



CONESTOGA

Connect Life and Learning

Student Name:	Aagam Sanjay Shah
Deliverable:	Practical Assignment 1
Course Name:	NTWK8201-24S-Sec2-Advanced Windows Desktop

Date Assigned:	13/09/2024
Date Due:	27/09/2024
Rules:	<ul style="list-style-type: none">• Individual.• Cheating is not allowed.• Plagiarism counts as cheating!• That FAILURE to submit work in the course can result in a grade of 'F' or 'I' for failure to complete the course!

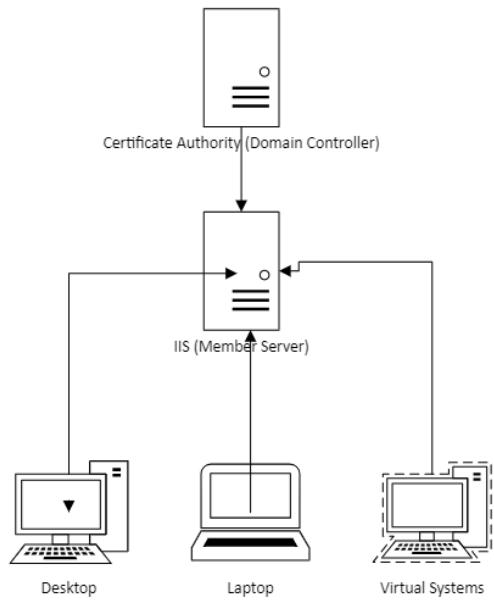
Table of Contents

Diagram.....	3
Install your first Windows Server with hostname lastname-DC1	4
Promote your first Windows Server to a domain controller with domain name lastname.local	4
Install your second Windows Server with hostname lastname-IIS and join it to lastname.local	6
Install your Windows client with hostname Lastname-C1 and join it to lastname.local	7
Create an OU structure and one security group per department with test users following best practices for the below departments.....	8
Install Active Directory Certificate Services and configure your lastname-DC1 as a Certificate Authority	10
Install IIS on your member server.....	18
Edit the default website to use HTTPS with a signed certificate from your Certificate Authority.....	19
Opening <code>http://shah.local/certsrv</code> with administrator user and password	22
Importing downloaded Certificate and installing to Personal	25
Creating Host record in Forward Lookup Zone (DNS Manager)	27
Removing Default Site and creating new site as Shah and giving binding type as https.....	28
Test the website with your client's machine. The certificate MUST show trusted from the client.	29

Active Directory Certificate Authority and IIS

Please provide a diagram of your environment and screenshots with descriptions of how you set up everything in this assignment. During your POC the professor will ask you to show them how you got everything working. Please refer to the rubric for information on grading.

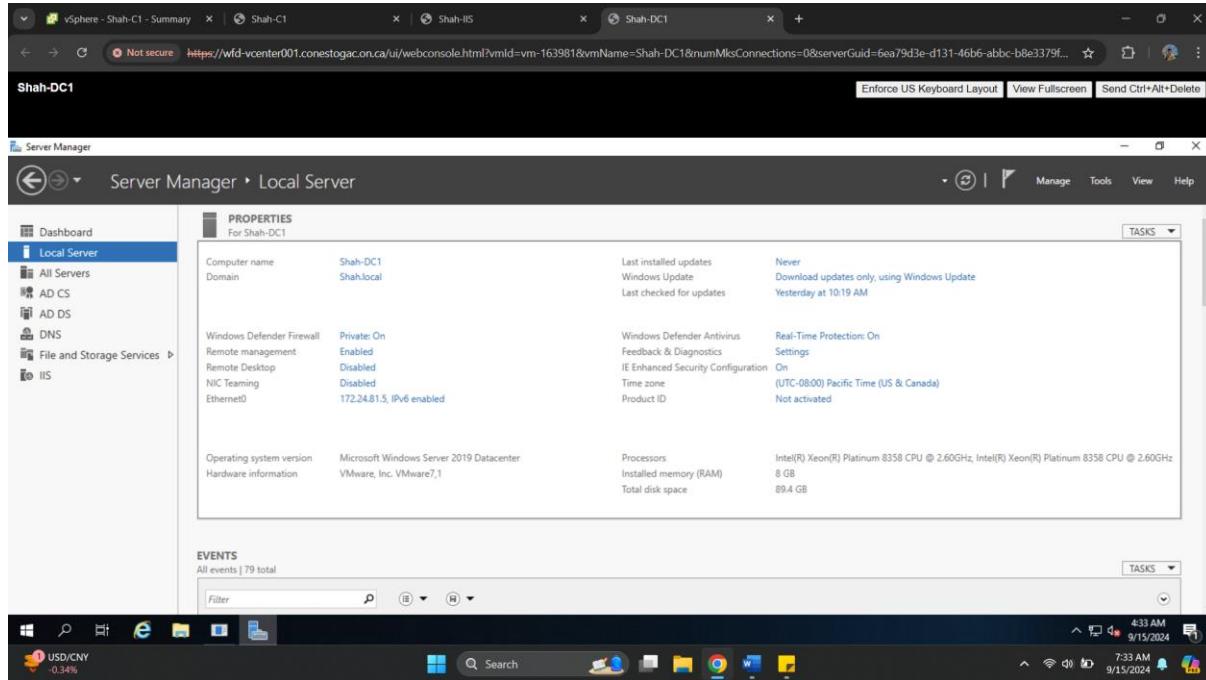
Diagram



Steps:

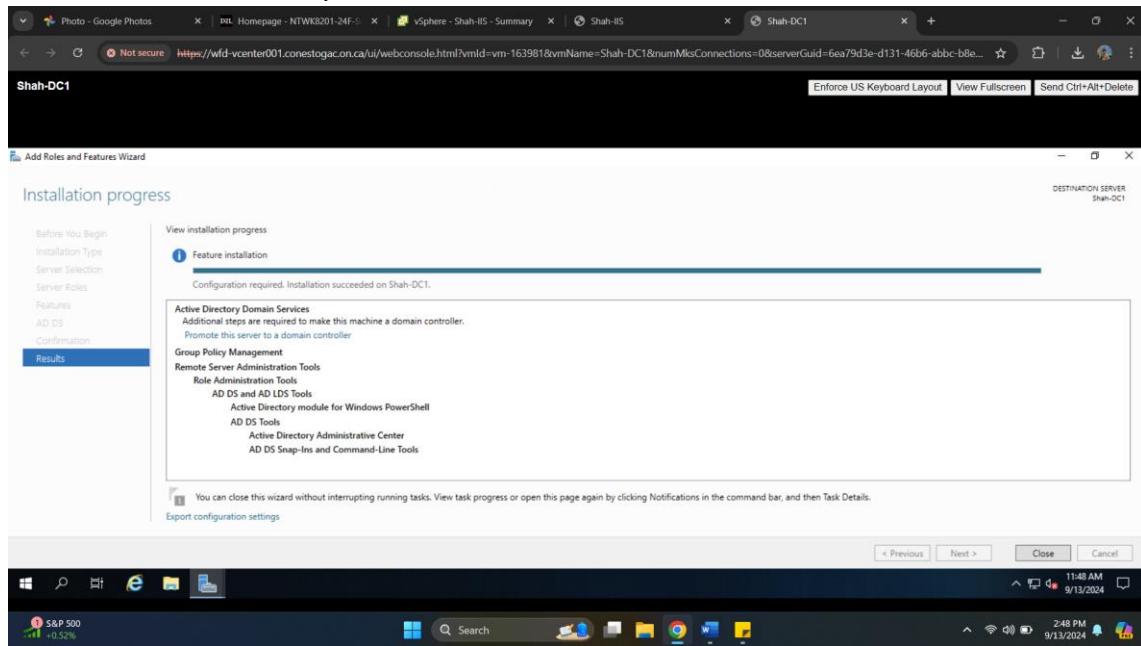
Install your first Windows Server with hostname **lastname-DC1**.

1x Domain Controller with Active Directory Domain Services and Active Directory Certificate Services Certificate Authority (IP:172.24.81.5)

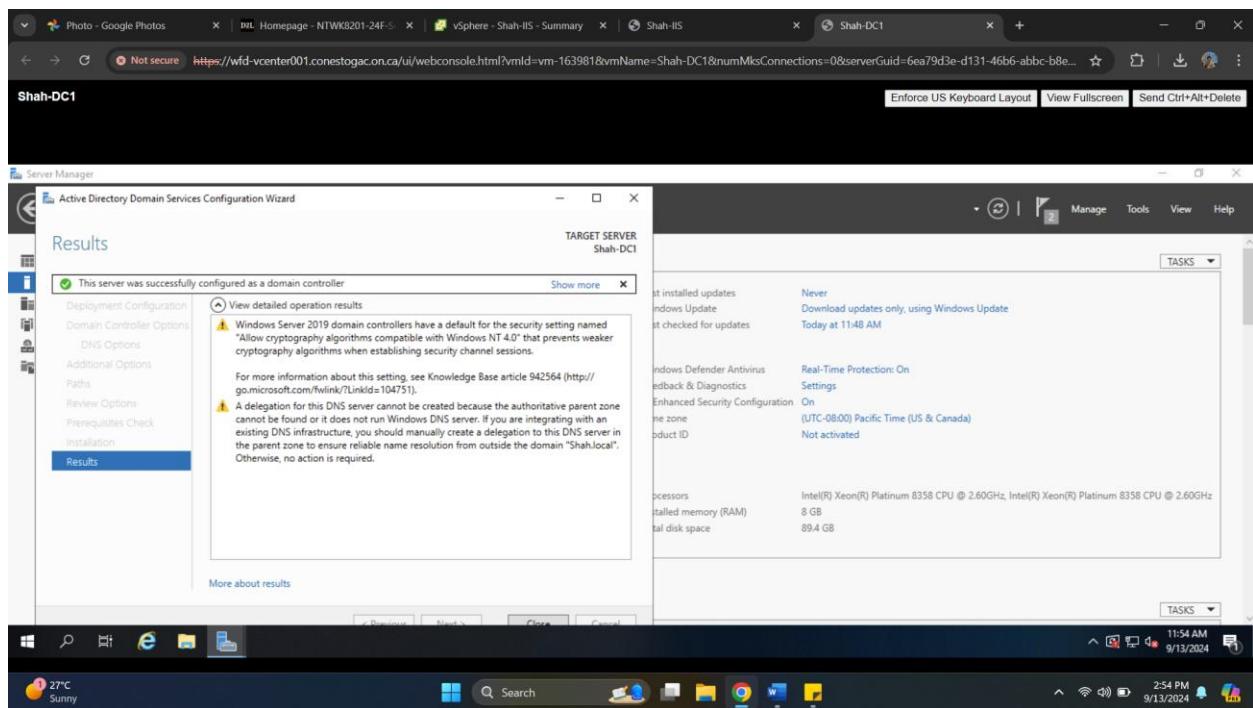


Promote your first Windows Server to a domain controller with domain name **lastname.local**.

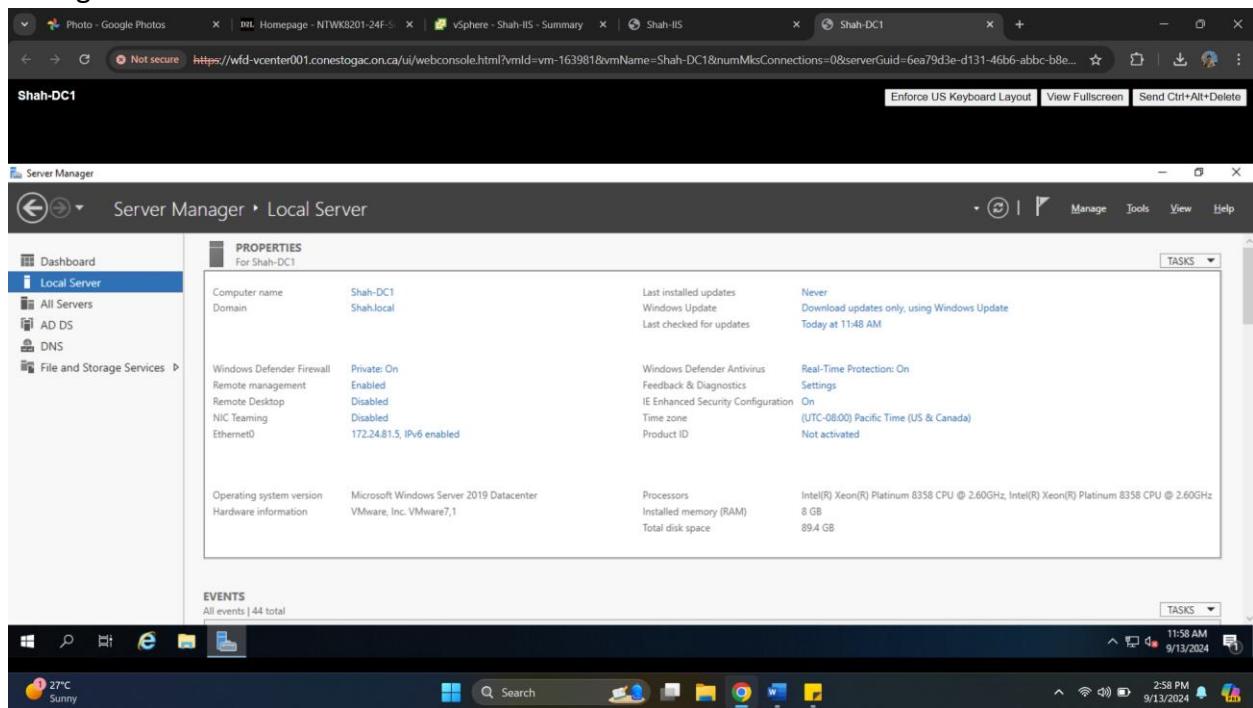
Installed Active Directory Domain Services on SHAH-DC1



Promoted SHAH-DC1 to Domain Controller

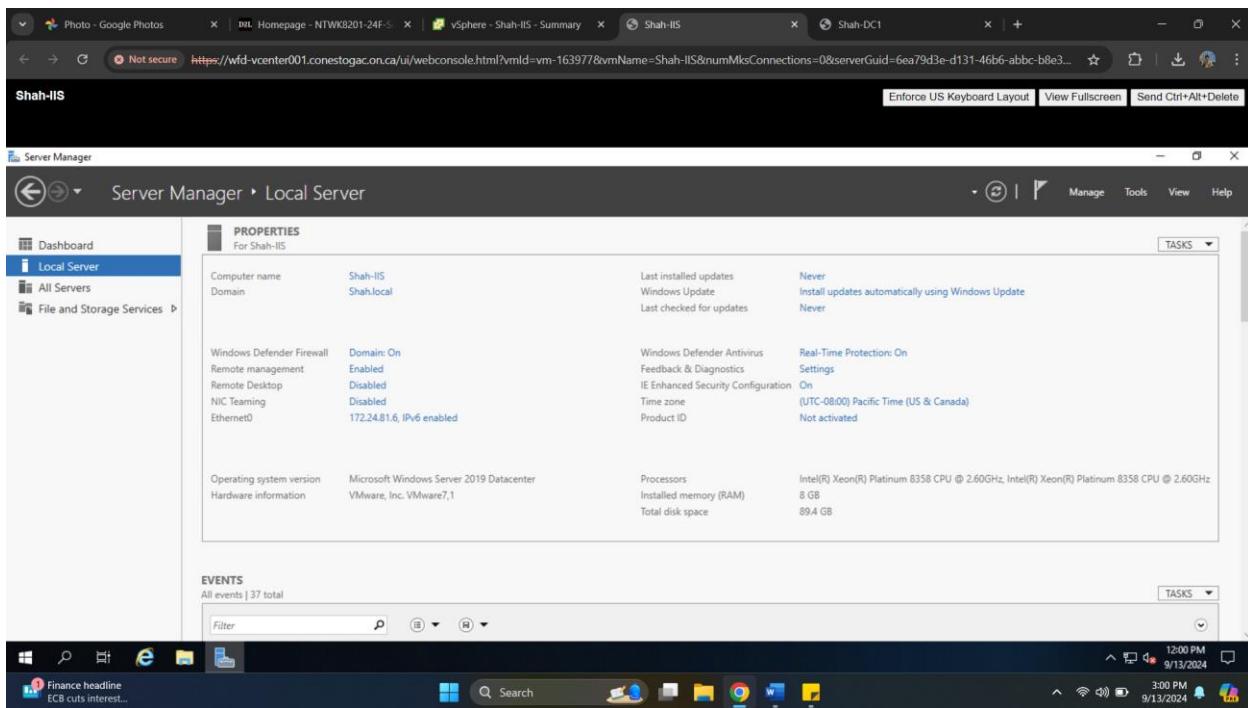
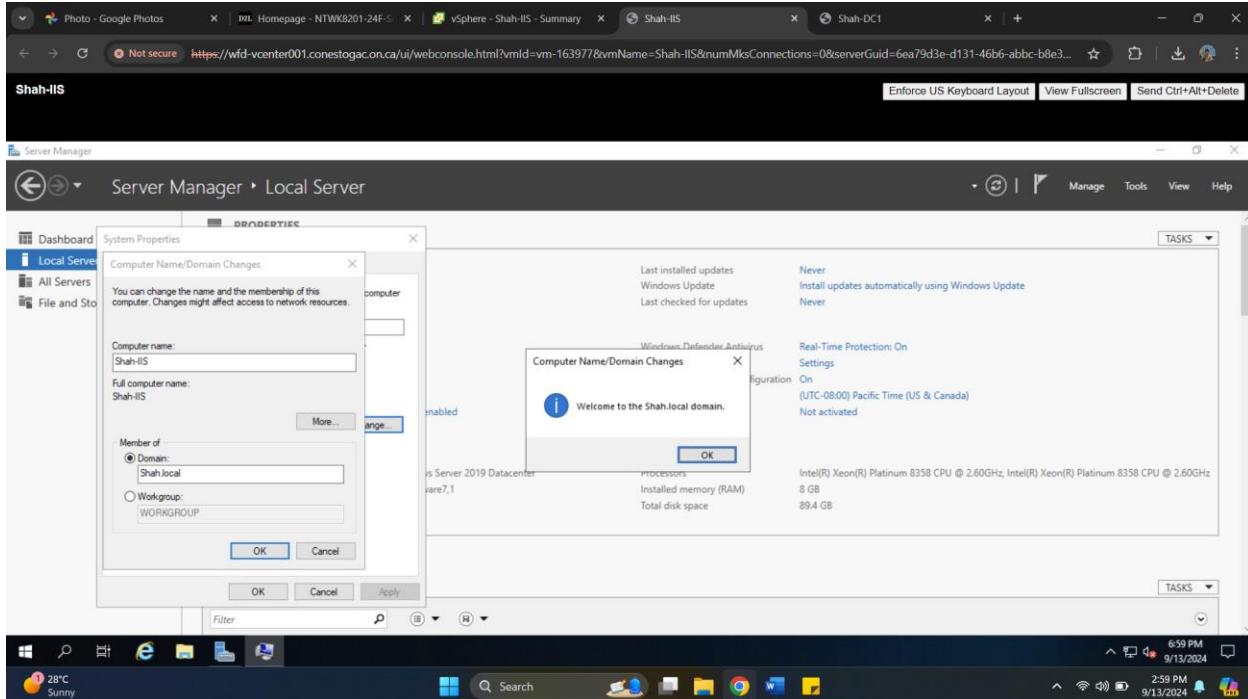


Configured Domain Name as Shah.local



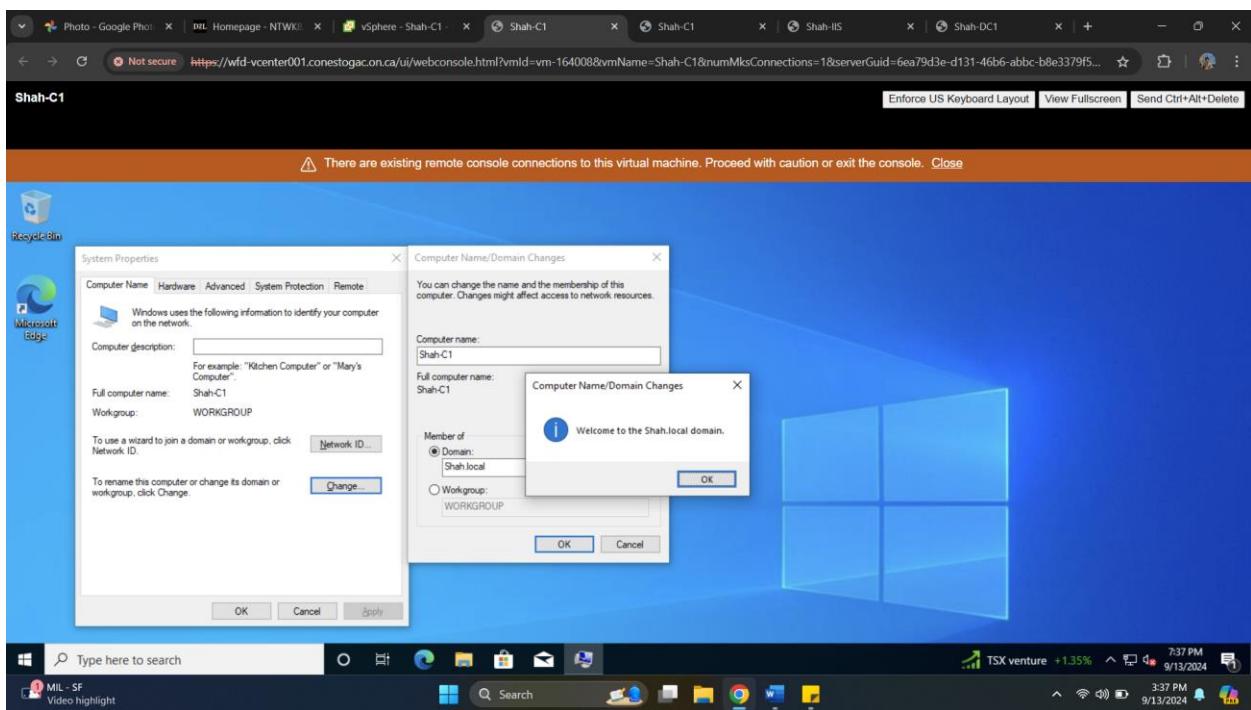
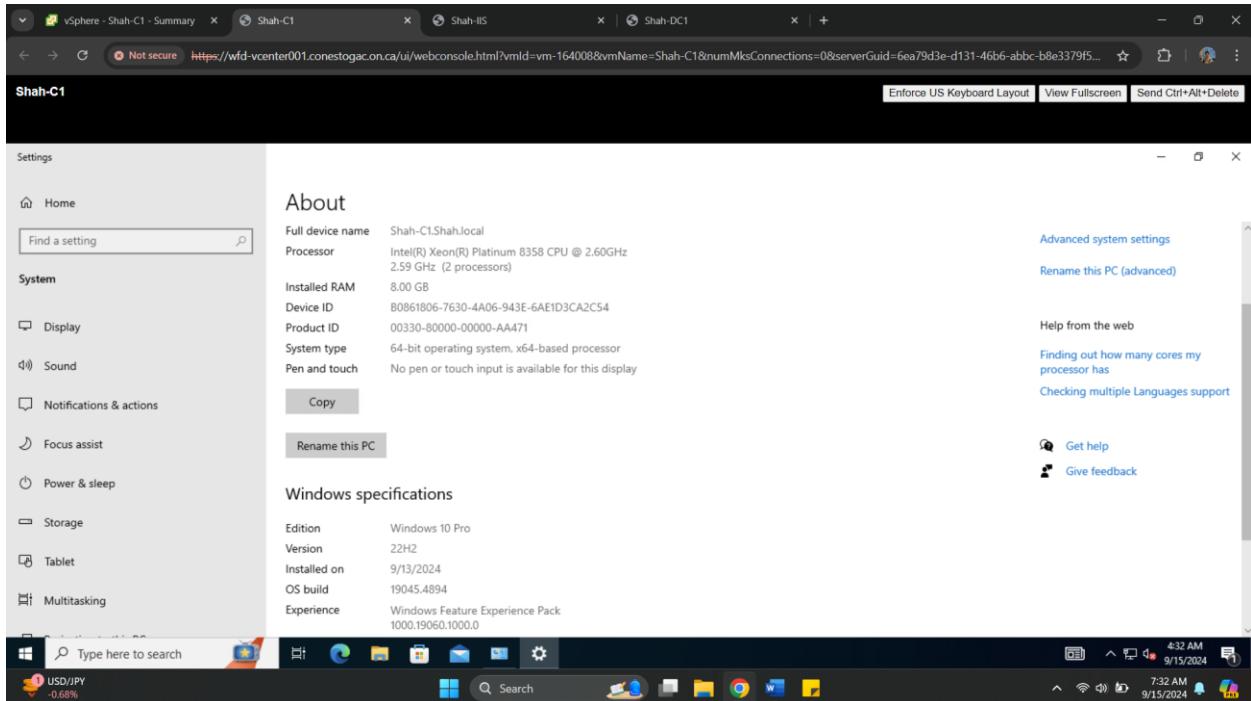
Install your second Windows Server with hostname **lastname-IIS** and join it to **lastname.local**.

1x Member Server with IIS (IP: 172.24.81.6)



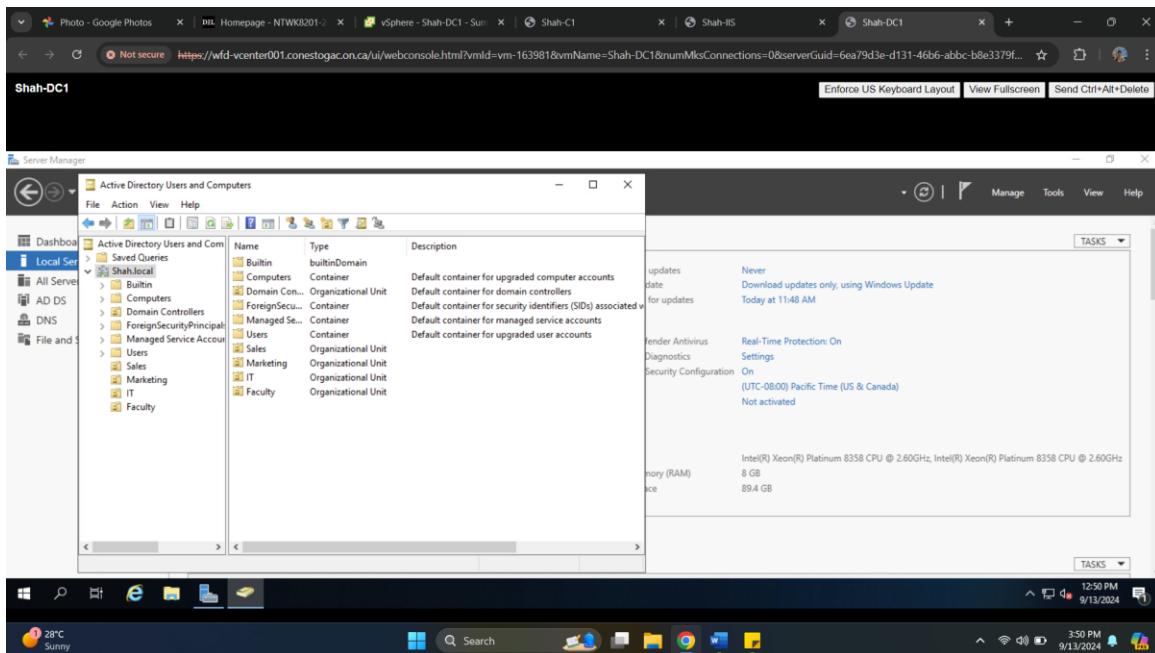
Install your Windows client with hostname **Lastname-C1** and join it to **lastname.local**.

1x Windows 10 Domain joined machine (172.24.81.7)

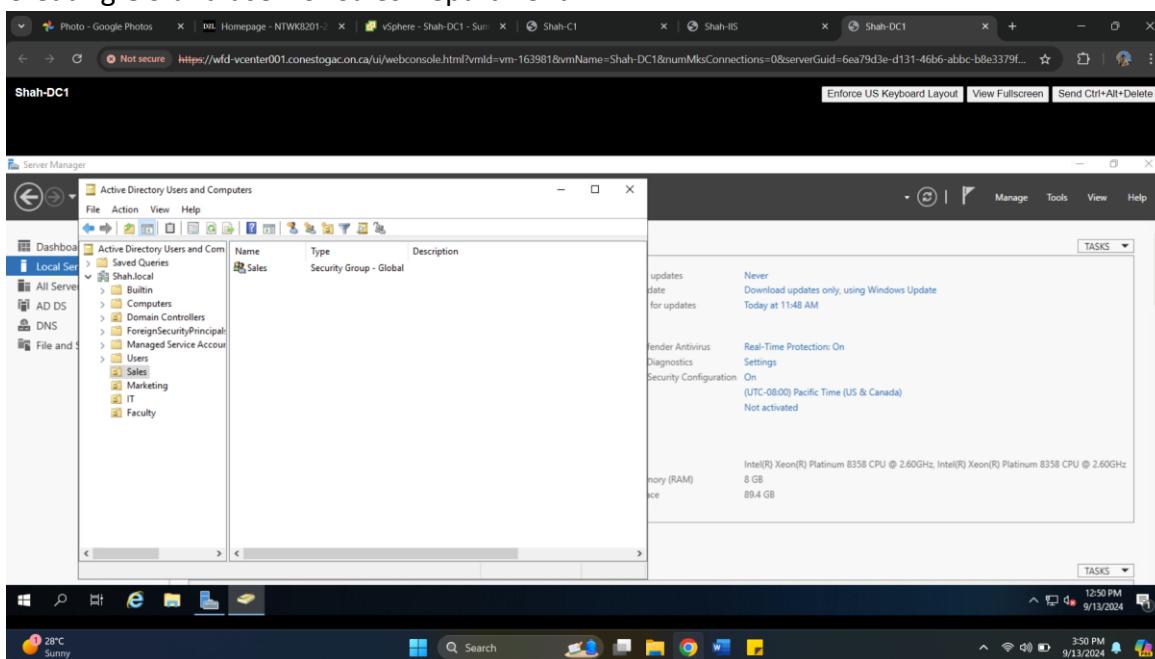


Create an OU structure and one security group per department with test users following best practices for the below departments.

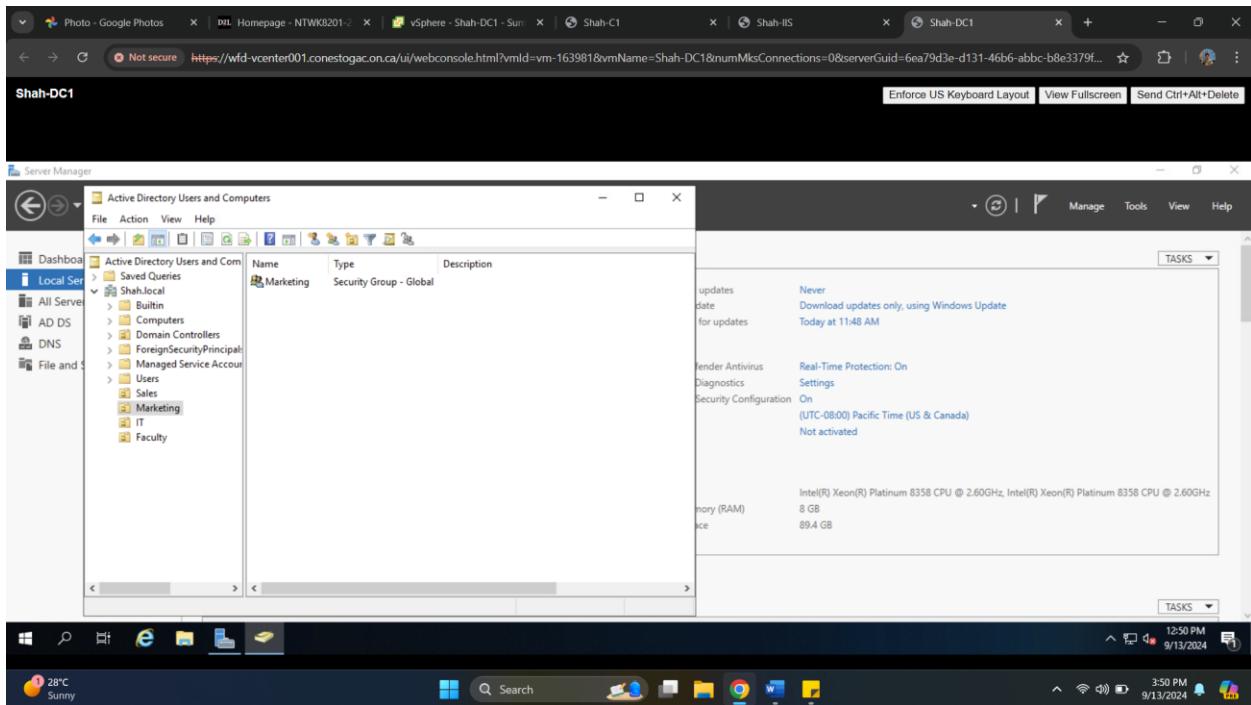
- a. Sales
- b. Marketing
- c. IT
- d. Faculty



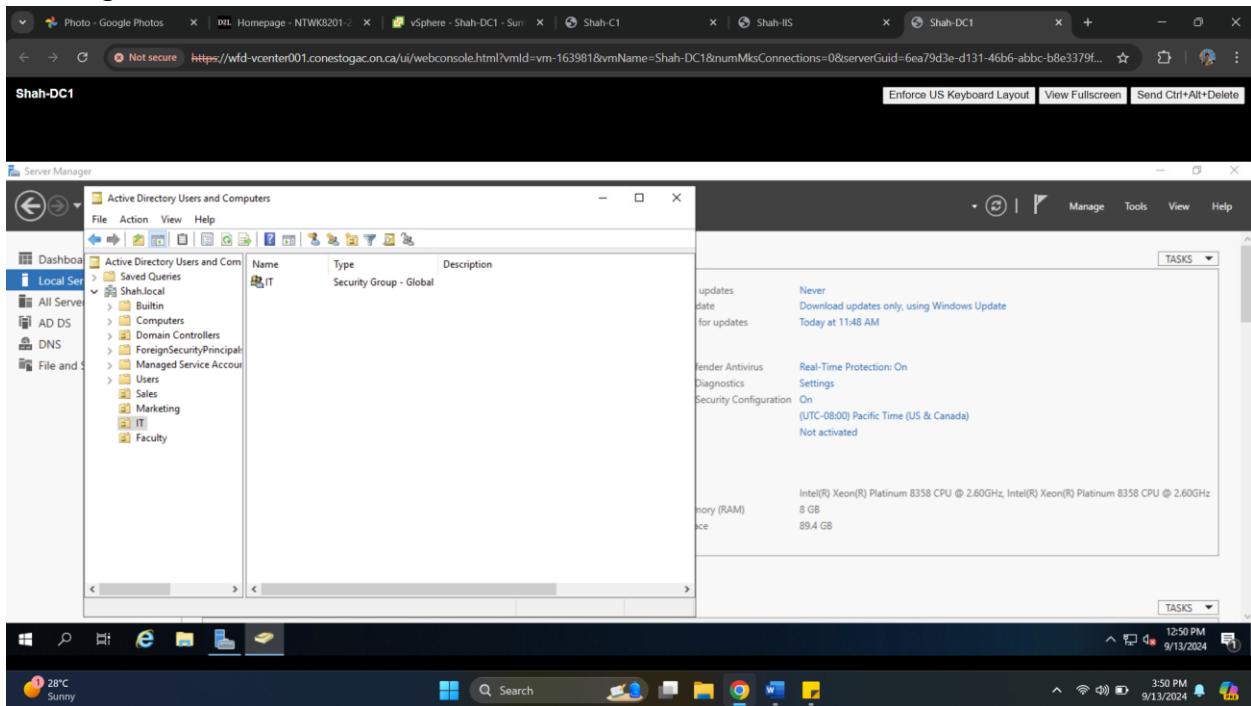
Creating OU and user for Sales Department



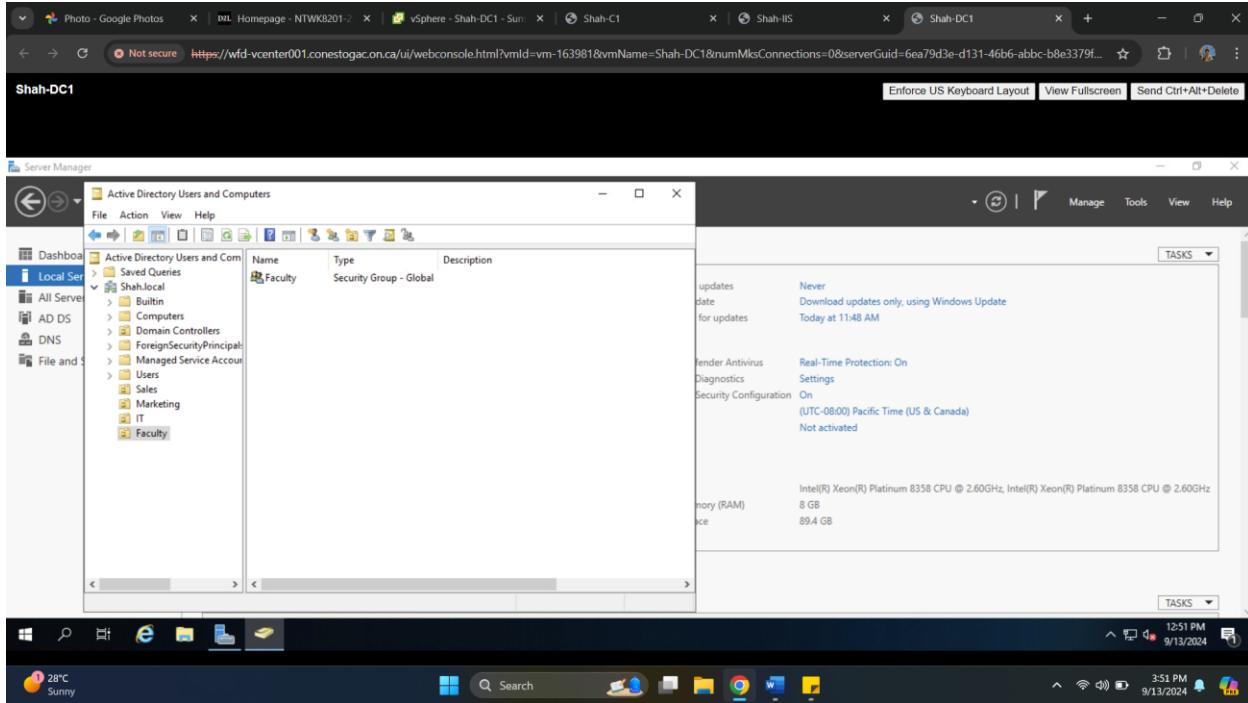
Creating Marketing OU and Test user



Creating IT OU and Test user

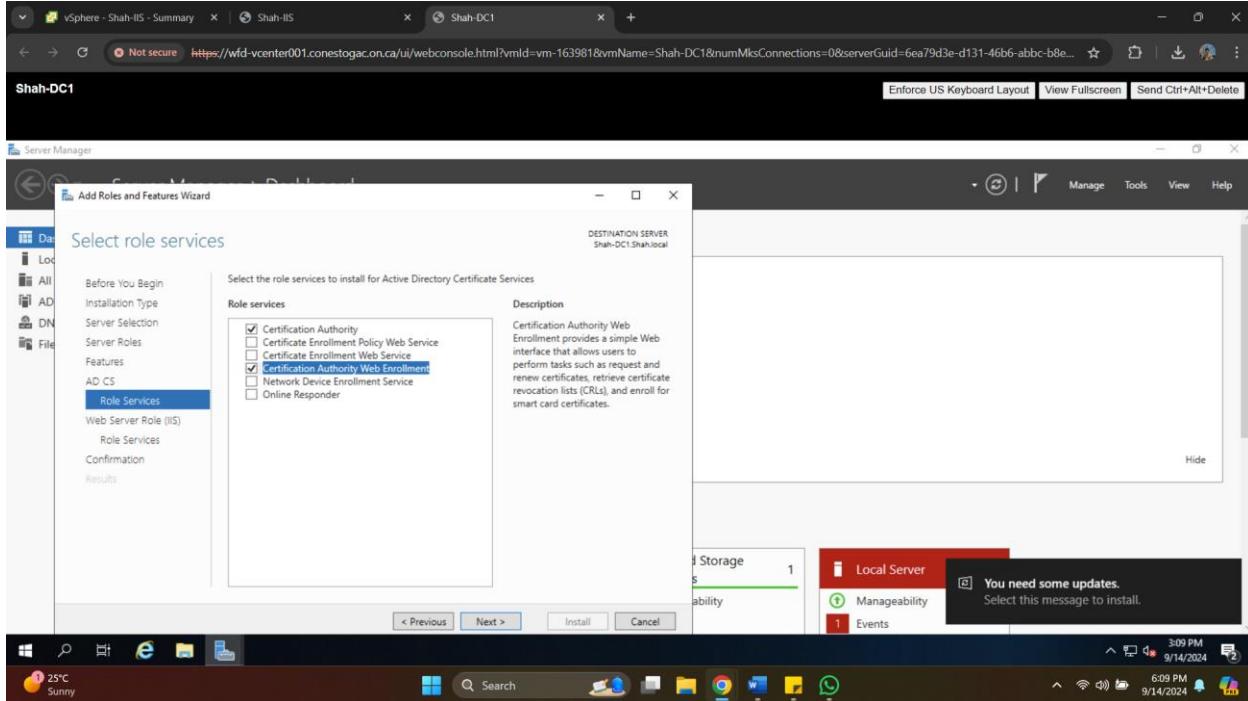


Creating Faculty OU and Test User

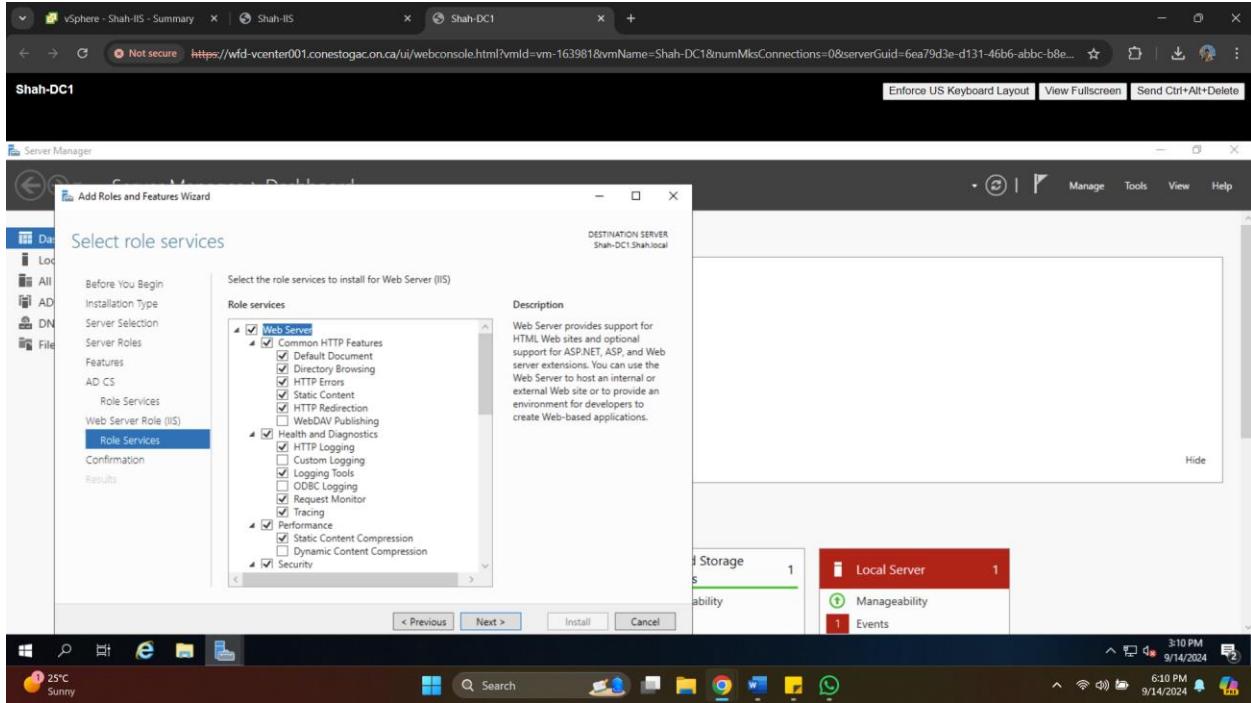


Install Active Directory Certificate Services and configure your lastname-DC1 as a Certificate Authority.

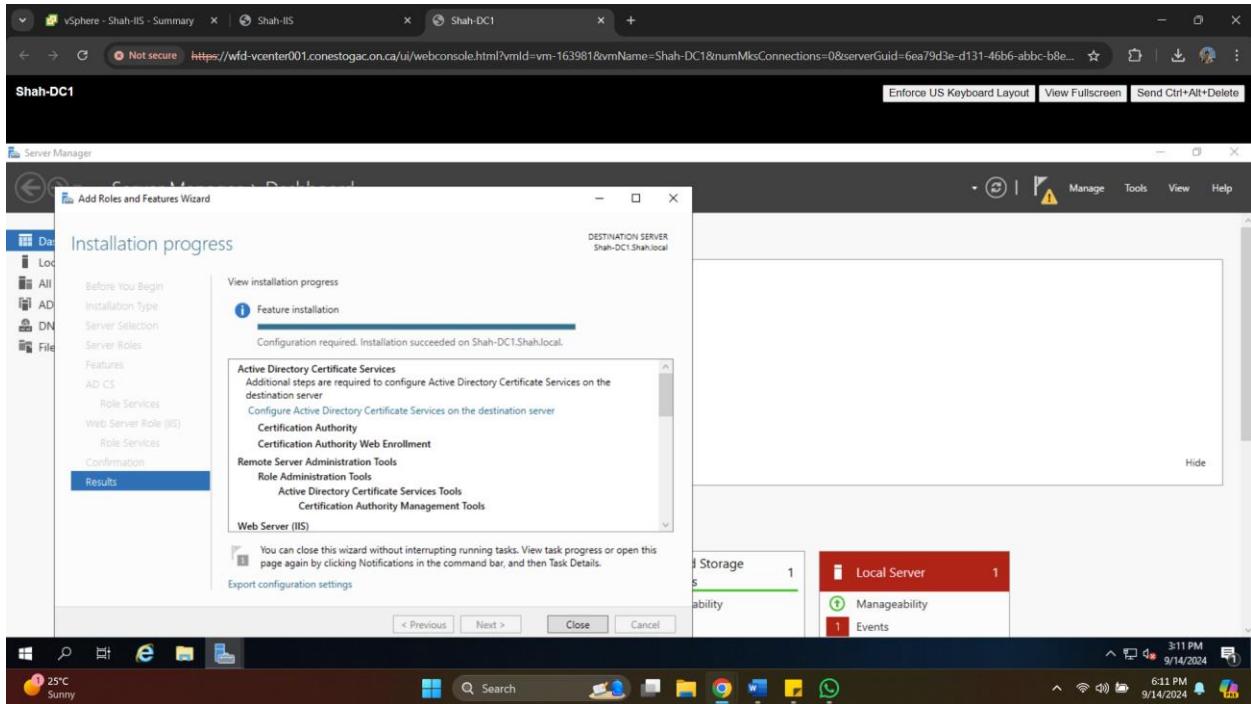
Selecting roles to install as Certification Authority and Certification Authority Web Enrollment.



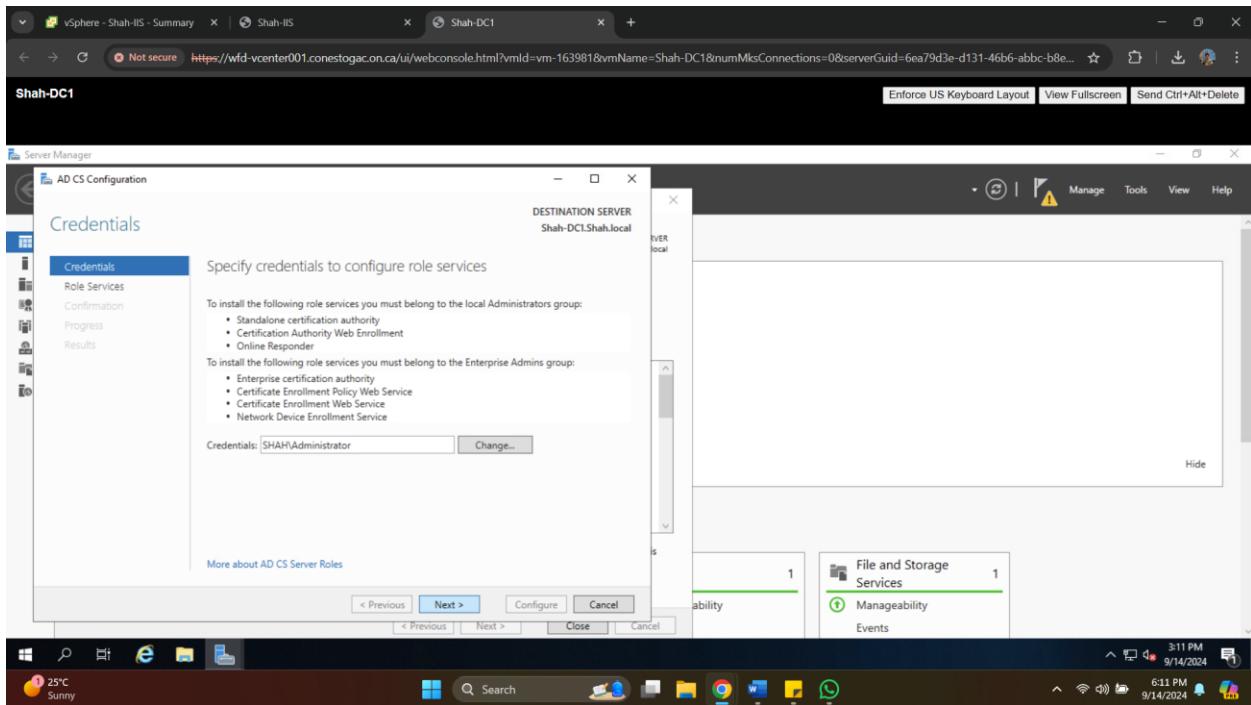
Selecting roles to install on Web Server on Shah-DC1



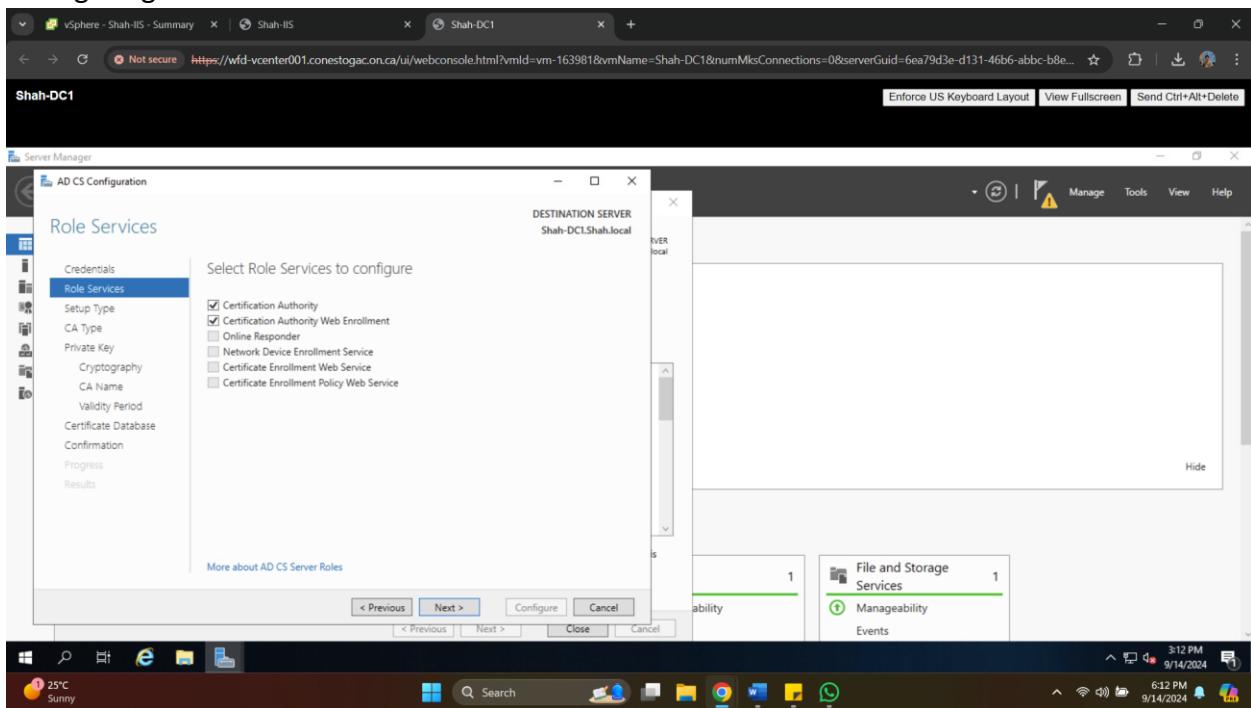
Successfully installing roles and features on Shah-DC1



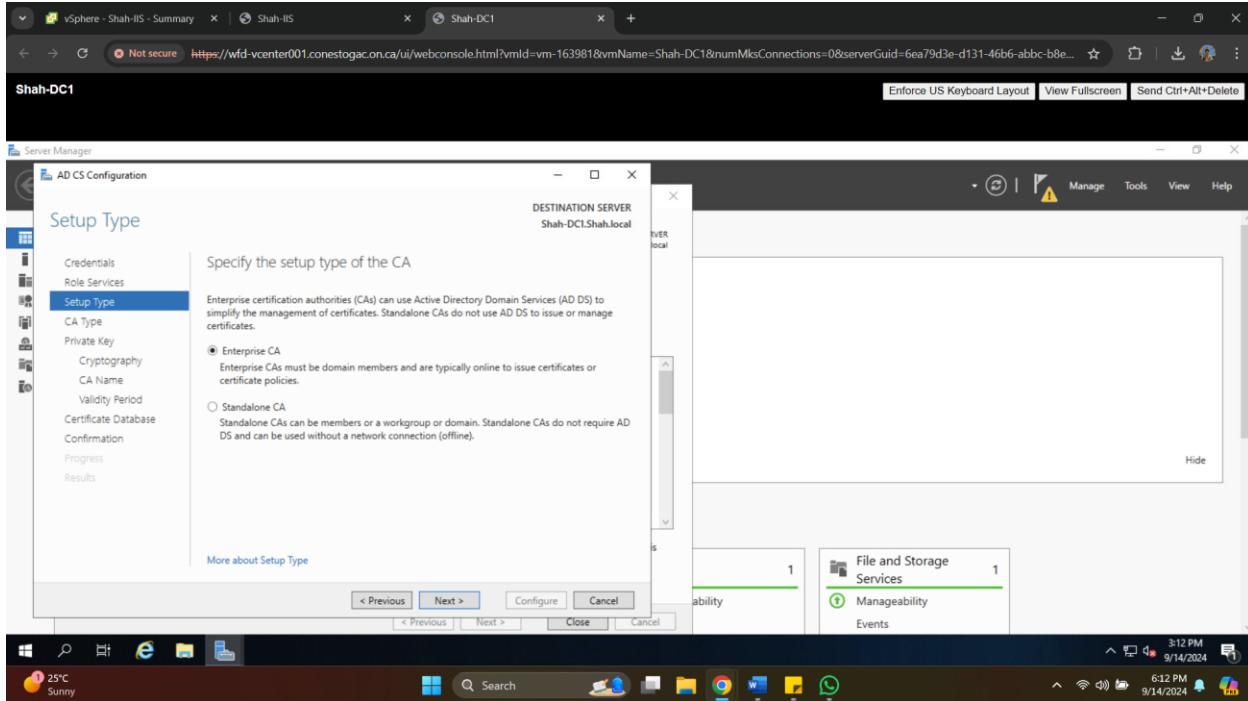
Specifying credentials to configure role services



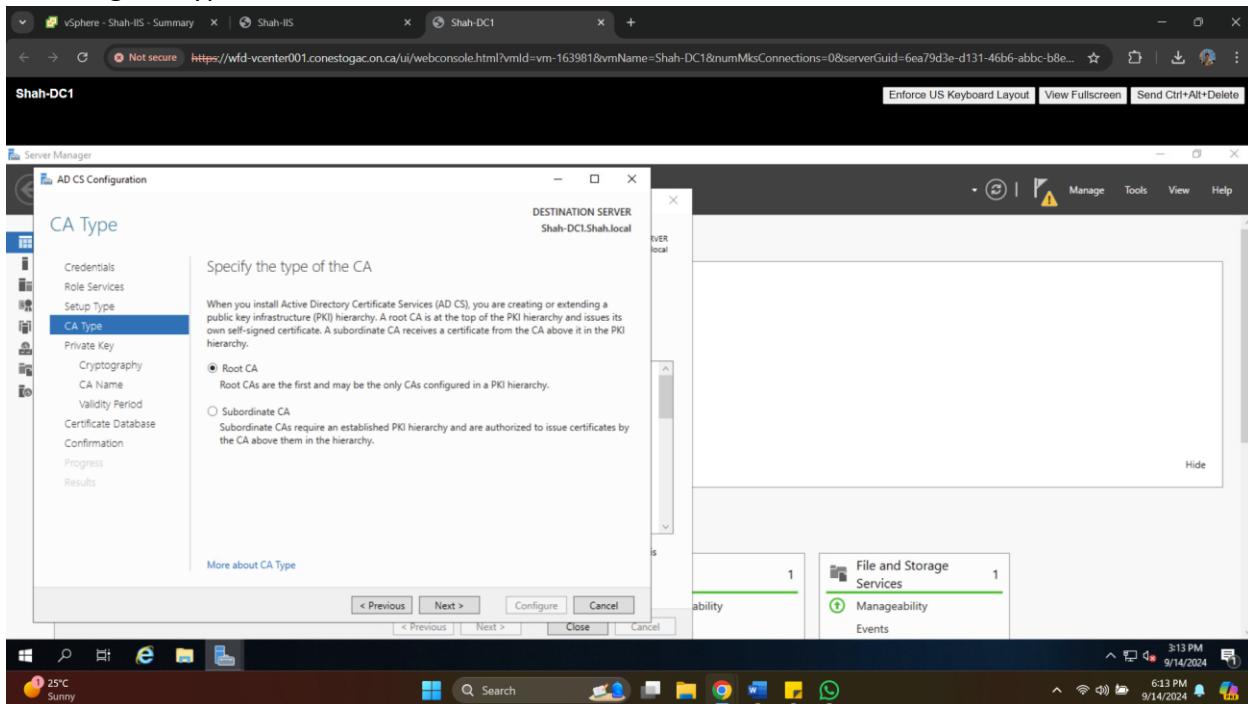
Configuring AD CS role services



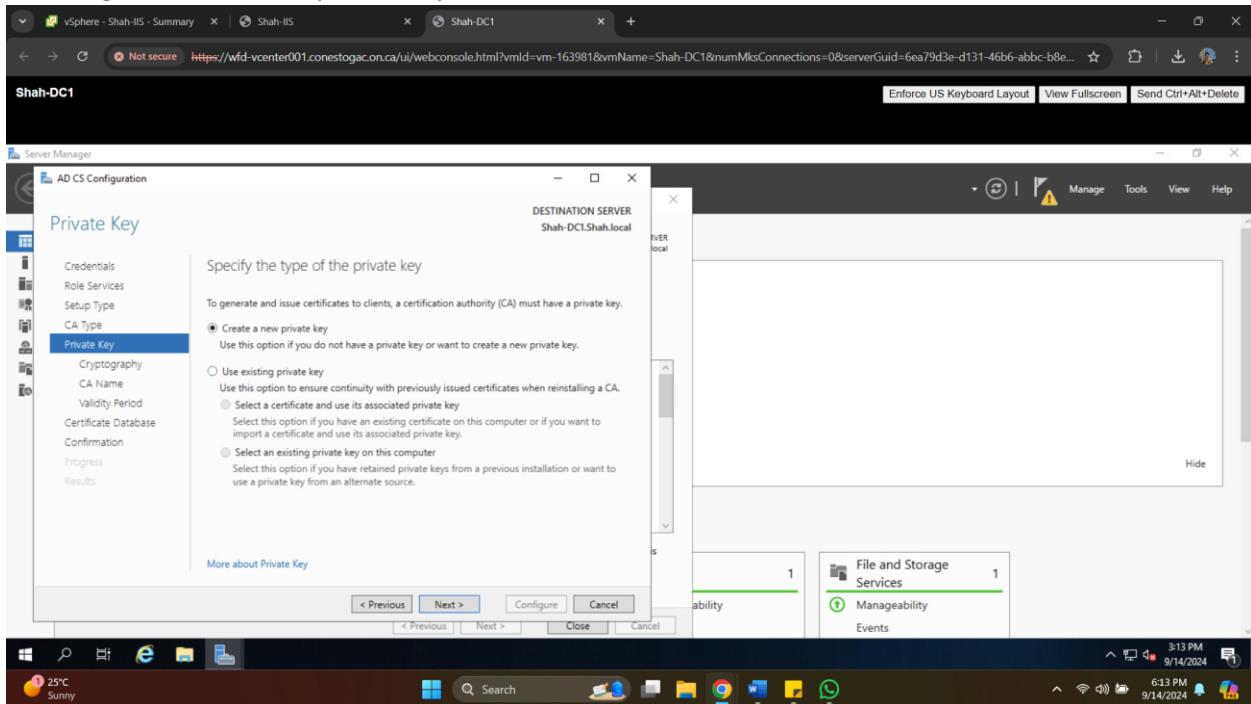
Selecting setup type of the CA as Enterprise CA



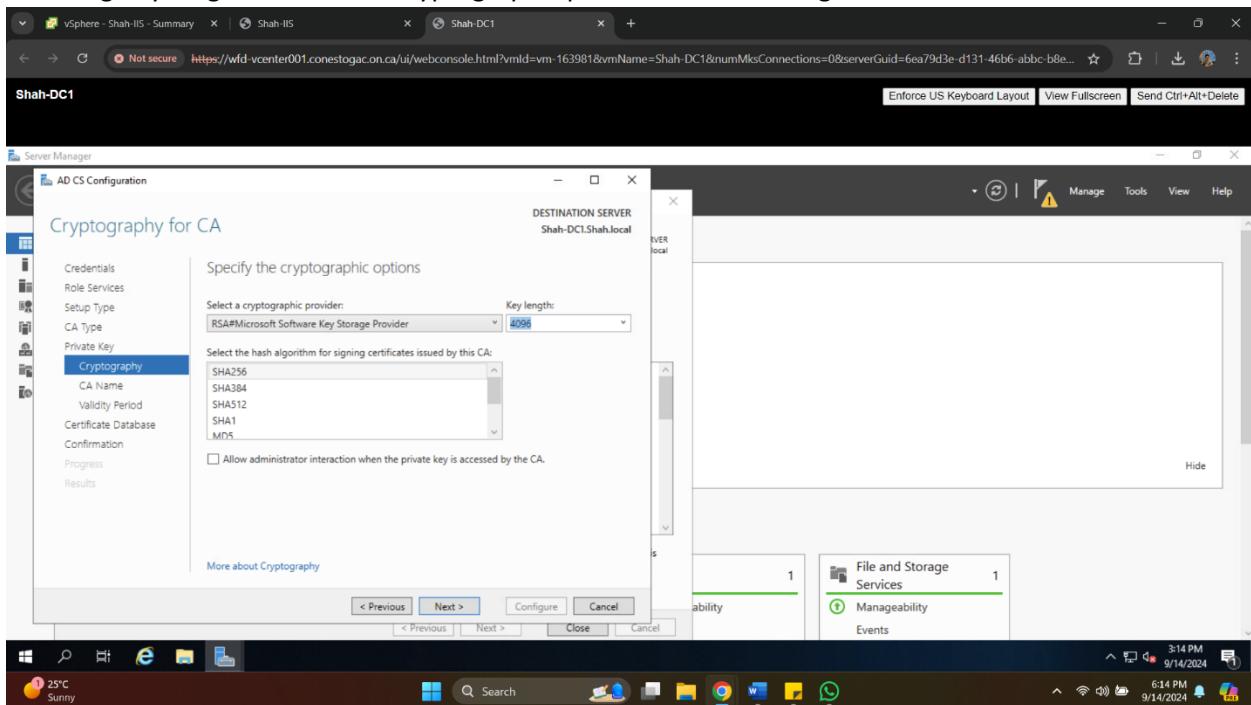
Selecting the type of the CA as Root CA



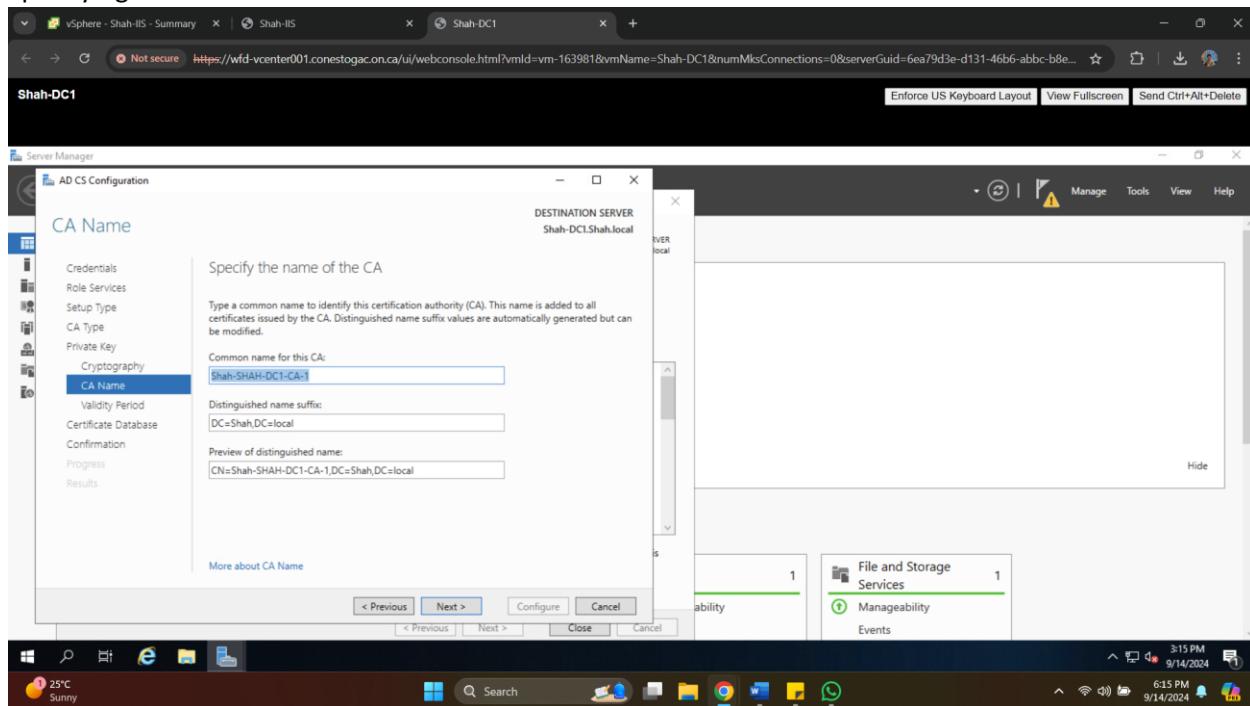
Selecting to Create a new private key.



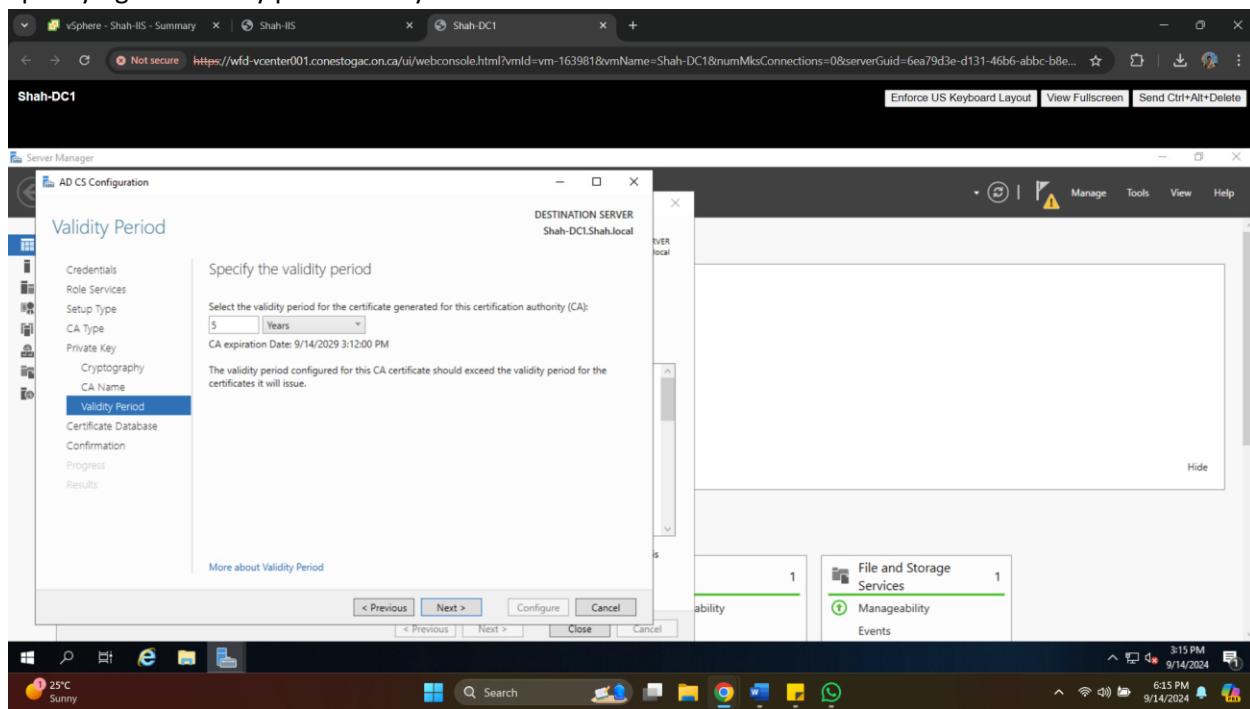
Selecting Key length as 4096 for Cryptographic provider with hash algorithm of SHA256



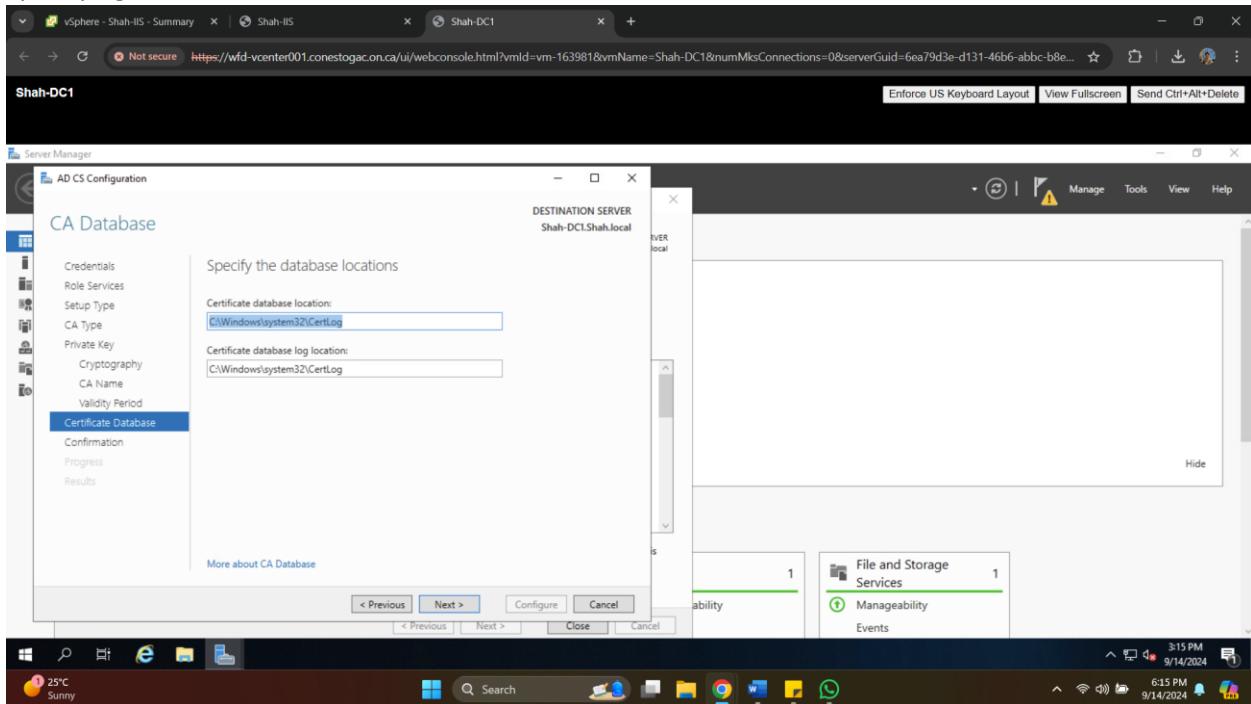
Specifying the name of the CA



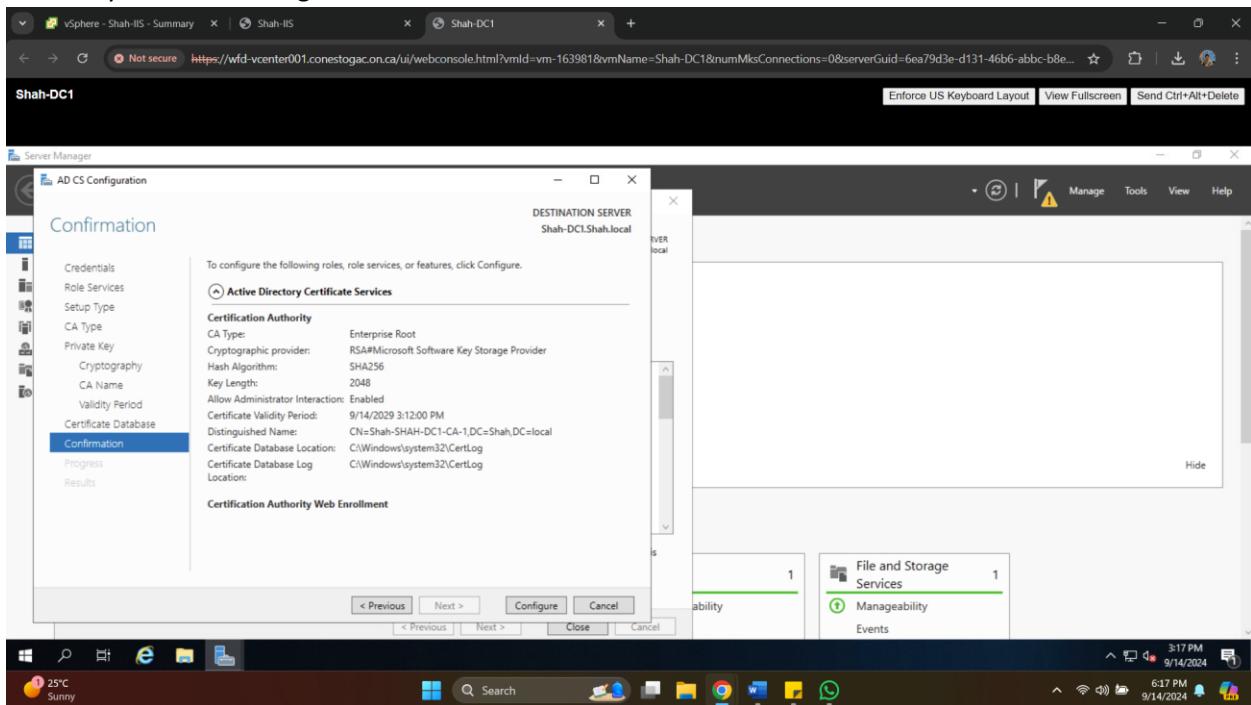
Specifying the validity period as 5 years



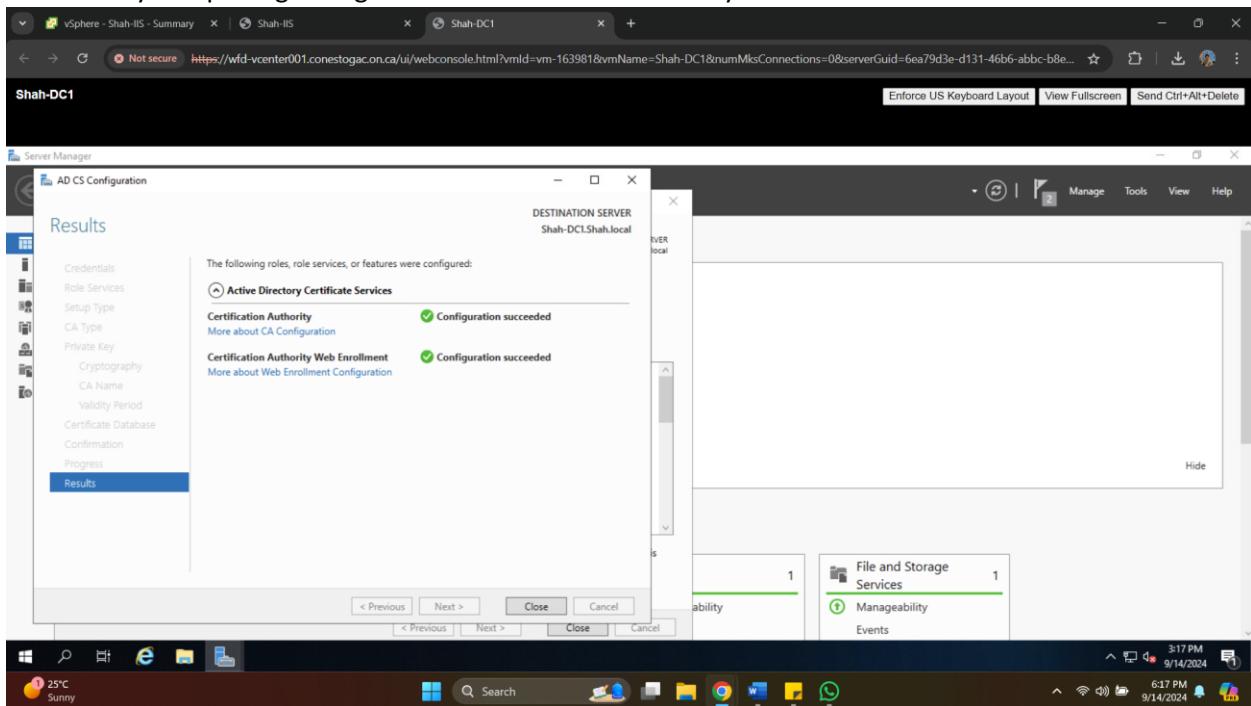
Specifying the database locations



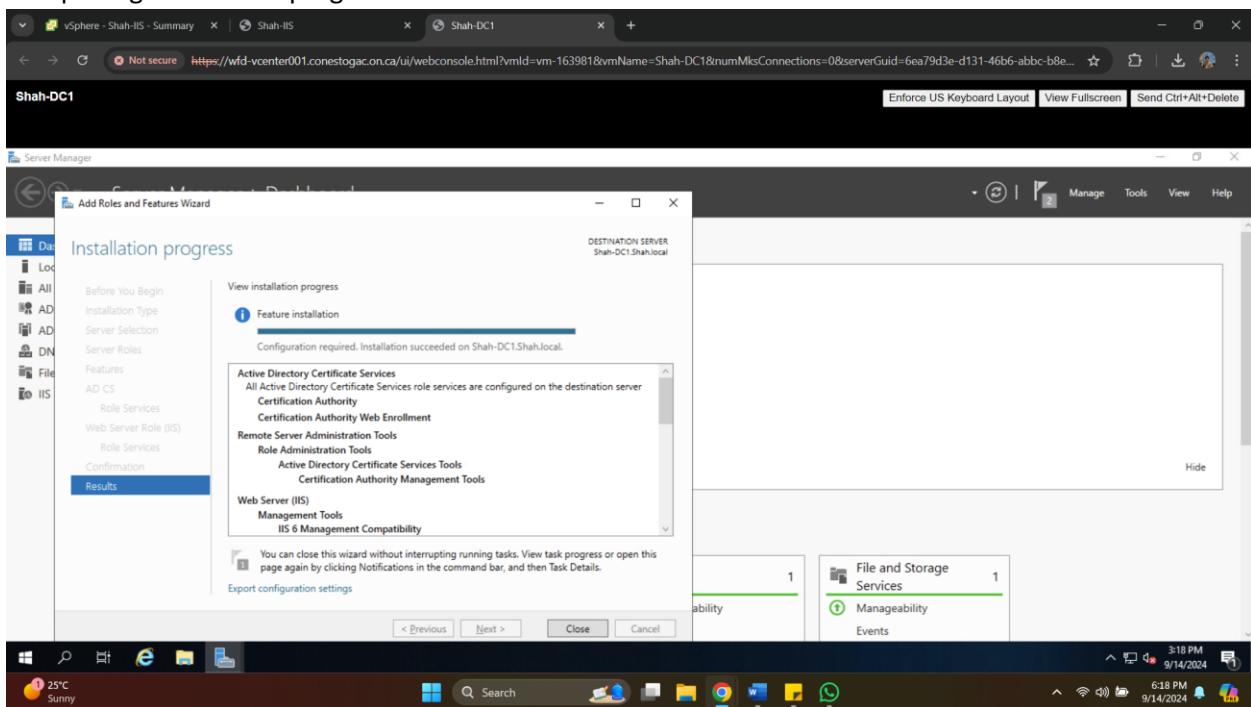
Summary of AD CS Configuration



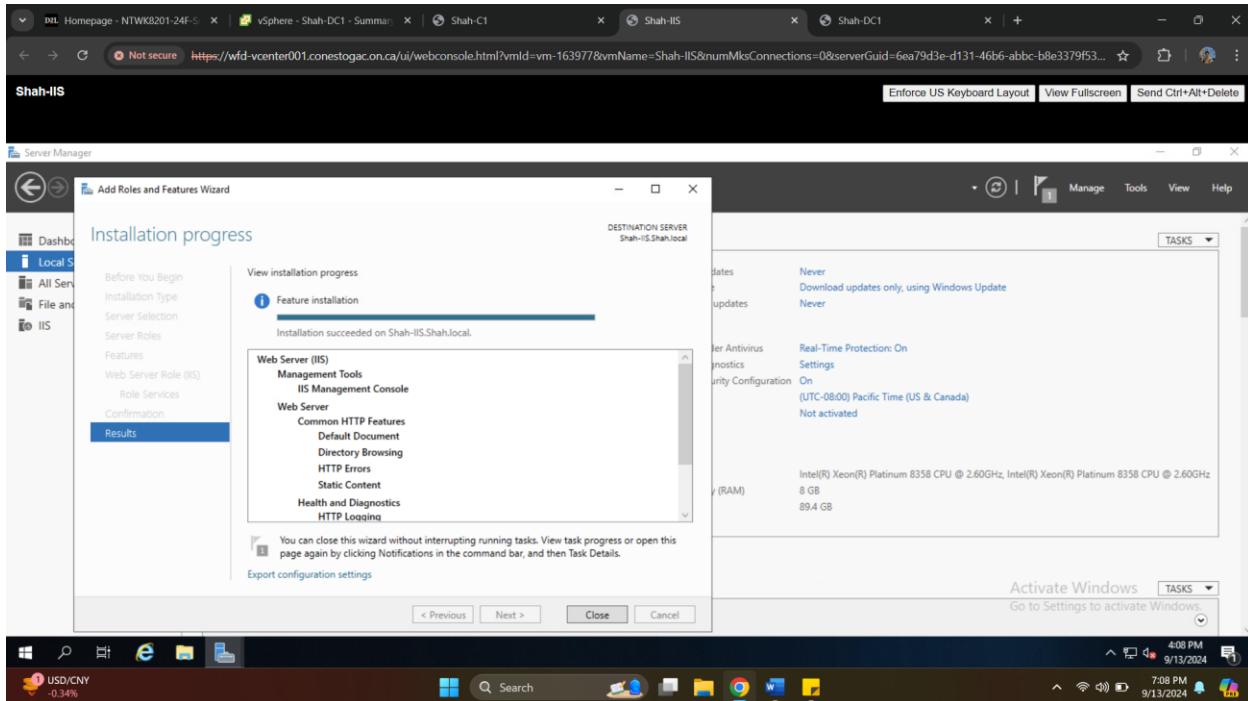
Successfully completing configuration of Certificate Authority and Web Enrollment



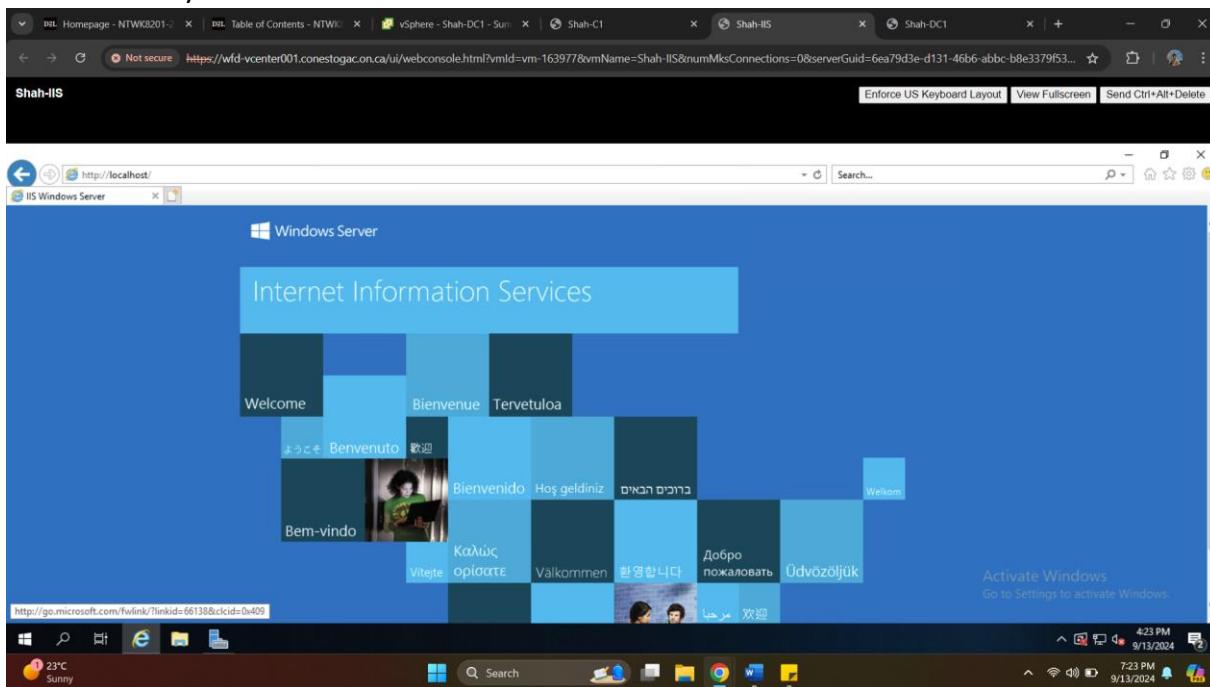
Completing installation progress



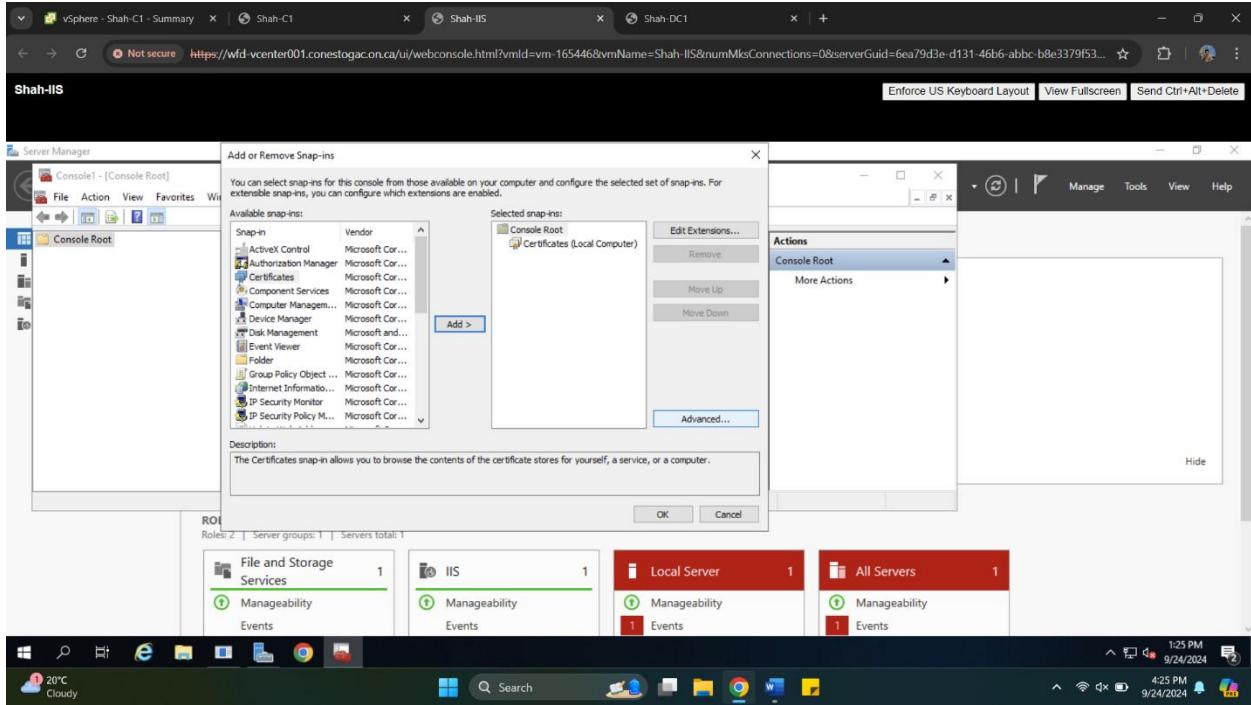
Install IIS on your member server.



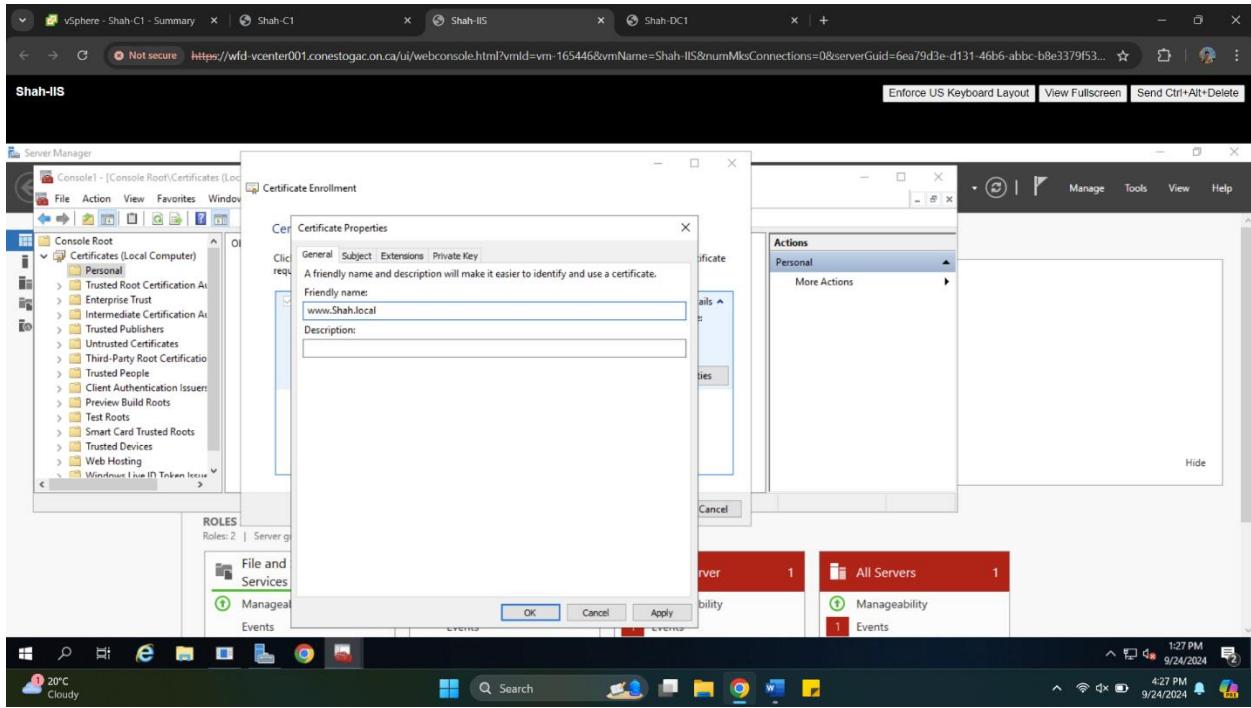
IIS successfully installed



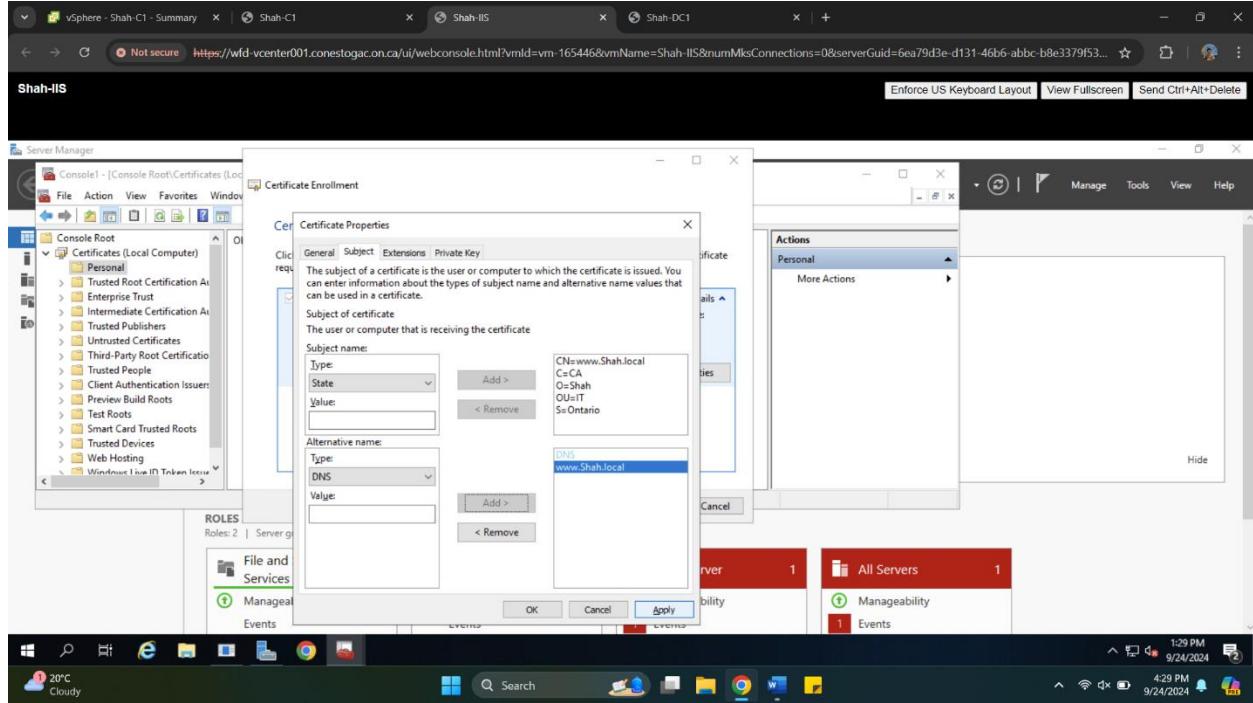
Edit the default website to use HTTPS with a signed certificate from your Certificate Authority.



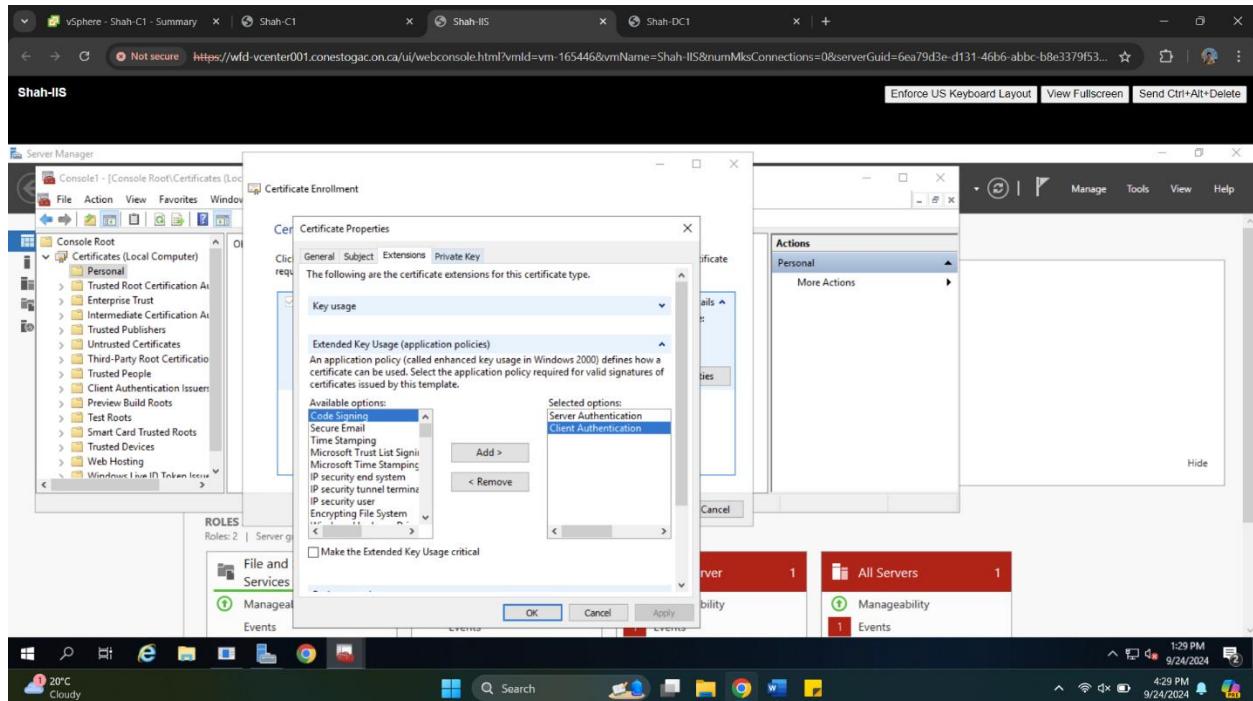
Providing Certificate Properties name as www.Shah.local



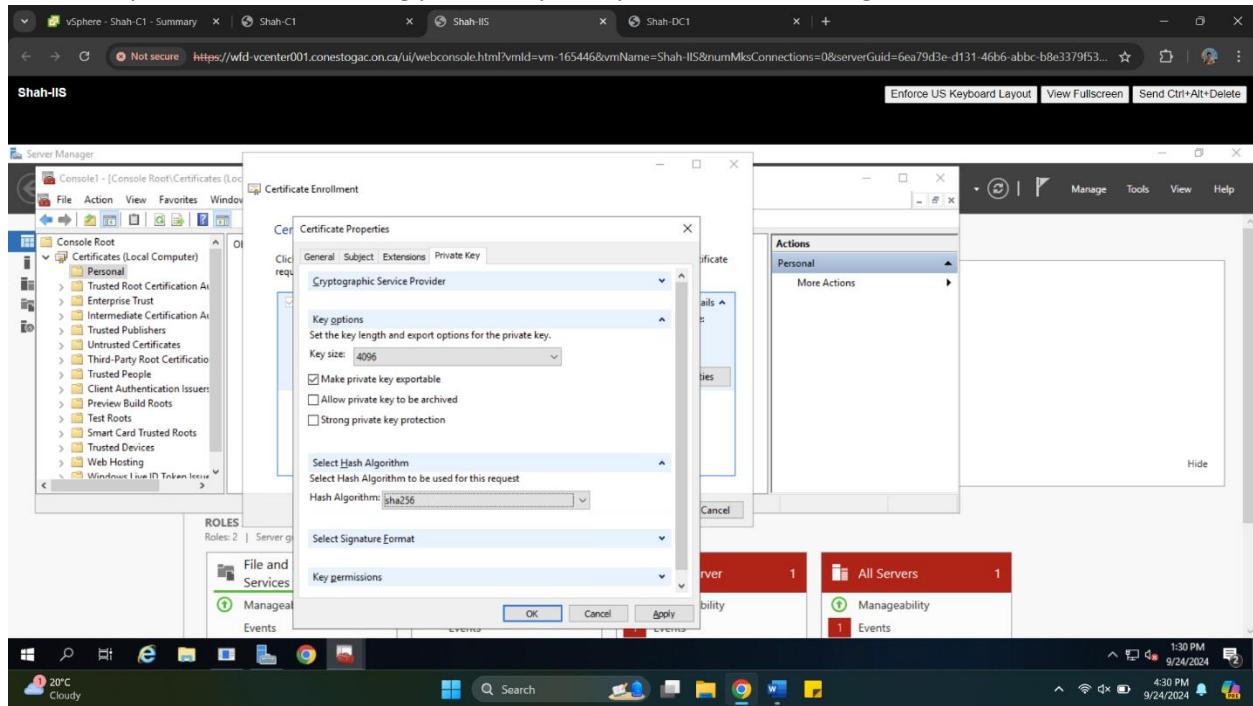
Providing Subject names CN=www.Shah.local, C=CA, O=Shah, OU=IT, S=Ontario Alternative Name DNS=www.Shah.local



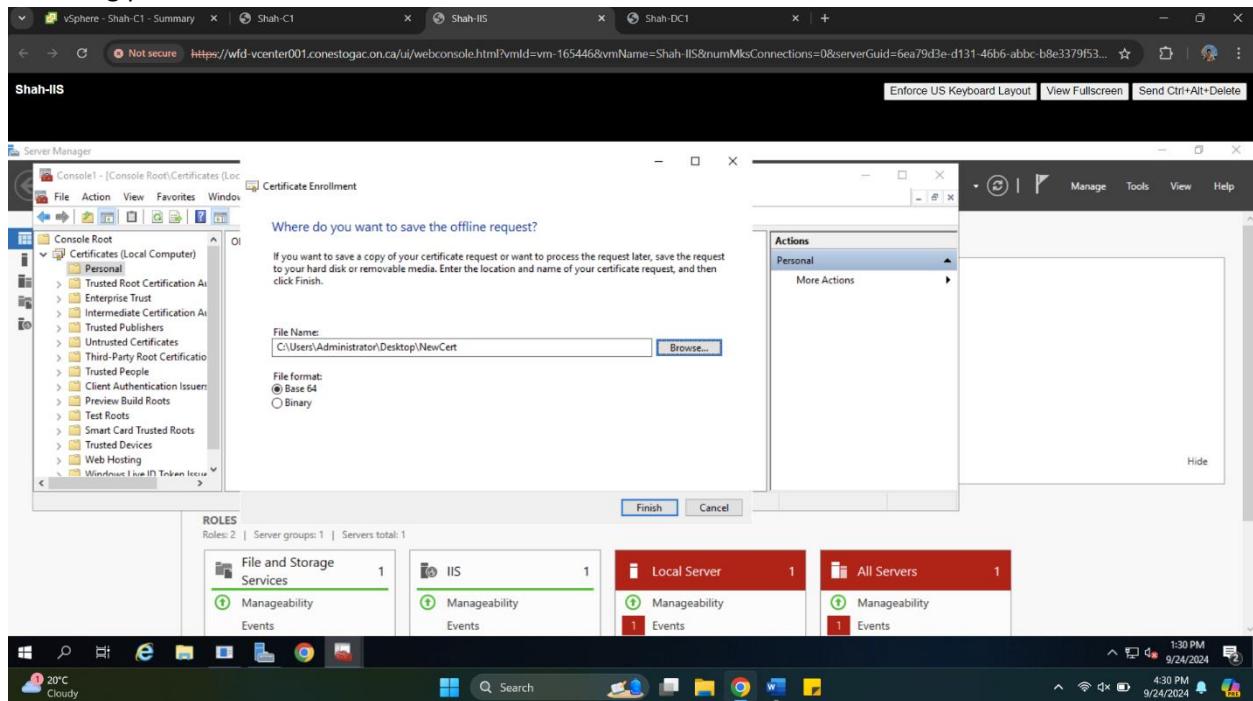
Extensions- Server Authentication and Client Authentication



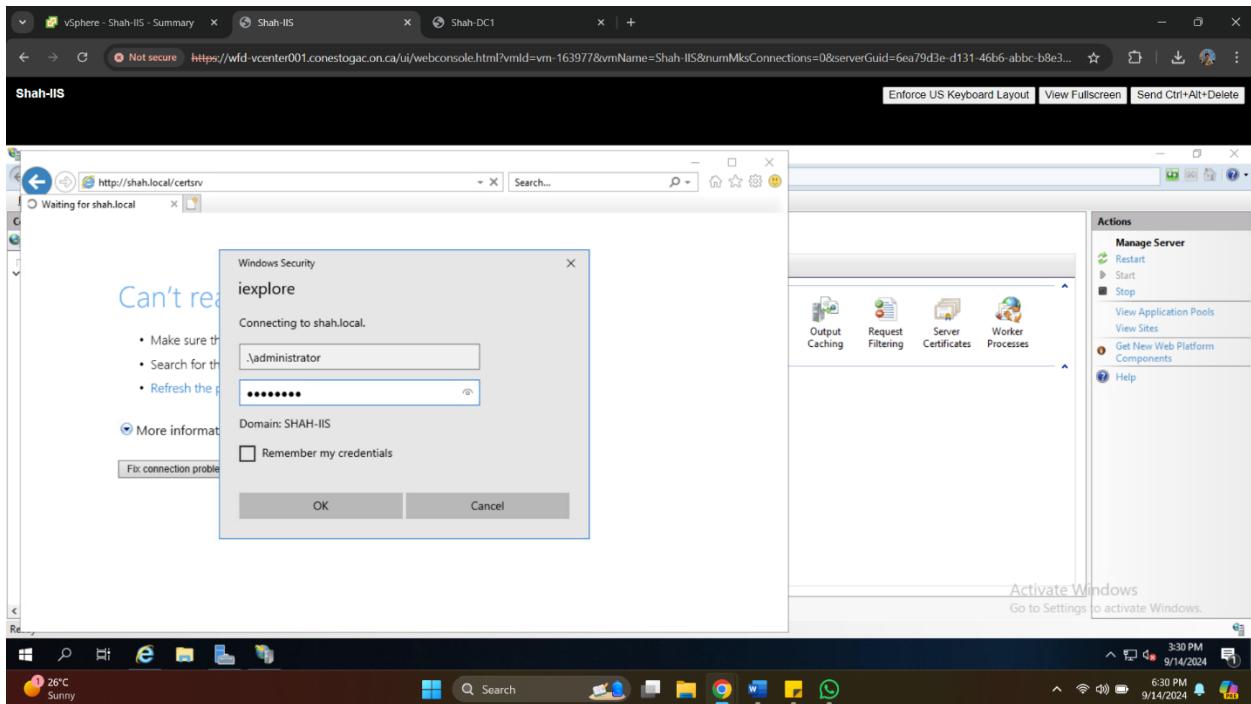
Private Key size=4096 and making private key as exportable and hash algorithm as sha256



Providing path and file format as Base64



Opening http://shah.local/certsrv with administrator user and password



Selecting Request a certificate

A screenshot of a web browser displaying the Microsoft Active Directory Certificate Services (AD CS) website. The URL is "https://wfd.vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-163977&vmName=Shah-IIS&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-b8e3...". The page title is "Microsoft Active Directory ...". The main content area is titled "Welcome" and includes a paragraph about using certificates for verification and encryption. It also states that users can download CA certificates or view pending requests. A section titled "Select a task:" lists three options: "Request a certificate", "View the status of a pending certificate request", and "Download a CA certificate, certificate chain, or CRL". The bottom right corner of the screen shows a watermark for "Activate Windows" with the instruction "Go to Settings to activate Windows".



Selecting advance certificate request option

Shah-IIS

Not secure https://vfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-163977&vmName=Shah-IIS&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-...

Microsoft Active Directory ...

Microsoft Active Directory Certificate Services – Shah-SHAH-DC1-CA-1

Request a Certificate

Select the certificate type:

User Certificate

Or, submit an [advanced certificate request](#).

Activate Windows
Go to Settings to activate Windows.

Selecting Create and submit a request to this CA

Shah-IIS

Not secure https://vfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-163977&vmName=Shah-IIS&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-...

Microsoft Active Directory ...

Microsoft Active Directory Certificate Services – Shah-SHAH-DC1-CA-1

Advanced Certificate Request

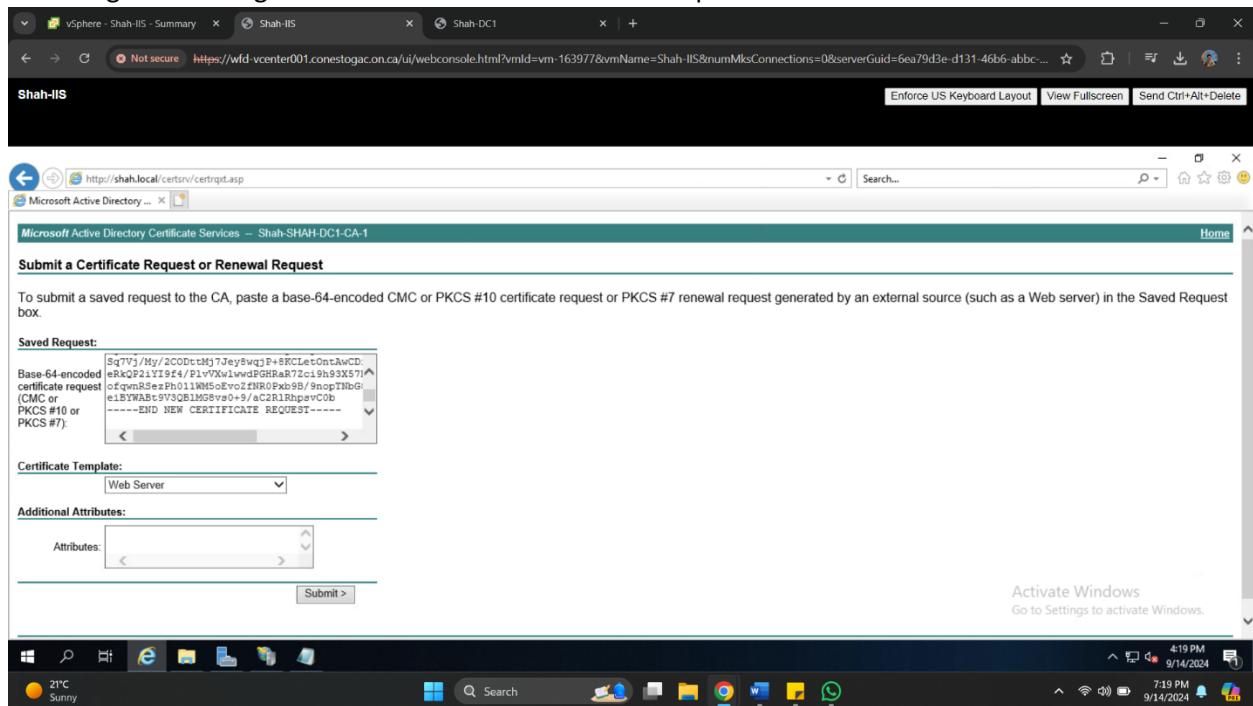
The policy of the CA determines the types of certificates you can request. Click one of the following options to:

[Create and submit a request to this CA.](#)

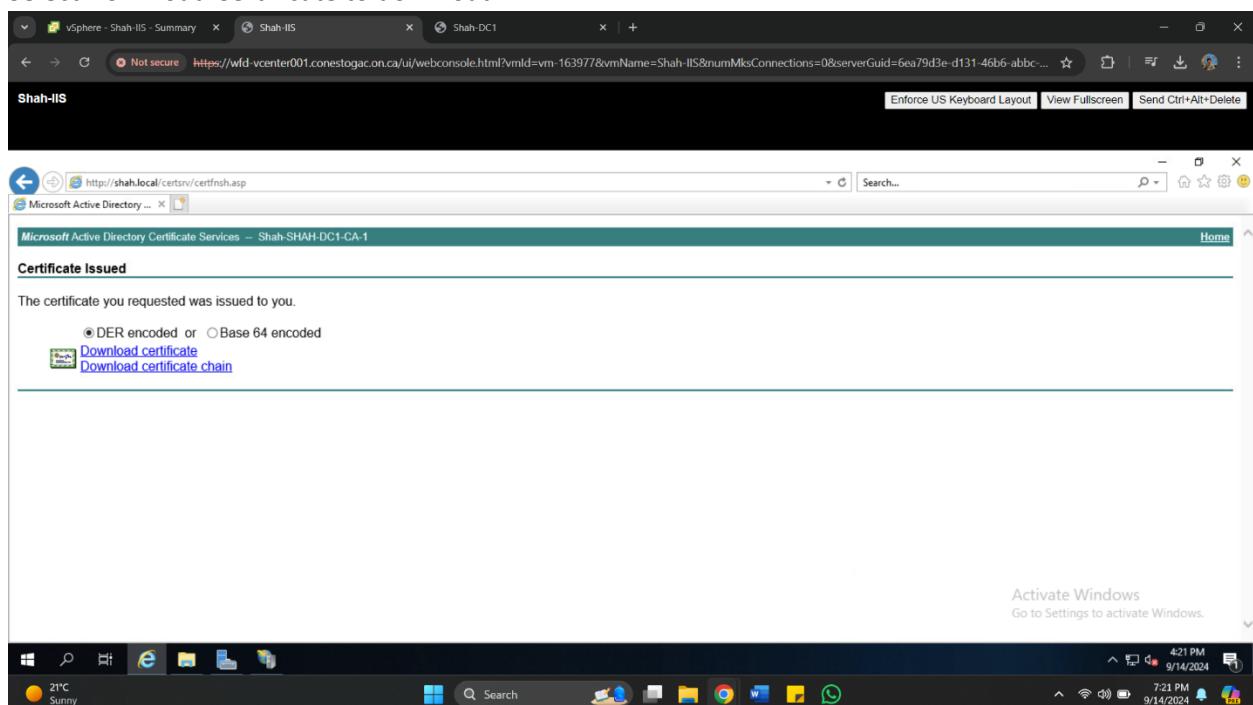
[Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.](#)

Activate Windows
Go to Settings to activate Windows.

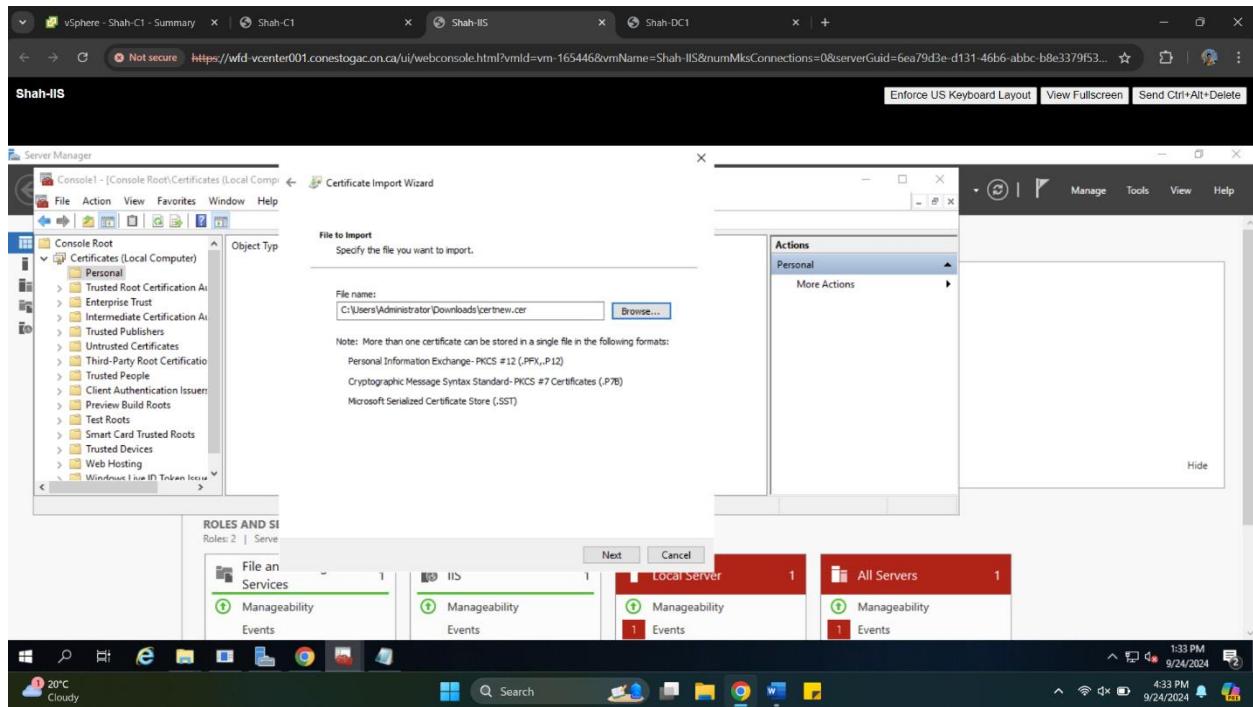
Providing certificate generated before and certificate template as Web Server and submit



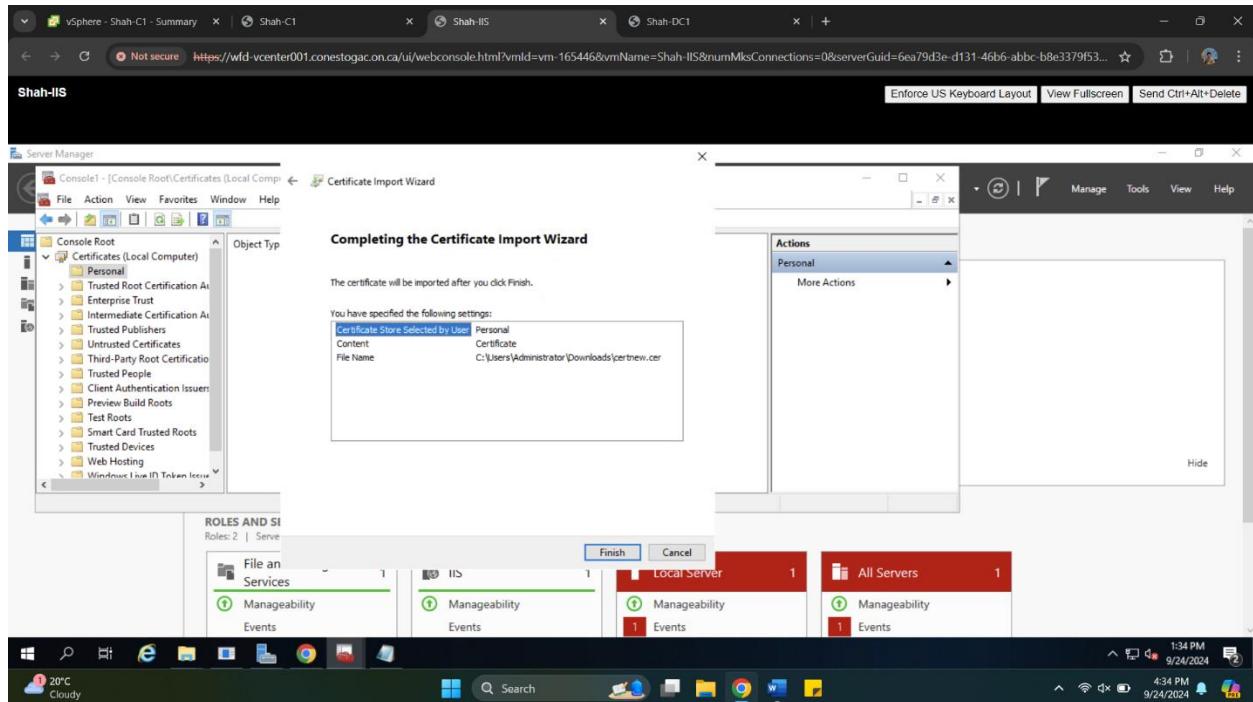
Select Download Certificate to download



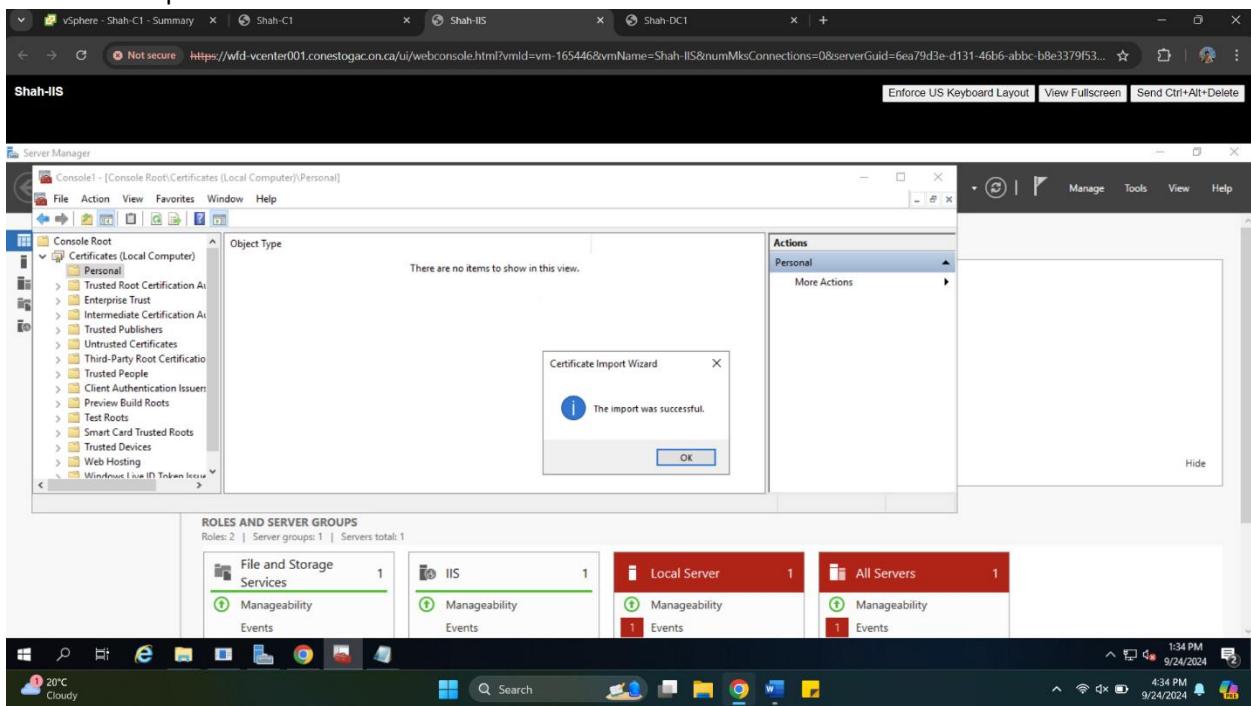
Importing downloaded Certificate and installing to Personal



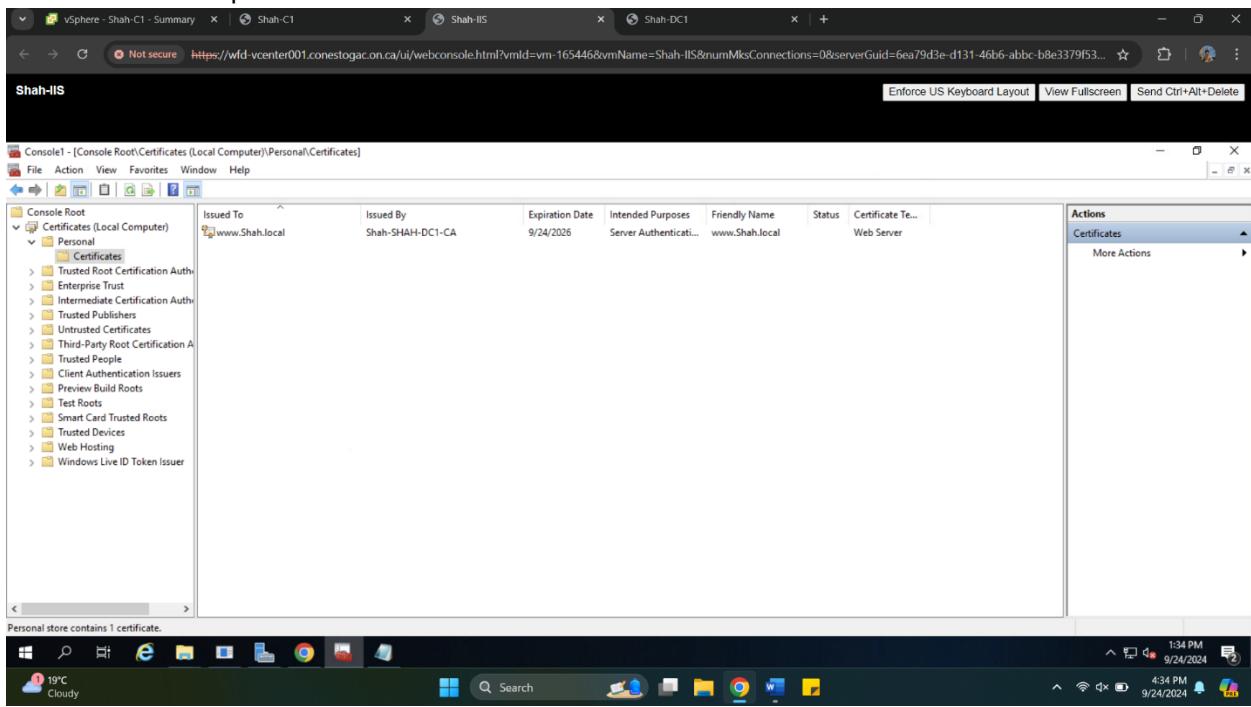
Successfully completing the import of certificate and storing as personal



Successful import of certificate

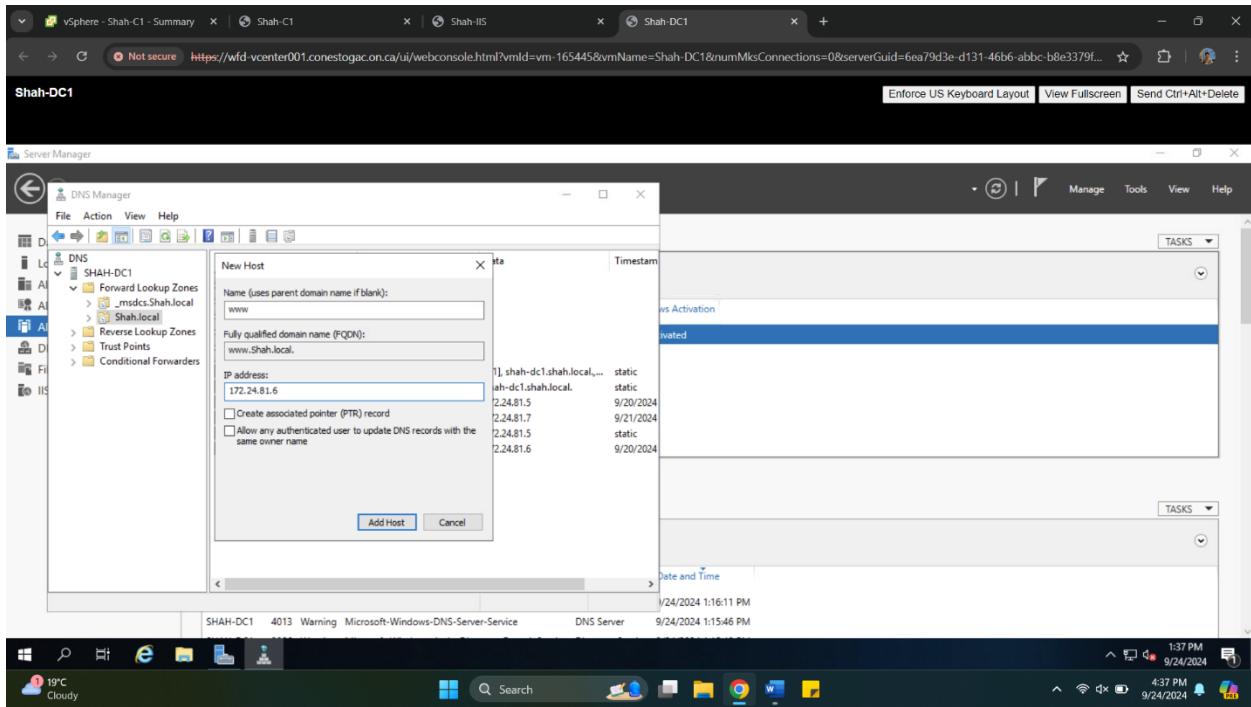


After successful import of certificate we can see the certificate in MMC

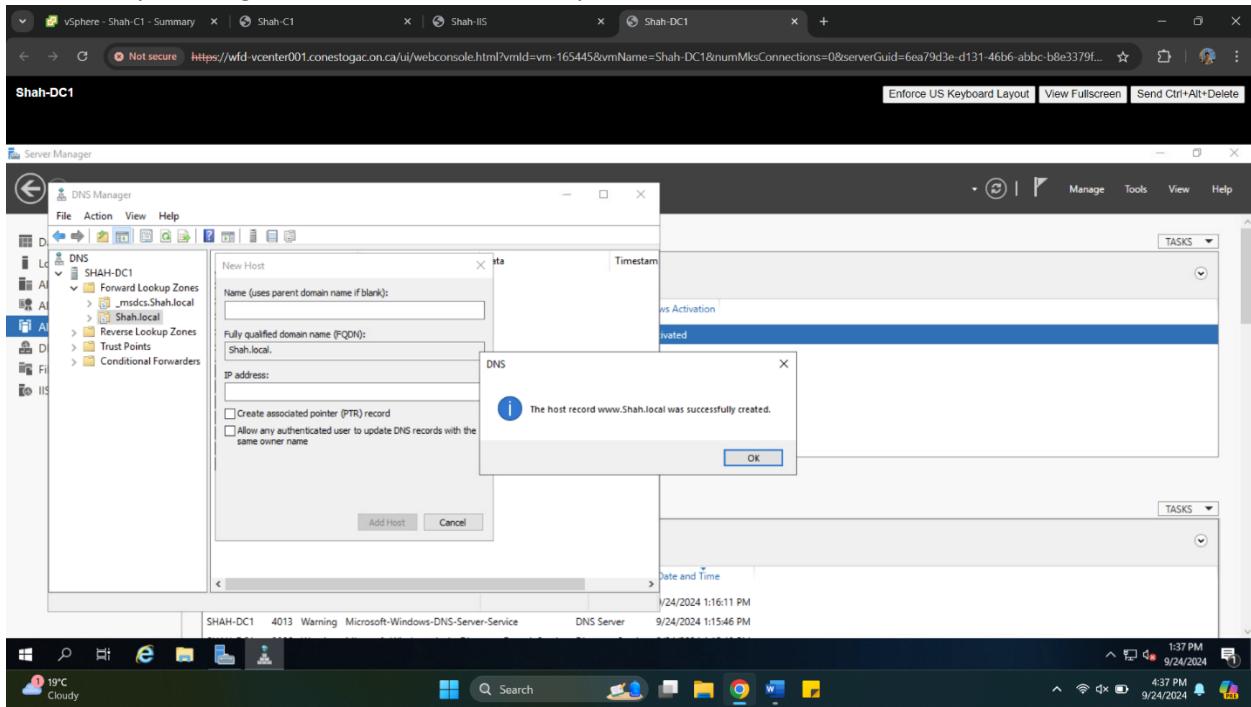


Creating Host record in Forward Lookup Zone (DNS Manager)

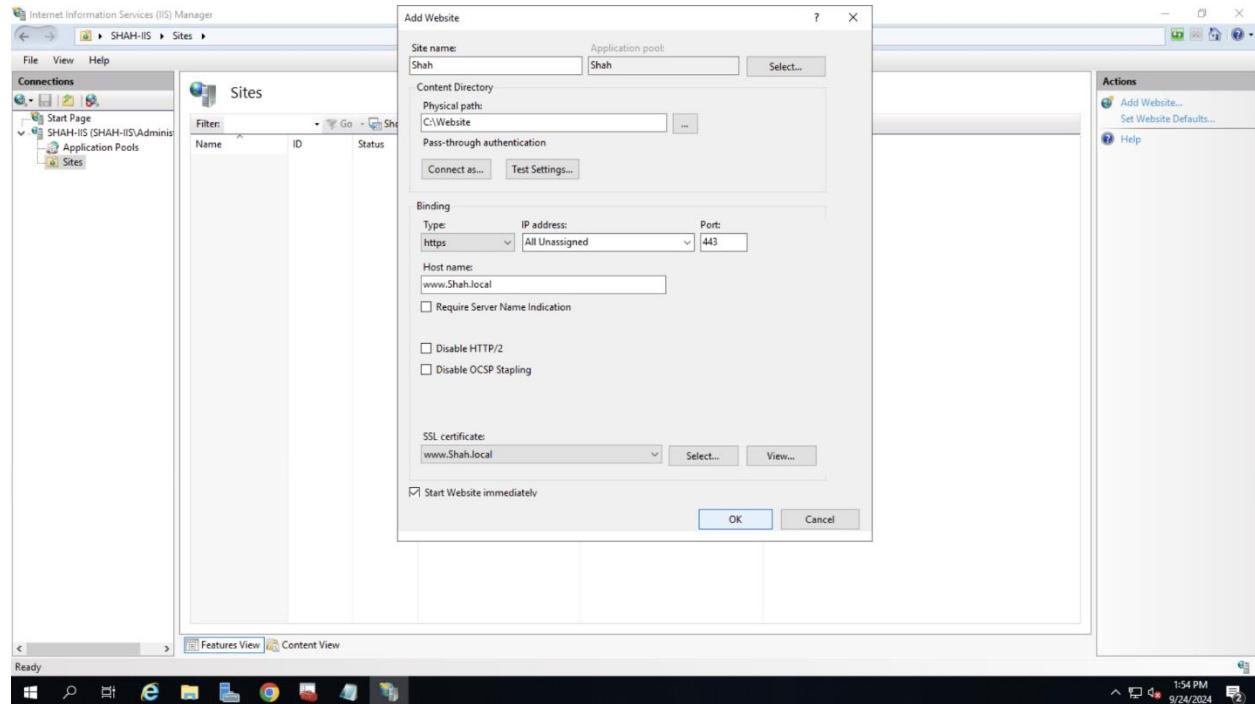
In DNS manager → Shah-DC1 → Forward Lookup Zones → shah.local → creating new host as www IP: 172.24.81.6



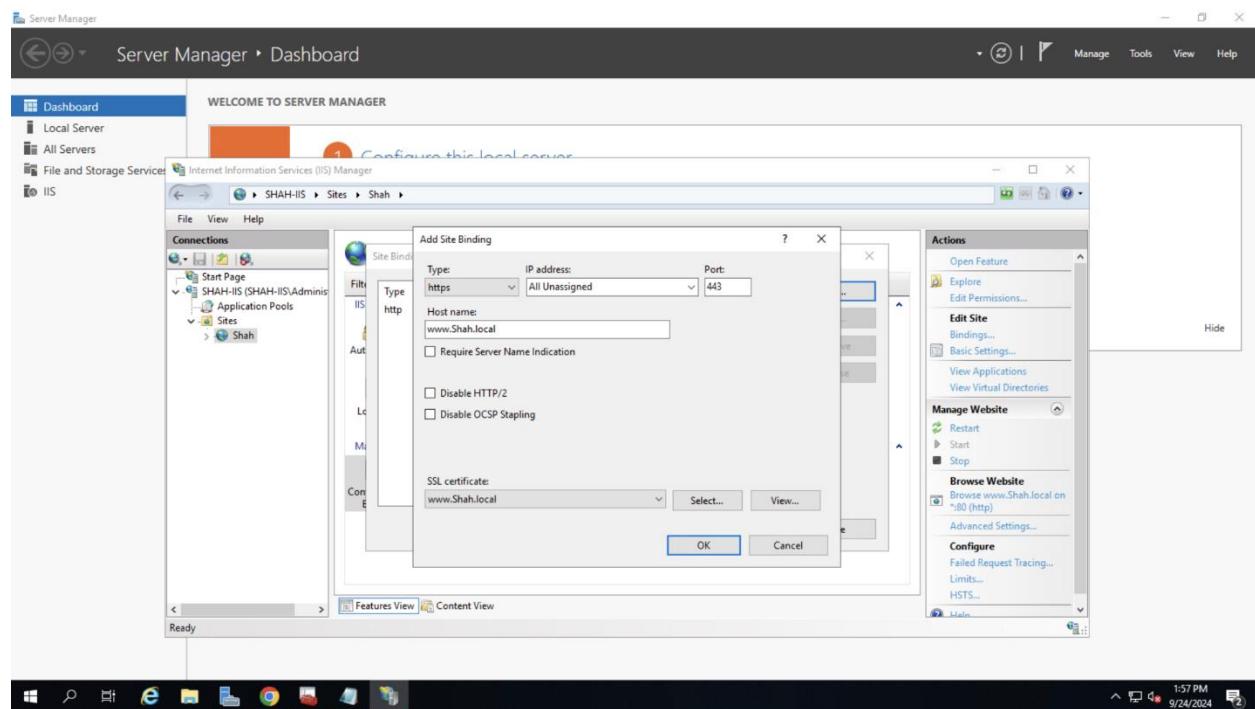
Successfully creating DNS host in Forward lookup



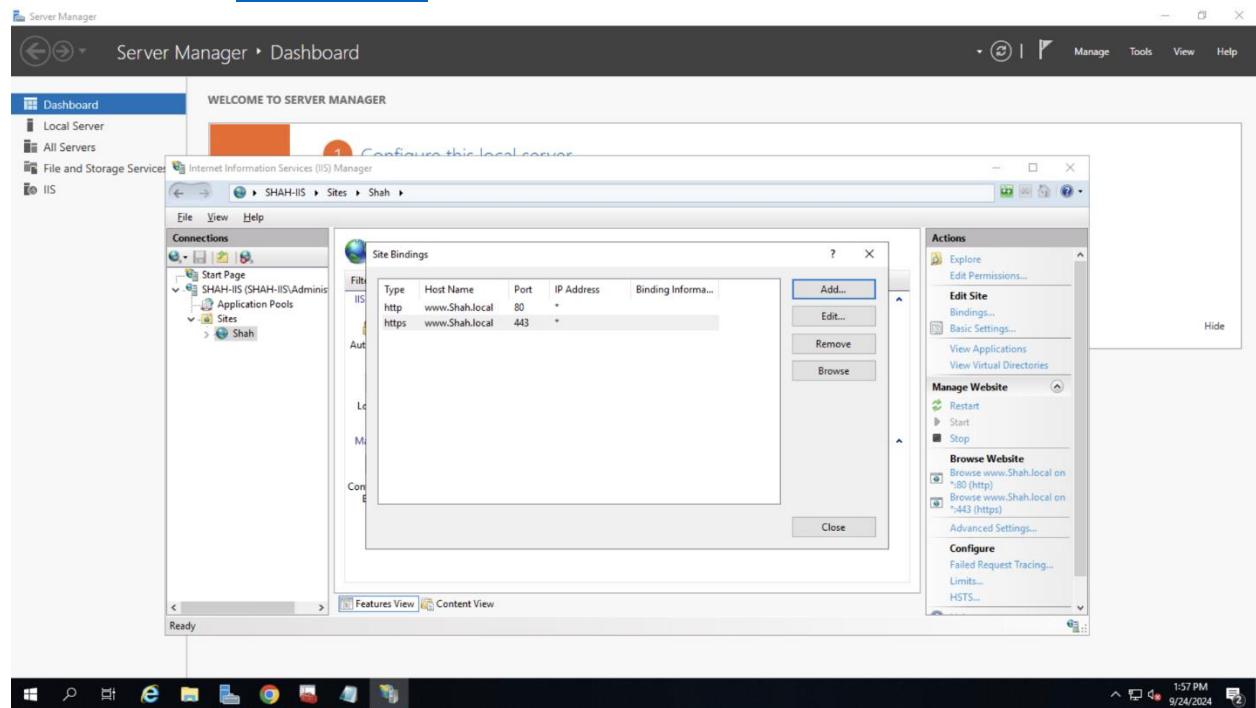
Removing Default Site and creating new site as Shah and giving binding type as https



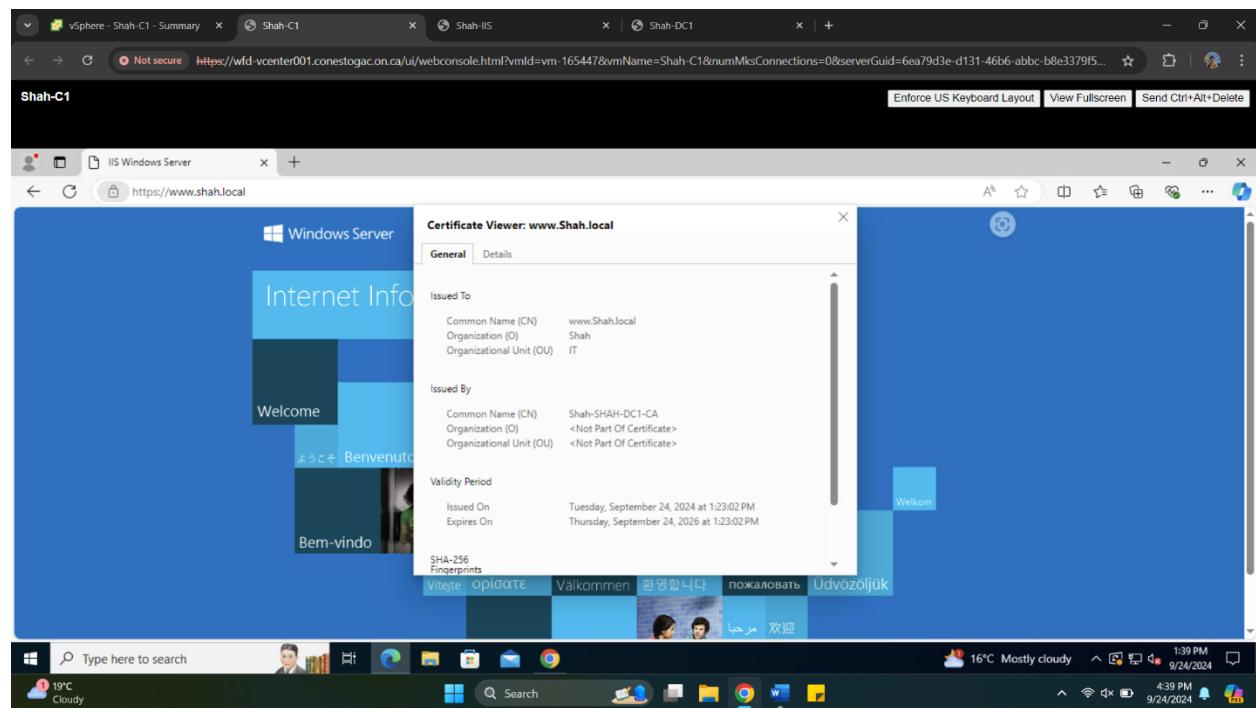
Creating new Site as Shah and binding the site as www.Shah.local with HTTPS, type port 443 and SSL certificate as www.Shah.local



Site is binded with www.Shah.local with HTTP and HTTPS



Test the website with your client's machine. The certificate MUST show trusted from the client.



Testing custom made website.

