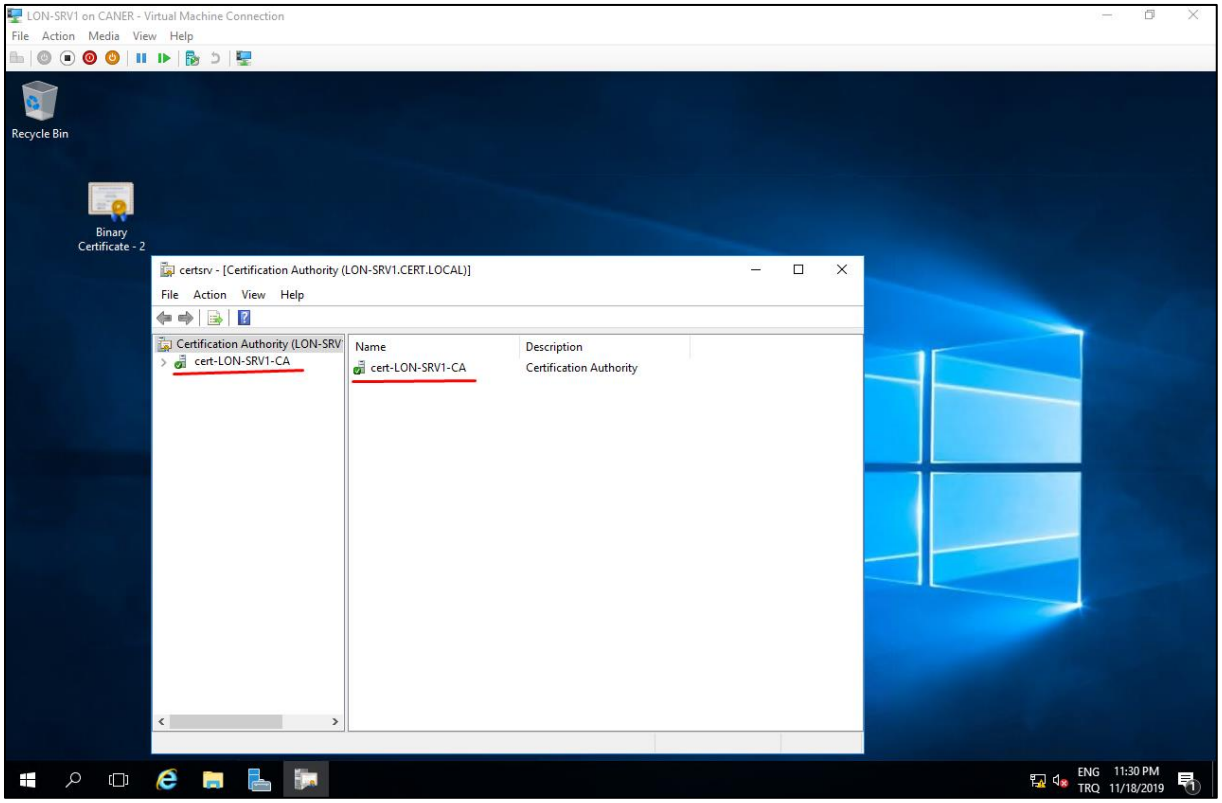
This warning is exactly as we wanted since we are getting the certificate from the Standalone Root CA and need to supply it manually. This adds a very certain layer of security to our topology since any unauthorized person needs to physically reach to our offline and disconnected Root CA, which is CA-SRV1, that we probably keep in a secure place.



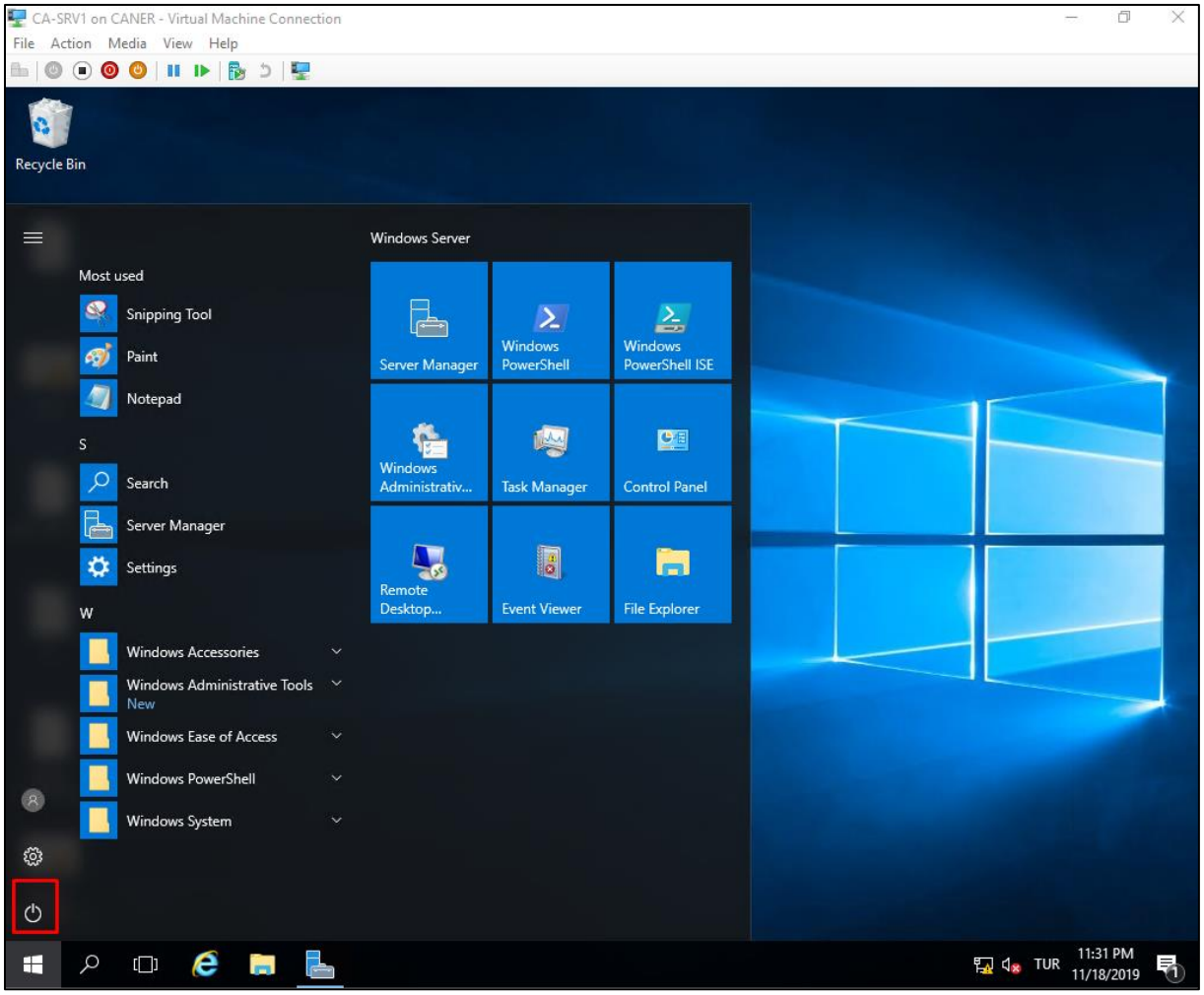
We choose the .p7b file that we created for this.



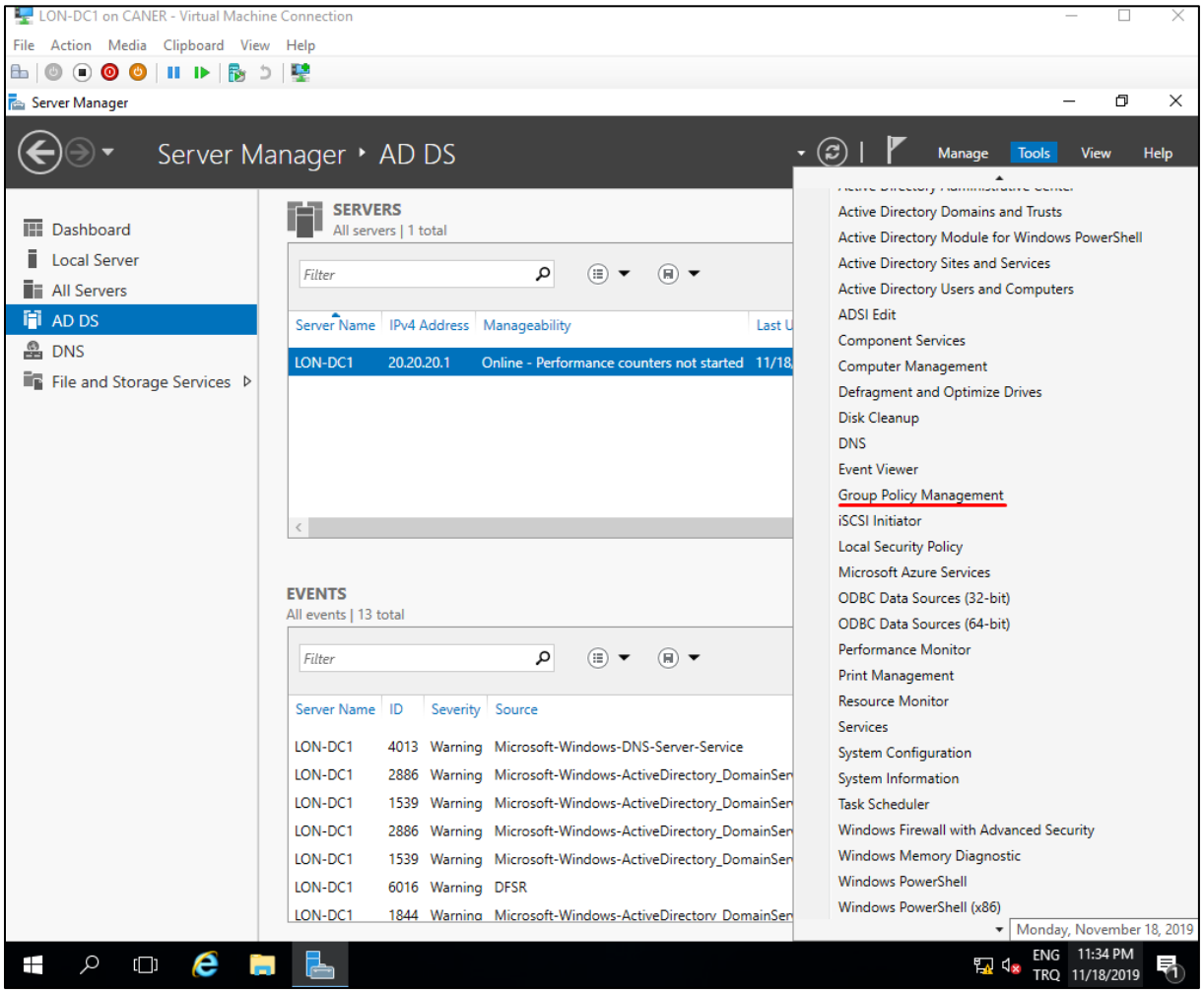
Now you can see that CA is online and can distribute the certificates.



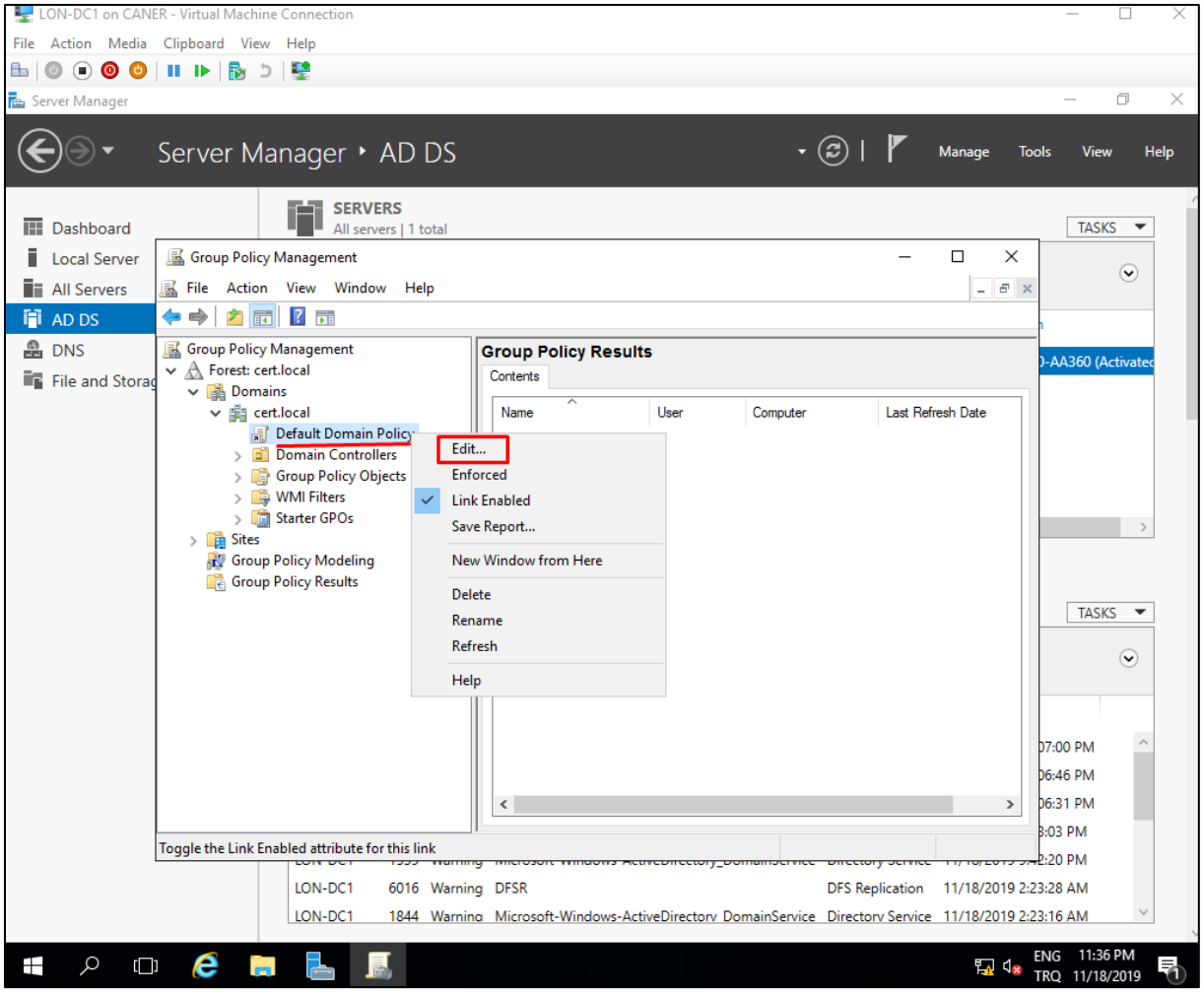
Now, we can safely turn off CA-SRV1 and keep it in a secure environment as mentioned.



To sum up, we created a certificate at the Root CA, moved it to the Subordinate to generate a .req file. Then, moved the .req file to issue a certificate and exported this generated certificate in .p7b format. Then, we moved the .p7b to Subordinate CA to start the certificate distribution and disconnected the Root CA entirely. However, we still have to do one last thing for this to work. The Subordinate CA is distributing the certificates but they are not allowed by the Active Directory and hence probably never reach their destinations. We need to go to the DC and set that the certificates from the Subordinate CA are trusted. To do this, we get to the Group Policy Management on the DC which is LON-DC1.

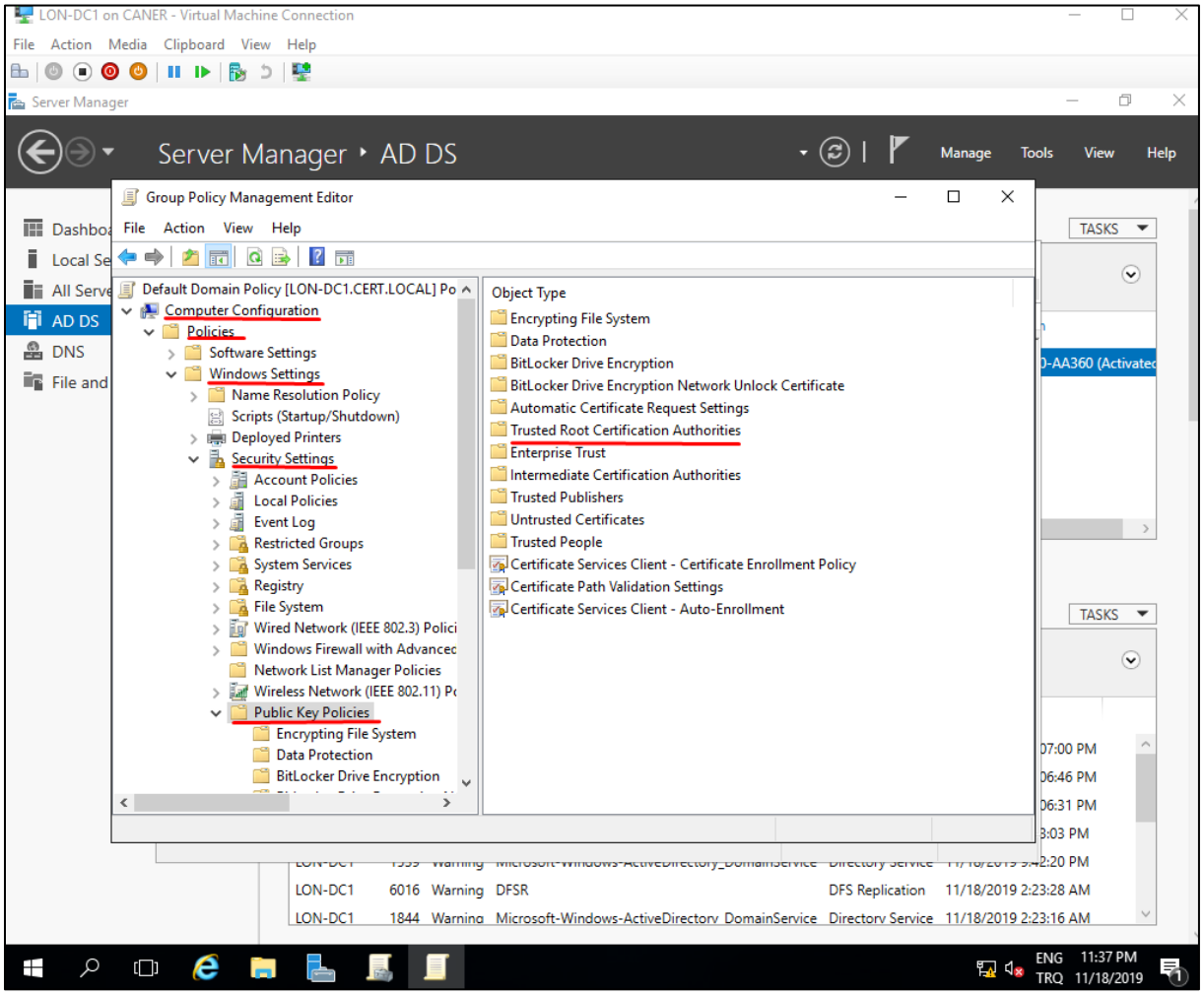


We Edit the Default Domain Policies…

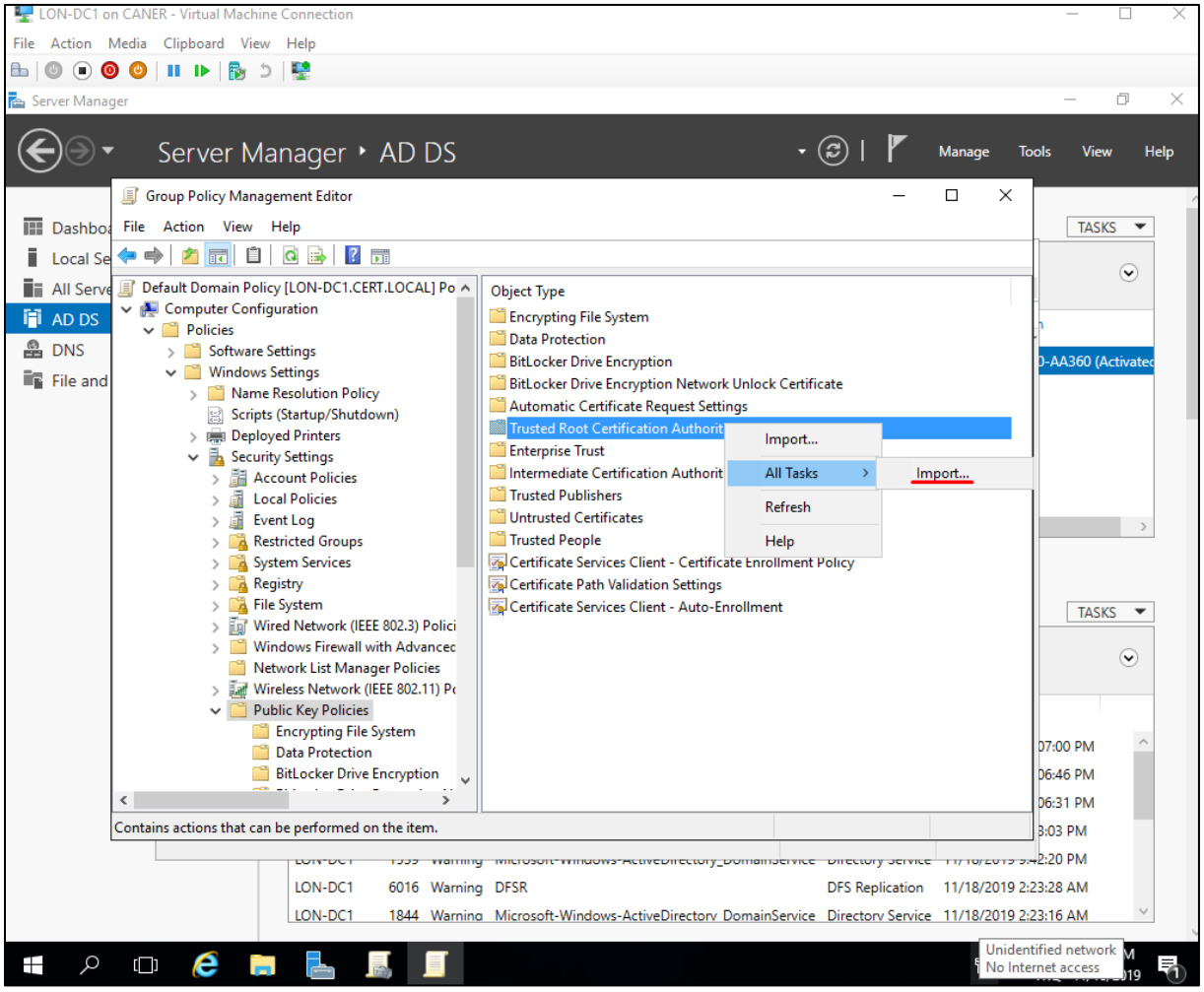


Then we follow this path:

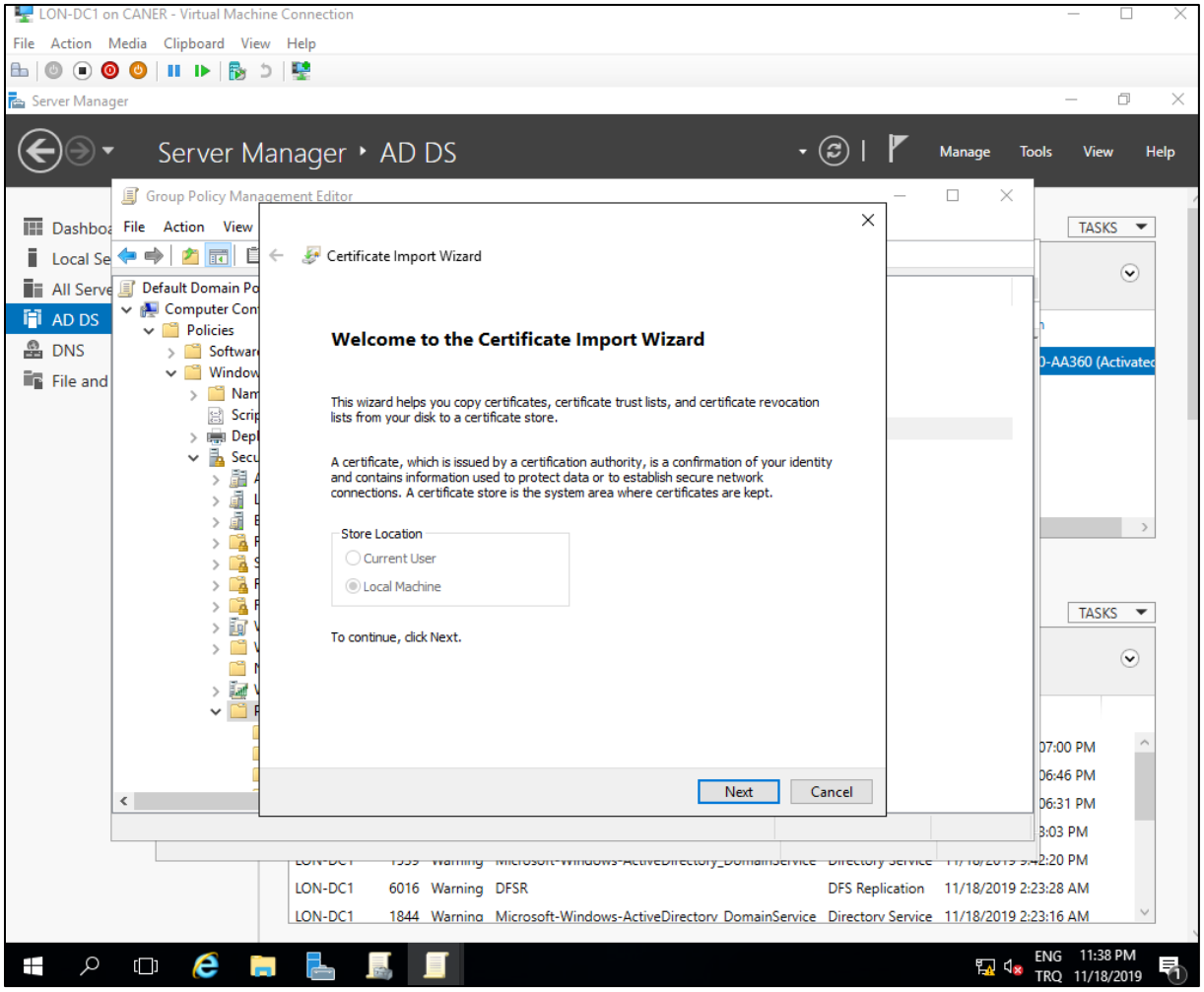
Computer Configuration → Policies → Windows Settings → Security Settings → Public Key Policies → Trusted Root Certification Authorities



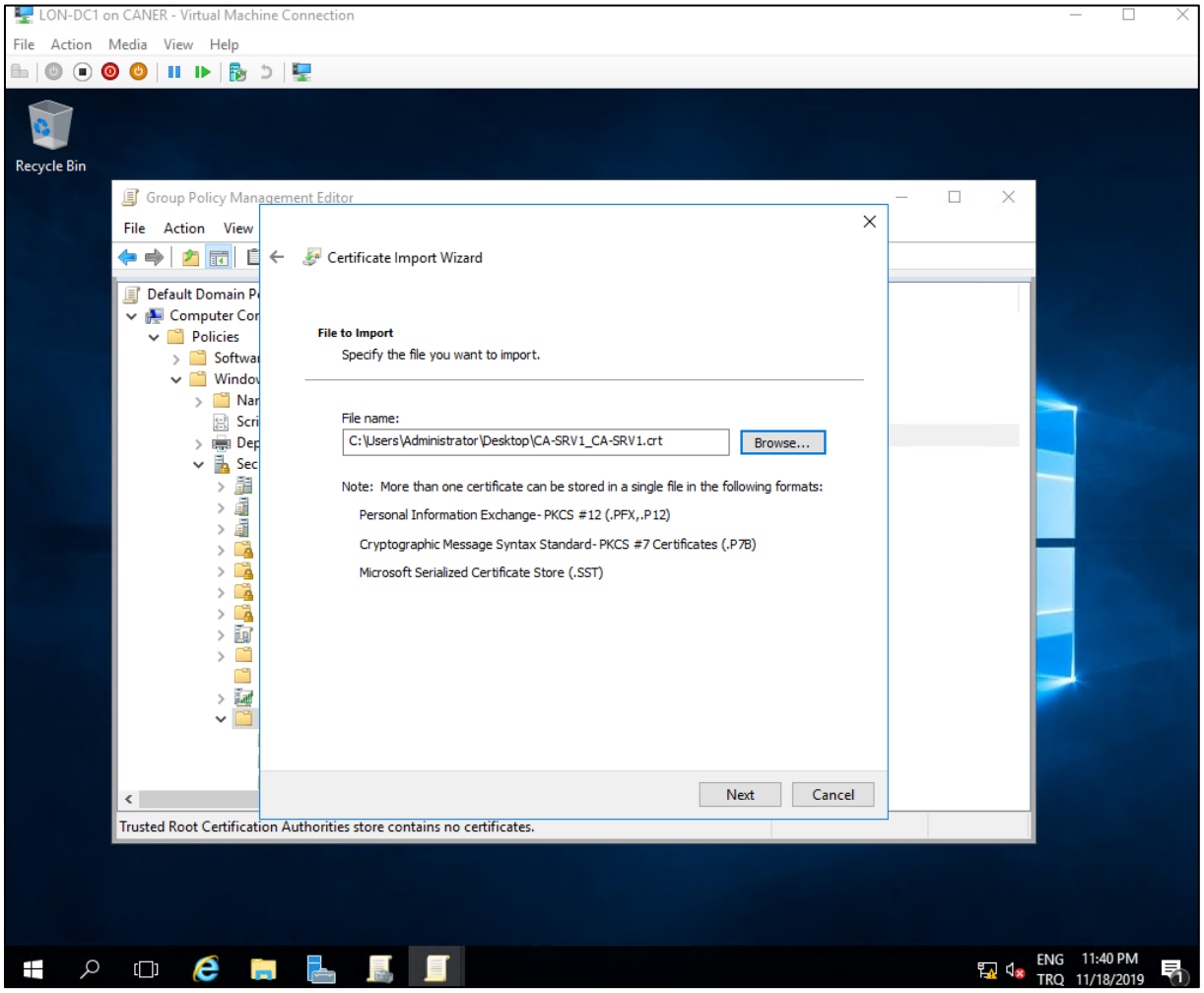
We right click on Trusted Root Certification Authorities to Import…



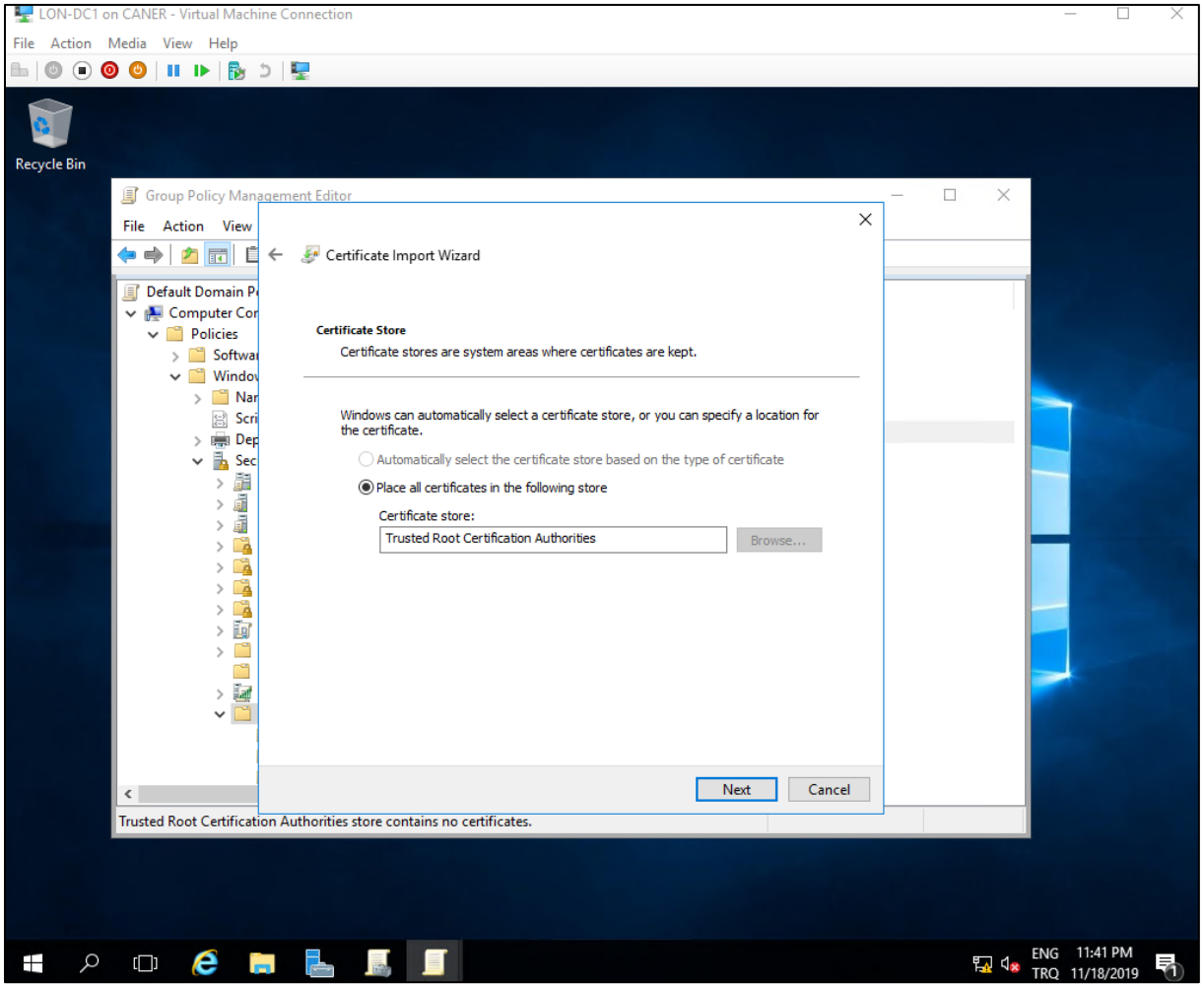
This initiates a new wizard.



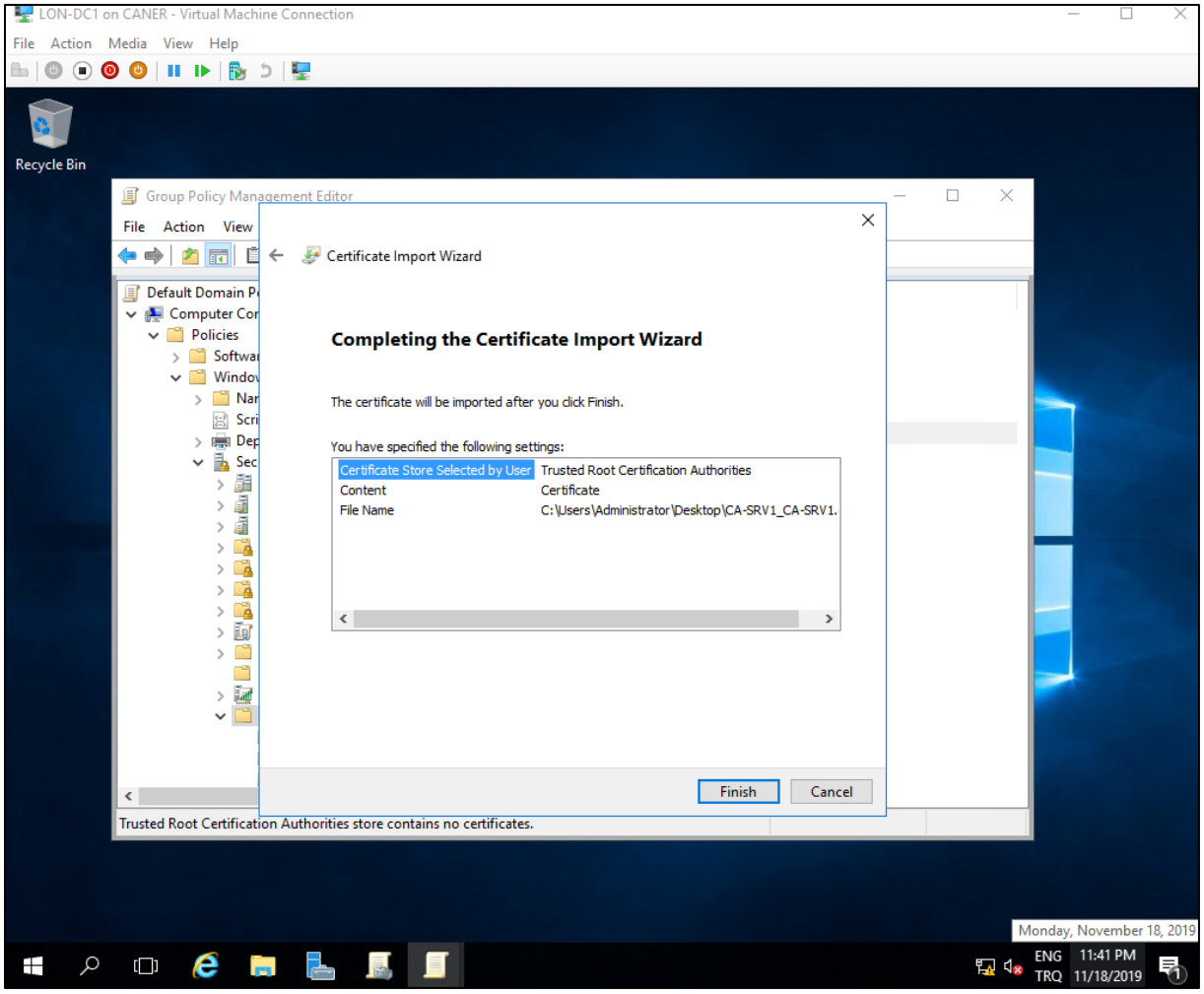
In here, we import the original certificate from the Root CA. The very first one that we generated. Note that this is a .crt file.



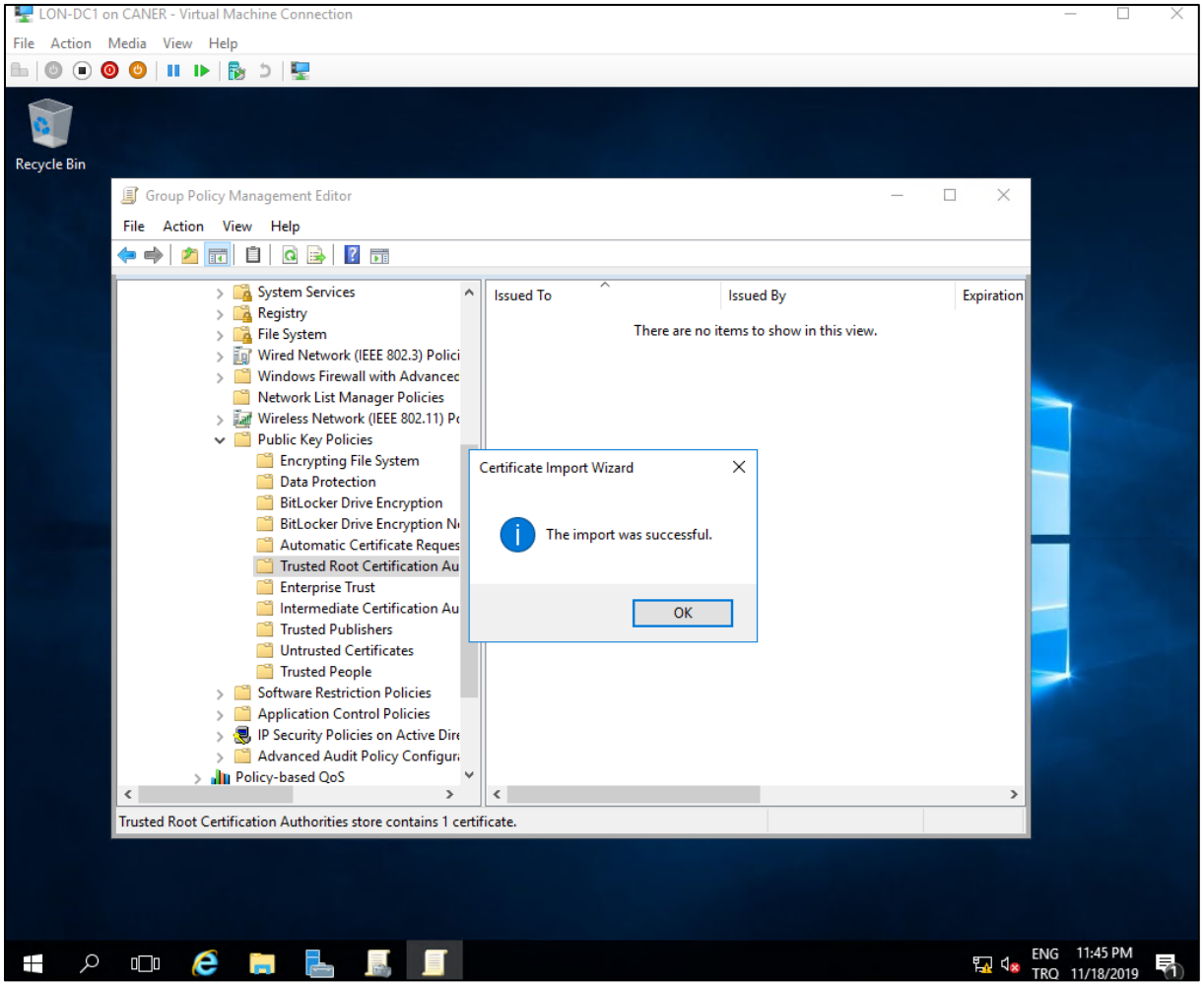
Then we place all of them to Trusted Root Certification Authorities.



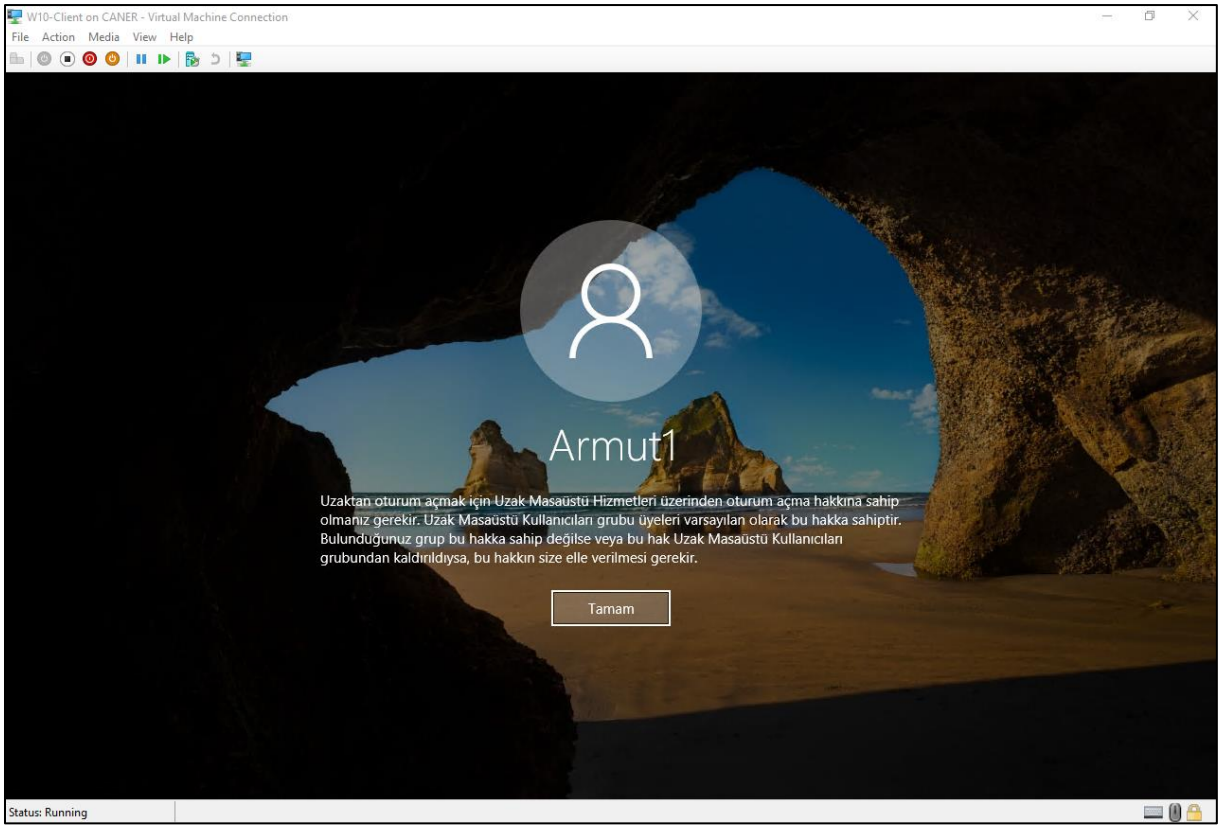
We click finish and…



… complete importing.

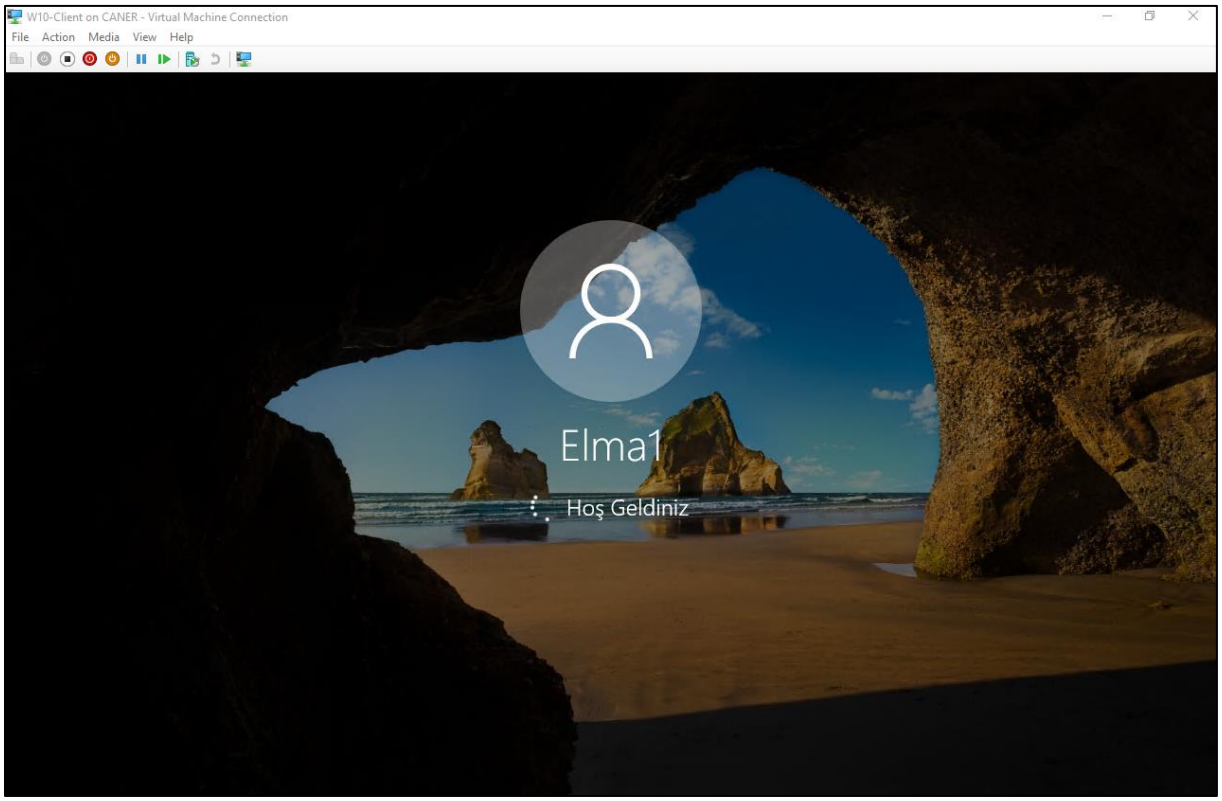


Now, we need to test whether everything we have done worked. Recall that we have removed every right regarding the certificate except for the members of a group called Elma. Only Elma members can Request or Read certificates and no other user can do anything. You can see that with our brand new Windows 10 PC, that simply joined the domain cer.local using its Administrator account, cannot login with a non-Elma account. Armut1 is not a member of Elma and cannot login since Armut1 cannot request certificate.



That error code simply proves that our certificate based security layer is working. At least, it keeps unidentified Users away from accessing the network. Now we have to see if we can still access it ourselves.

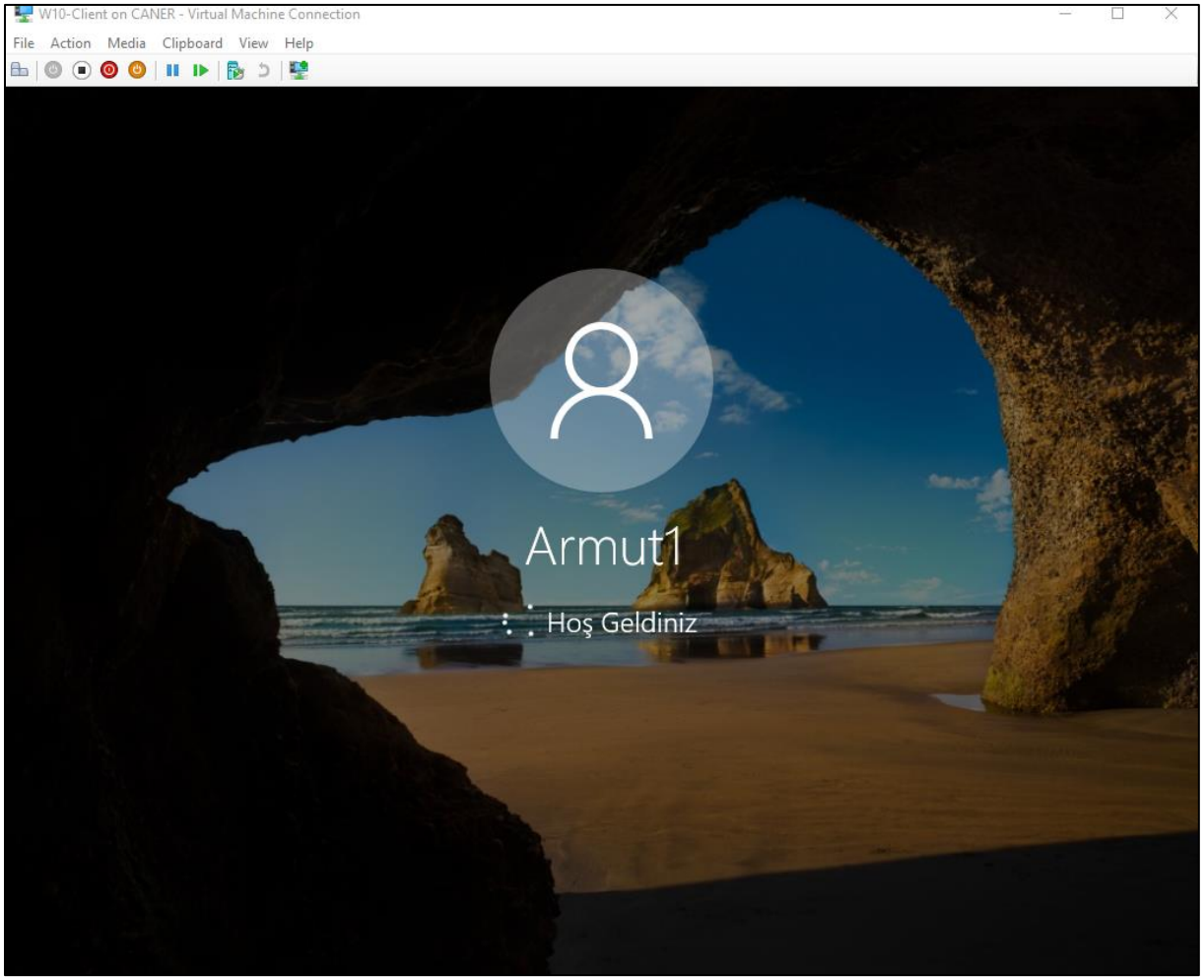
We try logging in with an Elma member Elma1.



Elma1 logs in with ease since it can request certificate permission.

Now note that certificates that we have created in this project are local computer based which means once Elma1 requested it, the certificate is now downloaded to this Windows 10 PC. ıf we change Users without rebooting the certificate could still be on the PC.

We test this by trying to immediately login with Armut1.

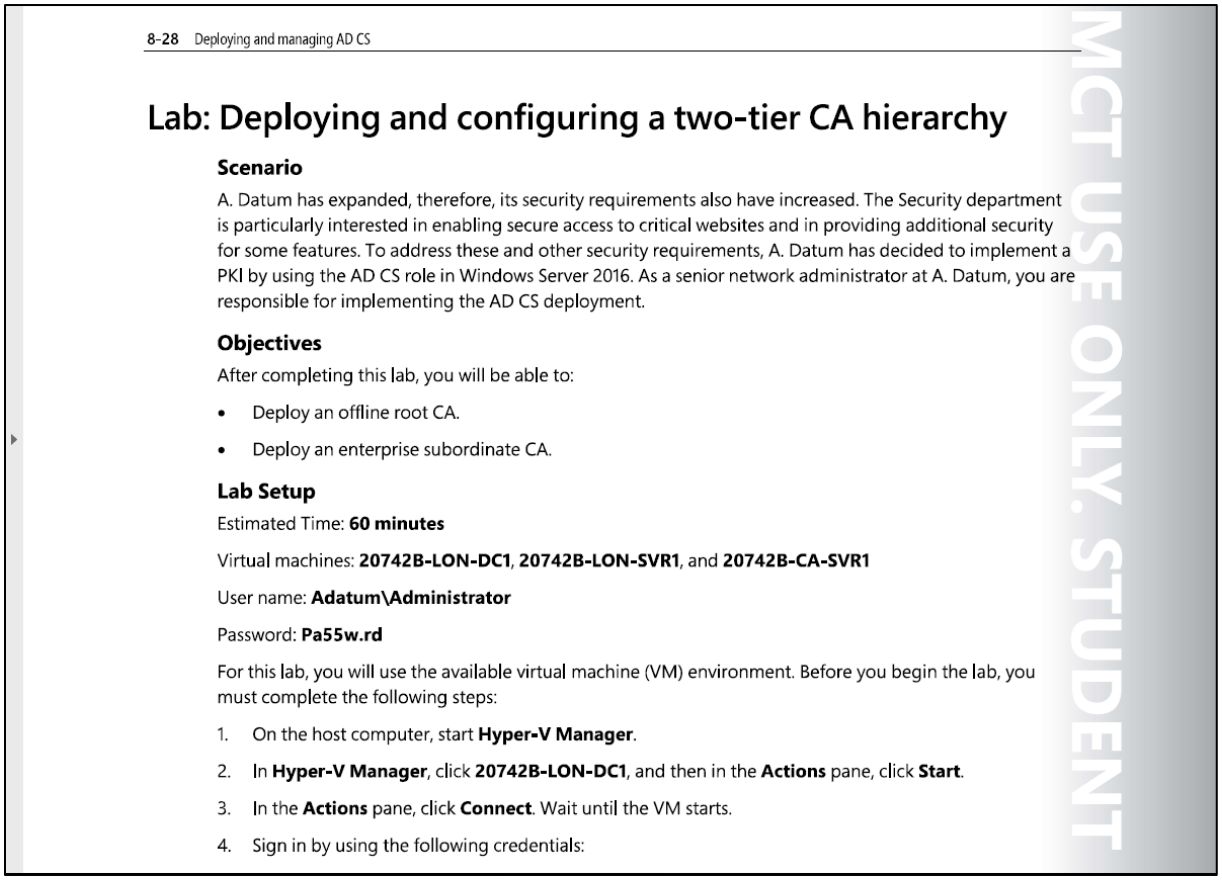


Now, it can log in and access the network. This might seem like a breach of security; however, depending on your needs this might be exactly as you wanted since you can make sure that Users must reboot each time they change Users. However, probably the easiest way to accomplish this is to simply create a certificate based on Current Users if you want to be working on an Active Directory. A simply Workgroup might manage with local computers better without Active Directory. You may choose what you do depending on your security needs. Restricting access to Users without Admin permit sounds like a clever idea in general.

3. Conclusion

In the first part of this project, we familiarized ourselves with Active Directory; there isn't much to say except that we accomplished all of our goals.

In the second part of the project, we followed a meticulous set of instruction on a PDF which I am in fact sharing here in case the files get separated:



8-28 Deploying and managing AD CS

Lab: Deploying and configuring a two-tier CA hierarchy

Scenario

A. Datum has expanded, therefore, its security requirements also have increased. The Security department is particularly interested in enabling secure access to critical websites and in providing additional security for some features. To address these and other security requirements, A. Datum has decided to implement a PKI by using the AD CS role in Windows Server 2016. As a senior network administrator at A. Datum, you are responsible for implementing the AD CS deployment.

Objectives

After completing this lab, you will be able to:

- Deploy an offline root CA.
- Deploy an enterprise subordinate CA.

Lab Setup

Estimated Time: **60 minutes**

Virtual machines: **20742B-LON-DC1**, **20742B-LON-SVR1**, and **20742B-CA-SVR1**

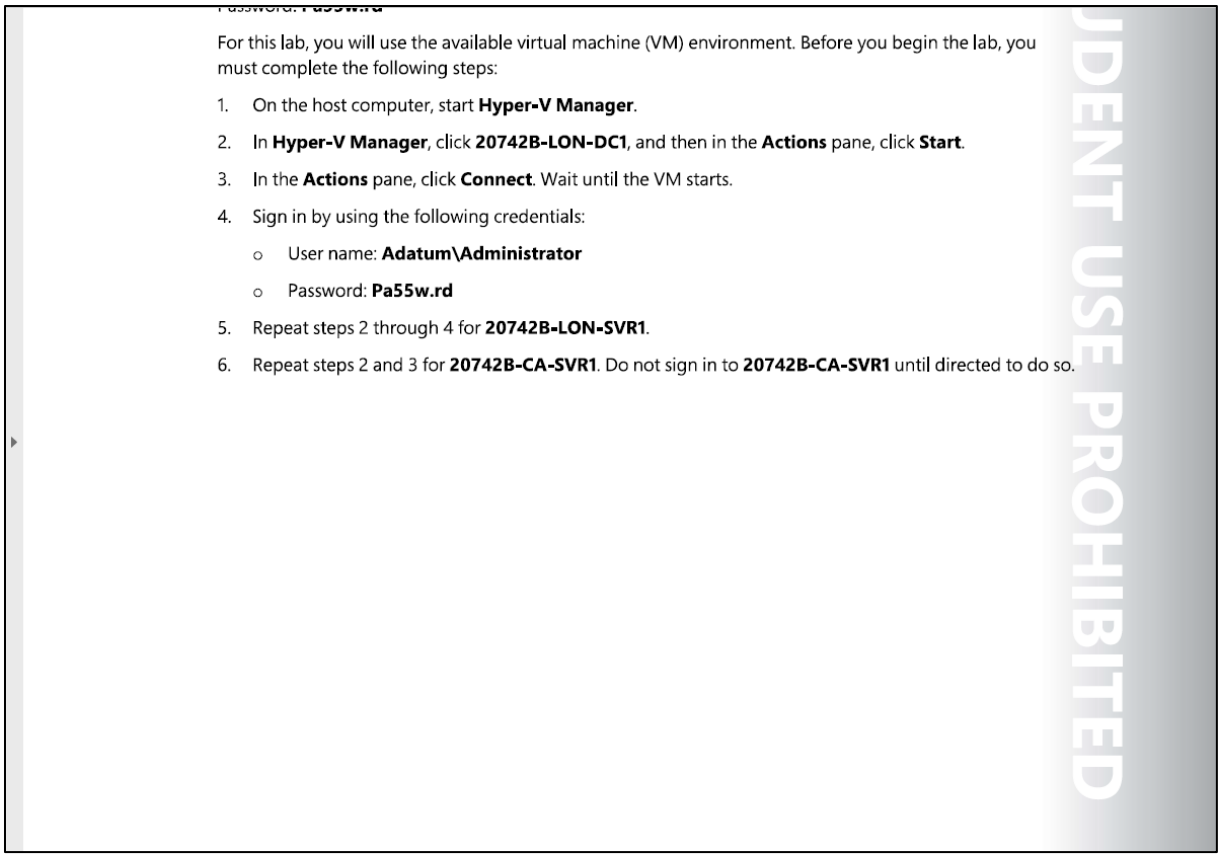
User name: **Adatum\Administrator**

Password: **Pa55w.rd**

For this lab, you will use the available virtual machine (VM) environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In **Hyper-V Manager**, click **20742B-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the VM starts.
4. Sign in by using the following credentials:

MCT USE ONLY. STUDENT



Password: **Pa55w.rd**

For this lab, you will use the available virtual machine (VM) environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In **Hyper-V Manager**, click **20742B-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the VM starts.
4. Sign in by using the following credentials:
   - User name: **Adatum\Administrator**
   - Password: **Pa55w.rd**
5. Repeat steps 2 through 4 for **20742B-LON-SVR1**.
6. Repeat steps 2 and 3 for **20742B-CA-SVR1**. Do not sign in to **20742B-CA-SVR1** until directed to do so.

UDENT USE PROHIBITED

Exercise 1: Deploying an offline root CA

Scenario

A. Datum wants to use certificates for various purposes. You need to install the appropriate CA infrastructure. Because A. Datum uses Windows Server 2016 AD DS, you decided to implement the AD CS role. When you reviewed the available designs, you decided to implement a standalone root CA. This CA will be taken offline after it issues a certificate for a subordinate CA. After installation, you must make sure that you configured the CDP and AIA locations correctly. You must also make sure that you have a Domain Name System (DNS) record for the offline root CA so that it is accessible from the network.

The main tasks for this exercise are as follows:

1. Create file and printer sharing exceptions.
2. Install and configure Active Directory Certificate Services (AD CS) on CA-SVR1.
3. Create a Domain Name System (DNS) record for an offline root CA.

▶ Task 1: Create file and printer sharing exceptions

1. Sign in to **CA-SVR1** as **Administrator** with the password **Pa55w.rd**.
2. On **CA-SVR1**, in the Network and Sharing Center, turn on file and printer sharing on guest and public networks.
3. On **LON-SVR1**, in the Network and Sharing Center, turn on file and printer sharing on the domain network.

▶ Task 2: Install and configure Active Directory Certificate Services (AD CS) on CA-SVR1

1. Switch to **CA-SVR1**, and then start **Server Manager**.
2. Use the **Add Roles and Features Wizard** to install the Active Directory Certificate Services role.
3. After installation completes successfully, click the **Configure Active Directory Certificate Services on the destination server** text.
4. Configure the AD CS role as a standalone root CA with the name **AdatumRootCA**.
5. Set the key length to **4096**, and then accept all other default values.

CT USE ONLY. STUDENT US

▶ Task 2: Install and configure Active Directory Certificate Services (AD CS) on CA-SVR1

1. Switch to **CA-SVR1**, and then start **Server Manager**.
2. Use the **Add Roles and Features Wizard** to install the Active Directory Certificate Services role.
3. After installation completes successfully, click the **Configure Active Directory Certificate Services on the destination server** text.
4. Configure the AD CS role as a standalone root CA with the name **AdatumRootCA**.
5. Set the key length to **4096**, and then accept all other default values.
6. On **CA-SVR1**, open the **Certification Authority** console.
7. Open the **Properties** dialog box for **AdatumRootCA**.
8. Configure the new locations for the CDP to be **http://lon-svr1.adatum.com/CertData/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl**.
9. Select the following options:
   - **Include in the CDP extension of issued certificates**
   - **Include in CRLs. Clients use this to find Delta CRL locations**
10. Configure new locations for AIA to be on **http://lon-svr1.adatum.com/CertData/<ServerDNSName>_<CaName><CertificateName>.crt**.
11. Select the **Include in the AIA extension of issued certificates** check box.
12. Publish the CRL on **CA-SVR1**.
13. Export the root CA certificate, and then copy the **.cer** file to **\\lon-svr1\C$**.
14. Copy the contents of folder **C:\Windows\System32\CertSrv\CertEnroll** to **\\lon-svr1\C$**.

DENT USE PROHIBITED

▶ Task 3: Create a Domain Name System (DNS) record for an offline root CA

1. On **LON-DC1**, in **Server Manager**, open the **DNS Manager** console.
2. Create a host resource record for **CA-SVR1** in the Adatum.com forward lookup zone.
3. Use IP address **172.16.0.40** for the **CA-SVR1** host resource record.

Results: After completing this exercise, you should have successfully installed and configured the standalone root certification authority (CA) role on the **CA-SVR1** server. Additionally, you should have created an appropriate DNS record in Active Directory Domain Services (AD DS) so that other servers can connect to **CA-SVR1**.

Exercise 2: Deploying an enterprise subordinate CA

Scenario

After deploying the standalone root CA, the next step is to deploy an enterprise subordinate CA. A. Datum wants to use an enterprise subordinate CA to utilize AD DS integration. Additionally, because the root CA is a standalone CA, you want to publish its certificate to all clients.

The main tasks for this exercise are as follows:

1. Install and configure AD CS on LON-SVR1.
2. Install a subordinate CA certificate.
3. Publish a root CA certificate through Group Policy.
4. Prepare for the next module.

▶ Task 1: Install and configure AD CS on LON-SVR1

1. On **LON-SVR1**, in **Server Manager**, install the Active Directory Certificate Services role. Include the Certification Authority and Certification Authority Web Enrollment role services.

MCT USE ONLY. STUDENT USE PROHIBITED

▶ Task 1: Install and configure AD CS on LON-SVR1

1. On **LON-SVR1**, in **Server Manager**, install the Active Directory Certificate Services role. Include the Certification Authority and Certification Authority Web Enrollment role services.
2. After installation is successful, click the **Configure Active Directory Certificate Services on the destination server** text.
3. Select the **Certification Authority** and **Certification Authority Web Enrollment** role services.
4. Configure **LON-SVR1** to be an **Enterprise CA**.
5. Configure the **CA Type** to be a **Subordinate CA**.
6. For the **CA Name**, type **Adatum-IssuingCA**.
7. Save the request file to the local drive.

▶ Task 2: Install a subordinate CA certificate

1. On **LON-SVR1**, install the **C:\RootCA.cer** certificate to the Trusted Root Certification Authority store.
2. Go to **Local Disk (C:)**, and then copy the **AdatumRootCA.crl** and **CA-SVR1_AdatumRootCA.crt** files to **C:\inetpub\wwwroot\CertData**.
3. Copy the **LON-SVR1.Adatum.com_Adatum-LON-SVR1-CA.req** request file to **\\CA-SVR1\C$**.
4. Switch to **CA-SVR1**.
5. From the **Certification Authority** console on **CA-SVR1**, submit a new certificate request by using the **.req** file that you copied in step 3.

MCT USE ONLY. STUDENT USE PROHIBITED

6. Issue the certificate, and then export it to .p7b format with a complete chain. Save the file to **\\lon-svr1\C$\SubCA.p7b**.
7. Switch to **LON-SVR1**.
8. Install the subordinate CA certificate on **LON-SVR1** by using the **Certification Authority** console.
9. Start the service. Ensure that the AD CS service successfully starts.
10. Switch to **CA-SVR1**, and then shut down the server.

▶ Task 3: Publish a root CA certificate through Group Policy

1. On **LON-DC1**, in **Server Manager**, open the **Group Policy Management Console**.
2. Edit the **Default Domain Policy**.
3. Publish the **RootCA.cer** file from **\\lon-svr1\C$** to the Trusted Root Certification Authorities store, which is located in **Computer Configuration\Policies\Windows Settings\Security Settings \Public Key Policies**.

Results: After completing this exercise, you should have successfully deployed and configured an enterprise subordinate CA. You also should have a subordinate CA certificate issued by a root CA installed on **LON-SVR1**. To establish trust between the root CA and domain member clients, you will use Group Policy to deploy a root CA certificate.

▶ Task 4: Prepare for the next module

After you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742B-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742B-LON-SVR1** and **20742B-CA-SVR1**.

MCT USE ONLY. STUDENT US

Lab: Deploying and configuring a two-tier CA hierarchy

Scenario

A. Datum has expanded, therefore, its security requirements also have increased. The Security department is particularly interested in enabling secure access to critical websites and in providing additional security for some features. To address these and other security requirements, A. Datum has decided to implement a PKI by using the AD CS role in Windows Server 2016. As a senior network administrator at A. Datum, you are responsible for implementing the AD CS deployment.

Objectives

After completing this lab, you will be able to:

- Deploy an offline root CA.
- Deploy an enterprise subordinate CA.

Lab Setup

Estimated Time: **60 minutes**

Virtual machines: **20742B-LON-DC1**, **20742B-LON-SVR1**, and **20742B-CA-SVR1**

User name: **Adatum\Administrator**

Password: **Pa55w.rd**

For this lab, you will use the available virtual machine (VM) environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In **Hyper-V Manager**, click **20742B-LON-DC1**, and then in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the VM starts.
4. Sign in by using the following credentials:
   - User name: **Adatum\Administrator**
   - Password: **Pa55w.rd**
5. Repeat steps 2 through 4 for **20742B-LON-SVR1**.
6. Repeat steps 2 and 3 for **20742B-CA-SVR1**. Do not sign in to **20742B-CA-SVR1** until directed to do so.

MCT USE ONLY. STUDENT USE P

A. Datum wants to use certificates for various purposes. You need to install the appropriate CA infrastructure. Because A. Datum uses Windows Server 2016 AD DS, you decided to implement the AD CS role. When you reviewed the available designs, you decided to implement a standalone root CA. This CA will be taken offline after it issues a certificate for a subordinate CA. After installation, you must make sure that you configured the CDP and AIA locations correctly. You must also make sure that you have a Domain Name System (DNS) record for the offline root CA so that it is accessible from the network.

The main tasks for this exercise are as follows:

1. Create file and printer sharing exceptions.
2. Install and configure Active Directory Certificate Services (AD CS) on CA-SVR1.
3. Create a Domain Name System (DNS) record for an offline root CA.

▶ Task 1: Create file and printer sharing exceptions

1. Sign in to **CA-SVR1** as **Administrator** with the password **Pa55w.rd**.
2. On **CA-SVR1**, in the Network and Sharing Center, turn on file and printer sharing on guest and public networks.
3. On **LON-SVR1**, in the Network and Sharing Center, turn on file and printer sharing on the domain network.

▶ Task 2: Install and configure Active Directory Certificate Services (AD CS) on CA-SVR1

1. Switch to **CA-SVR1**, and then start **Server Manager**.
2. Use the **Add Roles and Features Wizard** to install the Active Directory Certificate Services role.
3. After installation completes successfully, click the **Configure Active Directory Certificate Services on the destination server** text.
4. Configure the AD CS role as a standalone root CA with the name **AdatumRootCA**.
5. Set the key length to **4096**, and then accept all other default values.
6. On **CA-SVR1**, open the **Certification Authority** console.
7. Open the **Properties** dialog box for **AdatumRootCA**.
8. Configure the new locations for the CDP to be **http://lon-svr1.adatum.com/CertData/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl**.
9. Select the following options:
   - **Include in the CDP extension of issued certificates**
   - **Include in CRLs. Clients use this to find Delta CRL locations**
10. Configure new locations for AIA to be on **http://lon-svr1.adatum.com/CertData/<ServerDNSName>_<CaName><CertificateName>.crt**.
11. Select the **Include in the AIA extension of issued certificates** check box.
12. Publish the CRL on **CA-SVR1**.
13. Export the root CA certificate, and then copy the **.cer** file to **\\lon-svr1\C$**.
14. Copy the contents of folder **C:\Windows\System32\CertSrv\CertEnroll** to **\\lon-svr1\C$**.

USE ONLY. STUDENT USE PROHIBITED

▶ Task 3: Create a Domain Name System (DNS) record for an offline root CA

1. On **LON-DC1**, in **Server Manager**, open the **DNS Manager** console.
2. Create a host resource record for **CA-SVR1** in the Adatum.com forward lookup zone.
3. Use IP address **172.16.0.40** for the **CA-SVR1** host resource record.

Results: After completing this exercise, you should have successfully installed and configured the standalone root certification authority (CA) role on the **CA-SVR1** server. Additionally, you should have created an appropriate DNS record in Active Directory Domain Services (AD DS) so that other servers can connect to **CA-SVR1**.

Exercise 2: Deploying an enterprise subordinate CA

Scenario

After deploying the standalone root CA, the next step is to deploy an enterprise subordinate CA. A. Datum wants to use an enterprise subordinate CA to utilize AD DS integration. Additionally, because the root CA is a standalone CA, you want to publish its certificate to all clients.

The main tasks for this exercise are as follows:

1. Install and configure AD CS on LON-SVR1.
2. Install a subordinate CA certificate.
3. Publish a root CA certificate through Group Policy.
4. Prepare for the next module.

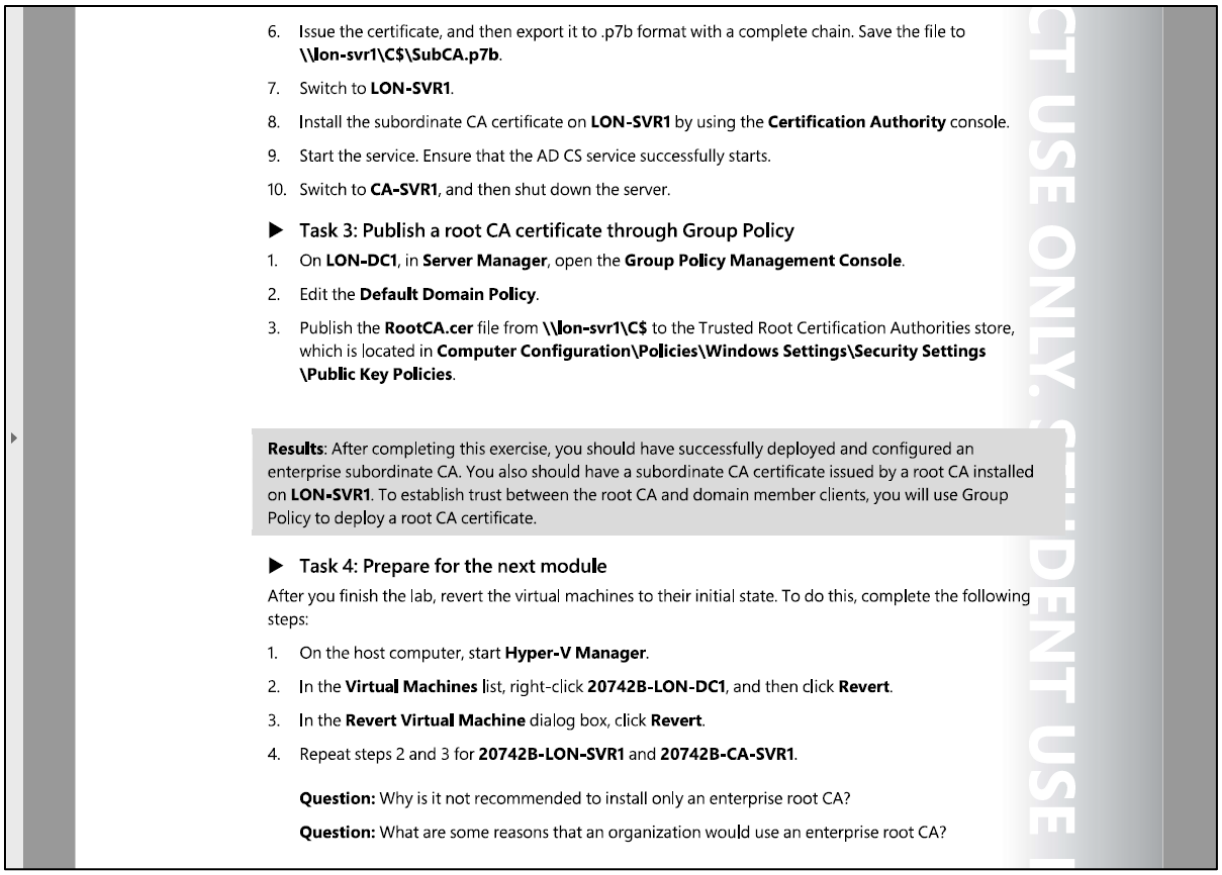
▶ Task 1: Install and configure AD CS on LON-SVR1

1. On **LON-SVR1**, in **Server Manager**, install the Active Directory Certificate Services role. Include the Certification Authority and Certification Authority Web Enrollment role services.
2. After installation is successful, click the **Configure Active Directory Certificate Services on the destination server** text.
3. Select the **Certification Authority** and **Certification Authority Web Enrollment** role services.
4. Configure **LON-SVR1** to be an **Enterprise CA**.
5. Configure the **CA Type** to be a **Subordinate CA**.
6. For the **CA Name**, type **Adatum-IssuingCA**.
7. Save the request file to the local drive.

▶ Task 2: Install a subordinate CA certificate

1. On **LON-SVR1**, install the **C:\RootCA.cer** certificate to the Trusted Root Certification Authority store.
2. Go to **Local Disk (C:)**, and then copy the **AdatumRootCA.crl** and **CA-SVR1_AdatumRootCA.crt** files to **C:\inetpub\wwwroot\CertData**.
3. Copy the **LON-SVR1.Adatum.com_Adatum-LON-SVR1-CA.req** request file to **\\CA-SVR1\C$**.
4. Switch to **CA-SVR1**.
5. From the **Certification Authority** console on **CA-SVR1**, submit a new certificate request by using the **.req** file that you copied in step 3.

T USE ONLY. STUDENT USE PROHIBITED



6. Issue the certificate, and then export it to .p7b format with a complete chain. Save the file to **\\lon-svr1\C$\SubCA.p7b**.
7. Switch to **LON-SVR1**.
8. Install the subordinate CA certificate on **LON-SVR1** by using the **Certification Authority** console.
9. Start the service. Ensure that the AD CS service successfully starts.
10. Switch to **CA-SVR1**, and then shut down the server.

▶ Task 3: Publish a root CA certificate through Group Policy

1. On **LON-DC1**, in **Server Manager**, open the **Group Policy Management Console**.
2. Edit the **Default Domain Policy**.
3. Publish the **RootCA.cer** file from **\\lon-svr1\C$** to the Trusted Root Certification Authorities store, which is located in **Computer Configuration\Policies\Windows Settings\Security Settings \Public Key Policies**.

Results: After completing this exercise, you should have successfully deployed and configured an enterprise subordinate CA. You also should have a subordinate CA certificate issued by a root CA installed on **LON-SVR1**. To establish trust between the root CA and domain member clients, you will use Group Policy to deploy a root CA certificate.

▶ Task 4: Prepare for the next module

After you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20742B-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20742B-LON-SVR1** and **20742B-CA-SVR1**.

Question: Why is it not recommended to install only an enterprise root CA?

Question: What are some reasons that an organization would use an enterprise root CA?

If you follow these instructions to the letter, it will work. Note on the changes of paths depending on computer names. Certificate parts of this project are a bit disaster prone since any mistake at an earlier step is hard to notice and may cause ultimate failure without a chance to fix it and it might require an AD reboot which is problematic to say the least. Make sure to set your security settings of the certificate before it is published to every part of the domain with Everyone allowed to download it. Otherwise, the certificate would be useless.

4. Evaluation

Honestly, this project worked quite well on the potential human error angle. We even tested with new members Elma2 and Armut2 on a brand new Windows 10 PC and got the very same results. There’s nothing further to report.