VM links

SHAH-DC1 → https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-129860&vmName=SHAH-DC1&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-b8e3379f5344&locale=en-US

SHAH-S1 → https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-129864&vmName=SHAH-S1&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-b8e3379f5344&locale=en-US

SHAH-C1 → https://wfd-vcenter001.conestogac.on.ca/ui/webconsole.html?vmId=vm-129966&vmName=SHAH-C1&numMksConnections=0&serverGuid=6ea79d3e-d131-46b6-abbc-b8e3379f5344&locale=en-US

IP details:

SHAH DC1 →172.16.214.50

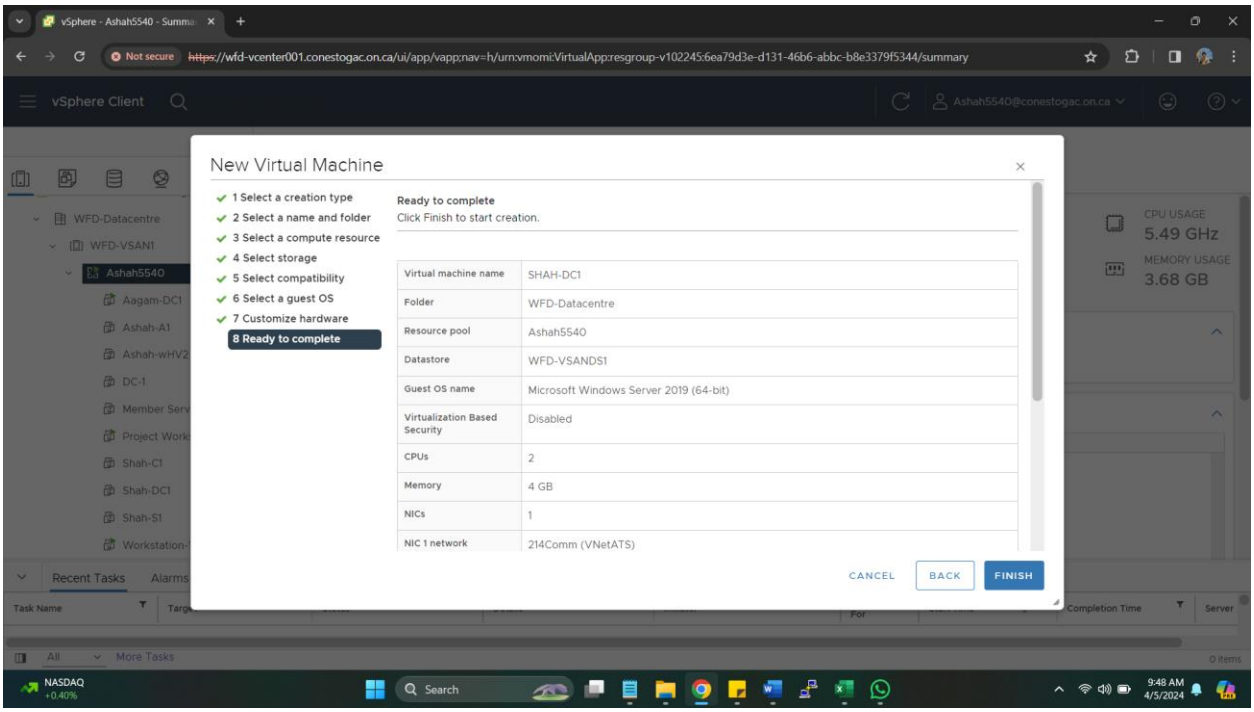
SHAH-S1→172.16.214.51

SHAH-C1→172.16.214.52

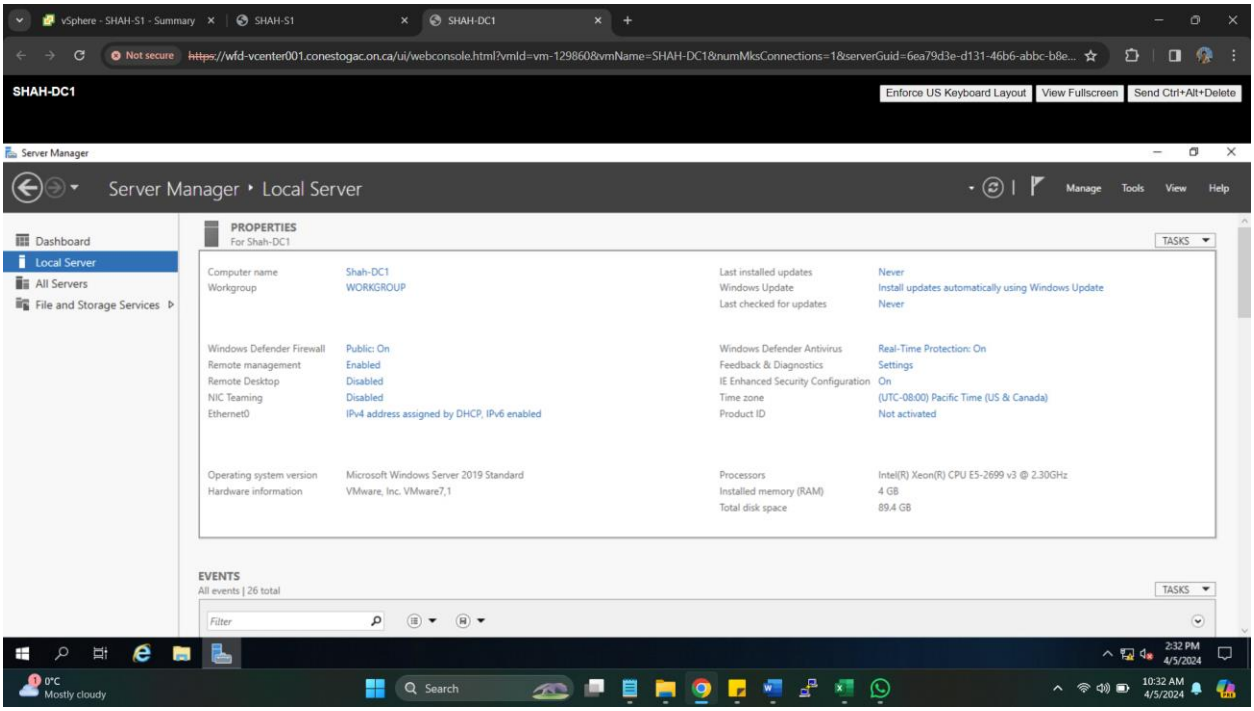
Domain name: Shah05.local

SHAH-DC1

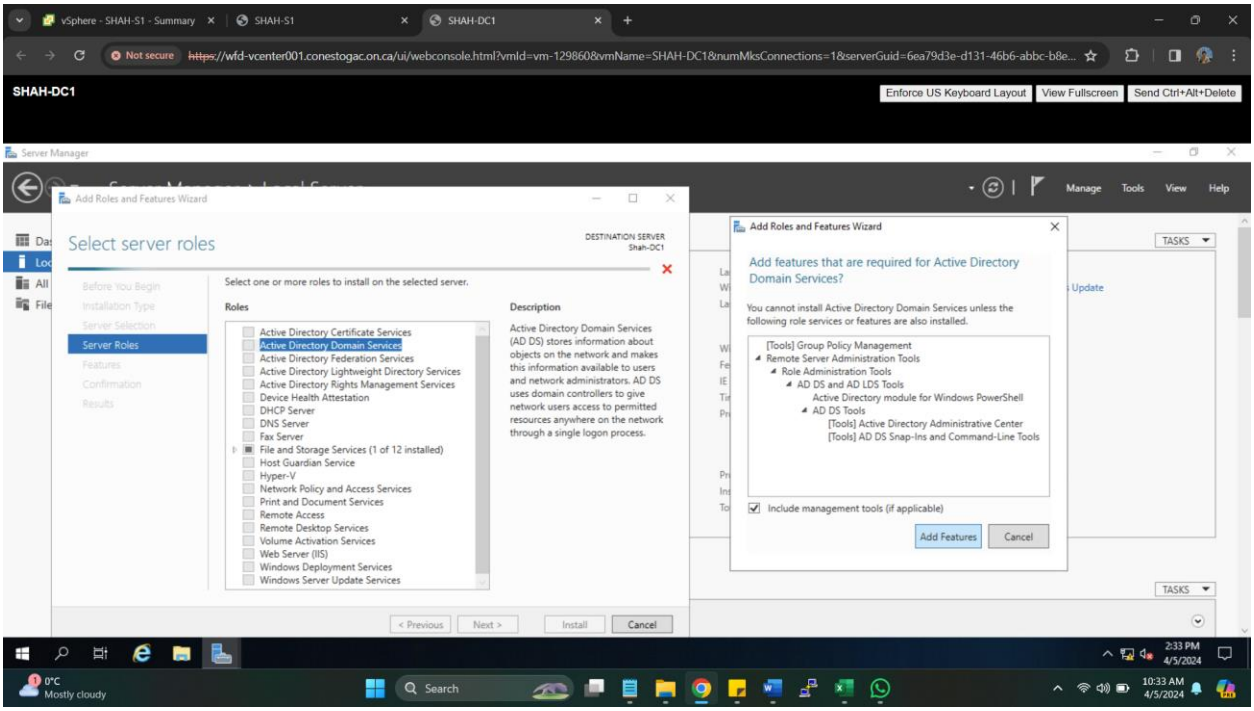
Summary of creating VM for SHAH-DC1 installation



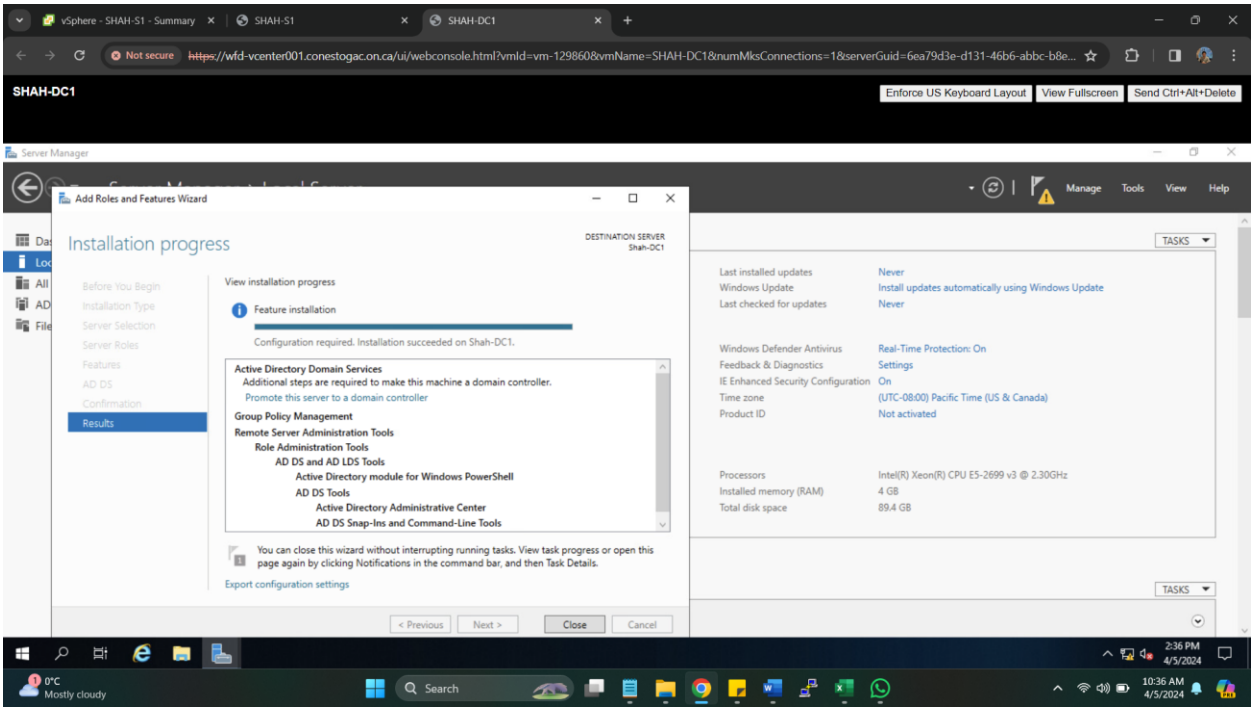
Successfully installing Windows Server 2019 standard on VM



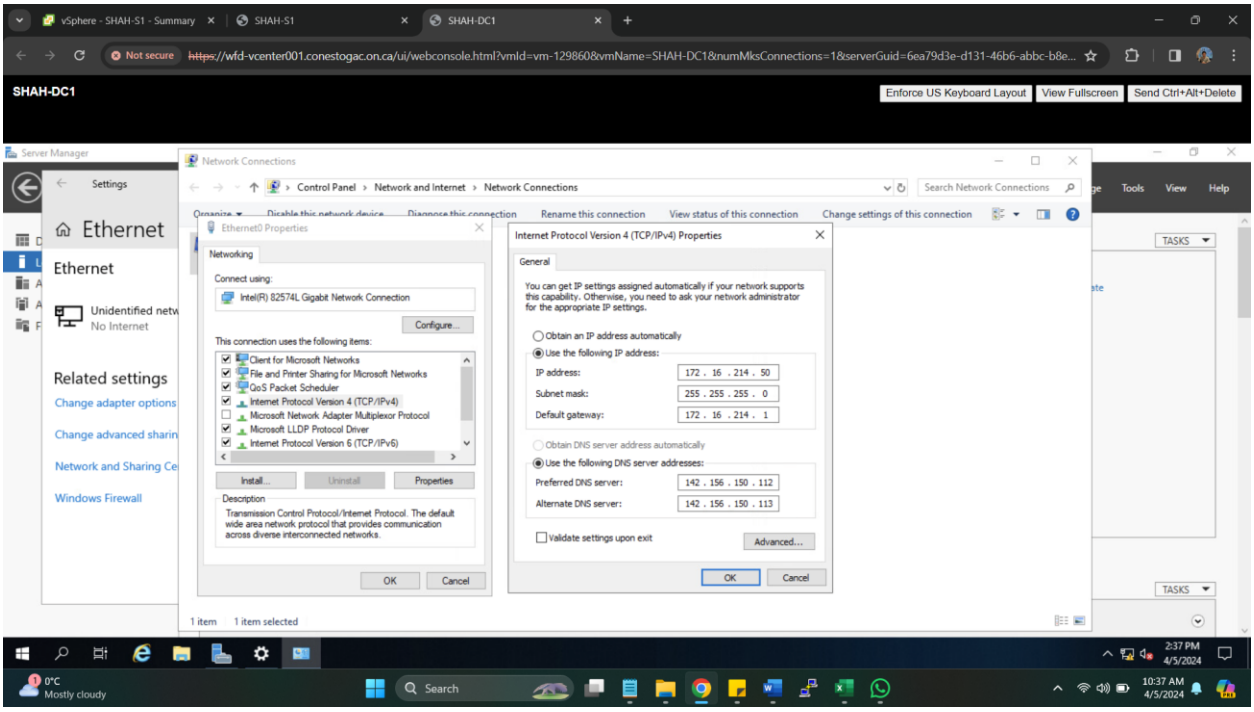
Selecting the role of ADDS and adding feature of it on server SHAH-DC1



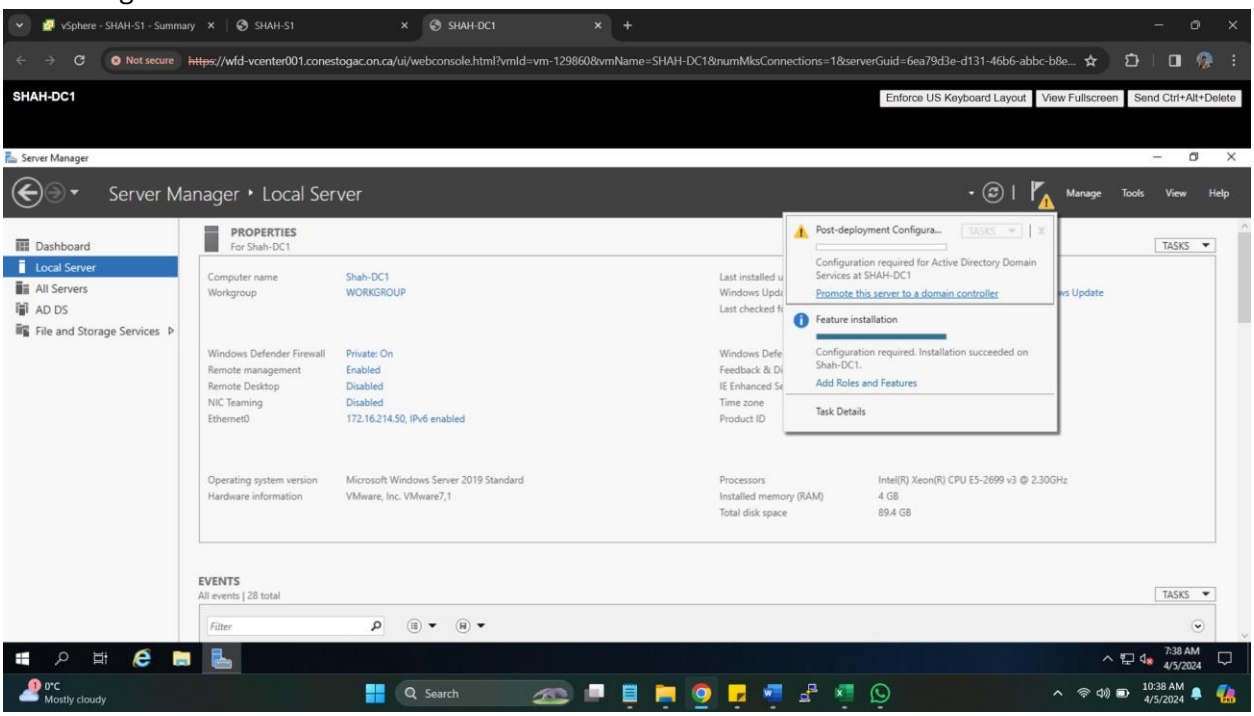
Successfully installing the ADDS feature.



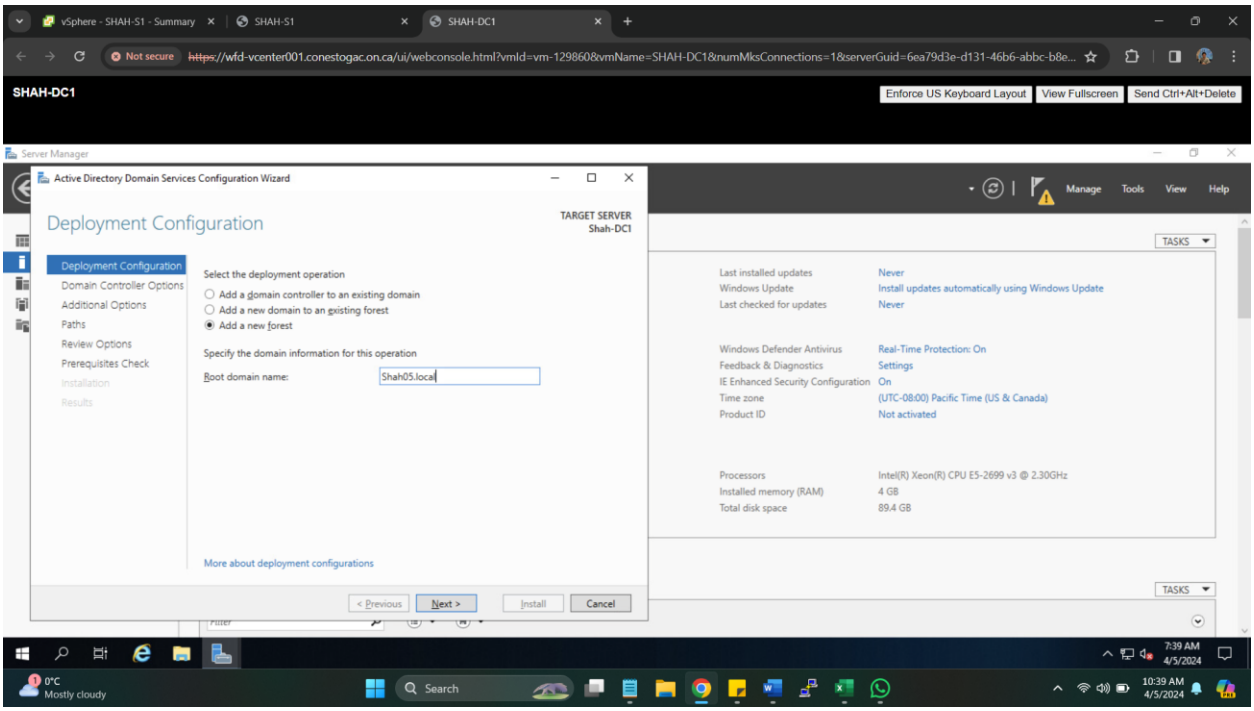
Configuring IP on Server SHAH-DC1 with primary DNS.



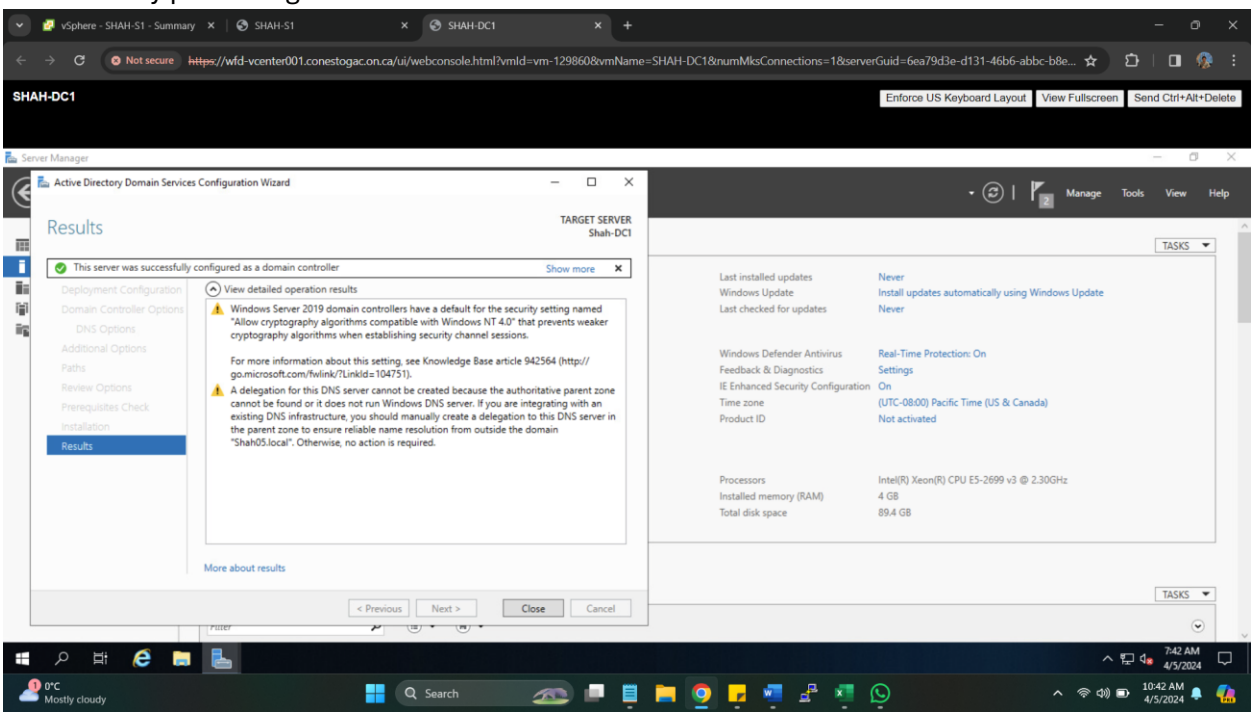
Promoting server to domain controller of SHAH-DC1



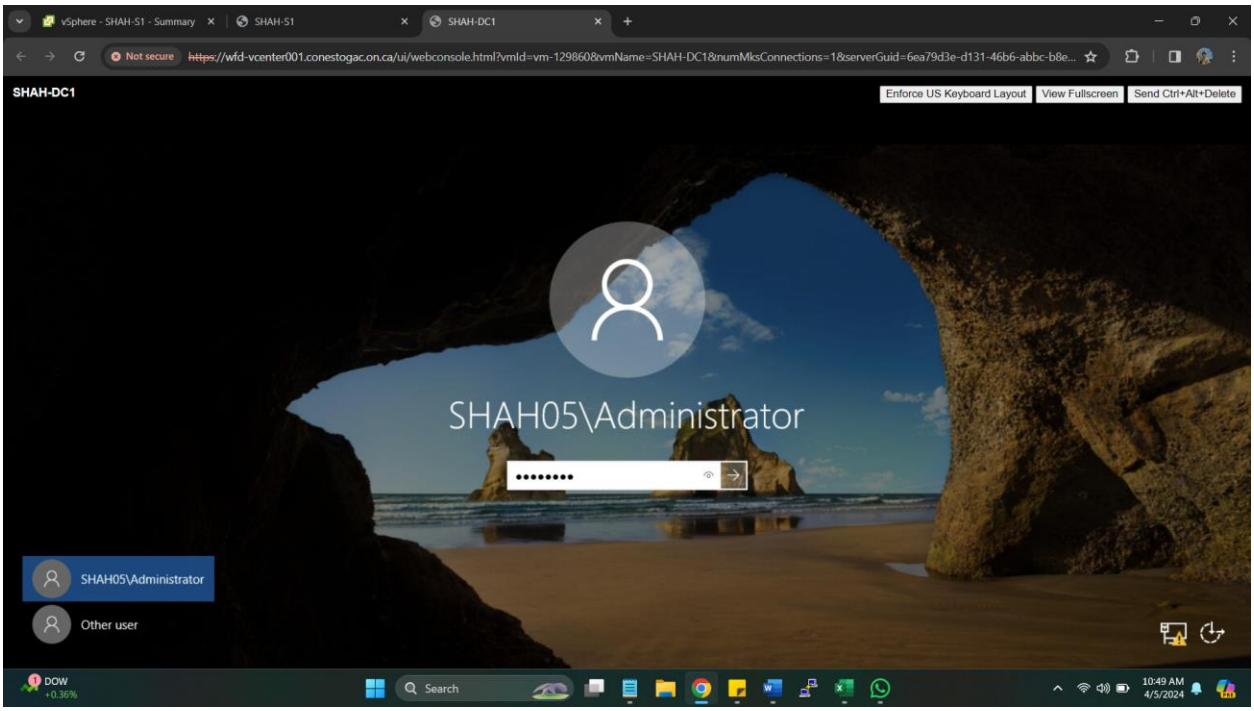
Adding new Forest as root domain name: SHAH05.local



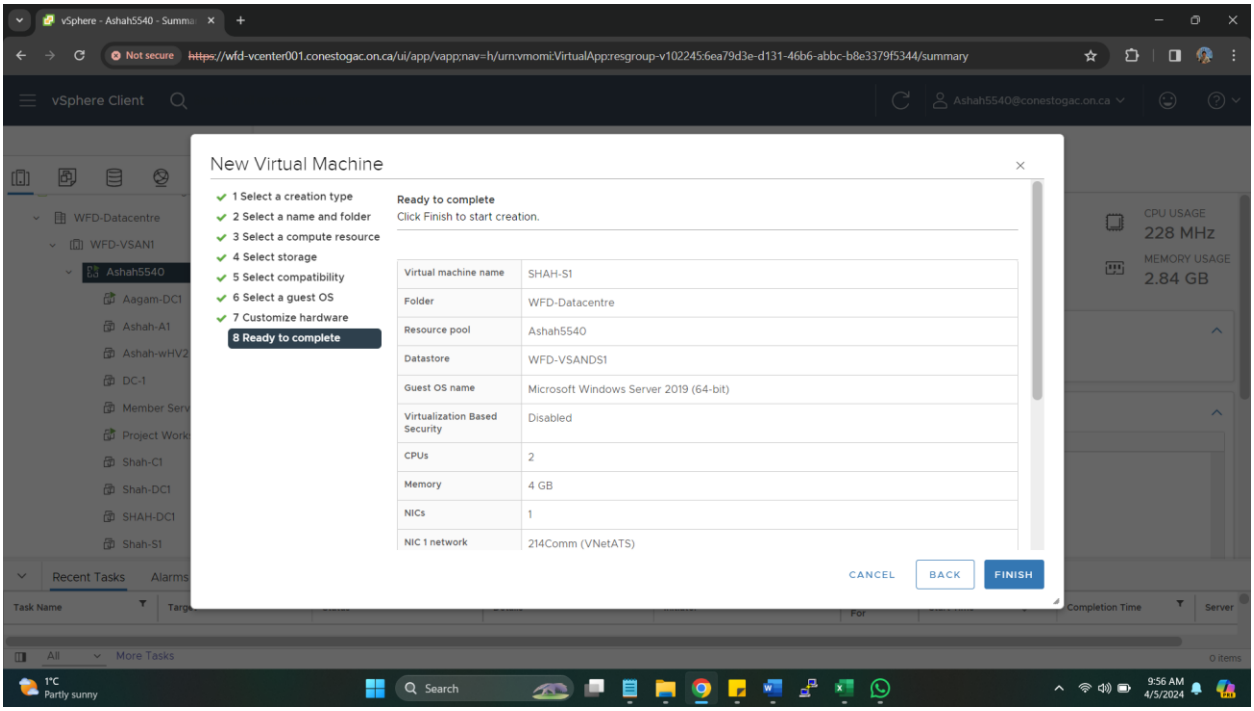
Successfully promoting server to Domain Controller

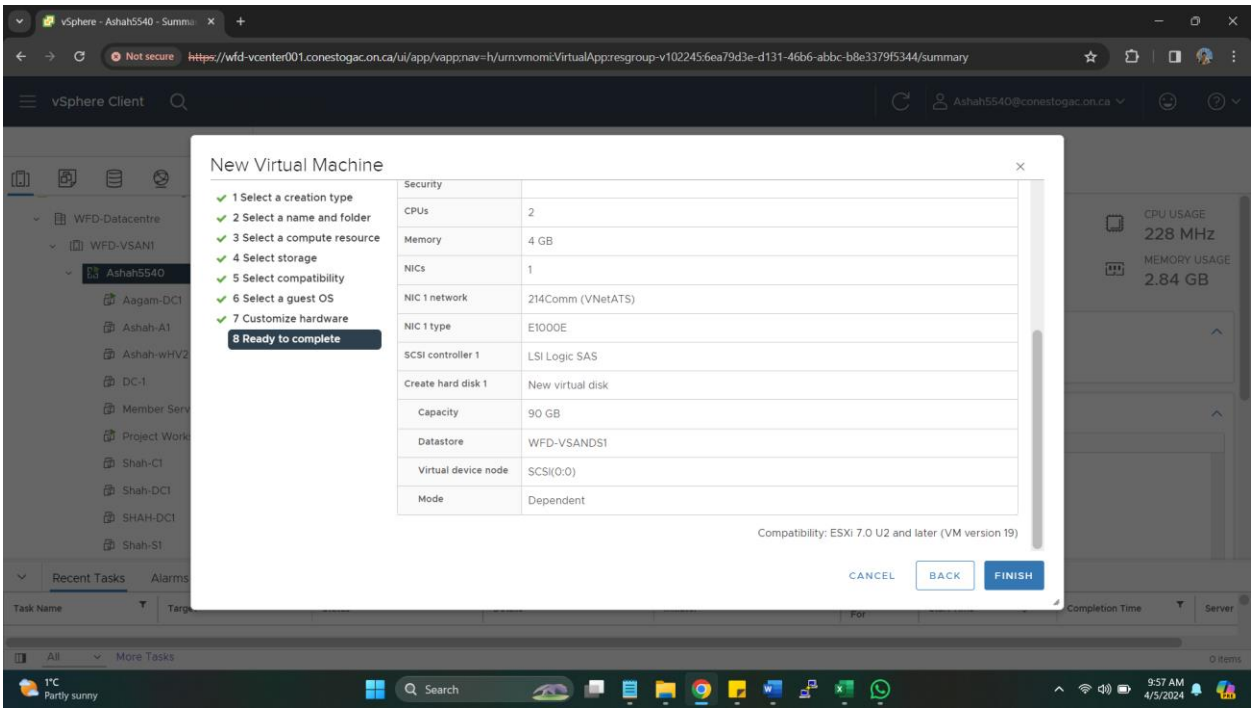


Domain Controller login in SHAH05.local by administrator password: Secret55

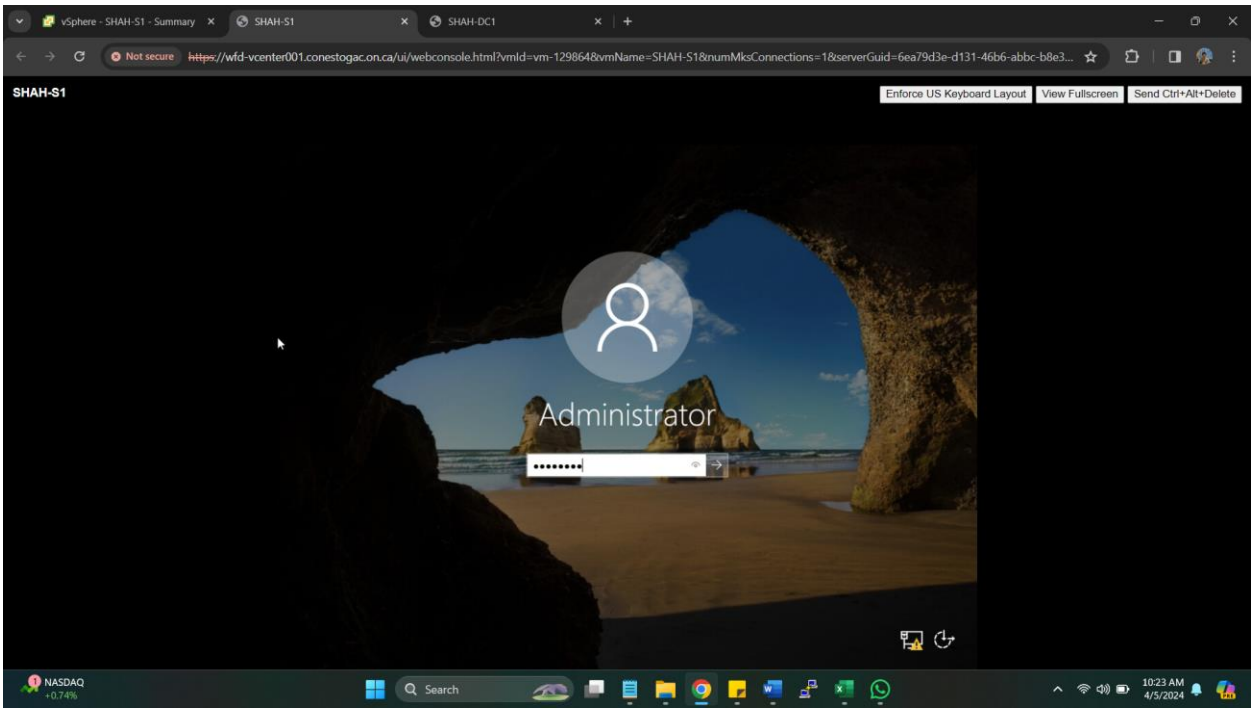


Summary of creating VM for member server installation as SHAH-S1

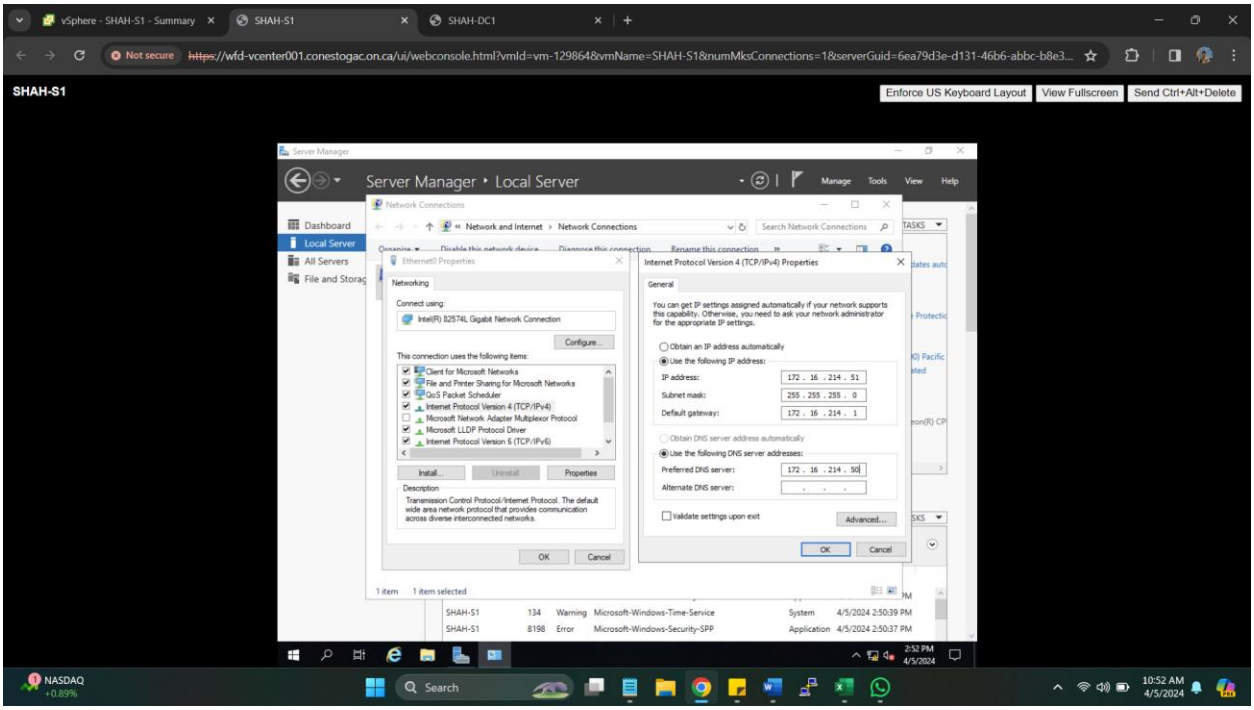

vSphere - Ashah5540 - Summa
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/app/vapp;nav=h/urn:vmomi:VirtualApp:resgroup-v102245:6ea79d3e-d131-46b6-abbc-b8e3379f5344/summary
vSphere Client
Ashah5540@conestogac.on.ca
New Virtual Machine
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete
Ready to complete
Click Finish to start creation.
Virtual machine name SHAH-S1
Folder WFD-Datacentre
Resource pool Ashah5540
Datastore WFD-VSANDS1
Guest OS name Microsoft Windows Server 2019 (64-bit)
Virtualization Based Security Disabled
CPUs 2
Memory 4 GB
NICs 1
NIC 1 network 214Comm (VNetATS)
CANCEL
BACK
FINISH
WFD-Datacentre
WFD-VSAN1
Ashah5540
Aagam-DC1
Ashah-A1
Ashah-wHV2
DC-1
Member Serv
Project Work
Shah-C1
Shah-DC1
SHAH-DC1
Shah-S1
CPU USAGE
228 MHz
MEMORY USAGE
2.84 GB
Recent Tasks
Alarms
Task Name
Completion Time
Server
More Tasks
0 items
1°C
Partly sunny
Search
9:56 AM
4/5/2024


vSphere - Ashah5540 - Summa
Not secure
https://wfd-vcenter001.conestogac.on.ca/ui/app/vapp;nav=h/urn:vmomi:VirtualApp:resgroup-v102245:6ea79d3e-d131-46b6-abbc-b8e3379f5344/summary
vSphere Client
Ashah5540@conestogac.on.ca
New Virtual Machine
1 Select a creation type
2 Select a name and folder
3 Select a compute resource
4 Select storage
5 Select compatibility
6 Select a guest OS
7 Customize hardware
8 Ready to complete
Security
CPUs 2
Memory 4 GB
NICs 1
NIC 1 network 214Comm (VNetATS)
NIC 1 type E1000E
SCSI controller 1 LSI Logic SAS
Create hard disk 1 New virtual disk
Capacity 90 GB
Datastore WFD-VSANDS1
Virtual device node SCSI(0:0)
Mode Dependent
Compatibility: ESXi 7.0 U2 and later (VM version 19)
CANCEL
BACK
FINISH
WFD-Datacentre
WFD-VSAN1
Ashah5540
Aagam-DC1
Ashah-A1
Ashah-wHV2
DC-1
Member Serv
Project Work
Shah-C1
Shah-DC1
SHAH-DC1
Shah-S1
CPU USAGE
228 MHz
MEMORY USAGE
2.84 GB
Recent Tasks
Alarms
Task Name
Completion Time
Server
More Tasks
0 items
1°C
Partly sunny
Search
9:57 AM
4/5/2024

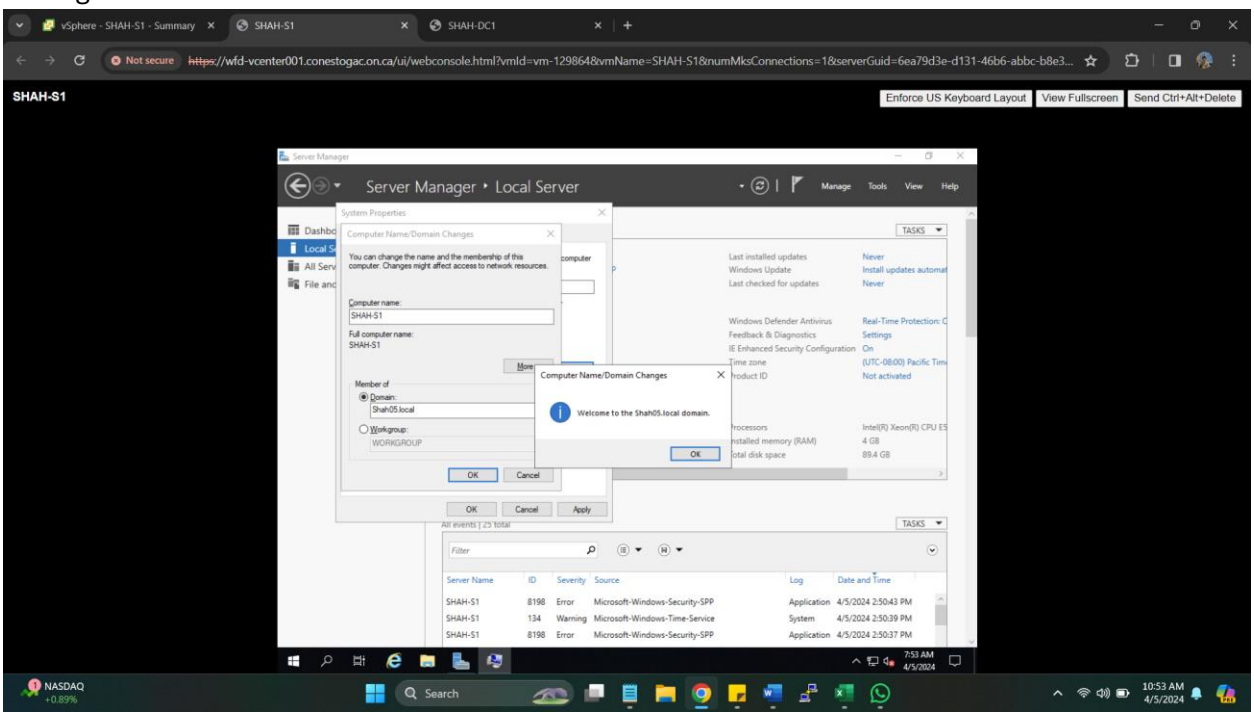
Password of member server: Secret55



Configuring IP of the member server as 172.16.214.51

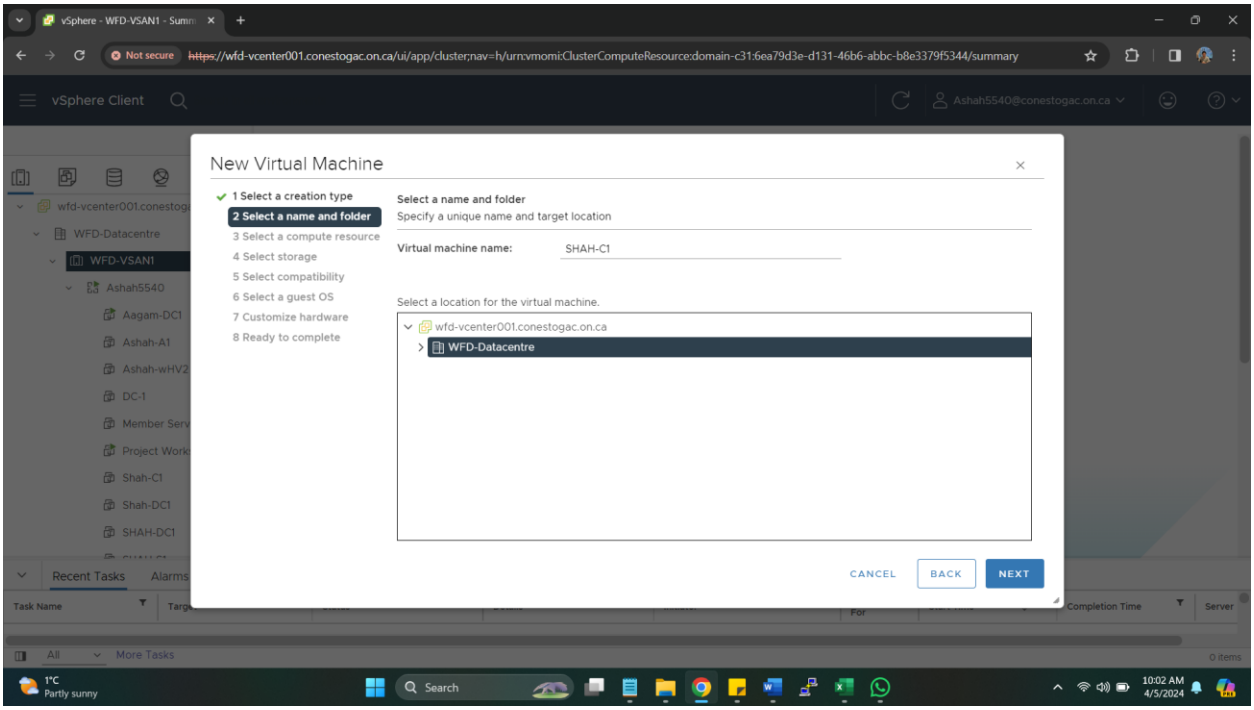


Joining the member server to domain: SHAH05.local

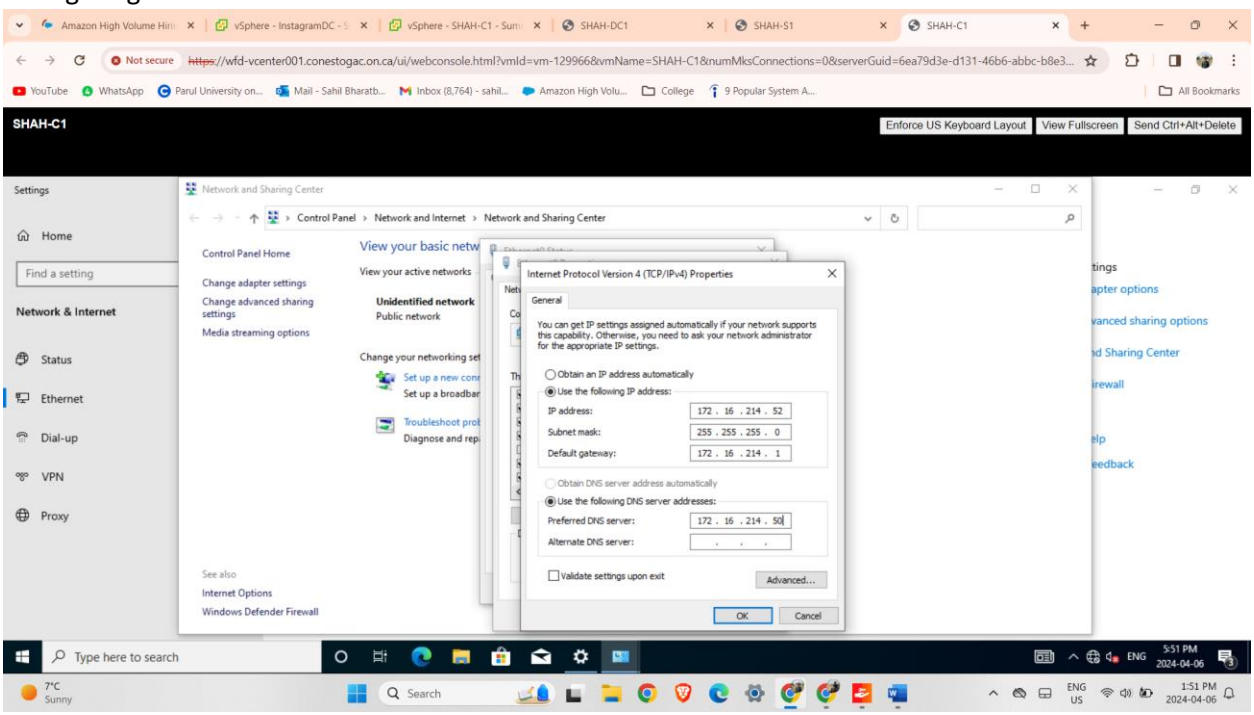


SHAH-C1

Creating VM for SHAH-C1 workstation.



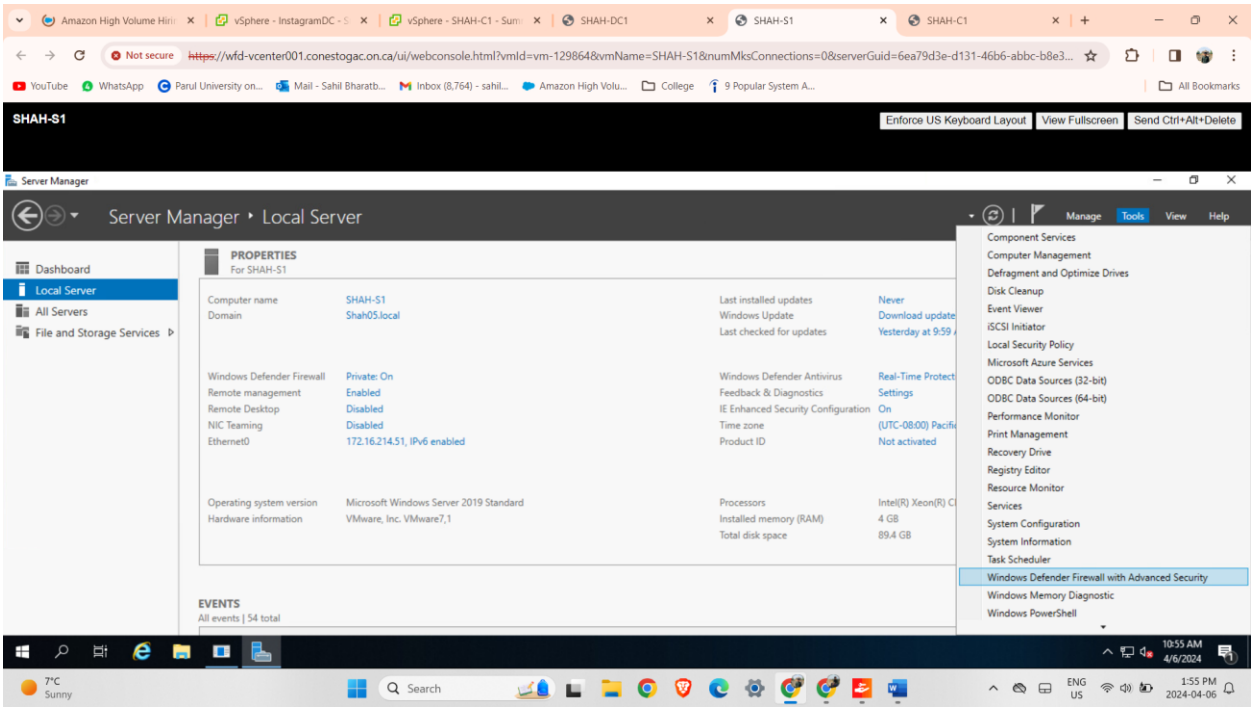
Configuring IP of the workstation as 172.16.214.52



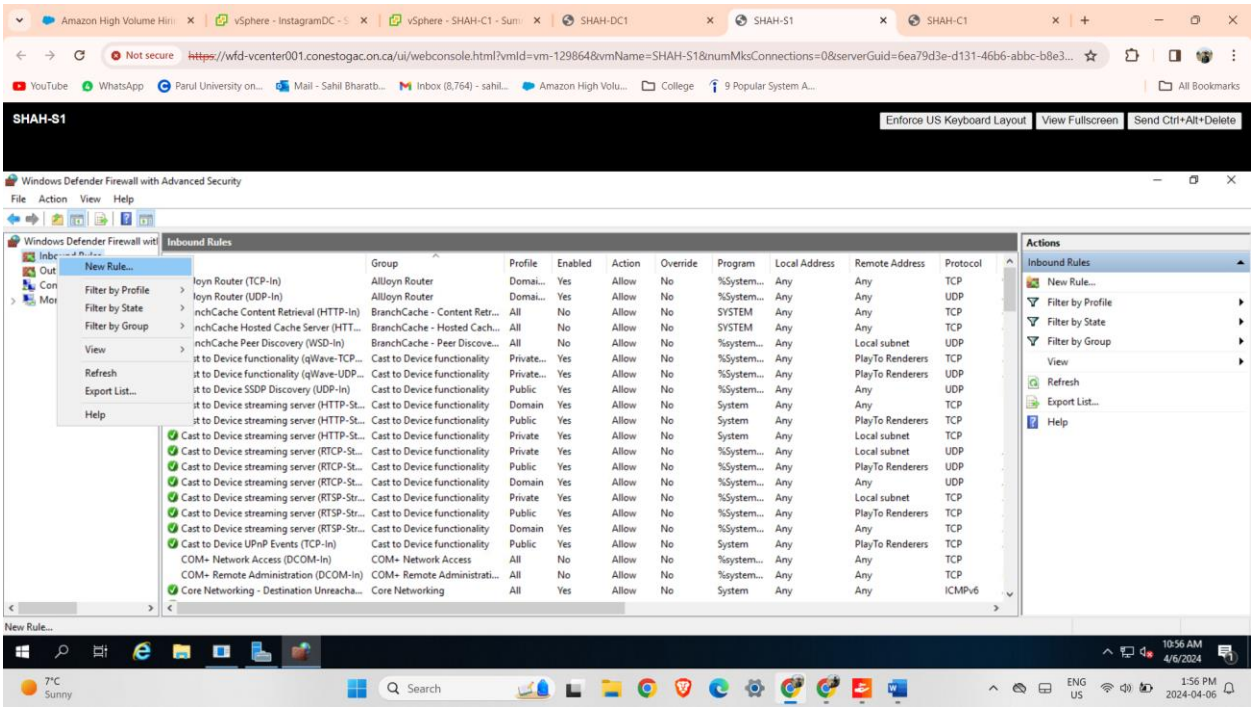
Part 1: Server Hardening and Firewalls

1) Create the below rules in **Windows Defender Firewall with advanced security** on **SHAH-S1**.

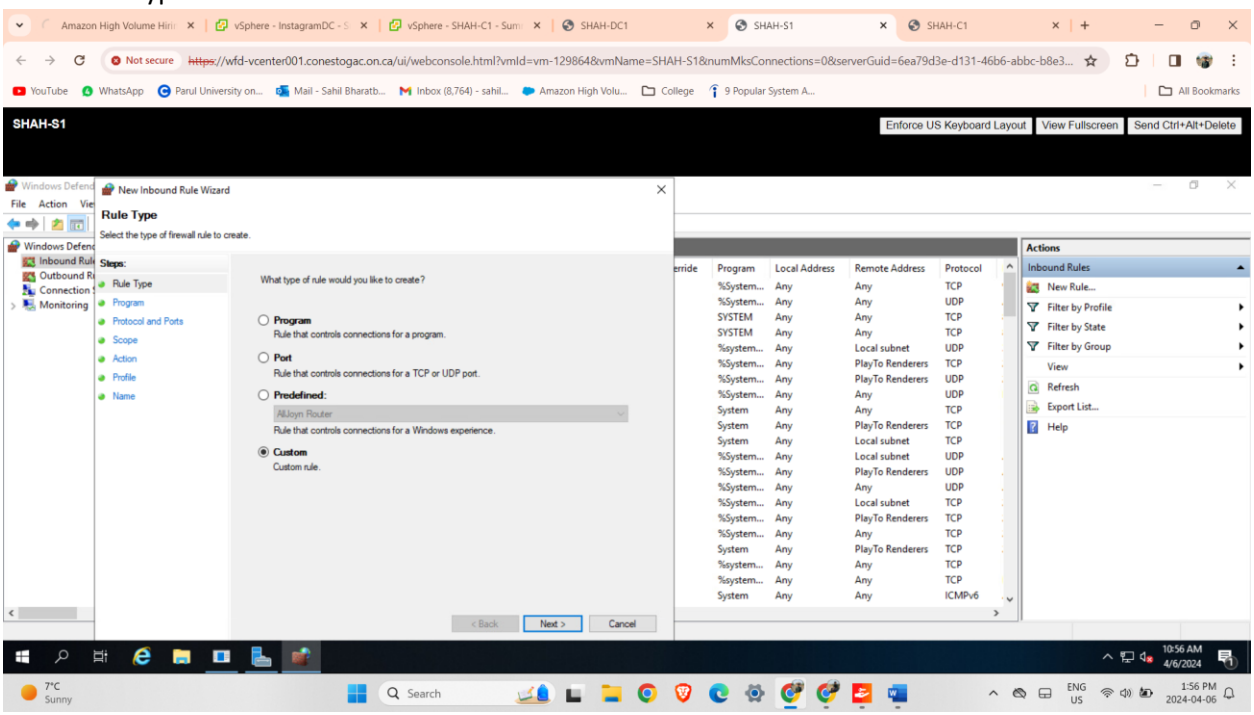
Allow ICMPv4



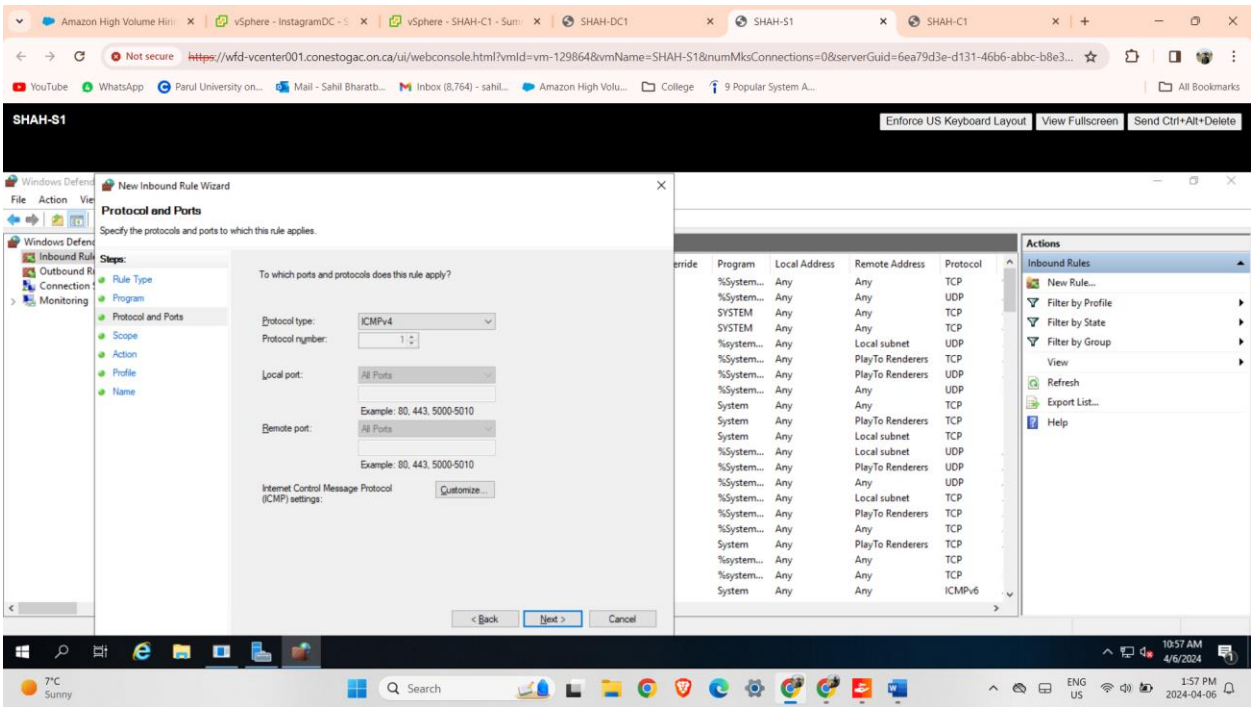
In Windows Defender firewall with advanced security, select new rule



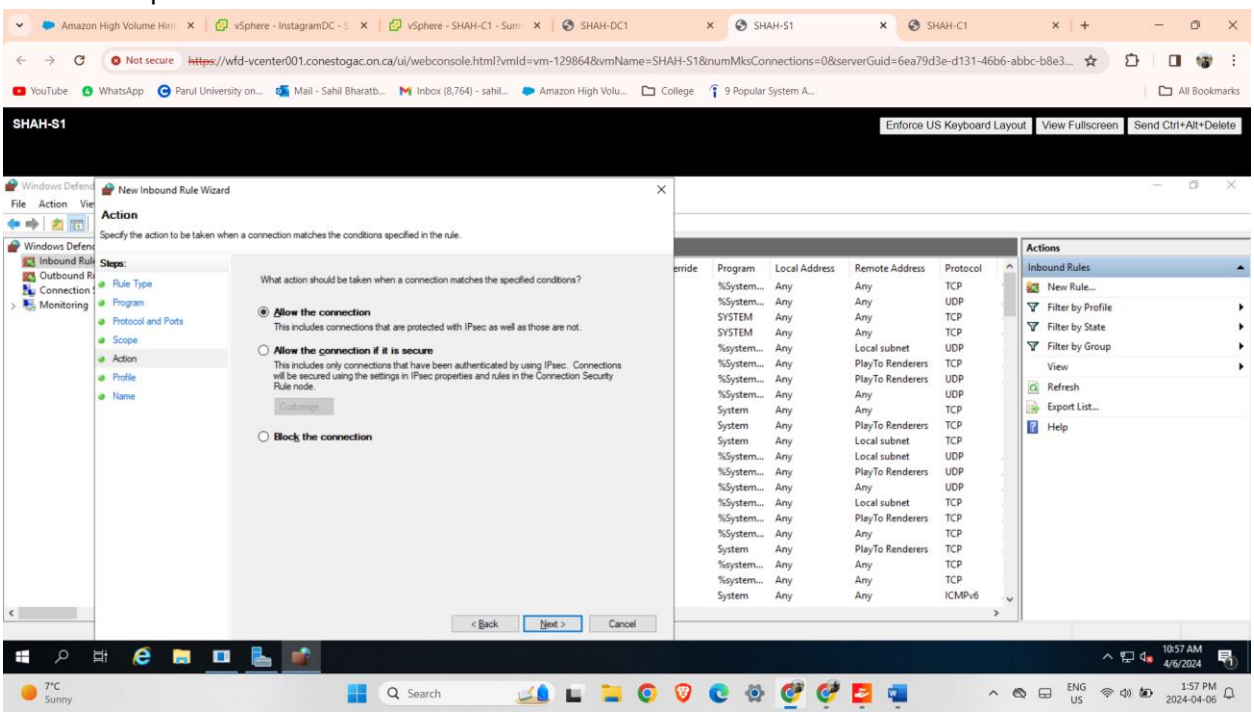
Select rule type as custom



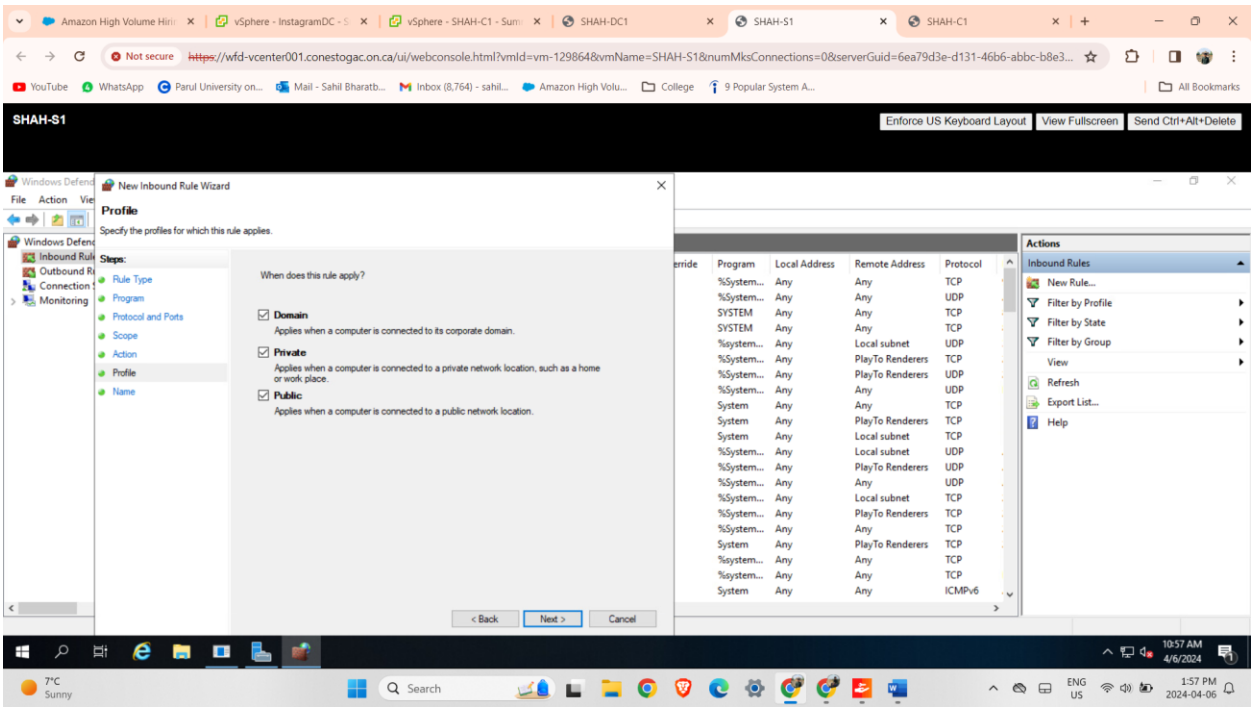
Select port and protocols



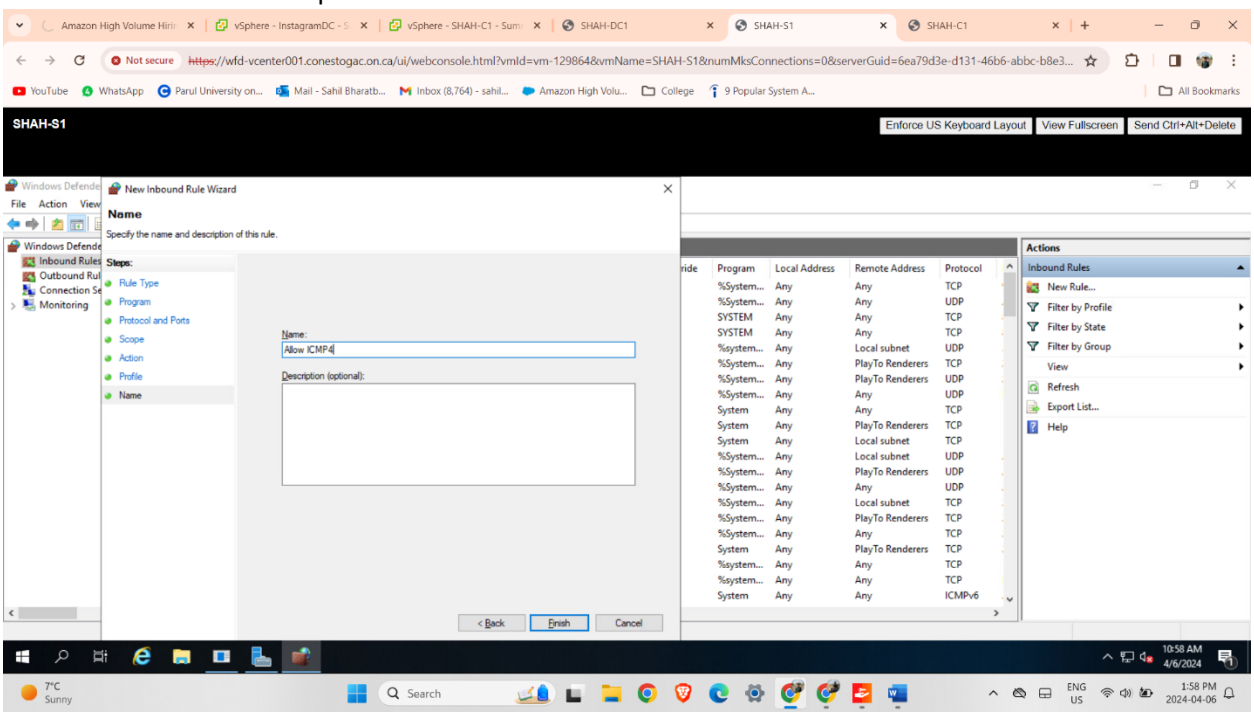
Select the option “allow the connection”



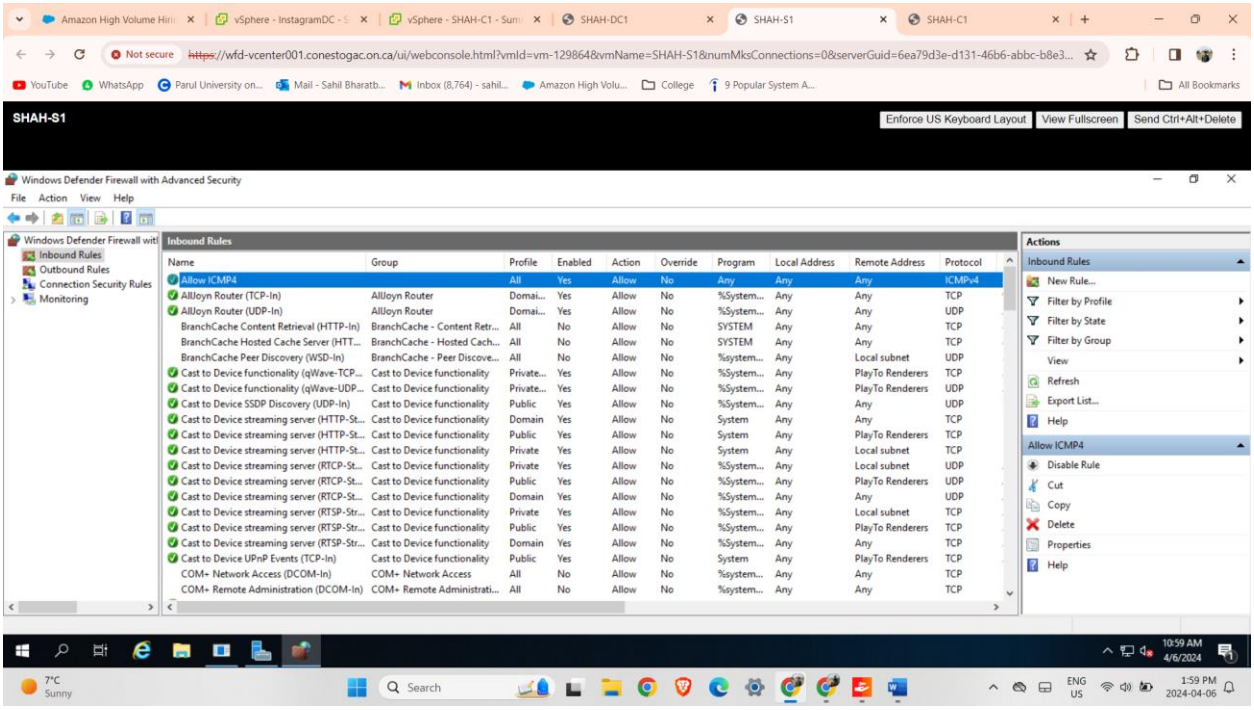
Select the domain, private and public, to apply the rule.



Provide a name and description for the creation of the new rule.

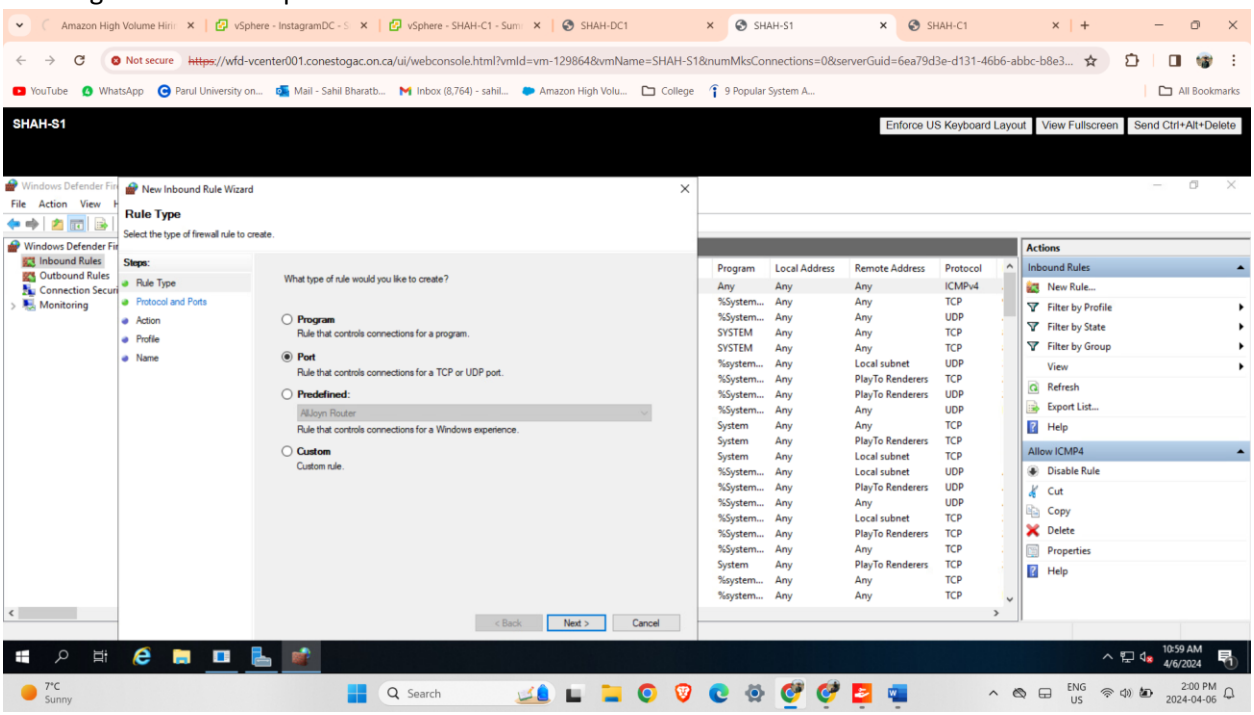


New rule successfully created

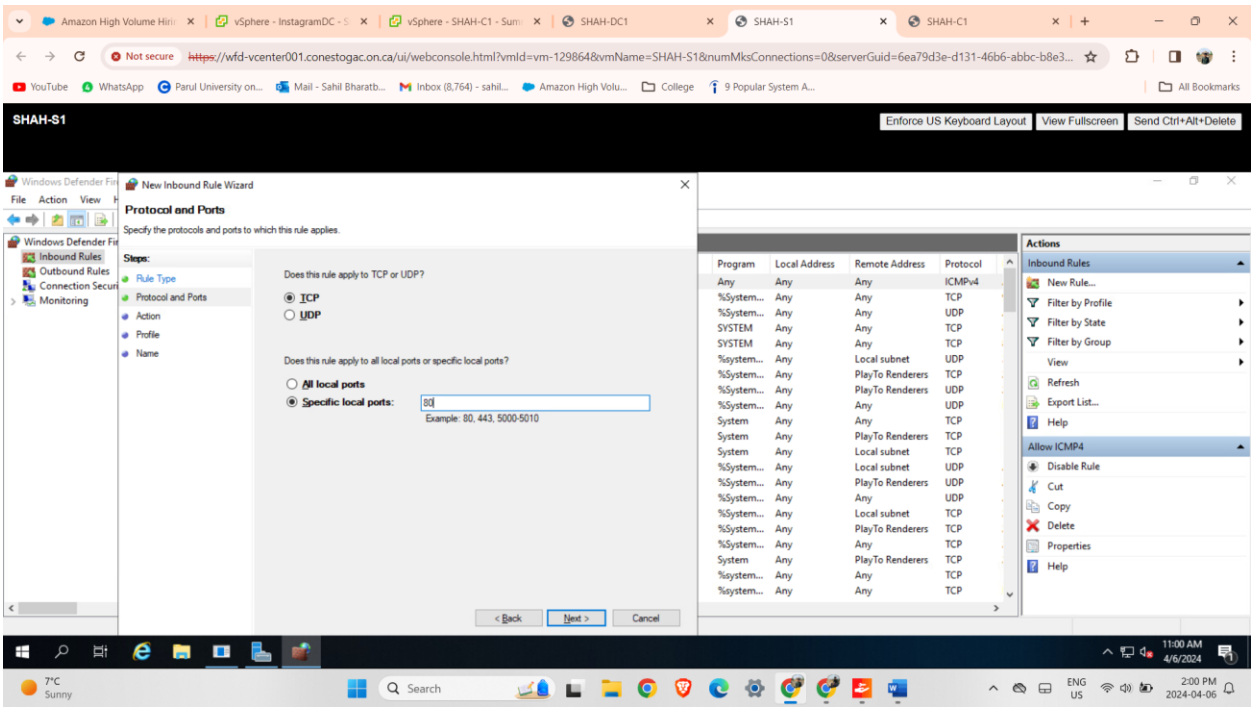


Allow HTTP TCP Port 80

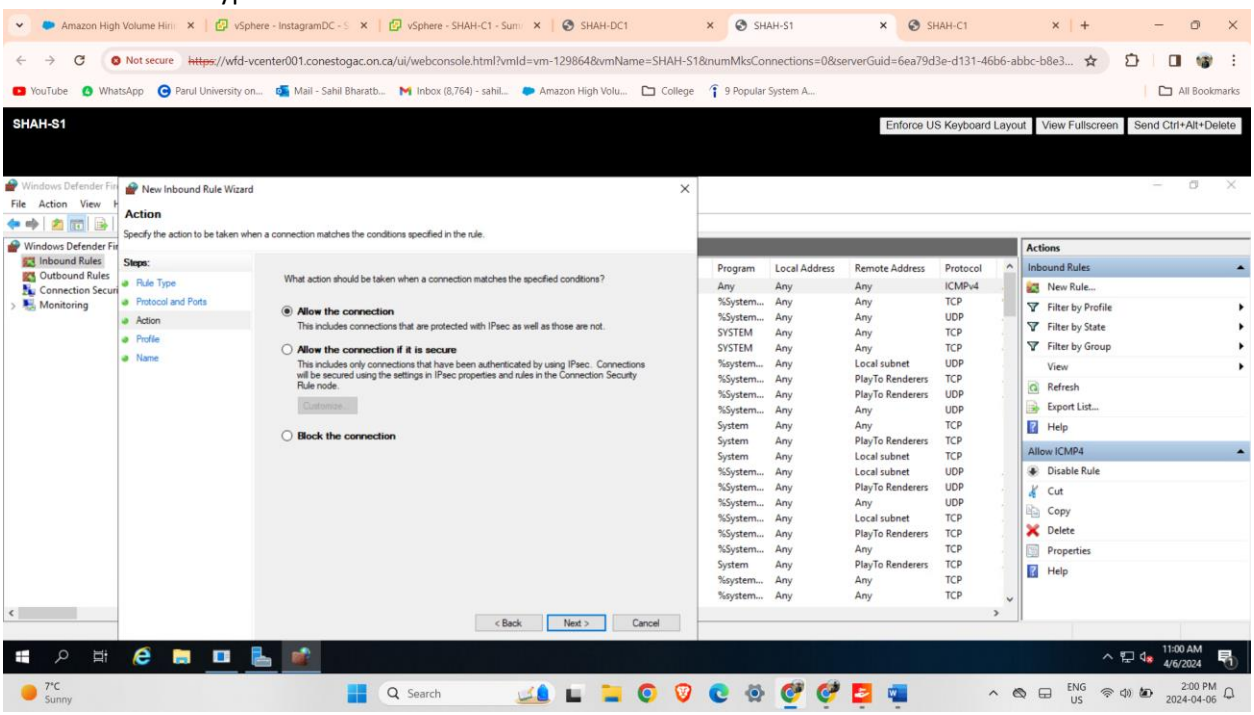
Creating a new rule for port 80



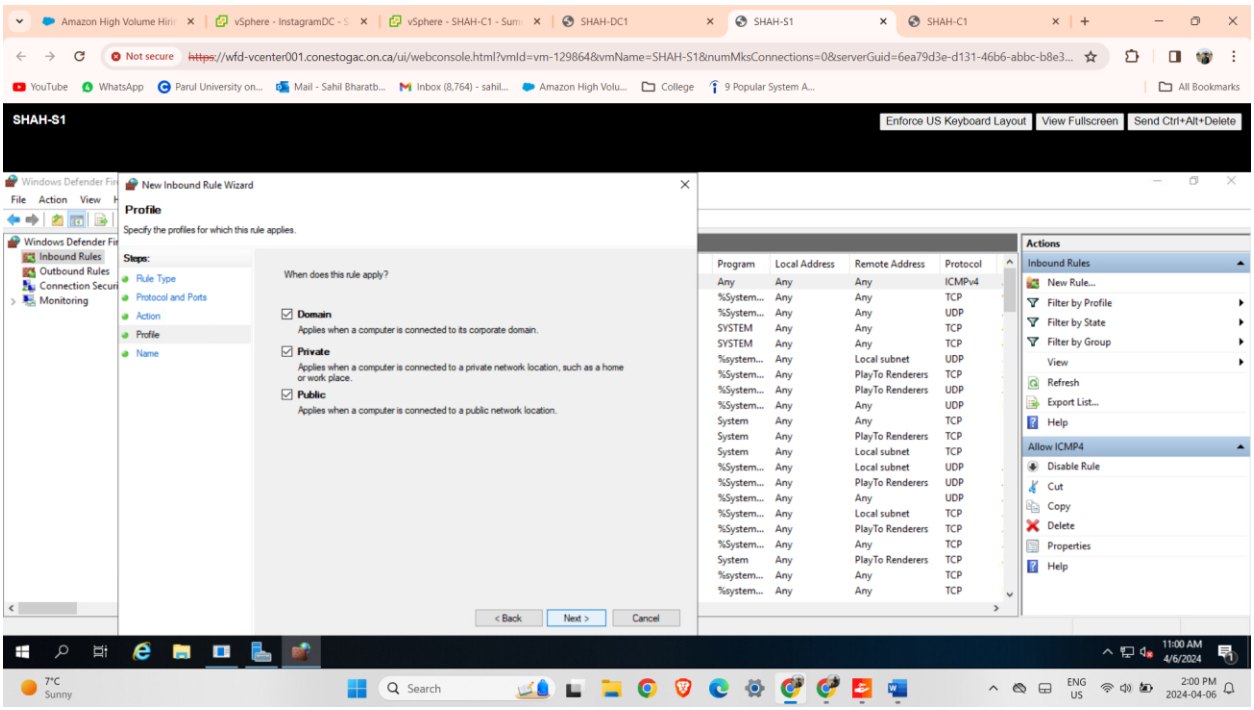
Select the rule type as TCP and specific local ports as 80



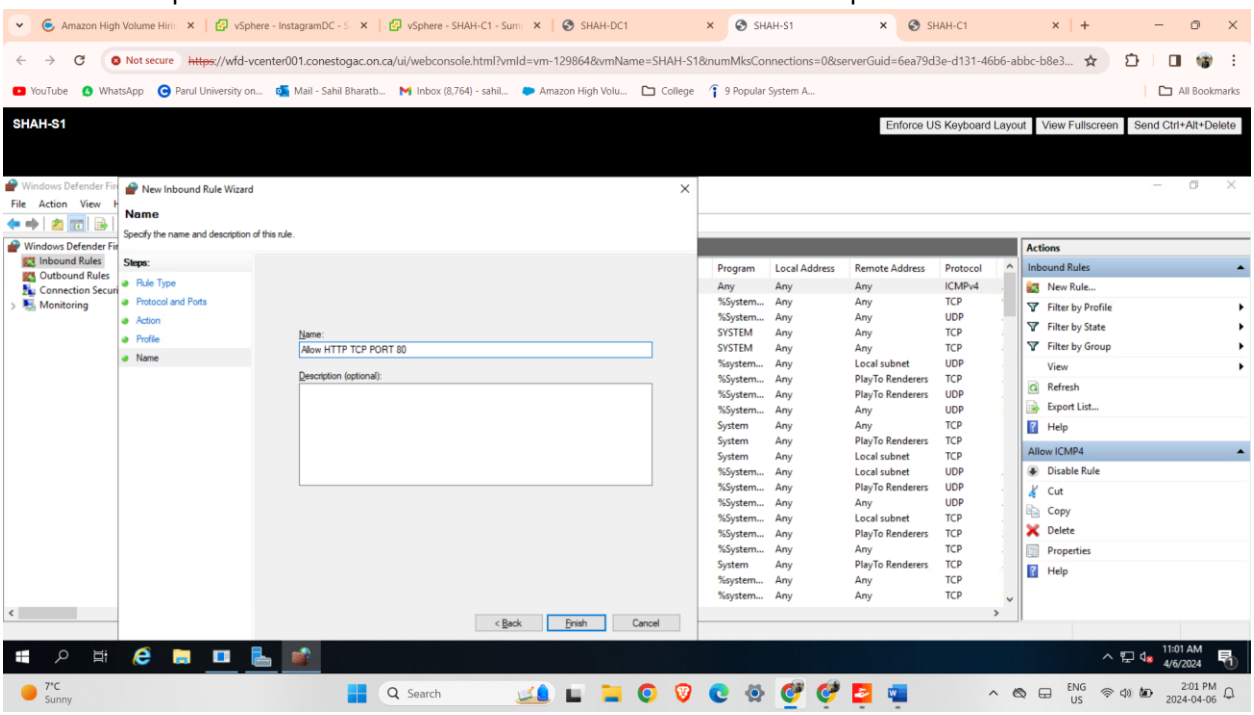
Select the action type as allow the connection



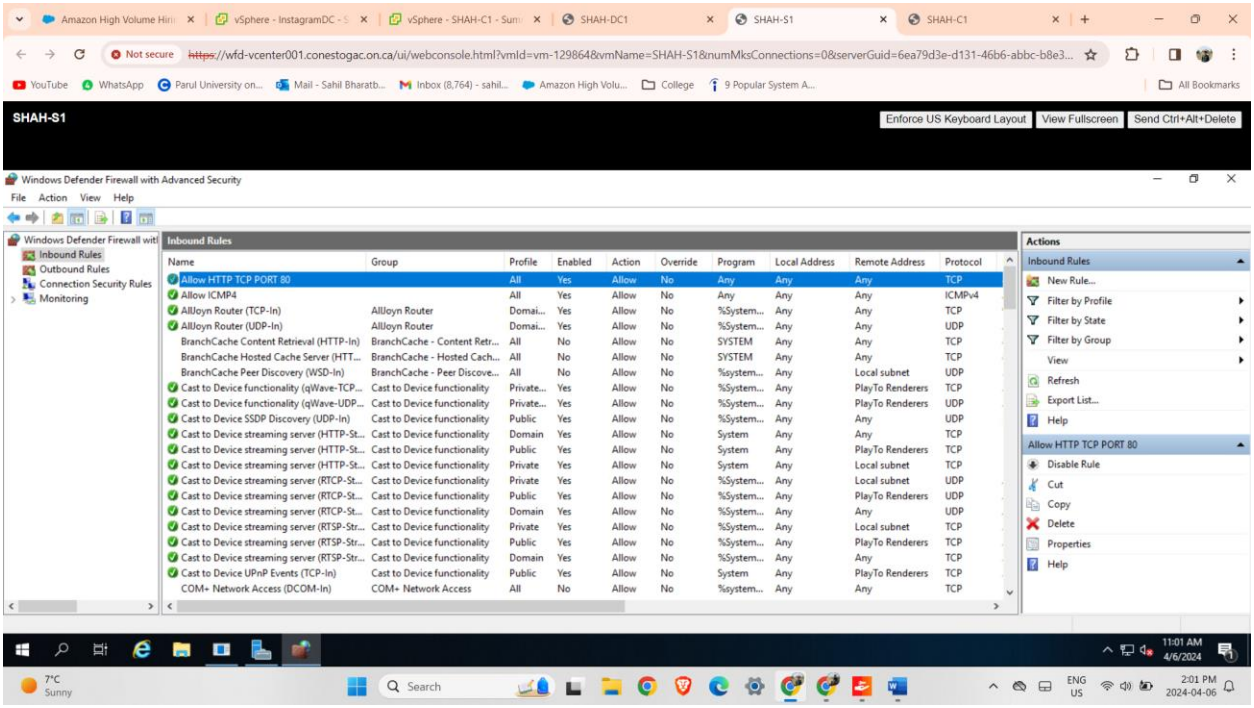
Select the rule to be applied on domain, private and public



Provide description and name for new rule creation as Allow HTTP TCP port 80

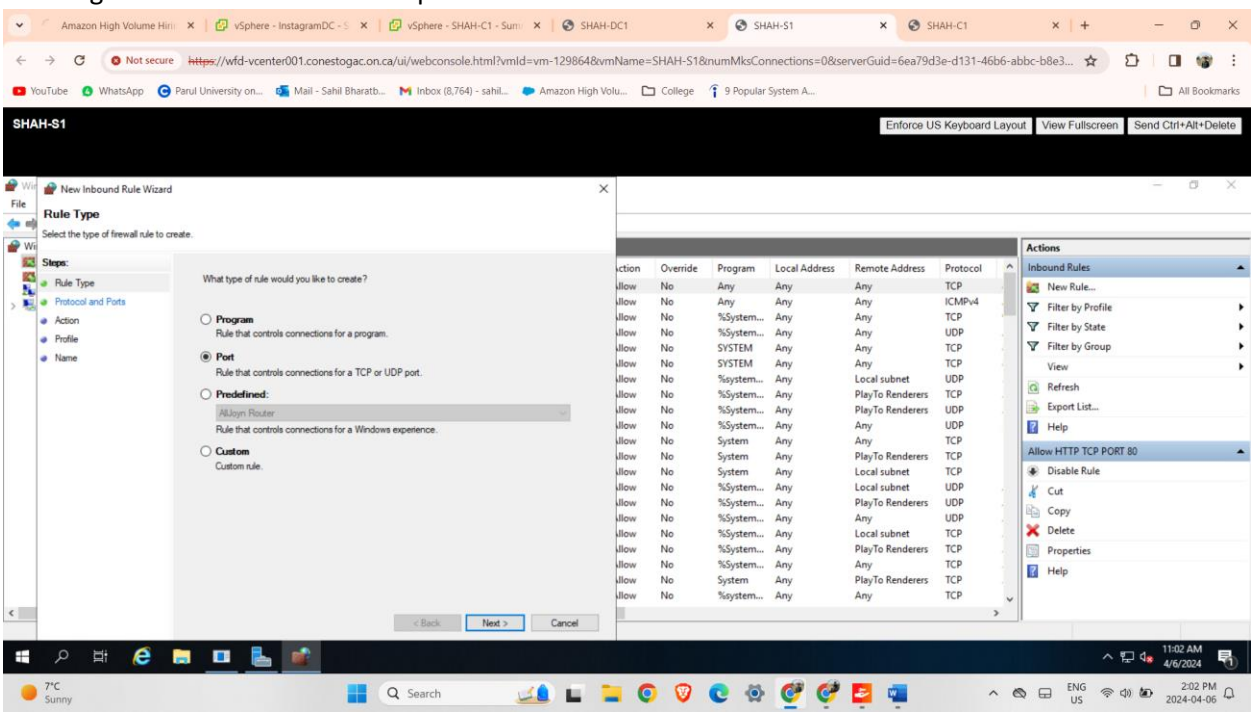


Successfully creating rule for HTTP TCP port 80

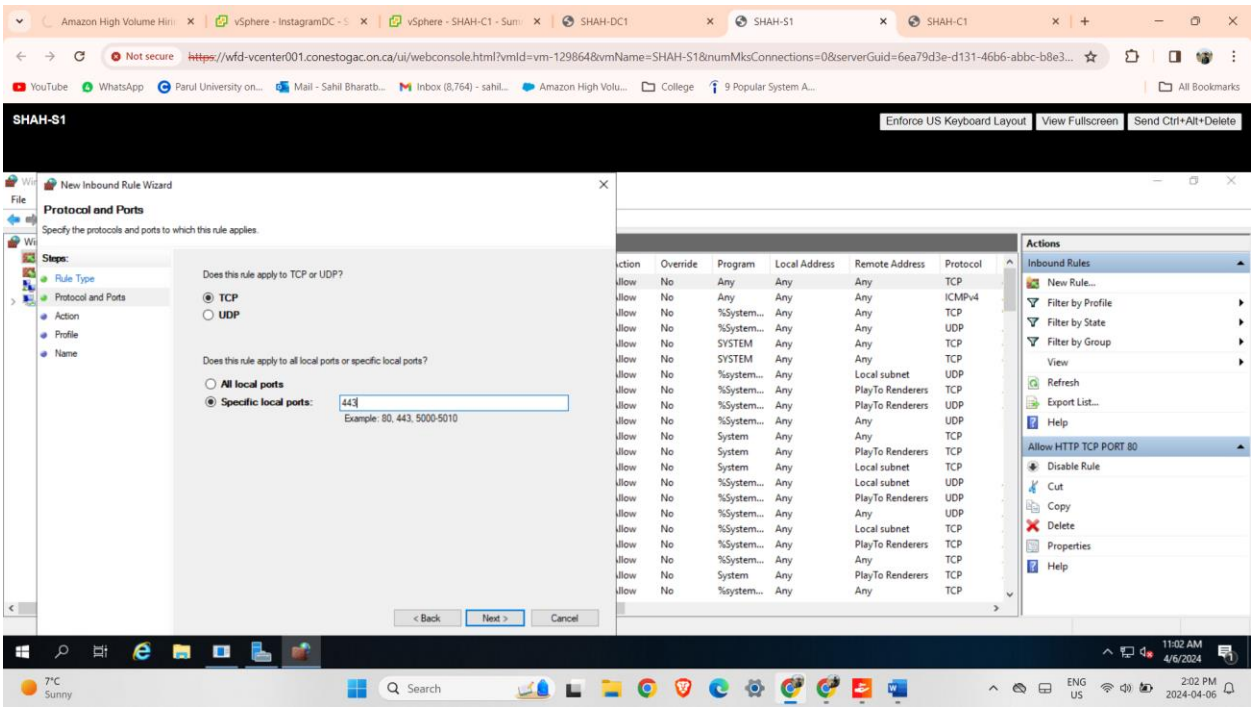


Allow HTTPS TCP Port 443

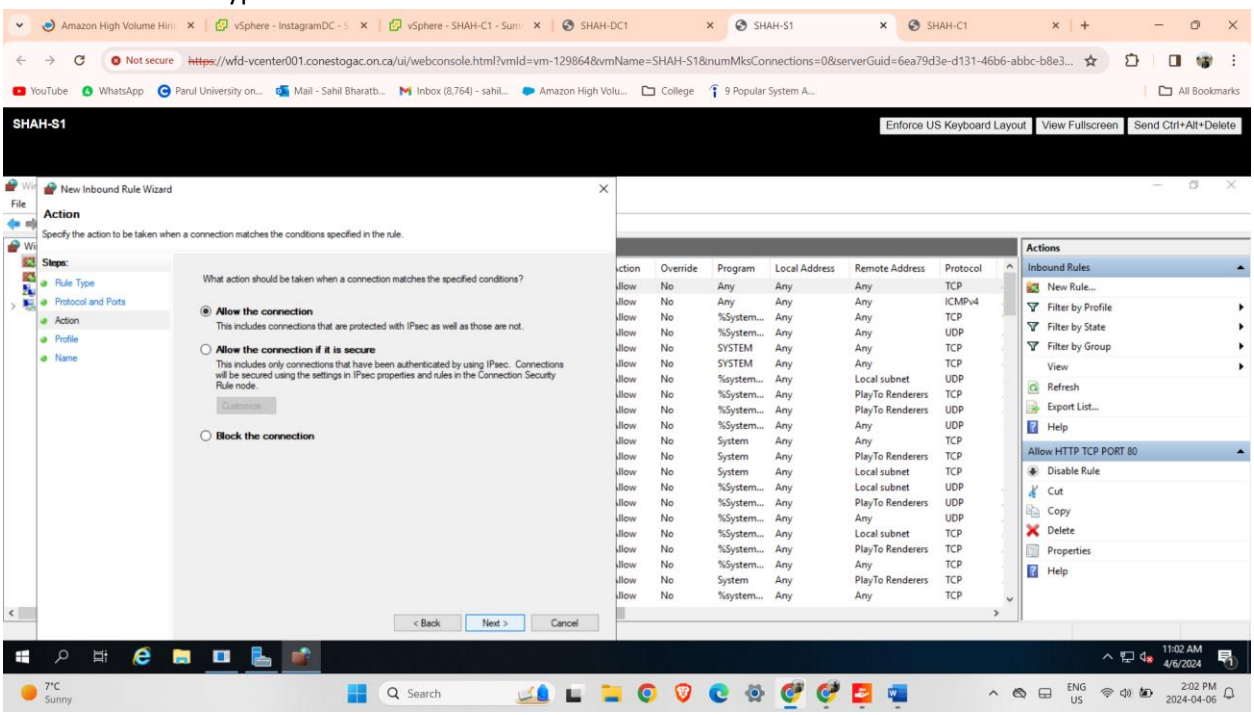
Creating a new rule for HTTPS TCP port 443



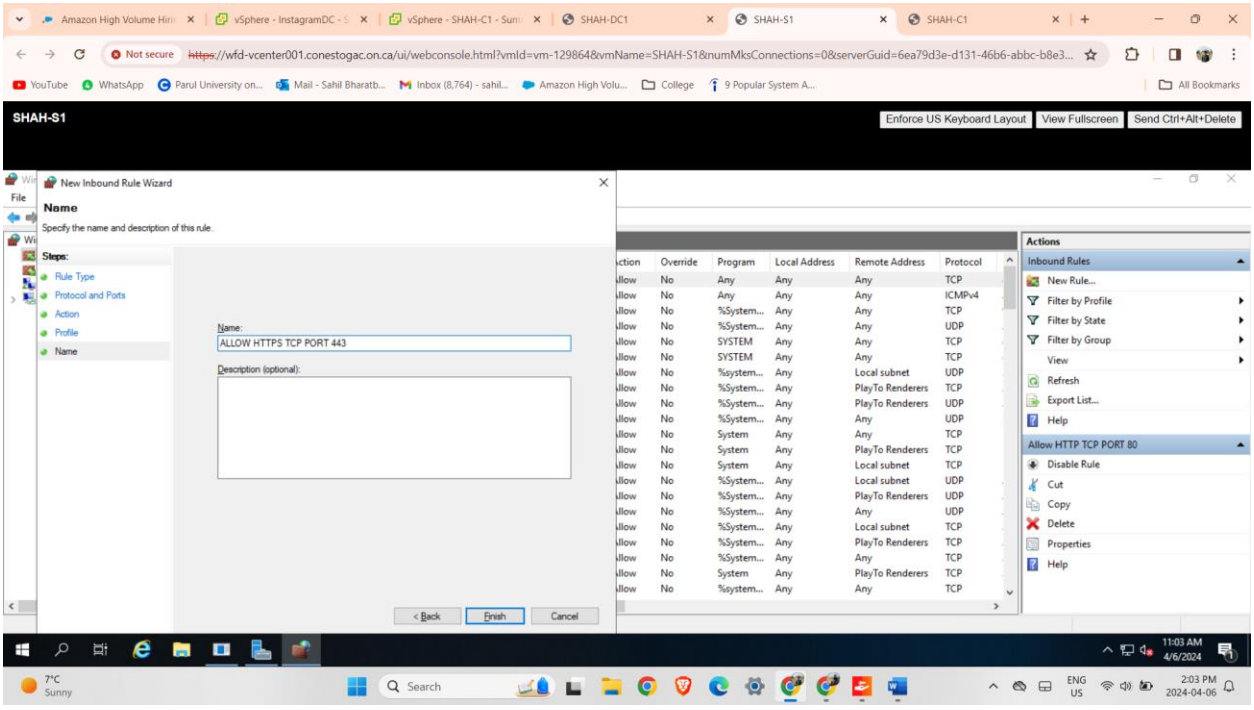
Select rule type as TCP and specific local ports as 443



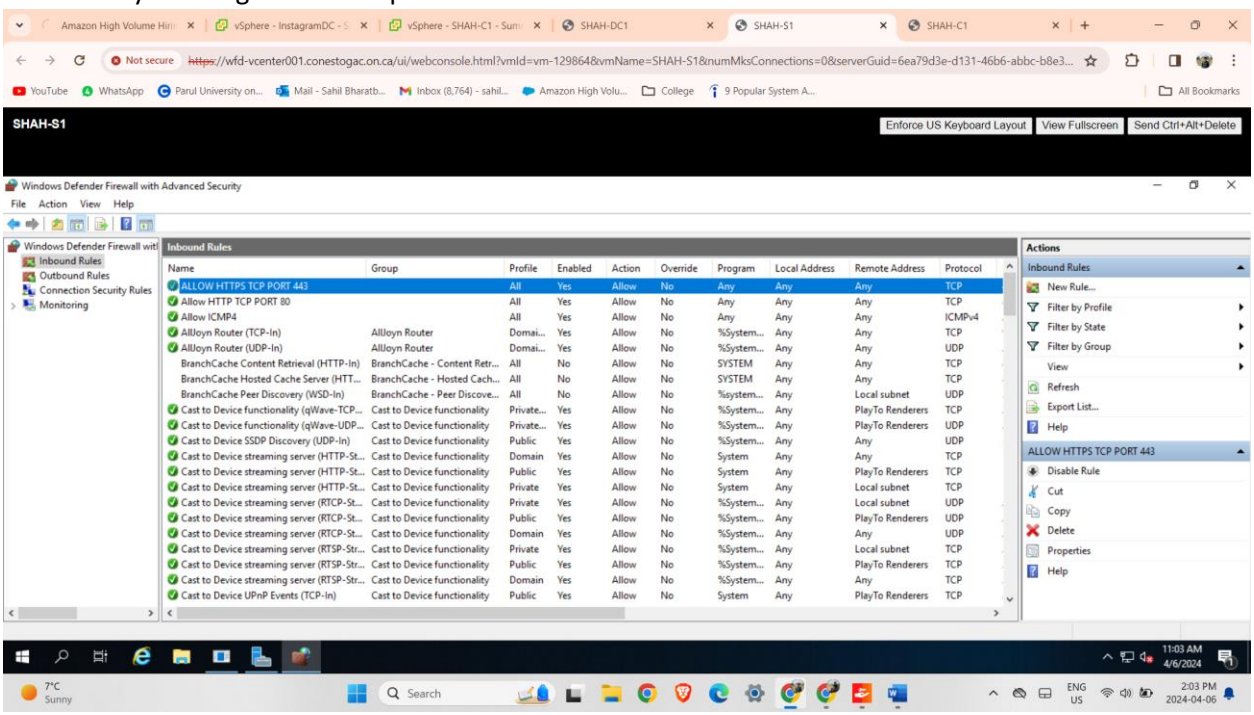
Provide an action type to allow the connection.



Specifying name type as “Allow HTTPS TCP port 443”

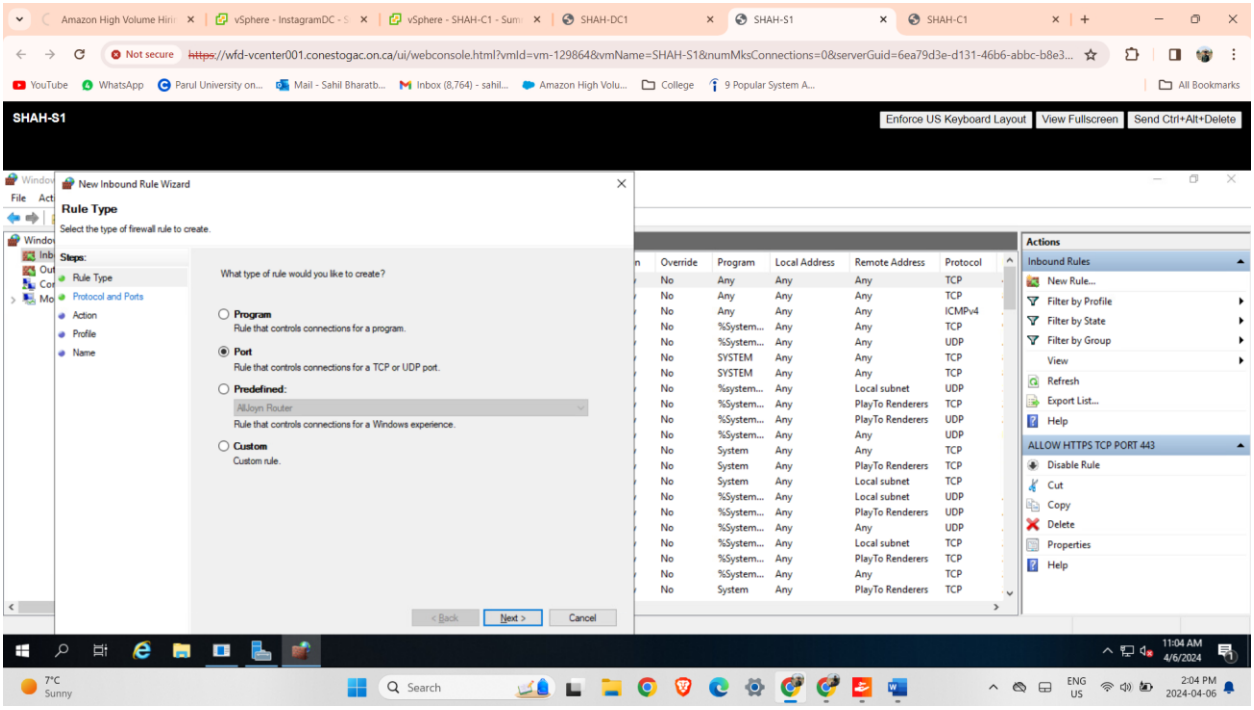


Successfully creating HTTPS TCP port 443 rule.

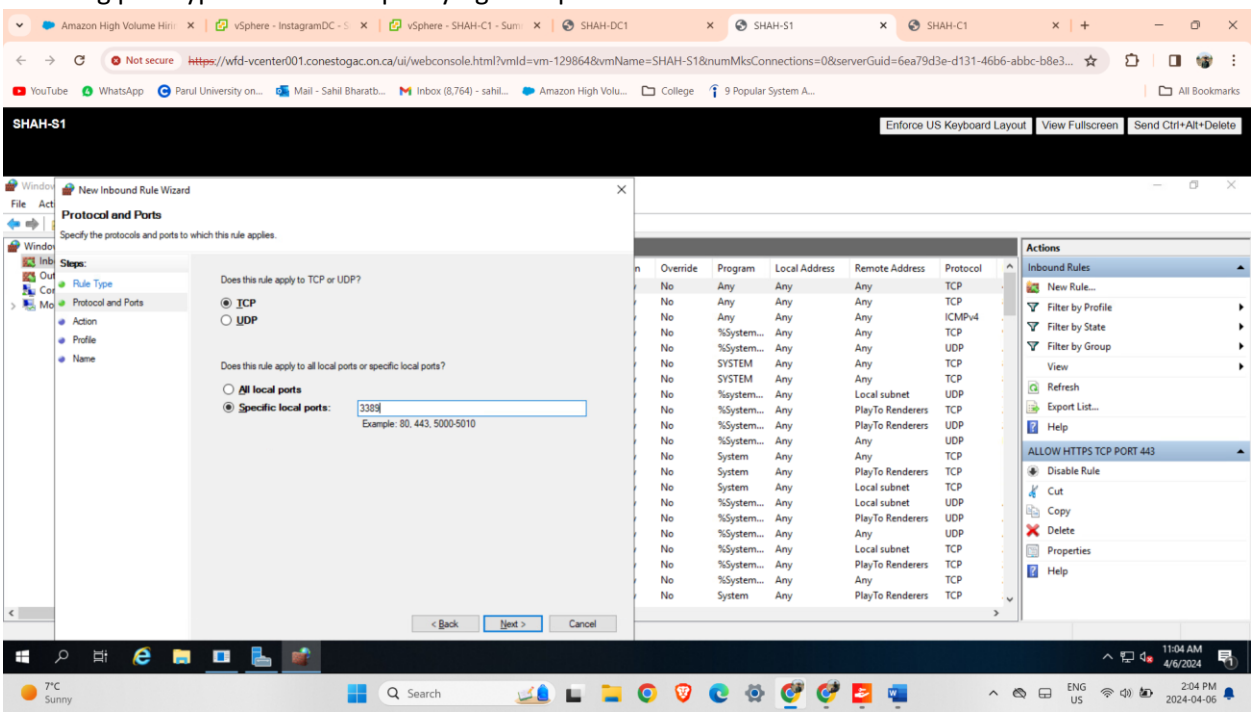


Allow RDP TCP Port 3389

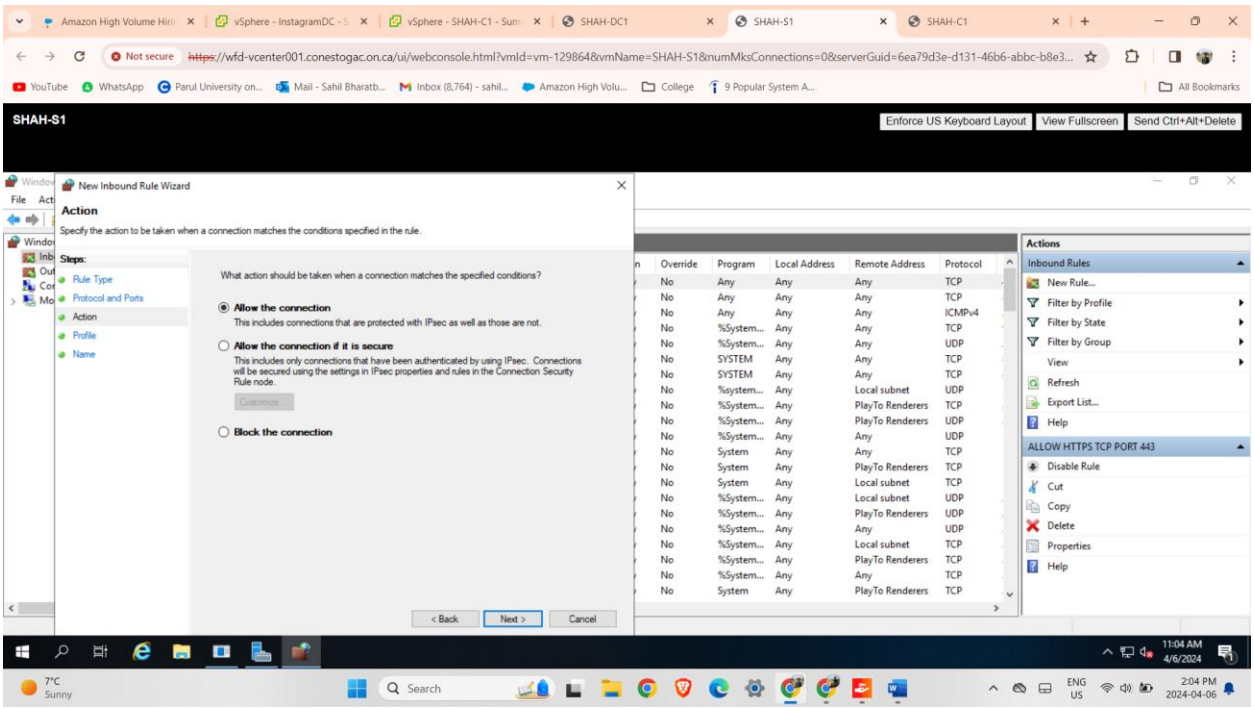
Creating new rule for RDP TCP 3389 port



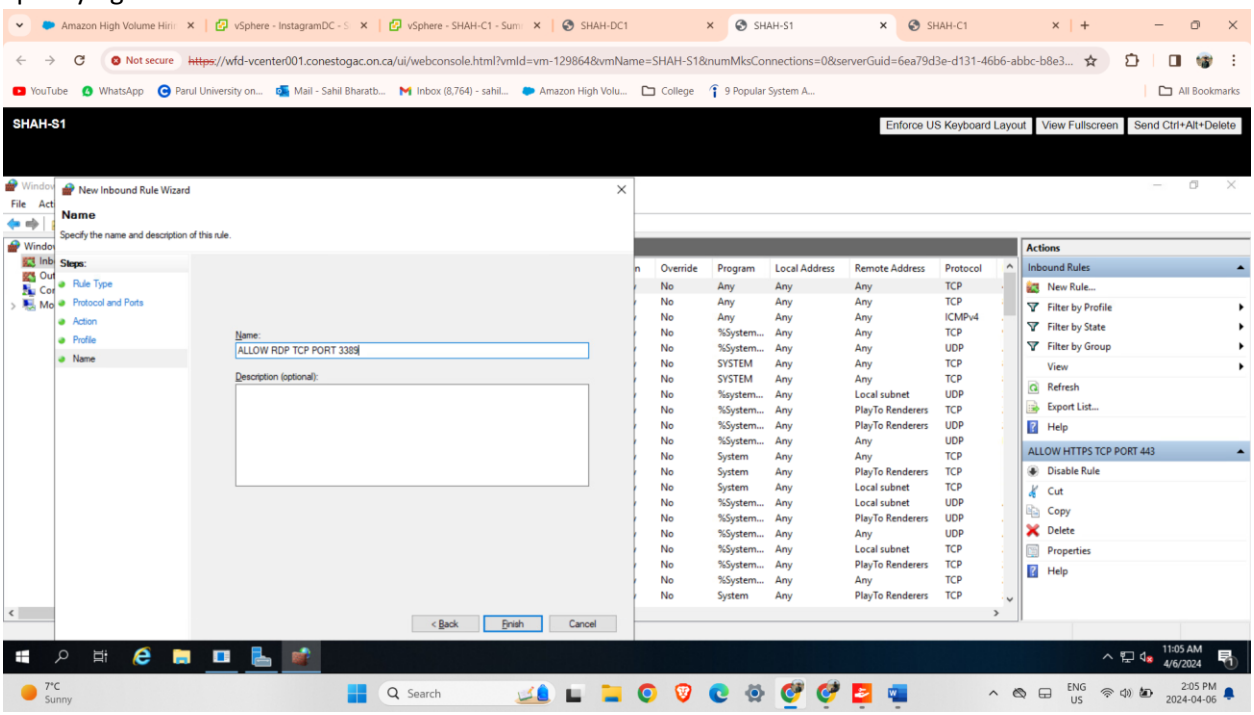
Selecting port type as TCP and specifying local ports as 3389



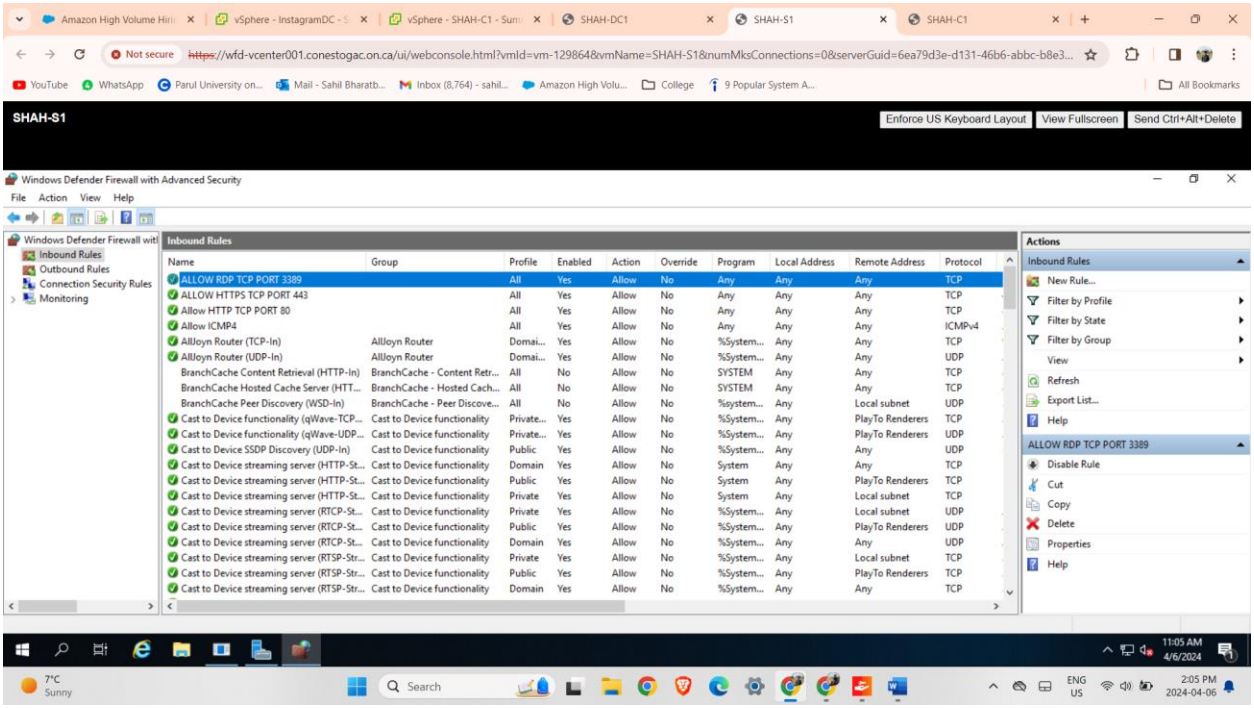
Select the action type to allow the connection.



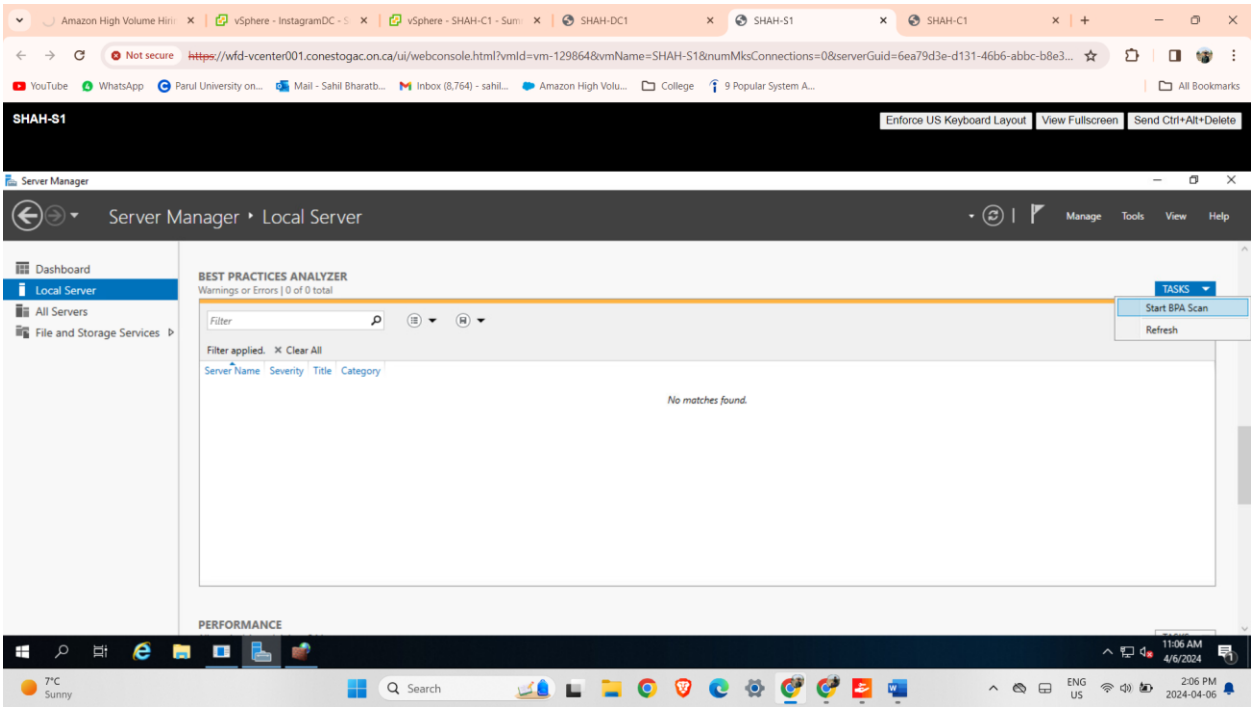
Specifying rule name as ALLOW RDP TCP Port 3389

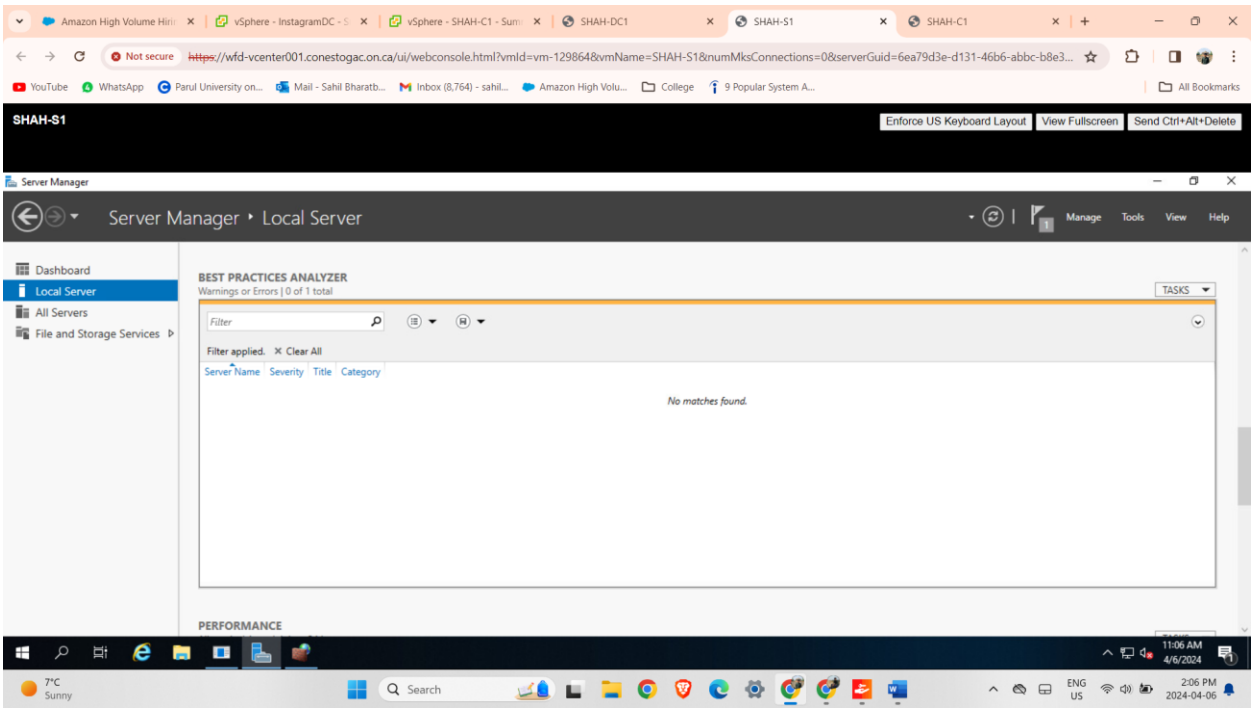


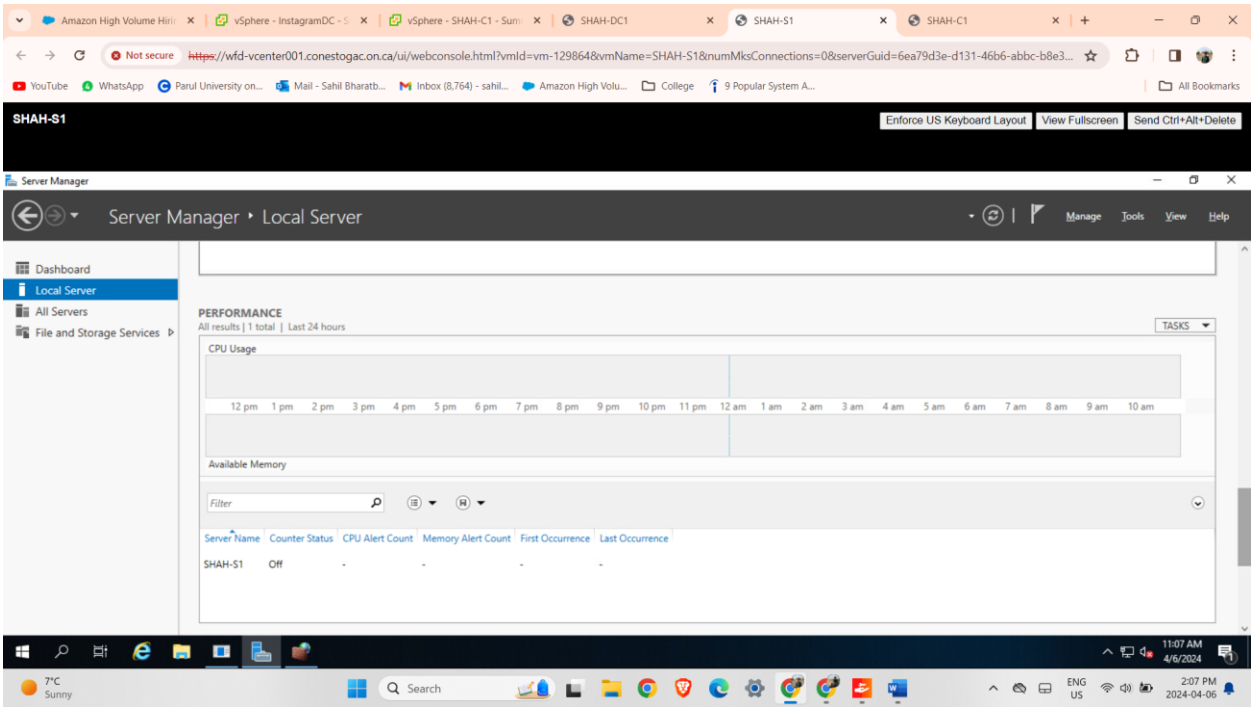
Successfully creating rule for RDP 3389



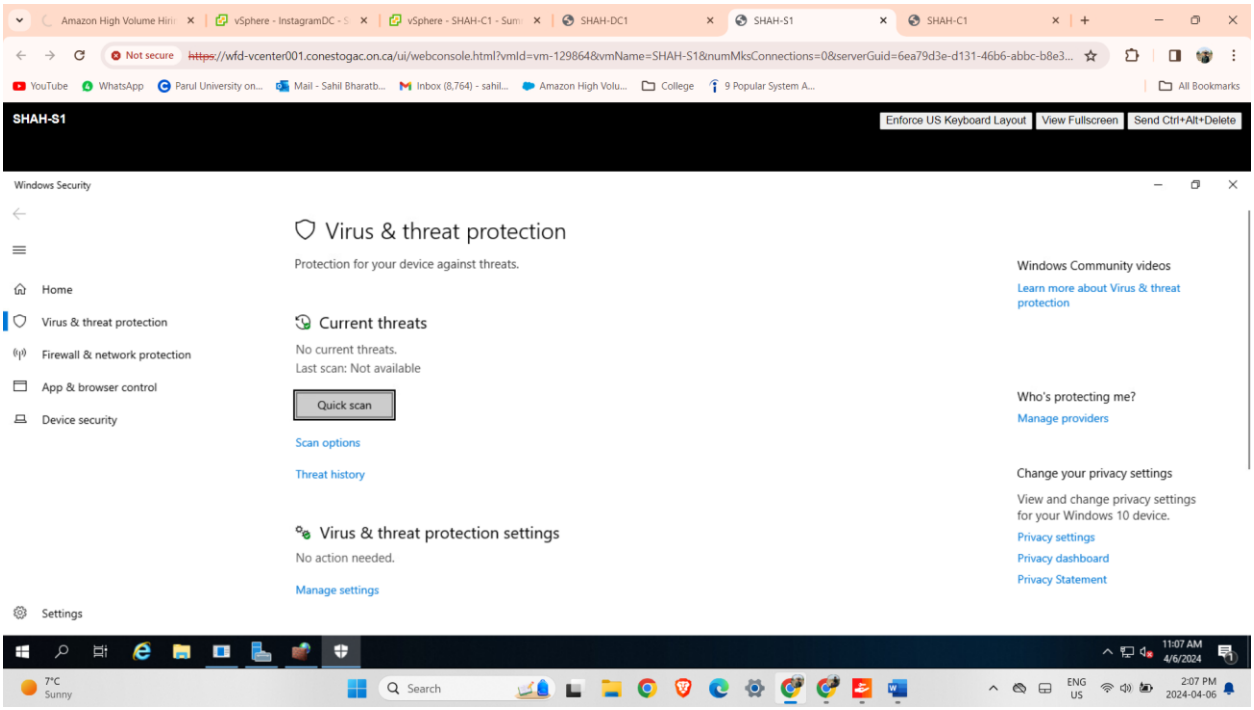
2] Run Best Practices Analyzer on SHAH-S1 (There may be no results after the scan that's ok).


SHAH-S1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Server Manager
Server Manager • Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
BEST PRACTICES ANALYZER
Warnings or Errors | 0 of 0 total
TASKS
Start BPA Scan
Refresh
Filter
Filter applied.
Clear All
Server Name
Severity
Title
Category
No matches found.
PERFORMANCE

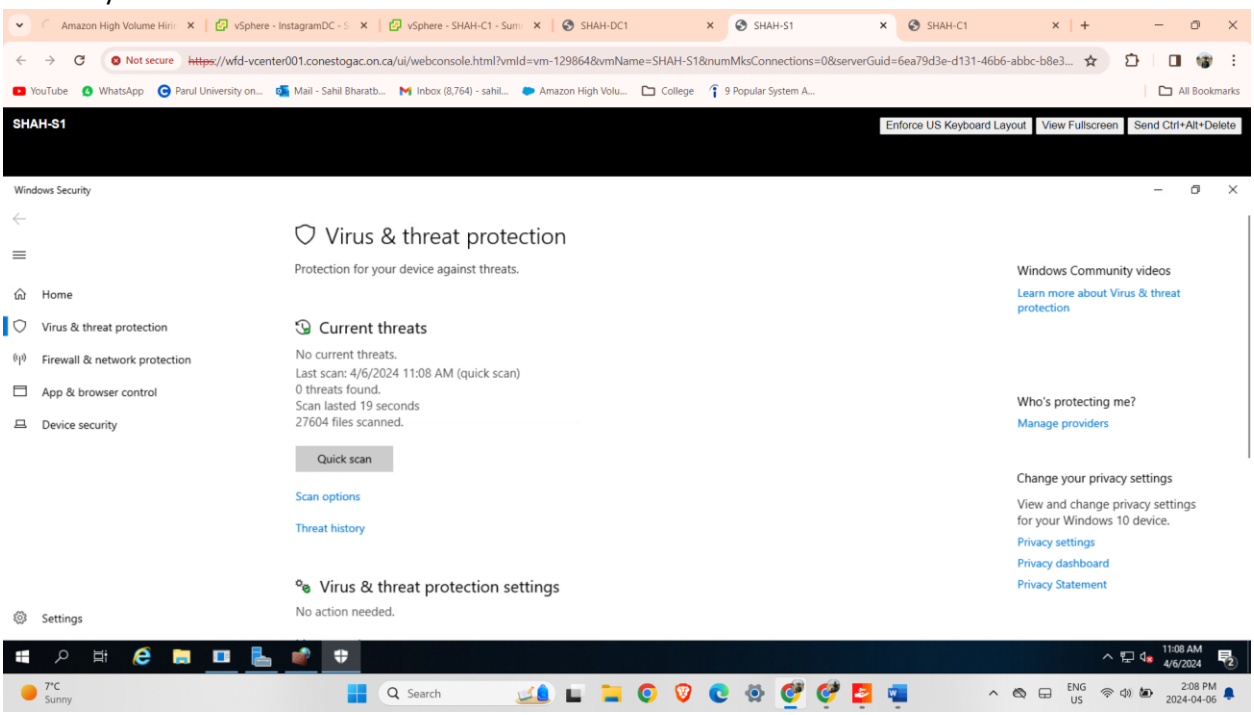

SHAH-S1
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Server Manager
Server Manager • Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
BEST PRACTICES ANALYZER
Warnings or Errors | 0 of 1 total
TASKS
Filter
Filter applied.
Clear All
Server Name
Severity
Title
Category
No matches found.
PERFORMANCE

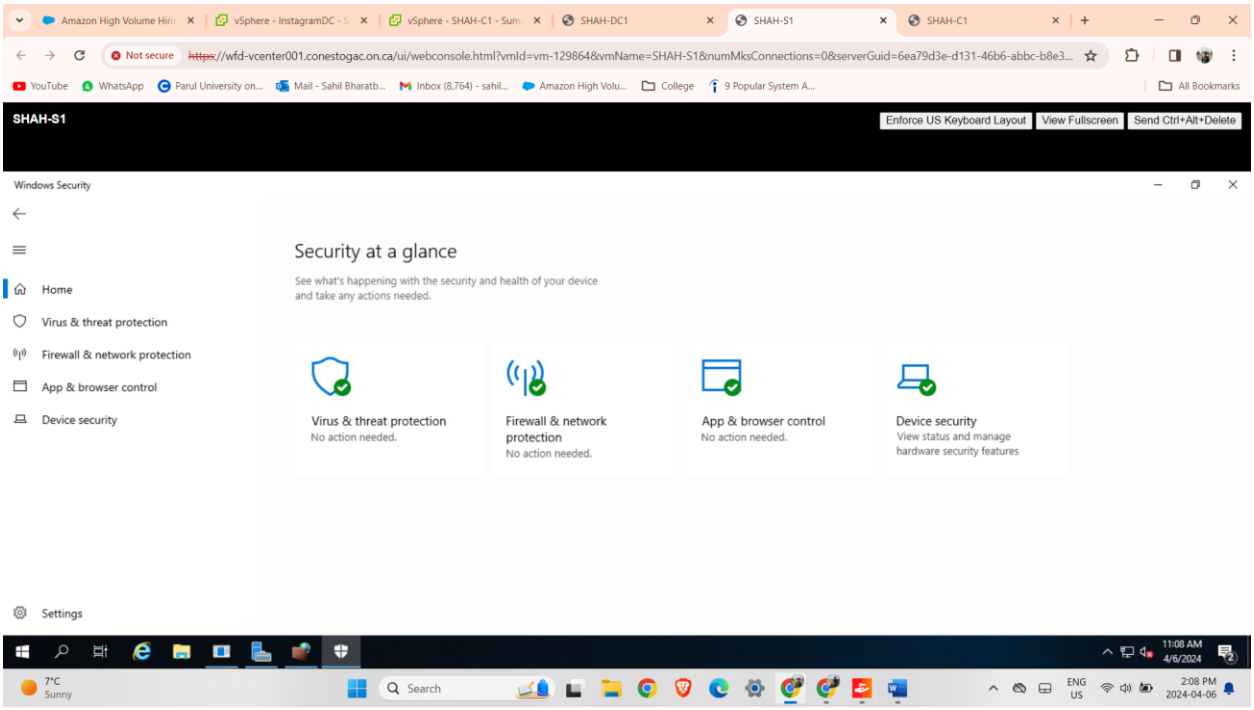


3] Run a quick scan in Windows Defender on SHAH-S1.



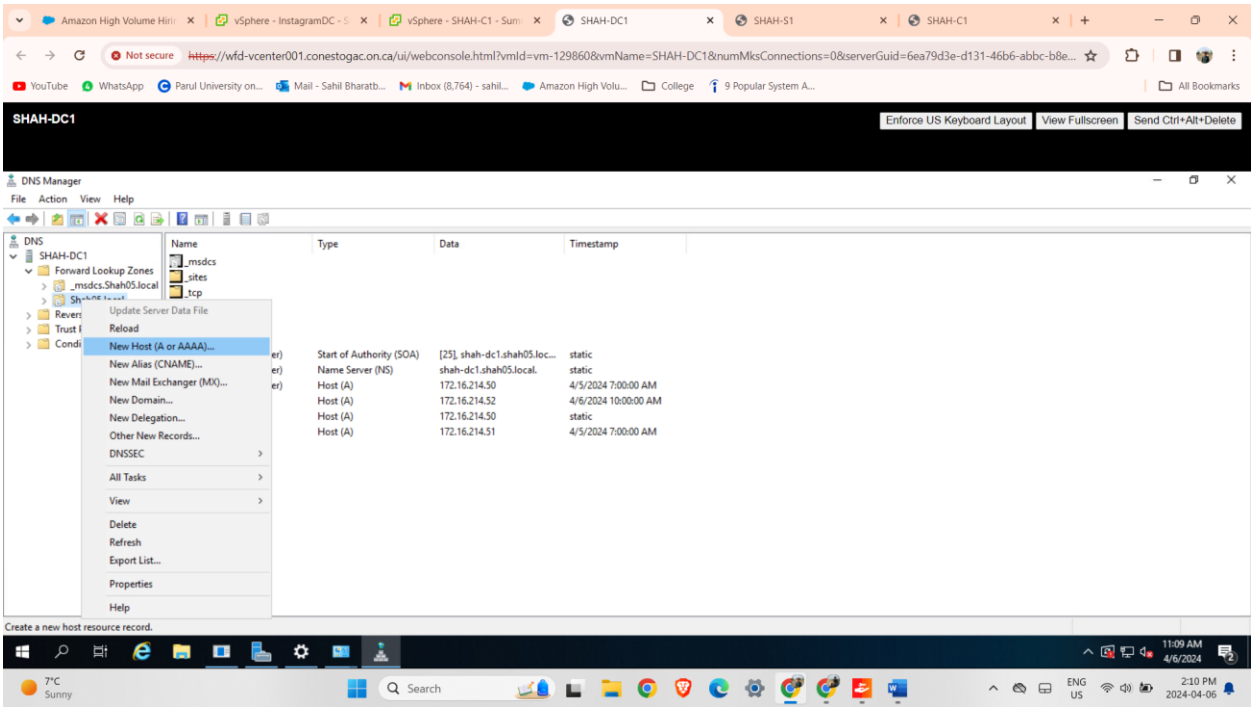
Summary of scan done.



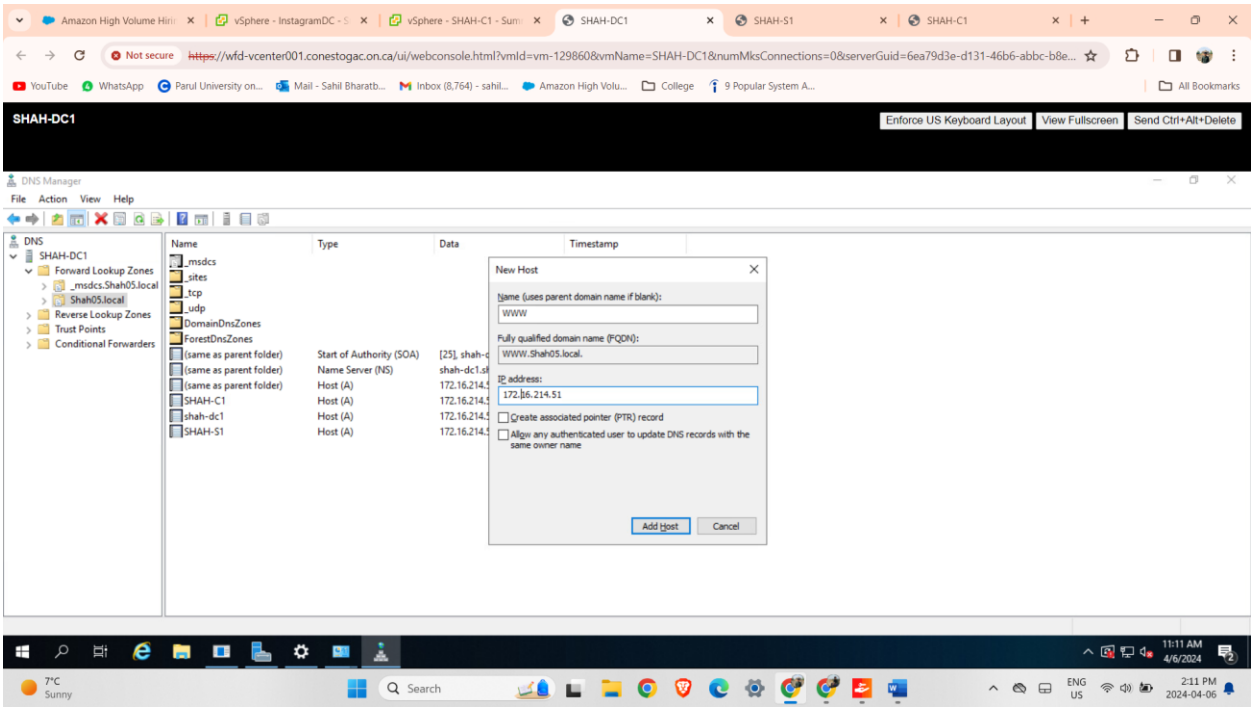


Part 2: Web Server (IIS)

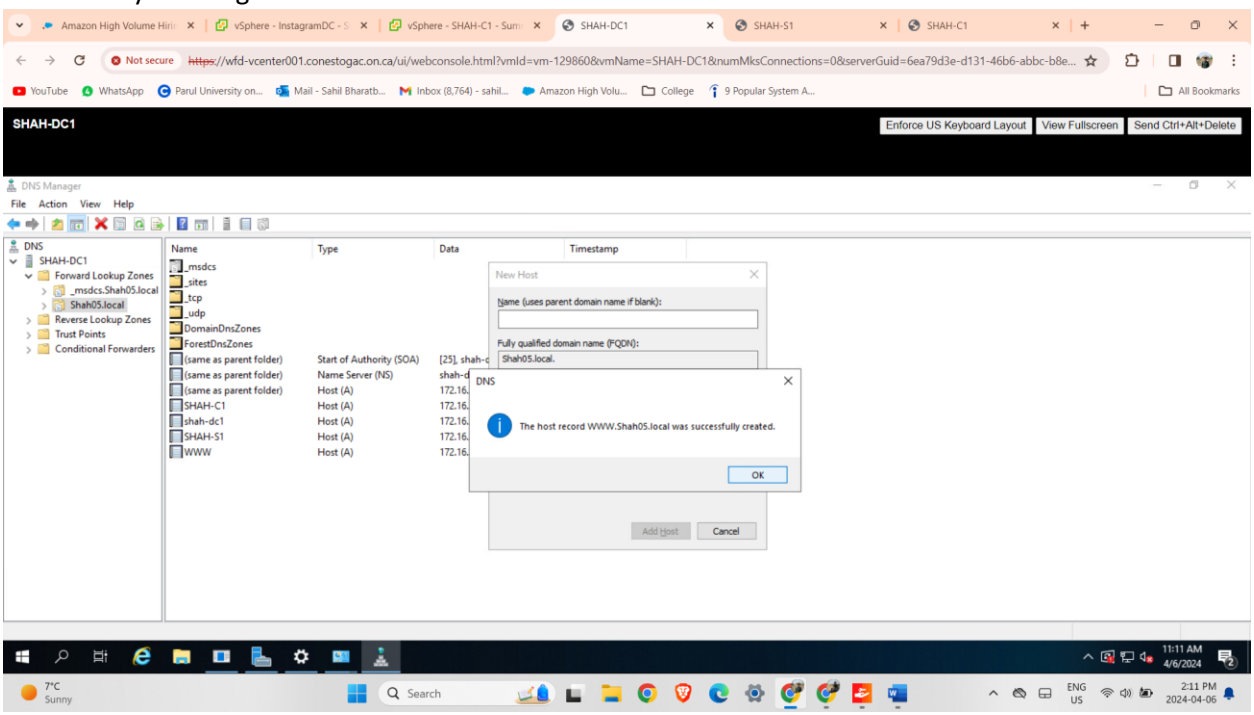
1] Create a Host A record on DC1 called www inside the Shah05.local forward lookup zone pointing to the IP address of SHAH-DC1.



Provide name for new A host as www with IP address as 172.16.214.51

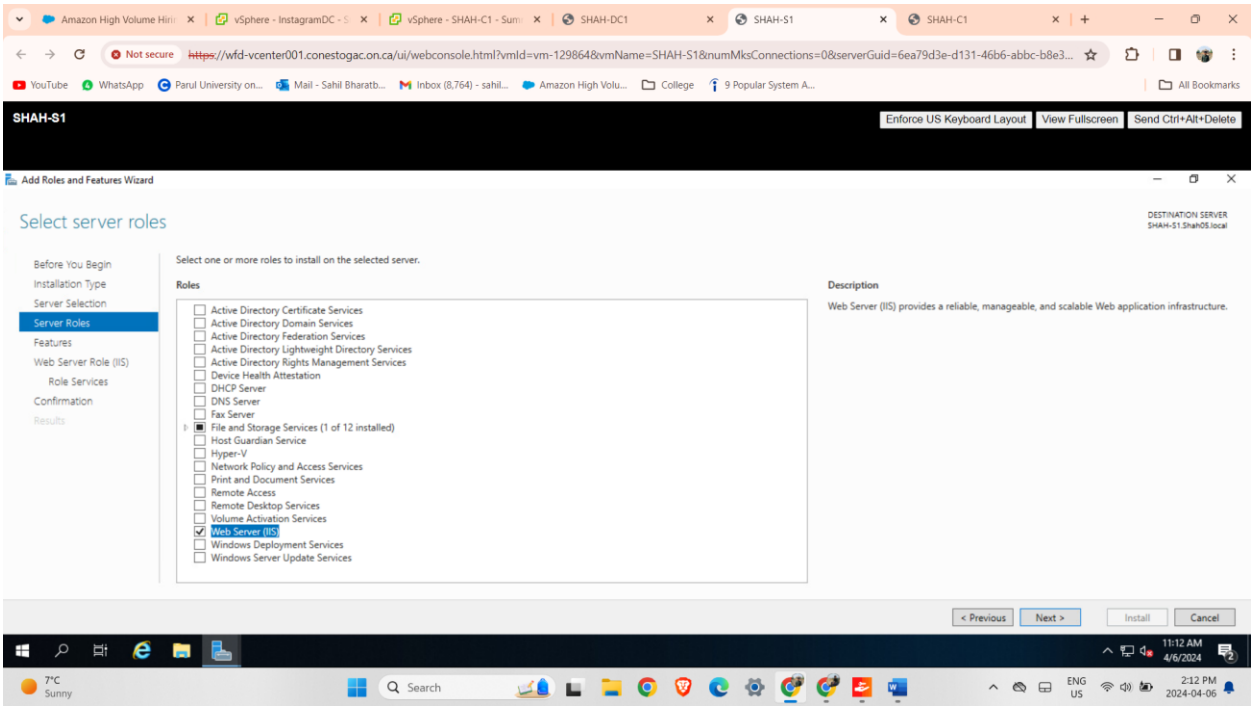


Successfully creating the host record.

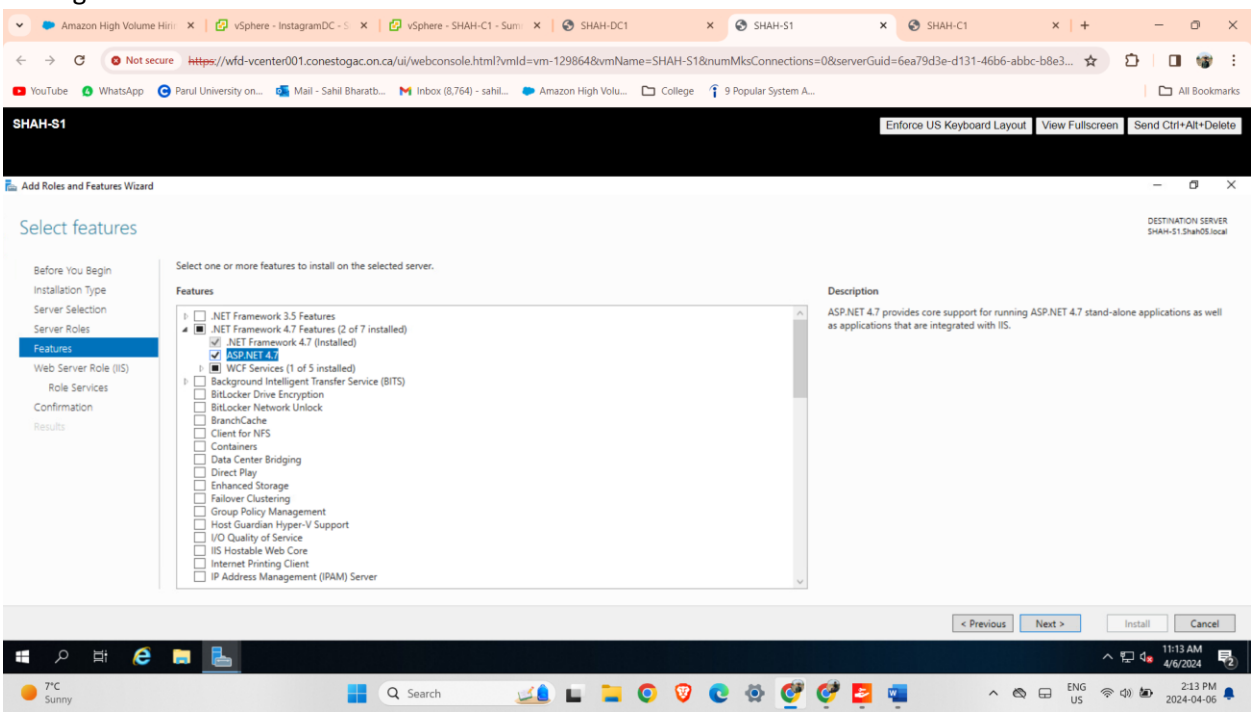


2] Install the IIS Role with the Application Development role feature on SHAH-S1. (Follow the IIS guide in week 13 for guidance).

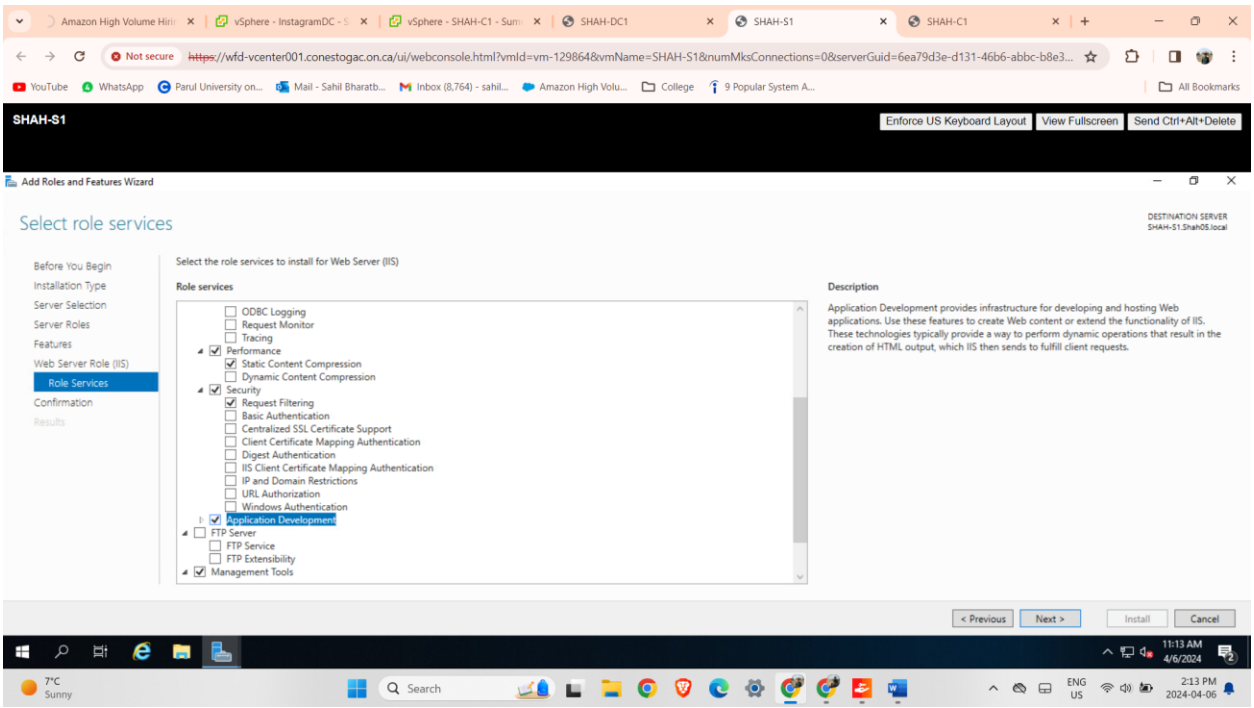
➔ Add web server (IIS) from Add Roles and Features.



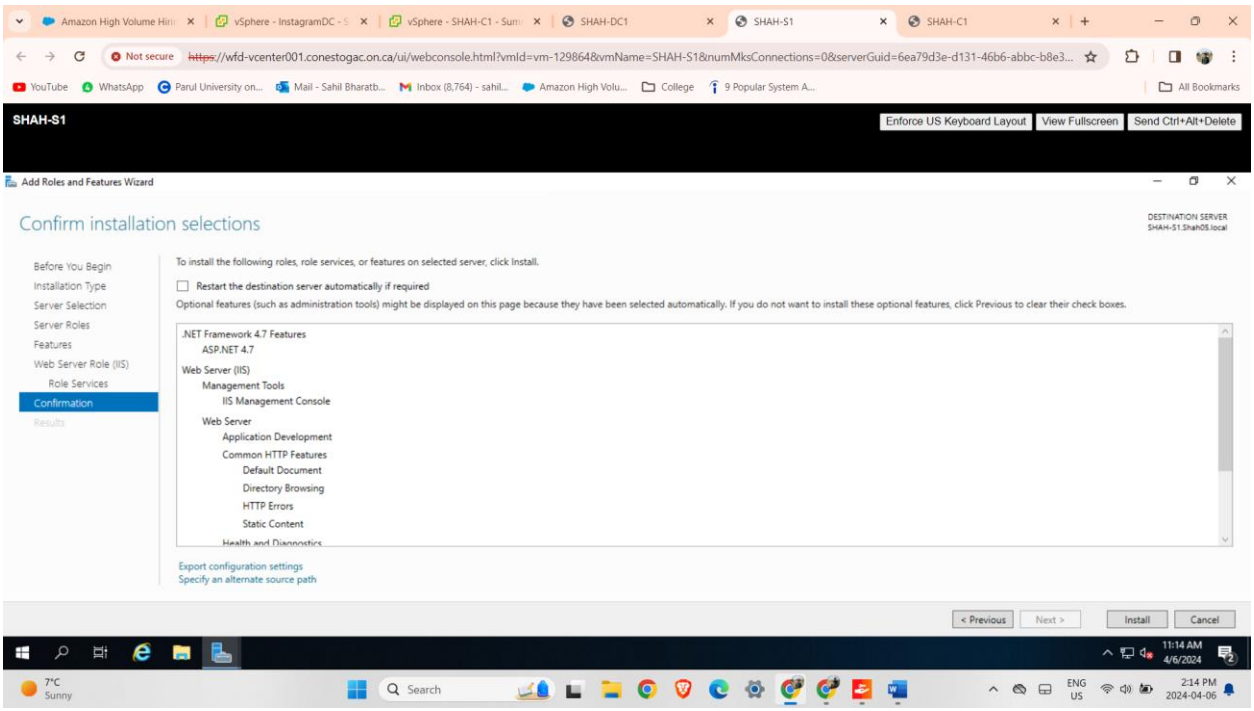
Adding feature of ASP.NET 4.7



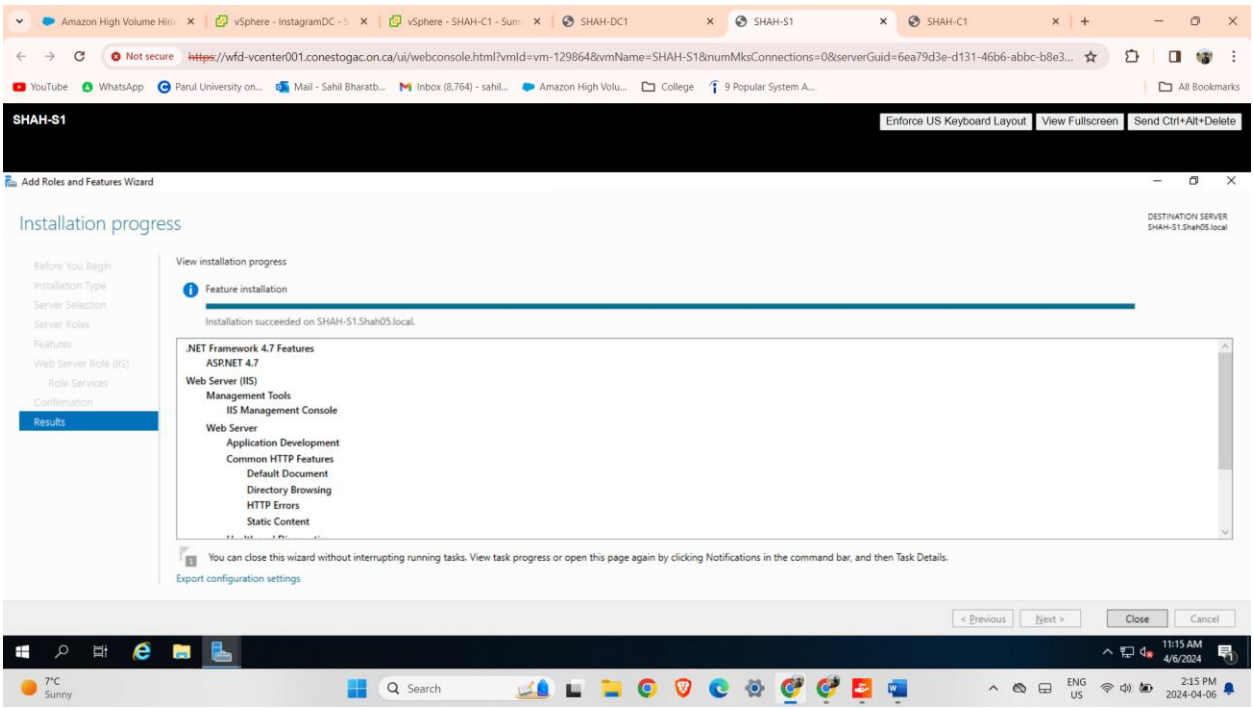
Enabling role services of Application development



Selection of Features and roles to install on SHAH-S1



Successfully installing the roles and features.



3] After IIS is installed, Access it from SHAH-C1 using www.shah05.local.