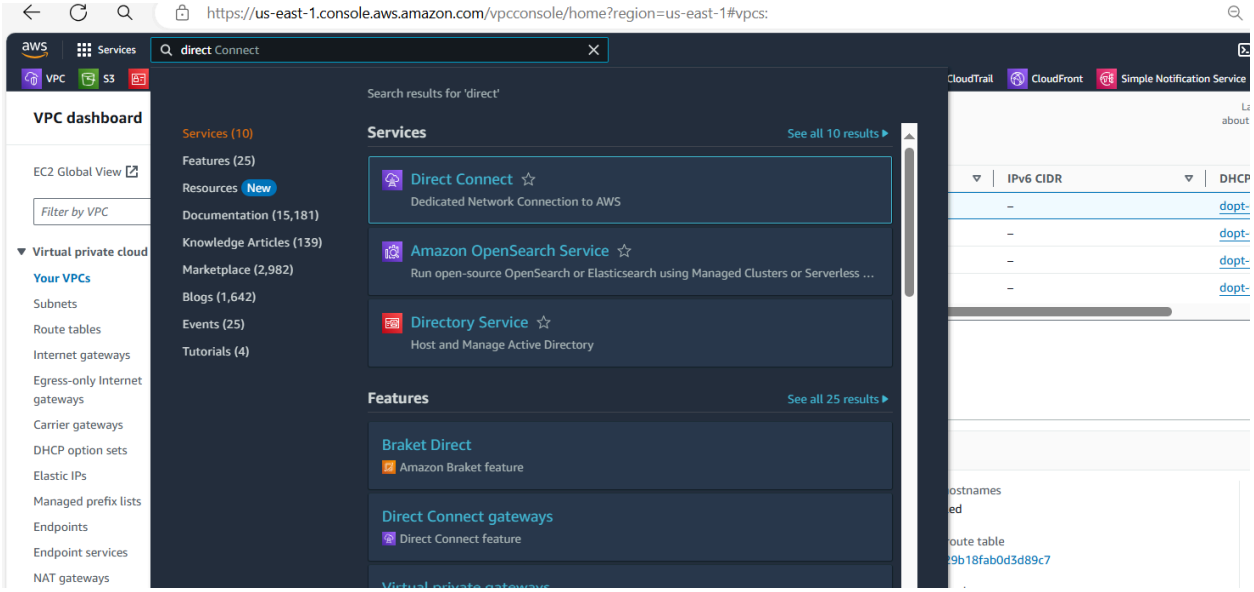
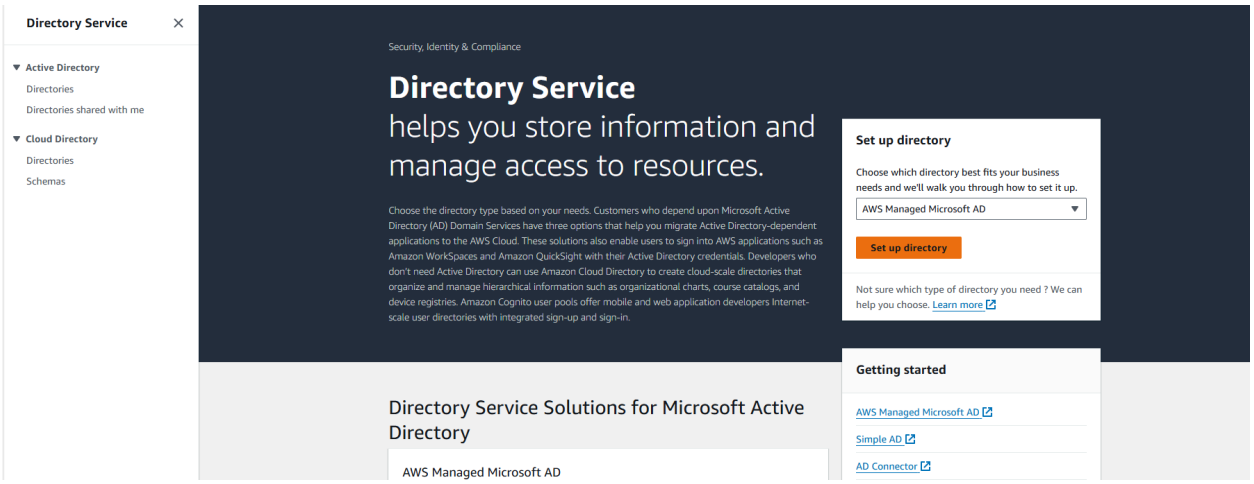
# How to Create AWS Managed AD And add Windows and Linux into AD Server and Create users

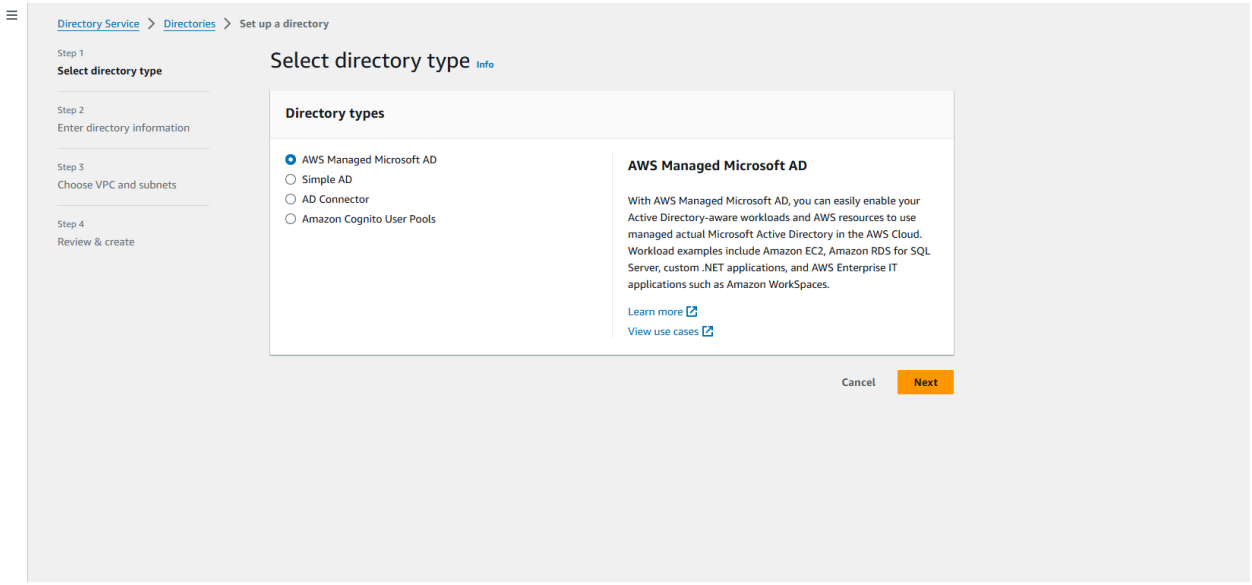
## 1-Click On Directory Service in AWS Console



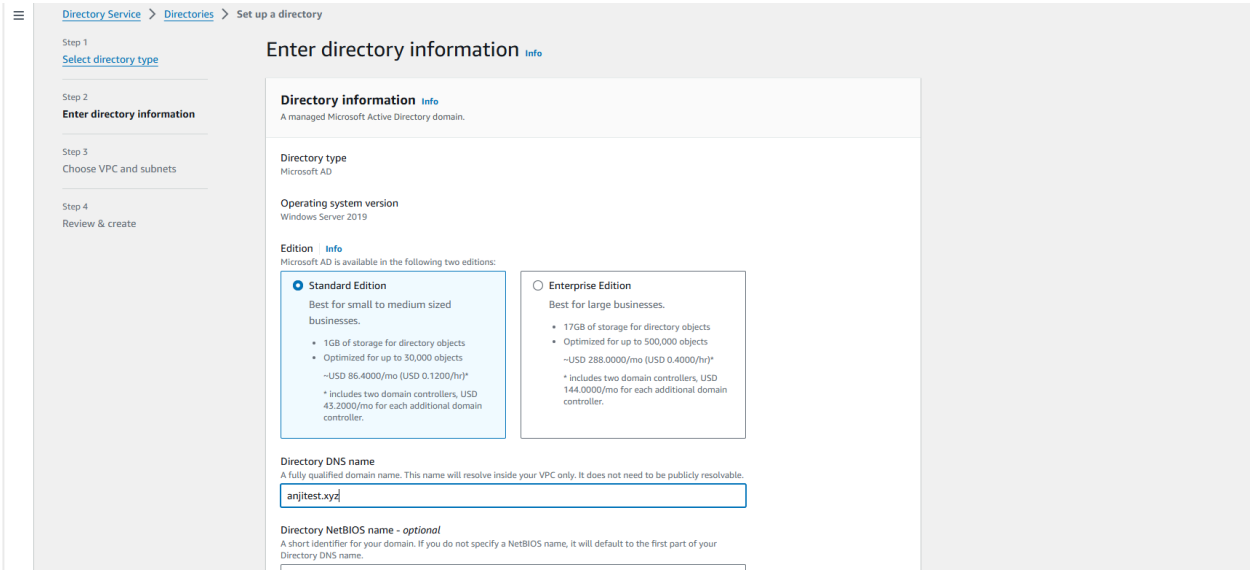

## 2-SetUp a Directory



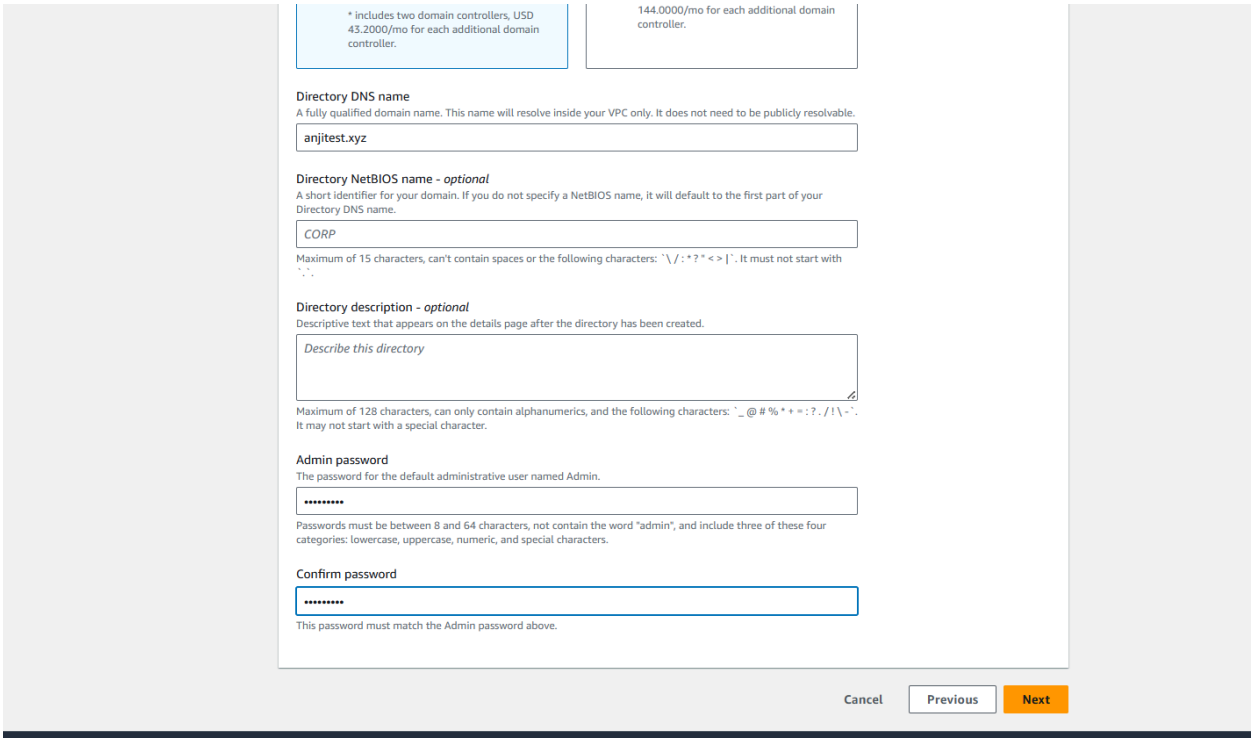

## 3-Select Aws Managed Directory



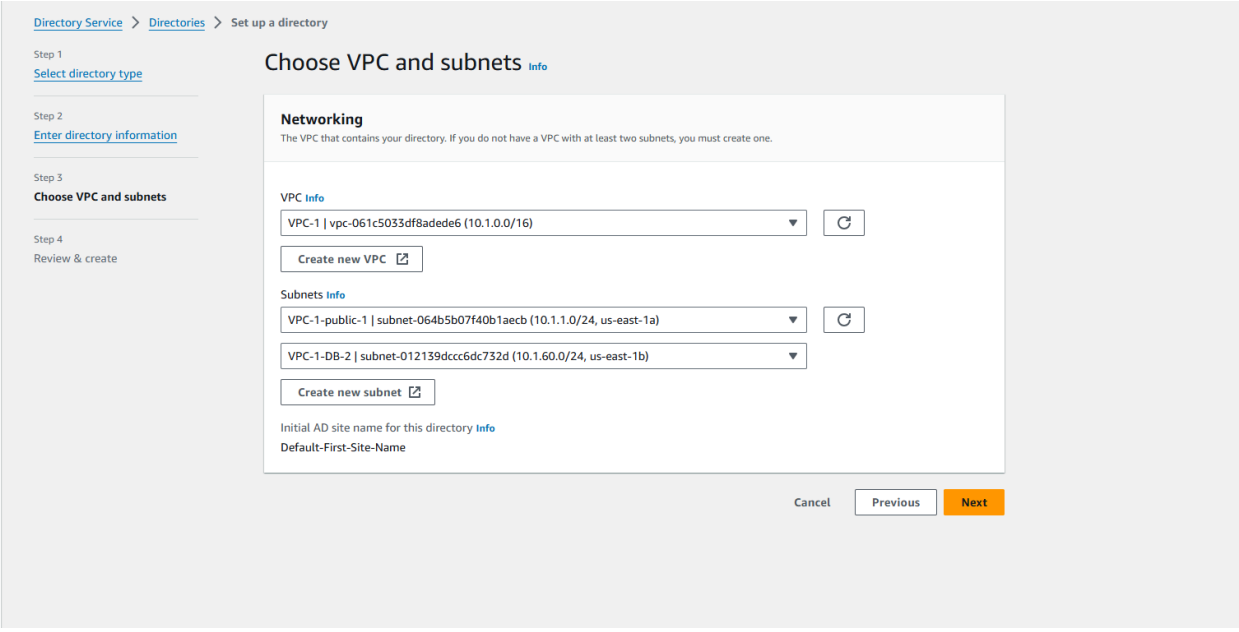

## 4-Select Standard or Enterprise Editions
## 5-Give Directory Name anjitest.xyz Any name is fine



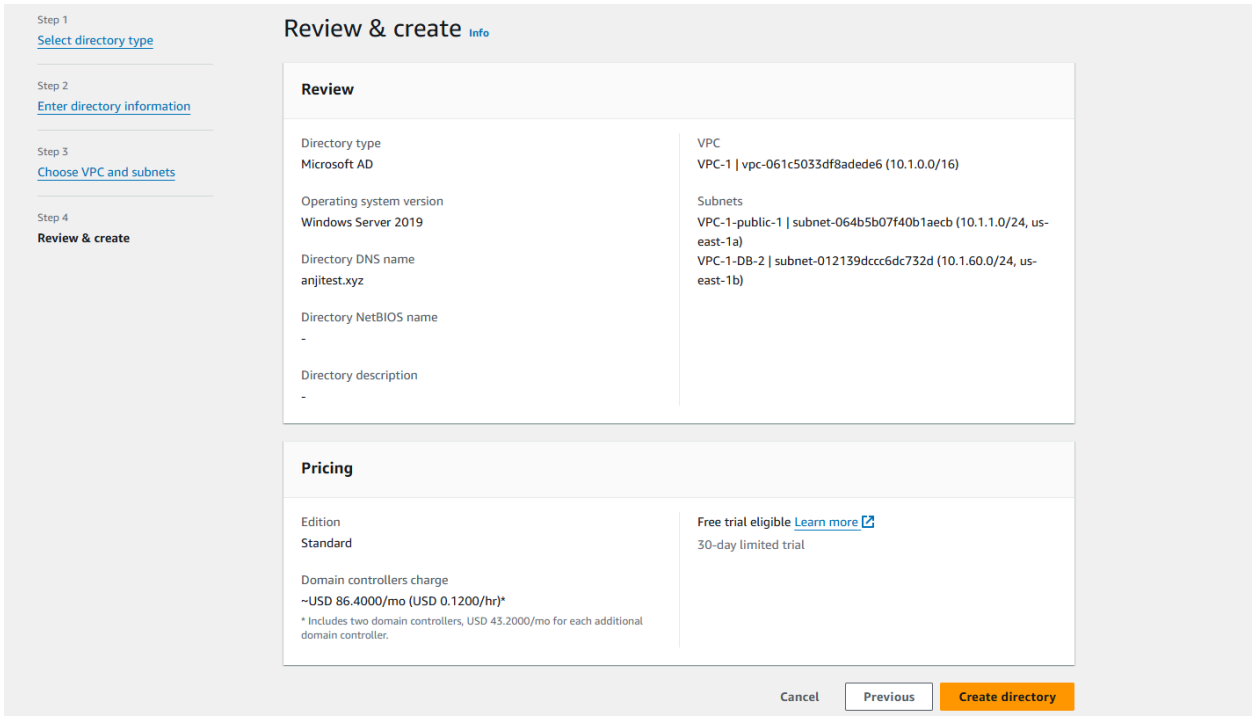

## 6-Give Password and click on Next



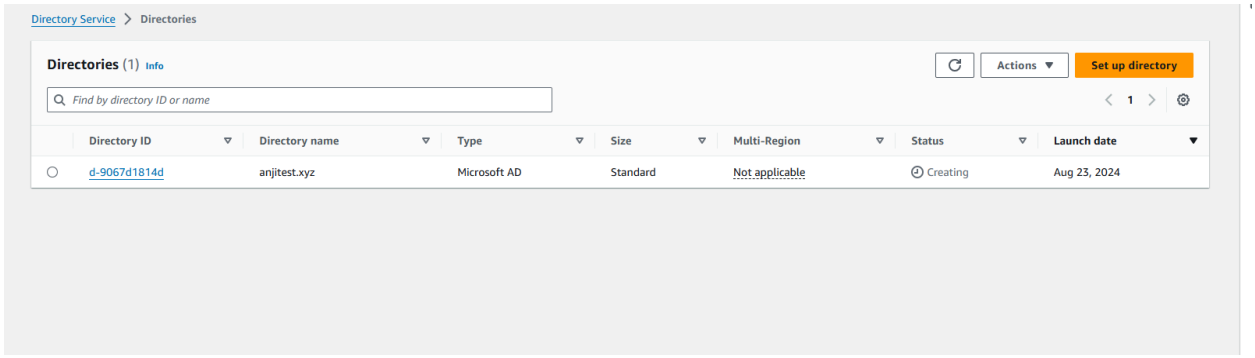

# 7-Select the VPC
# 8-Select the Subnets



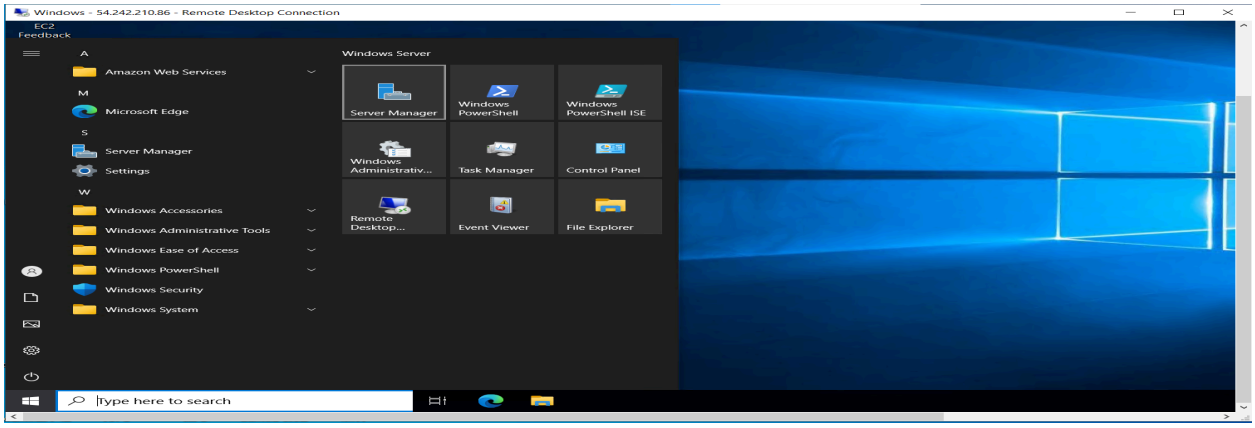

# 9-Click on Create Create Directory



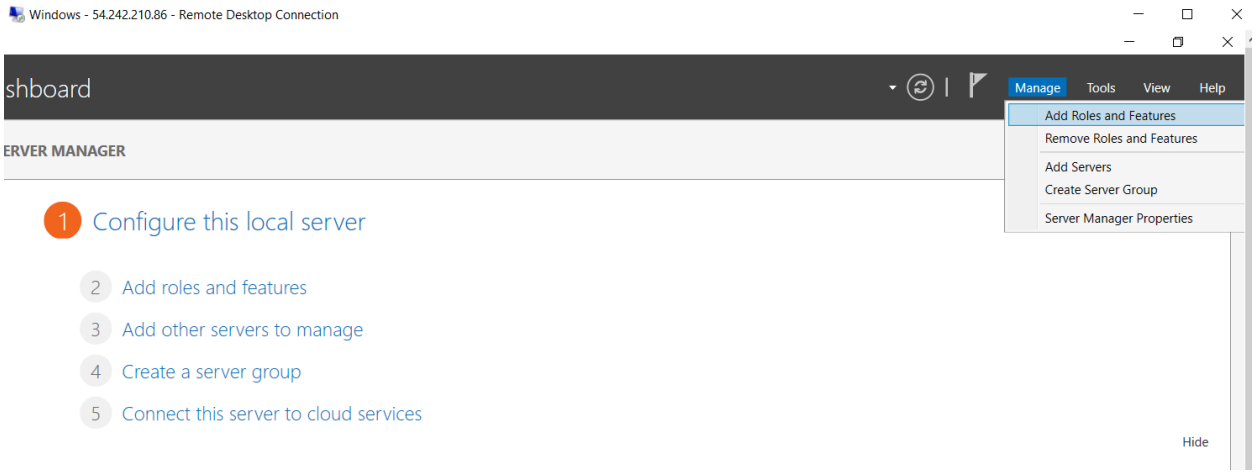

## 10-Click on Create. It takes 20-45 minutes



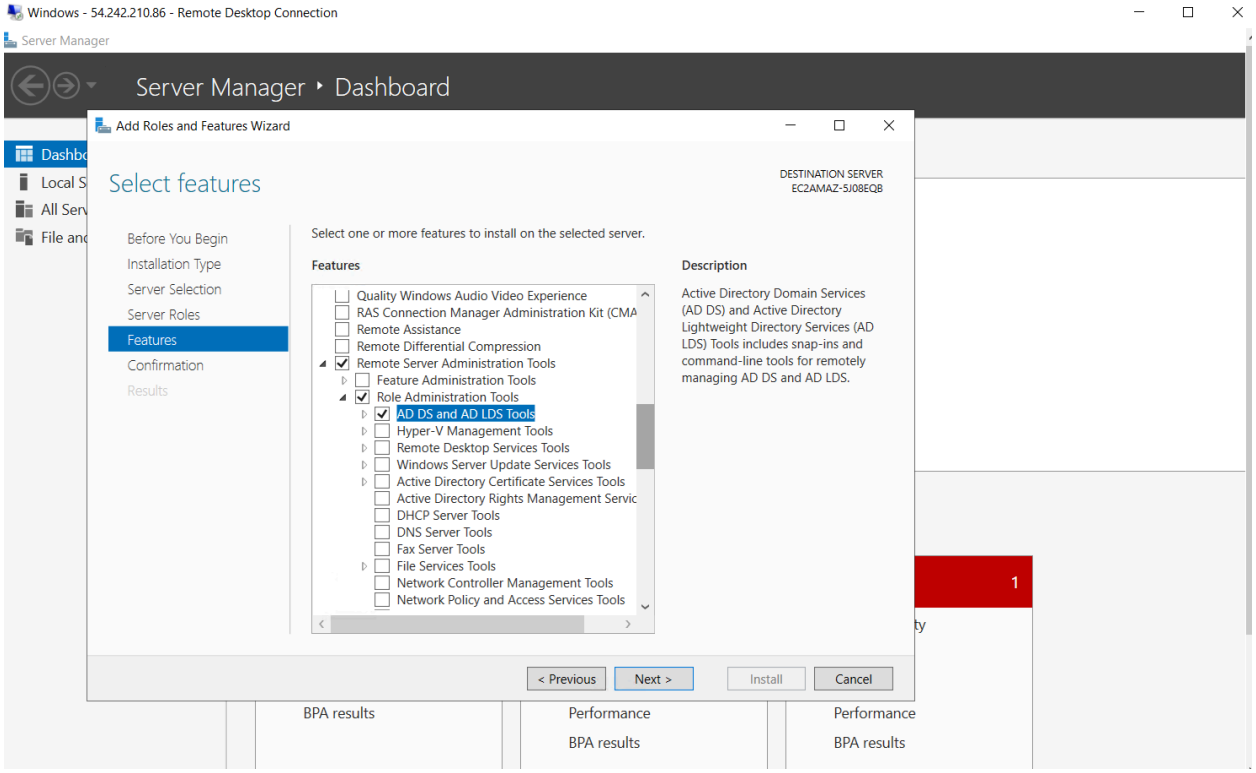

## 11-Connect the Windows server and click on Server Manager



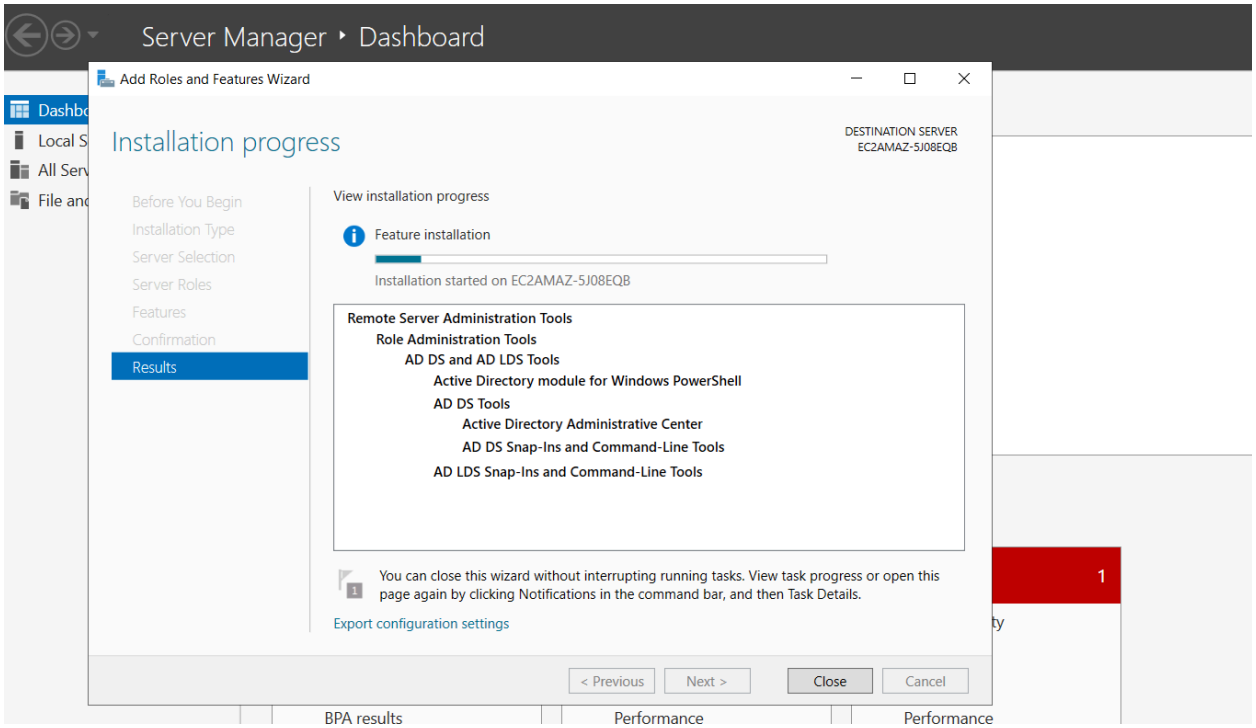
## 12-Click on Manage under Add Roles and features



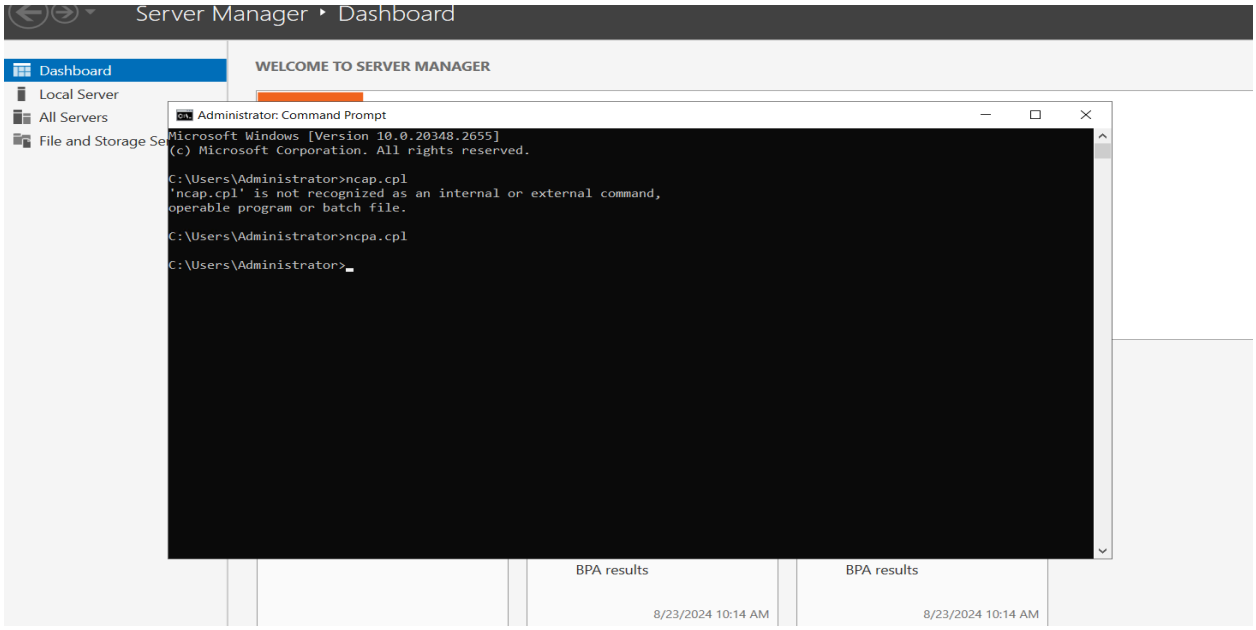

## 13-Click on Next and Next and Next and Next here select Remote server administrative tools under role administrative tools under AD DS and AD LDS tools then Next



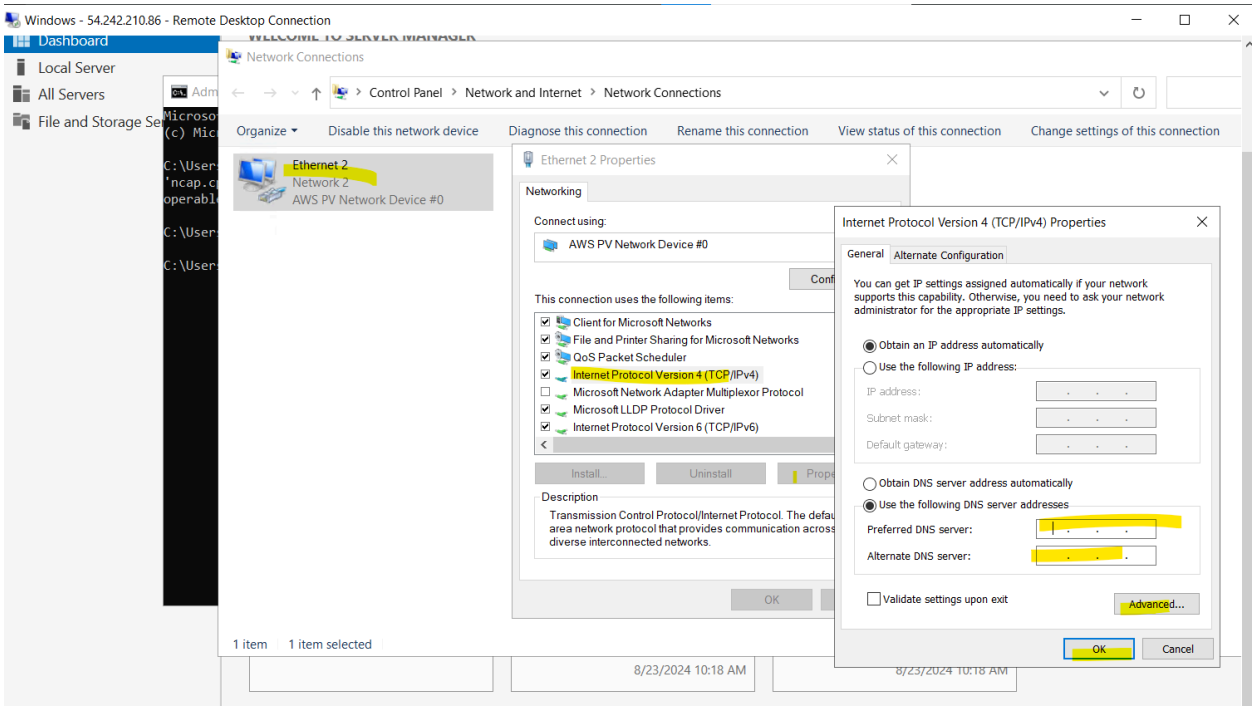

## 14-Click on next and Install

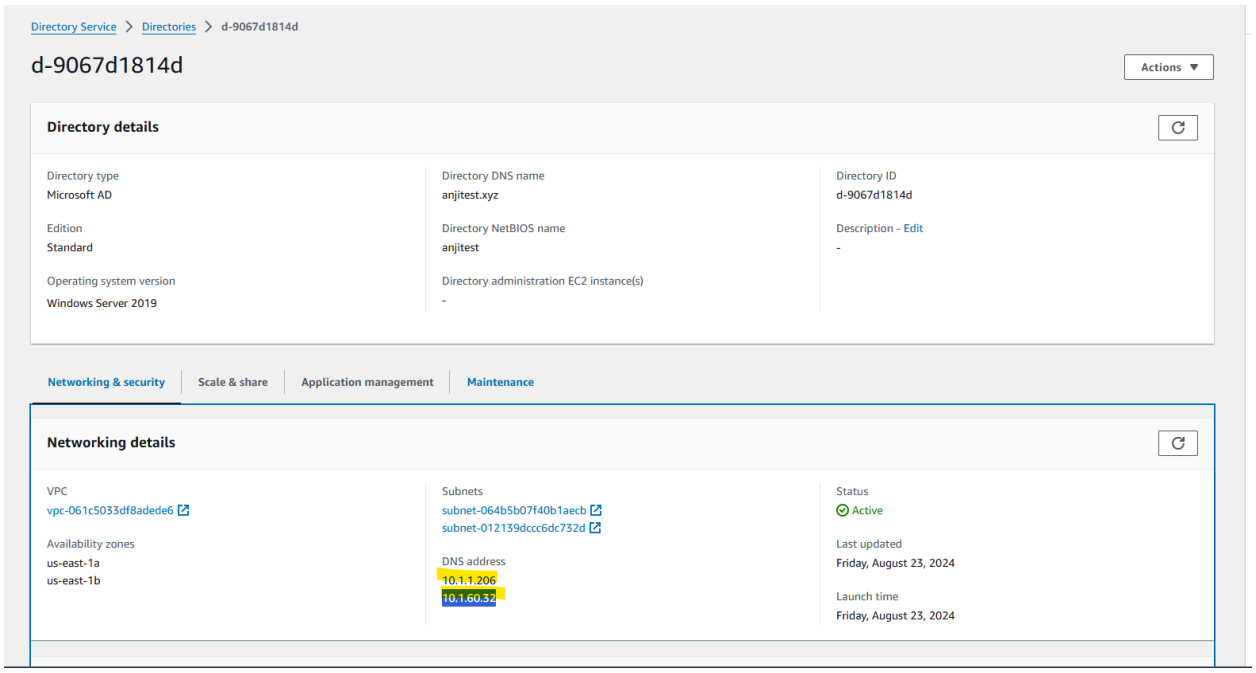


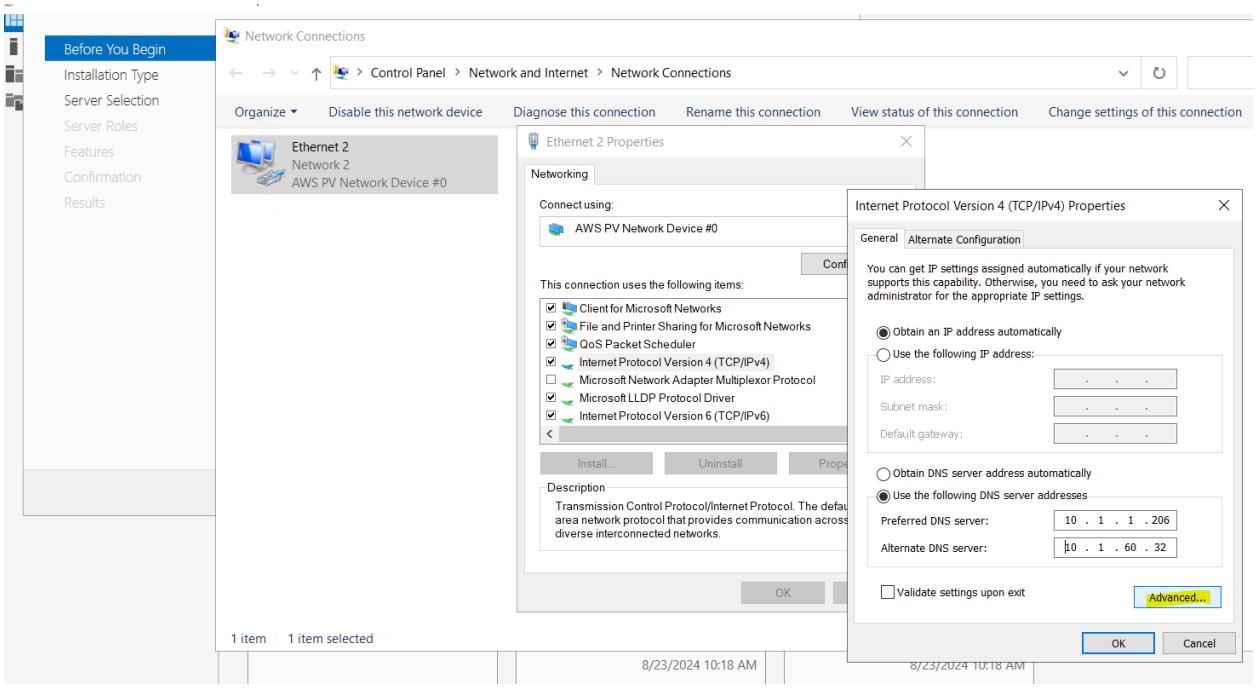

## 15-Click on CMD on the Windows server



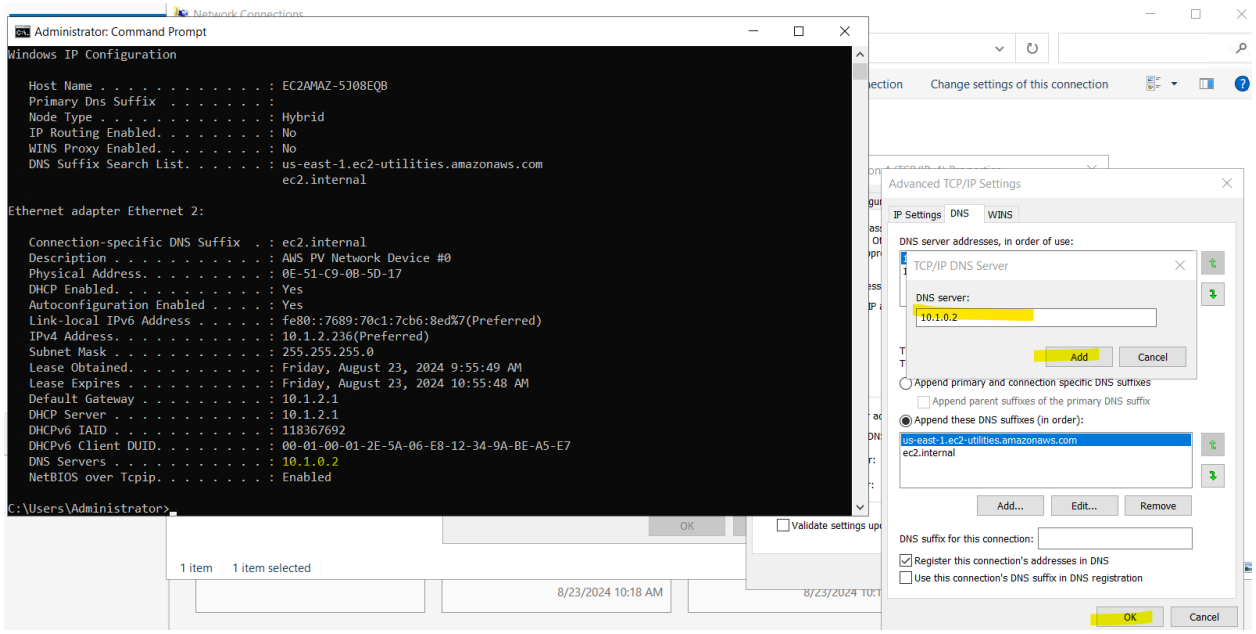

## 16-Click on Ipv4 properties to add AD Managed IPs into DNS Server IPs


Windows - 54.242.210.86 - Remote Desktop Connection
Dashboard
Local Server
All Servers
File and Storage Se
Network Connections
Control Panel > Network and Internet > Network Connections
Organize
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
Ethernet 2
Network 2
AWS PV Network Device #0
Ethernet 2 Properties
Networking
Connect using:
AWS PV Network Device #0
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Description
Transmission Control Protocol/Internet Protocol. The defau
area network protocol that provides communication across
diverse interconnected networks.
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel
1 item
1 item selected
8/23/2024 10:18 AM


Directory Service > Directories > d-9067d1814d
d-9067d1814d
Actions
Directory details
Directory type
Microsoft AD
Directory DNS name
anjitest.xyz
Directory ID
d-9067d1814d
Edition
Standard
Directory NetBIOS name
anjitest
Description - Edit
-
Operating system version
Windows Server 2019
Directory administration EC2 instance(s)
-
Networking & security
Scale & share
Application management
Maintenance
Networking details
VPC
vpc-061c5033df8adede6
Subnets
subnet-064b5b07f40b1aecb
subnet-012139dccc6dc732d
Status
Active
Availability zones
us-east-1a
us-east-1b
DNS address
10.1.1.206
10.1.60.32
Last updated
Friday, August 23, 2024
Launch time
Friday, August 23, 2024

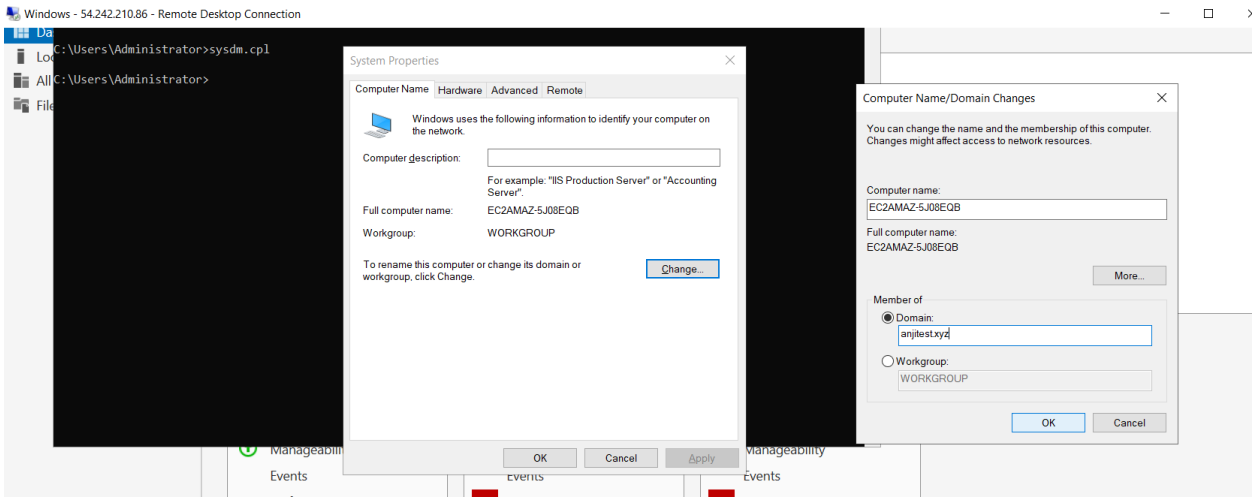


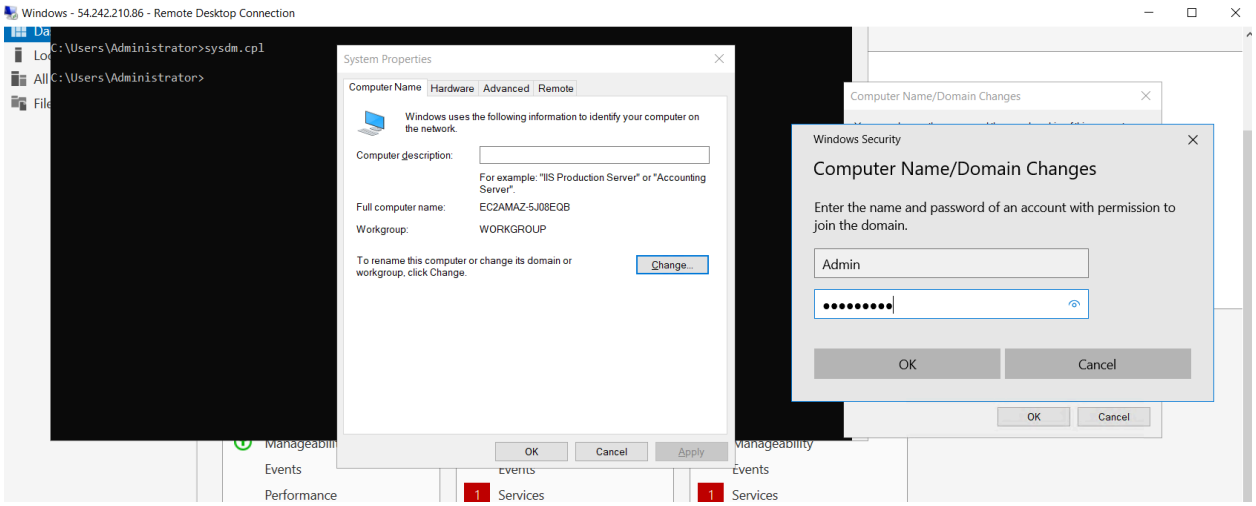

## 17-Click on Advanced to add your System DNS Server IP



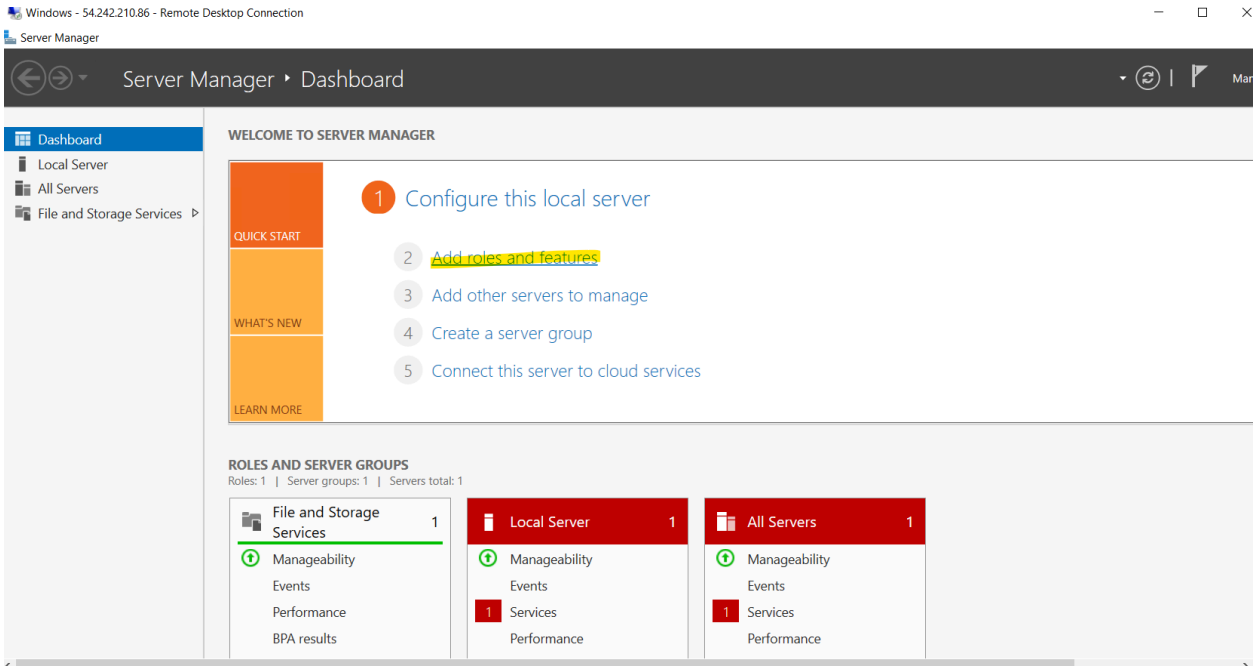

## 18-Now you can have DNS server IPs added into the system

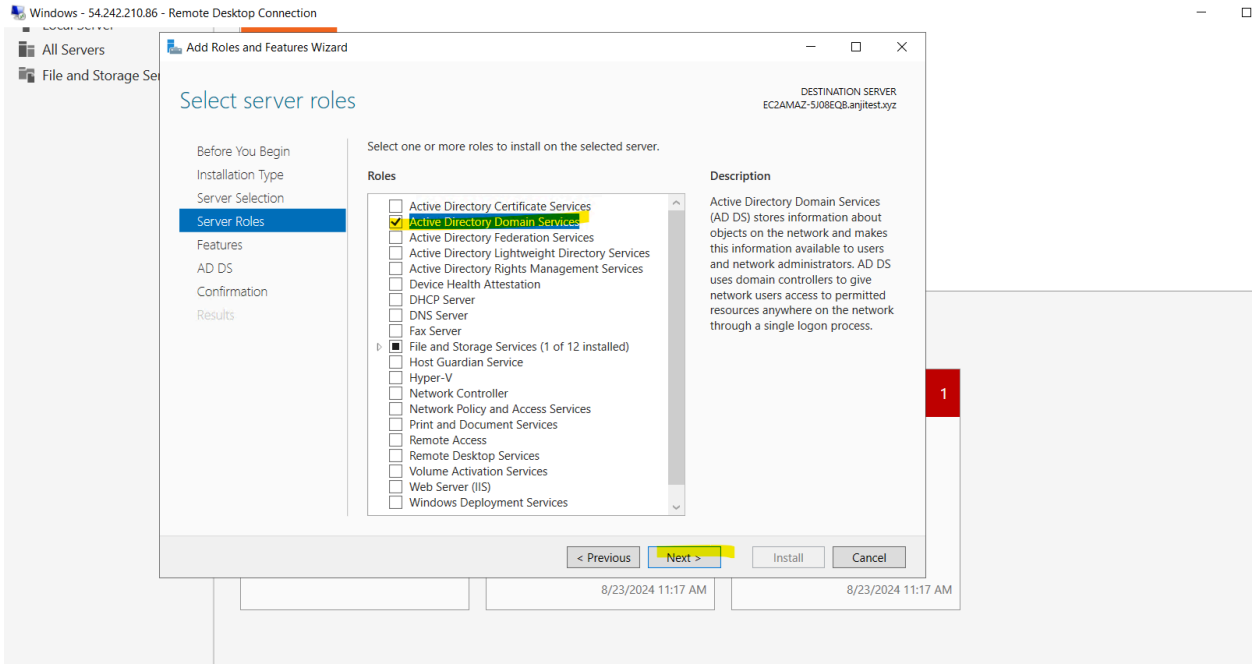

## 19-Click on cmd and type sysdm.cpl it will open click on change and select the Domain to give your domain anjitest.xyz then it will ask for a prompt username and password

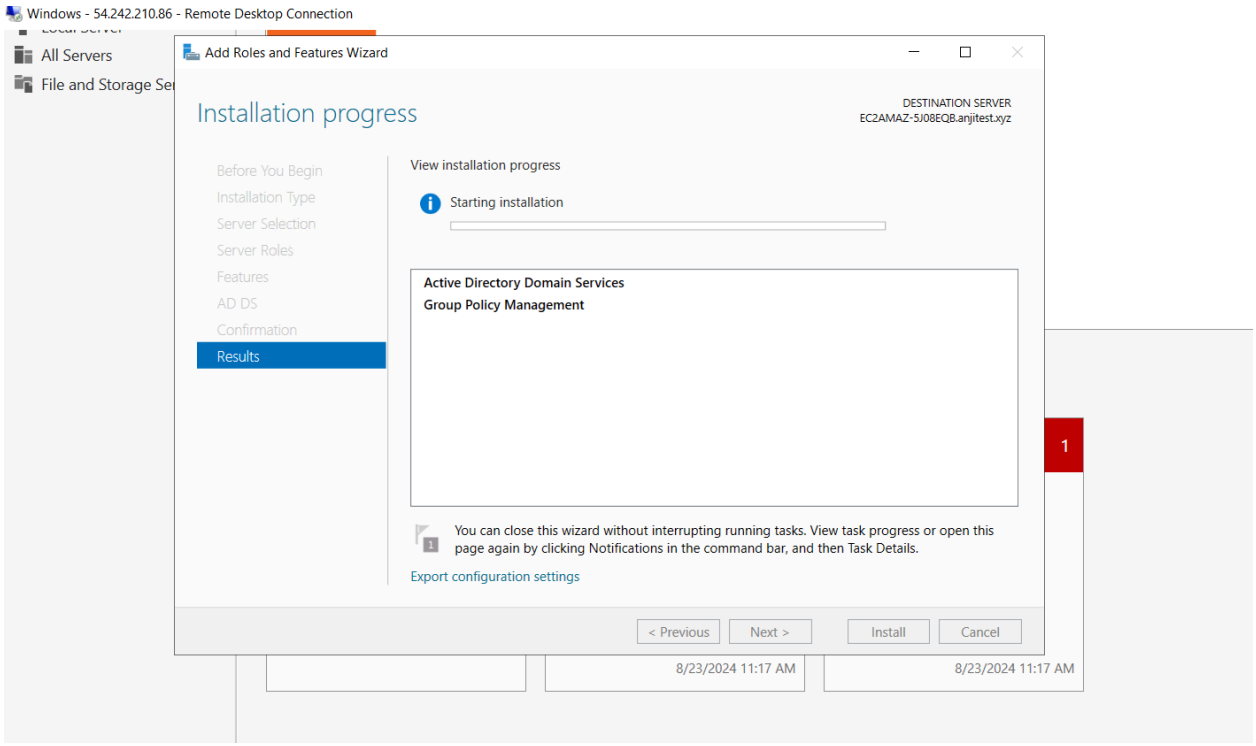




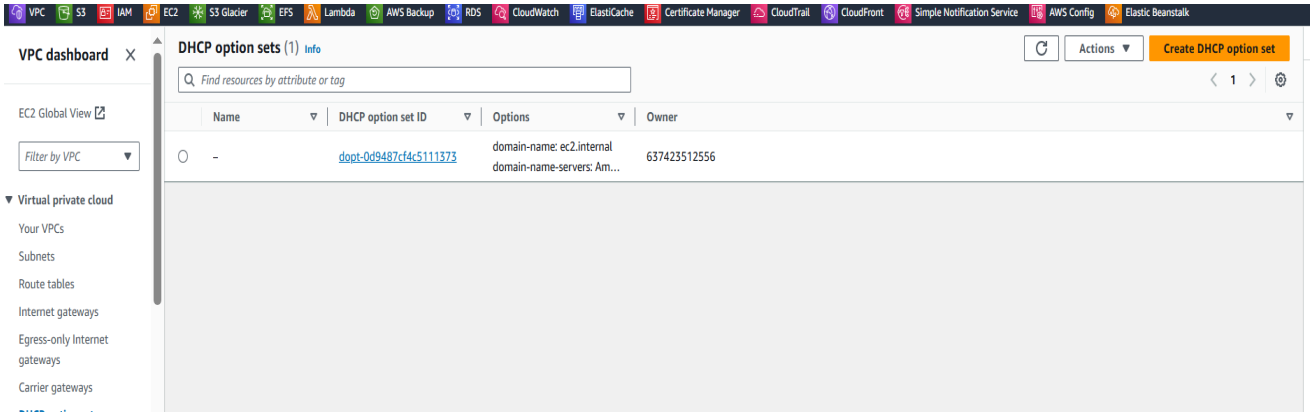

# It will Restart the prompt give it to Restart.



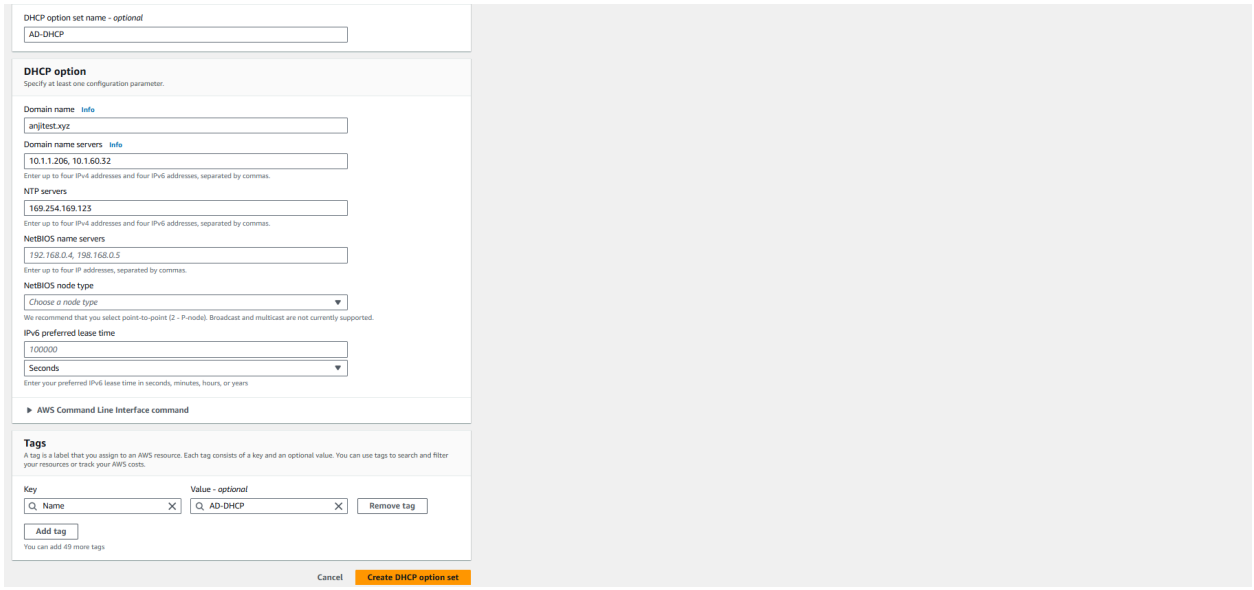


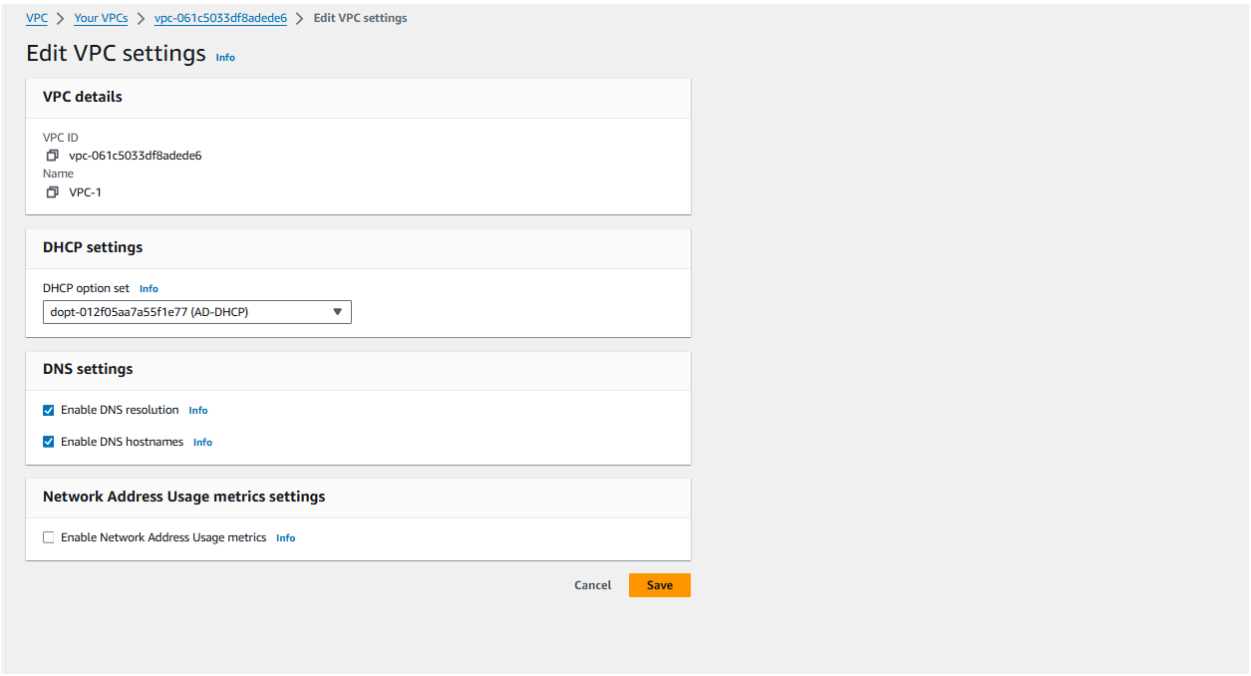

## 21-Click on Create DHCP Option-Set




## 22-Give Name and domain name and DNS IPs of the AD service and NTP Servers Click on create

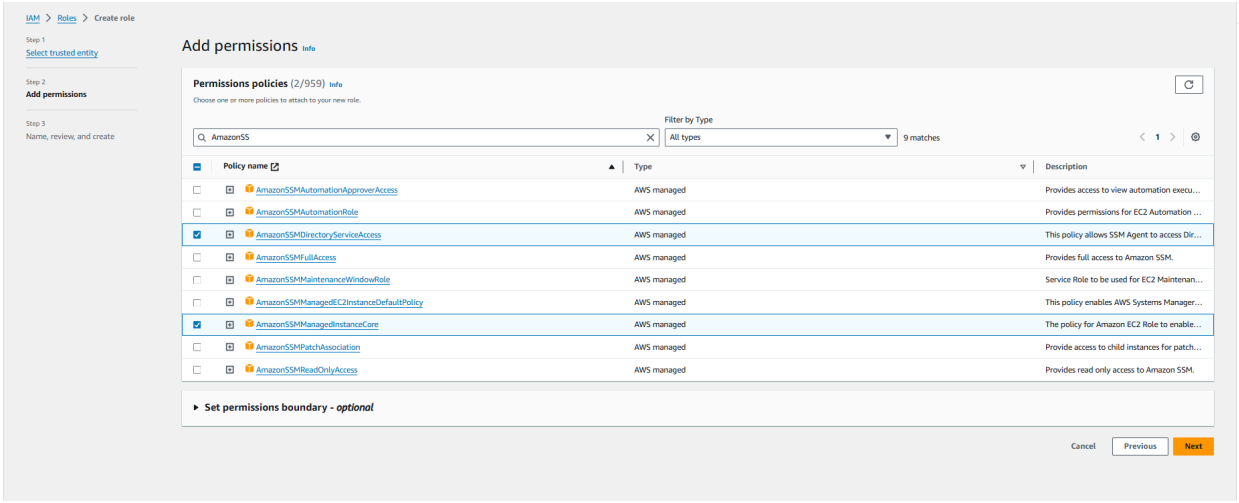


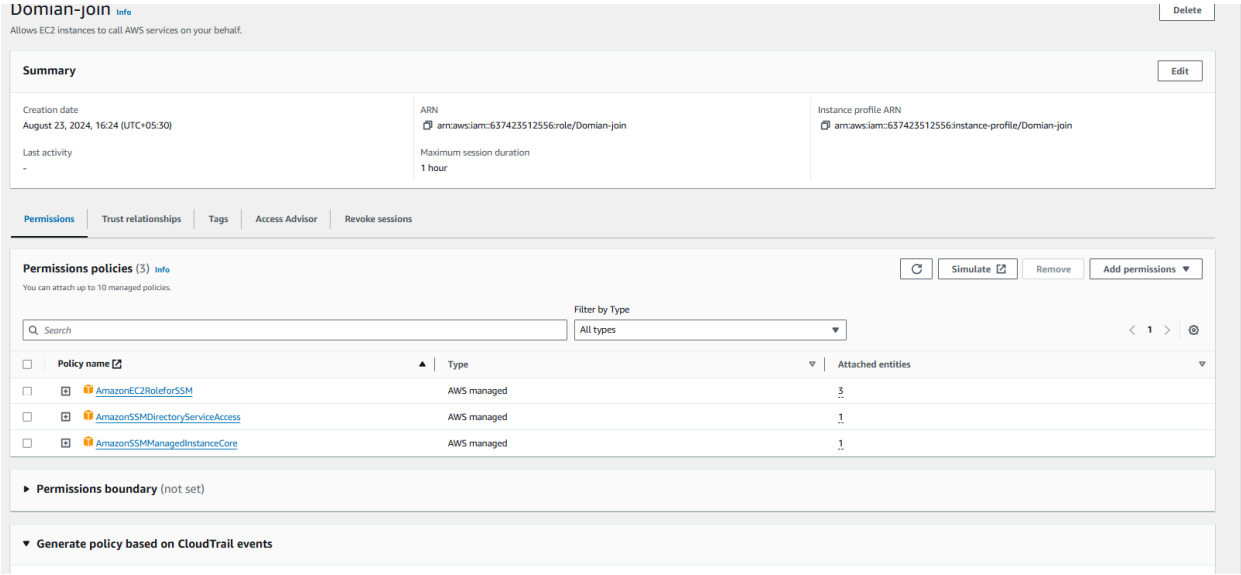

## 23-Click on VPC Actions click edit VPC settings select the DHCP you created here, and click on create .and one more thing here must be to enable DNS resolution



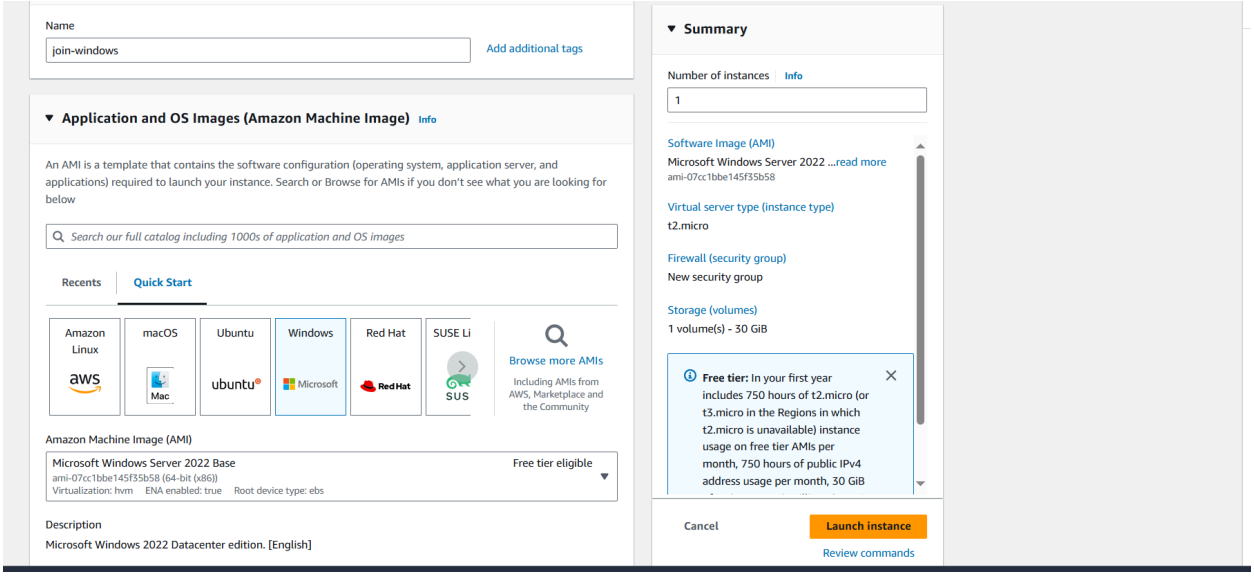

# 24-You Need to create a role using these policies

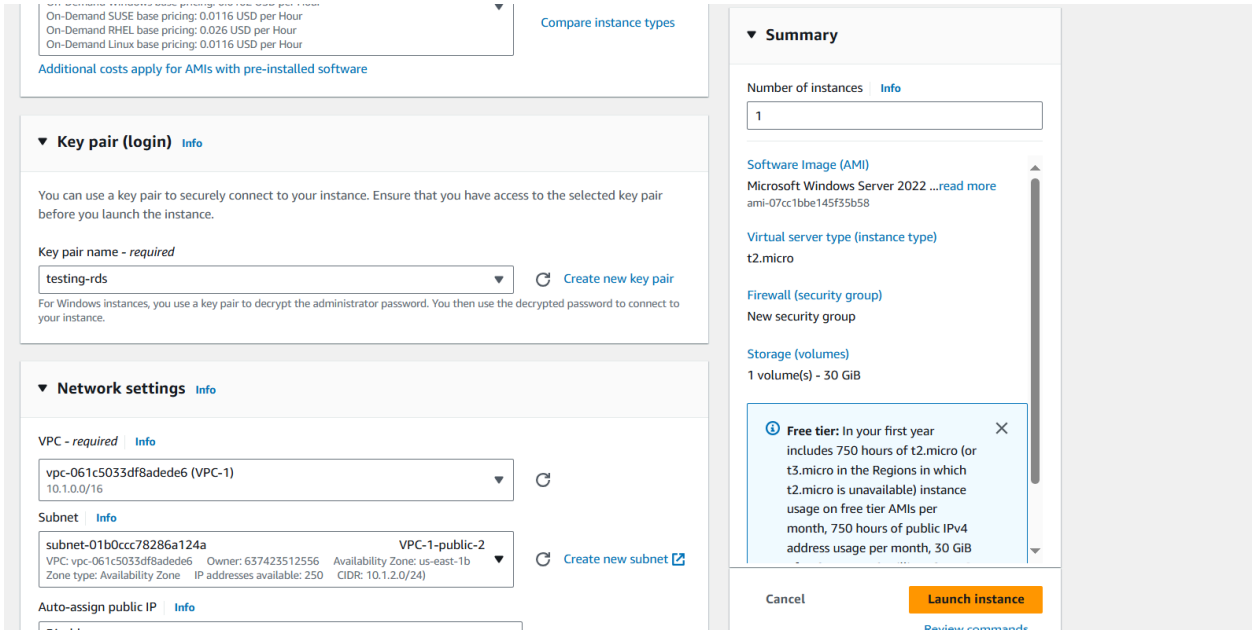
[AmazonSSMDirectoryServiceAccess]
[AmazonSSMManagedInstanceCore]

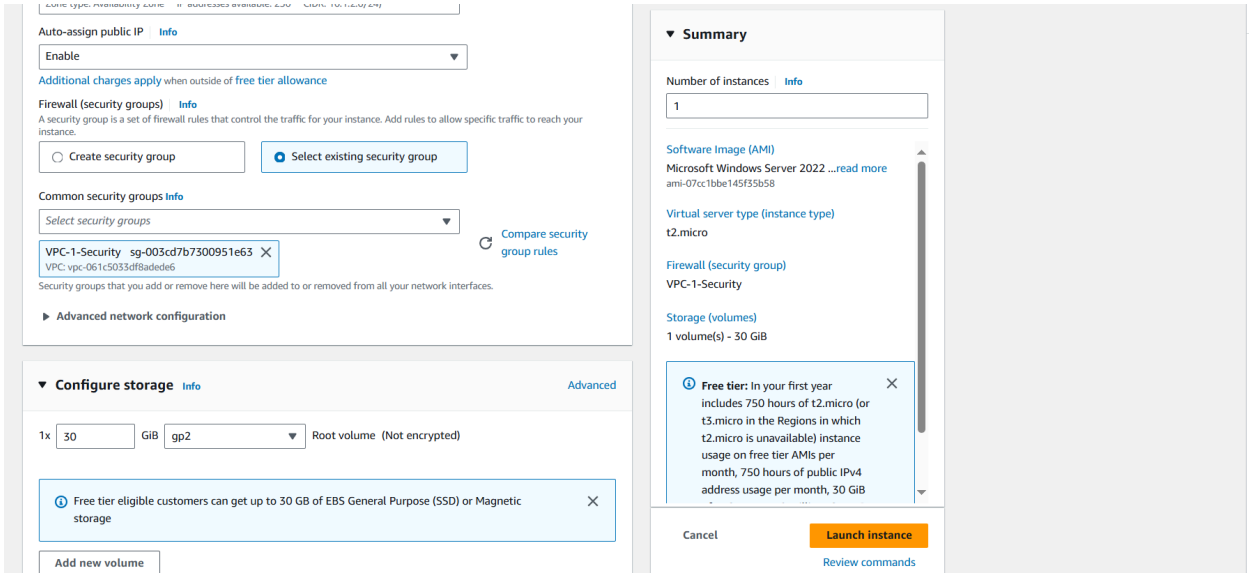




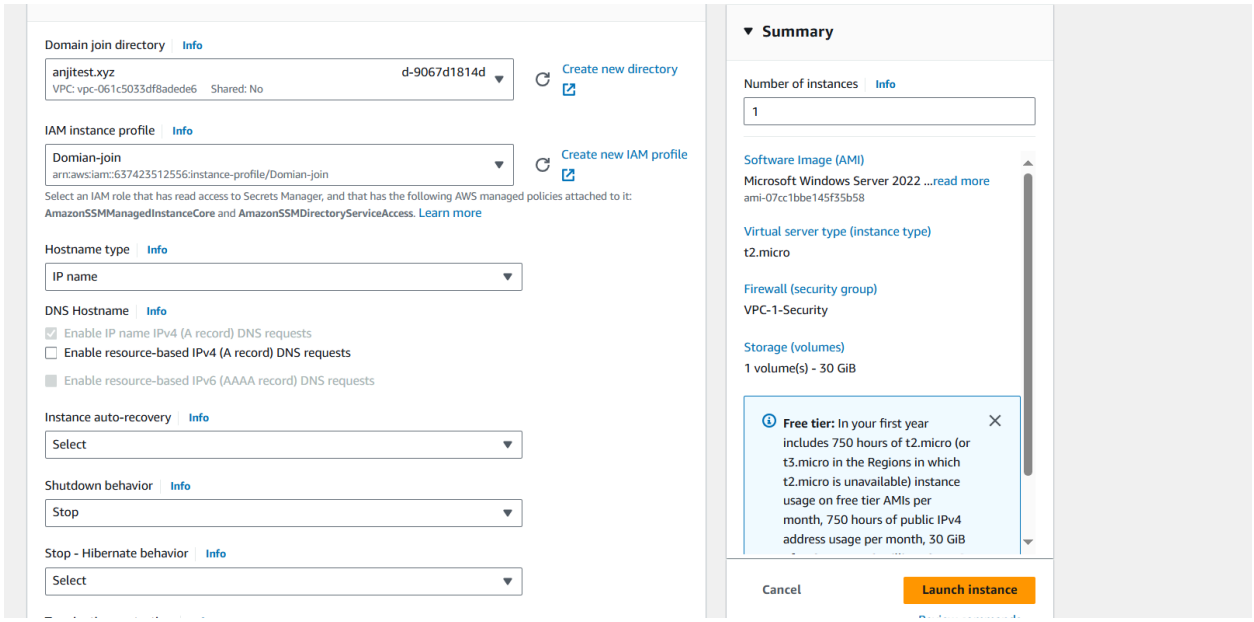

# 24-Launch Windows instance with





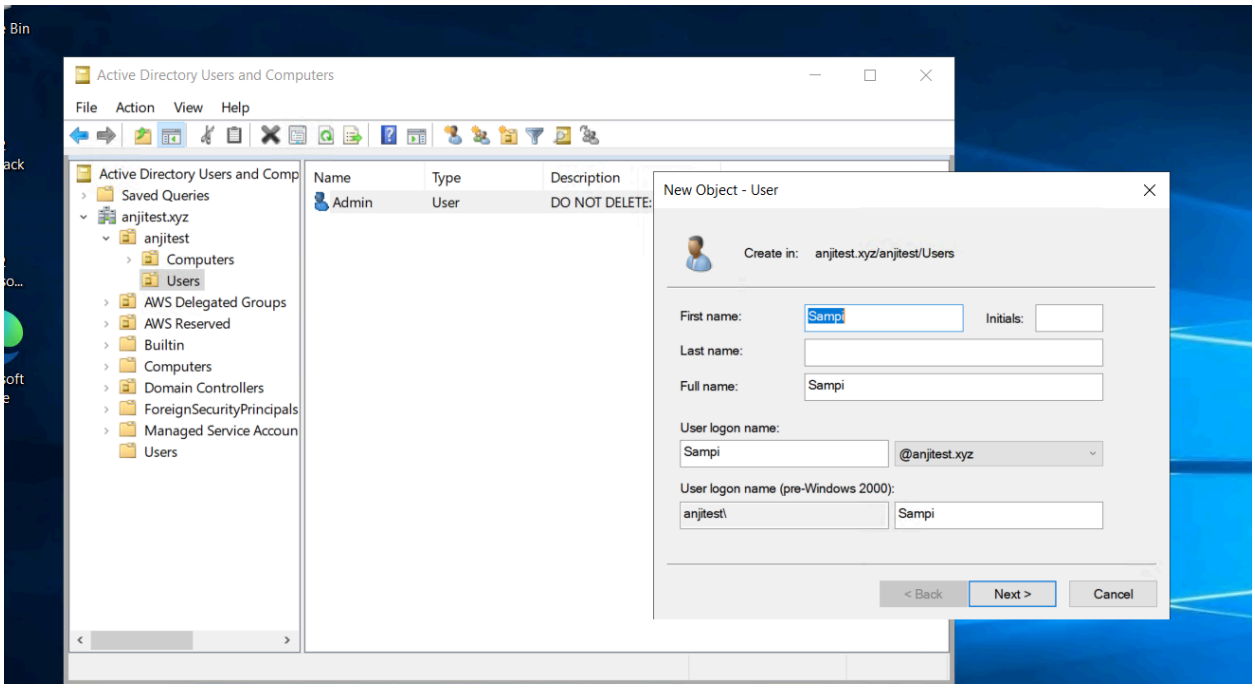

**Here add domain controller and iam you created join-domain**

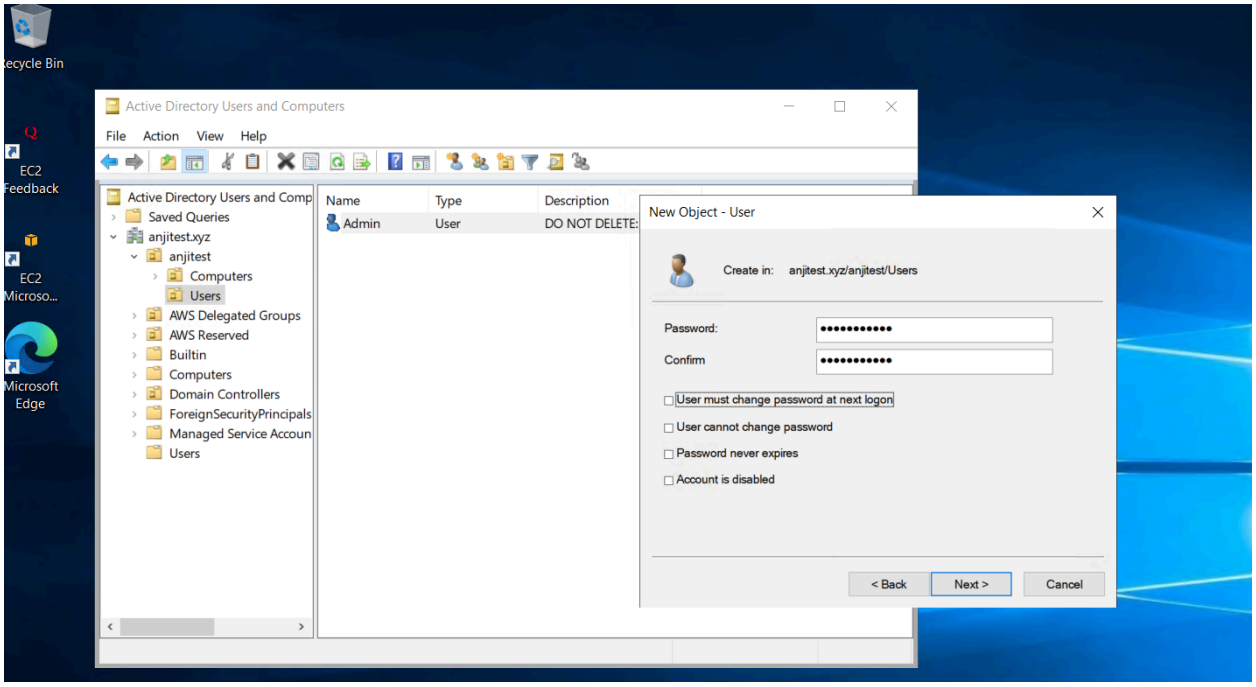



# 25-LogIn Into the AD-Server Create one or two users

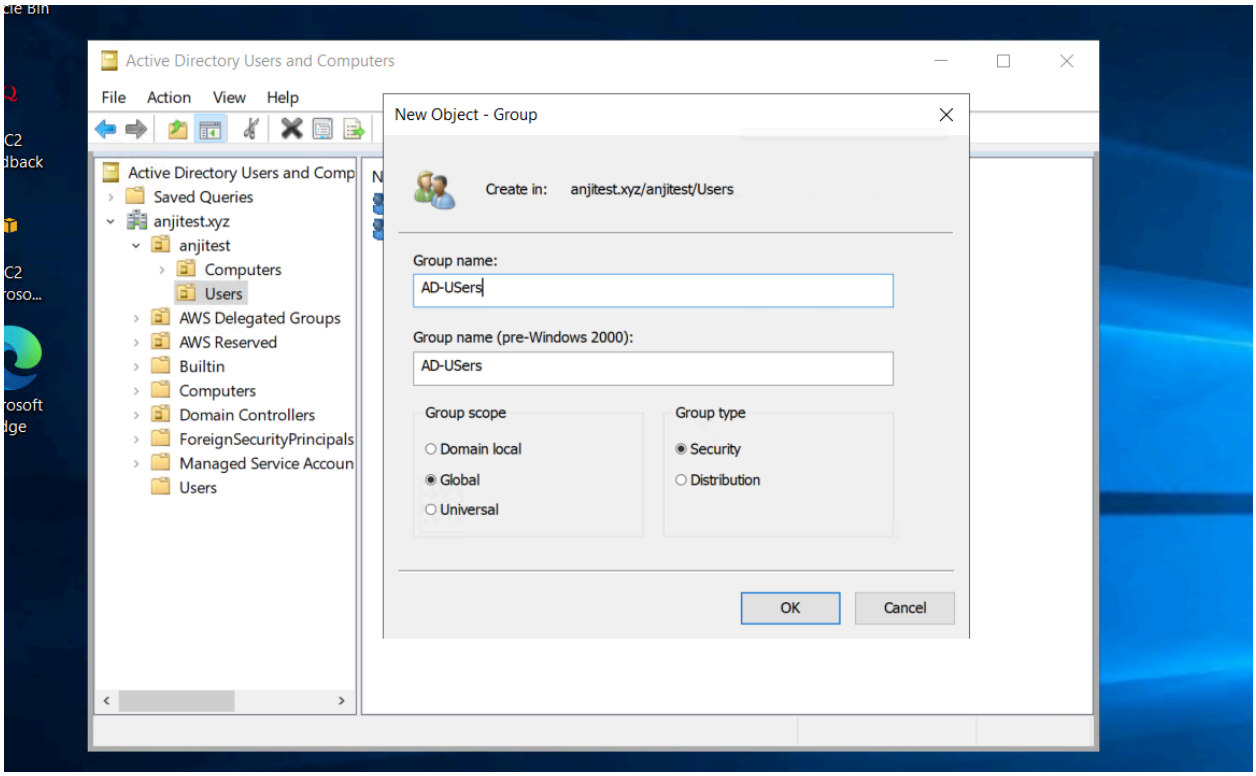
# Anji

# Sampi

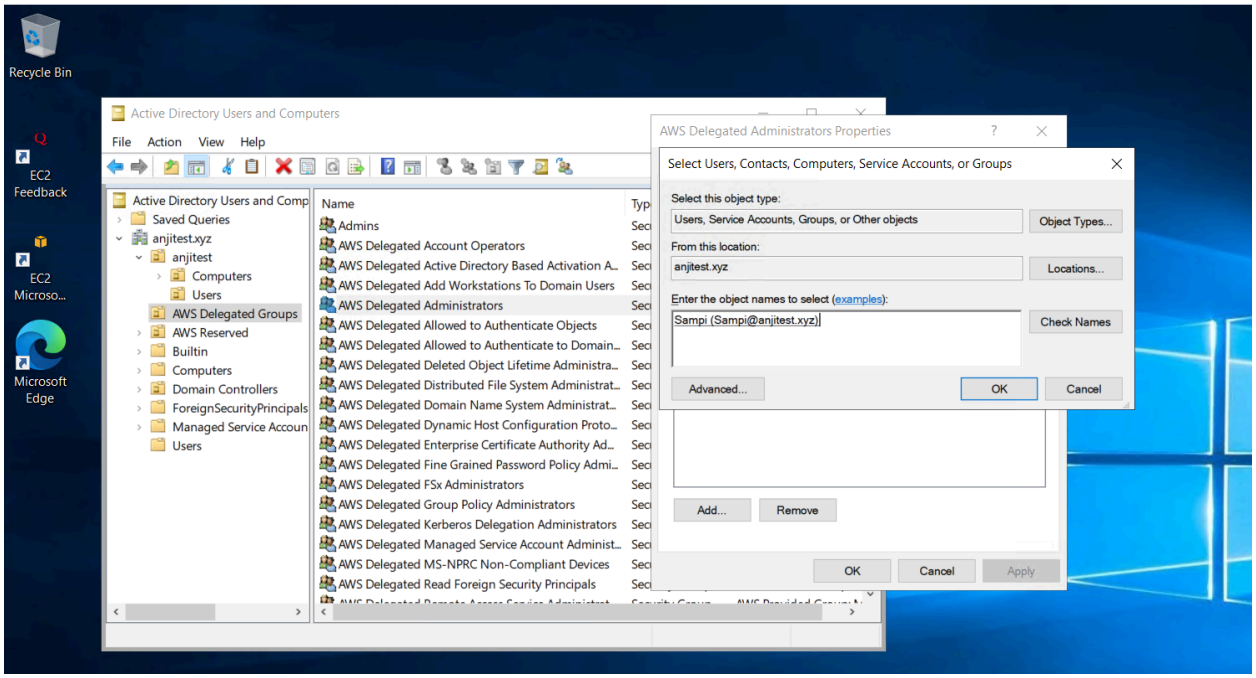




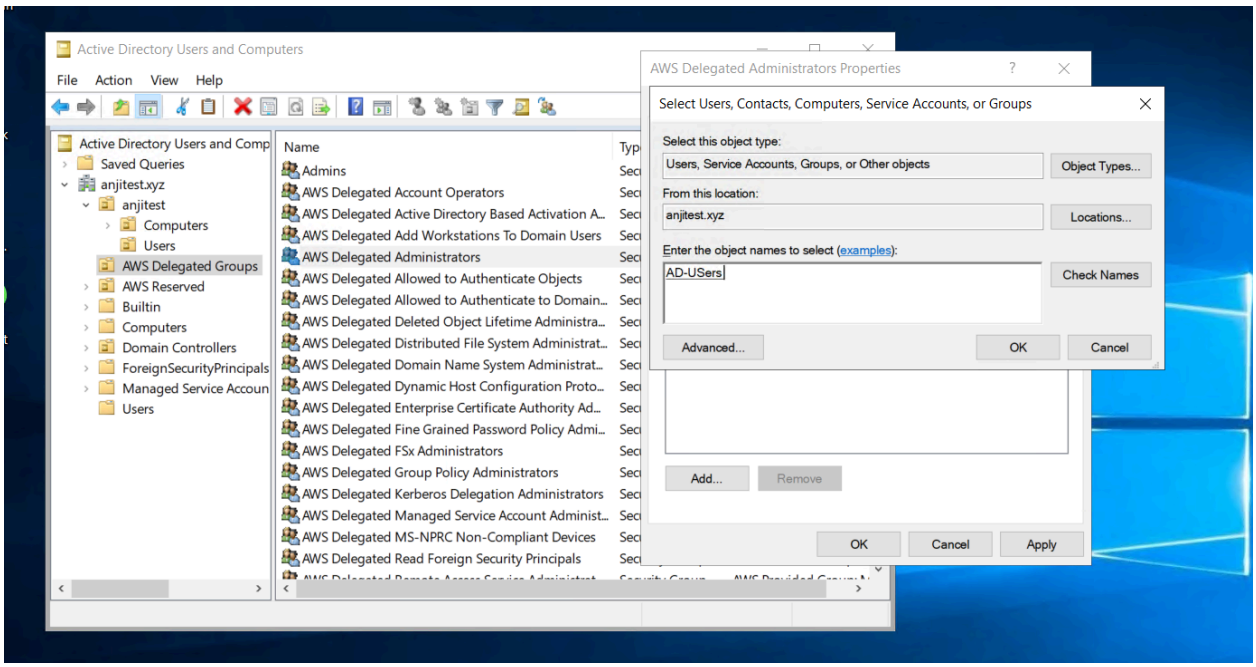

## Create one group



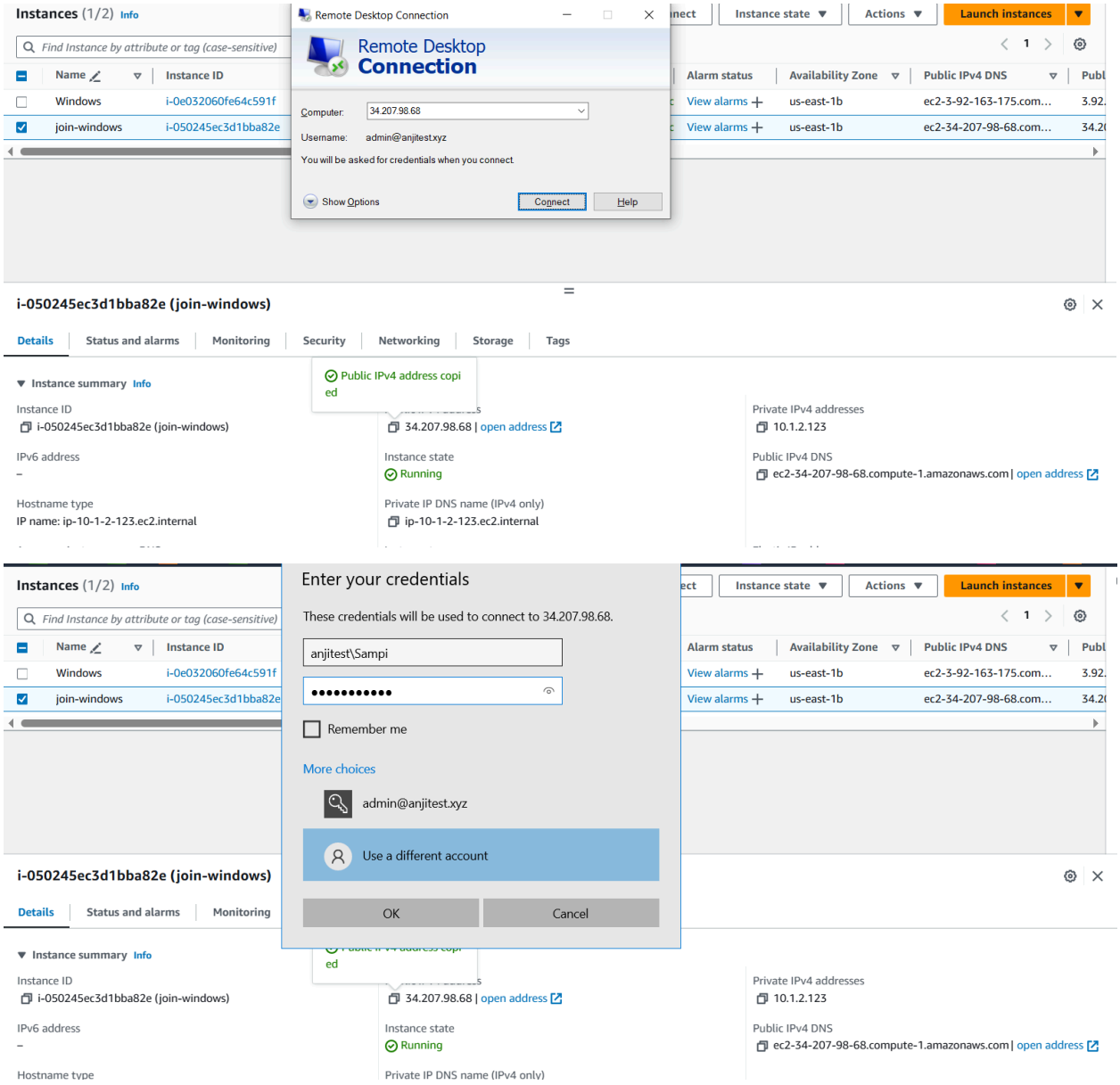

## Add the user to that group

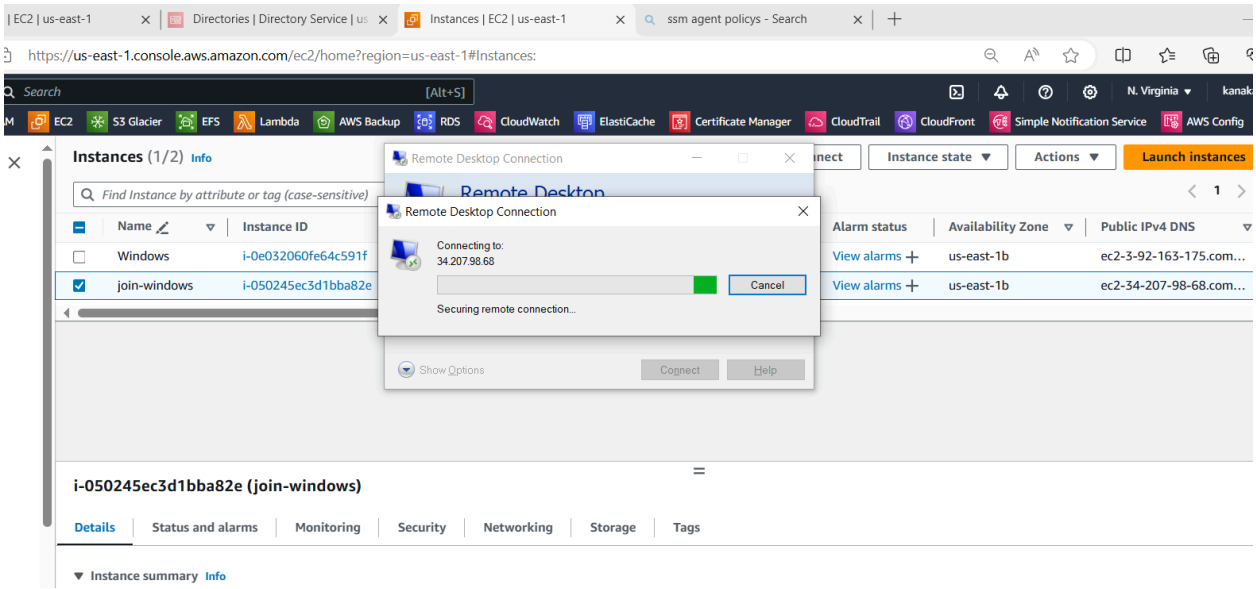



**The group also add to AWS Delegated Admin Group**

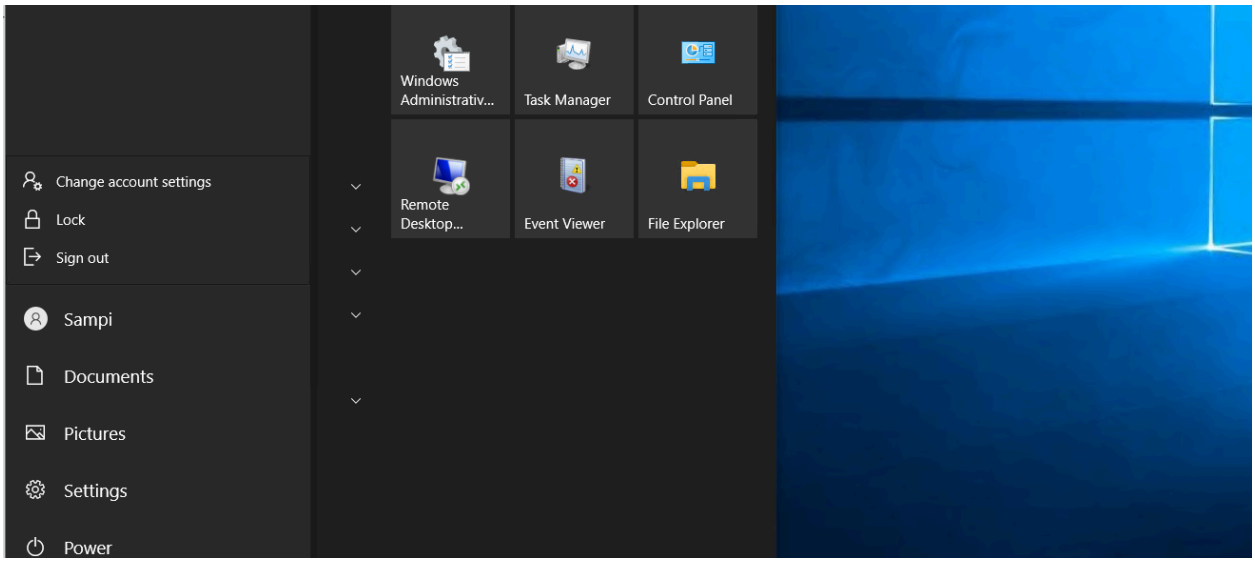


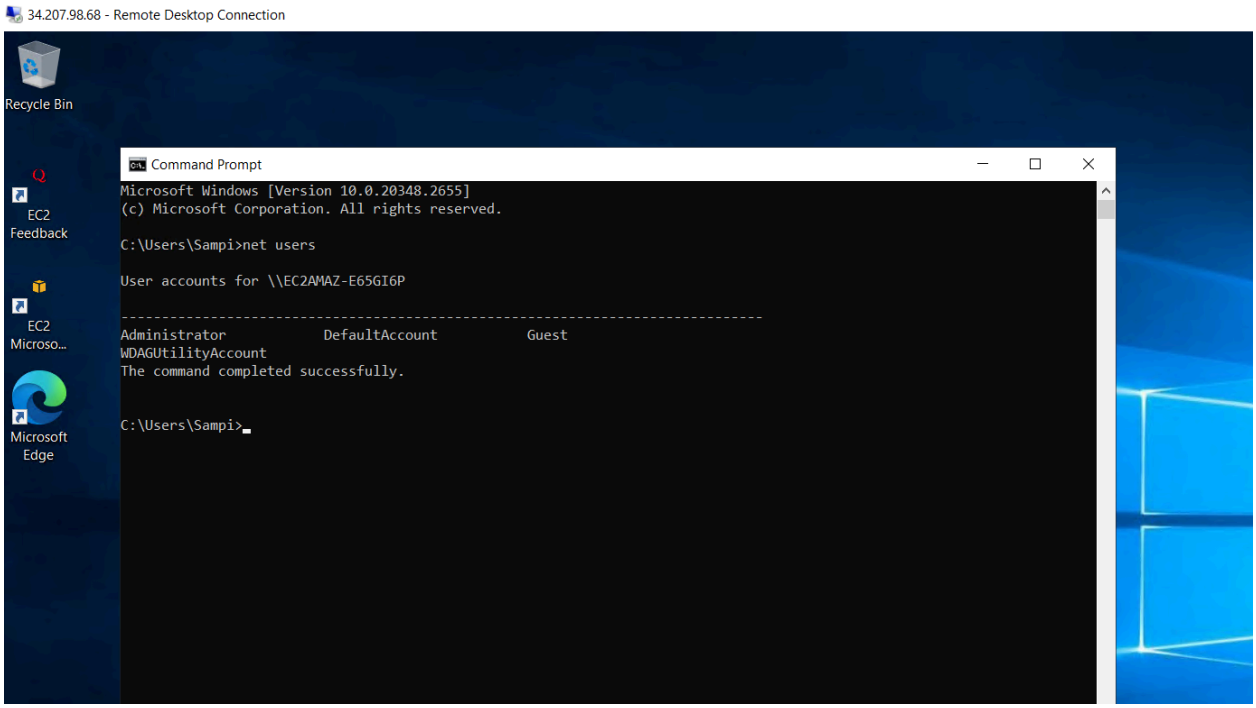

**26-now you can connect that user using any instance in the AD group**
**We have created one instance for testing purposes**
**We can connect or not see here**


Instances (1/2) Info
Find Instance by attribute or tag (case-sensitive)
Name
Instance ID
Windows
i-0e032060fe64c591f
join-windows
i-050245ec3d1bba82e
Instance state
Actions
Launch instances
Alarm status
Availability Zone
Public IPv4 DNS
View alarms
us-east-1b
ec2-3-92-163-175.com...
ec2-34-207-98-68.com...
Remote Desktop Connection
Remote Desktop Connection
Computer: 34.207.98.68
Username: admin@anjitest.xyz
You will be asked for credentials when you connect.
Show Options
Connect
Help
i-050245ec3d1bba82e (join-windows)
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Public IPv4 address copied
Instance ID
i-050245ec3d1bba82e (join-windows)
34.207.98.68 | open address
Private IPv4 addresses
10.1.2.123
IPv6 address
–
Instance state
Running
Public IPv4 DNS
ec2-34-207-98-68.compute-1.amazonaws.com | open address
Hostname type
IP name: ip-10-1-2-123.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-1-2-123.ec2.internal
Enter your credentials
These credentials will be used to connect to 34.207.98.68.
anjitest\Sampi
Remember me
More choices
admin@anjitest.xyz
Use a different account
OK
Cancel




## Now it is connected you can see the below image



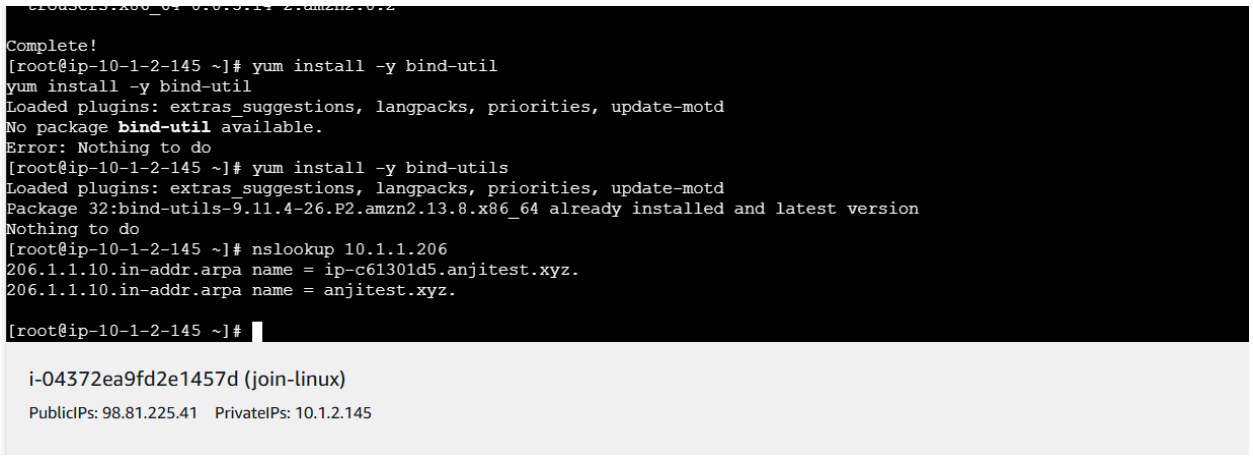



## Now Linux here we can see

## Launch one Linux server as usual and connect the server

## Run this commands

**yum -y install sssd realmd krb5-workstation samba-common-tools oddjob oddjob-mkhomedir samba-common**
**yum install -y bind-utils**



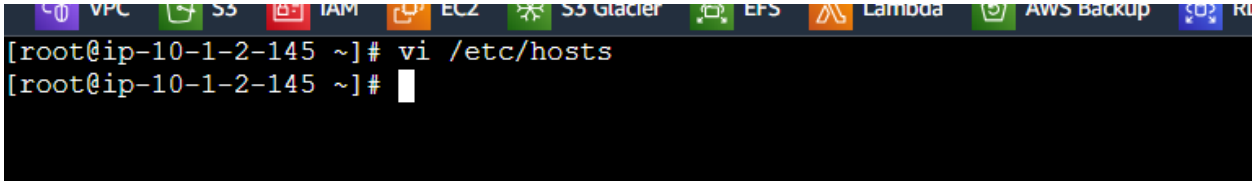
```
Complete!
[root@ip-10-1-2-145 ~]# yum install -y bind-util
yum install -y bind-util
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
No package bind-util available.
Error: Nothing to do
[root@ip-10-1-2-145 ~]# yum install -y bind-utils
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Package 32:bind-utils-9.11.4-26.P2.amzn2.13.8.x86_64 already installed and latest version
Nothing to do
[root@ip-10-1-2-145 ~]# nslookup 10.1.1.206
206.1.1.10.in-addr.arpa name = ip-c61301d5.anjitest.xyz.
206.1.1.10.in-addr.arpa name = anjitest.xyz.

[root@ip-10-1-2-145 ~]# nslookup 10.1.60.32
32.60.1.10.in-addr.arpa name = ip-c6130295.anjitest.xyz.
32.60.1.10.in-addr.arpa name = anjitest.xyz.

[root@ip-10-1-2-145 ~]#
```

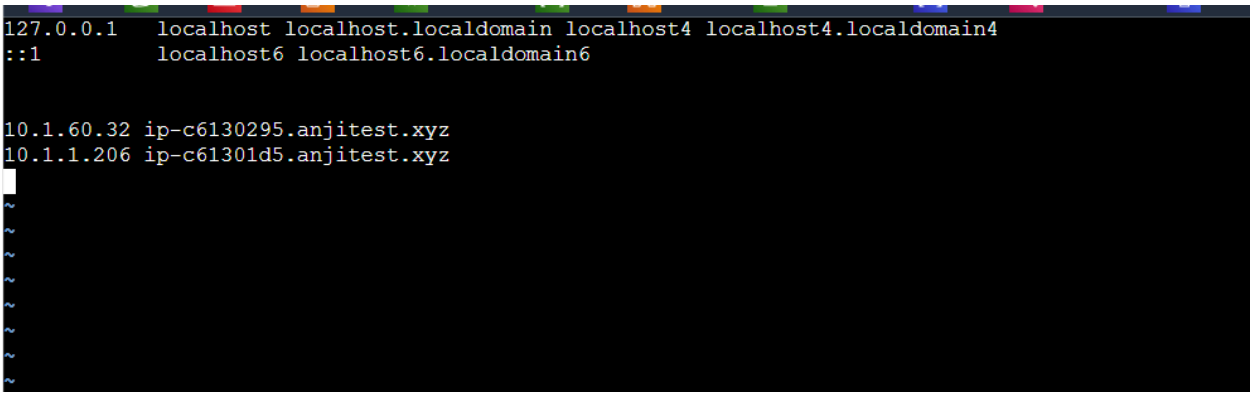
i-04372ea9fd2e1457d (join-linux)

PublicIPs: 98.81.225.41 PrivateIPs: 10.1.2.145

**10.1.60.32 ip-c6130295.anjitest.xyz**
**10.1.1.206 ip-c61301d5.anjitest.xyz**

**Then add this to this file**
**Vi /etc/hosts**



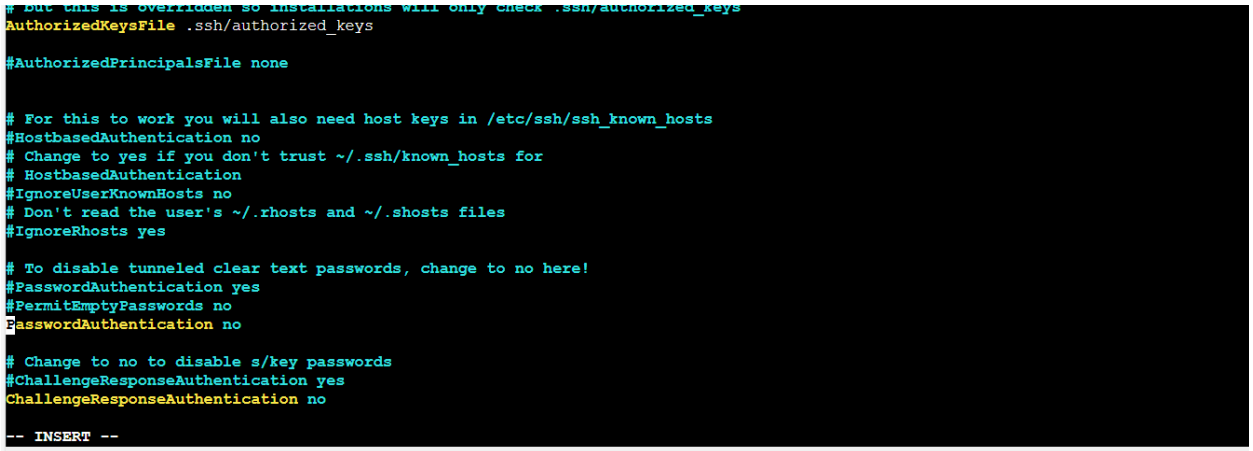




**realm join --user=admin anjitest.xyz**
**It will prompt password of AD directory password to give**

**Then enable password-based authentication in Linux using the below steps**

```
[root@ip-10-1-2-145 ~]# vi /etc/hosts
[root@ip-10-1-2-145 ~]# realm join --user=admin anjitest.xyz
Password for admin:
[root@ip-10-1-2-145 ~]# vi /etc/ssh/sshd_config
```

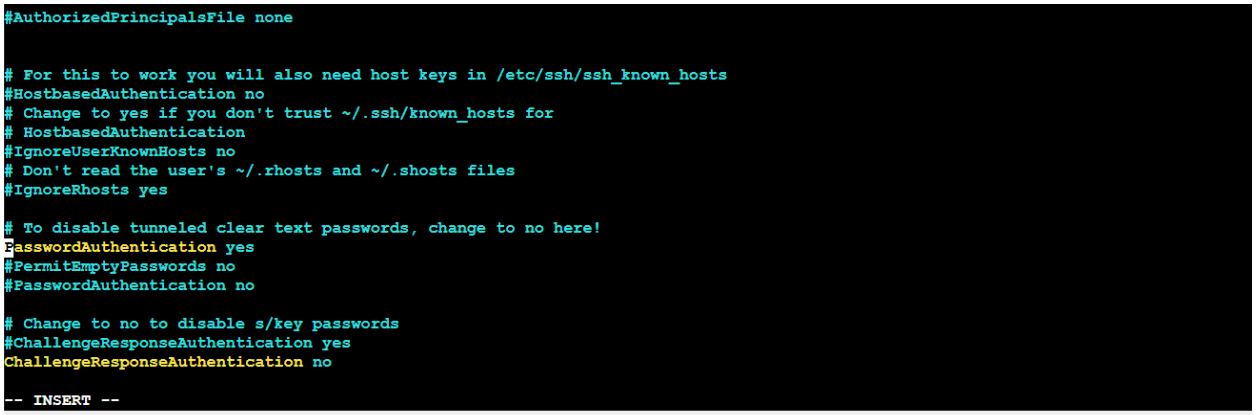
## First image




i-04372ea9fd2e1457d (join-linux)

PublicIPs: 98.81.225.41 PrivateIPs: 10.1.2.145

## Changed after




i-04372ea9fd2e1457d (join-linux)

PublicIPs: 98.81.225.41 PrivateIPs: 10.1.2.145

**Service sshd restart**
**Service sssd restart**

```
[root@ip-10-1-2-145 ~]# service sshd restart
Redirecting to /bin/systemctl restart sshd.service
[root@ip-10-1-2-145 ~]# service sssd restart
Redirecting to /bin/systemctl restart sssd.service
[root@ip-10-1-2-145 ~]#
```

i-04372ea9fd2e1457d (join-linux)

PublicIPs: 98.81.225.41 PrivateIPs: 10.1.2.145

**Visudo**

**%AWSAdministrators@anjitest.xyz ALL=(ALL) NOPASSWD: ALL**
**%AWS\ Delegated\ Administrators@anjitest.xyz ALL=(ALL) NOPASSWD: ALL**

```
[root@ip-10-1-2-145 ~]# service sshd restart
Redirecting to /bin/systemctl restart sshd.service
[root@ip-10-1-2-145 ~]# service sssd restart
Redirecting to /bin/systemctl restart sssd.service
[root@ip-10-1-2-145 ~]# visudo
[root@ip-10-1-2-145 ~]#
```

i-04372ea9fd2e1457d (join-linux)

PublicIPs: 98.81.225.41 PrivateIPs: 10.1.2.145

```
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
~
~
~
-- INSERT --                                                    110,33-46
```

i-04372ea9fd2e1457d (join-linux)

PublicIPs: 98.81.225.41 PrivateIPs: 10.1.2.145

```
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING, PROCESSES, LOCATE, DRIVERS

## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL
%AWSAdministrators@anjitest.xyz ALL=(ALL)       NOPASSWD: ALL
%AWS\ Delegated\ Administrators@anjitest.xyz ALL=(ALL)       NOPASSWD: ALL


## Allows members of the users group to mount and unmount the
## cdrom as root
# %users  ALL=/sbin/mount /mnt/cdrom, /sbin/umount /mnt/cdrom

## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now

## Read drop-in files from /etc/sudoers.d (the # here does not mean a comment)
#includedir /etc/sudoers.d
-- INSERT --
```

i-04372ea9fd2e1457d (join-linux)

PublicIPs: 98.81.225.41  PrivateIPs: 10.1.2.145

## You can see the user in linux which we created in Windows
## Command: id Sampi@anjitest.xyz

```
[root@ip-10-1-2-145 ~]# service sshd restart
Redirecting to /bin/systemctl restart sshd.service
[root@ip-10-1-2-145 ~]# service sssd restart
Redirecting to /bin/systemctl restart sssd.service
[root@ip-10-1-2-145 ~]# visudo
[root@ip-10-1-2-145 ~]# visudo

[No write since last change]

Press ENTER or type command to continue
visudo: /etc/sudoers.tmp unchanged
[root@ip-10-1-2-145 ~]# visudo
visudo: /etc/sudoers.tmp unchanged
[root@ip-10-1-2-145 ~]# id Sampi@anjitest.xyz
uid=1796601145(sampi@anjitest.xyz) gid=1796600513(domain users@anjitest.xyz) groups=1796600513(domain users@anjitest.xyz),1796601137(aws delegated terminal server licensing administr
s@anjitest.xyz),1796601140(aws delegated domain name system administrators@anjitest.xyz),1796601142(aws delegated server administrators@anjitest.xyz),1796601121(aws delegated account
rators@anjitest.xyz),1796601126(aws delegated distributed file system administrators@anjitest.xyz),1796601127(aws delegated dynamic host configuration protocol administrators@anjitest
s),1796601134(aws delegated replicate directory changes administrators@anjitest.xyz),1796601109(dnsadmins@anjitest.xyz),1796601130(aws delegated group policy administrators@anjitest.
1796601136(aws delegated system management administrators@anjitest.xyz),1796601139(aws delegated add workstations to domain users@anjitest.xyz),1796601133(aws delegated remote acces
rvice administrators@anjitest.xyz),1796601131(aws delegated managed service account administrators@anjitest.xyz),1796601141(aws delegated kerberos delegation administrators@anjitest.
1796601122(aws delegated active directory based activation administrators@anjitest.xyz),1796601120(aws delegated fsx administrators@anjitest.xyz),1796601132(aws delegated read forei
ecurity principals@anjitest.xyz),1796601125(aws delegated deleted object lifetime administrators@anjitest.xyz),1796601129(aws delegated fine grained password policy administrators@an
t.xyz),1796601138(aws delegated user principal name suffix administrators@anjitest.xyz),1796601135(aws delegated sites and services administrators@anjitest.xyz),1796601128(aws deleg
enterprise certificate authority administrators@anjitest.xyz),1796601119(aws delegated administrators@anjitest.xyz)
[root@ip-10-1-2-145 ~]#
```

i-04372ea9fd2e1457d (join-linux)

PublicIPs: 98.81.225.41  PrivateIPs: 10.1.2.145

## Tests the user will able to log in or not

```
Host key verification failed.

C:\Users\Minfy>ssh Sampi@anjitest.xyz@98.81.225.41
The authenticity of host '98.81.225.41 (98.81.225.41)' can't be established.
ECDSA key fingerprint is SHA256:dlziTj8HfcXgpd0TATKQUU6TMAS0BIWxCVIzHfJnc+A.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '98.81.225.41' (ECDSA) to the list of known hosts.
Sampi@anjitest.xyz@98.81.225.41's password:
Creating home directory for Sampi@anjitest.xyz.
       #_
   ~\_  ####_        Amazon Linux 2
  ~~  \_#####\
  ~~     \###|       AL2 End of Life is 2025-06-30.
  ~~       \#/ ___
   ~~       V~' '->
    ~~~         /    A newer version of Amazon Linux is available!
      ~~._.   _/
         _/ _/       Amazon Linux 2023, GA and supported until 2028-03-15.
       _/m/'           https://aws.amazon.com/linux/amazon-linux-2023/

[sampi@anjitest.xyz@ip-10-1-2-145 ~]$
```

## You can see successfully connected users in Linux using ssh

## Adding Telnet for Testing Purpose Click on Manage add roles and features Click on Next and Next and Next and Next here select the telnet client and click on Install