

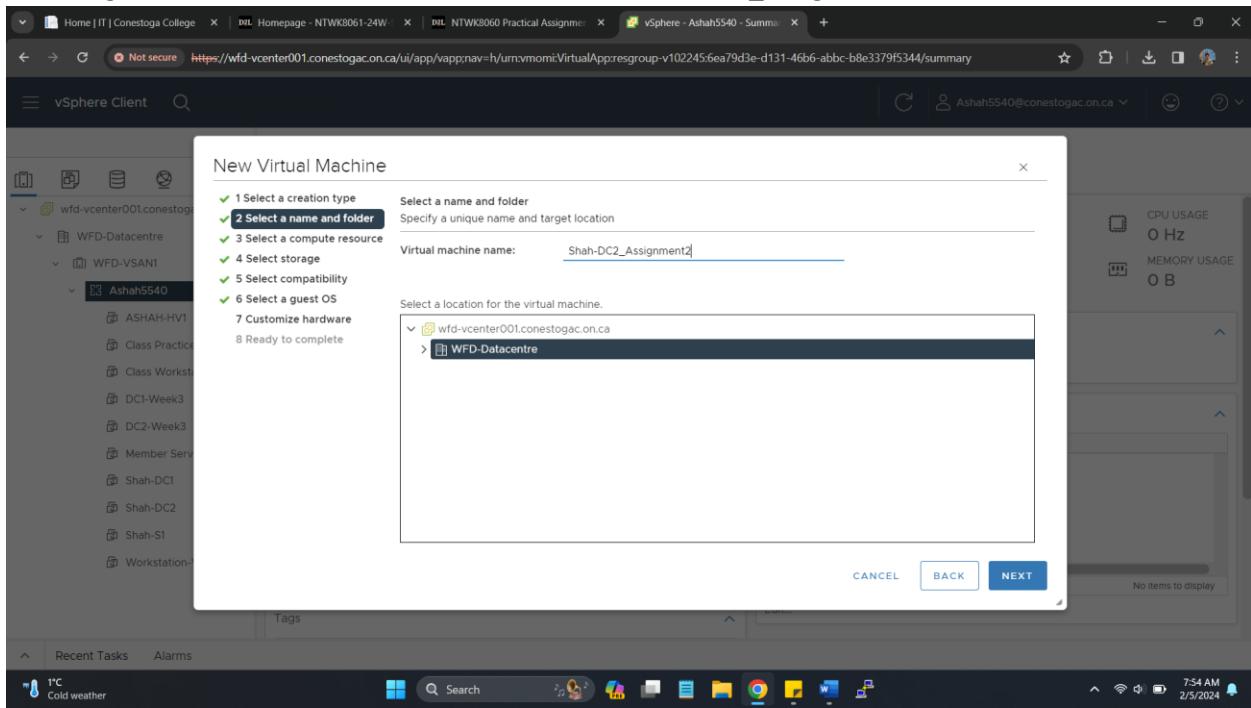
Table of Contents

1)	Create an AD domain with the domain name yourlastnamea2.local with the below specifications...	2
2)	Create a Global Security Group named IT and add a user to it	27
3)	Create a file share on the member server called “IT Files”	32
4)	Create a text file in the share called log.txt	33
5)	Set the share permissions on the share to Everyone Full Control.....	34
6)	Set the NTFS permissions to allow only the IT group to access the share.....	34
7)	Create a forward lookup zone named acme.local	36
8)	Create a reverse lookup zone for your com port IP range.....	39
9)	Install and configure the DHCP Role with the below scope.....	44
10)	Set the Windows Workstation to DHCP and show it receiving an IP address from your DHCP Server	54

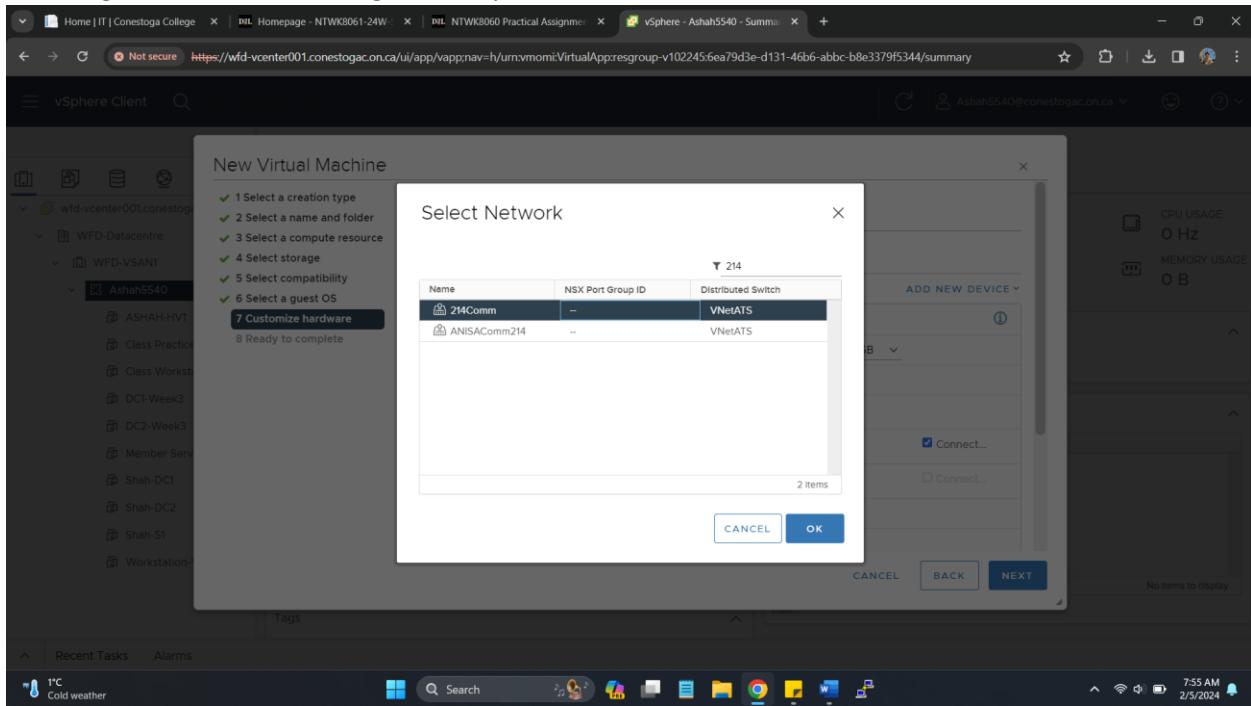
- 1) Create an AD domain with the domain name yourlastnamea2.local with the below specifications.

- 1x Domain Controller → Shah-DC_Assignment2
- 1x Member Server → Shah-Member Server-Assigned2
- 1x Windows Workstation → Shah-Workstation-Assigned2

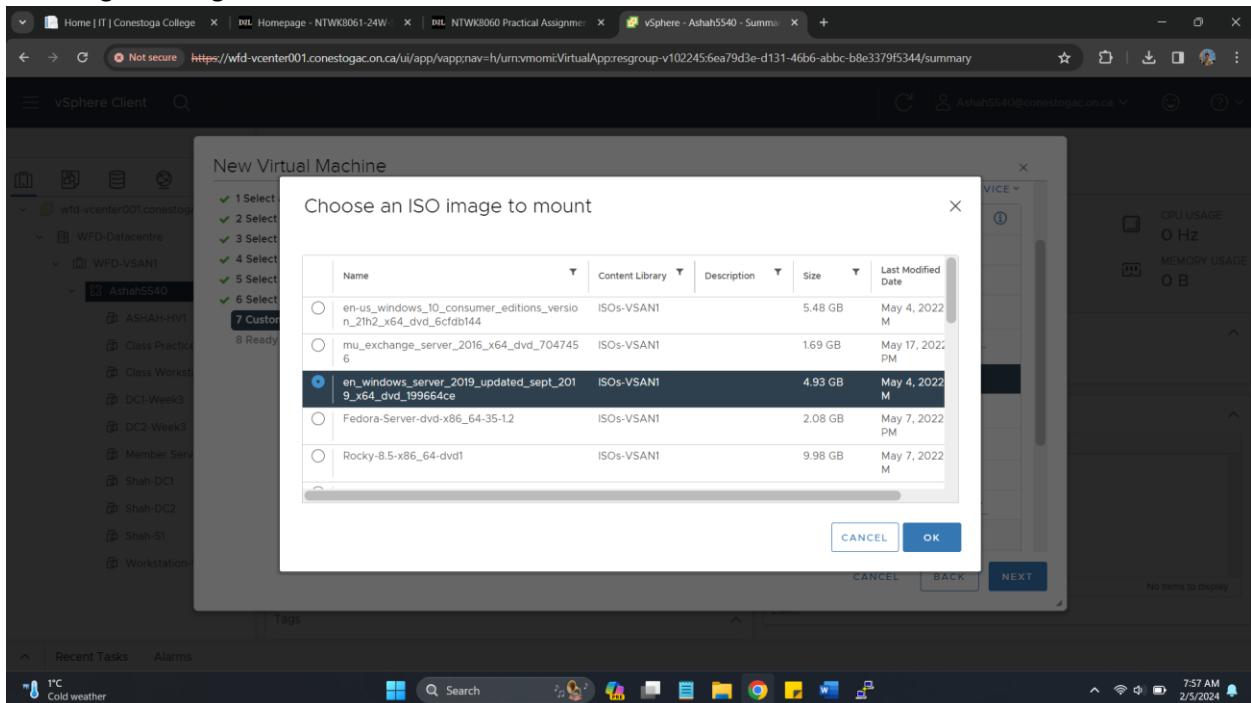
Providing Domain Controller virtual machine name as Shah-DC_Assignment2



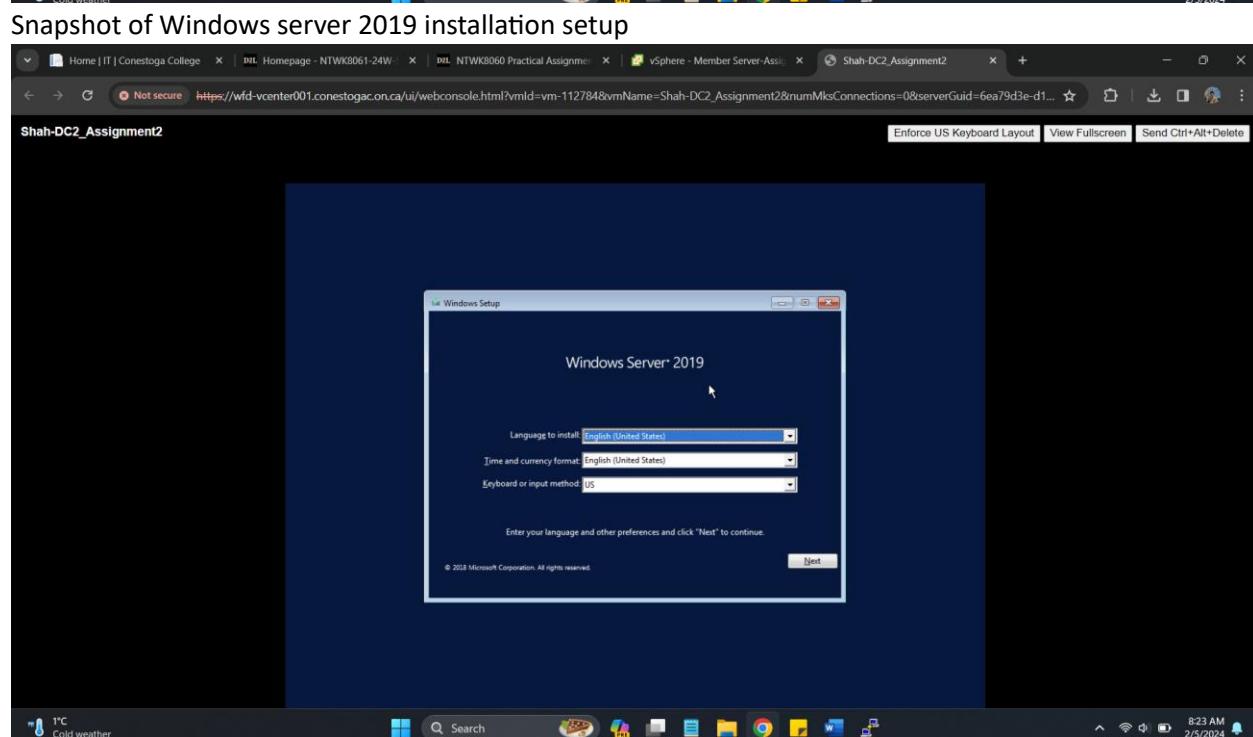
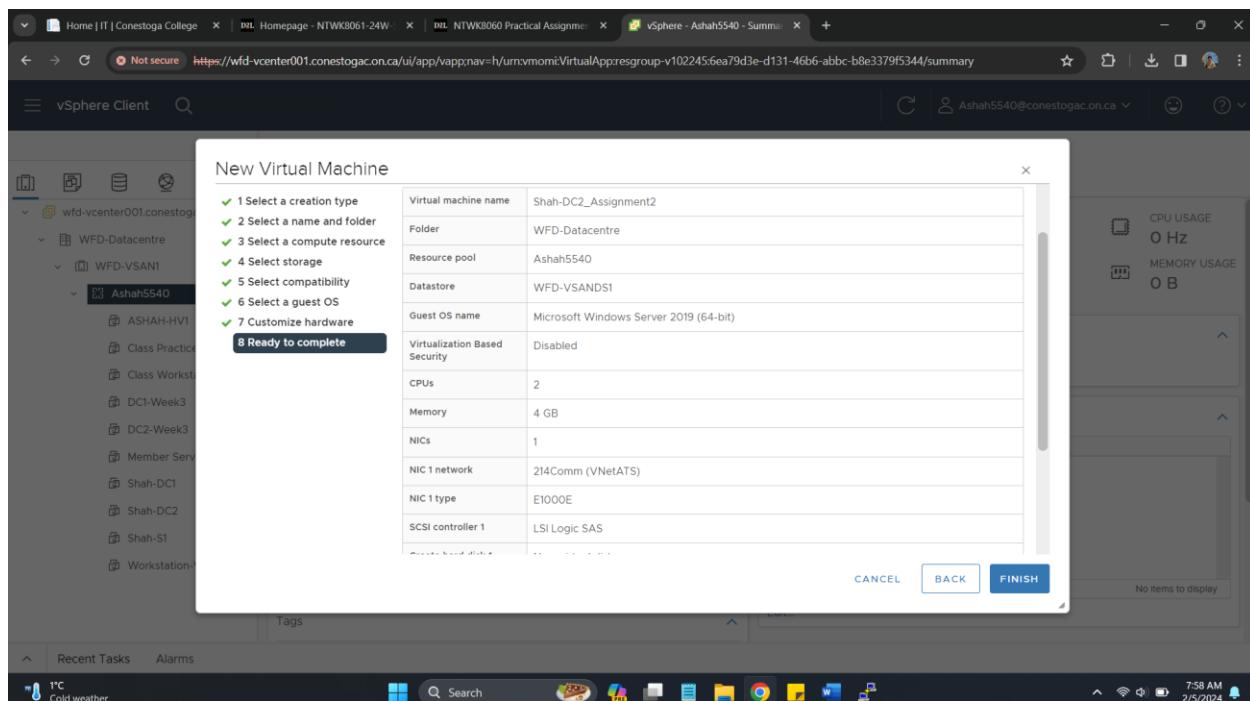
Selecting COM Port 214 as assigned to my student ID Ashah5540



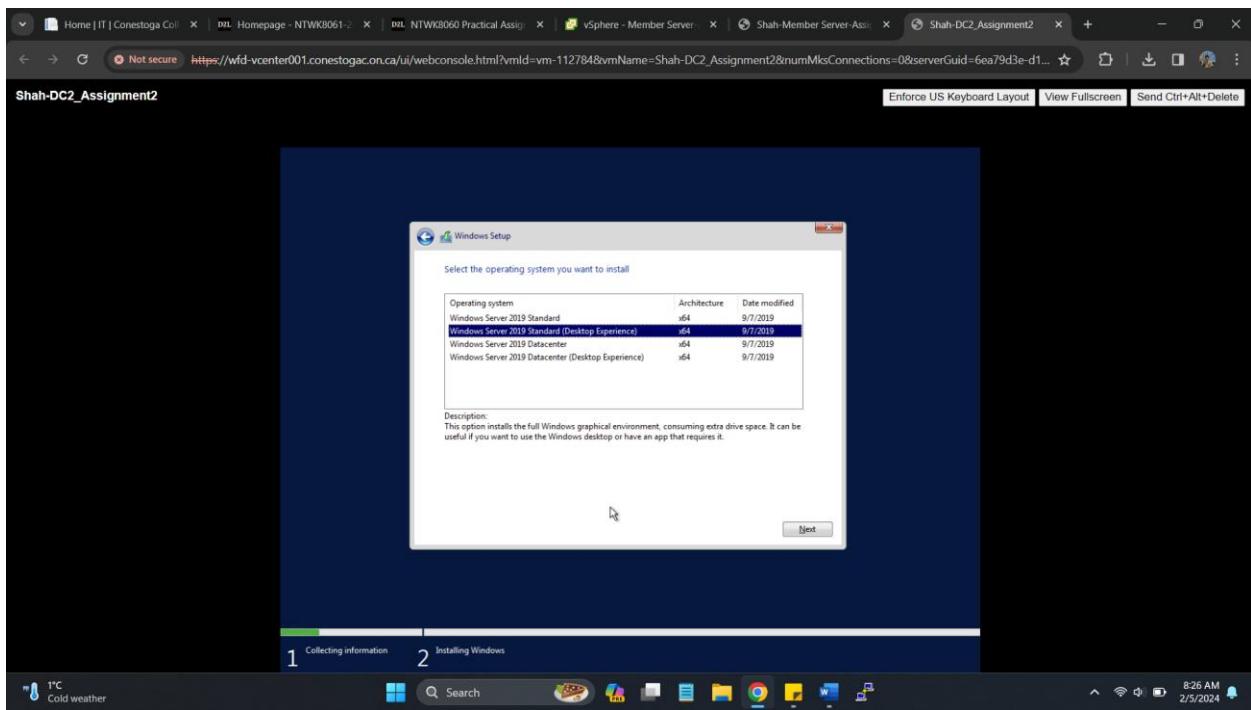
Selecting ISO image Windows server 2019 to mount



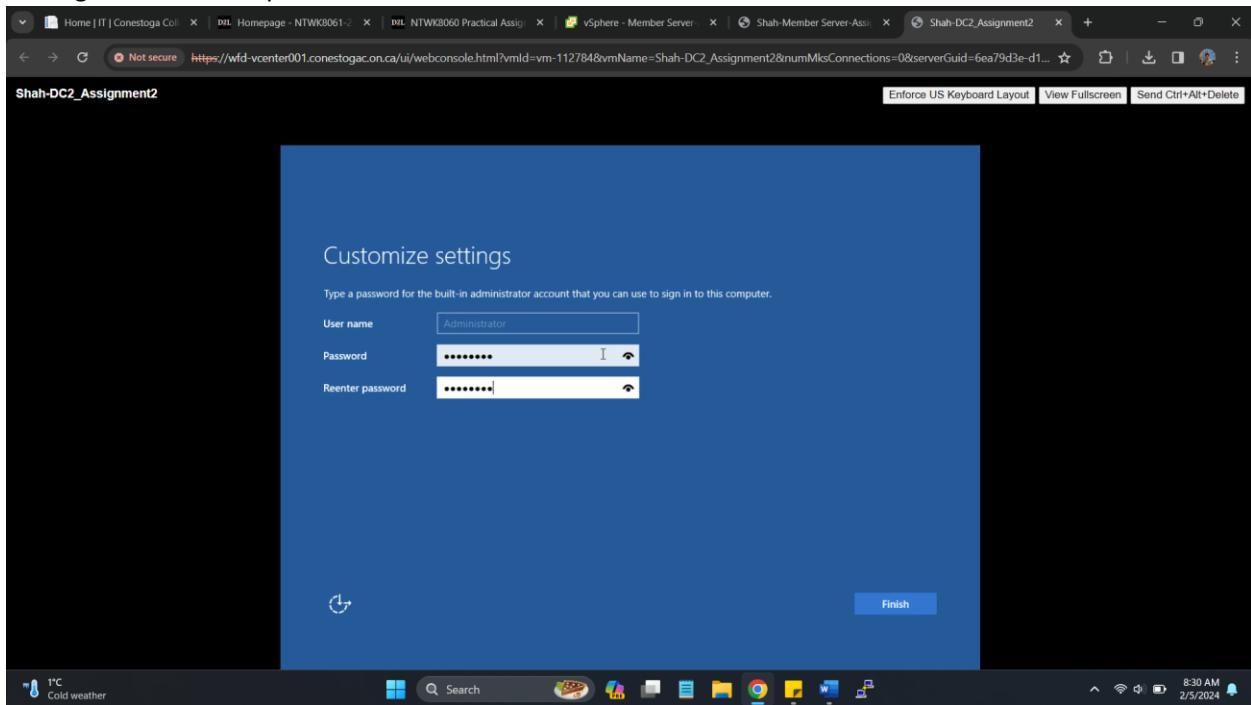
Summary of VM creation for Domain Controller.



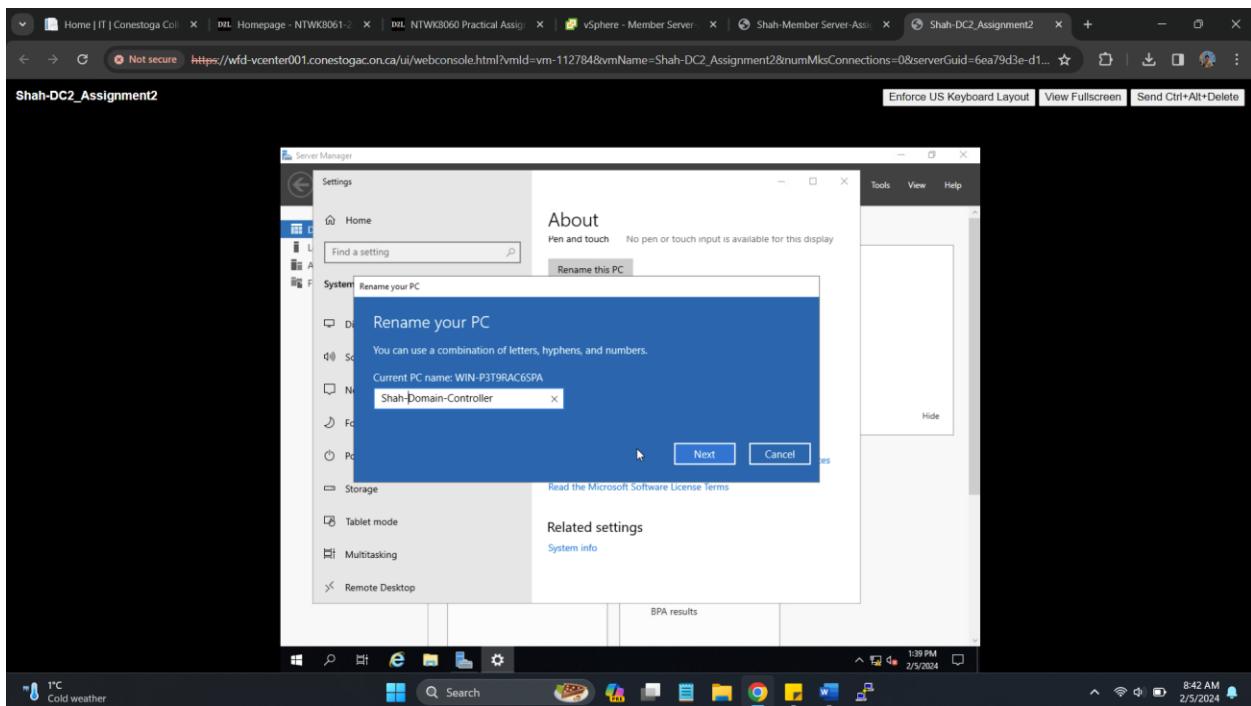
Selecting Windows Server 2019 Standard Desktop Experience version for installation



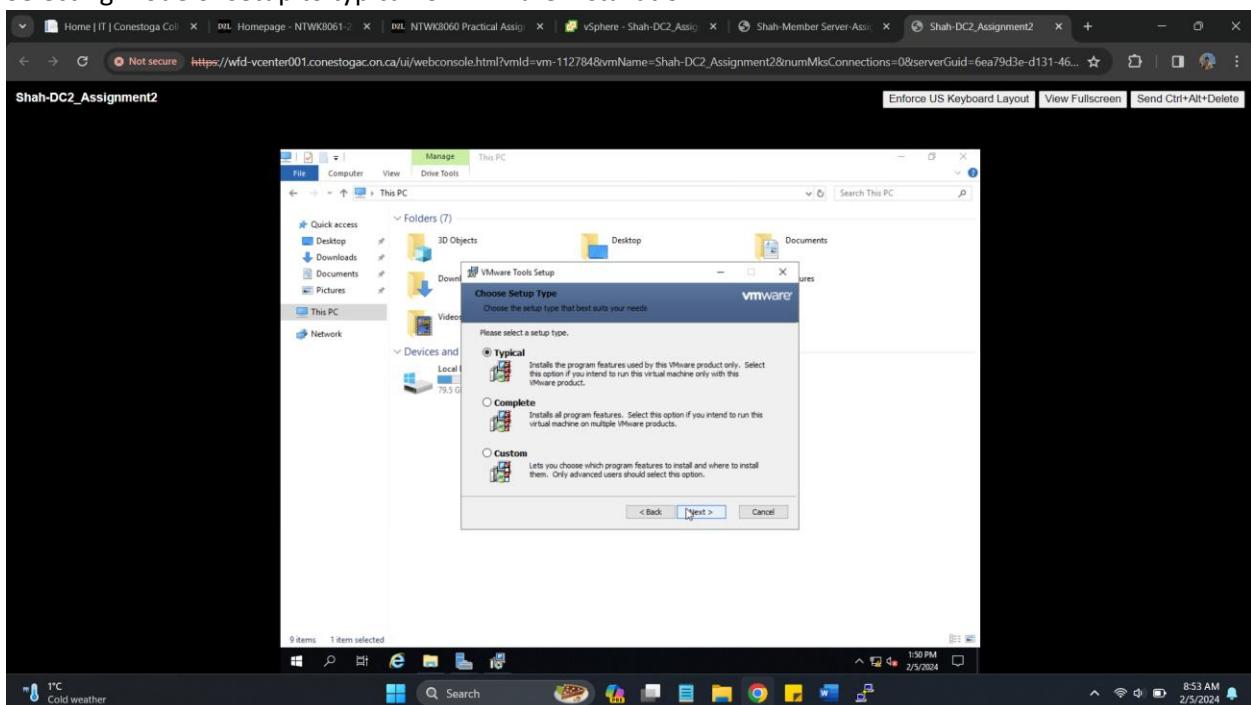
Setting Administrator password for 1st time



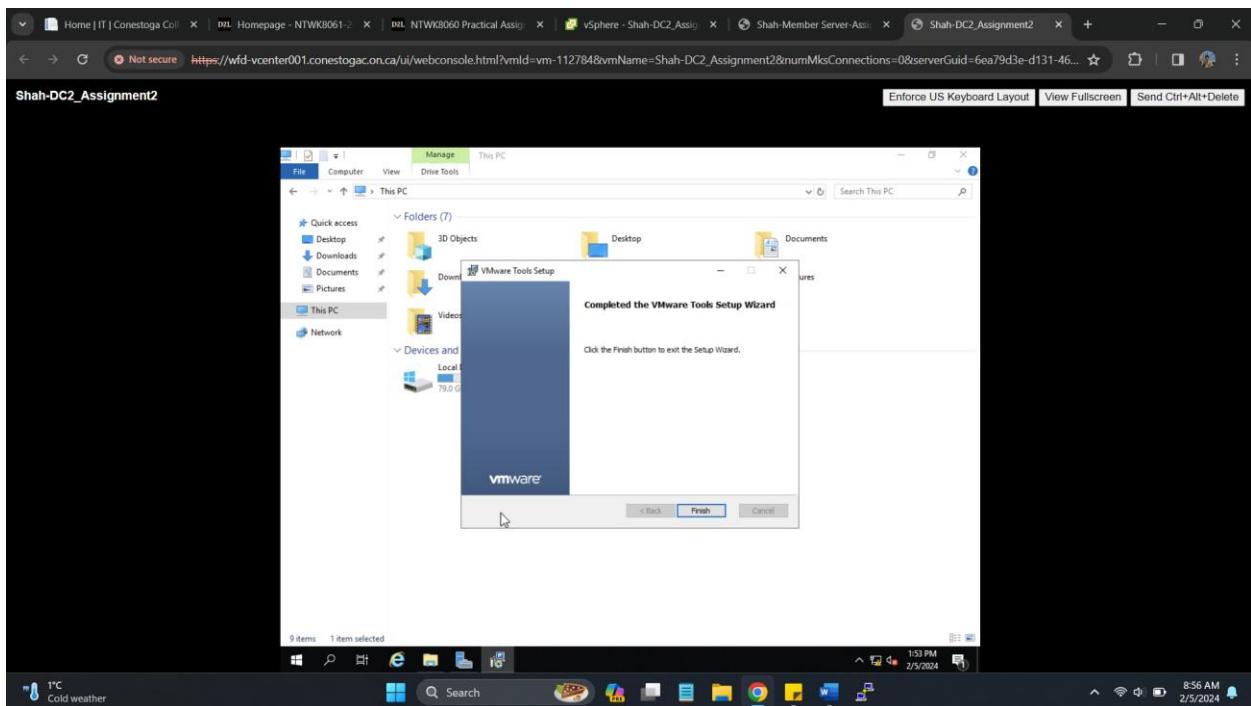
Changing server Domain Controller Name to Shah-Domain-Controller



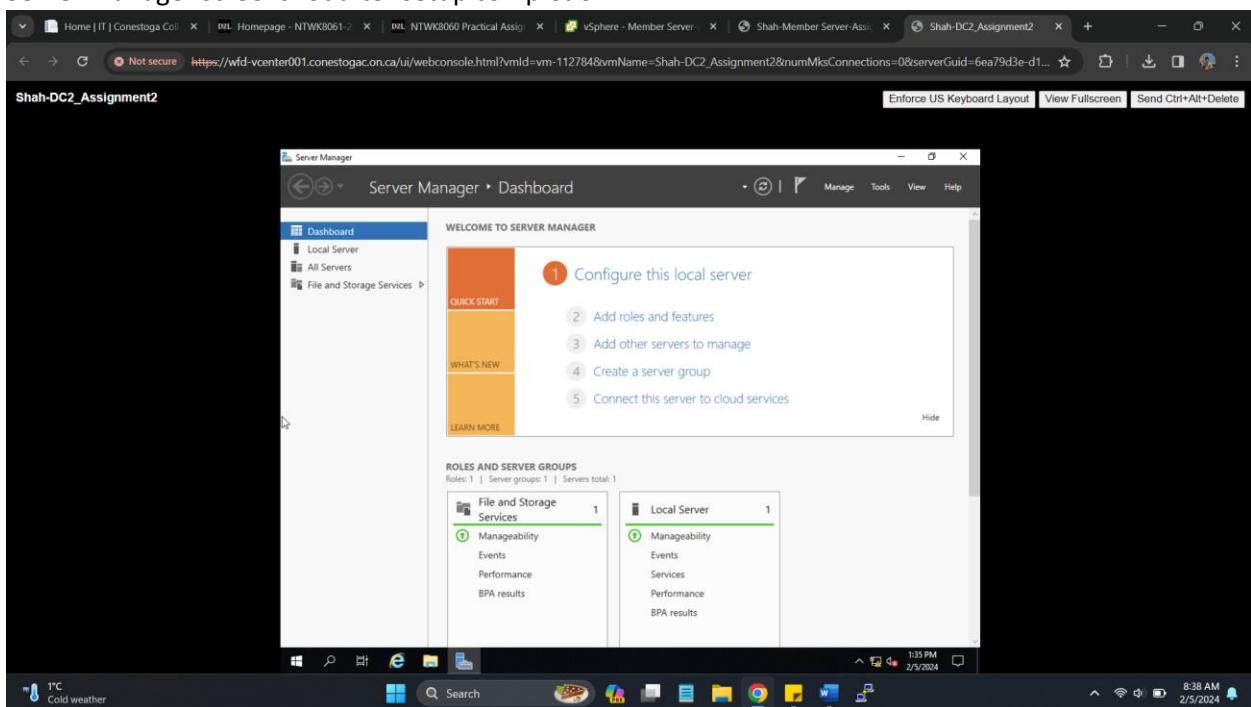
Selecting mode of setup to typical for VMware installation



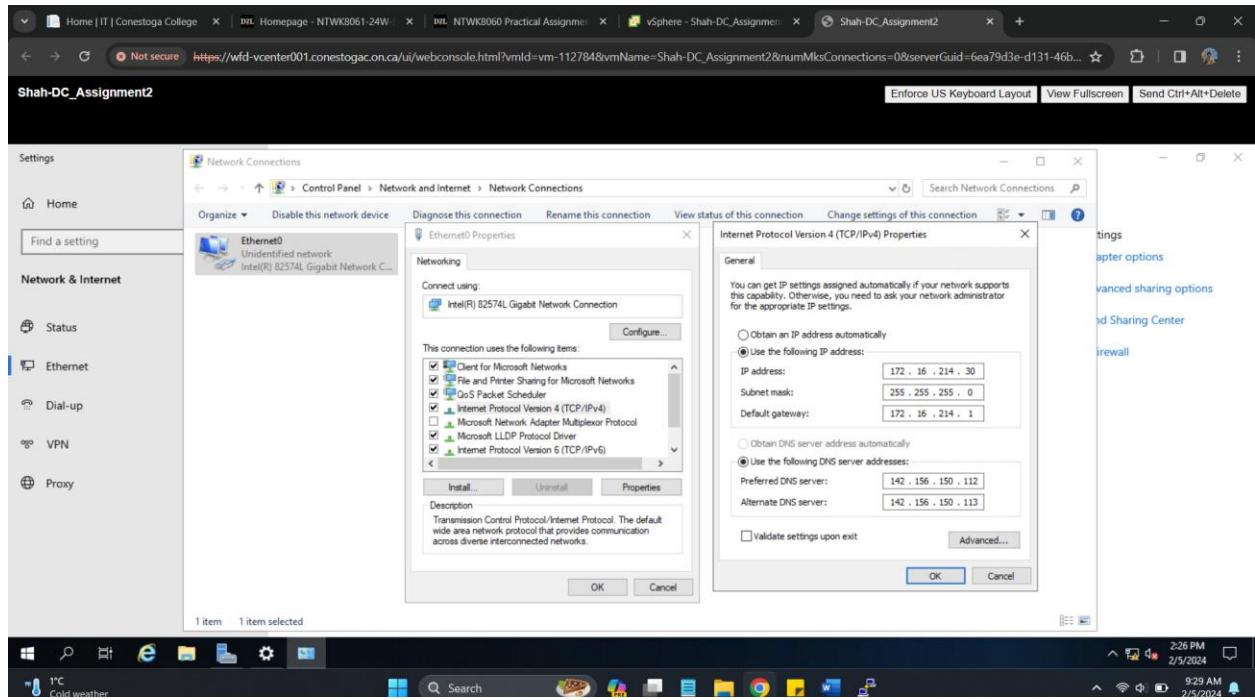
Completion of VMware tools installation



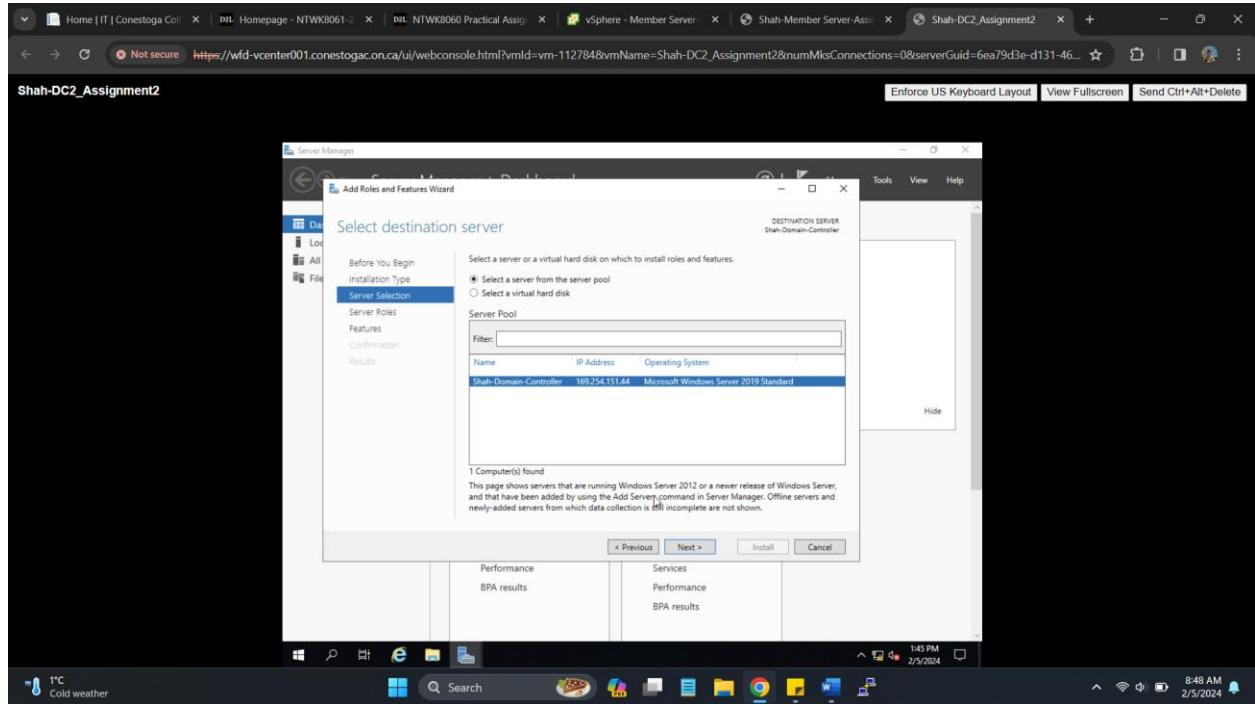
Server manager screenshot after setup completion.



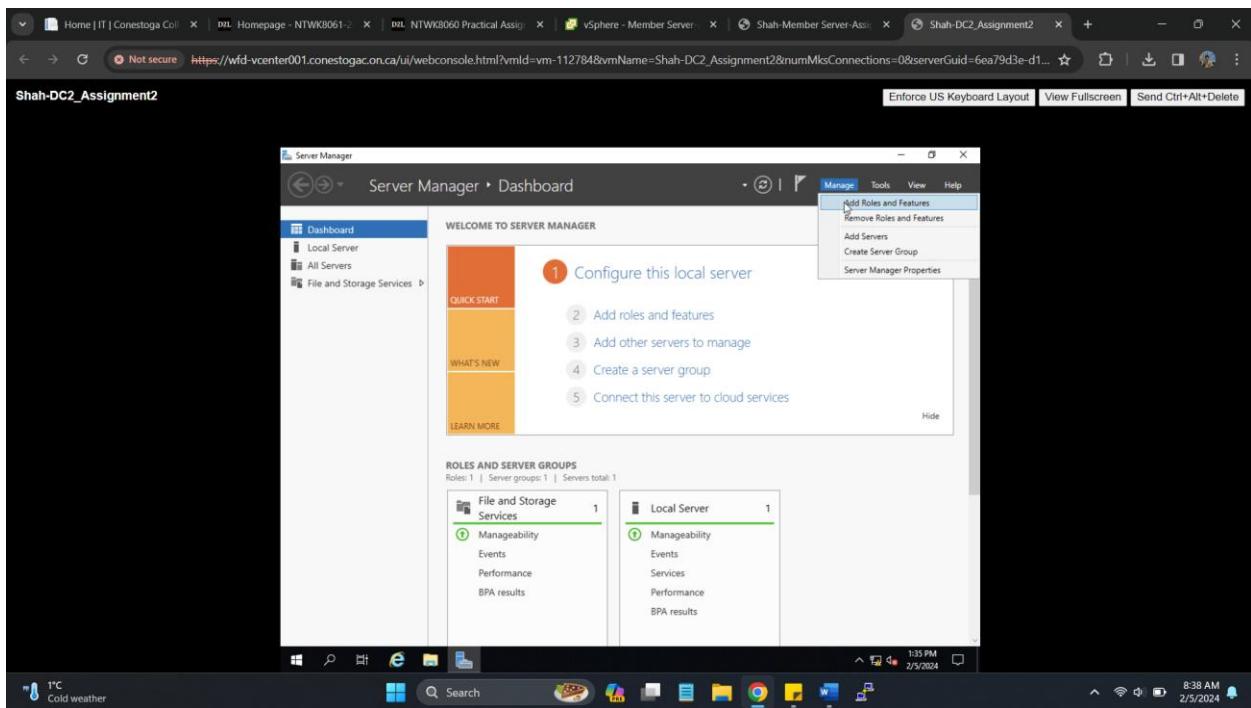
Setting IP details for Domain controller as 172.16.214.30 with subnet mask and DNS server Ip's



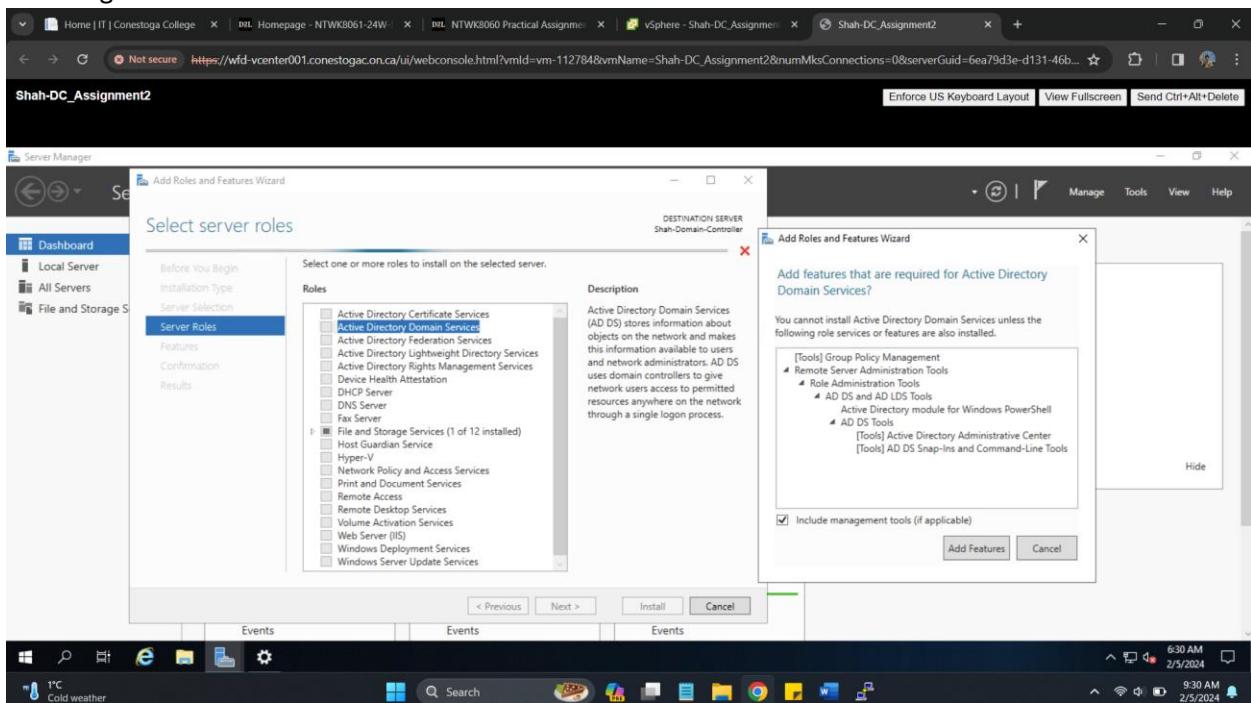
Selecting Destination server from the server pool



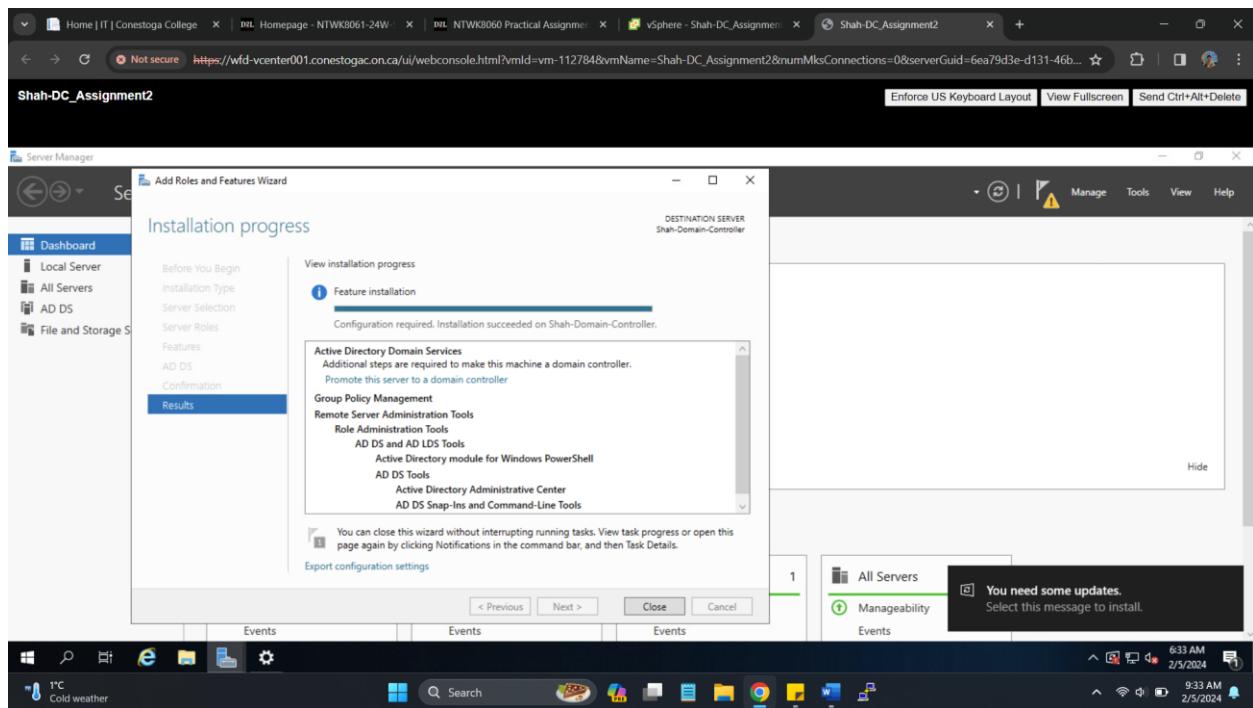
Adding roles and features to Domain controller server for Active Directory Domain Services



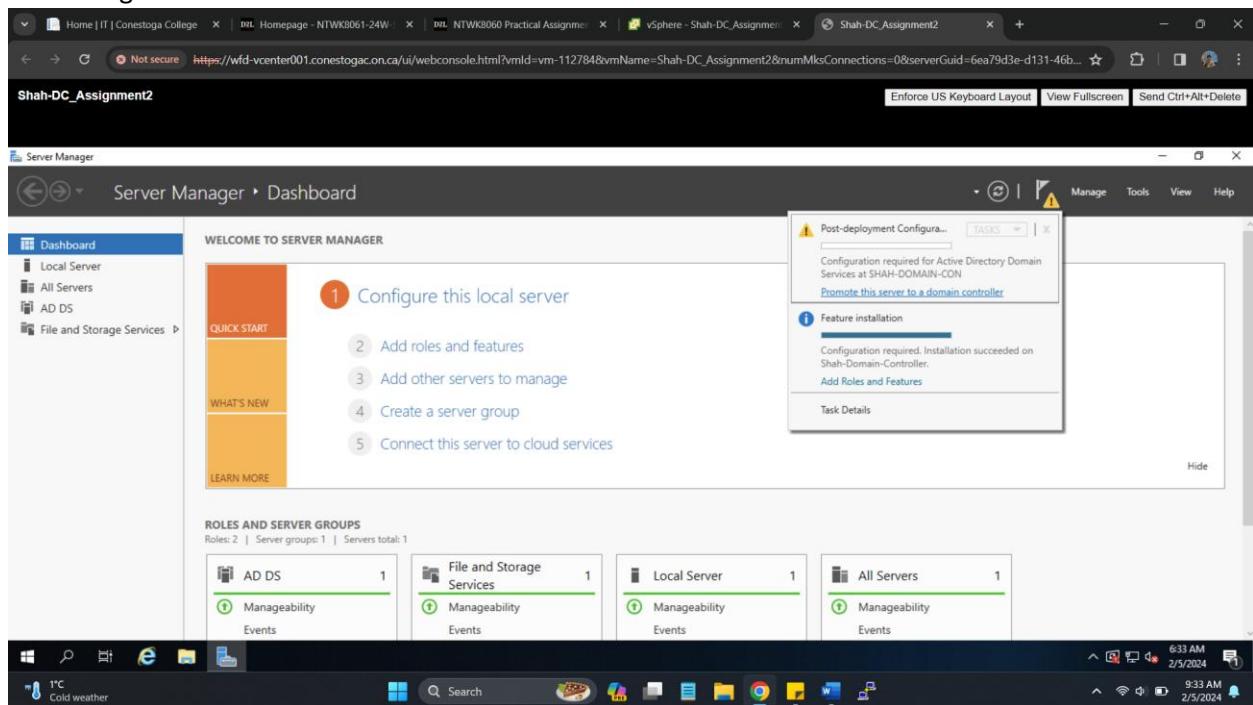
Selecting features to be added in the server



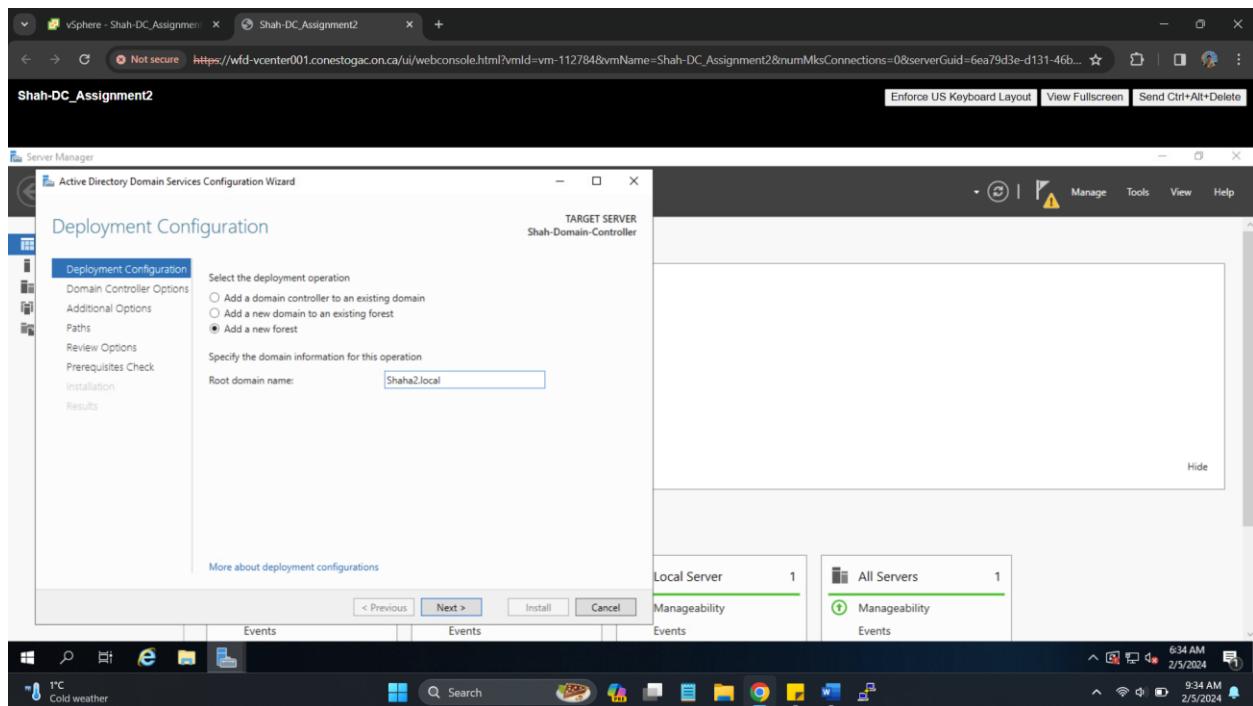
Feature installation summary of ADDS



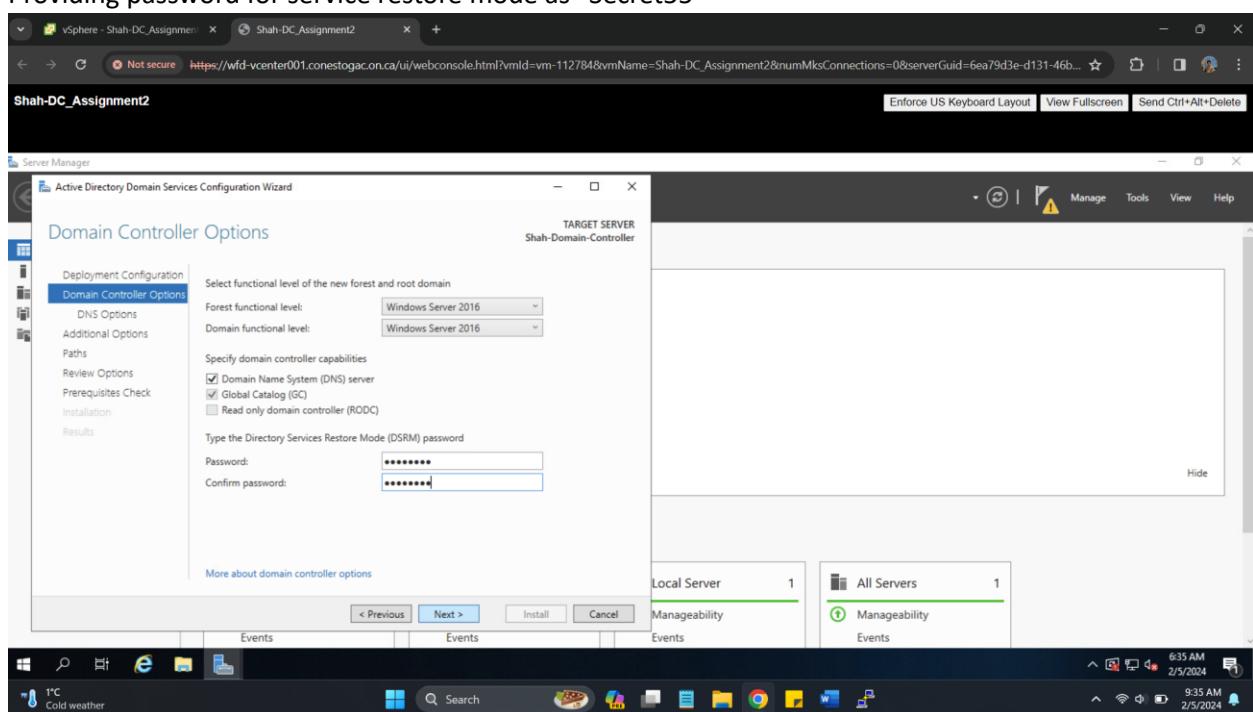
Promoting Server to Domain Controller



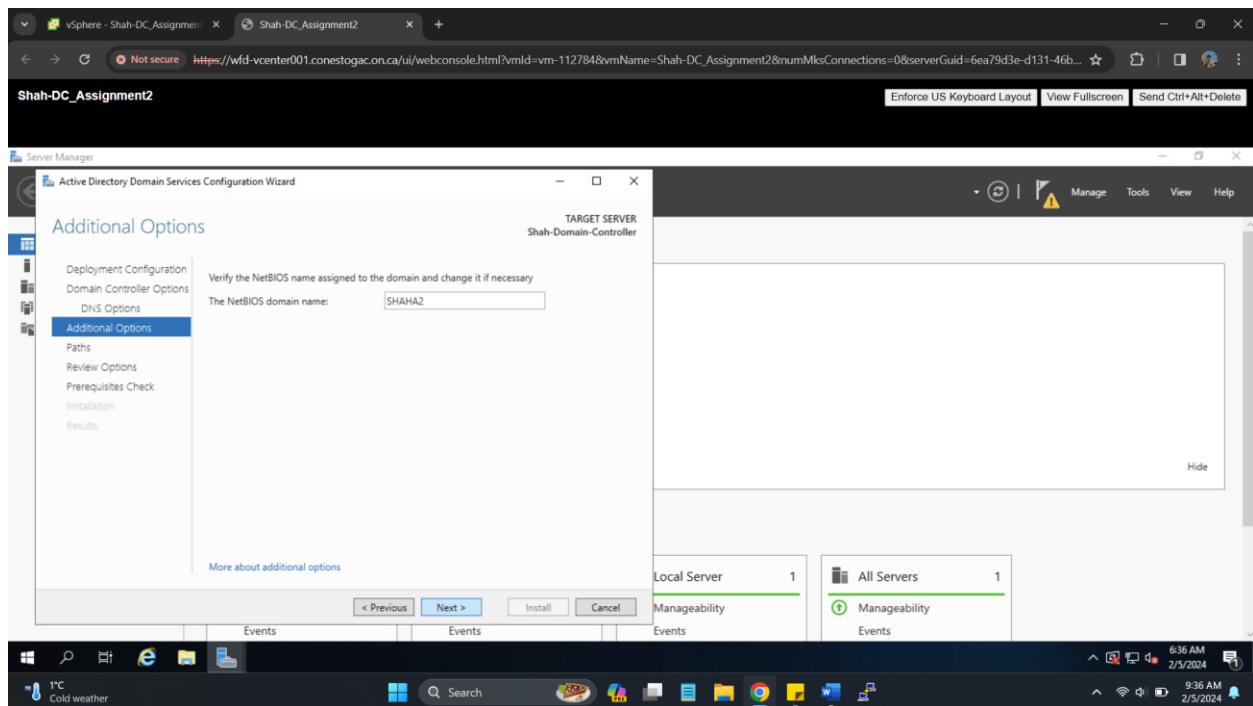
Creation of new Forest as it is for first time, Root domain name as "Shaha2.local"



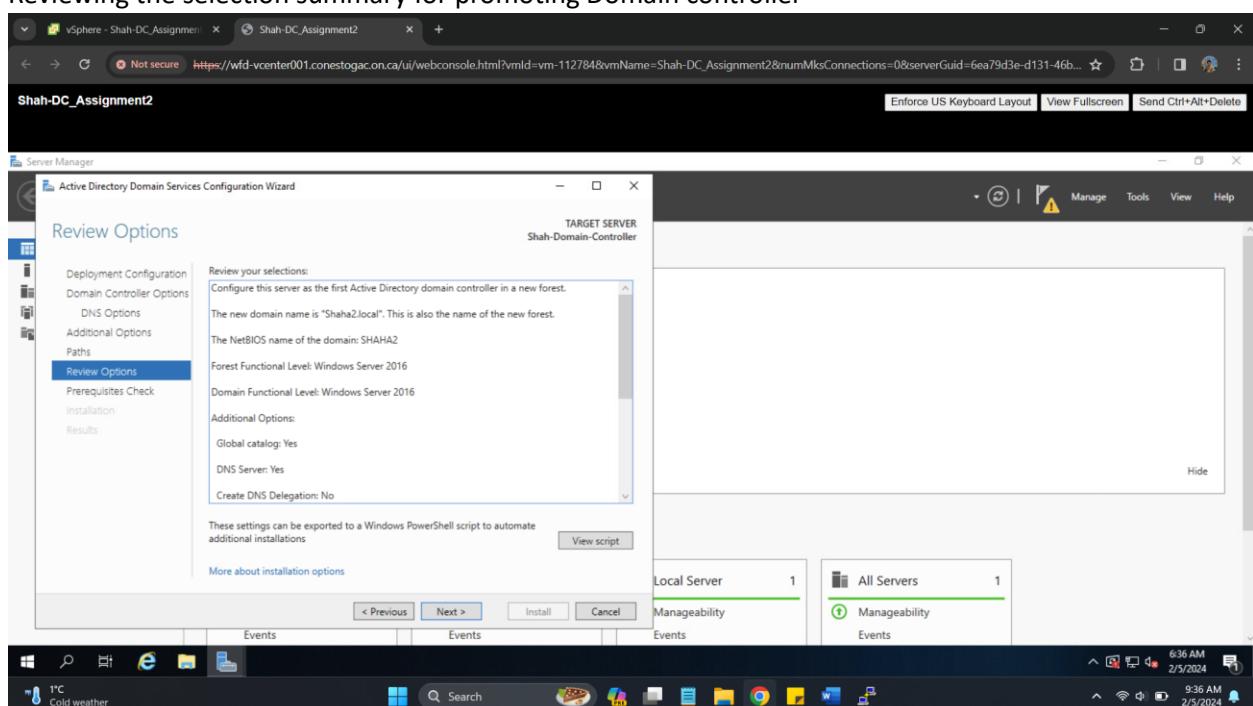
Providing password for service restore mode as "Secret55"



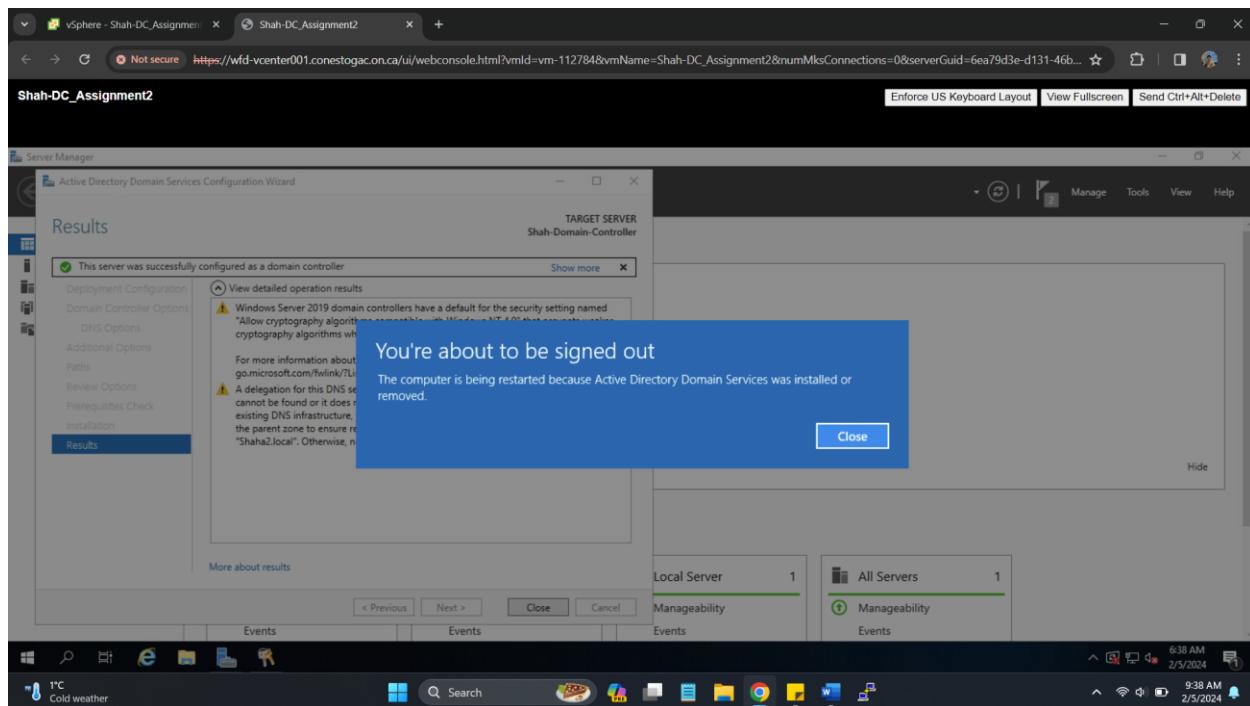
Setting the NetBIOS domain name as SHAHA2



Reviewing the selection summary for promoting Domain controller



Server successfully promoted to Domain Controller and further server needs to be restarted



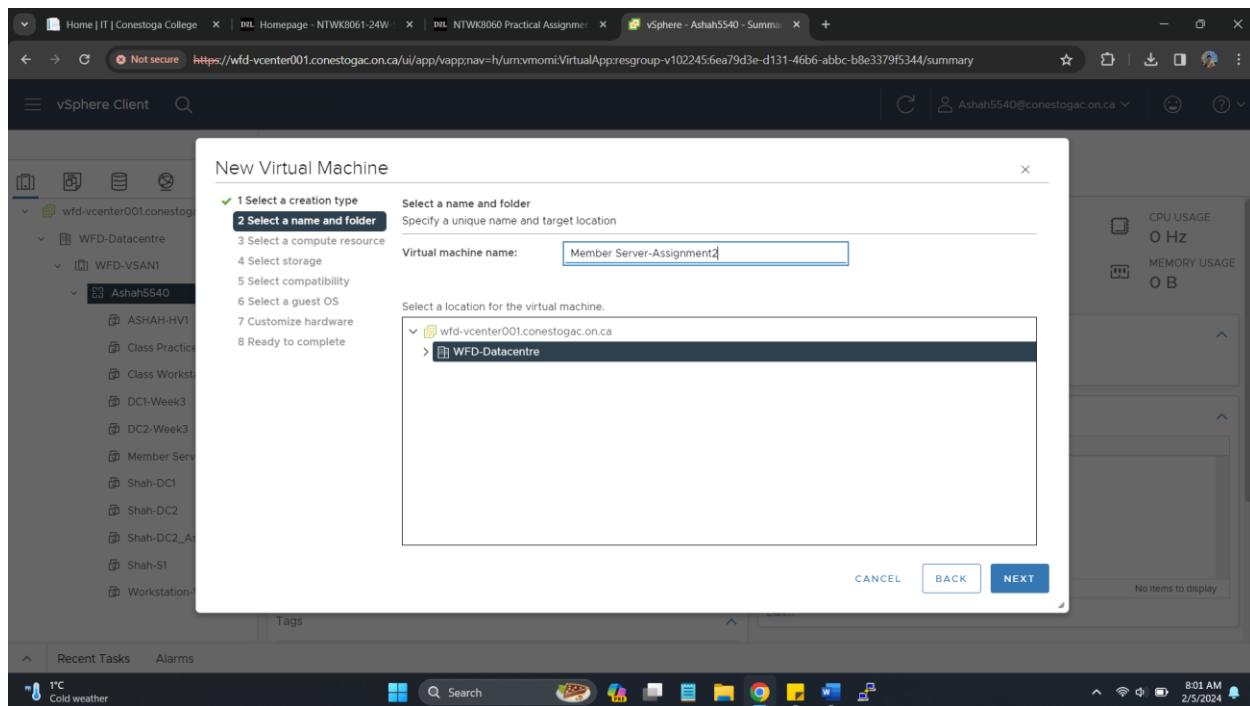
Summary of local server with domain name and summary

PROPERTIES
For Shah-Domain-Controller

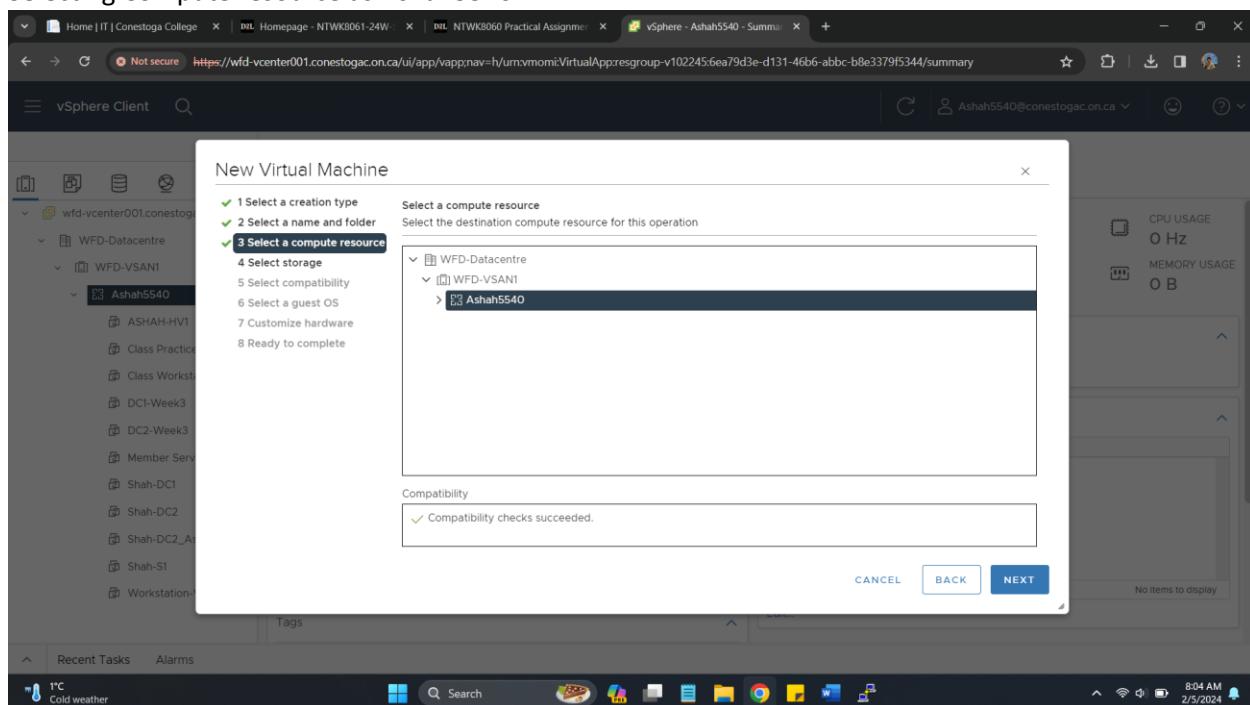
Computer name	Shah-Domain-Controller	Last installed updates	Never
Domain	Shaha2.local	Windows Update	Download updates only, using Windows Update
		Last checked for updates	Today at 6:32 AM
Windows Defender Firewall	Private: On	Windows Defender Antivirus	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
Ethernet0	172.16.214.30, IPv6 enabled	Product ID	Not activated
Operating system version	Microsoft Windows Server 2019 Standard	Processors	Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.30GHz
Hardware information	VMware, Inc. VMware7.1	Installed memory (RAM)	4 GB
		Total disk space	89.4 GB

EVENTS
All events | 41 total

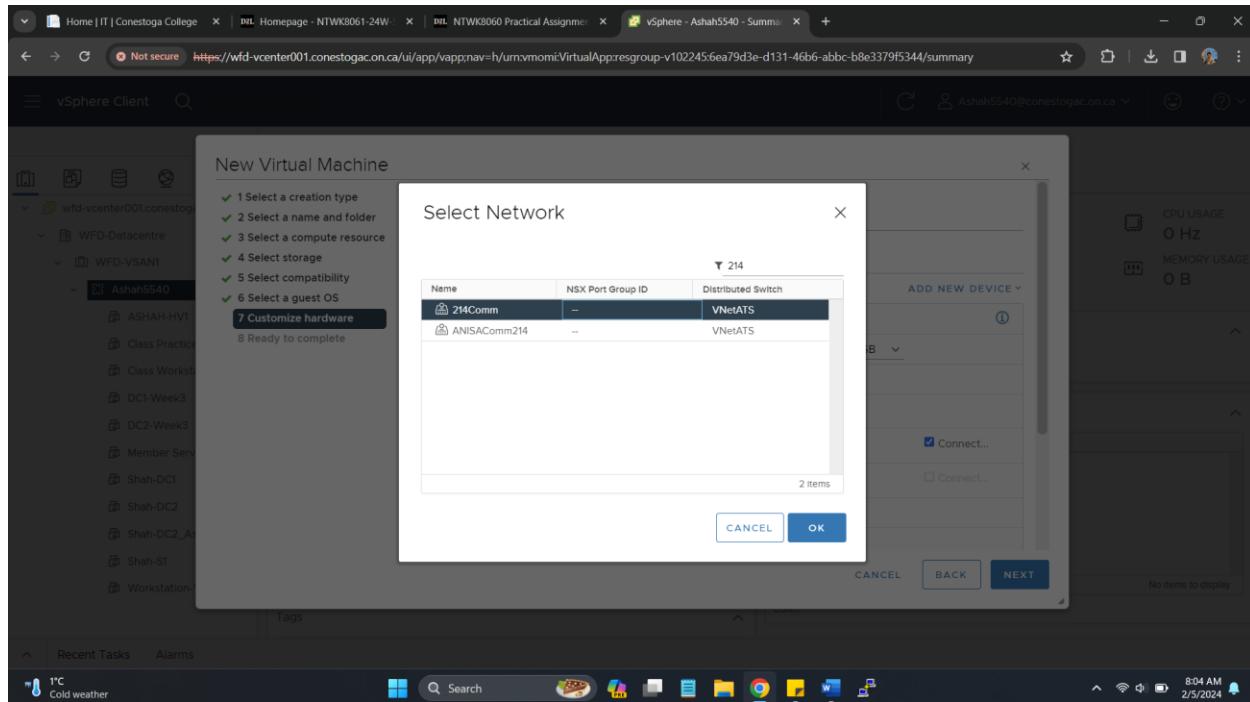
Providing name to New Virtual Machine to host as "Member Server-Assignment2"



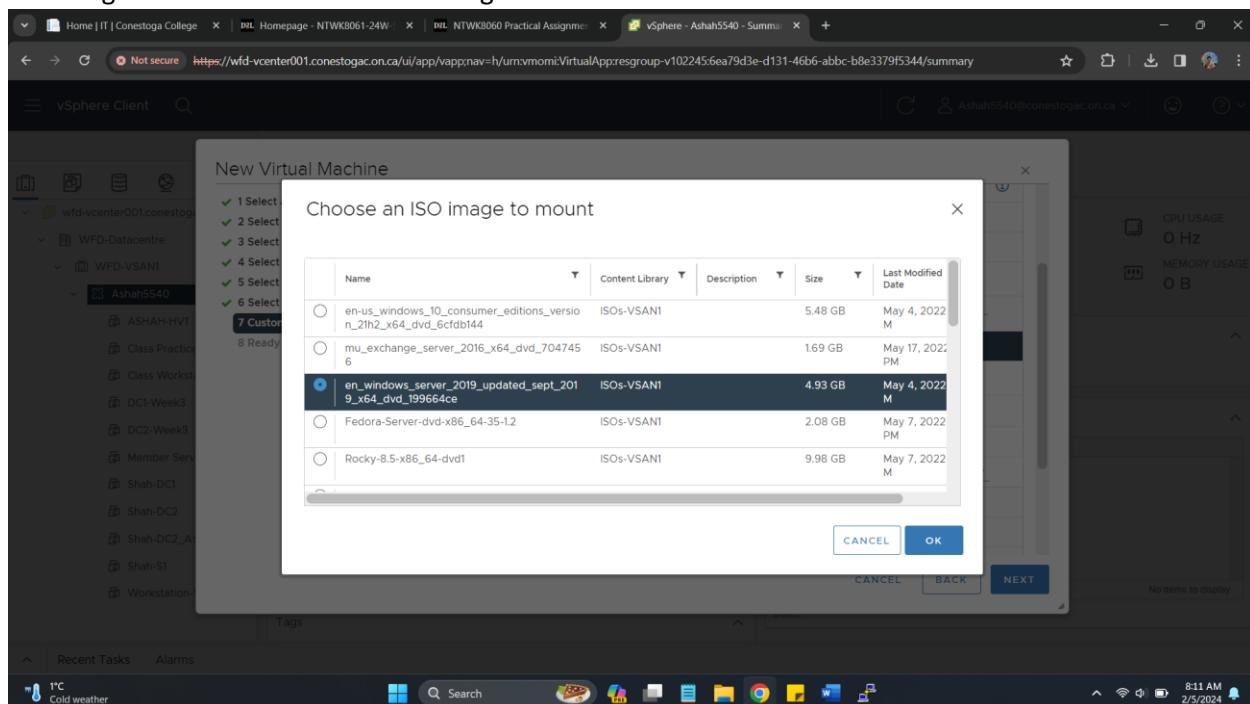
Selecting Compute resource as Ashah5540



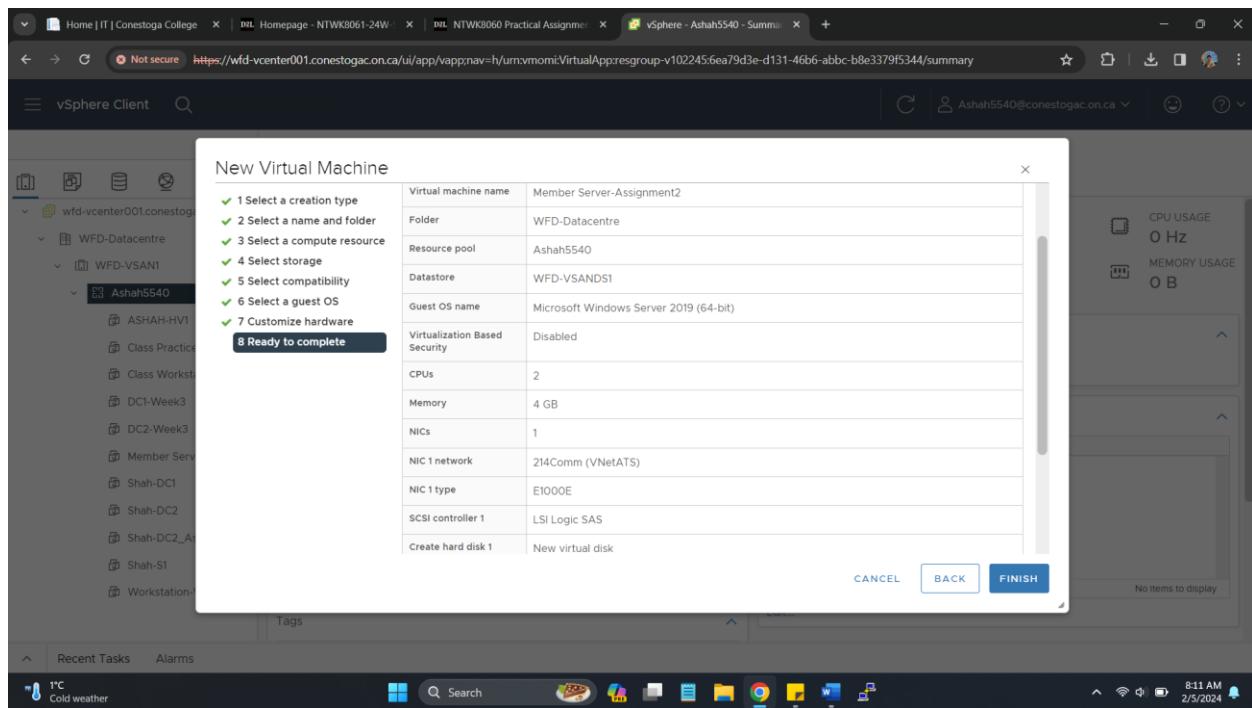
Selecting COM port 214 as network "172.16.214.0/24"



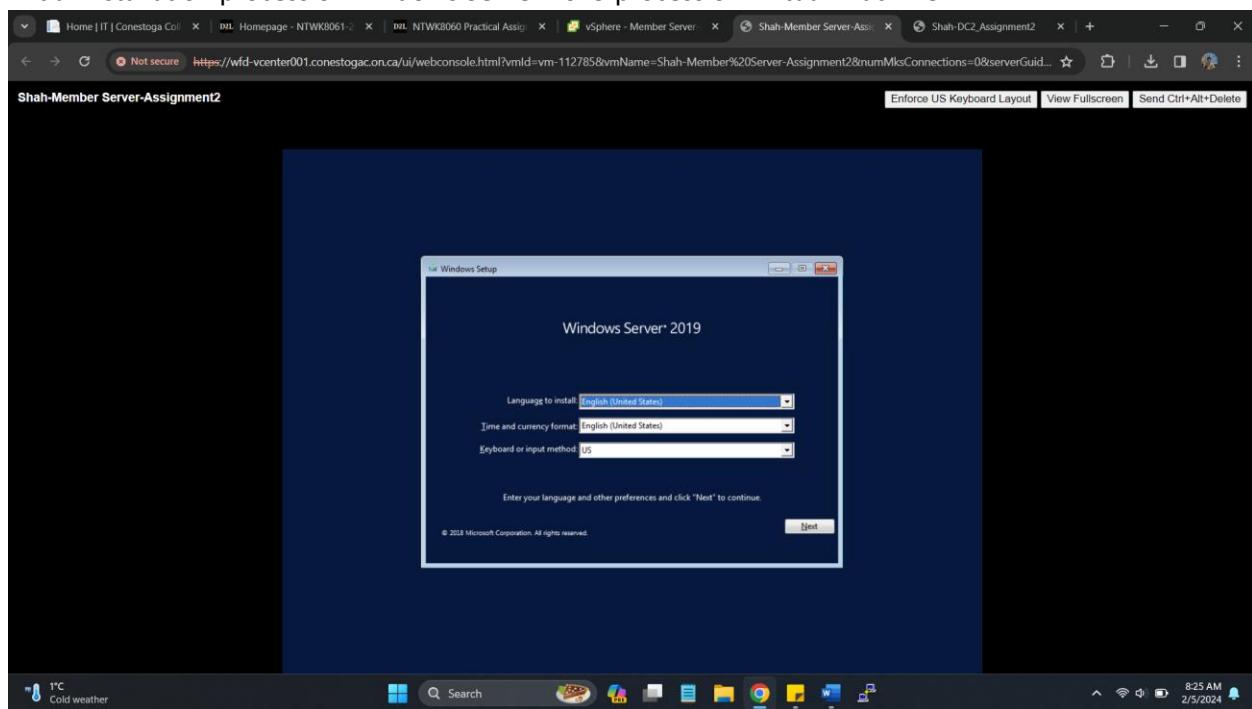
Selecting Windows Server 2019 ISO image to be mounted on Virtual machine as member server



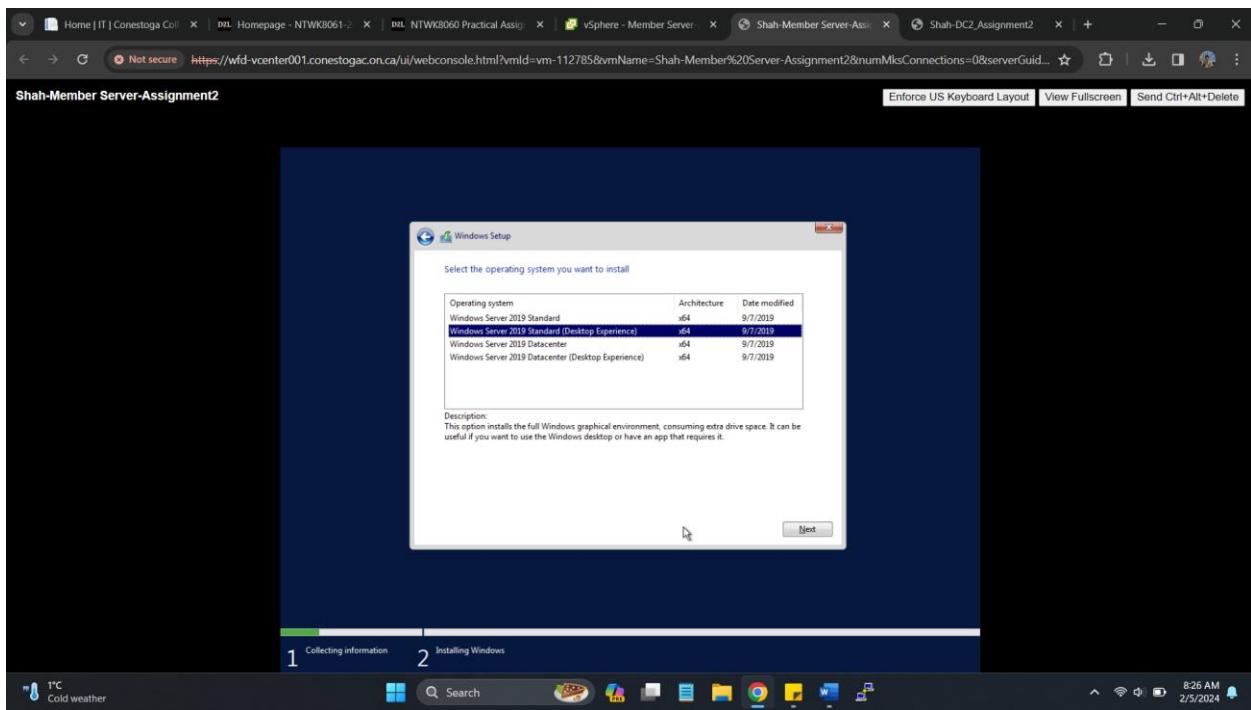
Summary of Member server installation



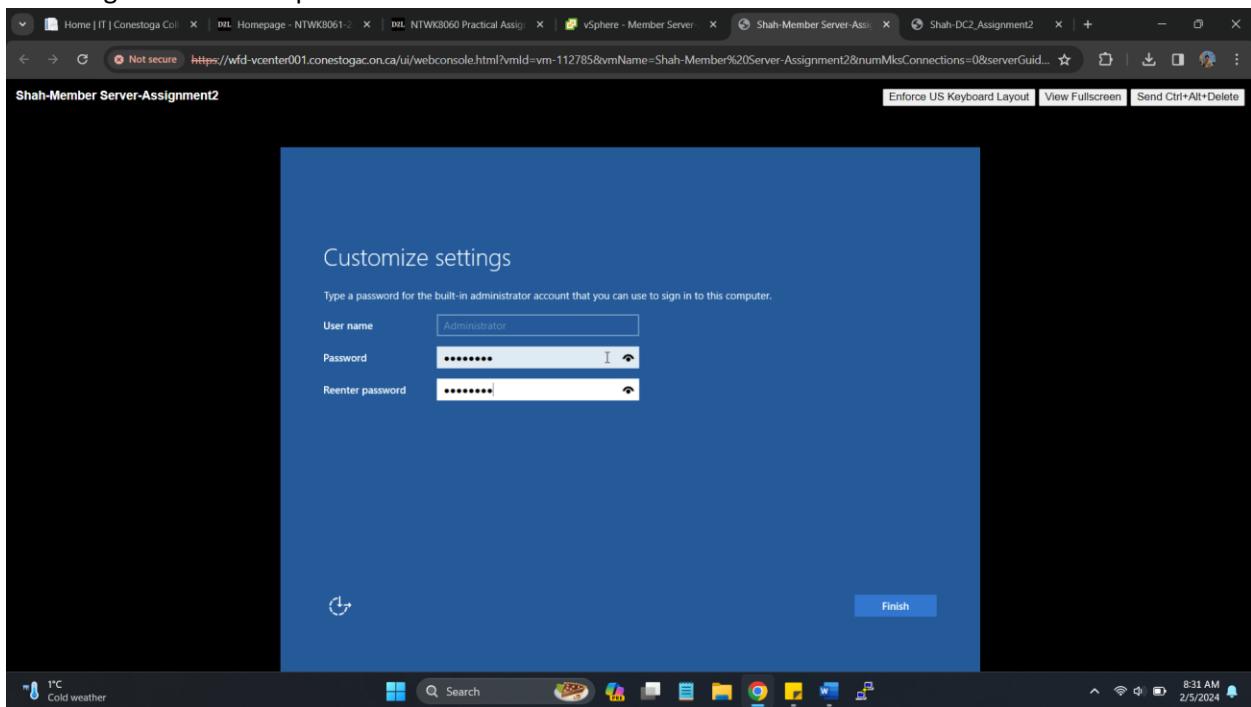
Initial installation process of Windows Server 2019 process on Virtual Machine



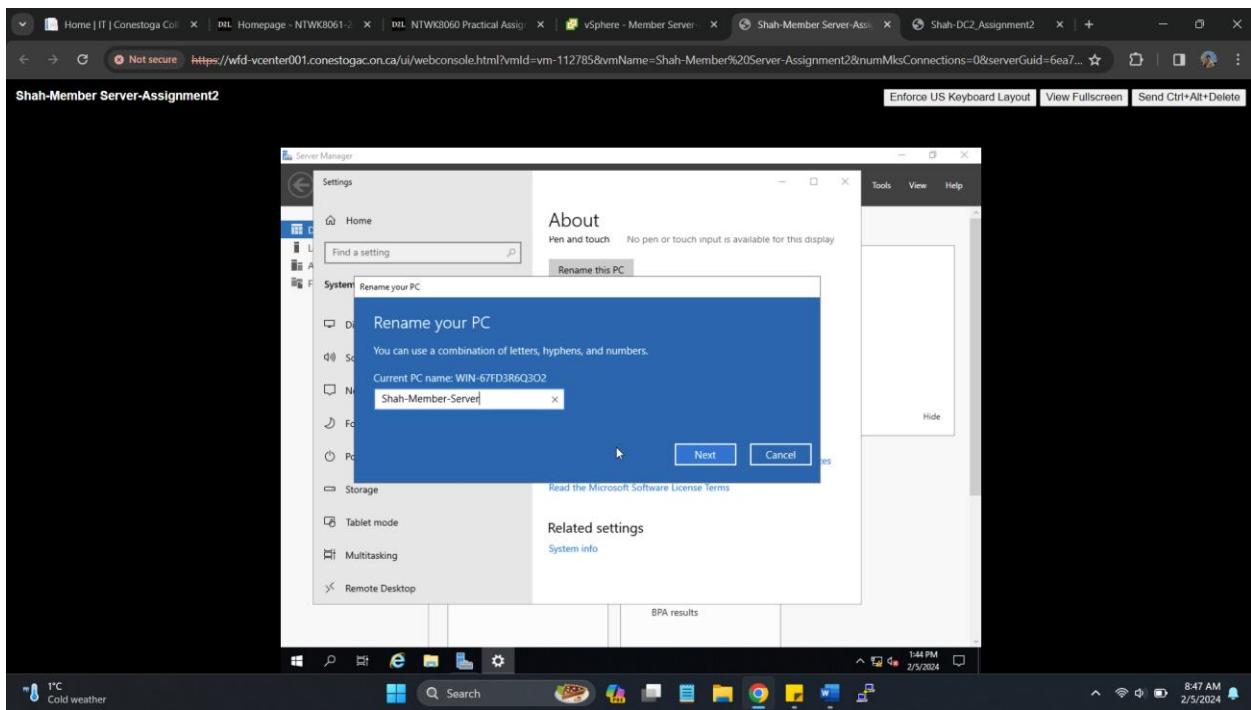
Selecting Operating System version as Windows Server 2019 standard (Desktop Experience)



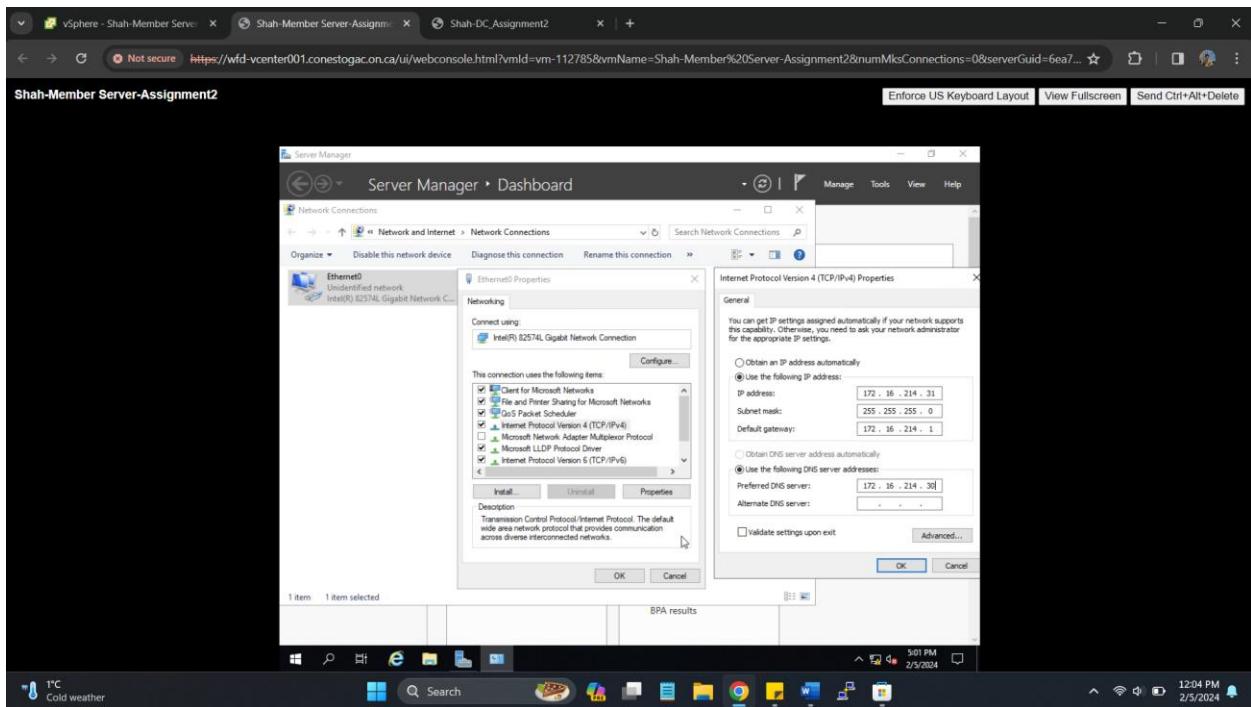
Providing Administrator password as "Secret55"



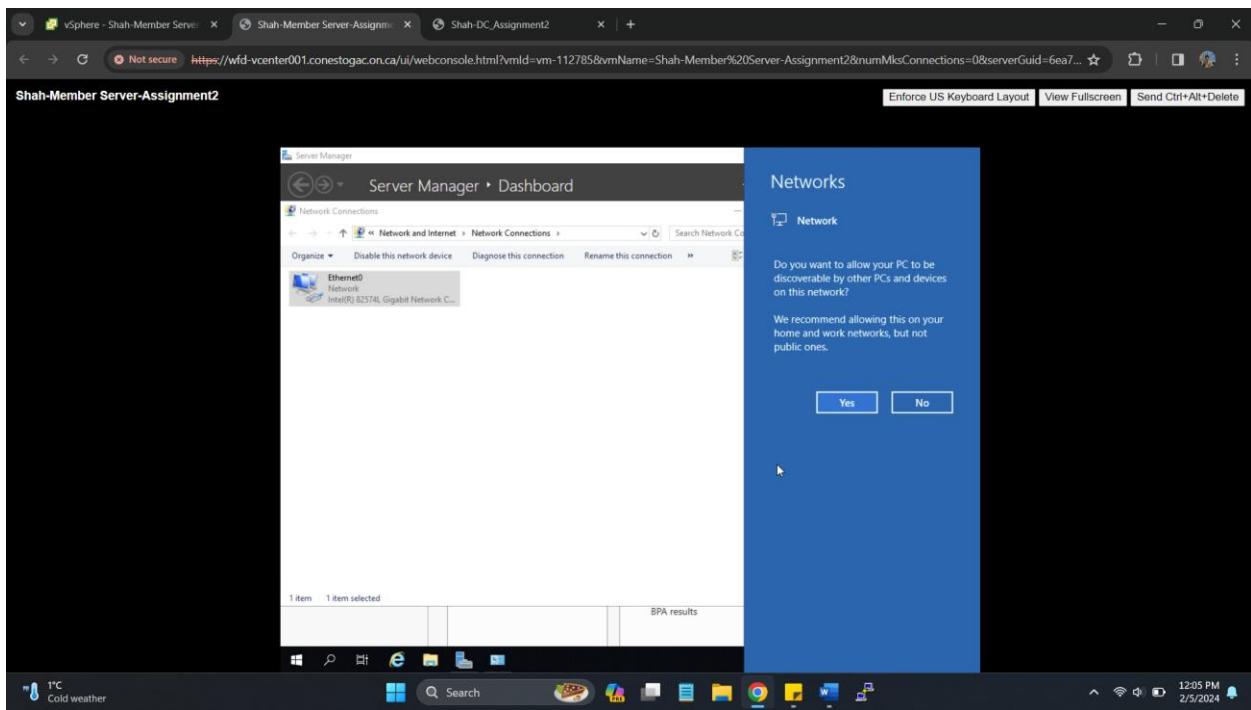
Renaming PC name to Shah-Member-Sever



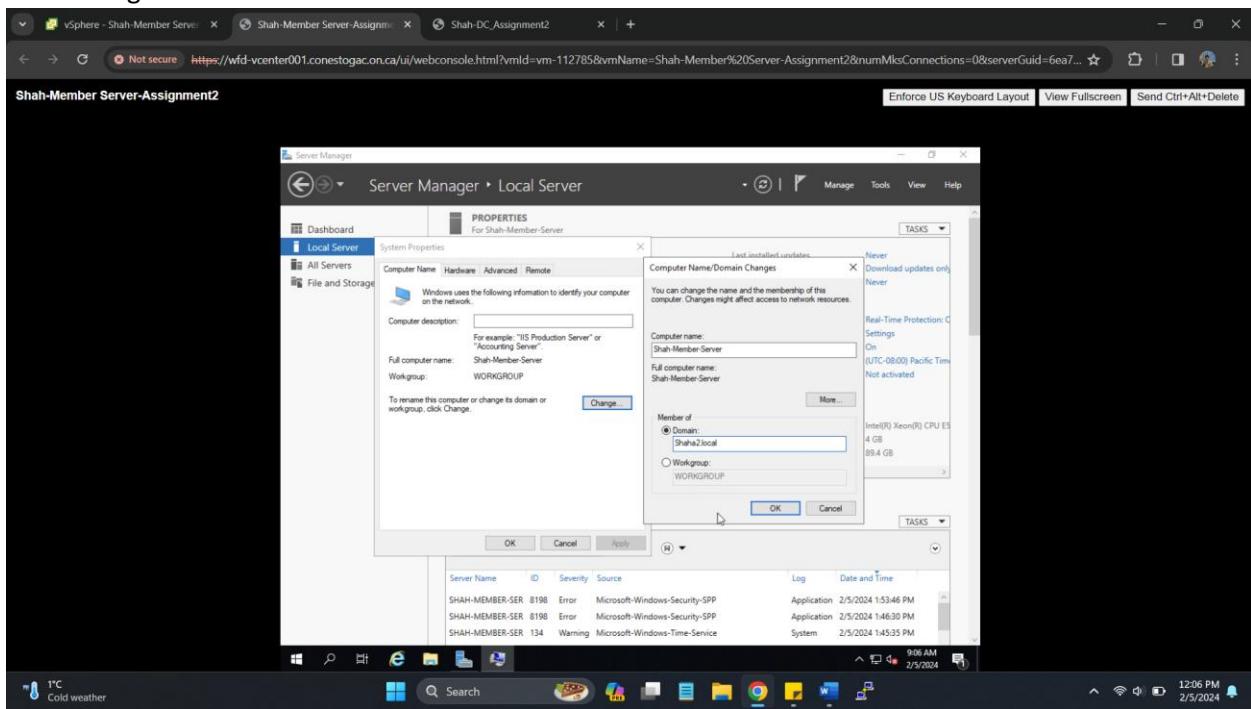
Setting IP details as 172.16.214.31 with default gateway 172.16.214.1 with preferred DNS server as 172.16.214.30



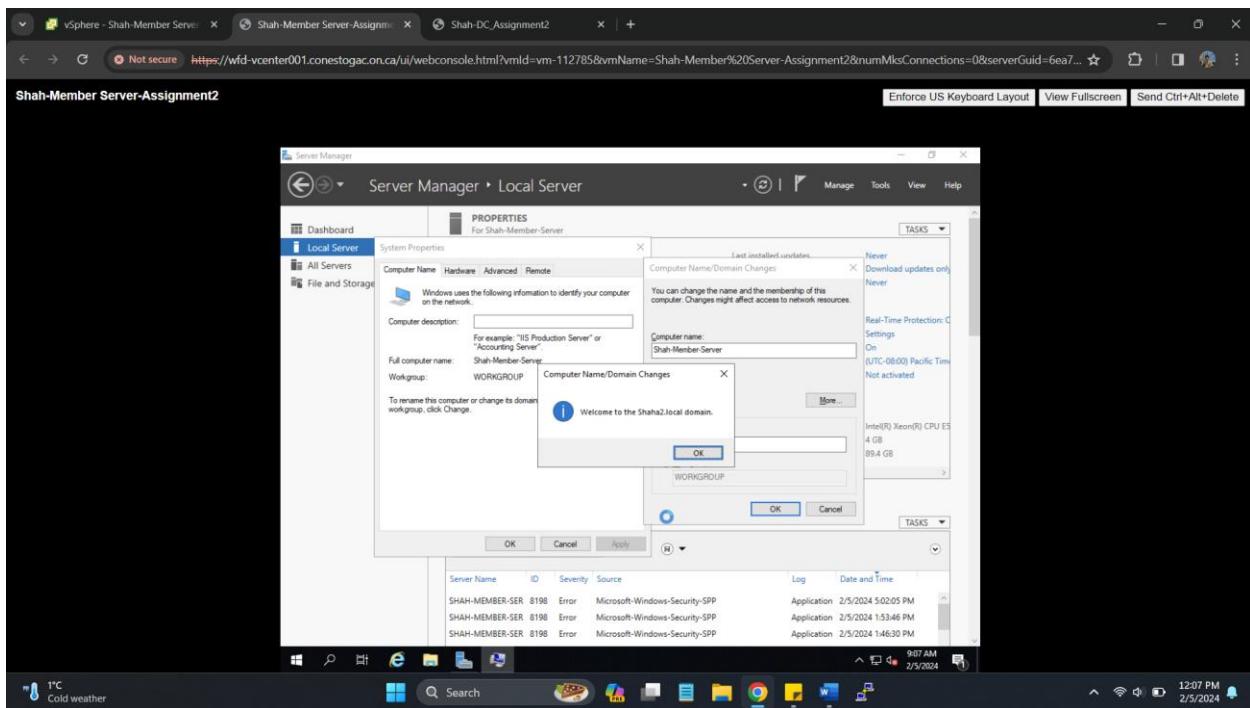
Connecting to the network for the IP details provided.



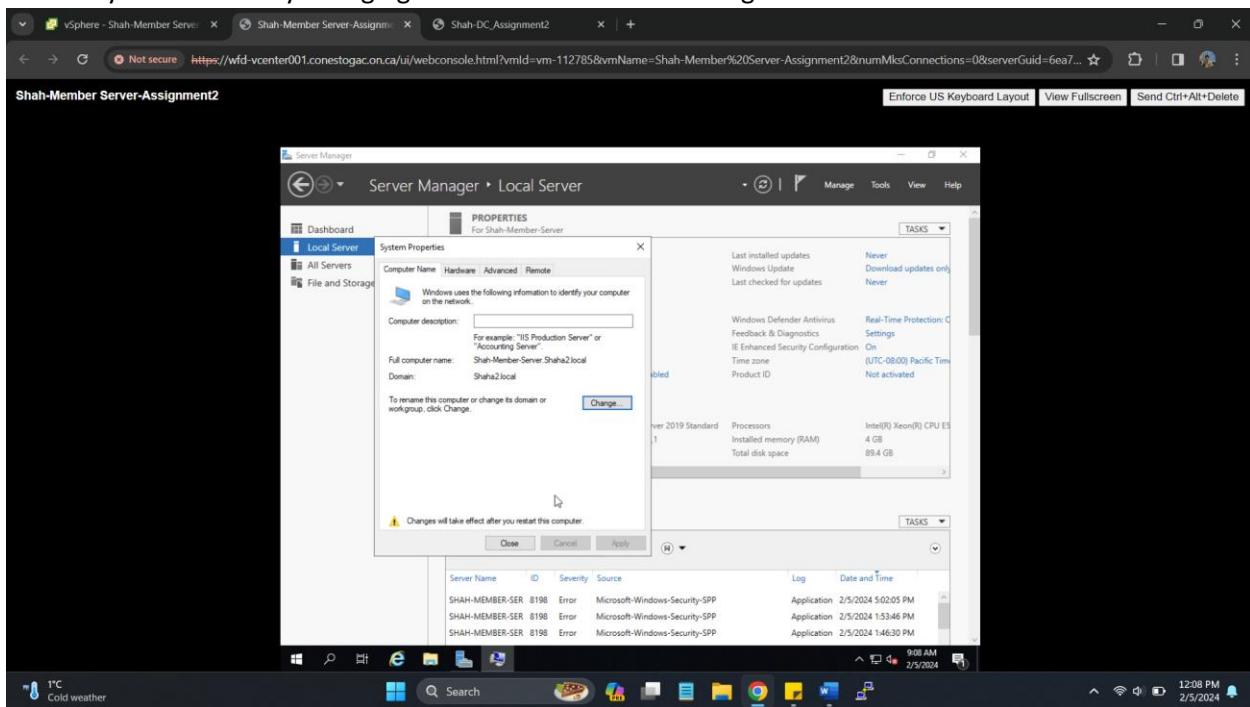
Connecting member server with Domain: Shaha2.local



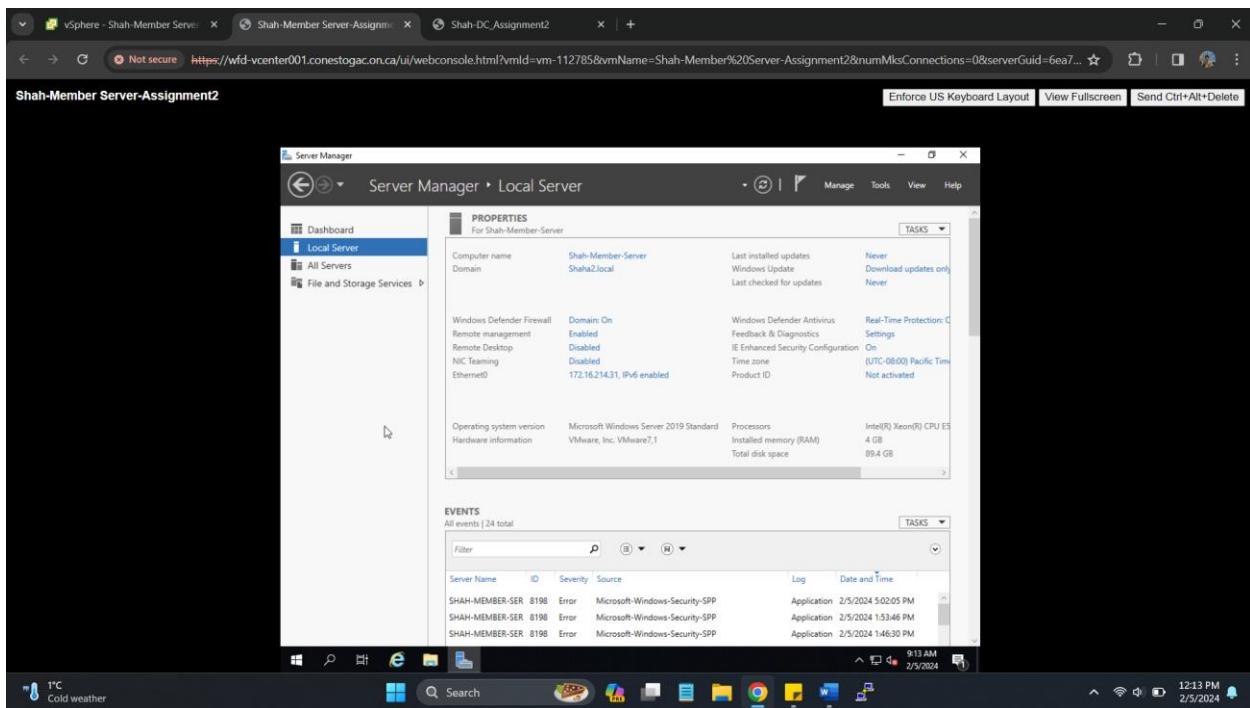
Successfully connecting member server to Shaha2.local



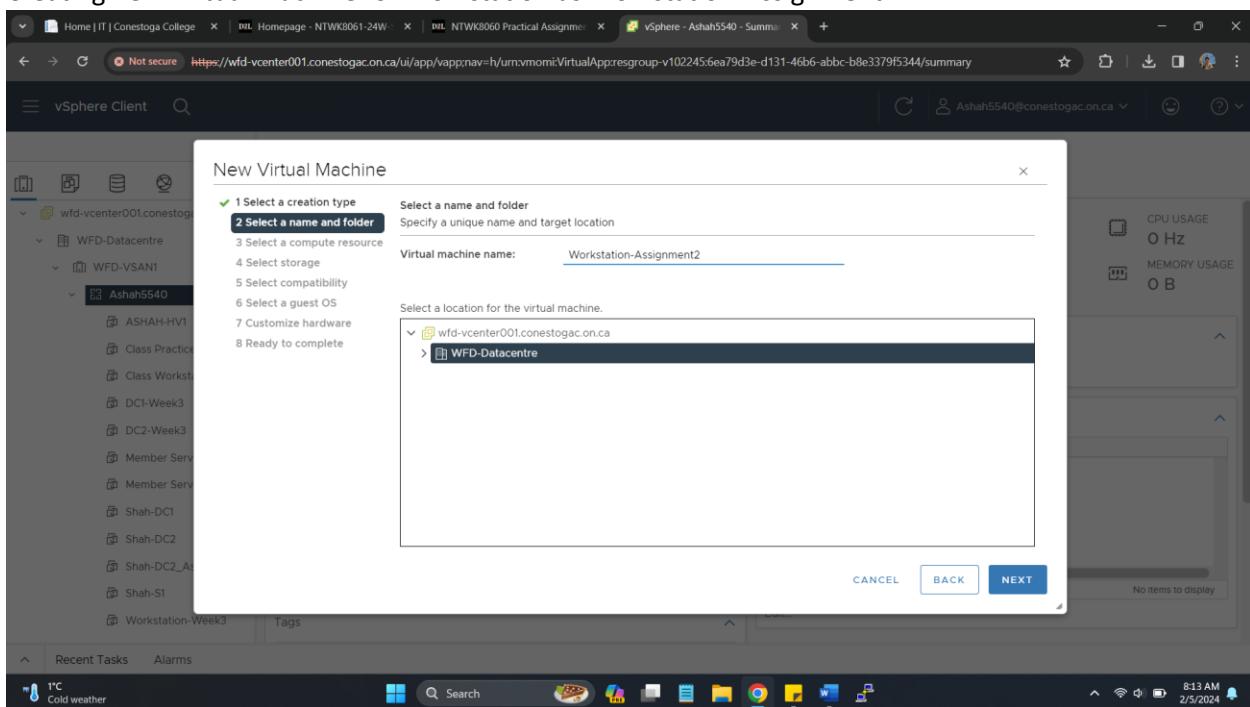
Summary of successfully changing server name and connecting it to Shaha2.local domain



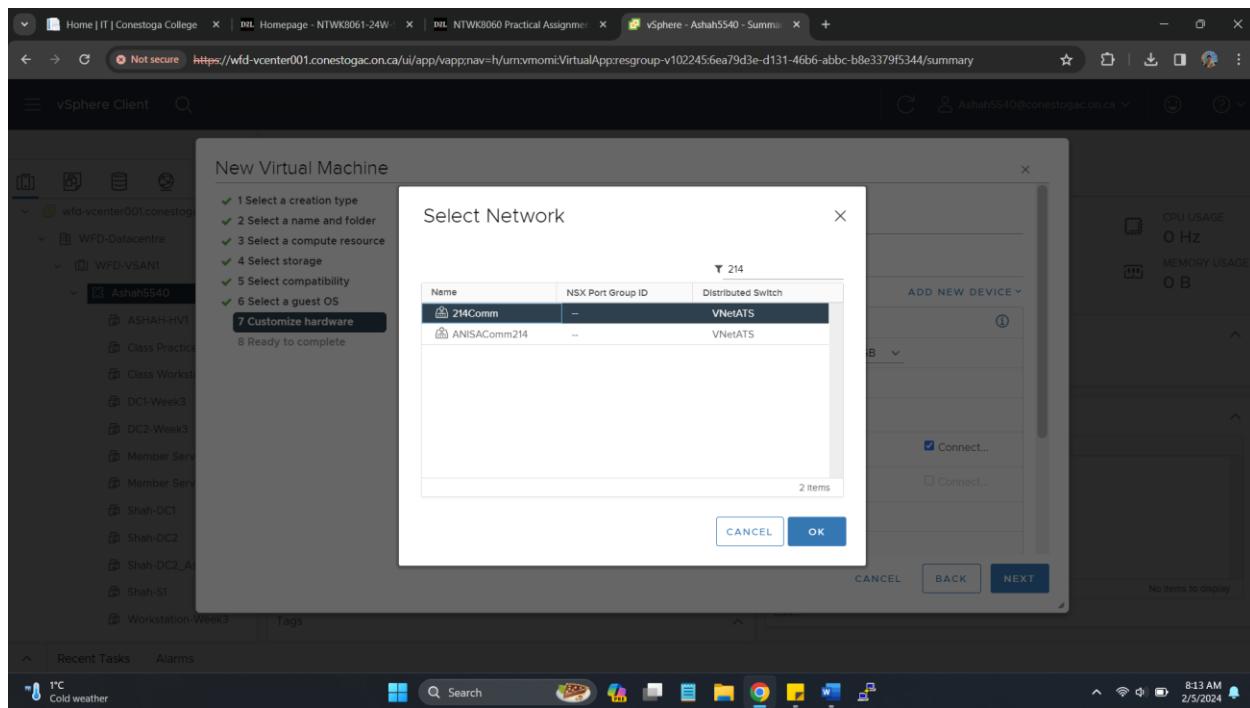
Details of member server with IP , and domain details



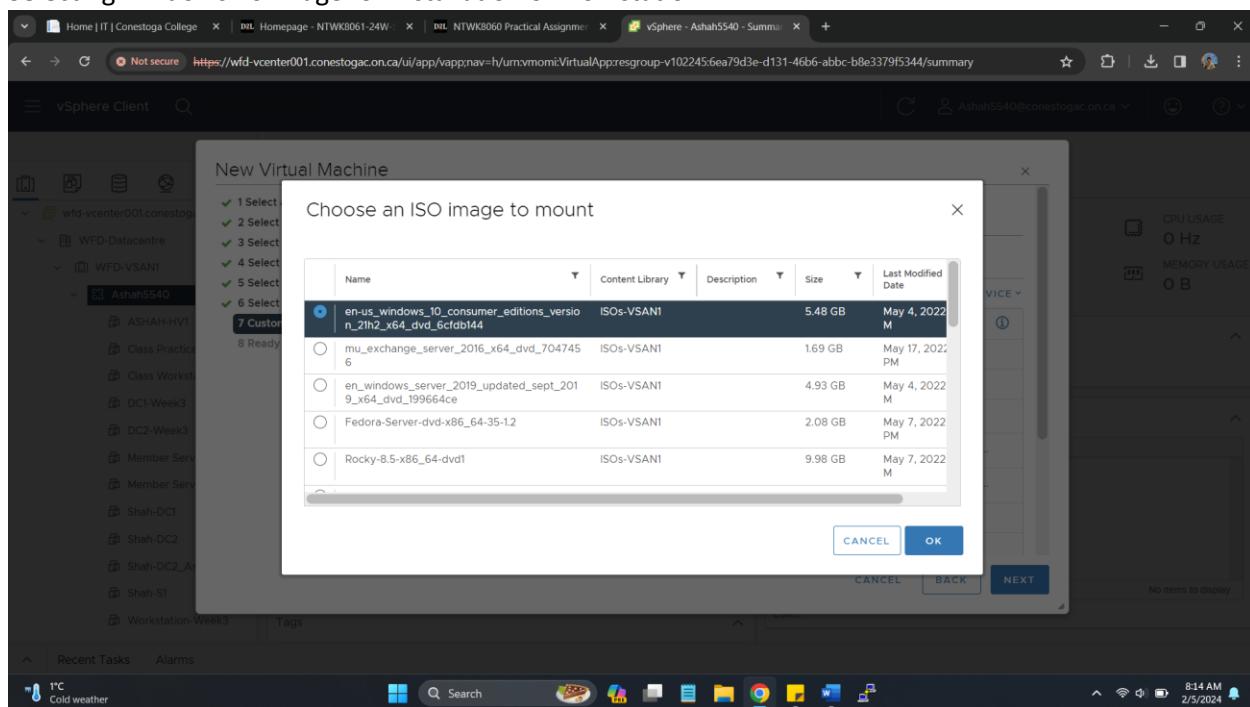
Creating new Virtual machine for Workstation as Workstation-Assignment2



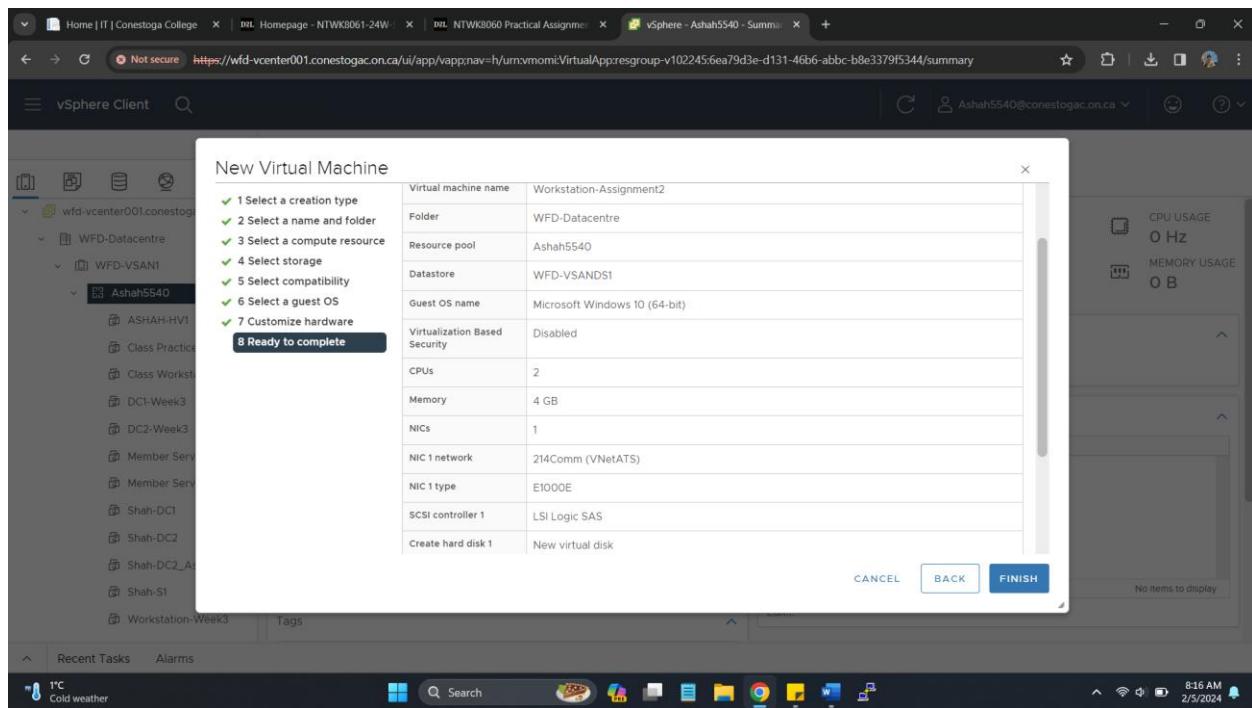
Selecting Com port as 214 for connecting it to network assigned to Ashah5540 student id 8935540



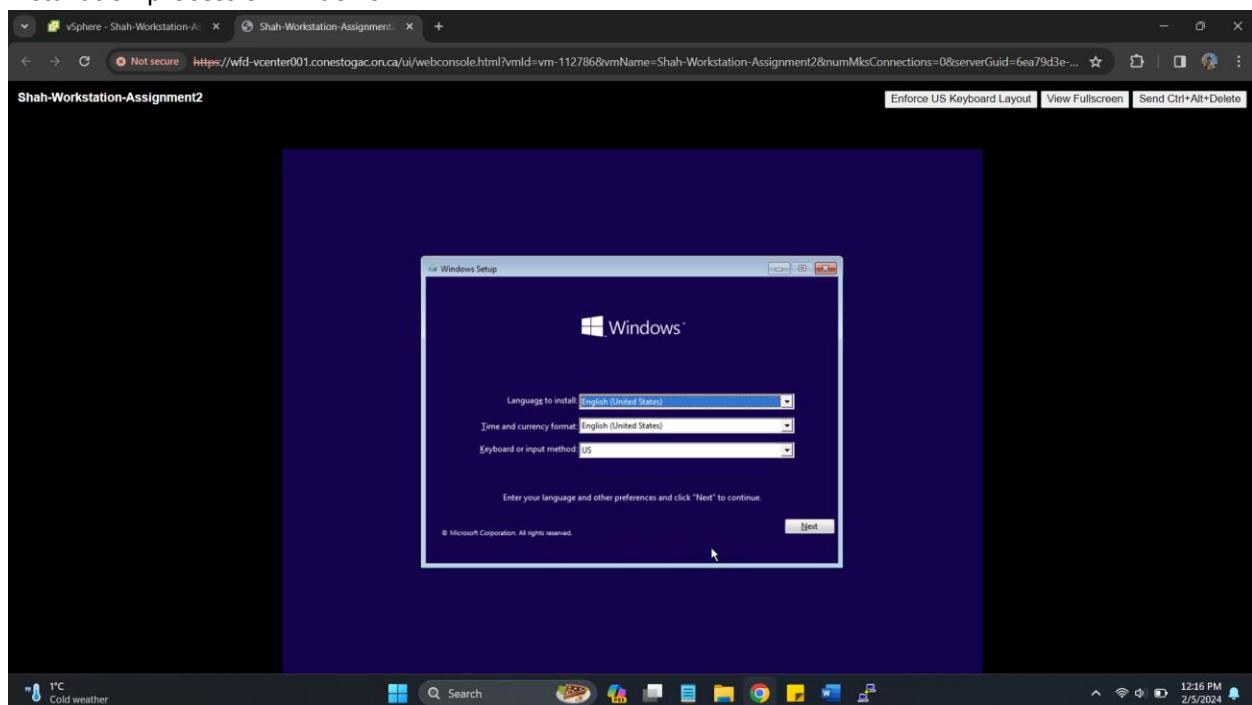
Selecting windows 10 image for installation of workstation



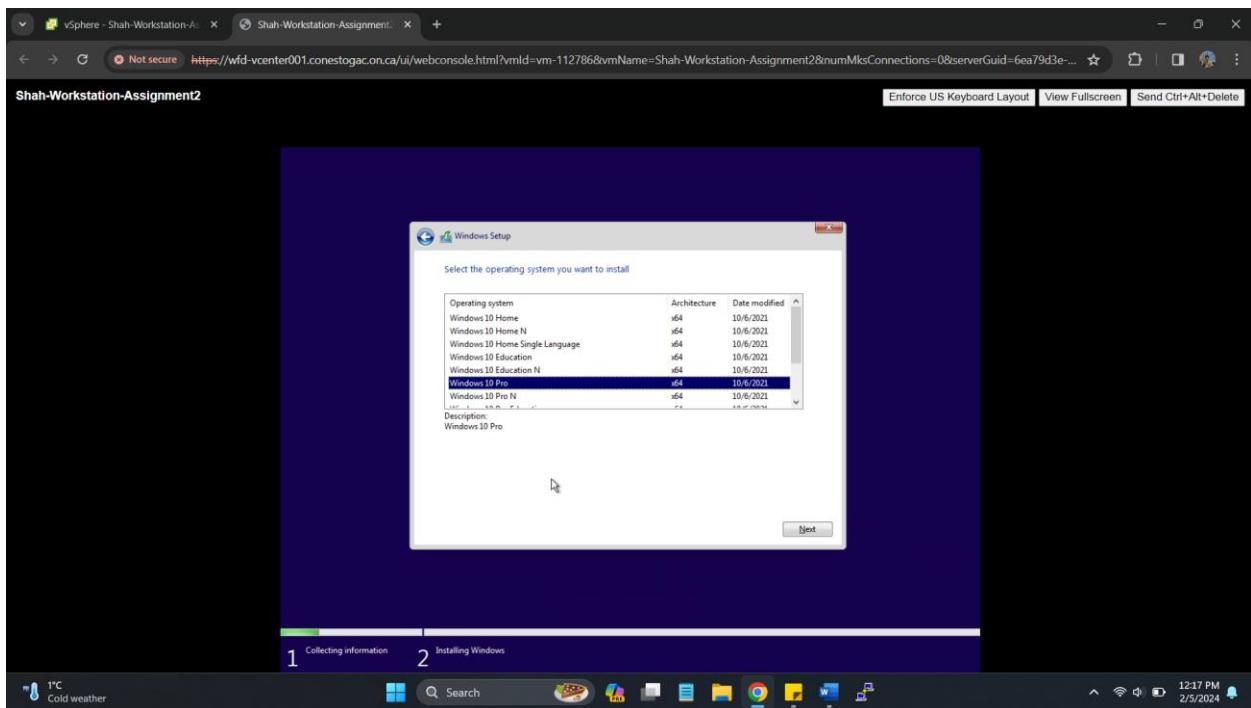
Summary of new workstation to be created as virtual machine.



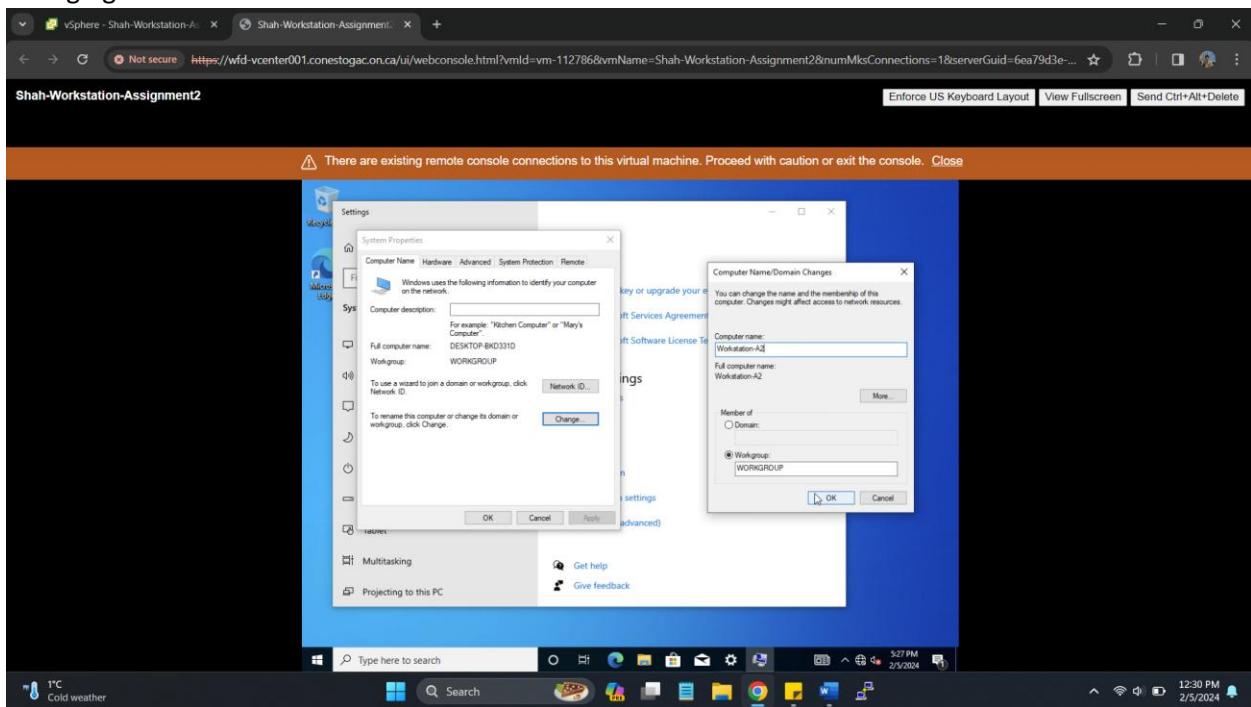
Installation process of windows



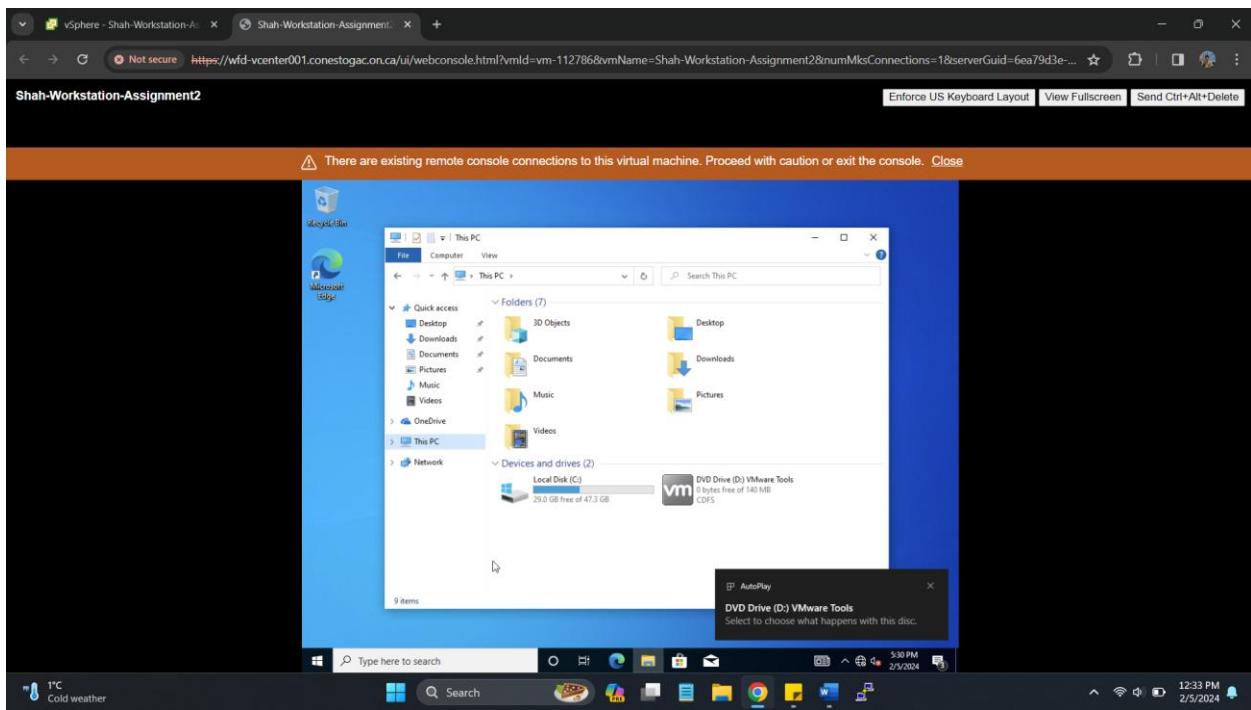
Selecting Windows 10 Pro version for installation of workstation.



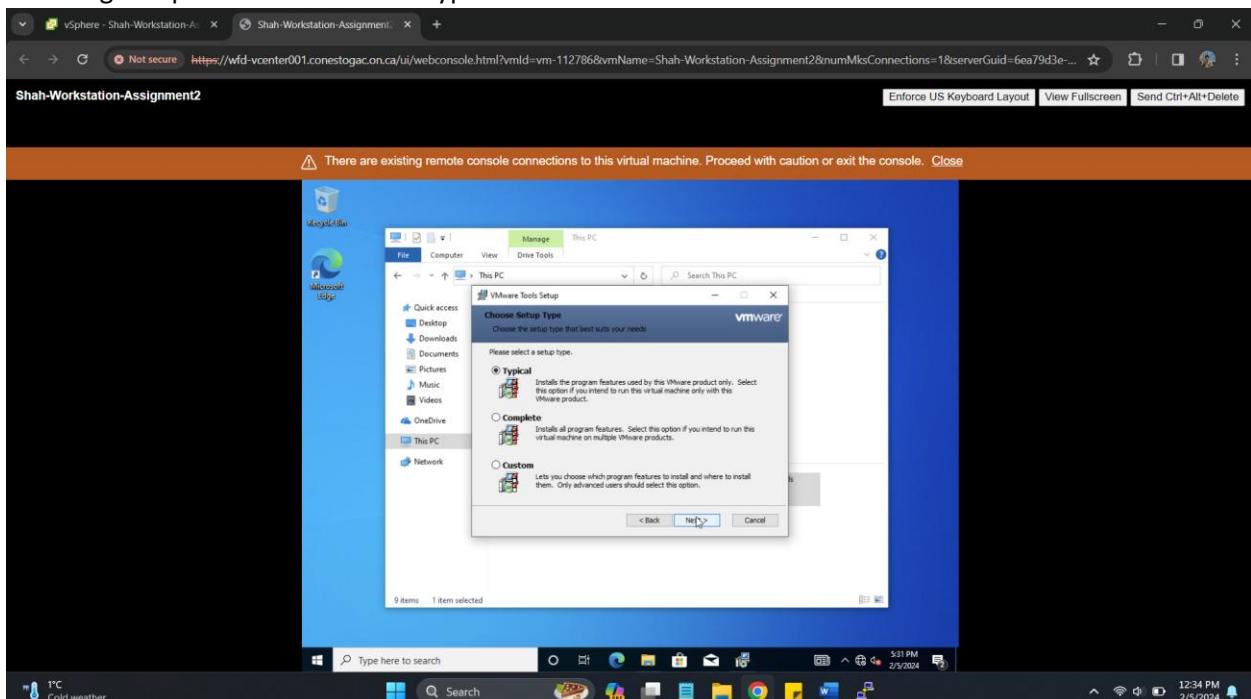
Changing workstation name to Workstation-A2



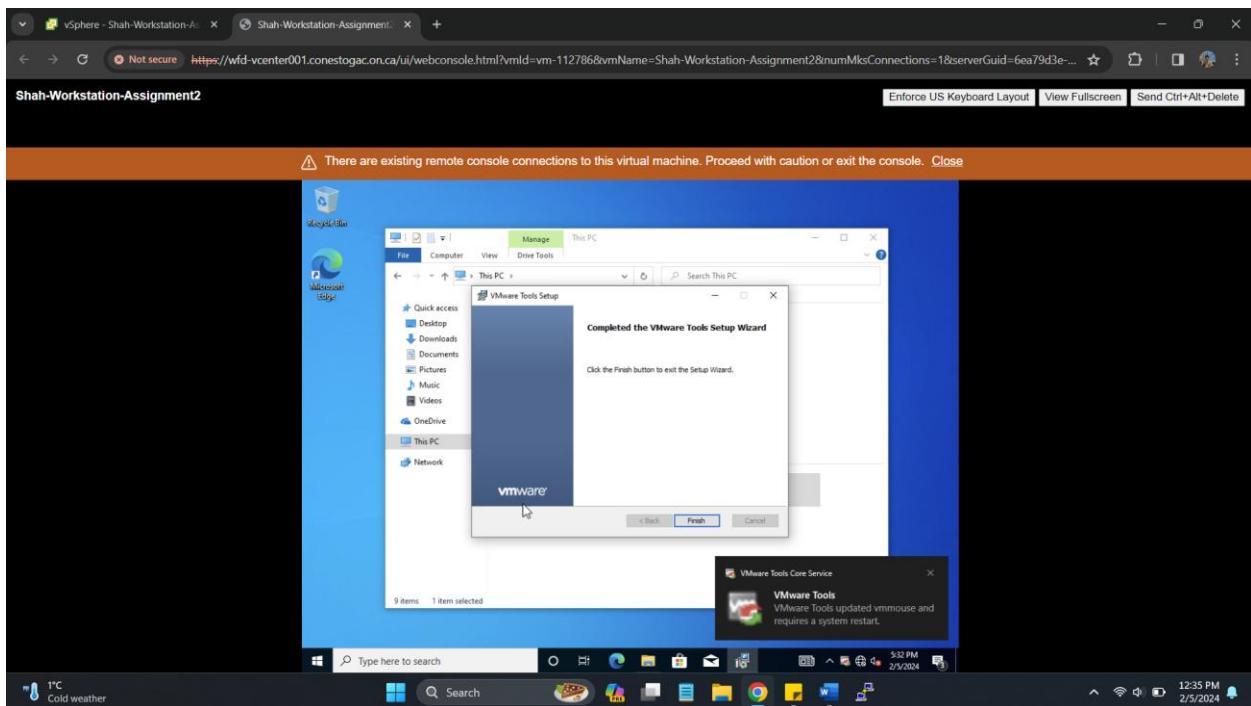
Installing VMware tools on workstation VM



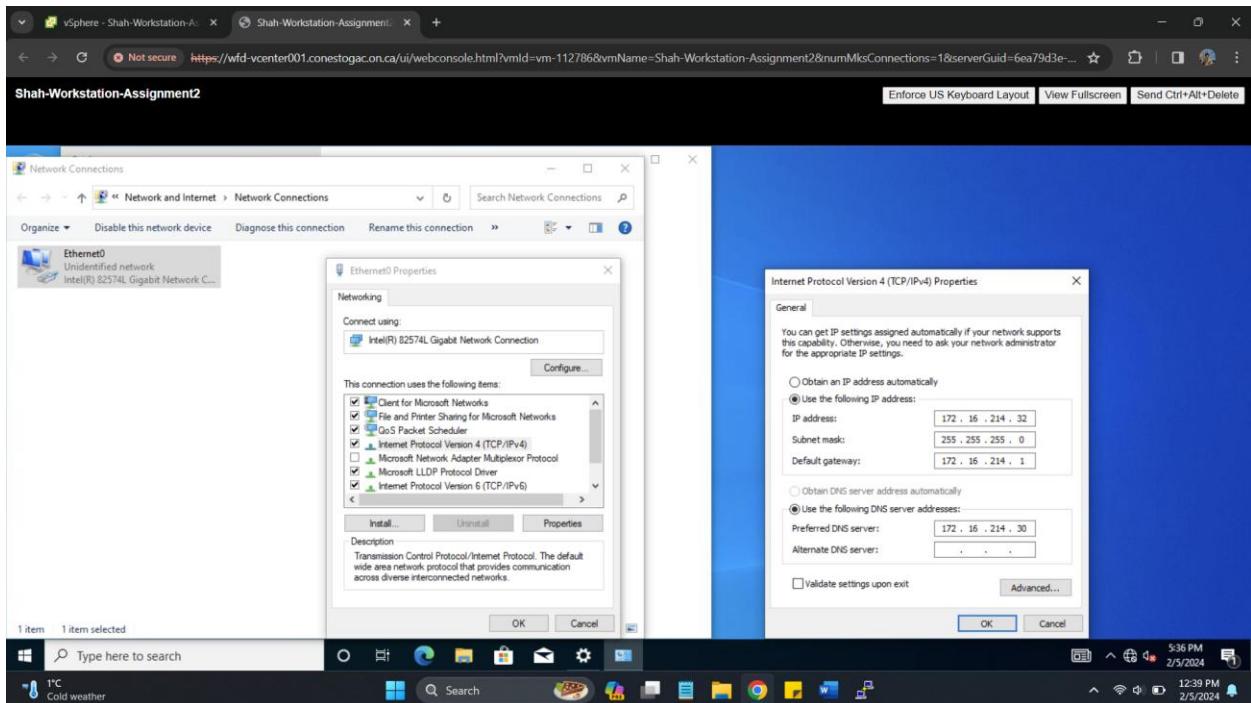
Selecting setup of Vmware tools as typical mode



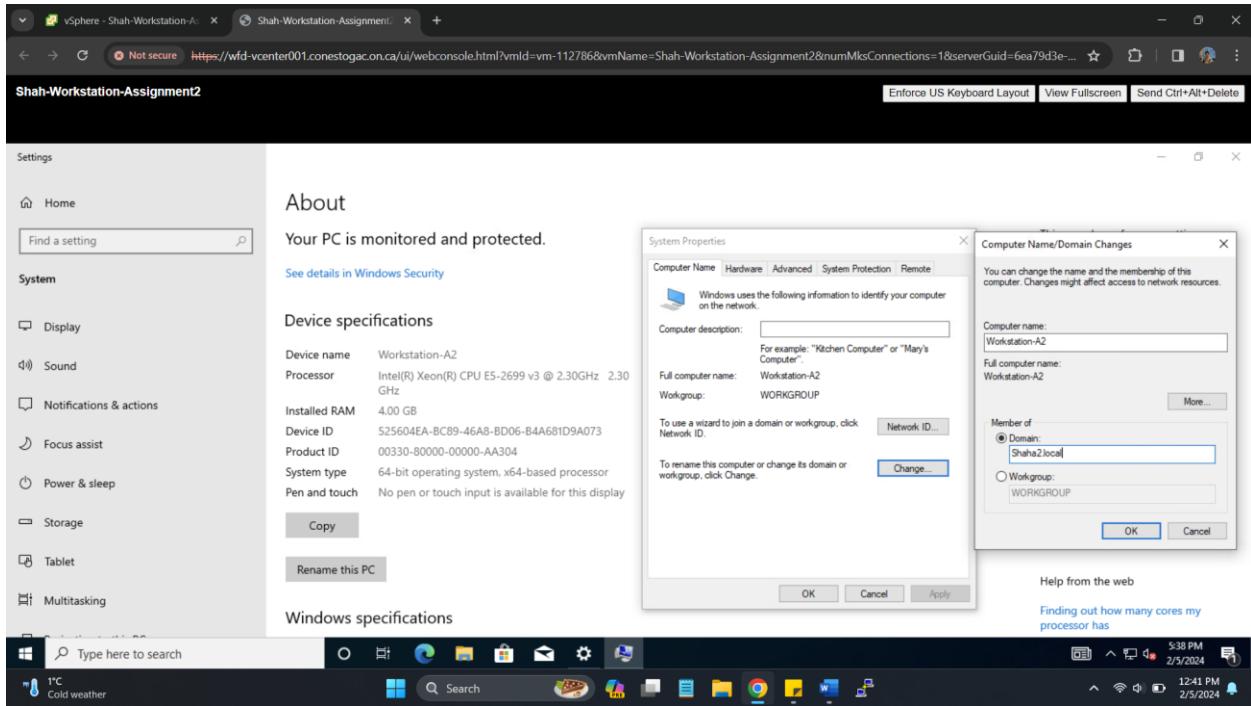
Completion of setup installation



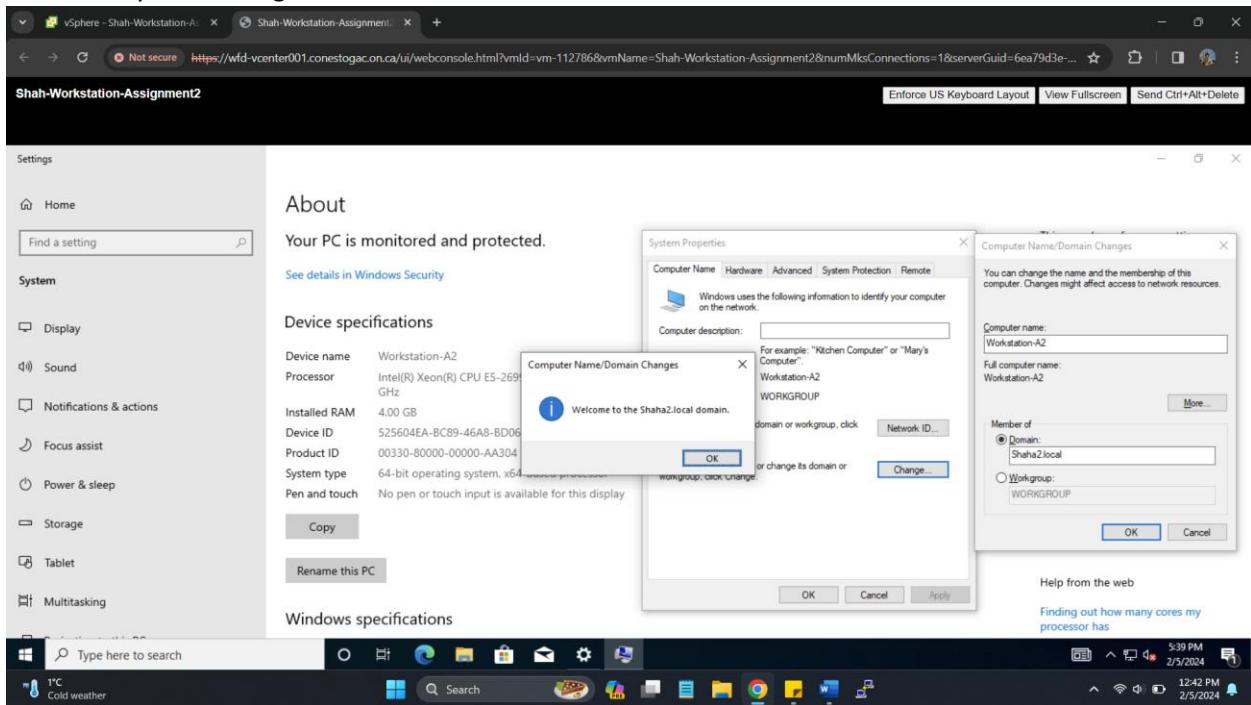
Providing IP to workstation as 172.16.214.32 with subnet details and gateway as 172.16.214.1 and DNS server as 172.16.214.30



Connecting workstation to domain "Shaha2.local"

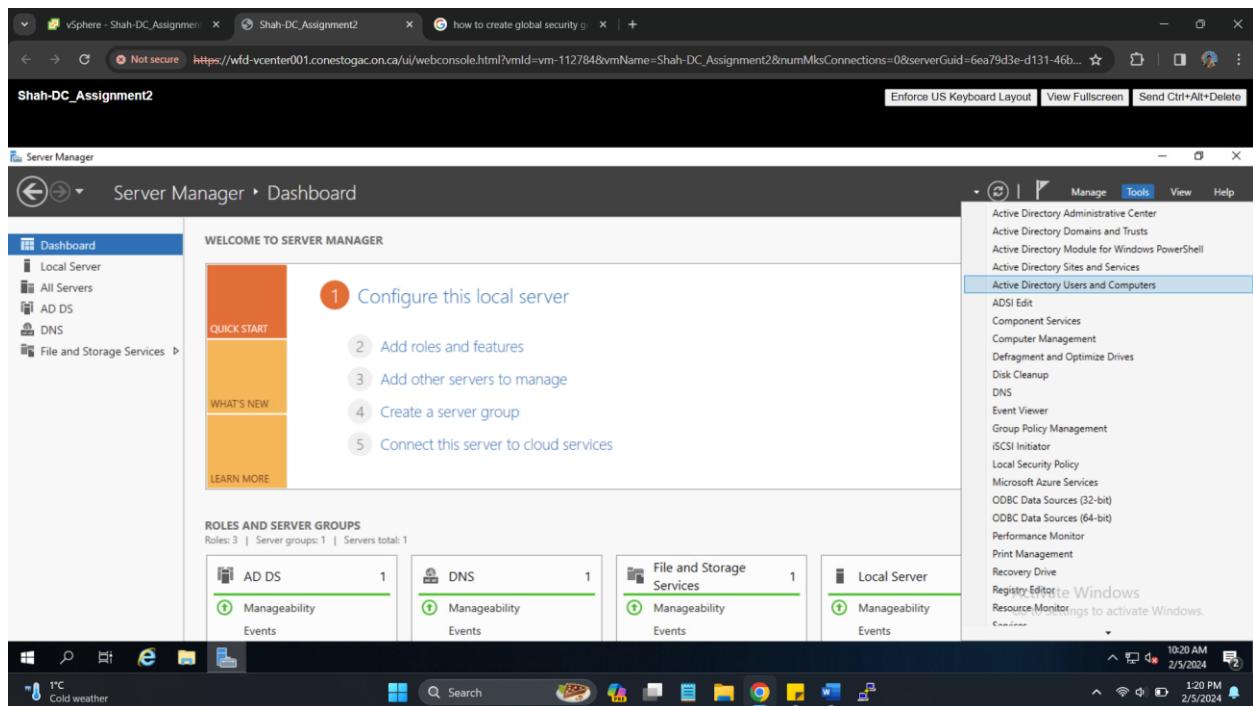


Successfully connecting workstation to domain.

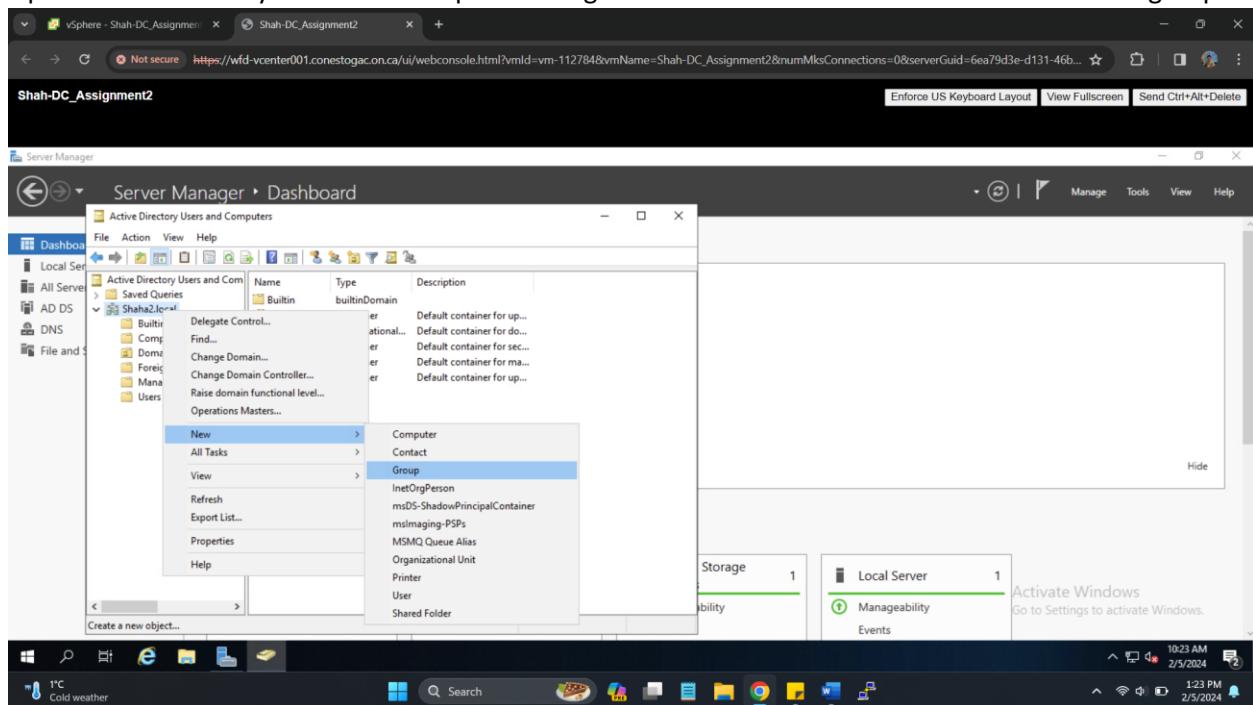


2) Create a Global Security Group named IT and add a user to it.

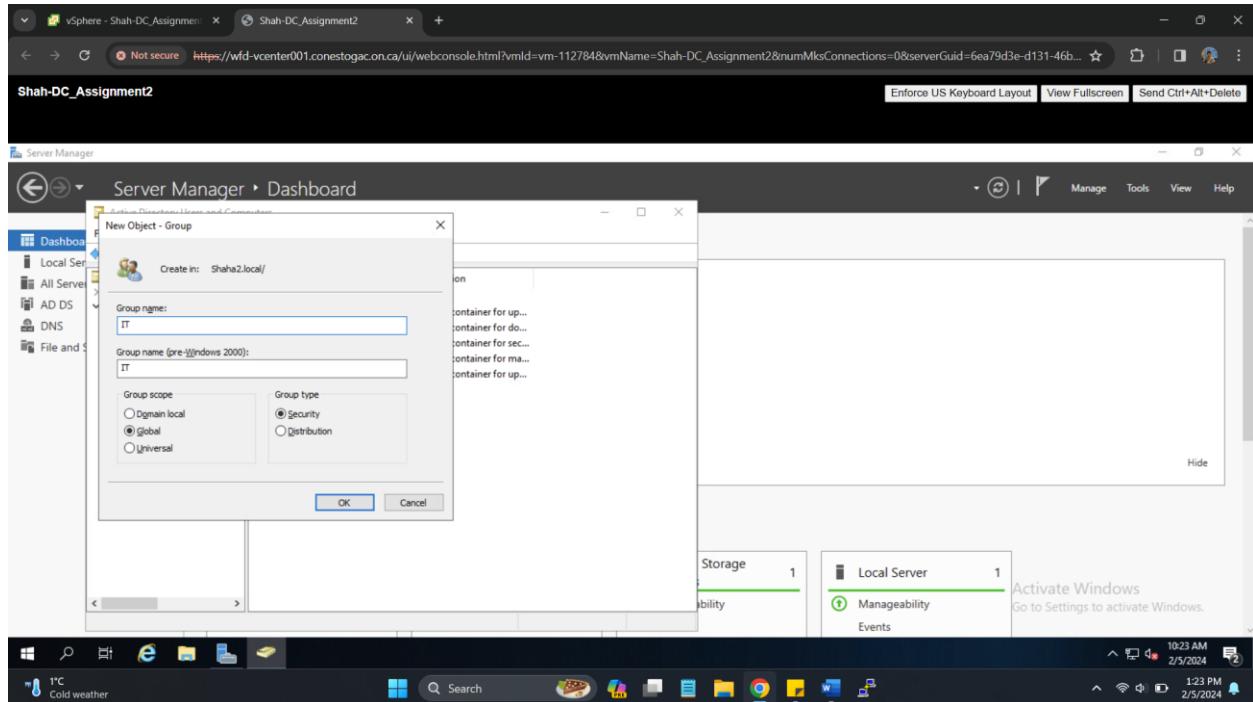
To create Global Security Group on Domain controller → open tools in server manager → select Active Directory Users and Computers



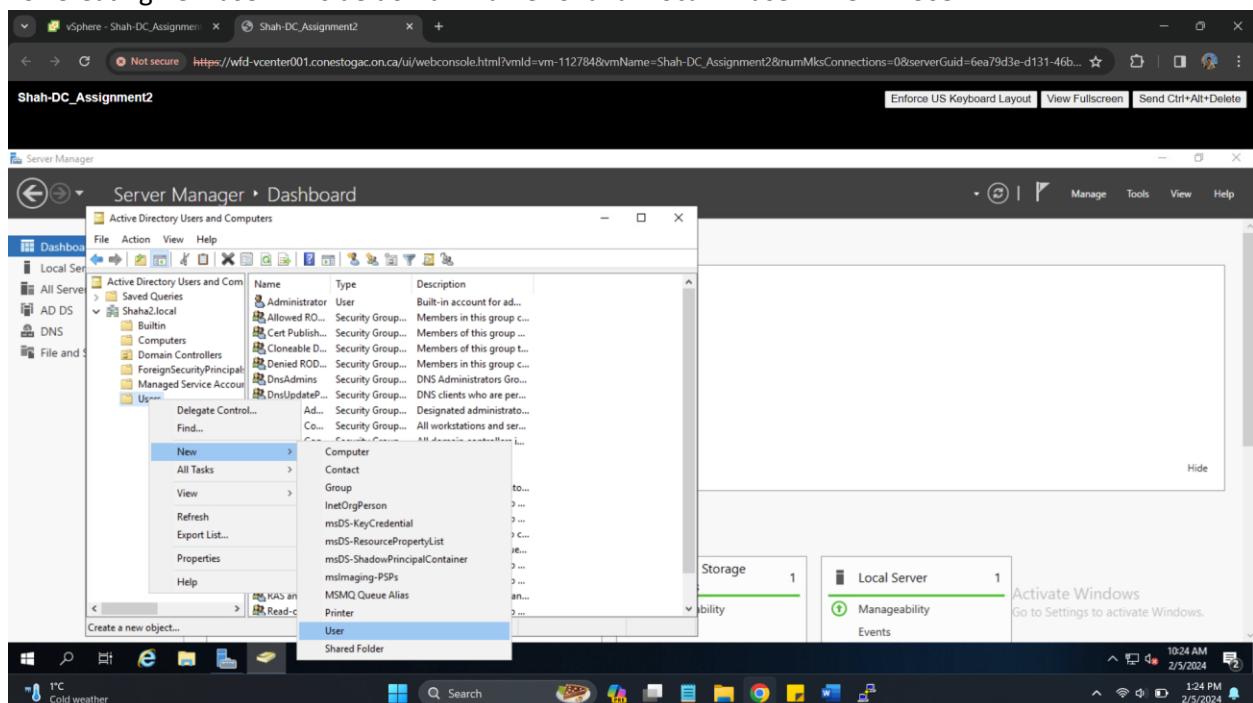
Open Active Directory Users and Computers → right click domain name "Shaha2.local" → new → group



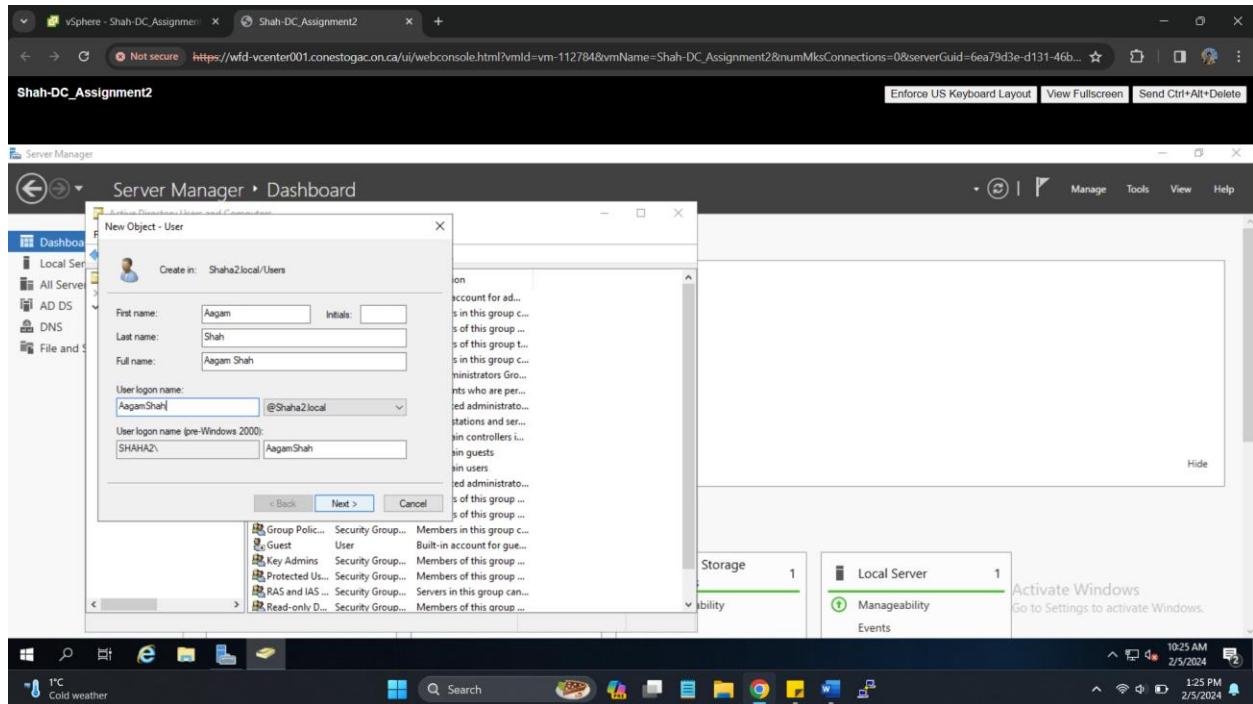
Provide group name as IT with defining group scope global and type as security.



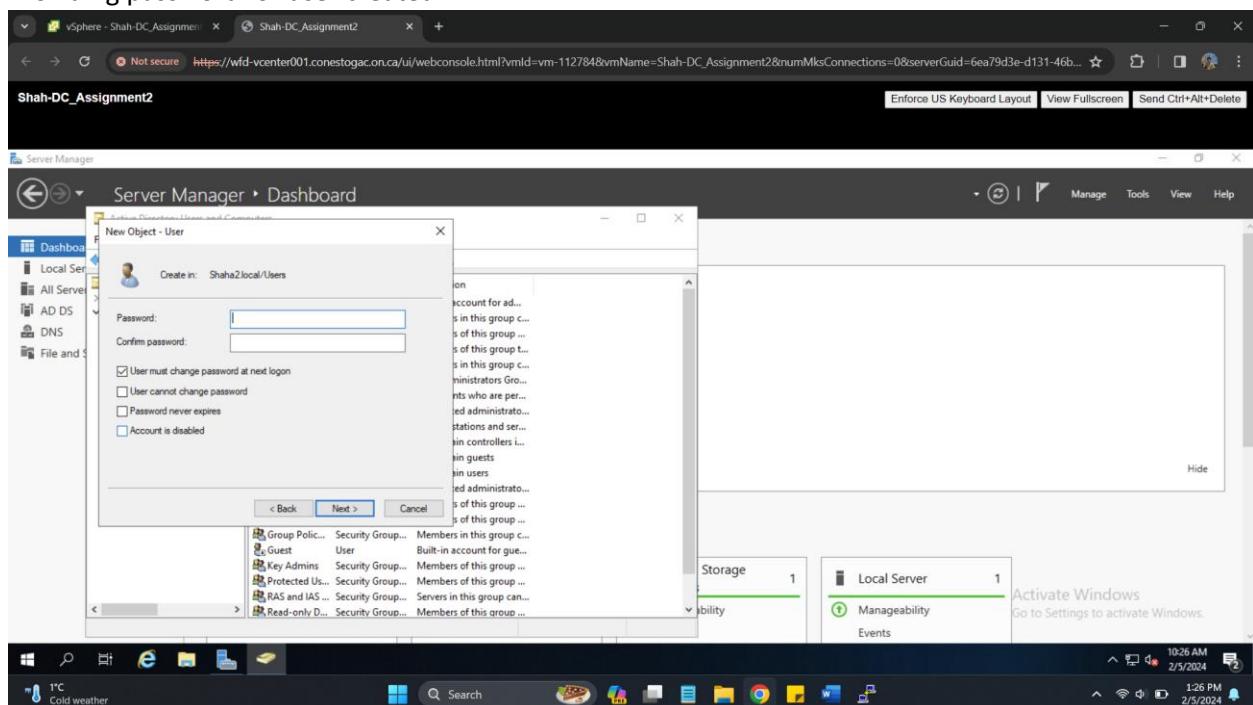
For Creating new user → inside domain name "Shaha2.local" → user → new → User



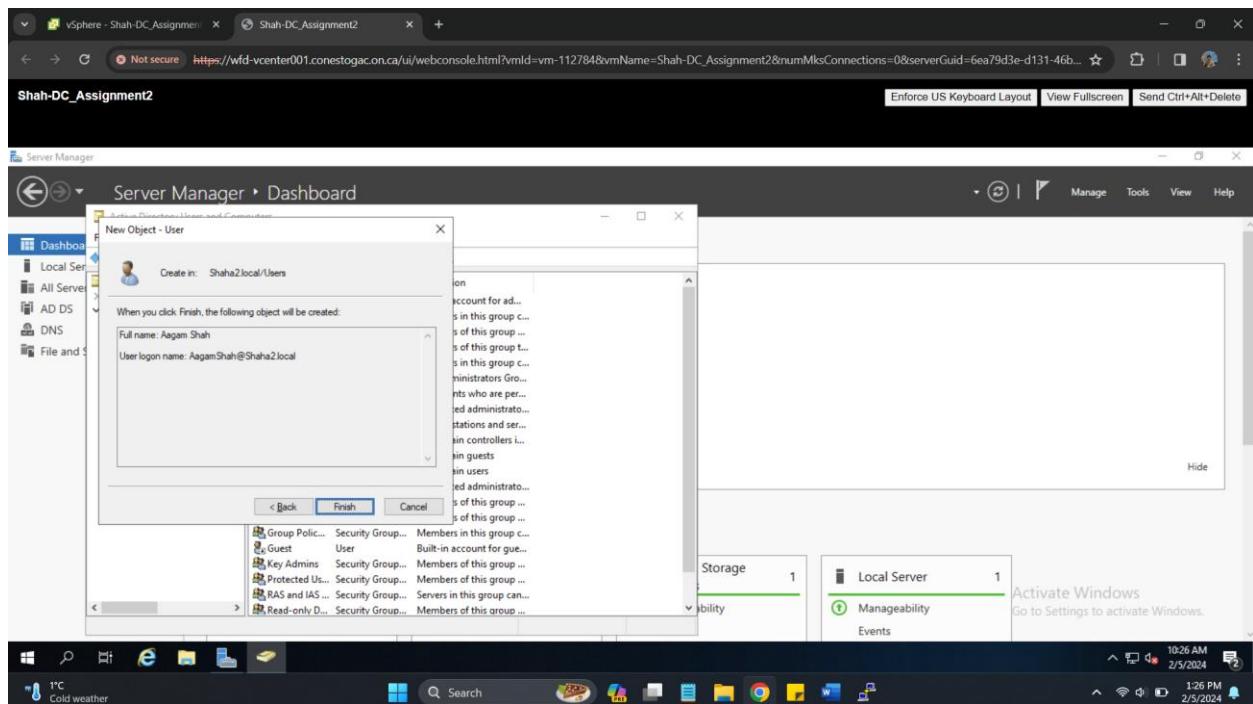
Creating new object-user → name as "AagamShah"



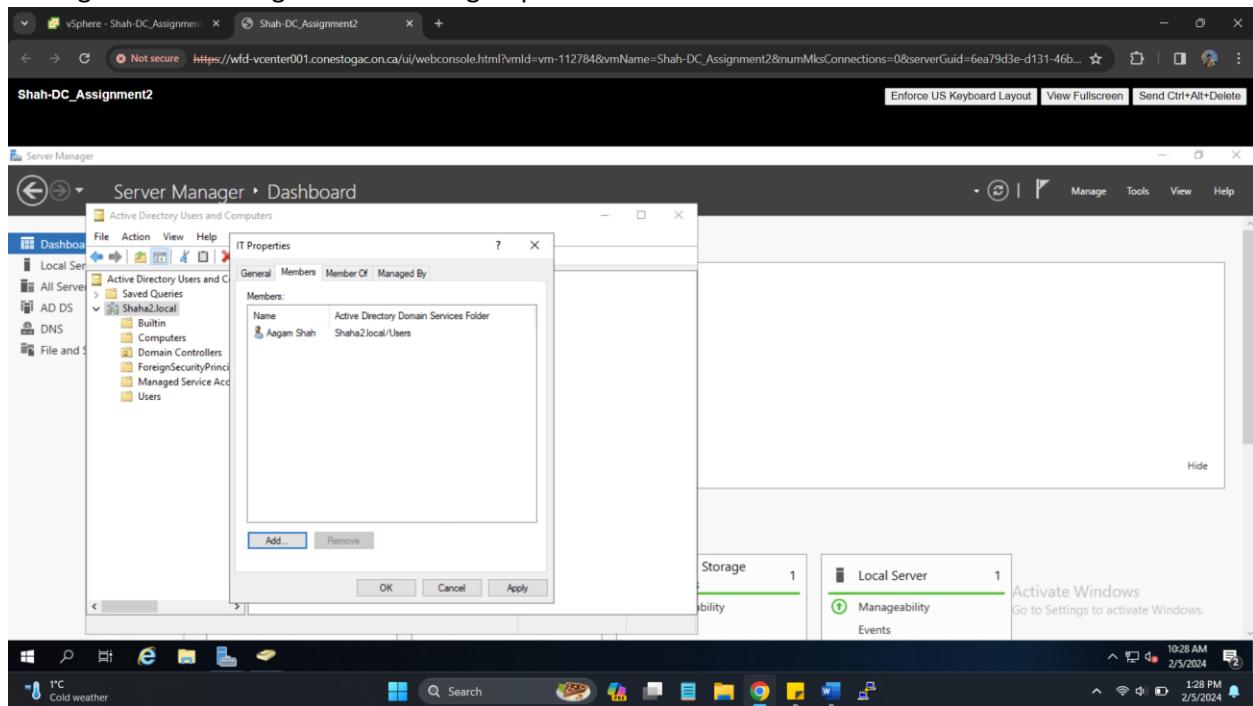
Providing password for user created.



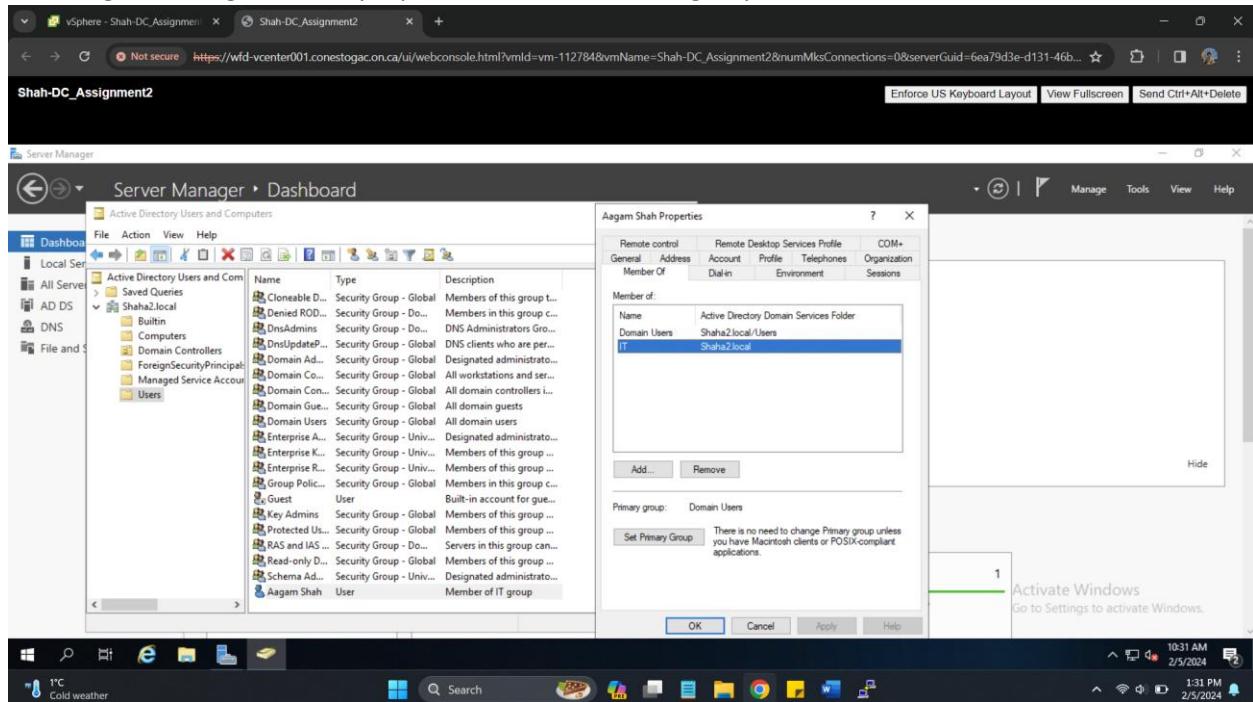
Summary of new object-user creation



Adding user name “Aagam Shah” to IT group as members

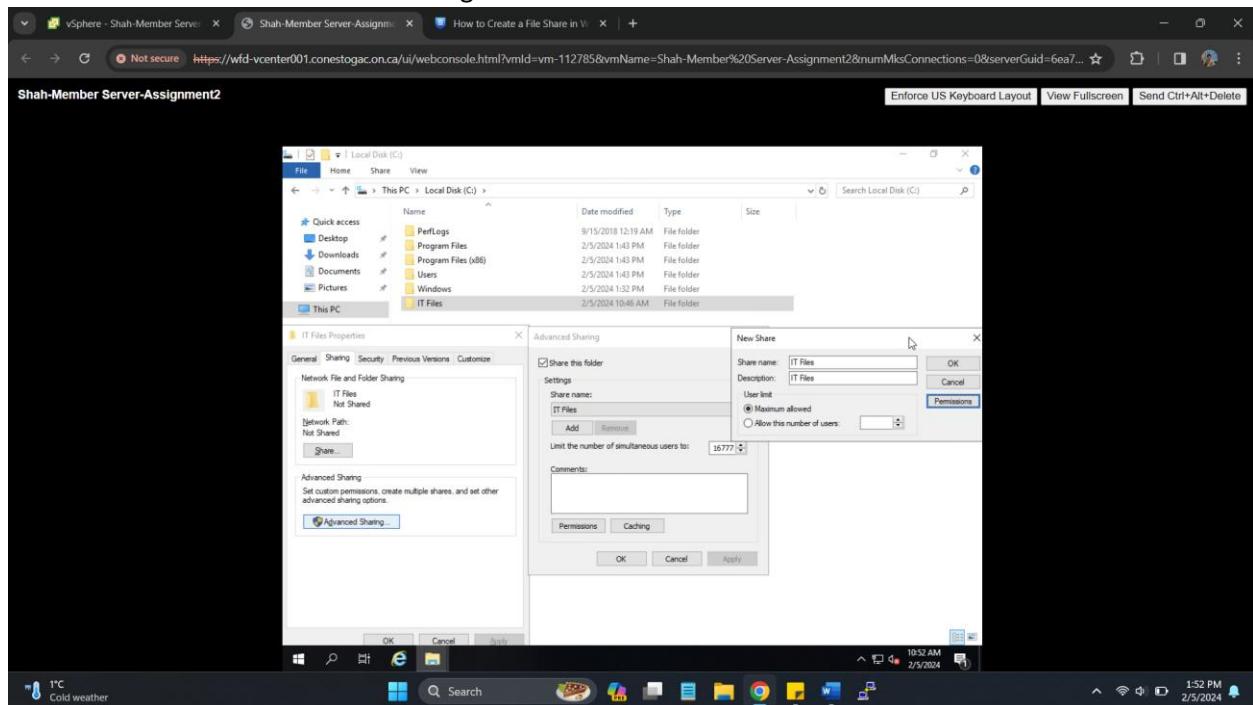


Checking User "Aagam Shah" properties as member of IT group of domain Shaha2.local

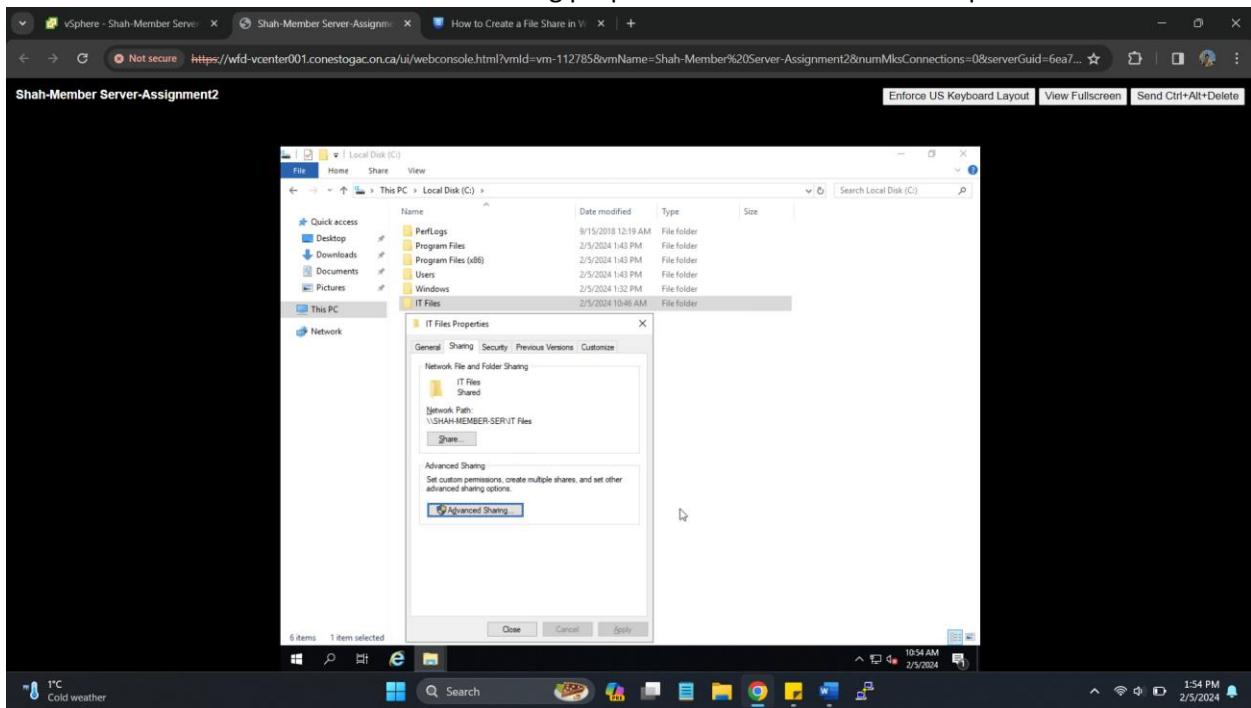


3) Create a file share on the member server called "IT Files".

Create a folder named "IT Files" and right click → properties → shaing tab → Advance sharing → select share this folder.-->Permissions to assign access

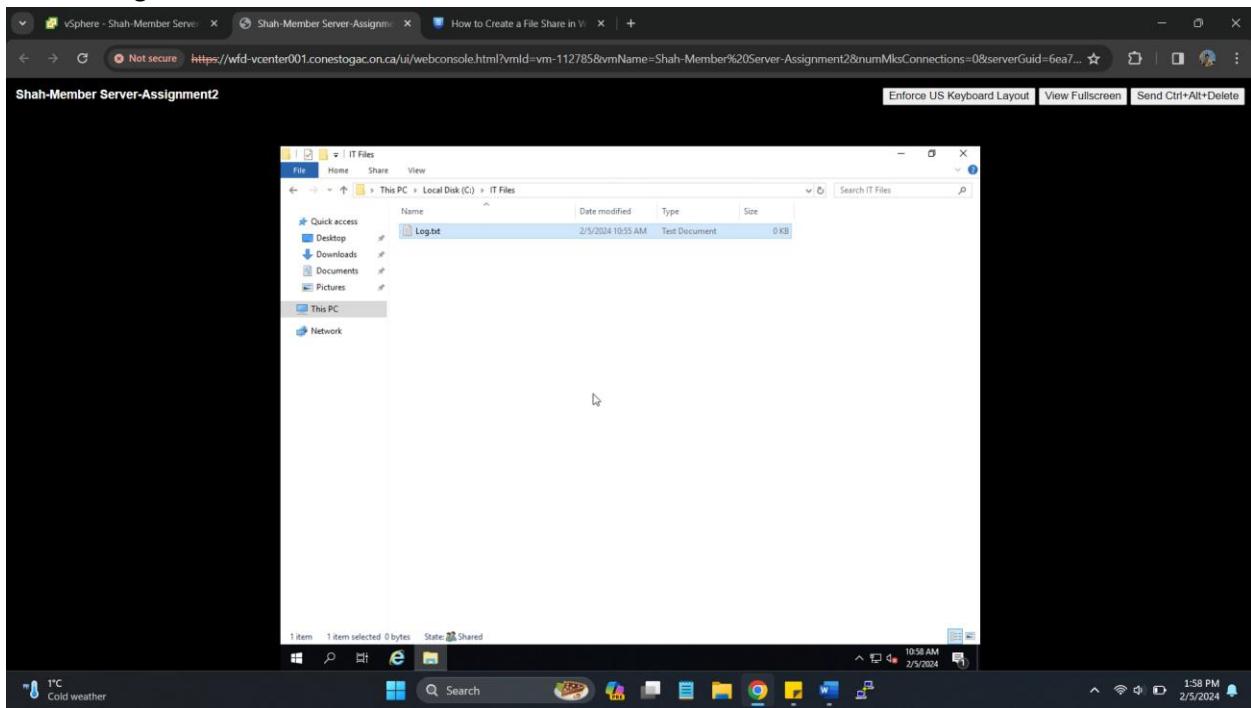


Once its a shared folder → check folder sharing properties → it will show network path



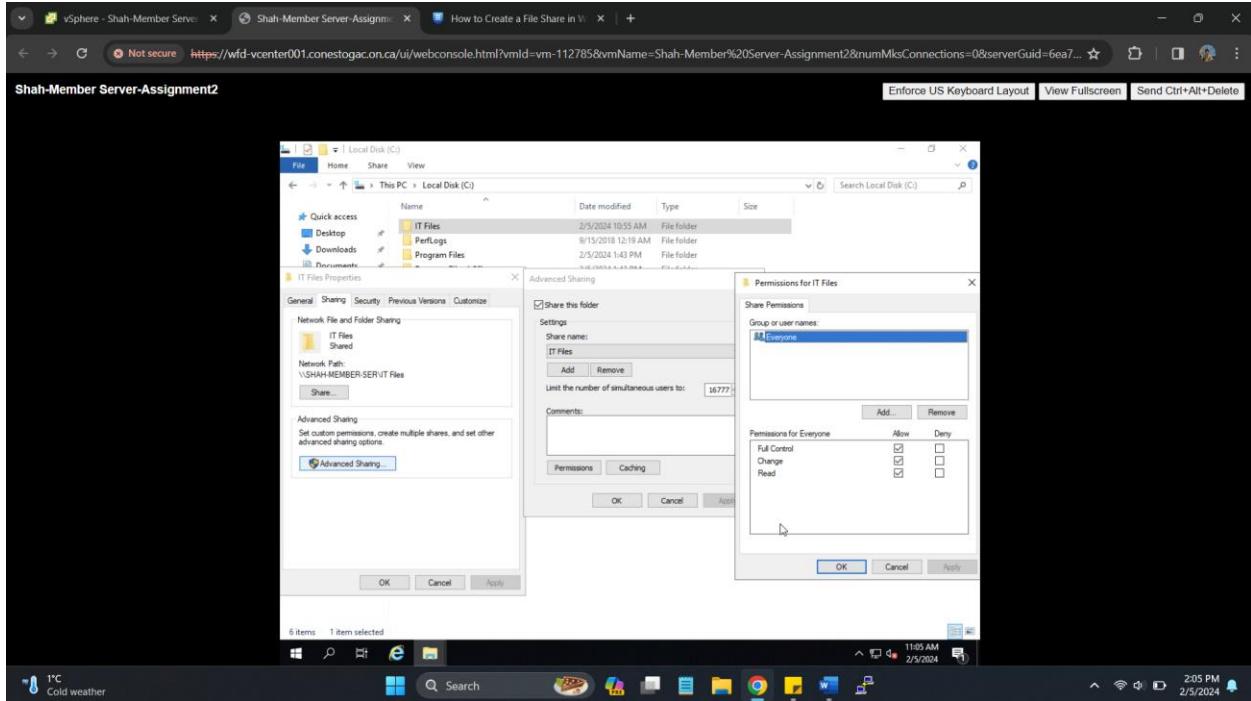
4) Create a text file in the share called log.txt.

Create a log.txt file in shared IT files folder.



5) Set the share permissions on the share to Everyone Full Control.

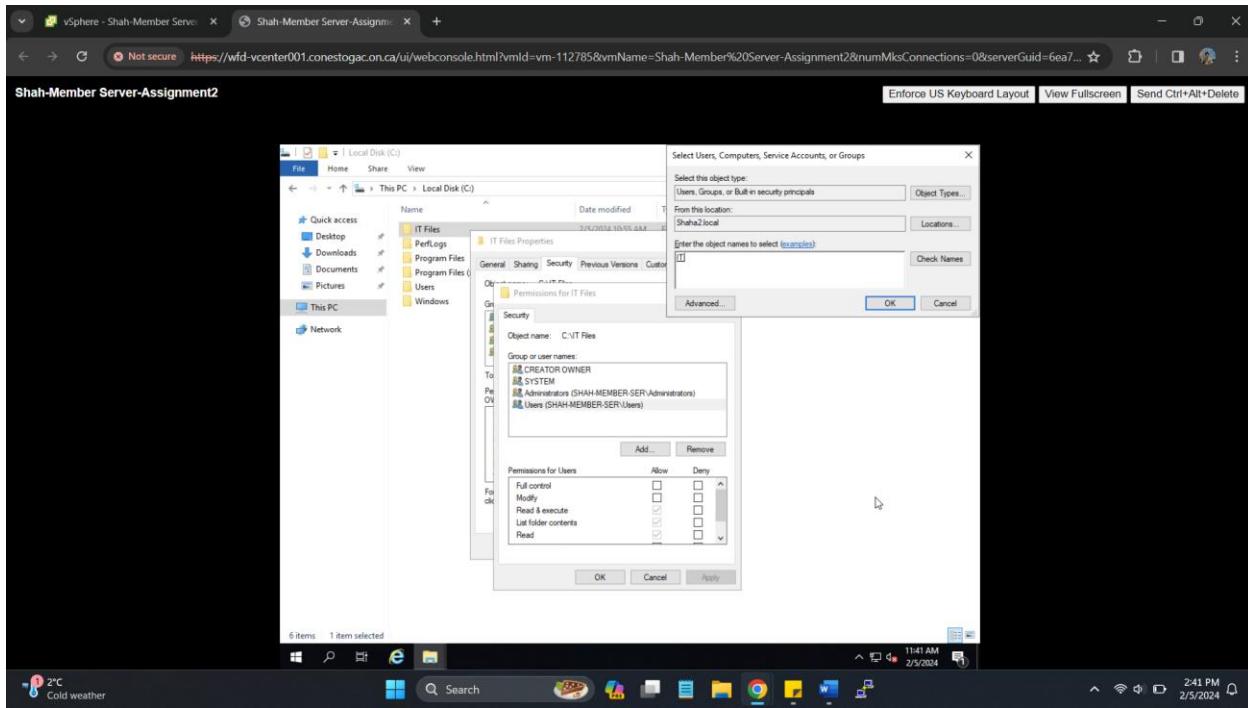
Go to properties of IT files folder → sharing tab → Advance sharing → permissions → select everyone and select full control check box → apply to provide full control access.



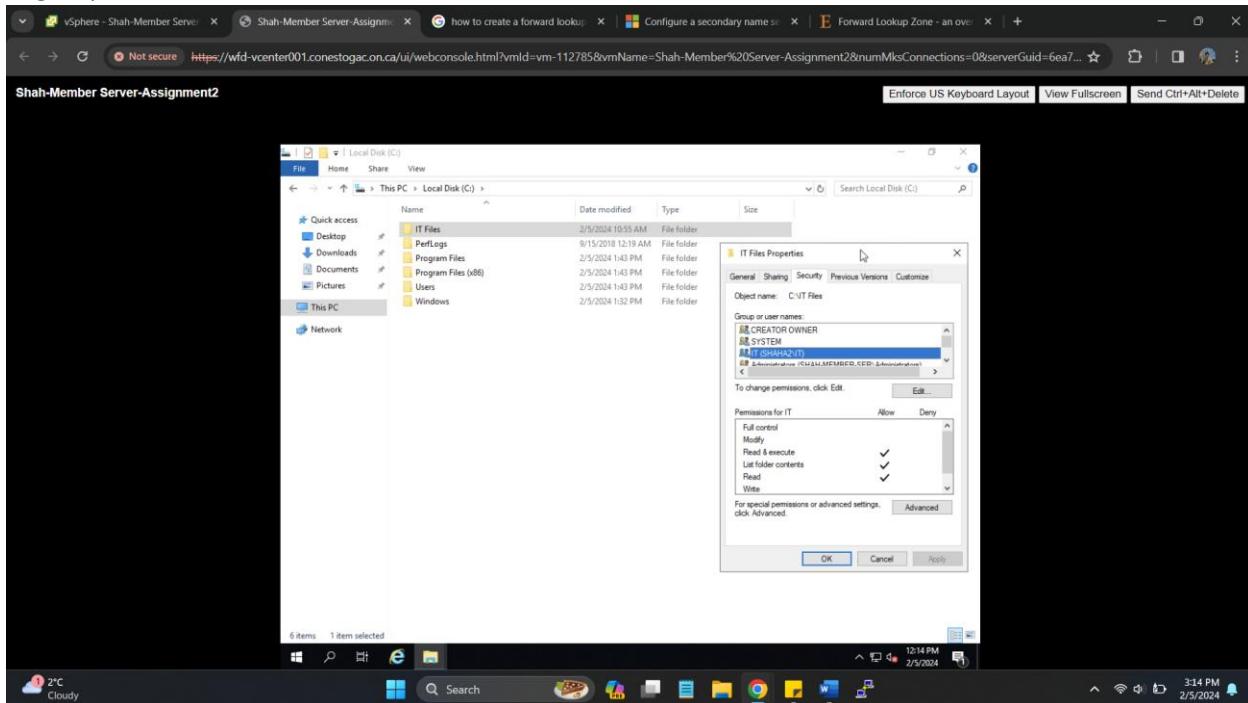
6) Set the NTFS permissions to allow only the IT group to access the share.

To allow Global security group members to access the folder

Go to IT files folder → right click properties → Security Tab → Add → enter IT as object names → OK

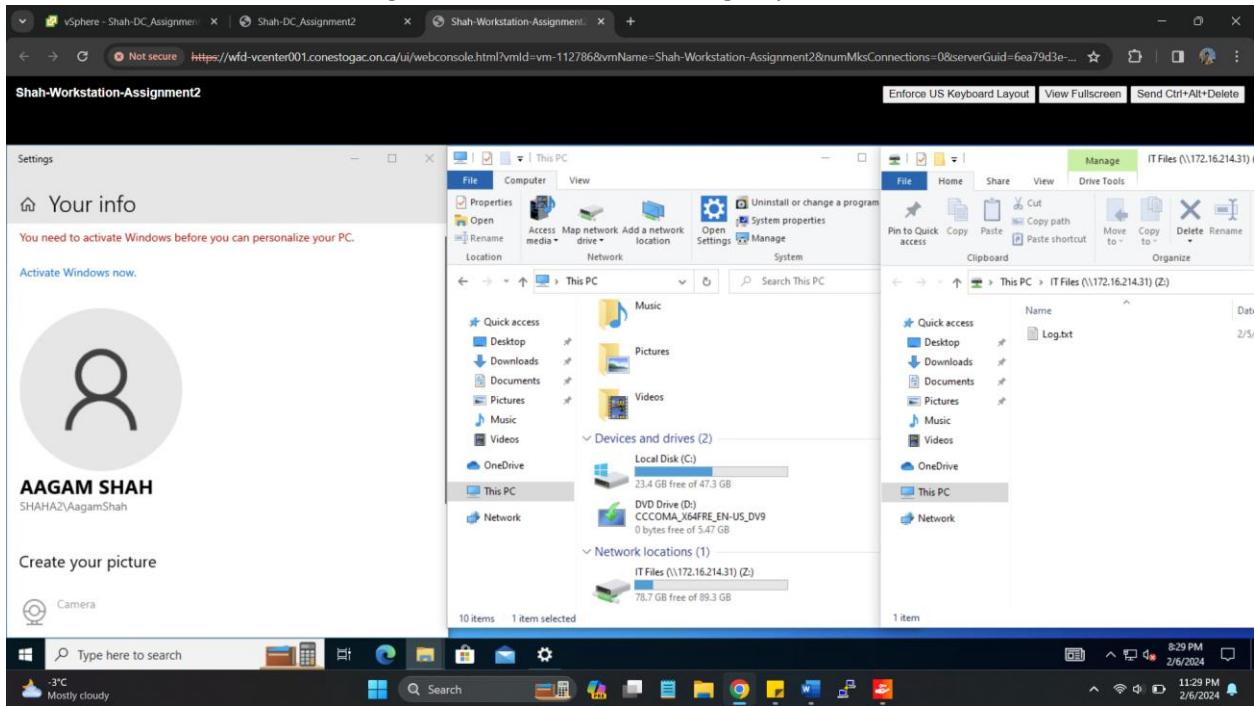


To check access provided → IT files folder → right click properties → Security Tab → Check “IT” mentioned in group and usernames



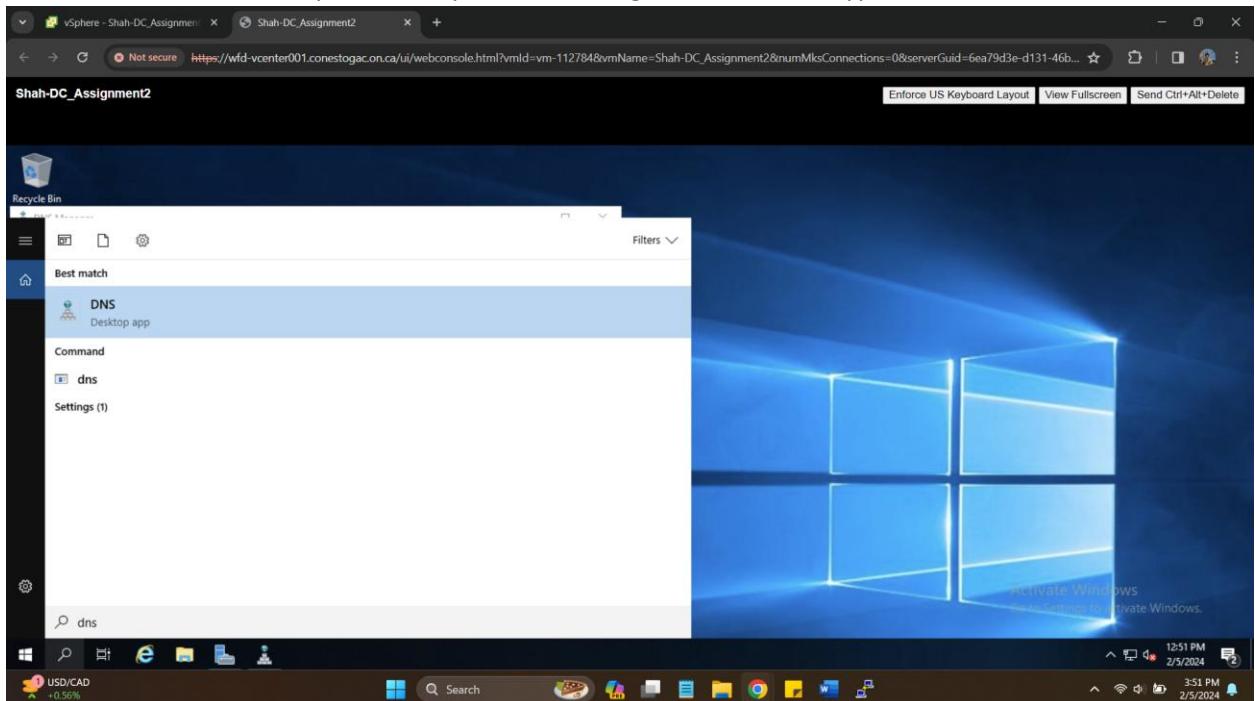
Login by Aagam Shah user AD ID → add sharing Folder as IT Files → and check file Log.txt available in it,

User can access file, because Aagam Shah is a member of IT group.

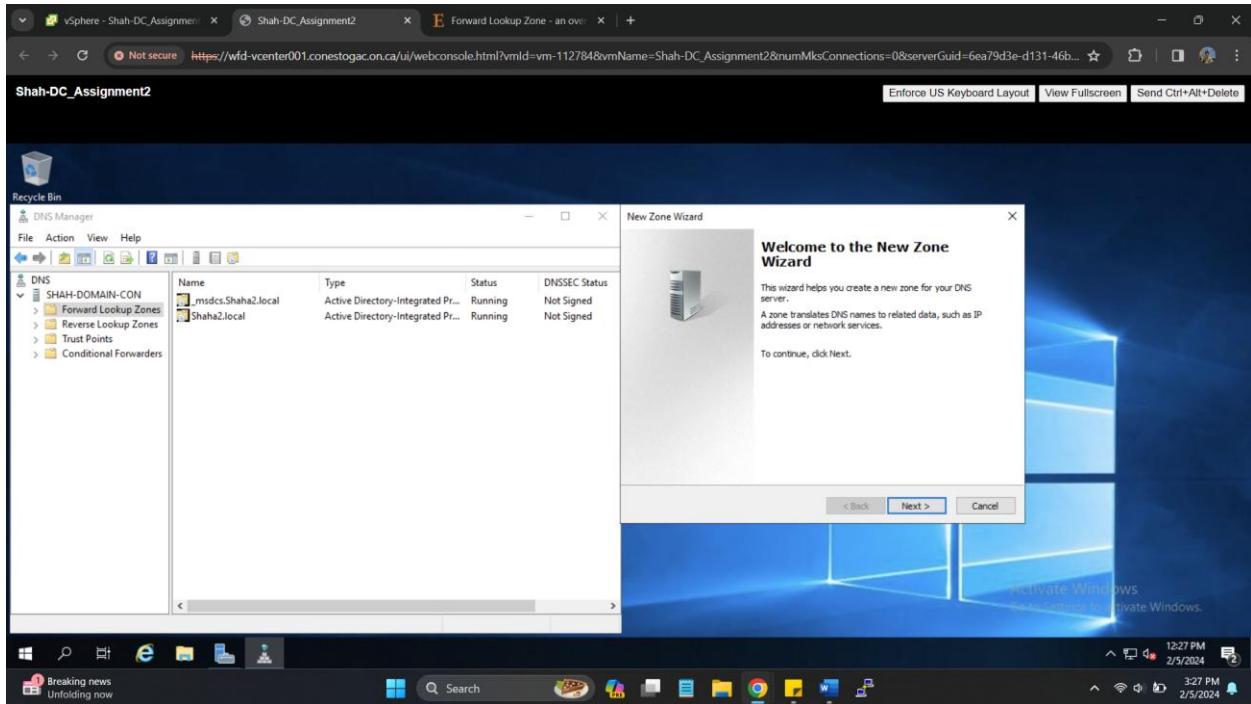


7) Create a forward lookup zone named acme.local.

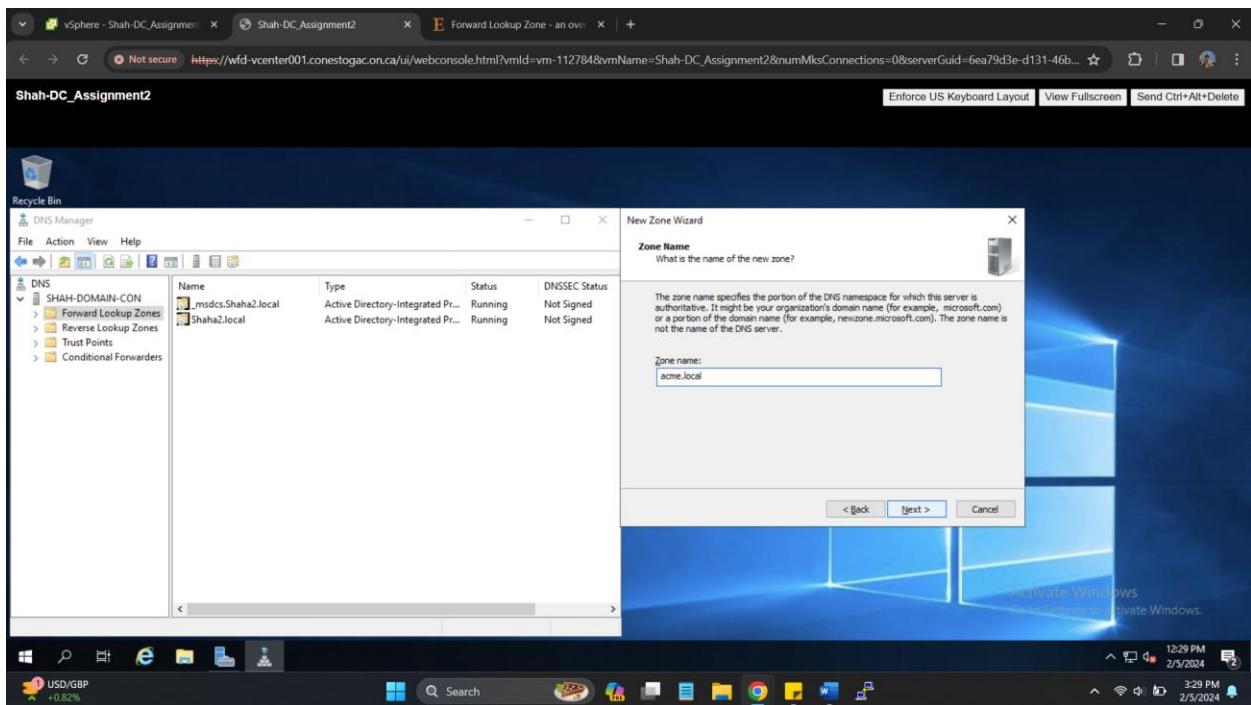
To create a forward lookup zone → open DNS Manager from Start or type DNS in search bar



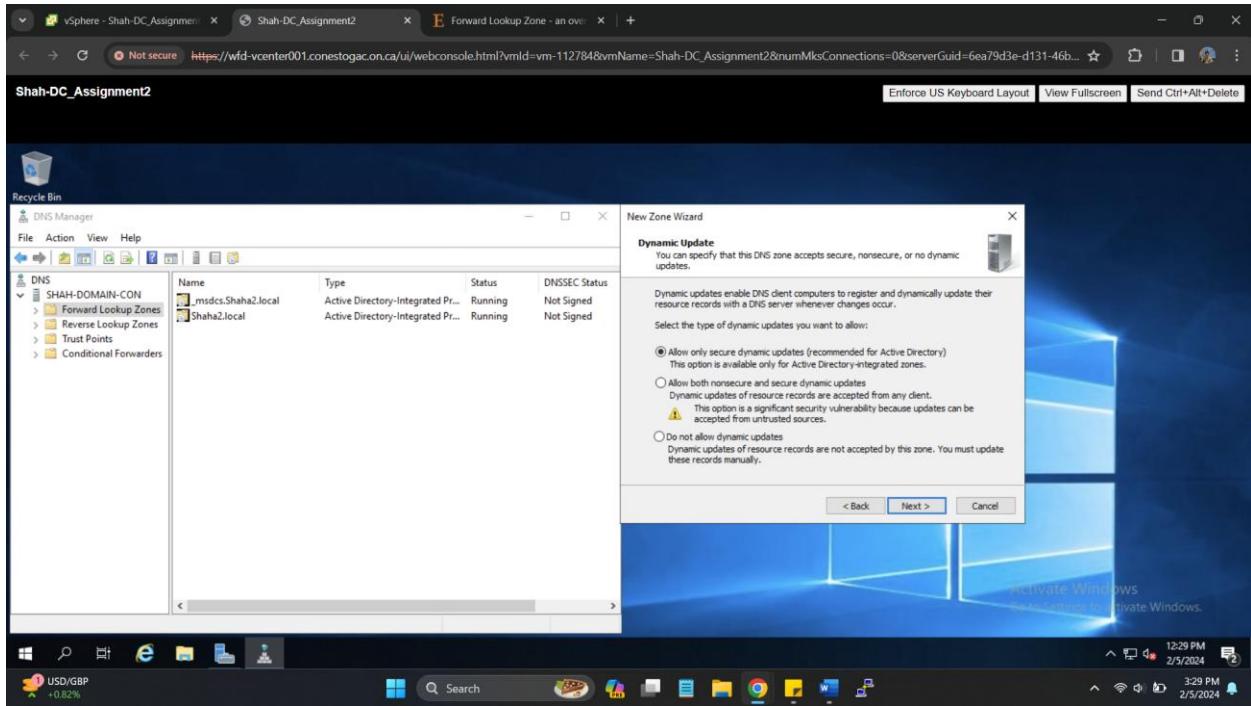
Go to DNS Manager → Under DNS → Select your domain "SHAH-DOMAIN-CON" → Forward Lookup zones → Right click create new zone → next



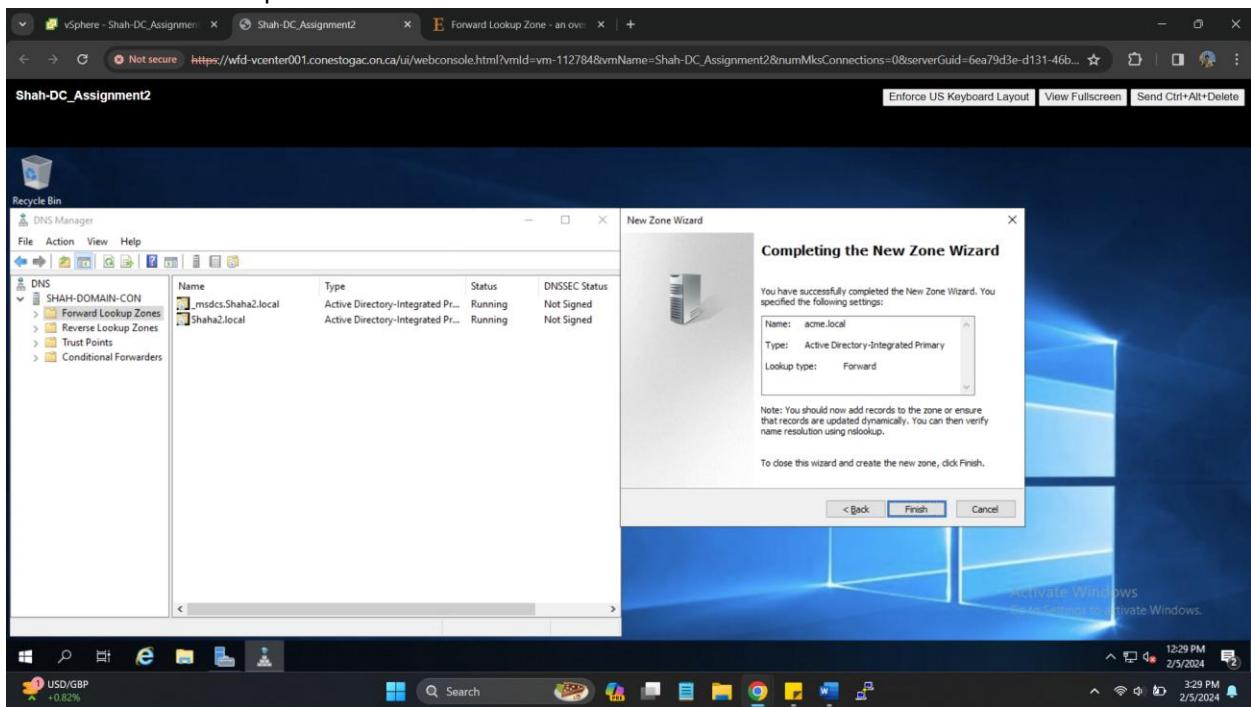
Provide Zone name as "acme.local"



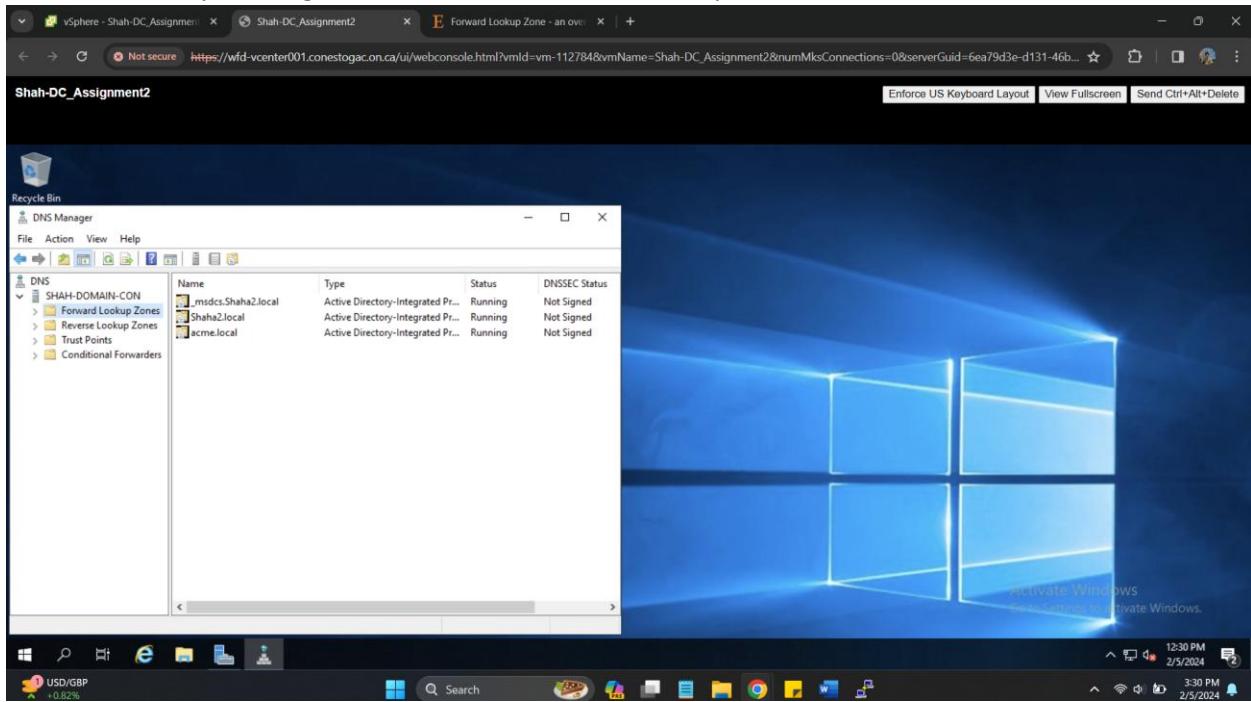
Select dynamic update option as allow only secure updates



Click on Finish to complete the new zone creation wizard

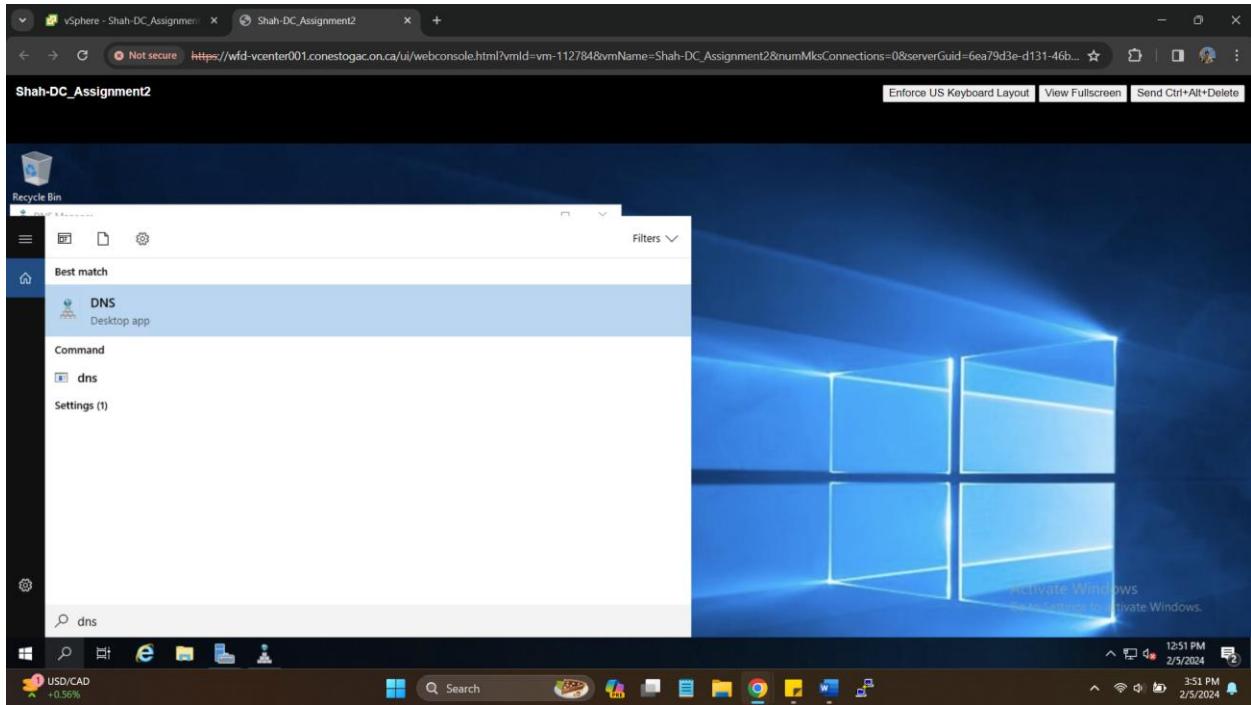


After successfully creating acme.local zone in forward lookup zone it will show listed in name.

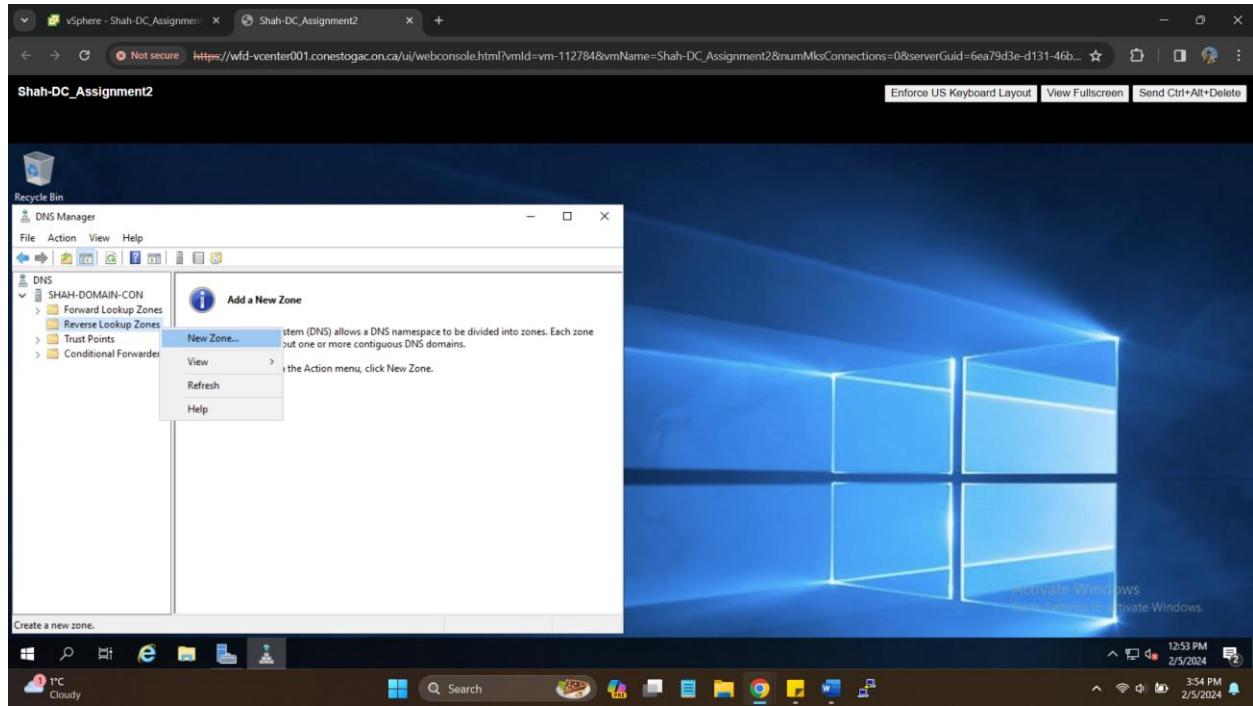


8) Create a reverse lookup zone for your com port IP range.

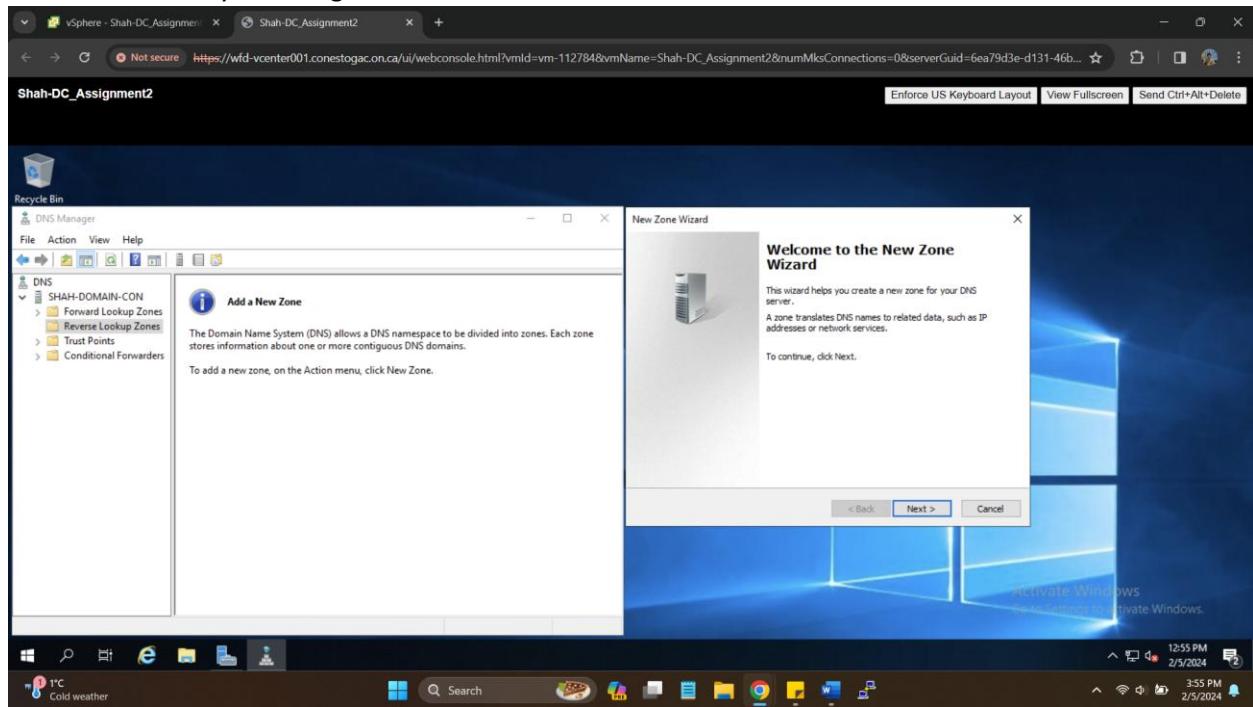
To create a reverse lookup zone, open DNS app



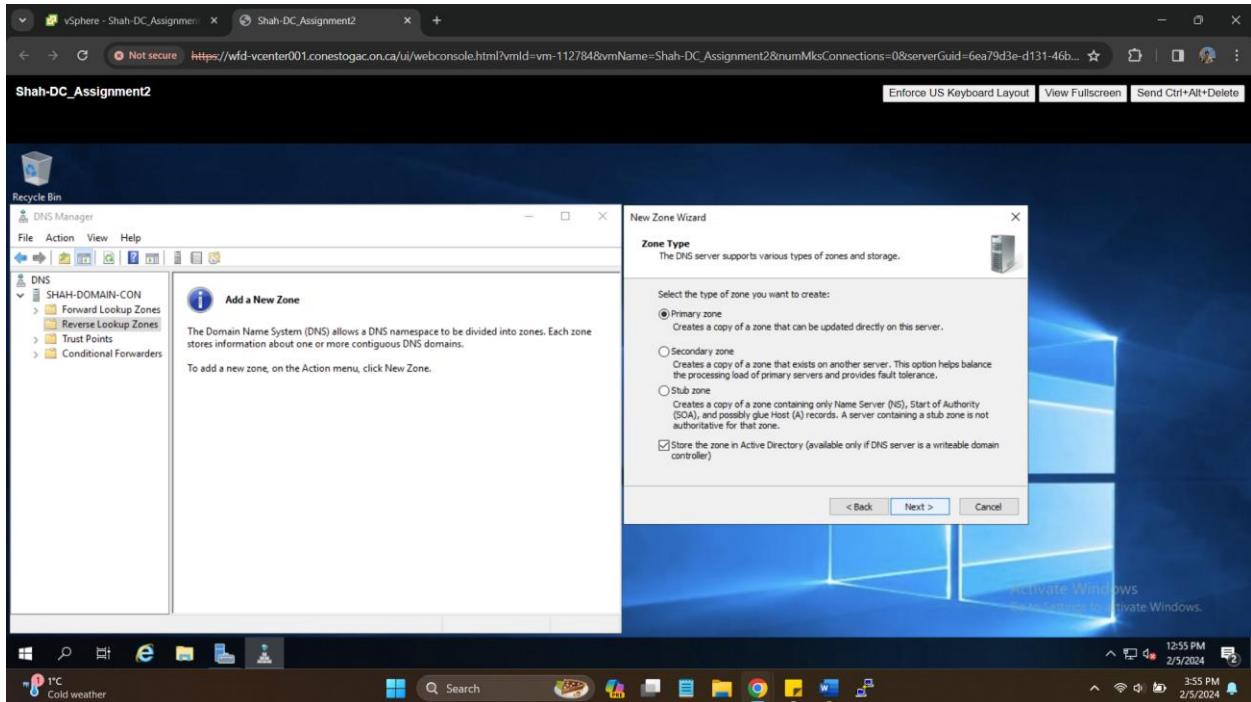
Go to DNS → Shah-Domain-Con → Reverse lookup zones → Create new zone



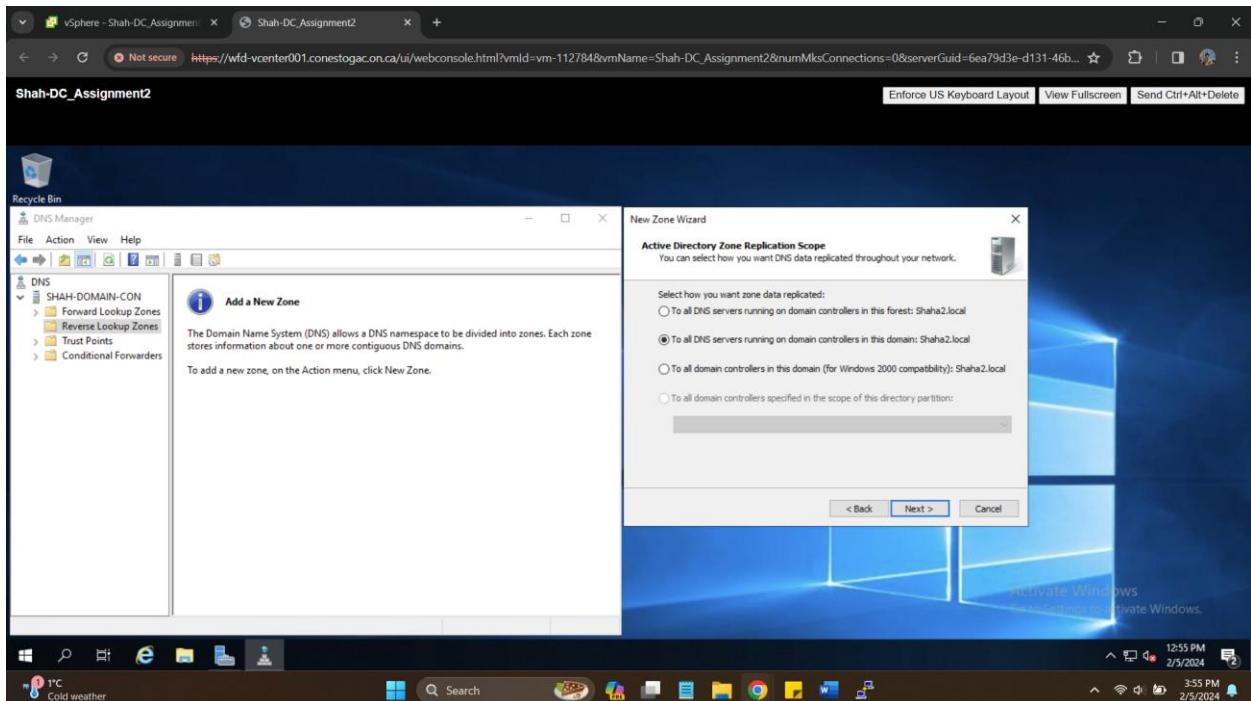
Add a new zone by selecting next in wizard



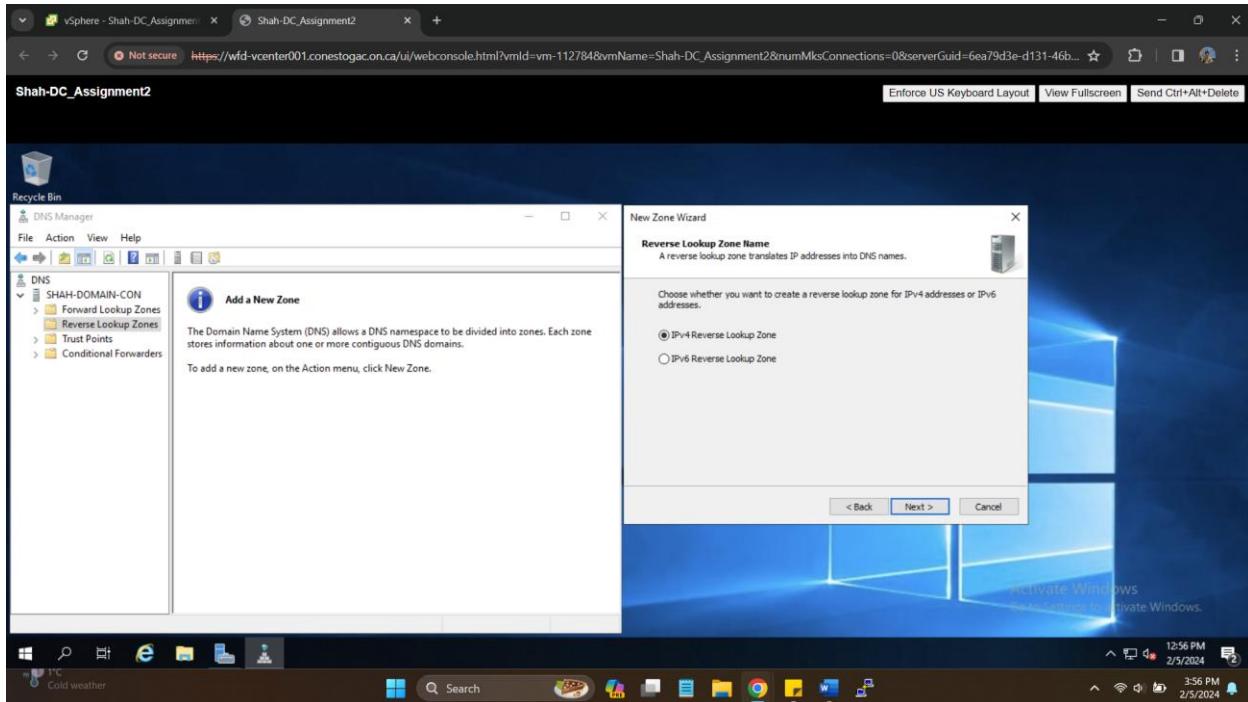
Select type of zone as primary zone



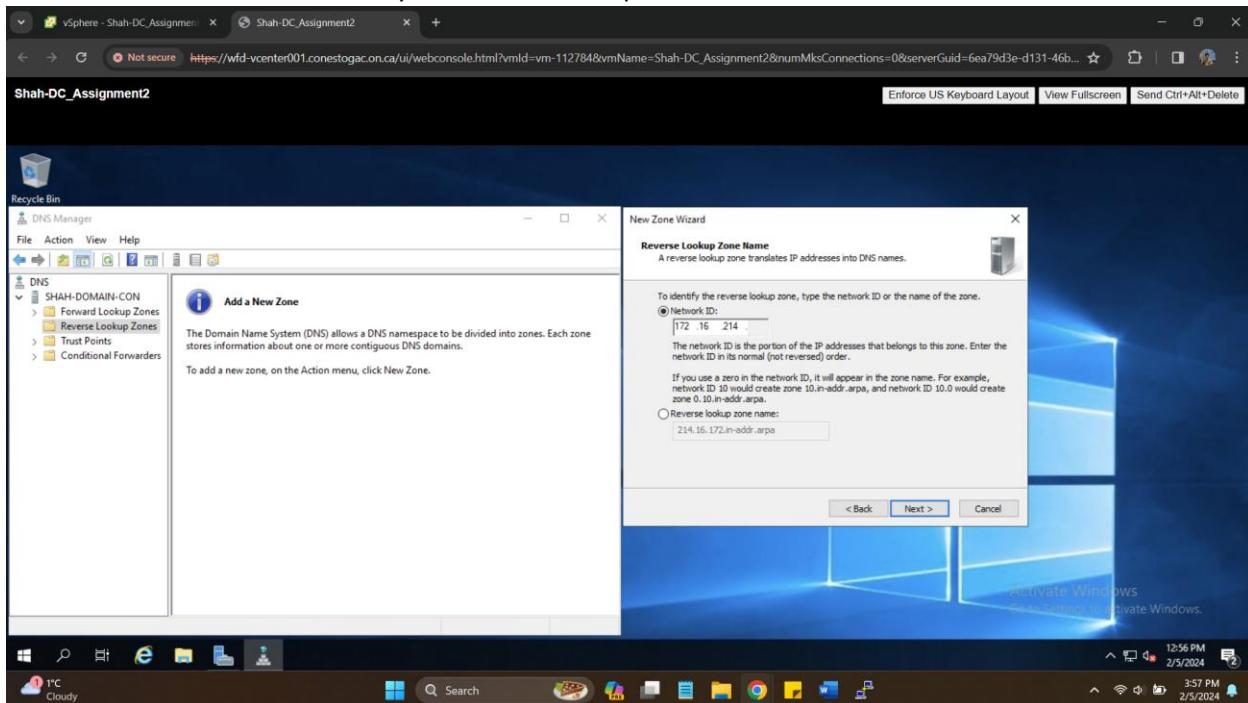
Select AD zone replication scope to all DNS servers running on domain controllers in the domain: Shaha2.local and select next



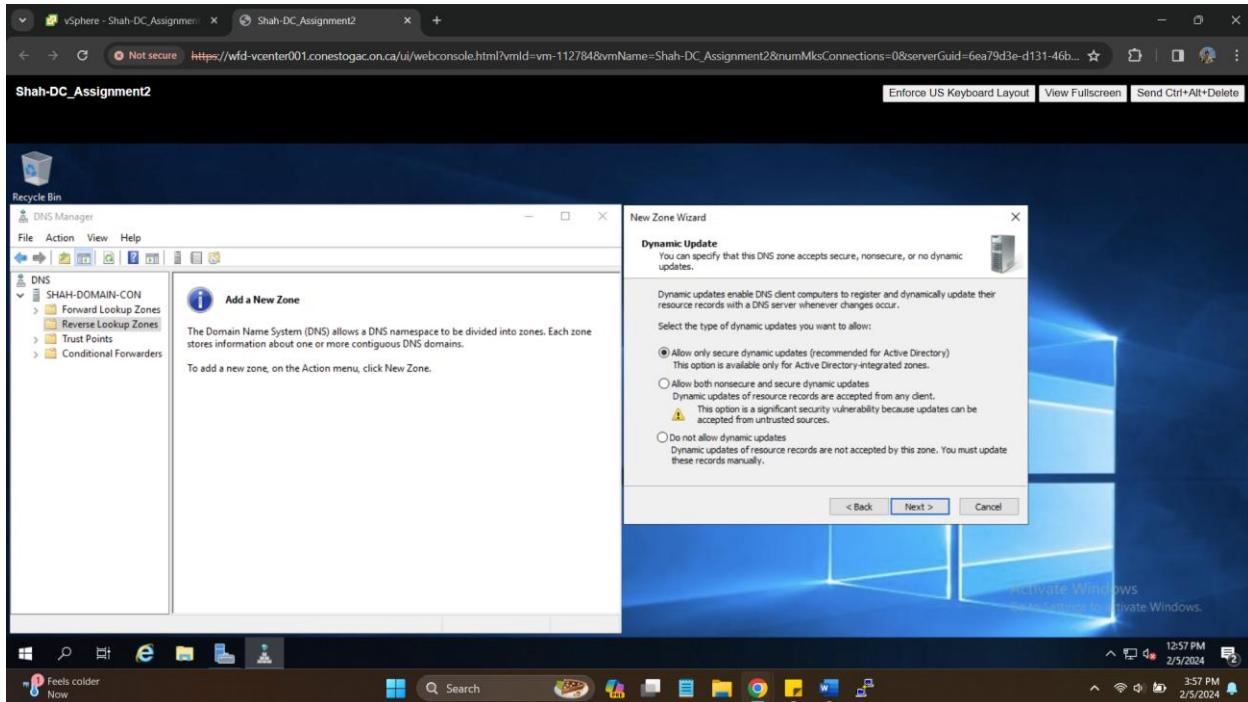
Select IPv4 reverse lookup zone and select next



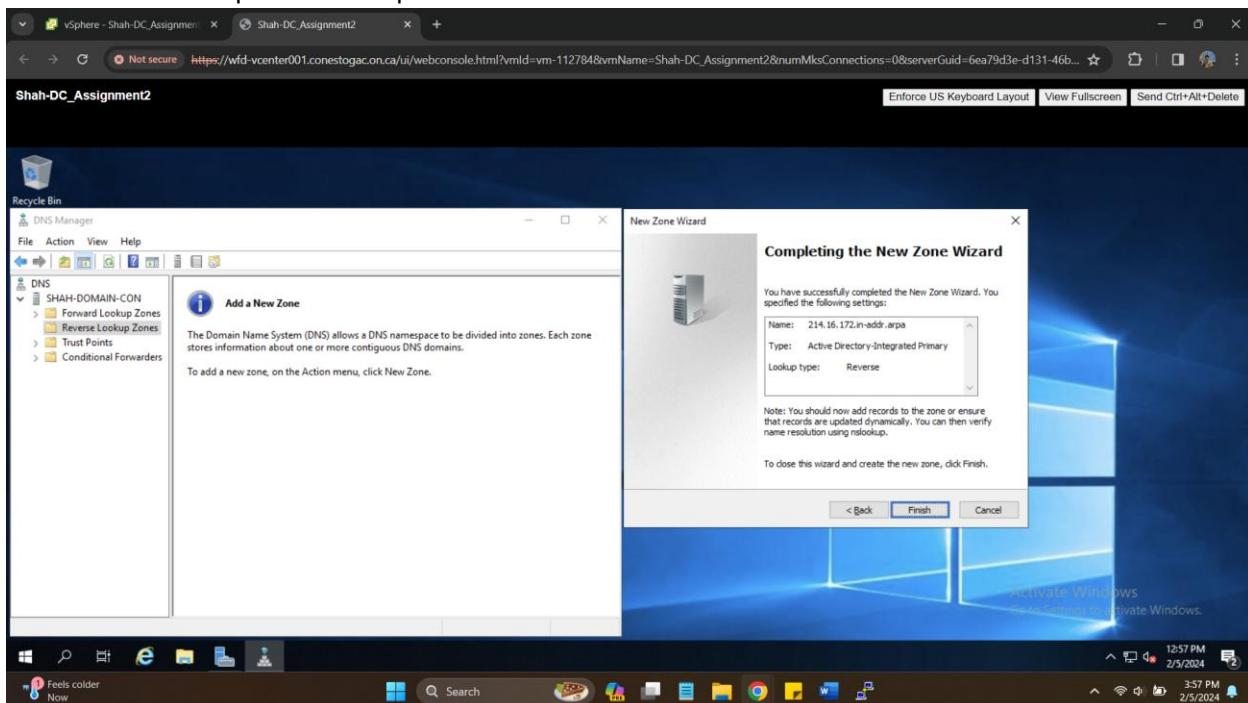
Provide the network ID to identify the reverse lookup zone



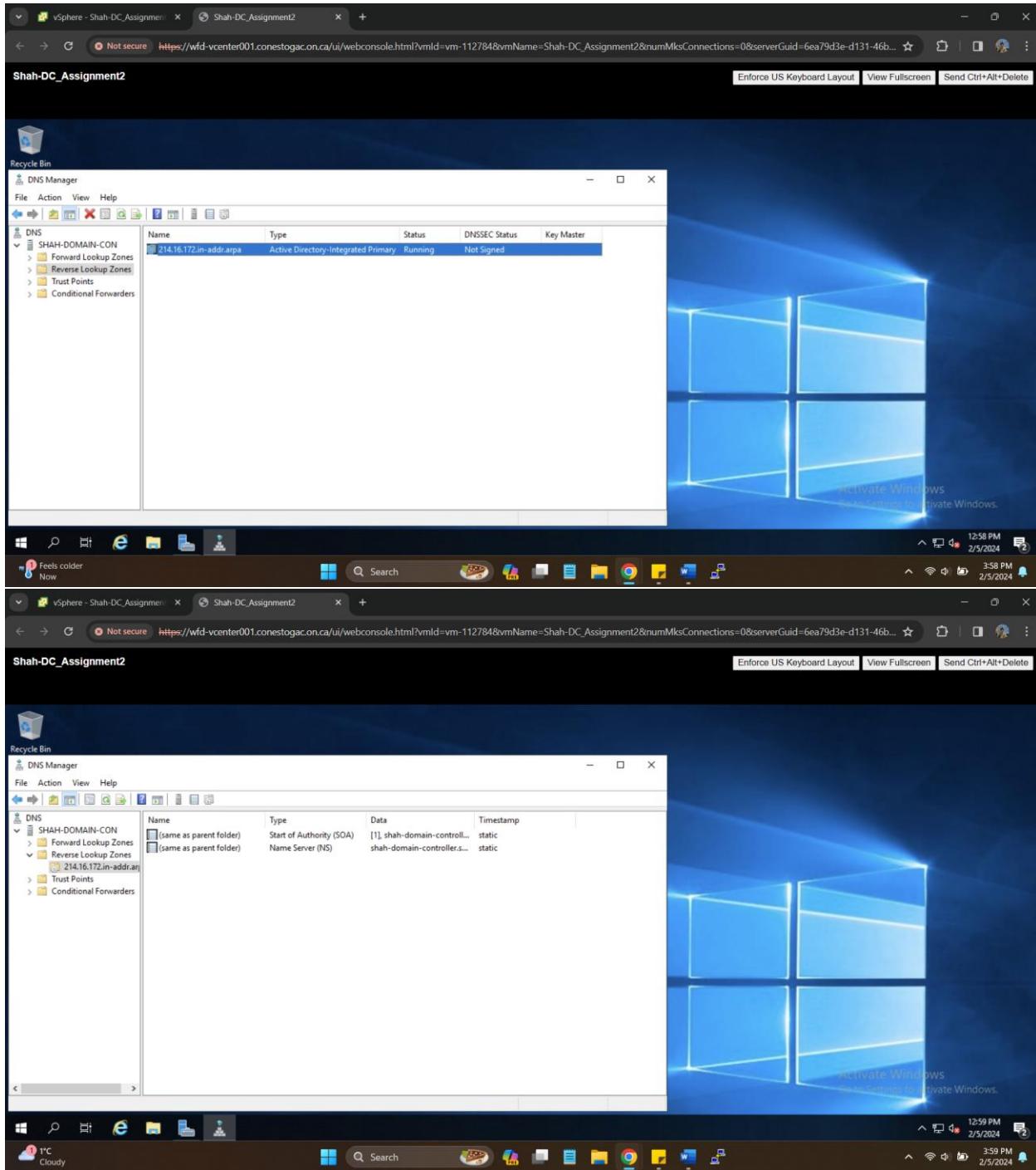
Select option add zone to allow only secure updates



Once reverse lookup zone is completed click on finish



Inside Reverse lookup zone, there will be entry of zone created.



9) Install and configure the DHCP Role with the below scope.

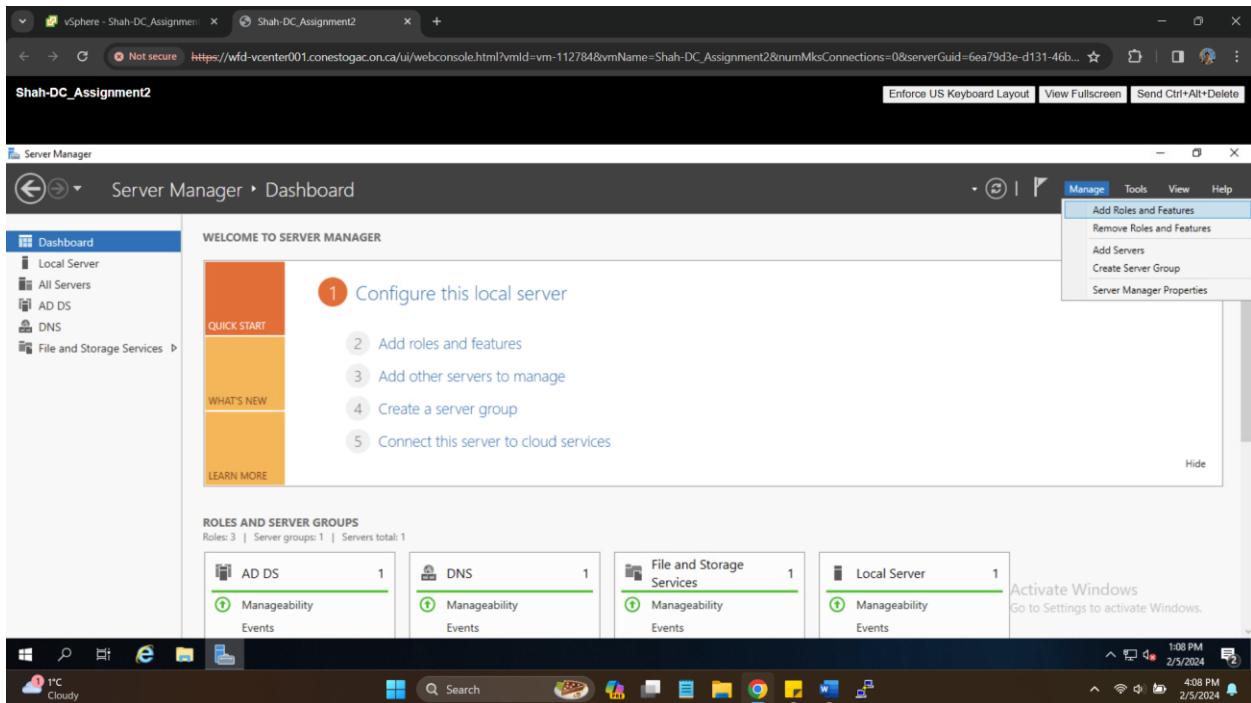
Scope – 172.17.x.40 – 172.17.x.60 → 172.16.214.40 – 172.16.214.60

GW – 172.17.x.1 → 172.16.214.1

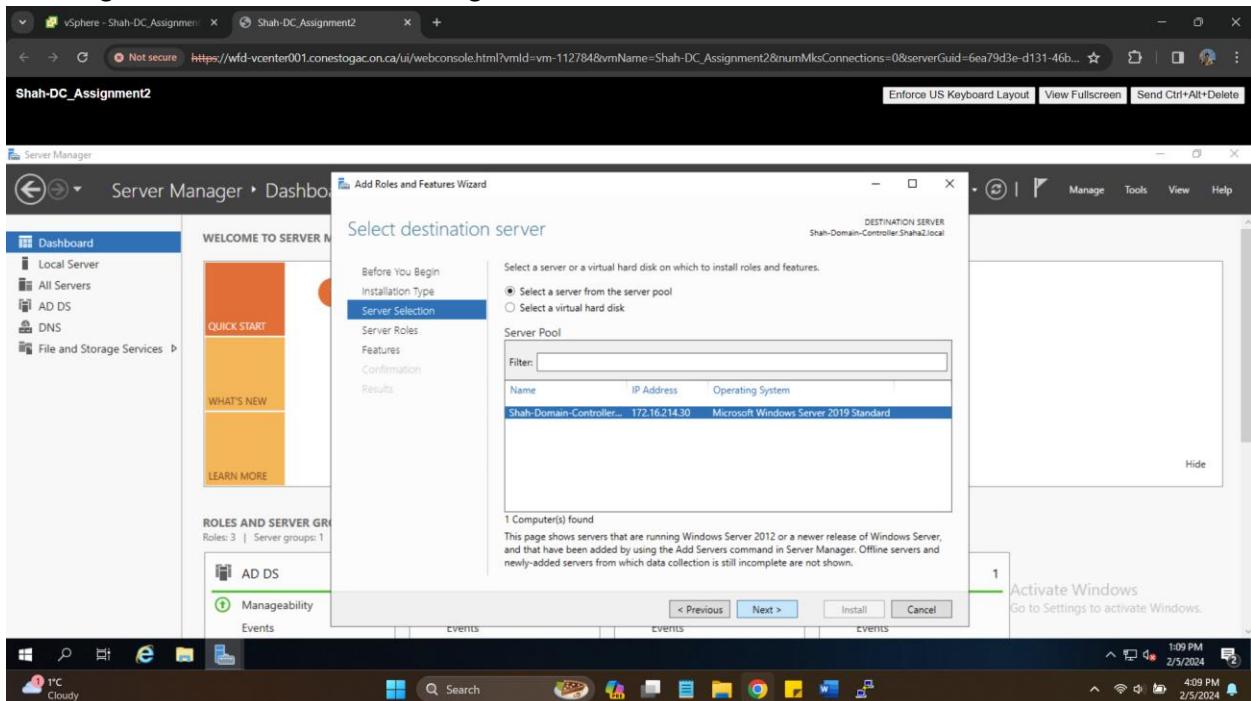
DNS – Domain Controller IP: 172.16.214.30

X = Com port number = 214

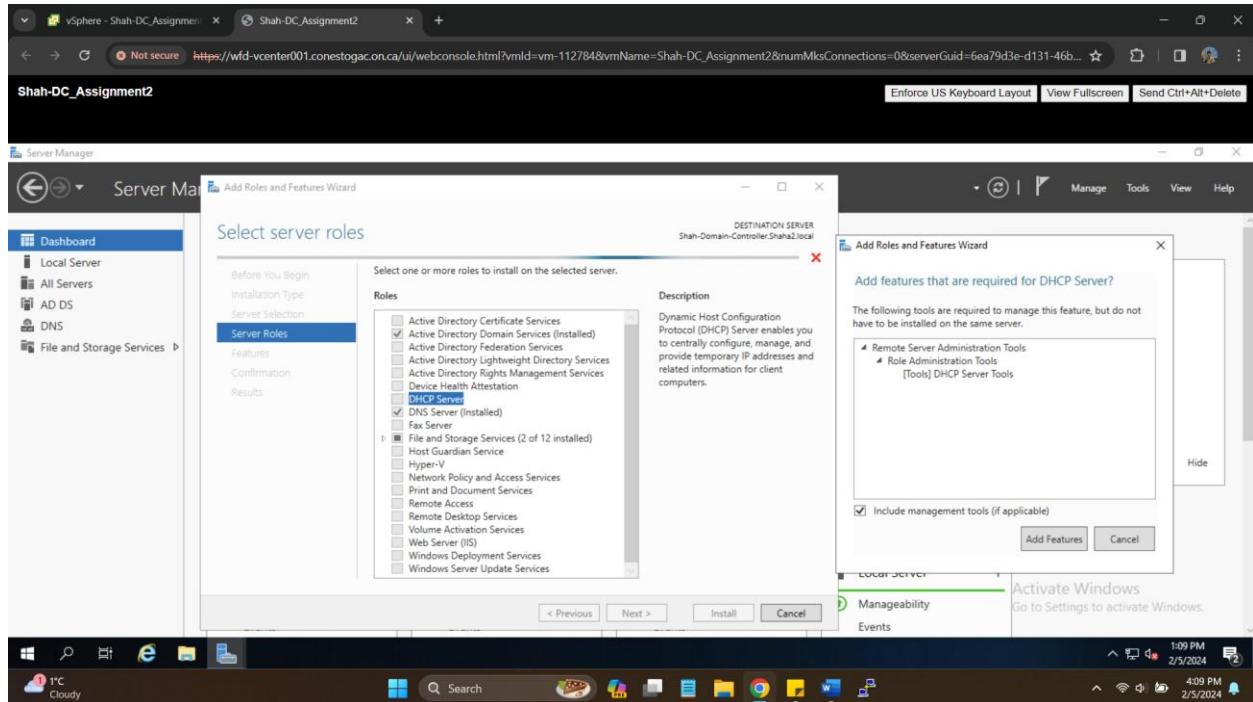
Adding Roles and Features for installing DHCP services on Domain Controller



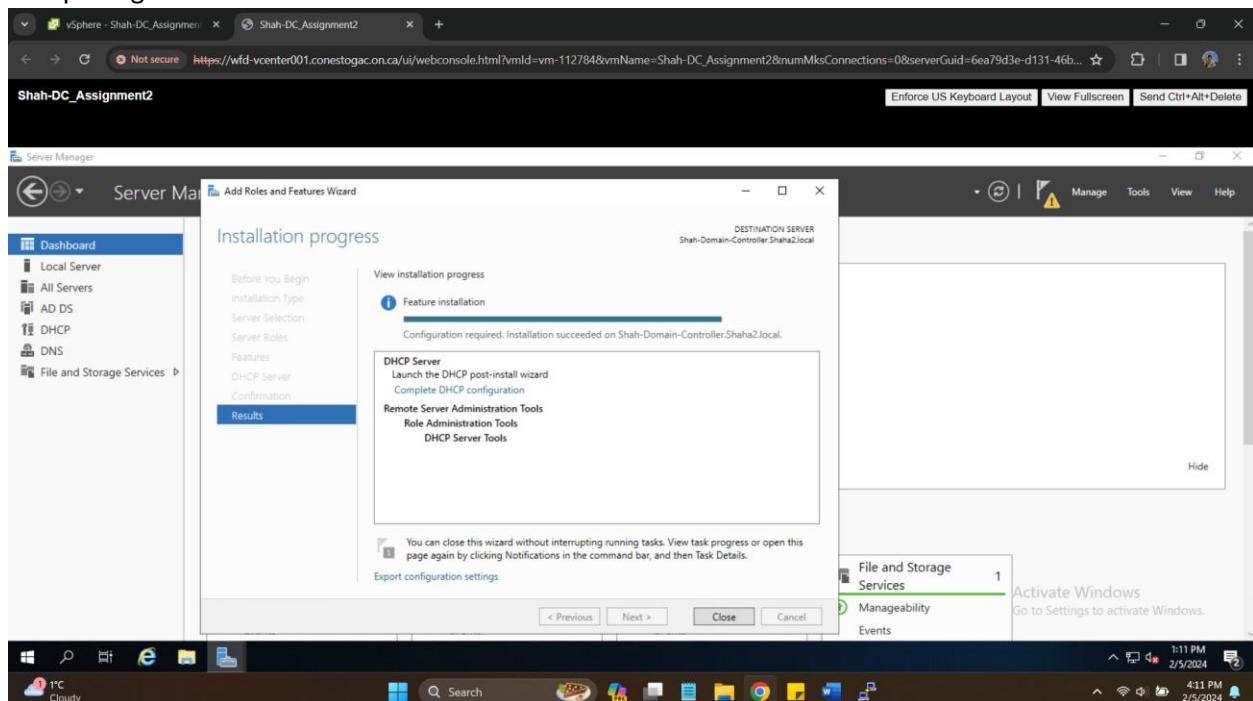
Checking the server selection for adding role and features on server



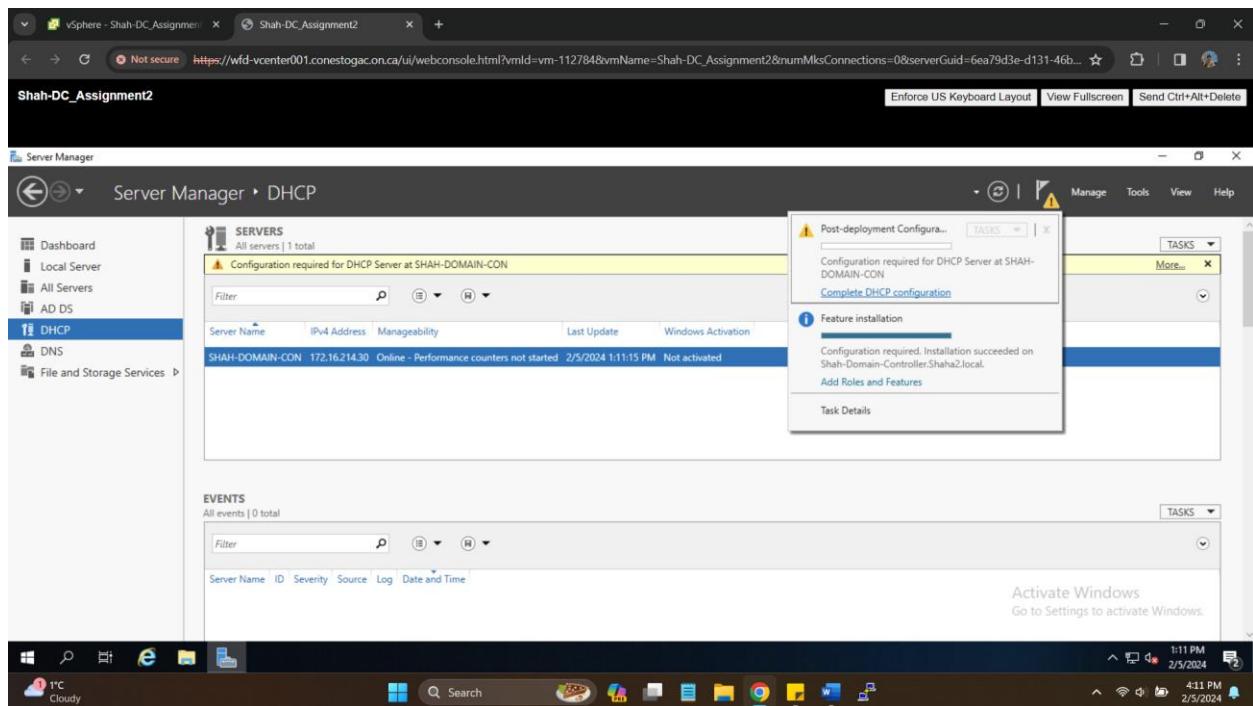
Selecting DHCP role on Domain controller to add feature



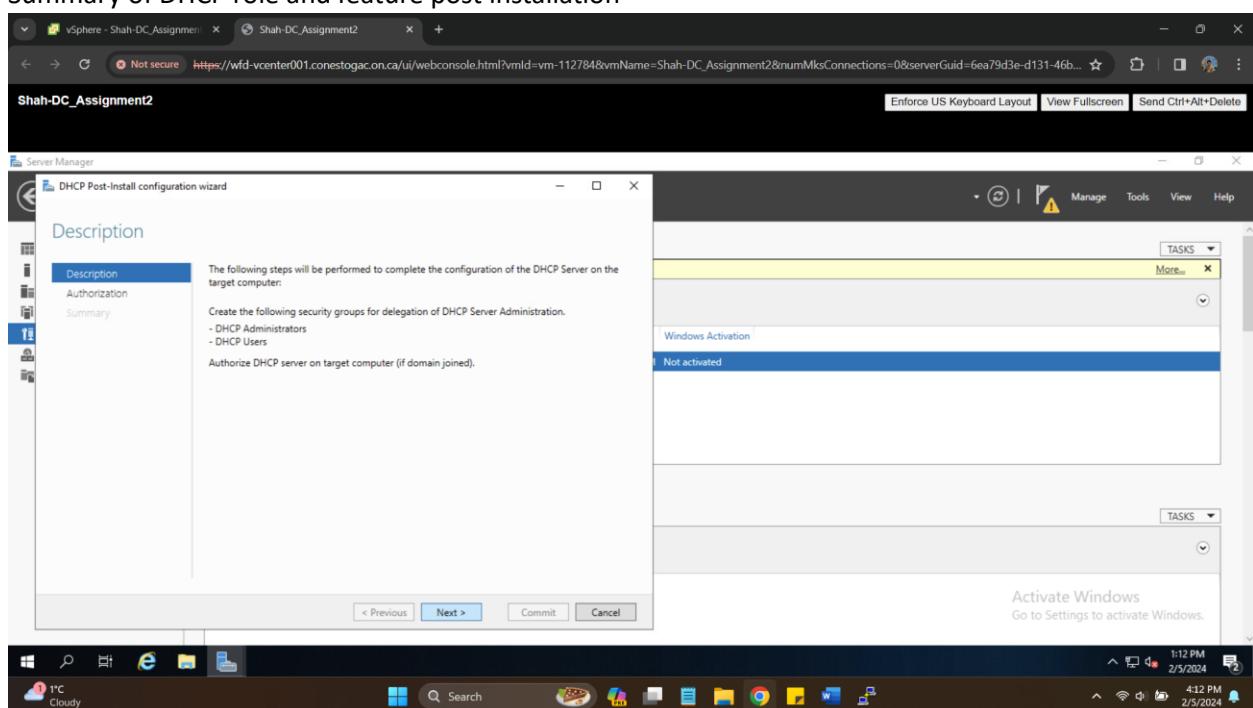
Completing DHCP roles and features installation on Domain Controller



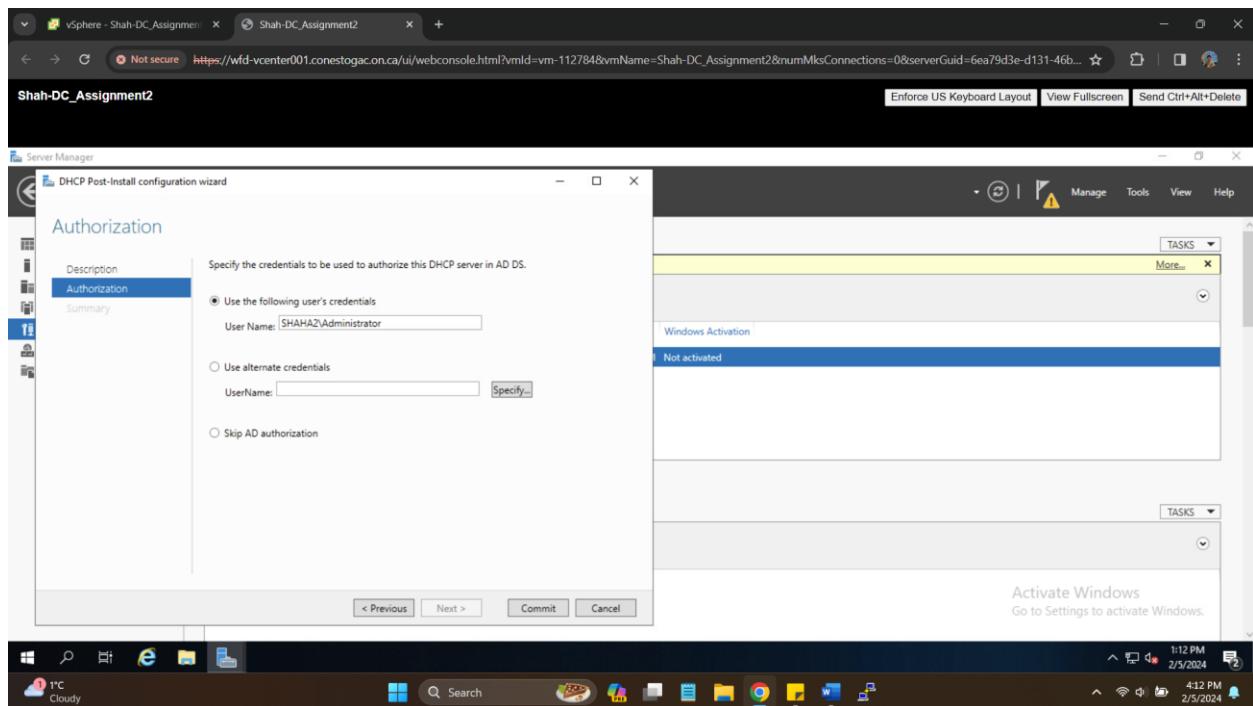
Checking DHCP installation status on the Domain Controller



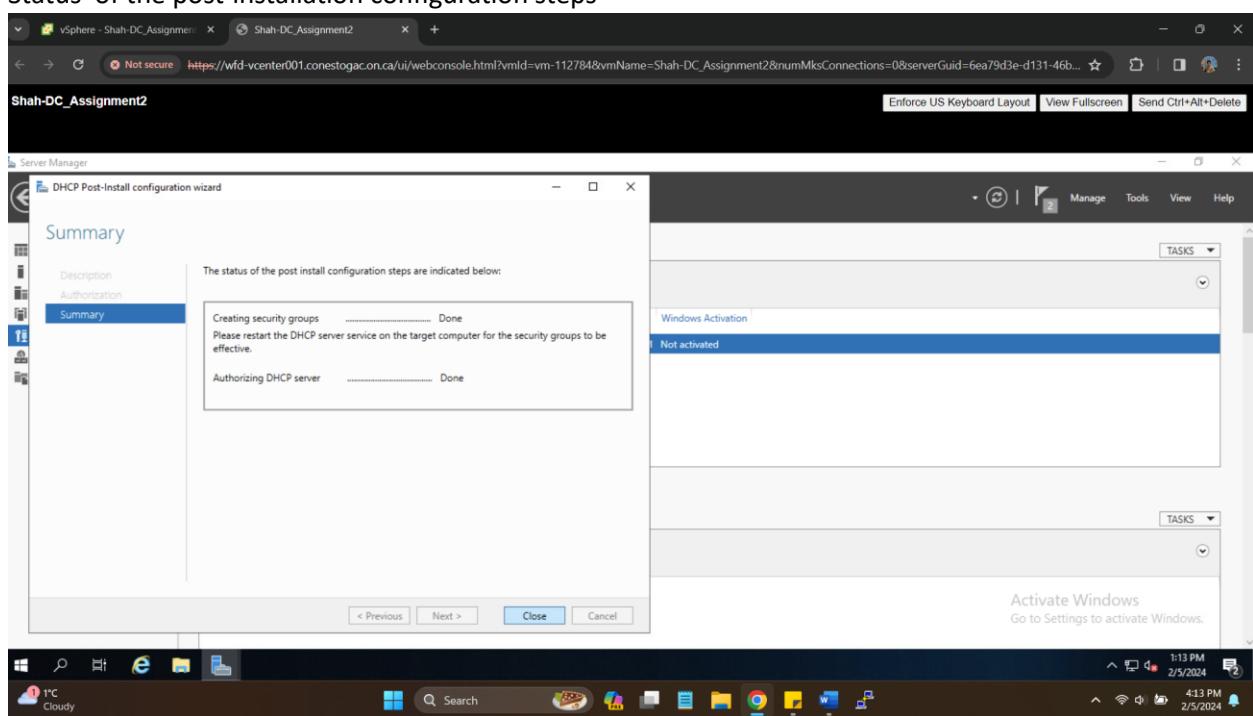
Summary of DHCP role and feature post installation



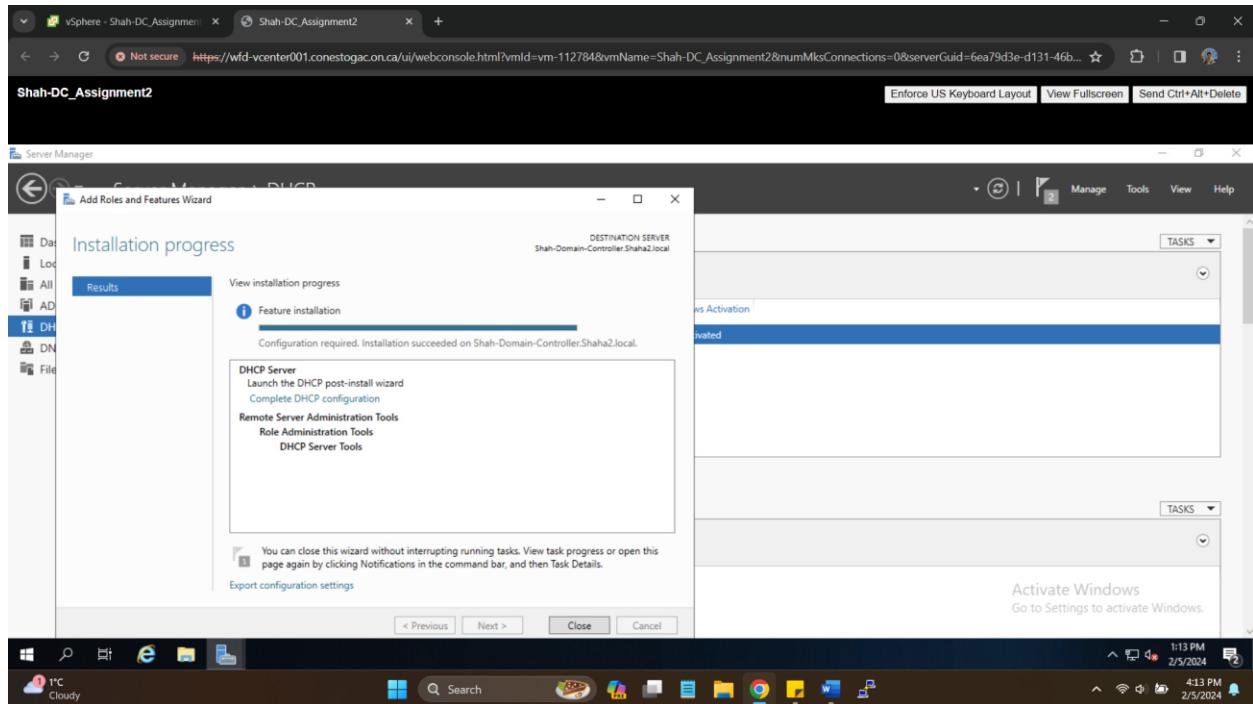
Providing Username to be used to authorize DHCP server in ADDS



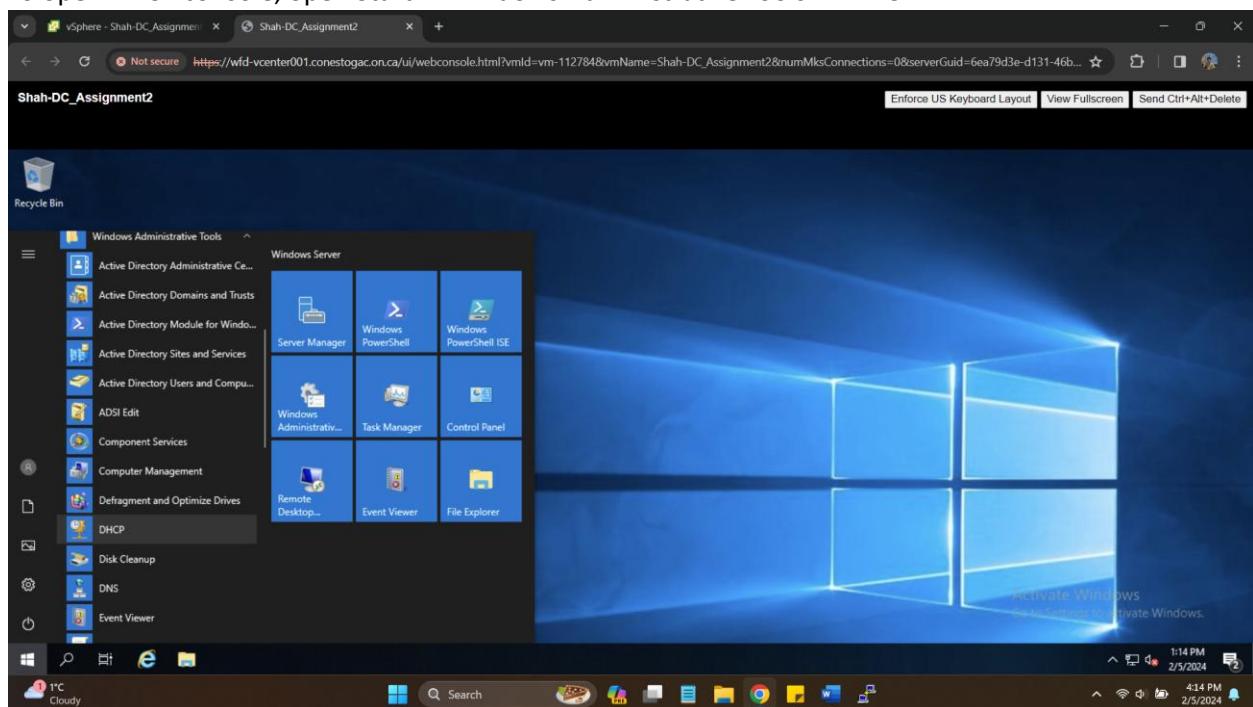
Status of the post-installation configuration steps



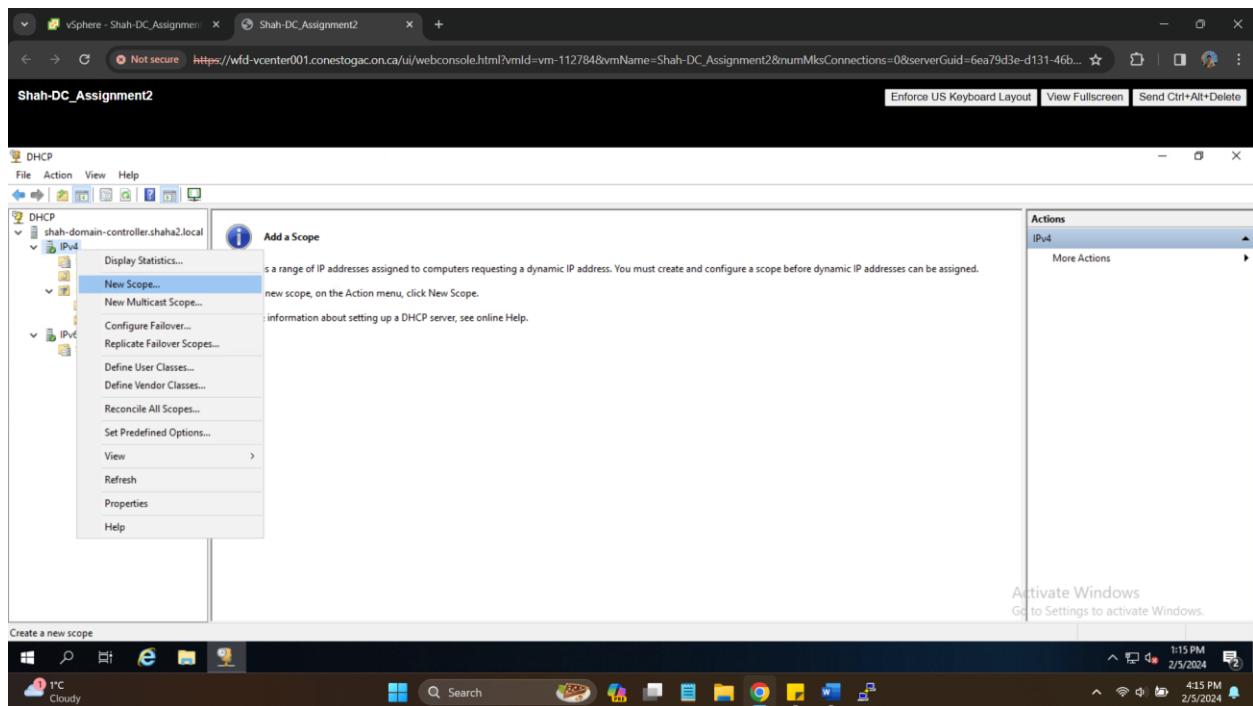
DHCP Feature Installation progress



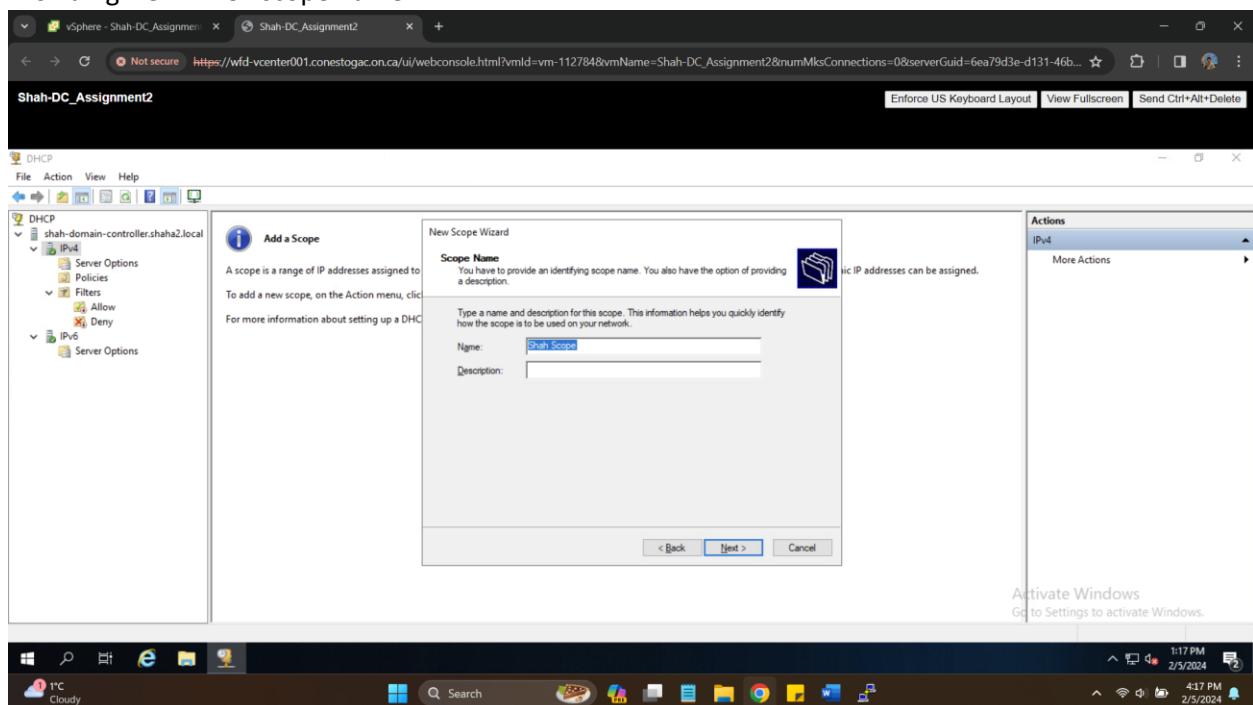
To open DHCP console, open Start → Windows Administrative Tools → DHCP



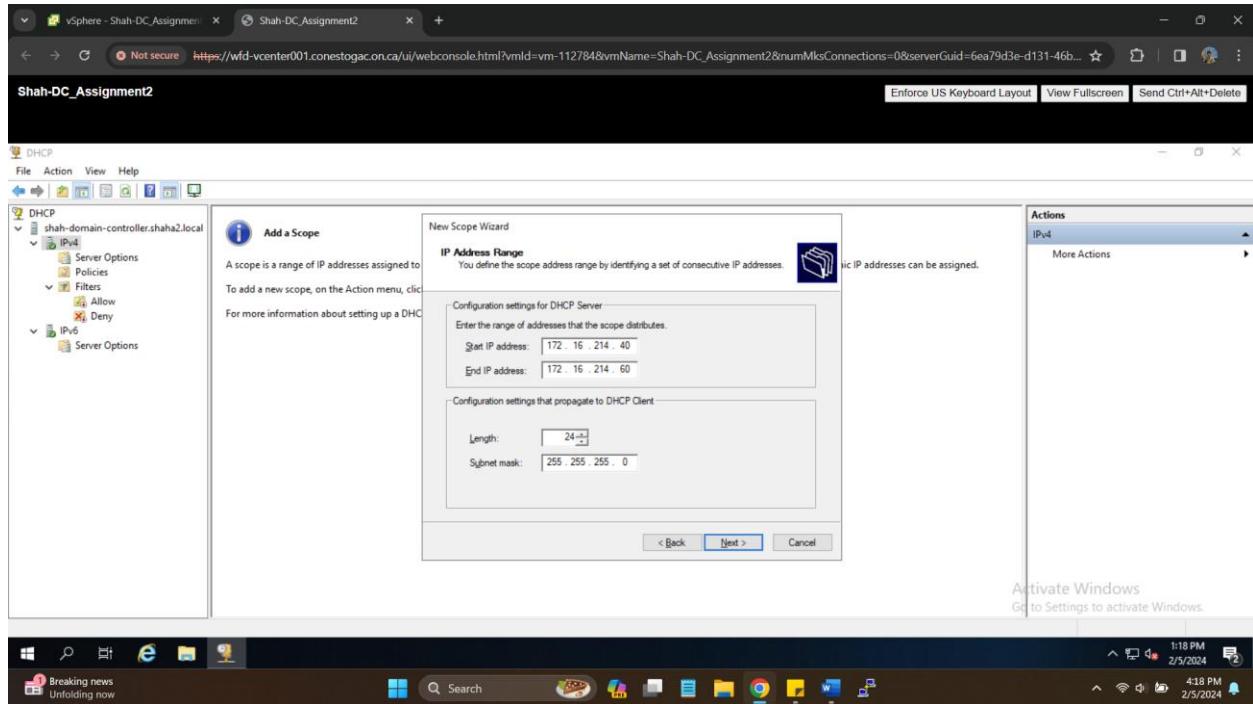
Inside DHCP console → Select Domain → IPv4 → right click and select new scope



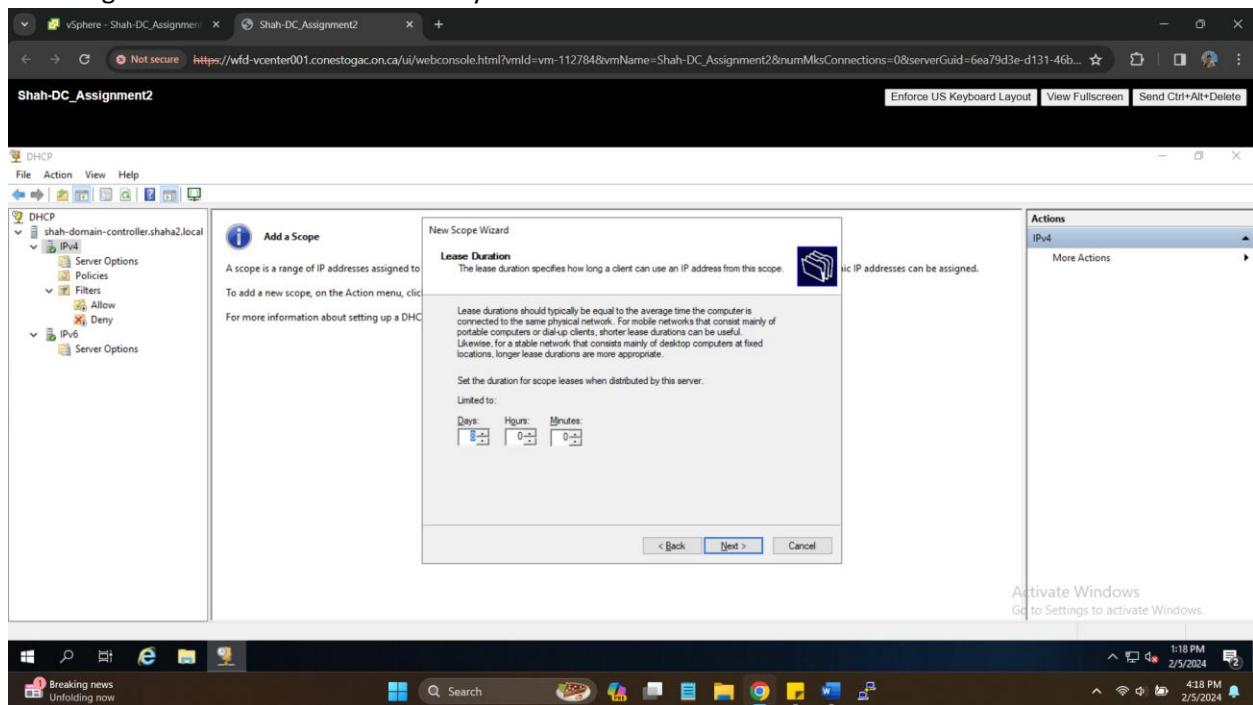
Providing New DHCP scope name



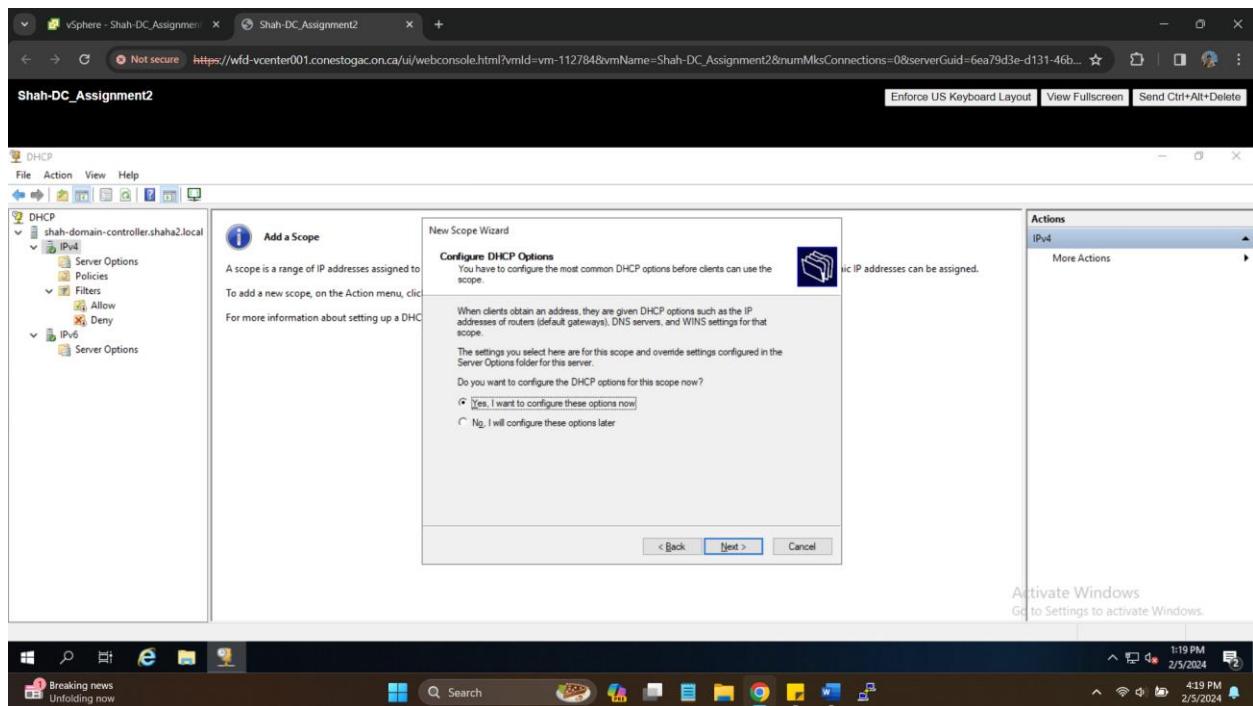
Providing IPv4 scope range 172.16.214.40 to 172.16.214.60 with subnet mask of 255.255.255.0



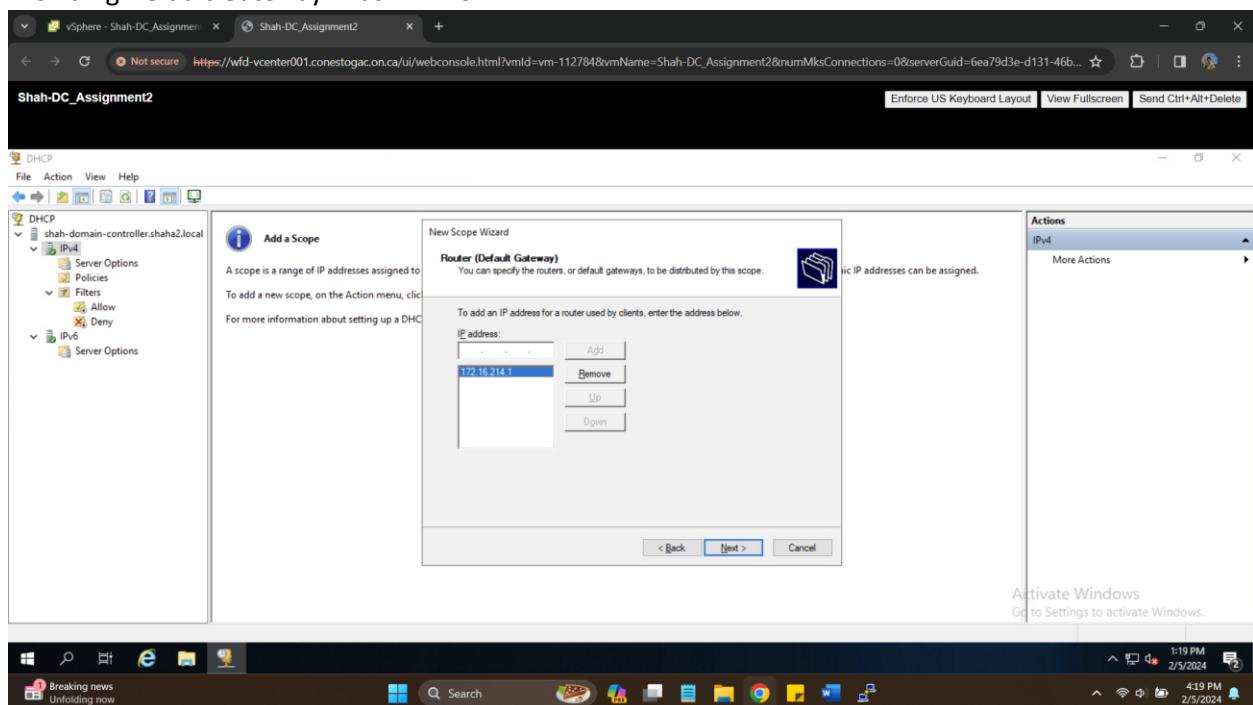
Selecting default lease duration to 8 days



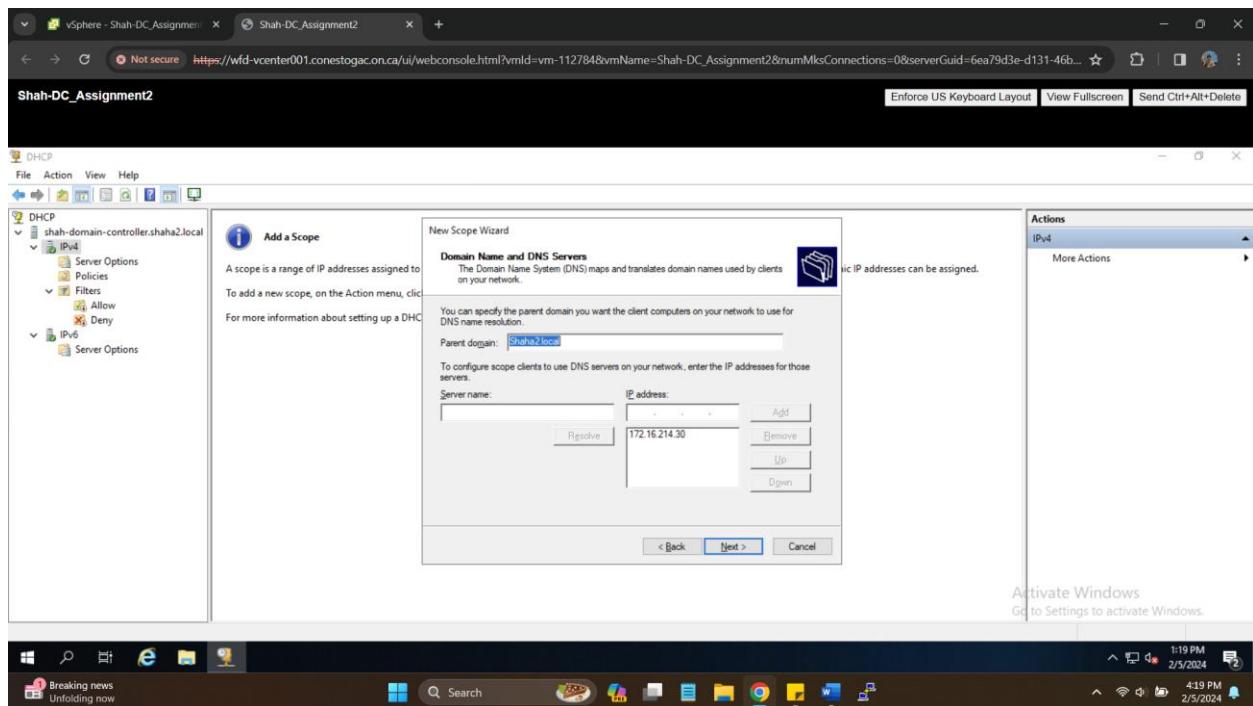
Selecting Yes or No to configure DHCP for this scope



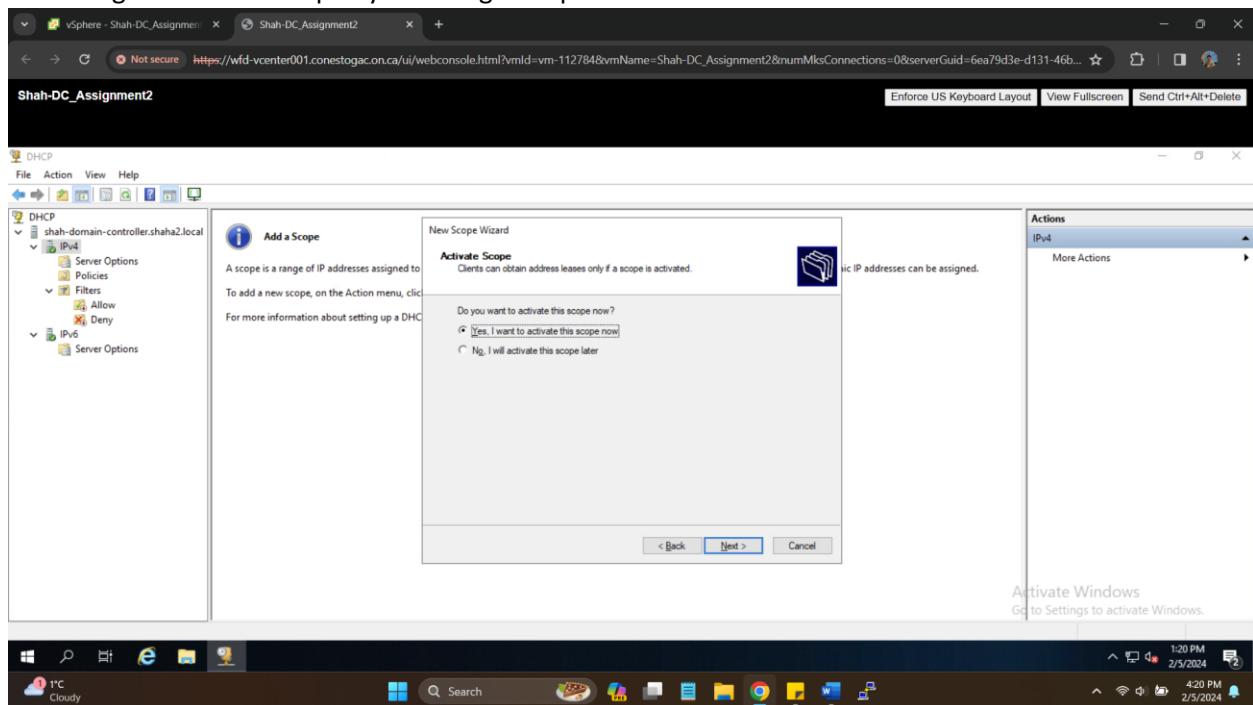
Providing Default Gateway IP as 172.16.214.1



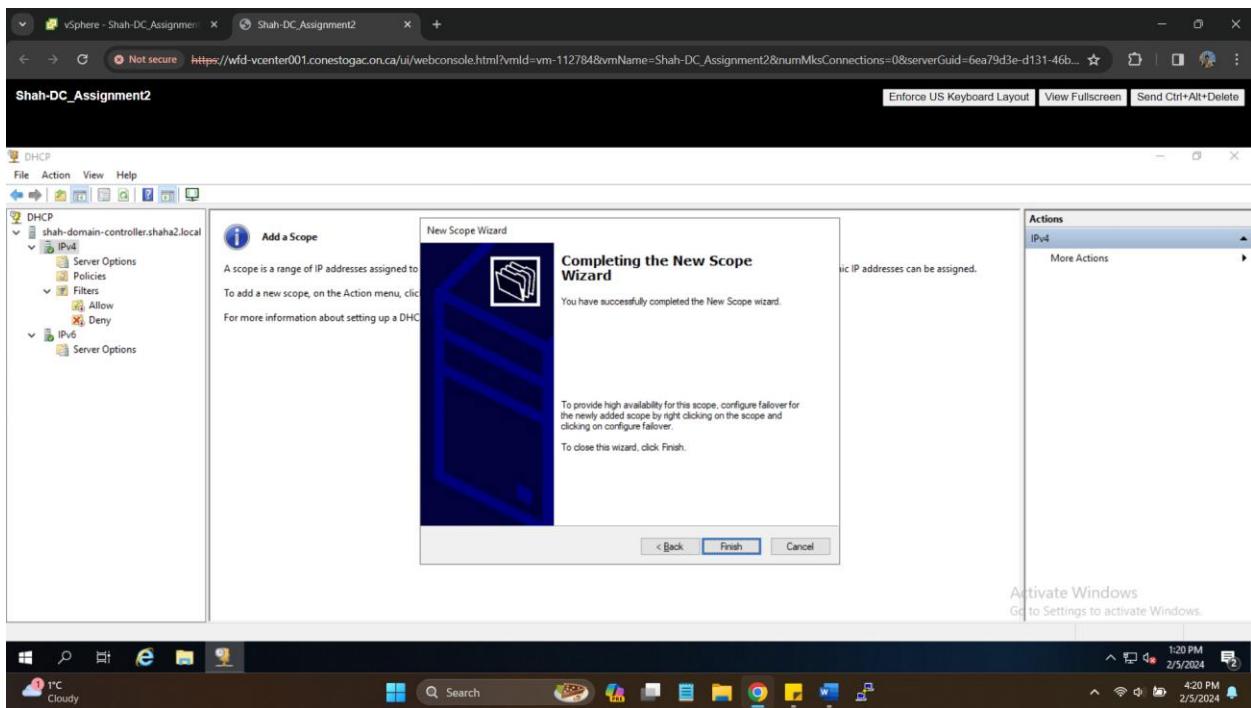
Providing Domain Name and Domain Controller IP used by clients.



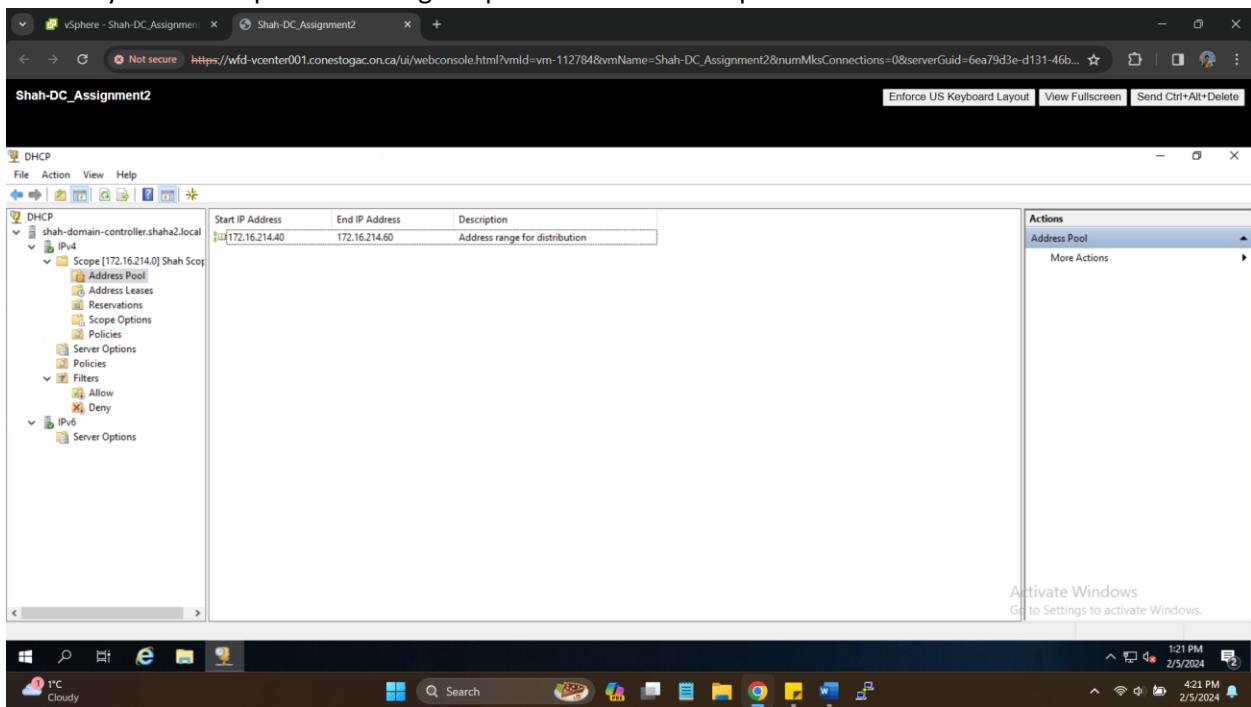
Activating the defined scope by selecting Yes option



Completion of new scope defining

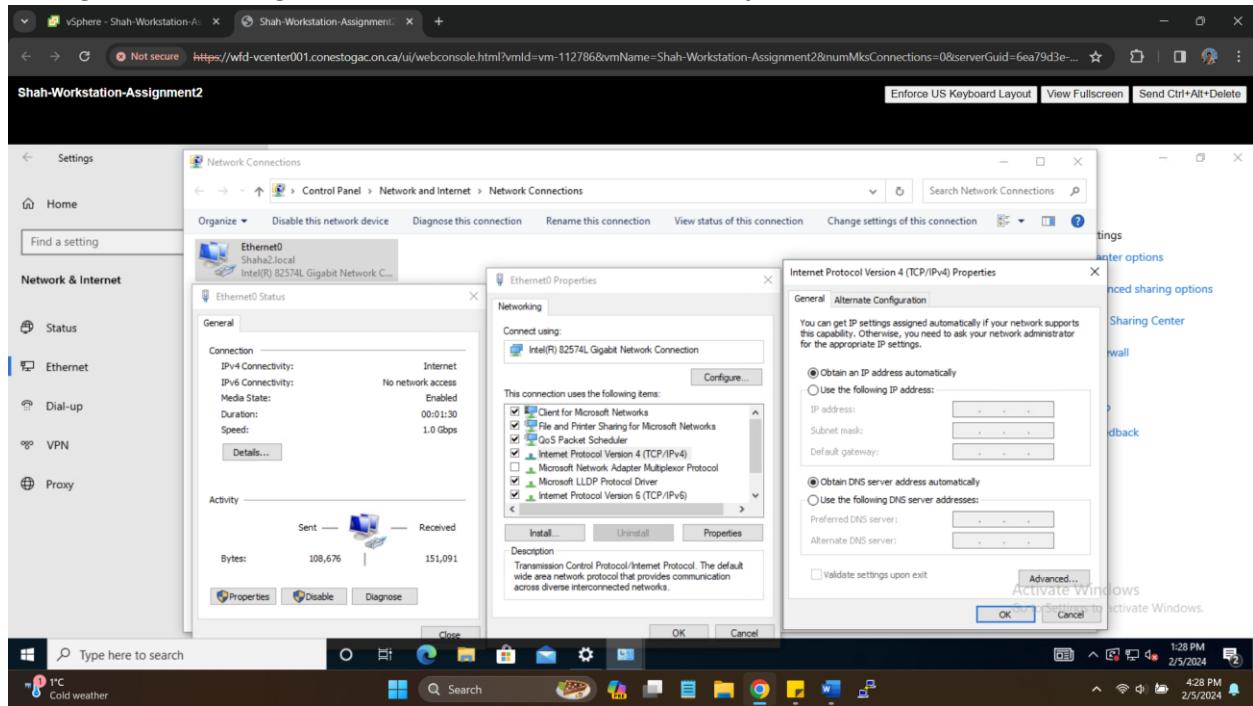


Summary of new scope with IP range as provided in DHCP scope on domain controller

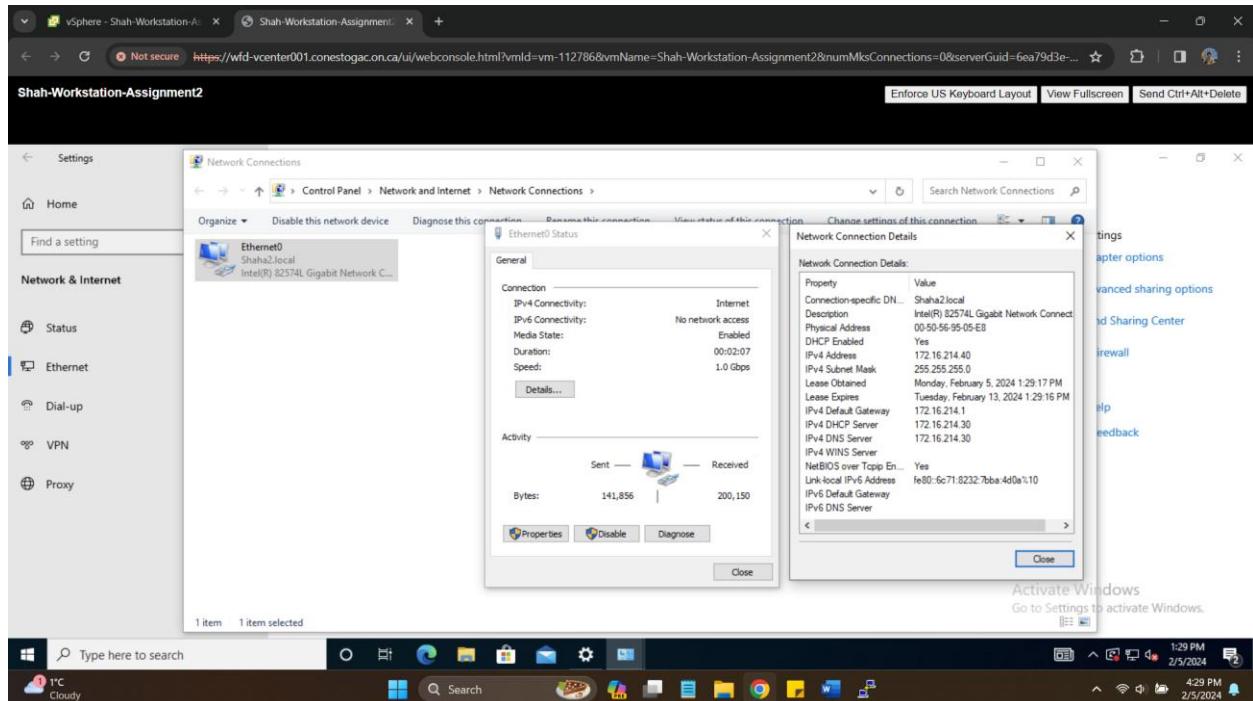


- 10) Set the Windows Workstation to DHCP and show it receiving an IP address from your DHCP Server.

Setting the IPv4 settings to obtain an IP address automatically on workstation.



Checking workstation IPv4 status of connected Ethernet port.



Domain controller configured with DHCP shows IP 172.16.214.40 leased IP to a workstation.

vSphere - Shah-DC_Assignment2

Not secure https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-112784&vmName=Shah-DC_Assignment2&numMksConnections=0&serverGuid=6ea79d3e-d131-46b...

Shah-DC_Assignment2

Enforce US Keyboard Layout View Fullscreen Send Ctrl+Alt+Delete

DHCP

File Action View Help

Client IP Address Name Lease Expiration Type Unique ID Description Network Access Protection Probation Expiration Filter Profile Actions

Client IP Address	Name	Lease Expiration	Type	Unique ID	Description	Network Access Protection	Probation Expiration	Filter Profile	Actions
172.16.214.40	Workstation-A2.Shaha2.local	2/13/2024 1:29:17 PM	DHCP	005056950...	Full Access	N/A	None		Address Leases More Actions ▾
172.16.214.40									More Actions ▾

shah-domain-controller.shaha2.local

IPv4 Scope [172.16.214.0] Shahn Scope Address Pool Address Leases Reservations Scope Options Policies Server Options Policies Filters Allow Deny IPv6 Server Options

Activate Windows Go to Settings to activate Windows.

1:31 PM 2/5/2024 4:31 PM 2/5/2024

DHCP

File Action View Help

Client IP Address Name Lease Expiration Type Unique ID Description Network Access Protection Probation Expiration Filter Profile Actions

Client IP Address	Name	Lease Expiration	Type	Unique ID	Description	Network Access Protection	Probation Expiration	Filter Profile	Actions
172.16.214.40	Workstation-A2.Shaha2.local	2/13/2024 1:29:17 PM	DHCP	005056950...	Full Access	N/A	None		Address Leases More Actions ▾
172.16.214.40									More Actions ▾

shah-domain-controller.shaha2.local

IPv4 Scope [172.16.214.0] Shahn Scope Address Pool Address Leases Reservations Scope Options Policies Server Options Policies Filters Allow Deny IPv6 Server Options

Activate Windows Go to Settings to activate Windows.

1:31 PM 2/5/2024 4:31 PM 2/5/2024