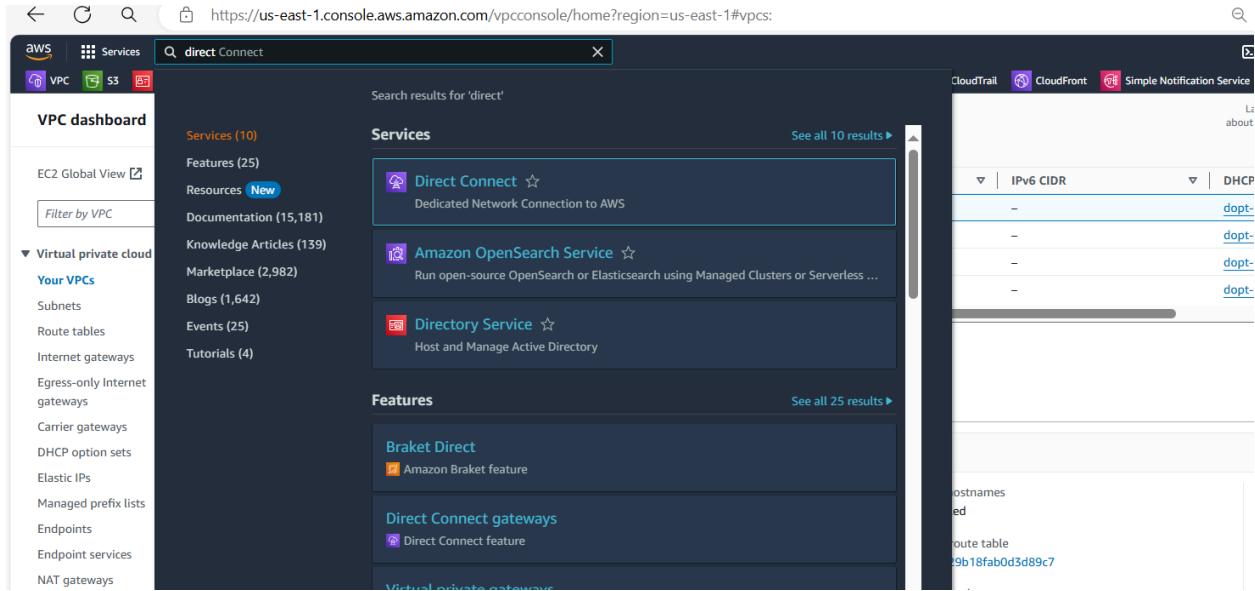


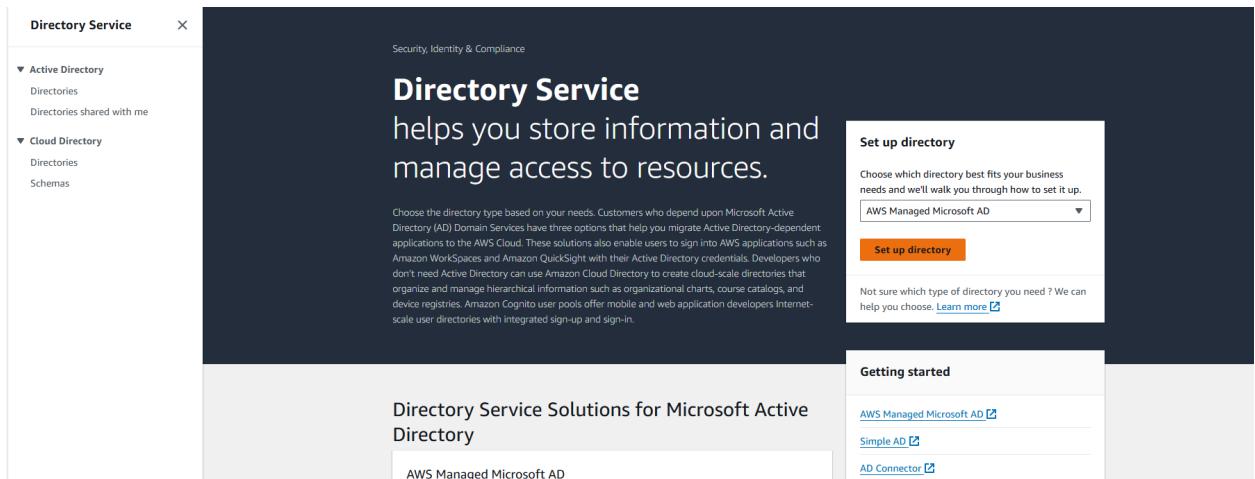
# How to Create AWS Managed AD And add Windows and Linux into AD Server and Create users

## 1-Click On Directory Service in AWS Console



The screenshot shows the AWS VPC console with a search bar at the top containing 'direct'. Below the search bar, there are two main sections: 'Services' and 'Features'. In the 'Services' section, 'Direct Connect' is listed under 'Dedicated Network Connection to AWS'. In the 'Features' section, 'Braket Direct' and 'Direct Connect gateways' are listed. To the right of these sections, there is a sidebar with tabs for CloudTrail, CloudFront, and Simple Notification Service.

## 2-SetUp a Directory



The screenshot shows the 'Directory Service' setup page. On the left, there is a sidebar with 'Active Directory' and 'Cloud Directory' sections. The main content area features a heading 'Directory Service' with the subtext 'helps you store information and manage access to resources.' Below this, there is a paragraph about migrating Active Directory to the AWS Cloud. To the right, there is a 'Set up directory' section with a dropdown menu set to 'AWS Managed Microsoft AD' and a 'Set up directory' button. At the bottom, there is a 'Getting started' section with links to 'AWS Managed Microsoft AD', 'Simple AD', and 'AD Connector'.

## 3-Select Aws Managed Directory

The screenshot shows the 'Select directory type' step of the AWS Directory Service setup wizard. On the left, a sidebar lists steps: Step 1 (Select directory type), Step 2 (Enter directory information), Step 3 (Choose VPC and subnets), and Step 4 (Review & create). The main panel title is 'Select directory type'. It contains a section titled 'Directory types' with four options: 'AWS Managed Microsoft AD' (selected, indicated by a blue circle), 'Simple AD', 'AD Connector', and 'Amazon Cognito User Pools'. To the right of this is a detailed description of 'AWS Managed Microsoft AD', which states: 'With AWS Managed Microsoft AD, you can easily enable your Active Directory-aware workloads and AWS resources to use managed actual Microsoft Active Directory in the AWS Cloud. Workload examples include Amazon EC2, Amazon RDS for SQL Server, custom .NET applications, and AWS Enterprise IT applications such as Amazon WorkSpaces.' Below the description are 'Learn more' and 'View use cases' links. At the bottom right are 'Cancel' and 'Next' buttons.

## 4-Select Standard or Enterprise Editions

5-Give Directory Name anjitest.xyz Any name is fine

The screenshot shows the 'Enter directory information' step of the AWS Directory Service setup wizard. The sidebar shows steps 1 through 4. The main panel title is 'Enter directory information'. It contains a 'Directory information' section stating 'A managed Microsoft Active Directory domain.' Below this is a 'Directory type' section showing 'Microsoft AD'. Under 'Operating system version' is 'Windows Server 2019'. A 'Edition' section follows, with 'Standard Edition' selected (indicated by a blue circle). The description for Standard Edition says: 'Best for small to medium sized businesses.' and lists storage (1GB), optimization (up to 30,000 objects), and cost (~USD 86.4000/mo). The 'Enterprise Edition' option is also shown with its description: 'Best for large businesses.' and lists storage (17GB), optimization (up to 500,000 objects), cost (~USD 288.0000/mo), and additional costs for each additional controller. Below these sections are fields for 'Directory DNS name' (containing 'anjitest.xyz') and 'Directory NetBIOS name - optional'.

6-Give Password and click on Next

<p>* includes two domain controllers, USD 43,2000/mo for each additional domain controller.</p>	<p>144.0000/mo for each additional domain controller.</p>
<p><b>Directory DNS name</b> A fully qualified domain name. This name will resolve inside your VPC only. It does not need to be publicly resolvable. <input type="text" value="anjitest.xyz"/></p>	
<p><b>Directory NetBIOS name - optional</b> A short identifier for your domain. If you do not specify a NetBIOS name, it will default to the first part of your Directory DNS name. <input type="text" value="CORP"/></p>	
<p><b>Directory description - optional</b> Descriptive text that appears on the details page after the directory has been created. <input type="text" value="Describe this directory"/></p>	
<p>Maximum of 128 characters, can only contain alphanumerics, and the following characters: `~@#%*+=:?./!\\-`. It must not start with a special character.</p>	
<p><b>Admin password</b> The password for the default administrative user named Admin. <input type="password" value="*****"/></p>	
<p>Passwords must be between 8 and 64 characters, not contain the word "admin", and include three of these four categories: lowercase, uppercase, numeric, and special characters.</p>	
<p><b>Confirm password</b> <input type="password" value="*****"/></p>	
<p>This password must match the Admin password above.</p>	
<input type="button" value="Cancel"/> <input type="button" value="Previous"/> <input style="background-color: orange; color: white; border: none;" type="button" value="Next"/>	

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

<p>Directory Service &gt; Directories &gt; Set up a directory</p> <p>Step 1 <a href="#">Select directory type</a></p> <p>Step 2 <a href="#">Enter directory information</a></p> <p>Step 3 <b>Choose VPC and subnets</b></p> <p>Step 4 <a href="#">Review &amp; create</a></p>	<p><b>Choose VPC and subnets</b> <a href="#">Info</a></p> <p><b>Networking</b> The VPC that contains your directory. If you do not have a VPC with at least two subnets, you must create one.</p> <p><b>VPC Info</b> VPC-1   vpc-061c5033df8adede6 (10.1.0.0/16) <input type="button" value="C"/> <input type="button" value="Create new VPC"/></p> <p><b>Subnets Info</b> VPC-1-public-1   subnet-064b5b07f40b1aecb (10.1.1.0/24, us-east-1a) <input type="button" value="C"/> VPC-1-DB-2   subnet-012139dccc6dc732d (10.1.60.0/24, us-east-1b) <input type="button" value="C"/> <input type="button" value="Create new subnet"/></p> <p>Initial AD site name for this directory <a href="#">Info</a> Default-First-Site-Name</p>
<input type="button" value="Cancel"/> <input type="button" value="Previous"/> <input style="background-color: orange; color: white; border: none;" type="button" value="Next"/>	

## 9-Click on Create Create Directory

Step 1  
[Select directory type](#)

Step 2  
[Enter directory information](#)

Step 3  
[Choose VPC and subnets](#)

Step 4  
**Review & create**

**Review & create Info**

Review	
Directory type	VPC
Microsoft AD	VPC-1   vpc-061c5033df8adede6 (10.1.0.0/16)
Operating system version	Windows Server 2019
Directory DNS name	VPC-1-public-1   subnet-064b5b07f40b1aecb (10.1.1.0/24, us-east-1a)
anjitest.xyz	VPC-1-DB-2   subnet-012139dcc6dc732d (10.1.60.0/24, us-east-1b)
Directory NetBIOS name	-
Directory description	-

Pricing	
Edition	Standard
Standard	Free trial eligible <a href="#">Learn more</a> 30-day limited trial
Domain controllers charge	~USD 86.4000/mo (USD 0.1200/hr)*
* Includes two domain controllers, USD 43.2000/mo for each additional domain controller.	

[Cancel](#) [Previous](#) **Create directory**

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

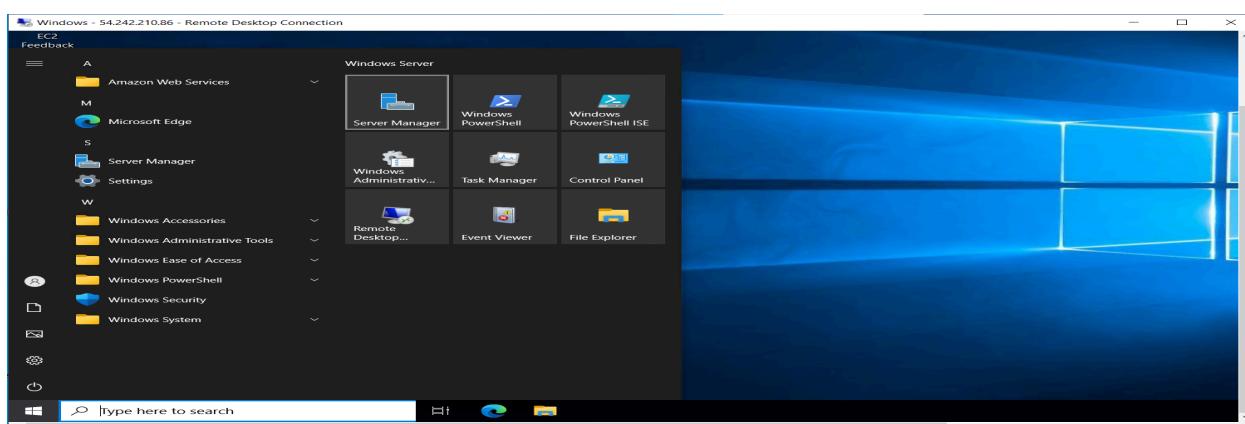
[Directory Service](#) > Directories

**Directories (1) Info**

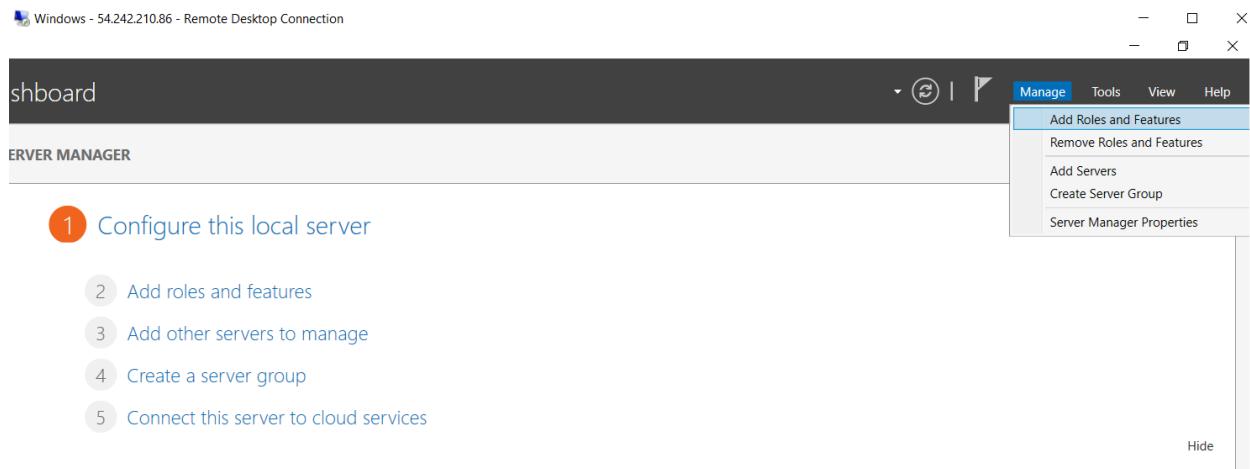
Directory ID	Directory name	Type	Size	Multi-Region	Status	Launch date
<a href="#">d-9067d1814d</a>	anjitest.xyz	Microsoft AD	Standard	Not applicable	<a href="#">Creating</a>	Aug 23, 2024

[Actions](#) **Set up directory**

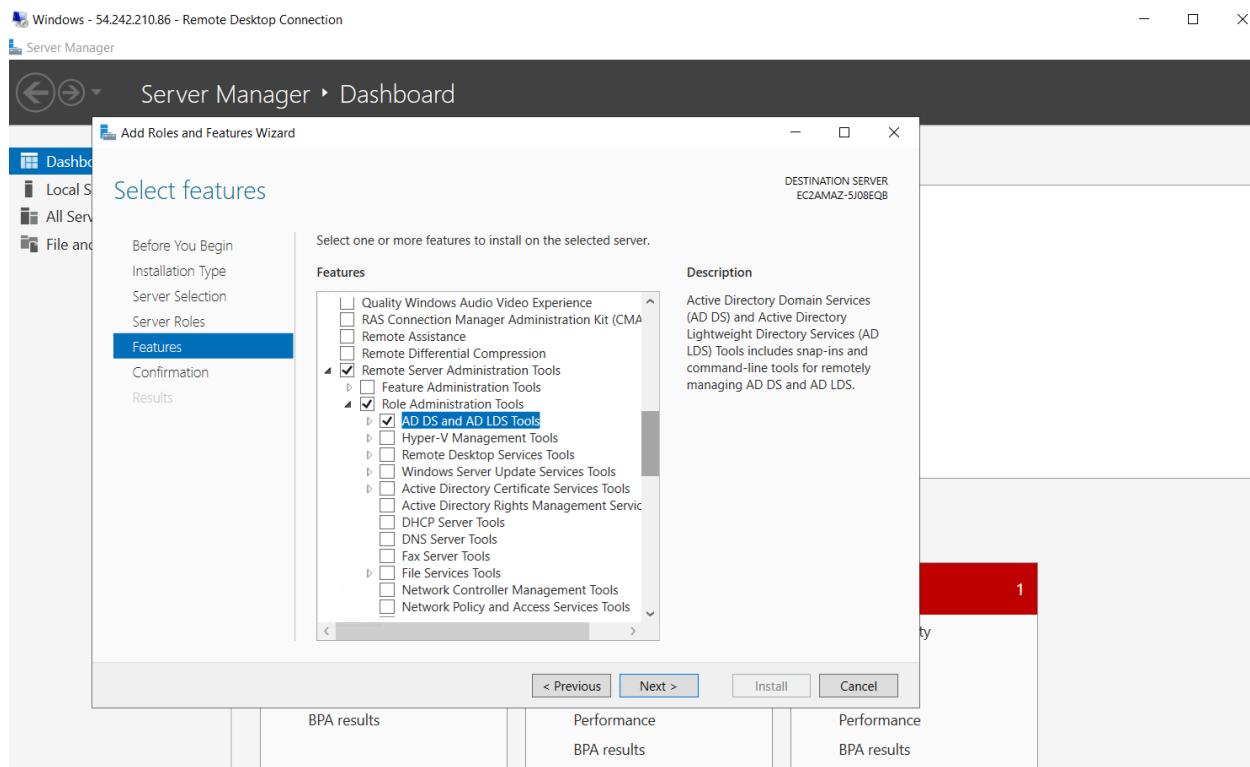
## 11-Connect the Windows server and click on Server Manager



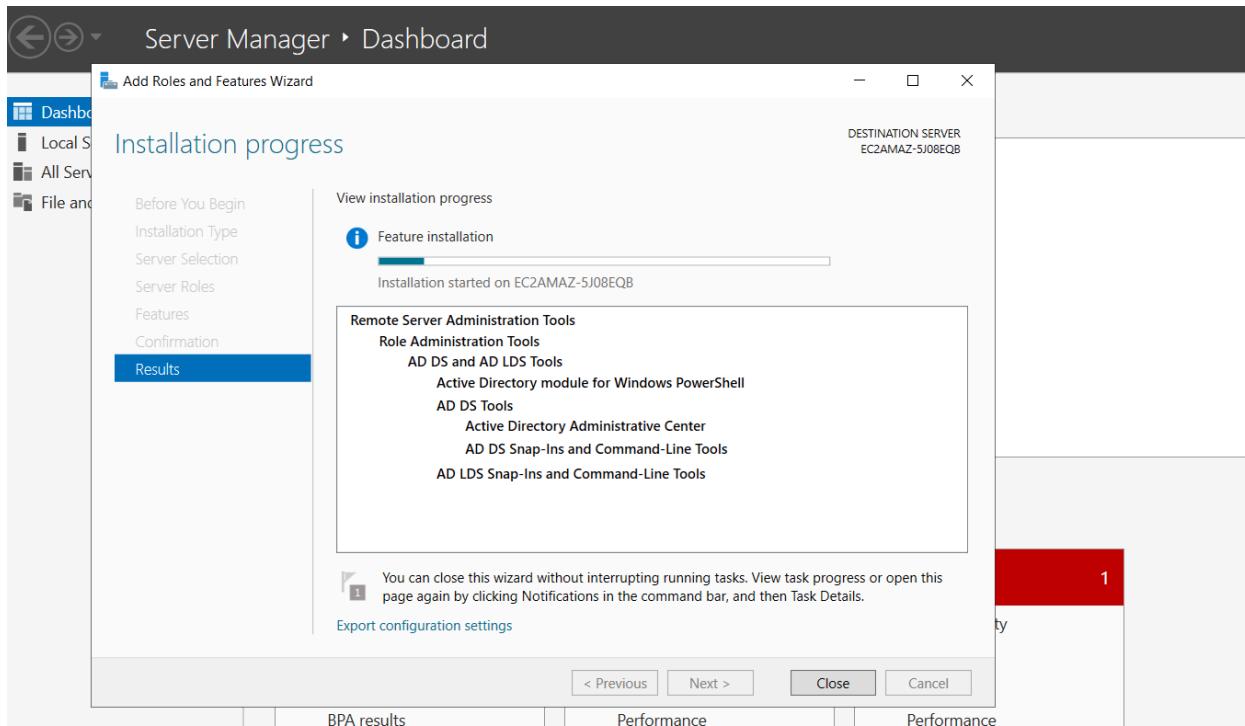
## 12-Click on Manage under Add Roles and features



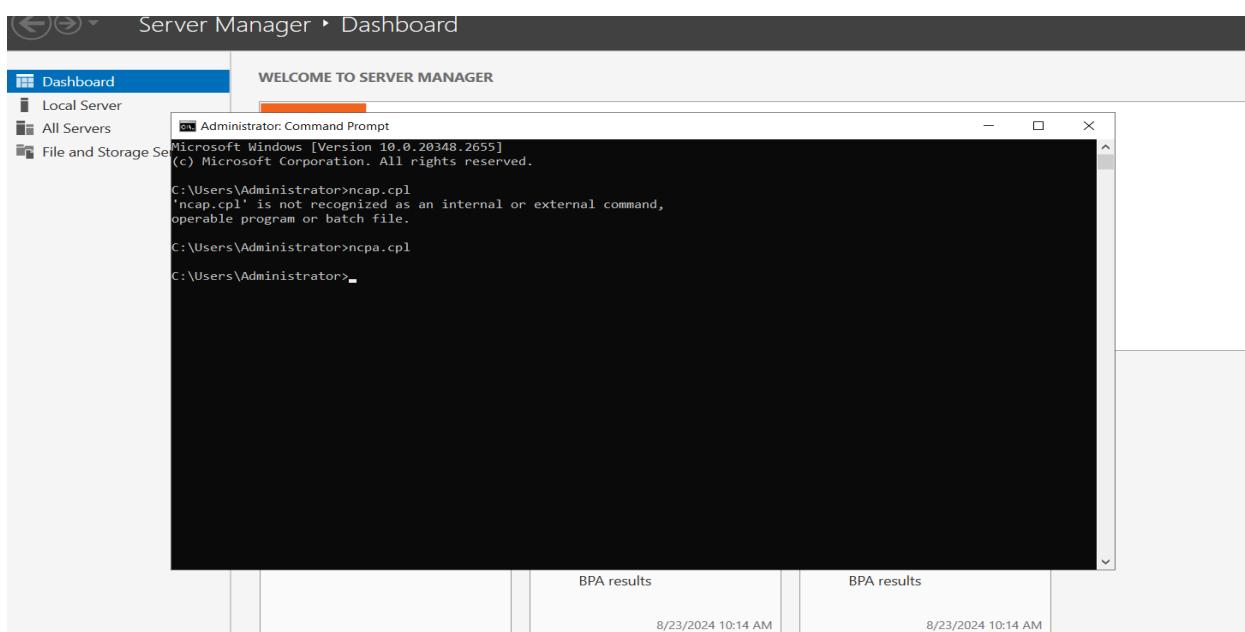
## 13-Click on Next and Next and Next here select Remote server administrative tools under role administrative tools under AD DS and AD LDS tools then Next



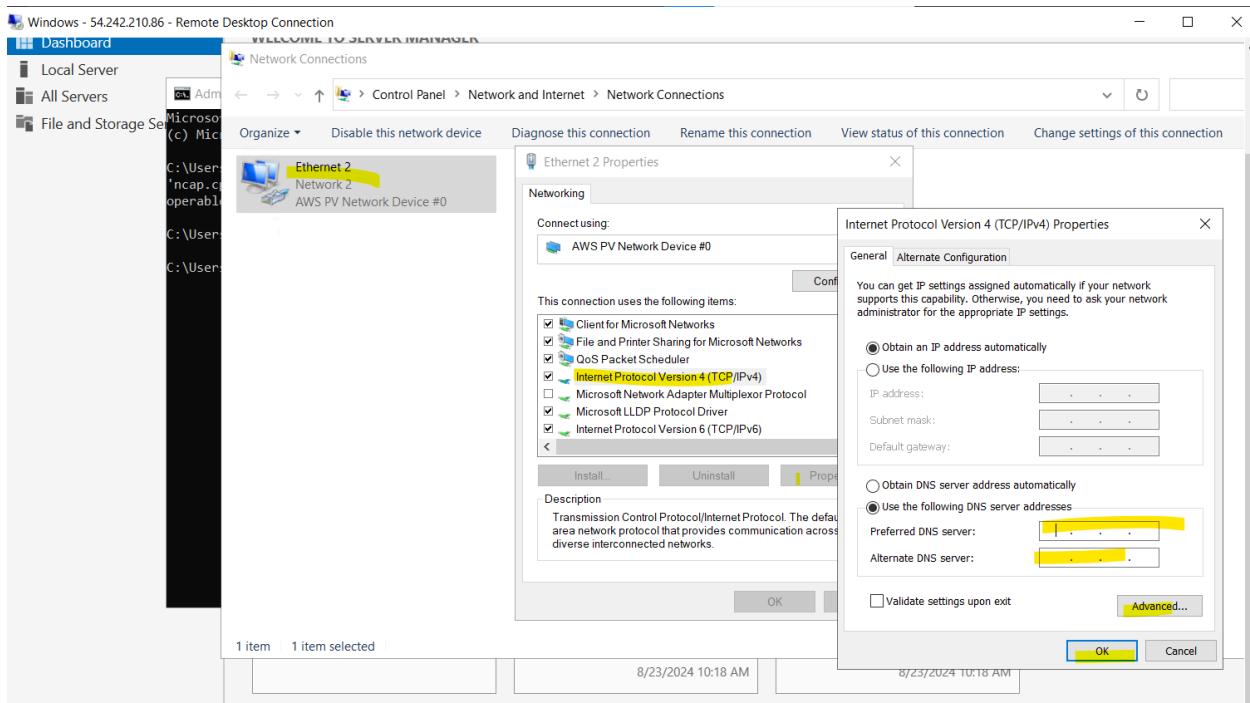
## 14-Click on next and Install



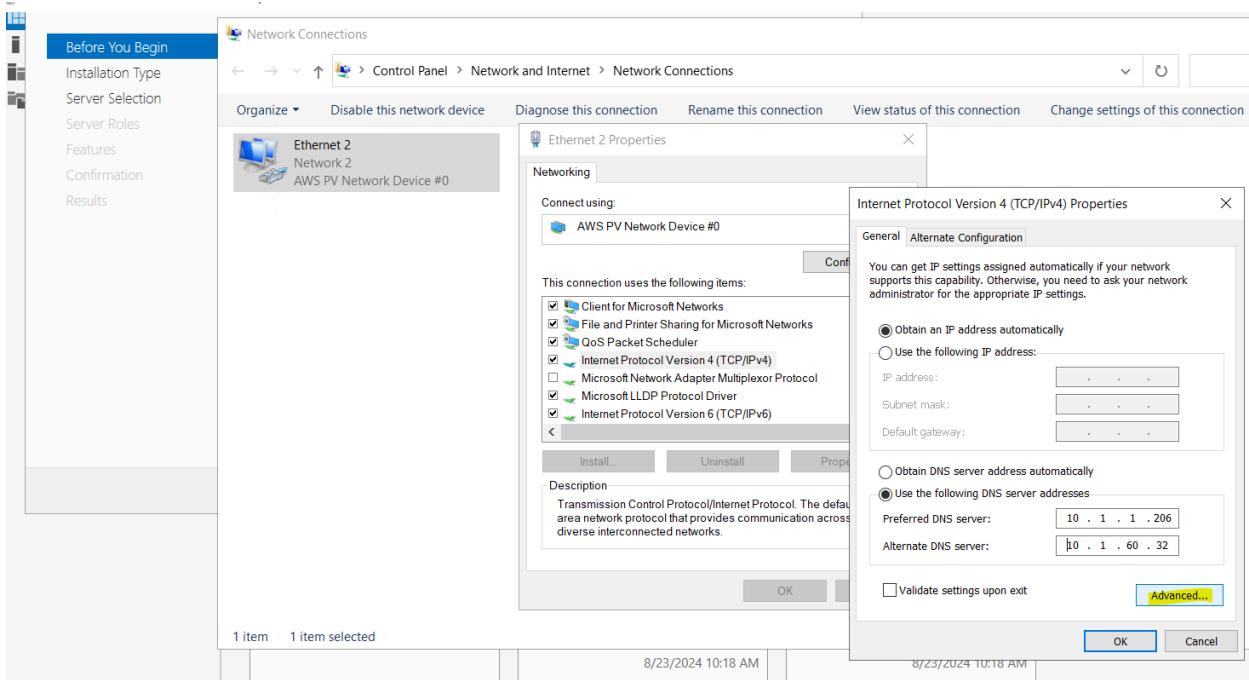
## 15-Click on CMD on the Windows server



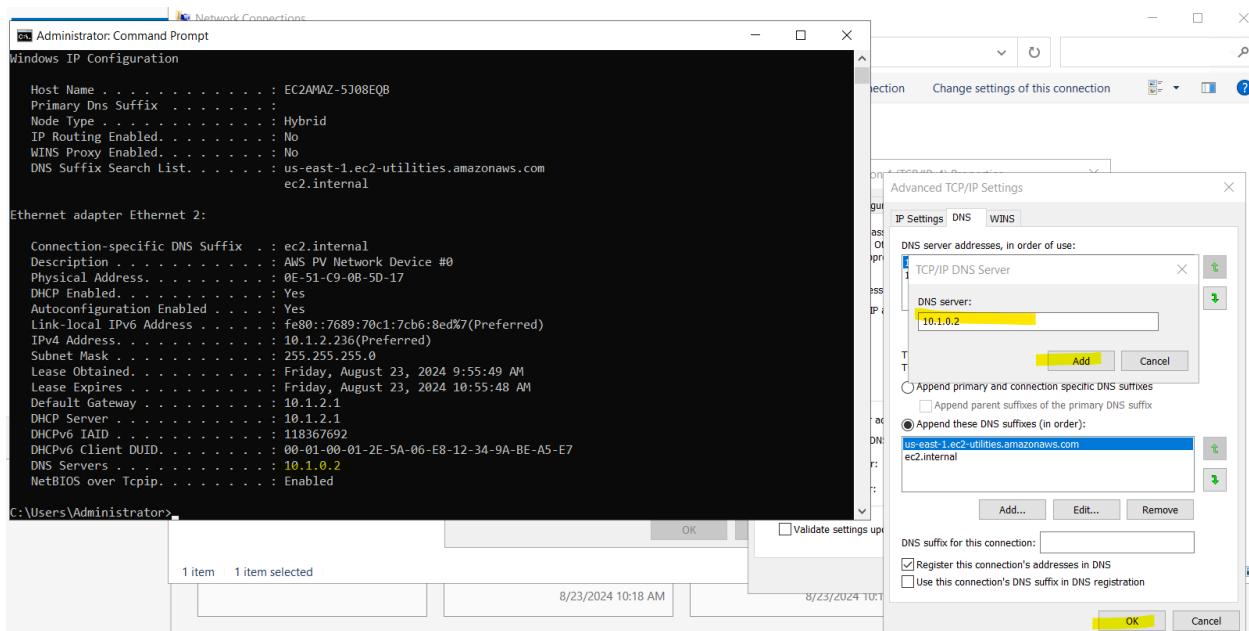
## 16-Click on Ipv4 properties to add AD Managed IPs into DNS Server IPs



The screenshot shows the AWS CloudWatch Metrics interface. The top navigation bar includes 'Directory Service > Directories > d-9067d1814d' and an 'Actions' dropdown. Below this, the directory details for 'd-9067d1814d' are displayed. The 'Networking & security' tab is selected. Under 'Networking details', it shows the VPC ID 'vpc-061c5033df8adeda6' and its subnets: 'subnet-064b5b07f40b1aecb' and 'subnet-012139dccc6dc732d'. The DNS address listed is '10.1.2.206'. To the right, the status is 'Active', last updated on 'Friday, August 23, 2024', and launched on 'Friday, August 23, 2024'. Other tabs visible include 'Scale & share', 'Application management', and 'Maintenance'.



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



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

```

Administrator: Command Prompt
Host Name . . . . . : EC2AMAZ-5J08EQB
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : us-east-1.ec2-utilities.amazonaws.com
ec2.internal

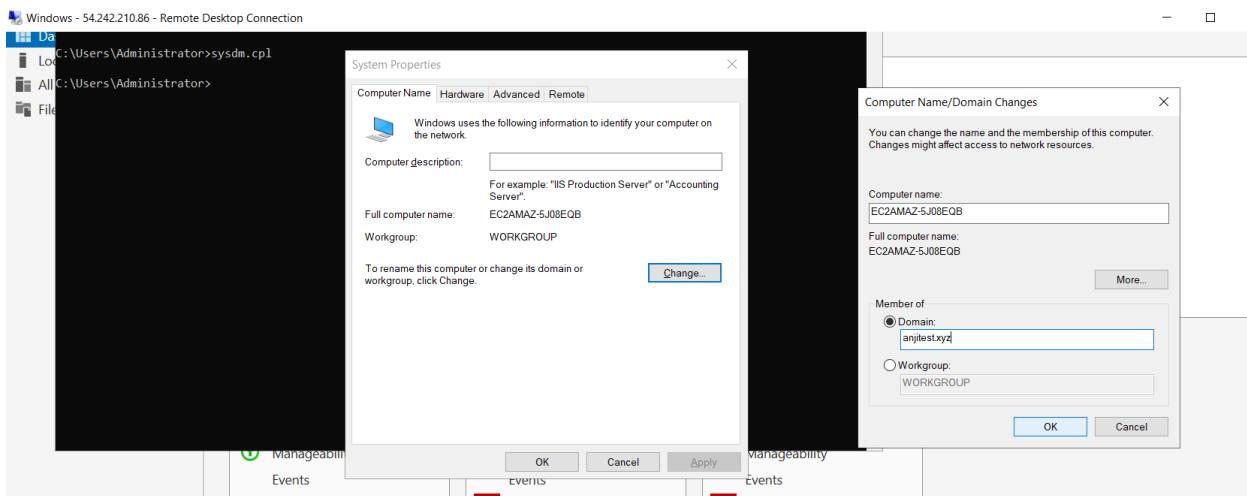
Ethernet adapter Ethernet 2:

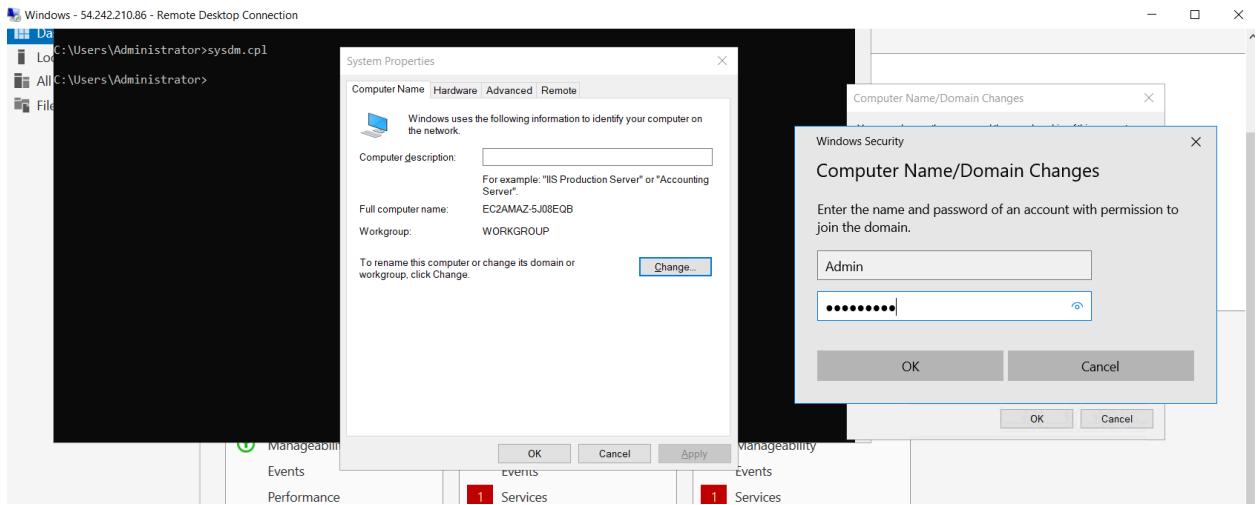
Connection-specific DNS Suffix . : ec2.internal
Description . . . . . : Alm PV Network Device
Physical Address. . . . . : 0E-51-C9-0B-5D-17
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::7689:70c1:7cb6:8ed%7(PREFERRED)
IPv4 Address. . . . . : 10.1.2.236(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Friday, August 23, 2024 9:55:49 AM
Lease Expires . . . . . : Friday, August 23, 2024 11:28:55 AM
Default Gateway . . . . . : 10.1.2.1
DHCP Server . . . . . : 10.1.2.1
DHCPv6 IAID . . . . . : 118367692
DHCPv6 Client DUID. . . . . : 00-01-00-01-2E-5A-06-E8-12-34-9A-BE-A5-E7
DNS Servers . . . . . : 10.1.1.206
10.1.60.32
10.1.0.2
NetBIOS over Tcpip. . . . . : Enabled

C:\Users\Administrator>

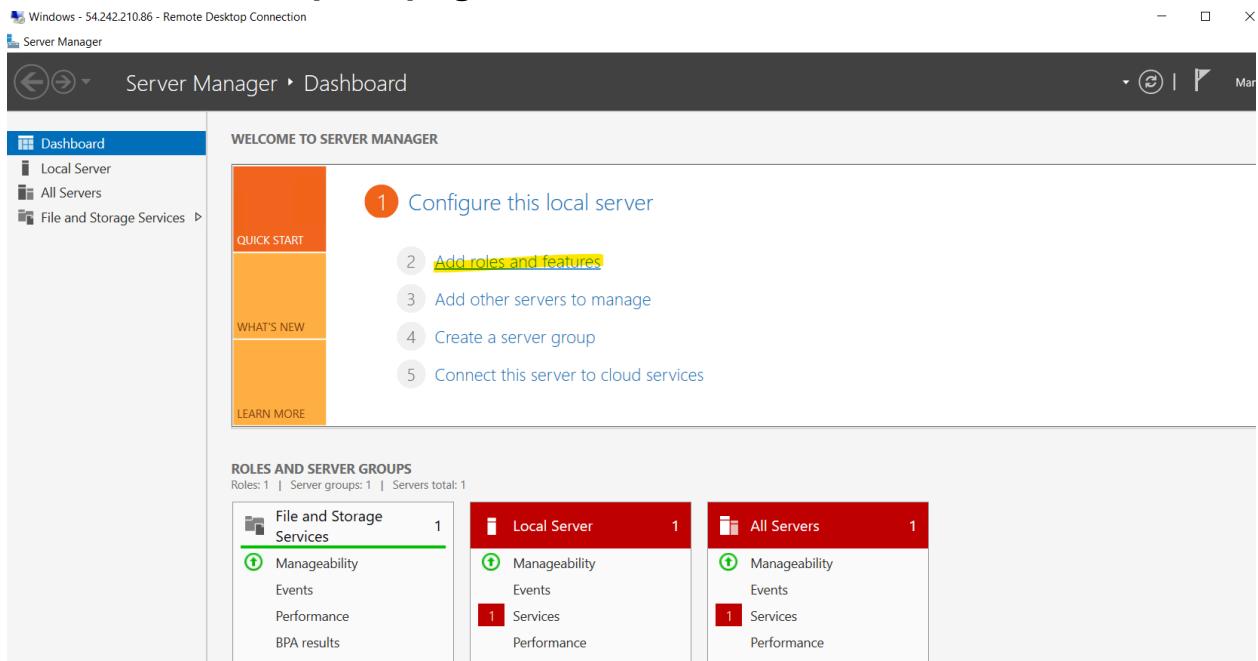
```

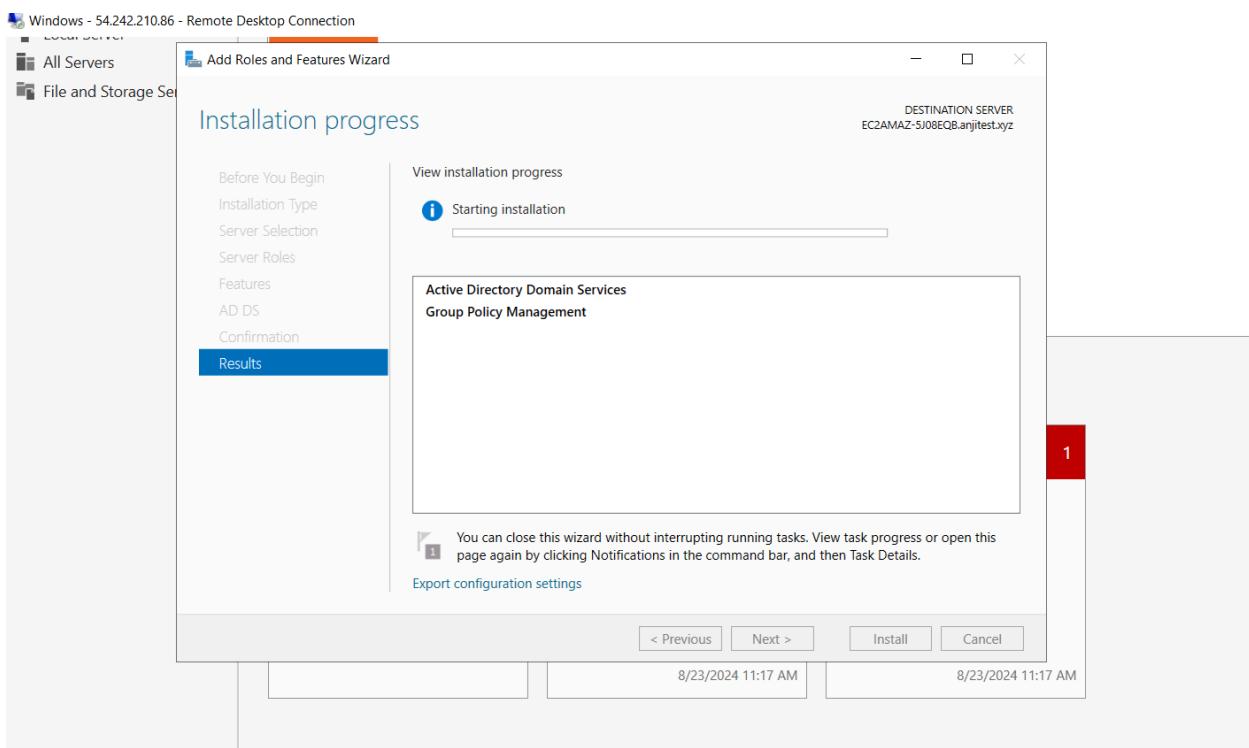
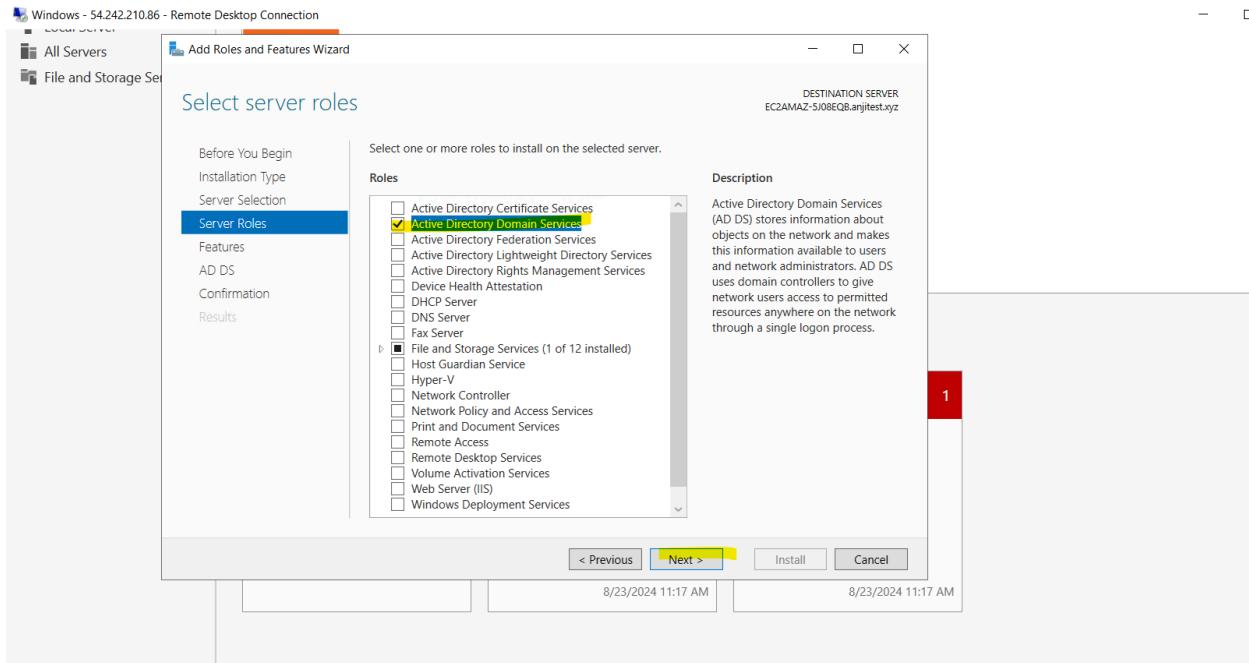
**19-Click on cmd and type sysdm.cpl it will open click on change and select the Domain to give your domain anjitest.xyz then it will ask for a prompt username and password**





## It will Restart the prompt give it to Restart.





## 21-Click on Create DHCP Option-Set

VPC dashboard X

DHCP option sets (1) Info

Find resources by attribute or tag

Name	DHCP option set ID	Options	Owner
-	<a href="#">dopt-0d9487cf4c5111373</a>	domain-name: ec2.internal domain-name-servers: Am...	637423512556

EC2 Global View ▾

Filter by VPC ▾

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only Internet gateways
- Carrier gateways

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

DHCP option set name - optional  
AD-DHCP

**DHCP option**  
Specify at least one configuration parameter.

Domain name [Info](#)  
aniltest.xyz

Domain name servers [Info](#)  
10.1.2.06, 10.1.60.32

NTP servers [Info](#)  
169.254.169.125

NetBIOS name servers [Info](#)  
192.168.0.4, 198.168.0.5

IPv6 preferred lease time [Info](#)  
70000  
Seconds

AWS Command Line Interface command

**Tags**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key [Name](#) Value - optional [AD-DHCP](#) Remove tag  
Add tag

You can add 49 more tags

Create DHCP option set

## 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

VPC > Your VPCs > [vpc-061c5033df8adede6](#) > Edit VPC settings

### Edit VPC settings Info

**VPC details**

VPC ID  
vpc-061c5033df8adede6  
Name  
VPC-1

**DHCP settings**

DHCP option set Info  
[dopt-012f05aa7a55f1e77 \(AD-DHCP\)](#)

**DNS settings**

Enable DNS resolution Info  
 Enable DNS hostnames Info

**Network Address Usage metrics settings**

Enable Network Address Usage metrics Info

Cancel Save

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

[AmazonSSMDirectoryServiceAccess](#)

[AmazonSSMManagedInstanceCore](#)

IAM > Roles > Create role

Step 1  
[Select trusted entity](#)

Step 2  
[Add permissions](#) Info

Step 3  
Name, review, and create

#### Add permissions Info

Permissions policies (2/959) Info

Choose one or more policies to attach to your new role.

Filter by Type  All types 9 matches

Policy name	Type	Description
<input type="checkbox"/> <a href="#">AmazonSSMAutomationApproverAccess</a>	AWS managed	Provides access to view automation execu...
<input type="checkbox"/> <a href="#">AmazonSSMAutomationRole</a>	AWS managed	Provides permissions for EC2 Automation ...
<input checked="" type="checkbox"/> <a href="#">AmazonSSMDirectoryServiceAccess</a>	AWS managed	This policy allows SSM Agent to access Dir...
<input type="checkbox"/> <a href="#">AmazonSSMPullAccess</a>	AWS managed	Provides full access to Amazon SSM.
<input type="checkbox"/> <a href="#">AmazonSSMMaintenanceWindowRole</a>	AWS managed	Service Role to be used for EC2 Maintenan...
<input type="checkbox"/> <a href="#">AmazonSSMManagedC2InstanceDefaultPolicy</a>	AWS managed	This policy enables AWS Systems Manager...
<input checked="" type="checkbox"/> <a href="#">AmazonSSMManagedInstanceCore</a>	AWS managed	The policy for Amazon EC2 Role to enable...
<input type="checkbox"/> <a href="#">AmazonSSMPatchAssociation</a>	AWS managed	Provide access to child instances for patch...
<input type="checkbox"/> <a href="#">AmazonSSMReadOnlyAccess</a>	AWS managed	Provides read only access to Amazon SSM.

[Set permissions boundary - optional](#)

Cancel Previous Next

**Domain-join** Info

Allows EC2 instances to call AWS services on your behalf.

**Summary**

Creation date August 23, 2024, 16:24 (UTC+05:30)	ARN <a href="#">arn:aws:iam::637423512556:role/Domain-join</a>	Instance profile ARN <a href="#">arn:aws:iam::637423512556:instance-profile/Domain-join</a>
Last activity -	Maximum session duration 1 hour	

**Permissions** [Edit](#)

**Permissions policies (3) Info**  
You can attach up to 10 managed policies.

Policy name	Type	Attached entities
<a href="#">AmazonEC2RoleforSSM</a>	AWS managed	3
<a href="#">AmazonSSMDirectoryServiceAccess</a>	AWS managed	1
<a href="#">AmazonSSMManagedInstanceCore</a>	AWS managed	1

**Permissions boundary (not set)**

**Generate policy based on CloudTrail events**

## 24-Launch Windows instance with

**Name**  
 Add additional tags

**Application and OS Images (Amazon Machine Image) Info**  
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

**Recents** [Quick Start](#)

Amazon Linux	macOS	Ubuntu	Windows	Red Hat	SUSE Li
--------------	-------	--------	---------	---------	---------

**Amazon Machine Image (AMI)**  
Microsoft Windows Server 2022 Base  
ami-07cc1bbe145f35b58 (64-bit (x86))  
Virtualization: hvm ENA enabled: true Root device type: ebs

**Summary**

Number of instances [Info](#)  
1

**Software Image (AMI)**  
Microsoft Windows Server 2022 ...[read more](#)  
ami-07cc1bbe145f35b58

**Virtual server type (instance type)**  
t2.micro

**Firewall (security group)**  
New security group

**Storage (volumes)**  
1 volume(s) - 30 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB

[Cancel](#) [Launch instance](#) [Review commands](#)

On-Demand SUSE base pricing: 0.0116 USD per Hour  
 On-Demand RHEL base pricing: 0.026 USD per Hour  
 On-Demand Linux base pricing: 0.0116 USD per Hour

Additional costs apply for AMIs with pre-installed software

**▼ Key pair (login) [Info](#)**

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*  
 [Create new key pair](#)

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

**▼ Network settings [Info](#)**

VPC - *required* [Info](#)  
 [Create new subnet](#)

Subnet [Info](#)  
  
 VPC: vpc-061c5033df8adeda6 Owner: 637423512556 Availability Zone: us-east-1b Zone type: Availability Zone IP addresses available: 250 CIDR: 10.1.2.0/24

Auto-assign public IP [Info](#)  
 Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) [Info](#)  
 A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.  
 Create security group  Select existing security group

Common security groups [Info](#)  
 [Compare security group rules](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

[Advanced network configuration](#)

**▼ Configure storage [Info](#)** Advanced

1x  GiB  Root volume (Not encrypted)

[Free tier eligible customers can get up to 30 GB of EBS General Purpose \(SSD\) or Magnetic storage](#)

[Add new volume](#)

**▼ Summary**

Number of instances [Info](#)

Software Image (AMI)  
 Microsoft Windows Server 2022 ...read more  
 ami-07cc1bbe145f35b58

Virtual server type (instance type)  
 t2.micro

Firewall (security group)  
 New security group

Storage (volumes)  
 1 volume(s) - 30 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB

[Cancel](#) [Launch instance](#) [Review commands](#)

Here add domain controller and iam you created join-domain

The screenshot shows the AWS CloudFormation 'Create new stack' dialog. On the left, there are several configuration sections:

- Domain join directory**: Set to 'anjitest.xyz' (VPC: vpc-061c5033df8adede6).
- IAM instance profile**: Set to 'Domian-join' (arn:aws:iam:637423512556:instance-profile/Domian-join).
- Hostname type**: Set to 'IP name'.
- DNS Hostname**: Options include 'Enable IP name IPv4 (A record) DNS requests' (checked), 'Enable resource-based IPv4 (A record) DNS requests', and 'Enable resource-based IPv6 (AAAA record) DNS requests'.
- Instance auto-recovery**: Set to 'Select'.
- Shutdown behavior**: Set to 'Stop'.
- Stop - Hibernate behavior**: Set to 'Select'.

On the right, the 'Summary' section shows:

- Number of instances**: 1
- Software Image (AMI)**: Microsoft Windows Server 2022 (ami-07cc1bbe145f53b58)
- Virtual server type (instance type)**: t2.micro
- Firewall (security group)**: VPC-1-Security
- Storage (volumes)**: 1 volume(s) - 30 GiB

A callout box highlights the 'Free tier' information: 'In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB storage per month.'

At the bottom right are 'Cancel' and 'Launch instance' buttons.

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

Anji  
Sampi

The screenshot shows the Windows Active Directory Users and Computers (ADUC) interface. On the left, the navigation pane shows the tree structure under 'anjitest.xyz'. A 'New Object - User' dialog box is open in the foreground, prompting for user details:

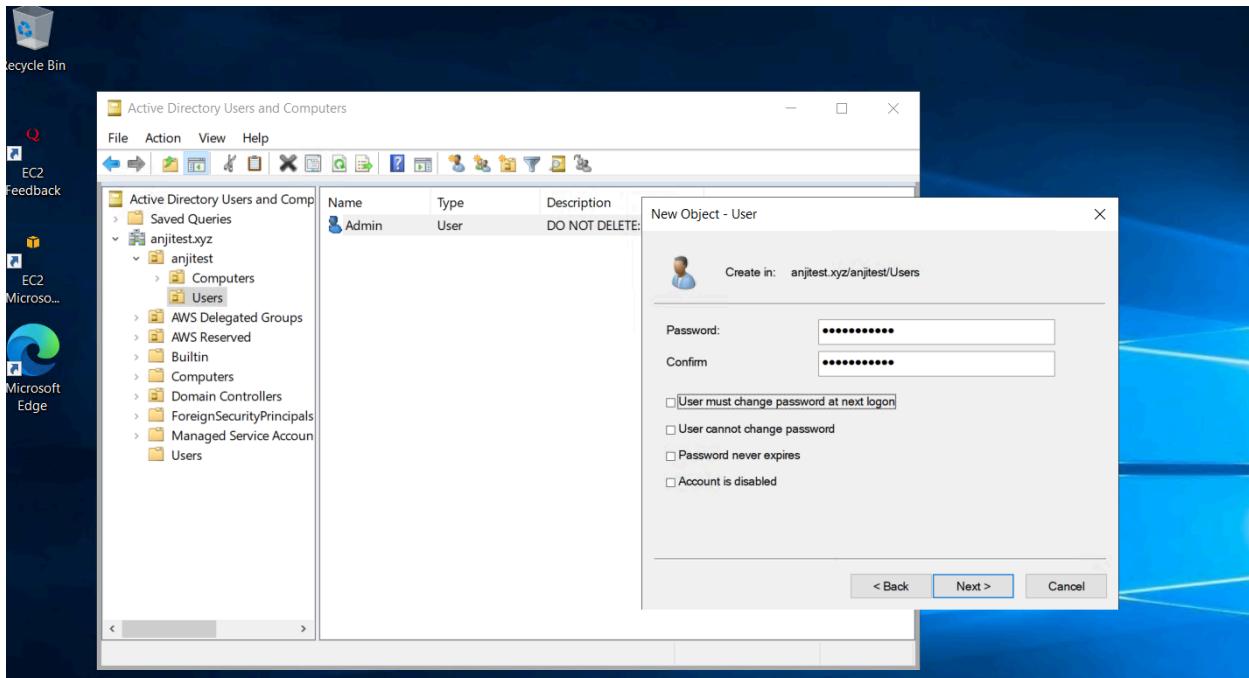
Name	Type	Description
Admin	User	DO NOT DELETE

The dialog fields are filled as follows:

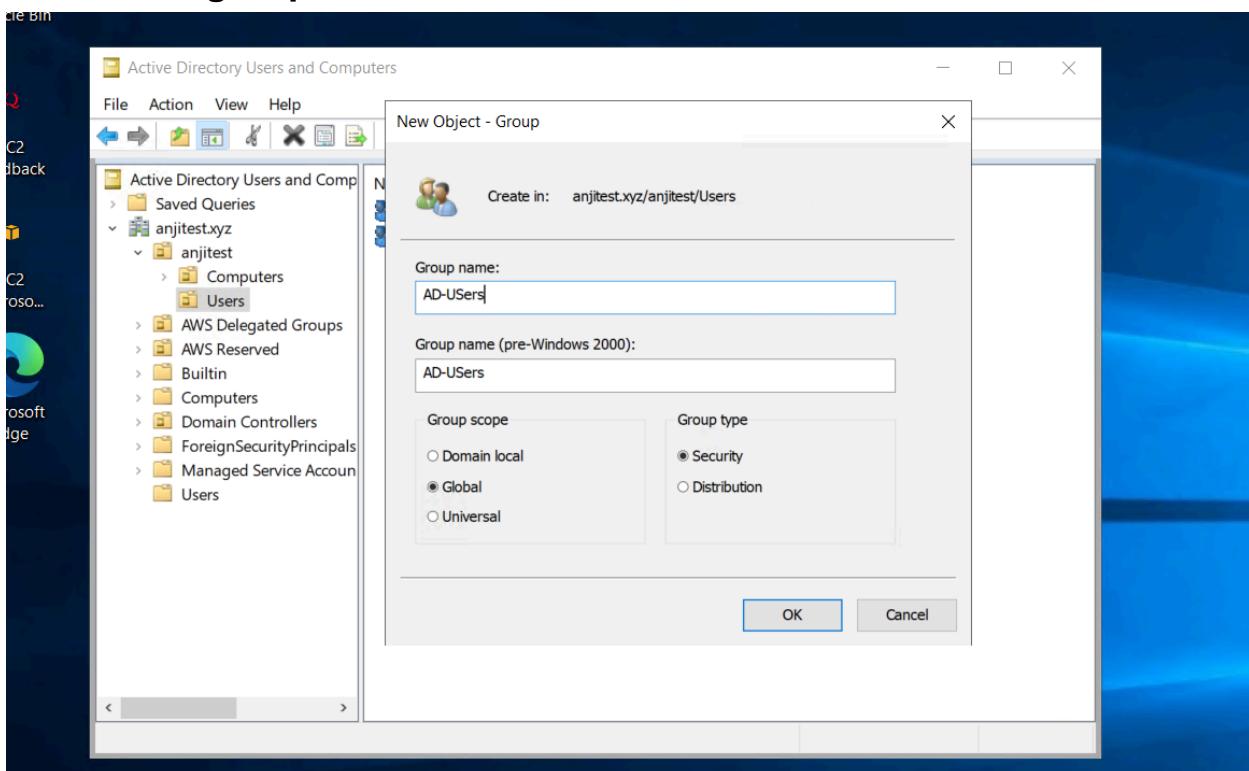
- Create in: anjitest.xyz/anjitest/Users
- First name: Samp
- Last name:
- Full name: Sampi
- User logon name: Sampi (@anjitest.xyz)
- User logon name (pre-Windows 2000): anjitest\ Sampi

At the bottom of the dialog are 'Next >' and 'Cancel' buttons.

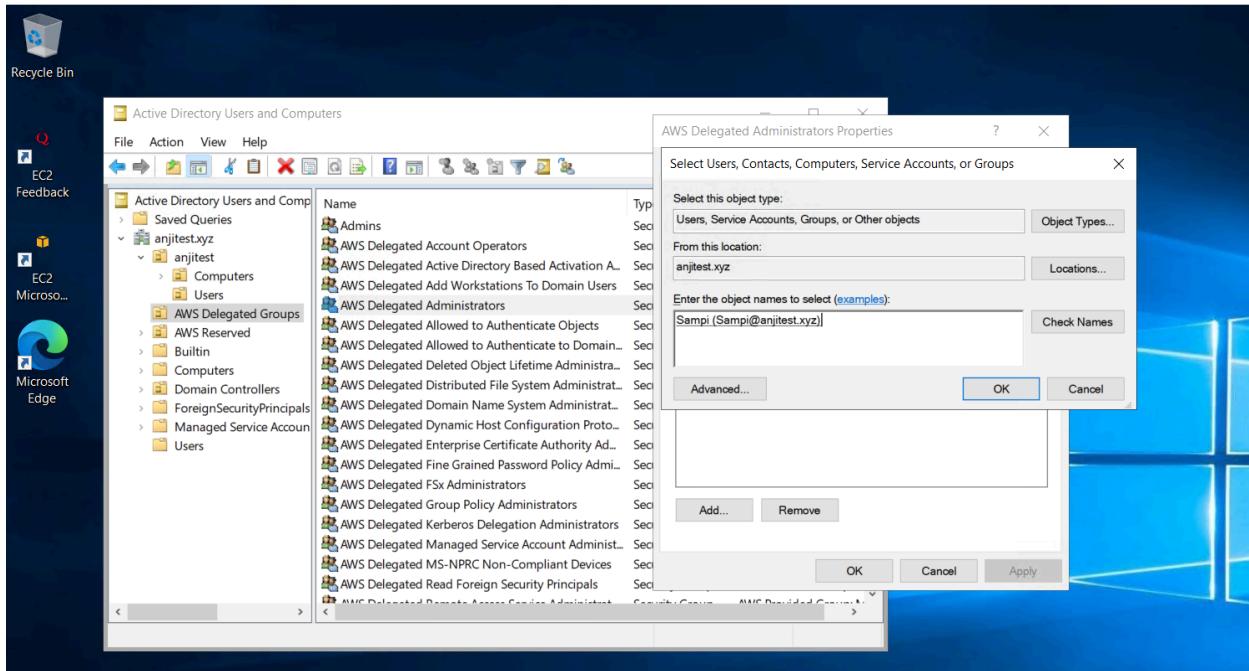
On the right, the main window displays a list of users in the 'anjitest' container, showing one entry: 'Admin' (User).



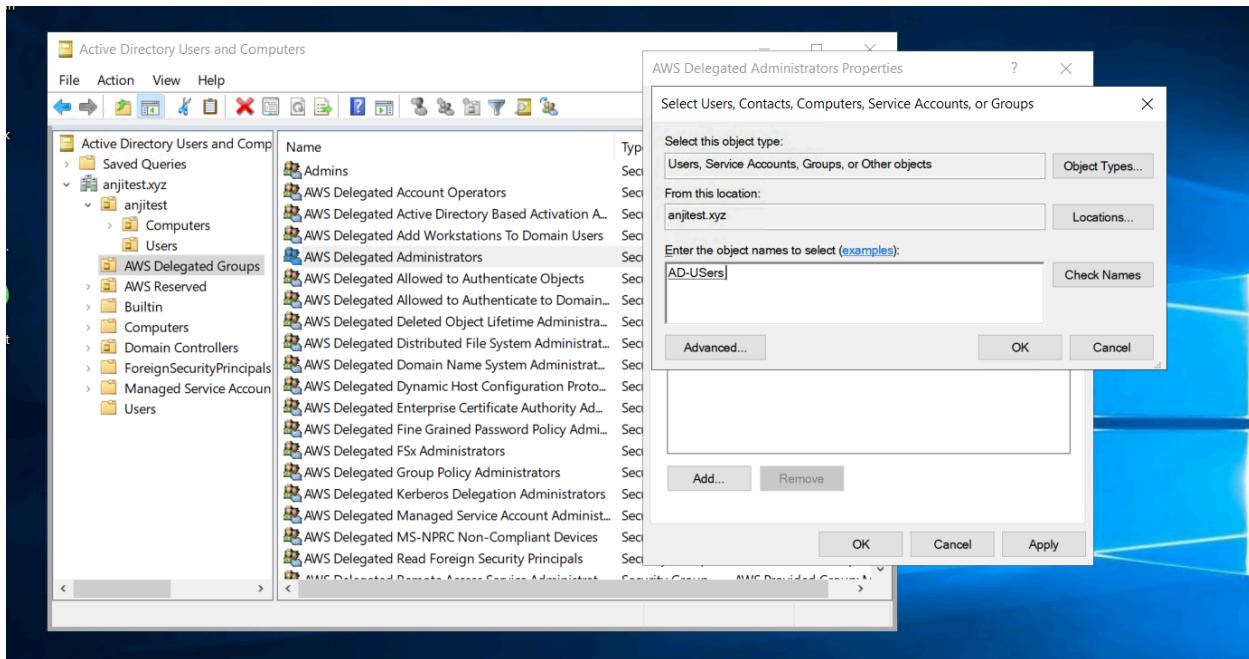
## Create one group



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

Name	Instance ID
Windows	i-0e032060fe64c591f
<b>join-windows</b>	<b>i-050245ec3d1bba82e</b>

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

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary Info

Instance ID: i-050245ec3d1bba82e (join-windows)

IPv6 address: -

Hostname type: IP name: ip-10-1-2-123.ec2.internal

Public IPv4 address copied: 34.207.98.68 | open address

Private IPv4 addresses: 10.1.2.123

Public IPv4 DNS: ec2-34-207-98-68.compute-1.amazonaws.com | open address

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

Instances (1/2) Info

Name	Instance ID
Windows	i-0e032060fe64c591f
<b>join-windows</b>	<b>i-050245ec3d1bba82e</b>

34.207.98.68 | open address

Instance state: Running

Private IP DNS name (IPv4 only): ip-10-1-2-123.ec2.internal

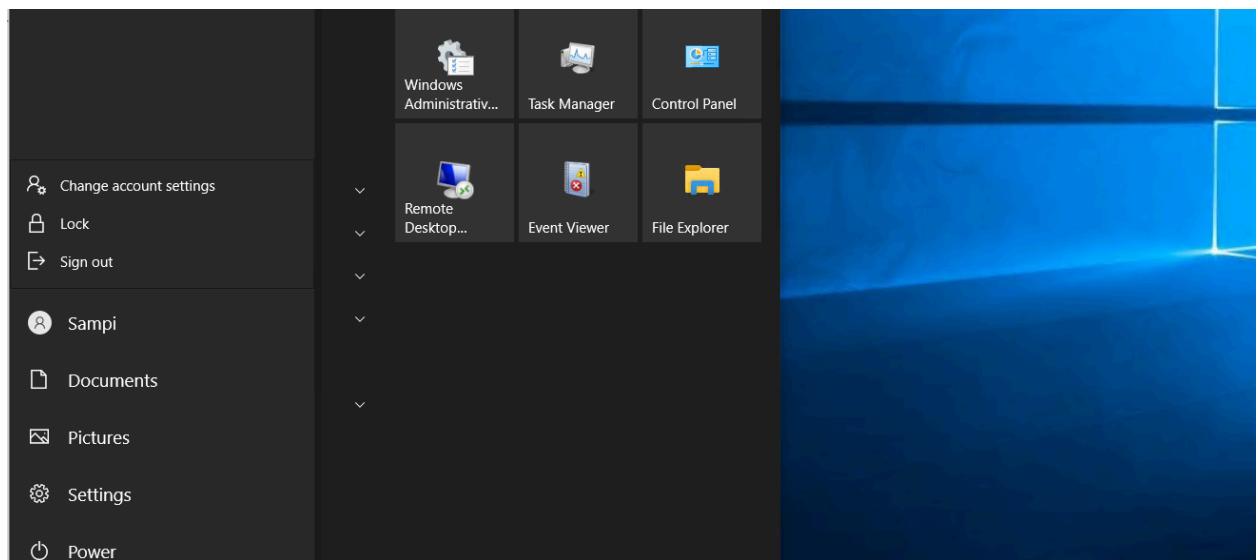
Alarm status | Availability Zone | Public IPv4 DNS | Public IPv4 DNS

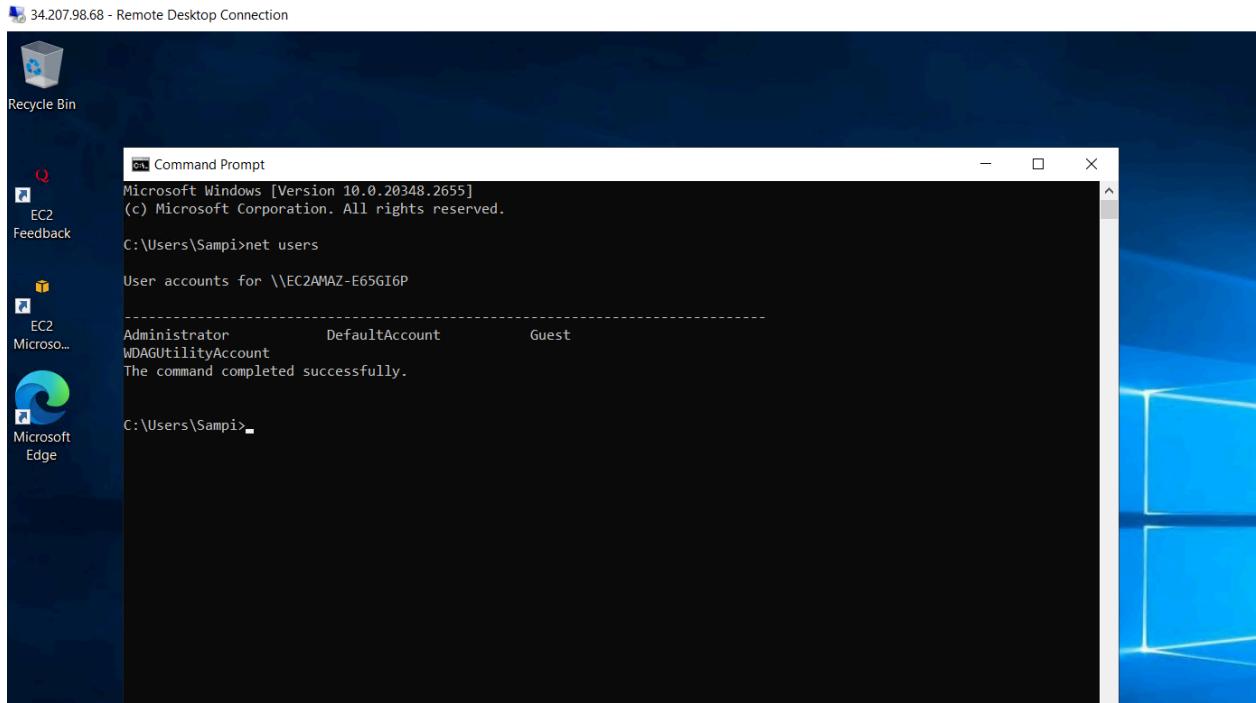
View alarms + us-east-1b ec2-3-92-163-175.com... 3.92

View alarms + us-east-1b ec2-34-207-98-68.com... 34.21

The screenshot shows the AWS EC2 Instances page. In the center, a 'Remote Desktop Connection' window is open, displaying the message 'Connecting to: 34.207.98.68'. Below it, a progress bar shows 'Securing remote connection...'. At the bottom of this window are 'Show Options', 'Connect', and 'Help' buttons. To the left of the connection window, there's a sidebar titled 'Instances (1/2) Info' with a search bar and a table showing two instances: 'Windows' (i-0e032060fe64c591f) and 'join-windows' (i-050245ec3d1bba82e). On the right, a table lists 'Alarm status', 'Availability Zone', and 'Public IPv4 DNS' for two instances: 'us-east-1b' (ec2-3-92-163-175.com...) and 'us-east-1b' (ec2-34-207-98-68.com...).

**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
```

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

i-04372ea9fd2e1457d (join-linux)
PublicIPs: 98.81.225.41 PrivateIPs: 10.1.2.145
```

```
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
10.1.1.10.in-addr.arpa name = ip-c61301d5.anjitest.xyz.
10.1.1.10.in-addr.arpa name = anjitest.xyz.

[root@ip-10-1-2-145 ~]# nslookup 10.1.60.32
10.1.1.10.in-addr.arpa name = ip-c6130295.anjitest.xyz.
10.1.1.10.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**

```
VPC S3 IAM EC2 S3 Glacier EFS Lambda AWS Backup RDS [root@ip-10-1-2-145 ~]# vi /etc/hosts
[root@ip-10-1-2-145 ~]#
```

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost6 localhost6.localdomain6

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

**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

```
# But this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile .ssh/authorized_keys

#AuthorizedPrincipalsFile none

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
#PasswordAuthentication no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

-- INSERT --

i-04372ea9fd2e1457d (join-linux)
PublicIPs: 98.81.225.41 PrivateIPs: 10.1.2.145
```

## Changed after

```
#AuthorizedPrincipalsFile none

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
#PasswordAuthentication no

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

-- INSERT --

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 umount 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

110,33-46

```

## 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
%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 umount 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 administrators@anjitest.xyz),1796601140(aws delegated domain name system administrators@anjitest.xyz),1796601142(aws delegated server administrators@anjitest.xyz),1796601121(aws delegated account administrators@anjitest.xyz),1796601126(aws delegated distributed file system administrators@anjitest.xyz),1796601127(aws delegated dynamic host configuration protocol administrators@anjitest.xyz),1796601134(aws delegated replicated directory change administrators@anjitest.xyz),1796601109(dnsadministrators@anjitest.xyz),1796601130(aws delegated group policy administrators@anjitest.xyz),1796601136(aws delegated system management administrators@anjitest.xyz),1796601139(aws delegated workstations@anjitest.xyz),1796601131(domain users@anjitest.xyz),1796601113(aws delegated remote access administrators@anjitest.xyz),1796601114(aws delegated managed computer administrators@anjitest.xyz),1796601119(aws delegated delegation administrators@anjitest.xyz),1796601122(aws delegated active directory based activation administrators@anjitest.xyz),1796601120(aws delegated fex administrators@anjitest.xyz),1796601122(aws delegated read foreign security principals@anjitest.xyz),1796601125(aws delegated deleted object lifetime administrators@anjitest.xyz),1796601129(aws delegated fine grained password policy administrators@anjitest.xyz),1796601128(aws delegated 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

```

Are you sure you want to continue connecting (yes/no/[fingerprint])?
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:dlzITj8HFcXgpd0TATKQJU6TMAS0B1WxCVIZHFJnc+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's password:
Creating home directory for Sampi@anjitest.xyz.

      _#
     ~\ _###_      Amazon Linux 2
    ~~\###\#
   ~~ \##\#      AL2 End of Life is 2025-06-30.
  ~~ \#/ .\_
 ~\~ \~\ / A newer version of Amazon Linux is available!
  ~\~ \~\ /_ Amazon Linux 2023, GA and supported until 2028-03-15.
     ~\~\ /_ https://aws.amazon.com/linux/amazon-linux-2023/
  ~\~\ /_m/`_>

[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**

