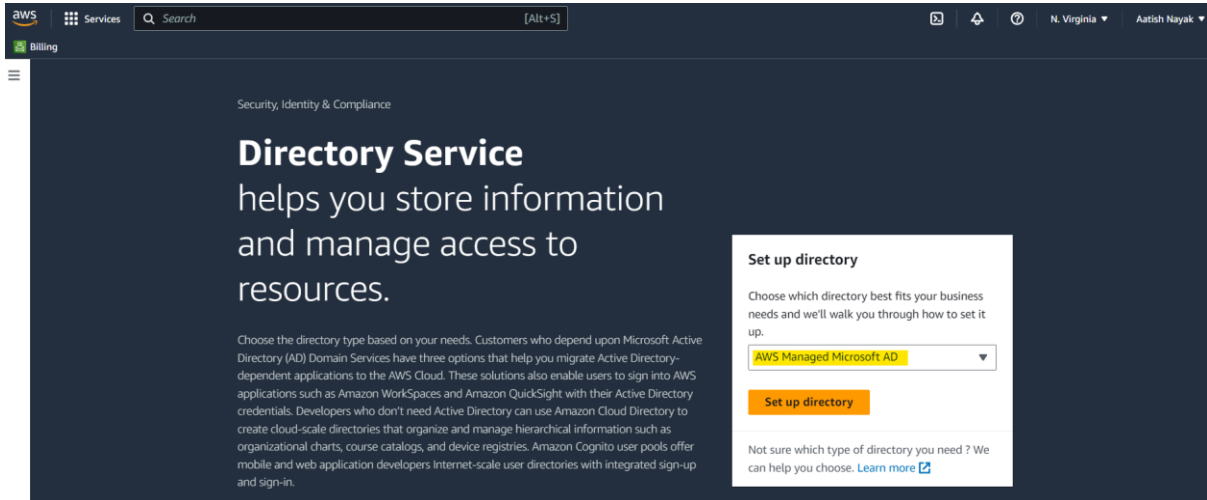


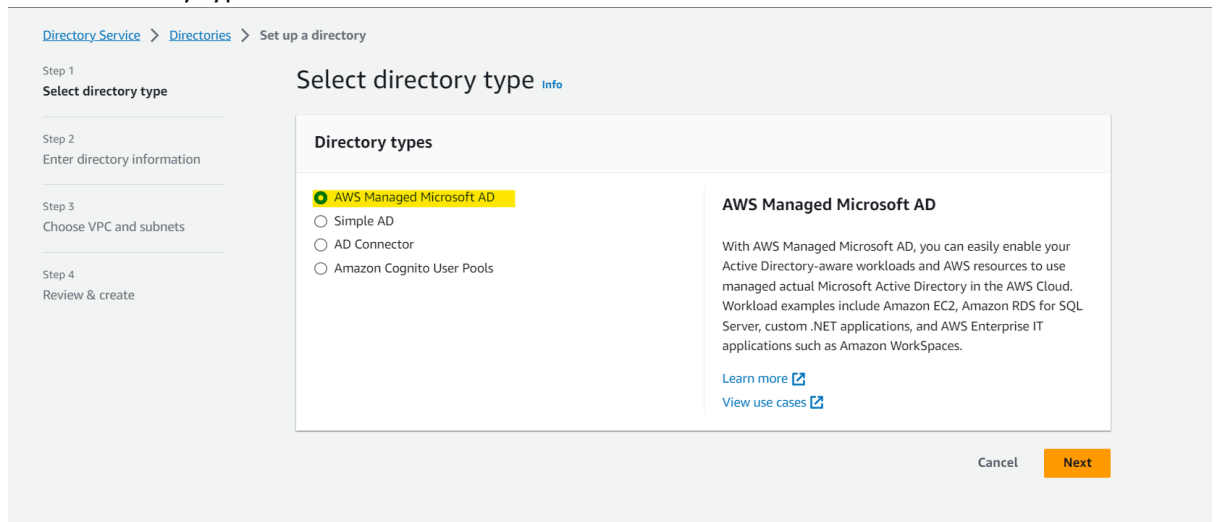
AWS Directory Service

- Create AWS Managed Microsoft AD



Click on Set up directory

- Select directory type



- Enter directory information

Step 2
Enter directory information
Step 3
Choose VPC and subnets
Step 4
Review & create

Directory information [Info](#)

A managed Microsoft Active Directory domain.

Directory type
Microsoft AD

Operating system version
Windows Server 2019

Edition [Info](#)
Microsoft AD is available in the following two editions:

☒ **Standard Edition**
Best for small to medium sized businesses.

- 1GB of storage for directory objects
- Optimized for up to 30,000 objects

~USD 86.4000/mo (USD 0.1200/hr)*
* Includes two domain controllers, USD 43.2000/mo for each additional domain controller.

☐ **Enterprise Edition**
Best for large businesses.

- 17GB of storage for directory objects
- Optimized for up to 500,000 objects

~USD 288.0000/mo (USD 0.4000/hr)*
* Includes two domain controllers, USD 144.0000/mo for each additional domain controller.

Directory DNS name
A fully qualified domain name. This name will resolve inside your VPC only. It does not need to be publicly resolvable.
FQDN such as "corp.example.com"

- Please fill in the following details and click on next

Directory DNS name

A fully qualified domain name. This name will resolve inside your VPC only. It does not need to be publicly resolvable.

Directory NetBIOS name - *optional*

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.

Maximum of 15 characters, can't contain spaces or the following characters: ` \ / : * ? " < > | ` . It must not start with ` .` .

Directory description - *optional*

Descriptive text that appears on the details page after the directory has been created.

Maximum of 128 characters, can only contain alphanumeric, and the following characters: ` _ @ # % * + = : ? . / ! \ - ` . It may not start with a special character.

Admin password

The password for the default administrative user named Admin.

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.

Confirm password

This password must match the Admin password above.


- Choose VPC and subnets
- Please select the Subnets in two zones or keep it as No preference


Choose VPC and subnets [Info](#)

Networking


The VPC that contains your directory. If you do not have a VPC with at least two subnets, you must create one.


VPC [Info](#)


vpc-08a00530d2770b20f (172.31.0.0/16) 

[Create new VPC](#) 

Subnets [Info](#)

No preference 

No preference 

[Create new subnet](#) 

Initial AD site name for this directory [Info](#)

Default-First-Site-Name

[Cancel](#) [Previous](#) [Next](#)


- Review & create

Step 4

Review & create

<p>Windows Server 2019</p> <p>Directory DNS name aatish.cloud</p> <p>Directory NetBIOS name aatish</p> <p>Directory description -</p>	<p>subnet-02c335b2b09febba2 (172.31.0.0/20, us-east-1c) subnet-06a37a952f3c5271e (172.31.16.0/20, us-east-1a)</p>
---	---

Pricing

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

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

- It will take 30 mins to set up the Directory

Directories (1) [Info](#)

Find by directory ID or name

< 1 > ⚙

Directory ID

Directory name

Type

Size

Multi-Region

Status

Launch date

○

d-906783f59e

aatish.cloud

Microsoft AD

Standard

Not applicable

🔄 Creating

Sep 3, 2023

- Create a EC2 Instance with Windows-Server 2019
- Click on Launch instance

New EC2 Experience Tell us what you think ×

EC2 Dashboard

EC2 Global View

Events

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

▼ Images

AMIs

AMI Catalog

▼ Elastic Block Store

Volumes

Resources

EC2 Global view [↗](#) ⚙ 🔄

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running) 0

Auto Scaling Groups 0

Dedicated Hosts 0

Elastic IPs 0

Instances 0

Key pairs 0

Load balancers 0

Placement groups 0

Security groups 2

Snapshots 0

Volumes 0

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▼

Migrate a server [↗](#)

Note: Your instances will launch in the US East (N. Virginia) Region

Service health

AWS Health Dashboard [↗](#) 🔄

Region

US East (N. Virginia)

Zones

Zone name

Zone ID

- Select Microsoft Windows

EC2 > Instances > Launch an instance

Launch an instance

Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Info

Name

Windows-Server

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

Q Search our full catalog including 1000s of application and OS images

Quick Start

Amazon Linux

aws

macOS

Mac

Ubuntu

ubuntu

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUS

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

▼ Summary

Number of instances

Info

1

Software Image (AMI)

Microsoft Windows Server 2022 ...read more

ami-09301a37d119fe4c5

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 30 GiB

Cancel

Launch instance

Review commands

- If you have a free tier account then always go with the free tier eligible option

Amazon Machine Image (AMI)

Microsoft Windows Server 2019 Base

Free tier eligible

ami-065b889ab5c33720e (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

Q |

Microsoft Windows Server 2022 Base

Free tier eligible

ami-09301a37d119fe4c5 (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

Microsoft Windows Server 2022 Core Base

Free tier eligible

ami-010394ab667fbb251 (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

Microsoft Windows Server 2019 Base

Free tier eligible

ami-065b889ab5c33720e (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

Microsoft Windows Server 2019 Core Base

Free tier eligible

ami-0b45099cfda802d86 (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

Microsoft Windows Server 2016 Base

Free tier eligible

ami-0eaa5dc91b7f6a340 (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

Microsoft Windows Server 2016 Core Base

Free tier eligible

ami-022248de413e8cf73 (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

Microsoft Windows Server 2022 with SQL Server 2022 Standard

Free tier eligible

ami-076afa65fdcae2a27 (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

- Create a .Pem key for Secure login

Create key pair ✕

Key pair name
Key pairs allow you to connect to your instance securely.

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type



☒ **RSA**
RSA encrypted private and public key pair

☐ **ED25519**
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

☒ **.pem**
For use with OpenSSH

☐ **.ppk**
For use with PuTTY

 When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#) 

Cancel Create key pair

- Please Allow RDP Traffic, HTTP, HTTPS

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

We'll create a new security group called 'launch-wizard-1' with the following rules:

☒ **Allow RDP traffic from**
Helps you connect to your instance


☒ **Allow HTTPS traffic from the internet.**
To set up an endpoint, for example when creating a web server

☒ **Allow HTTP traffic from the internet.**
To set up an endpoint, for example when creating a web server

 Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ✕

▼ 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 ✕

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

▼ Summary

Number of instances Info

Software Image (AMI)
Microsoft Windows Server 2019 ...[read more](#)
ami-065b889ab5c33720e

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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

Cancel Launch instance
[Review commands](#)

- Once you have selected the required options, please check on launch Instance

☒ Create security group
 ☐ Select existing security group

We'll create a new security group called 'launch-wizard-2' with the following rules:

- ☒ Allow SSH traffic from Anywhere 0.0.0.0/0
- ☒ Allow HTTPS traffic from the internet
- ☒ Allow HTTP traffic from the internet

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

▼ 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](#)

0 x File systems [Edit](#)

▼ Summary

Number of instances [Info](#)

1

[Software Image \(AMI\)](#)

Amazon Linux 2023 AMI 2023.1.2...[read more](#)

ami-051f7e7f6c2f40dc1

[Virtual server type \(instance type\)](#)

t2.micro

[Firewall \(security group\)](#)

New security group

[Storage \(volumes\)](#)

1 volume(s) - 8 GiB

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

► Advanced details [Info](#)

- Steps to login with Remote Desktop Connection
- Collect the Public IP, User Name, And Generate the Password using .Pemkey
- Copy the Public IP and click on Connect
-

EC2 > Instances > i-08081f4dc48247445		
Instance summary for i-08081f4dc48247445 (Windows-Server) Info		
Updated less than a minute ago		
<div> <div> <div>Instance ID</div> <div>i-08081f4dc48247445 (Windows-Server)</div> </div> <div> <div>IPv6 address</div> <div>–</div> </div> <div> <div>Hostname type</div> <div>IP name: ip-172-31-46-81.ec2.internal</div> </div> <div> <div>Answer private resource DNS name</div> <div>IPv4 (A)</div> </div> <div> <div>Auto-assigned IP address</div> <div>54.198.154.160 [Public IP]</div> </div> <div> <div>IAM Role</div> <div>–</div> </div> <div> <div>IMDSv2</div> <div>Optional</div> </div> </div> <div> <div>Public IPv4 address</div> <div>54.198.154.160 open address</div> <div>Instance state</div> <div>Running</div> <div>Private IP DNS name (IPv4 only)</div> <div>ip-172-31-46-81.ec2.internal</div> <div>Instance type</div> <div>t2.micro</div> <div>VPC ID</div> <div>vpc-08a00530d2770b20f</div> <div>Subnet ID</div> <div>subnet-0fd9d43b5550e6fb0</div> </div> <div> <div>Private IPv4 addresses</div> <div>172.31.46.81</div> <div>Public IPv4 DNS</div> <div>ec2-54-198-154-160.compute-1.amazonaws.com open address</div> <div>Elastic IP addresses</div> <div>–</div> <div>AWS Compute Optimizer finding</div> <div>Opt-in to AWS Compute Optimizer for recommendations. Learn more</div> <div>Auto Scaling Group name</div> <div>–</div> </div>		
<div> <div>Refresh</div> <div>Connect</div> <div>Instance state ▼</div> <div>Actions ▼</div> </div>		

- Click on RDP Client
- Copy the User Name
- Click on Get password and Upload the Pem-key
- Once you upload the Key, Click on Decrypt Password

EC2 > Instances > i-08081f4dc48247445 > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-08081f4dc48247445 (Windows-Server) using any of these options

Session Manager | **RDP client** | EC2 serial console

Instance ID
i-08081f4dc48247445 (Windows-Server)

Connection Type

☒ **Connect using RDP client**
Download a file to use with your RDP client and retrieve your password.

☐ **Connect using Fleet Manager**
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[Download remote desktop file](#)

When prompted, connect to your instance using the following details:

Public DNS
ec2-54-198-154-160.compute-1.amazonaws.com

User name
Administrator

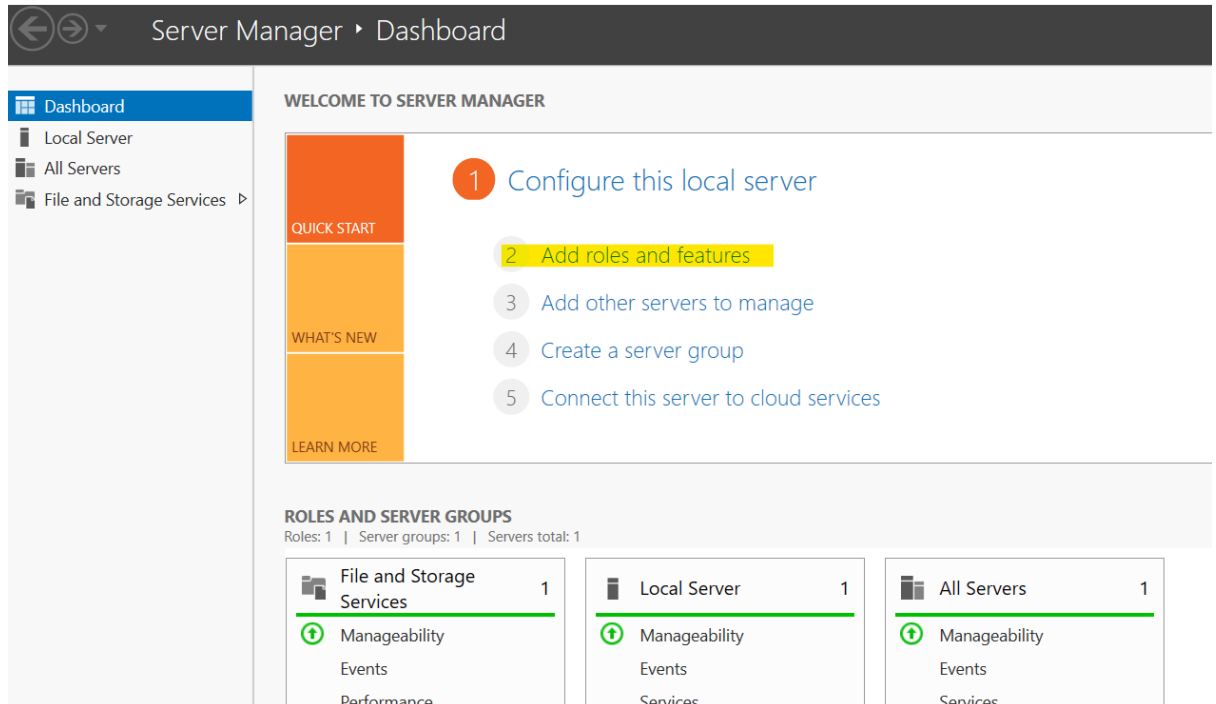
Password [Get password](#)

Info If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

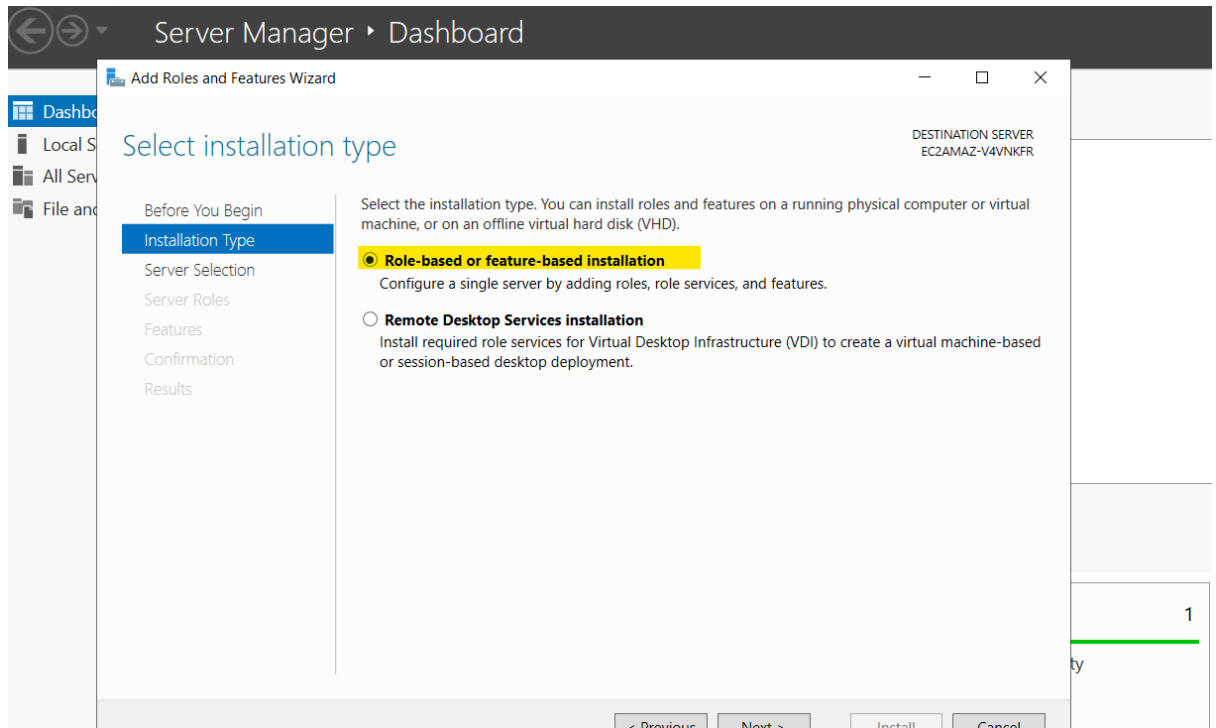
- Login using RDP

The screenshot shows the AWS Management Console interface for connecting to an EC2 instance. The 'Connect to instance' page is displayed, with the 'RDP client' tab selected. The instance ID is i-08081f4dc48247445 (Windows-Server). The 'Download remote desktop file' button is visible. The 'User name' is 'Administrator'. The 'Get password' button is highlighted. A 'Remote Desktop Connection' dialog box is open, showing the 'Computer' field with the IP address '54.198.154.160' and the 'User name' field with 'Administrator'. The 'Connect' button is highlighted.

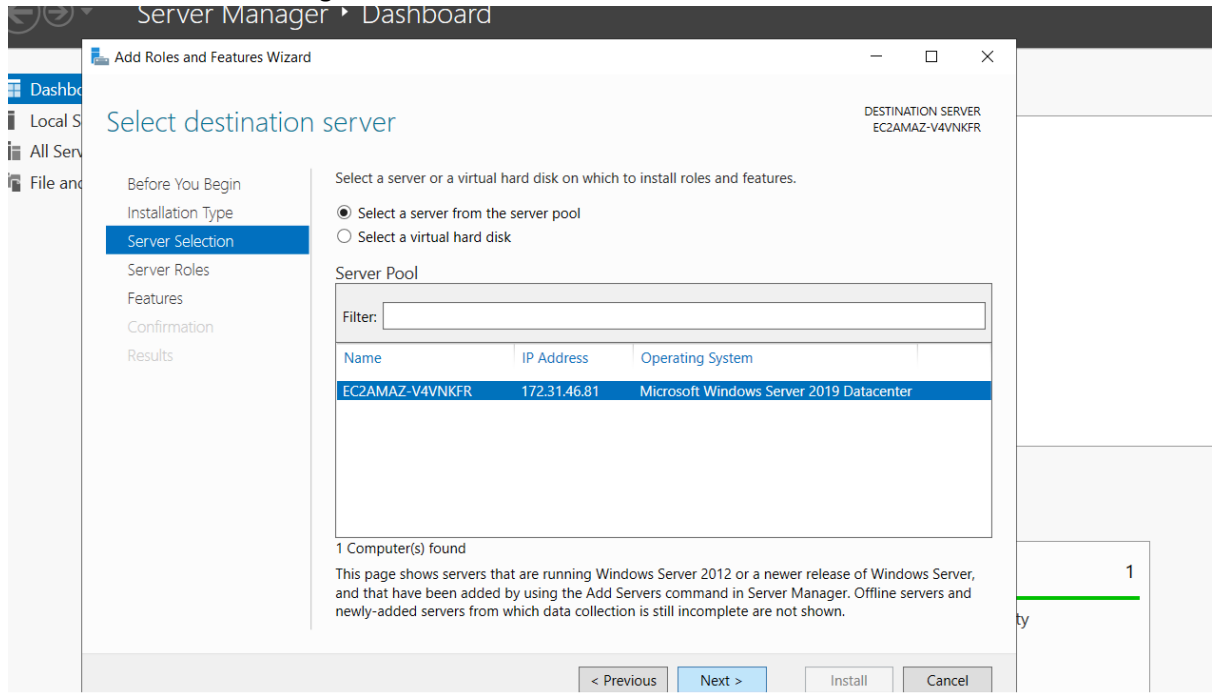
- Once you log in, go to server manager and click on add roles and features



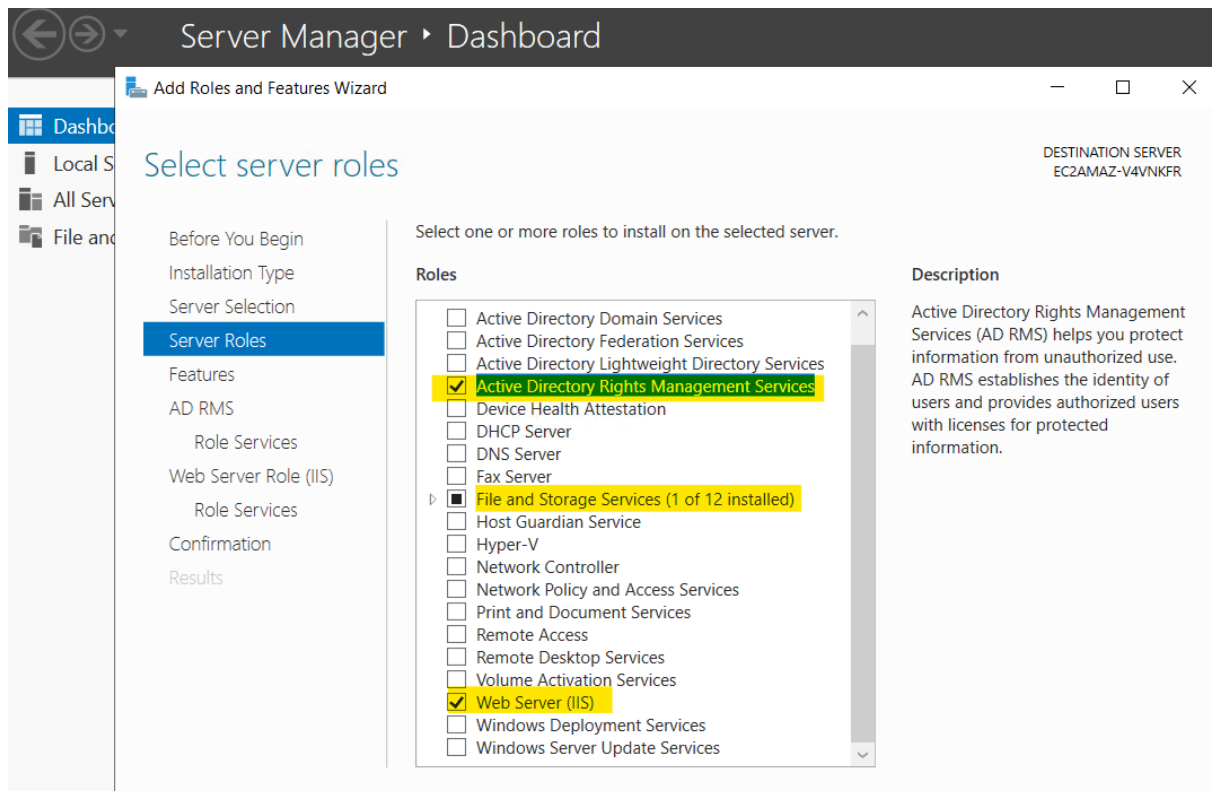
- Start the Installation



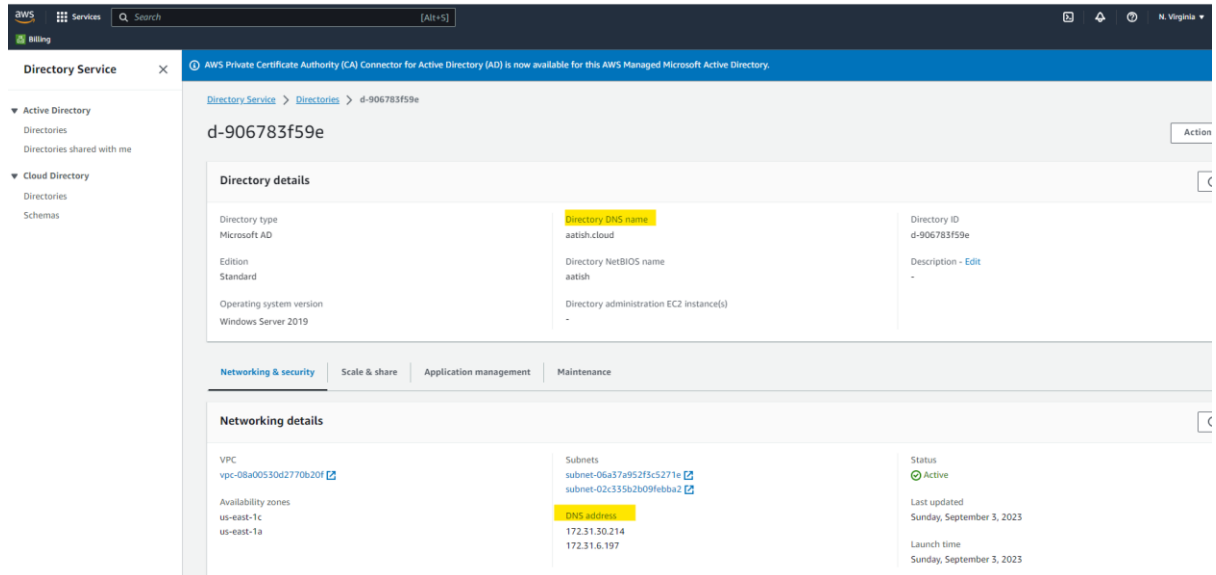
- Go with the Default Settings for Server Selection



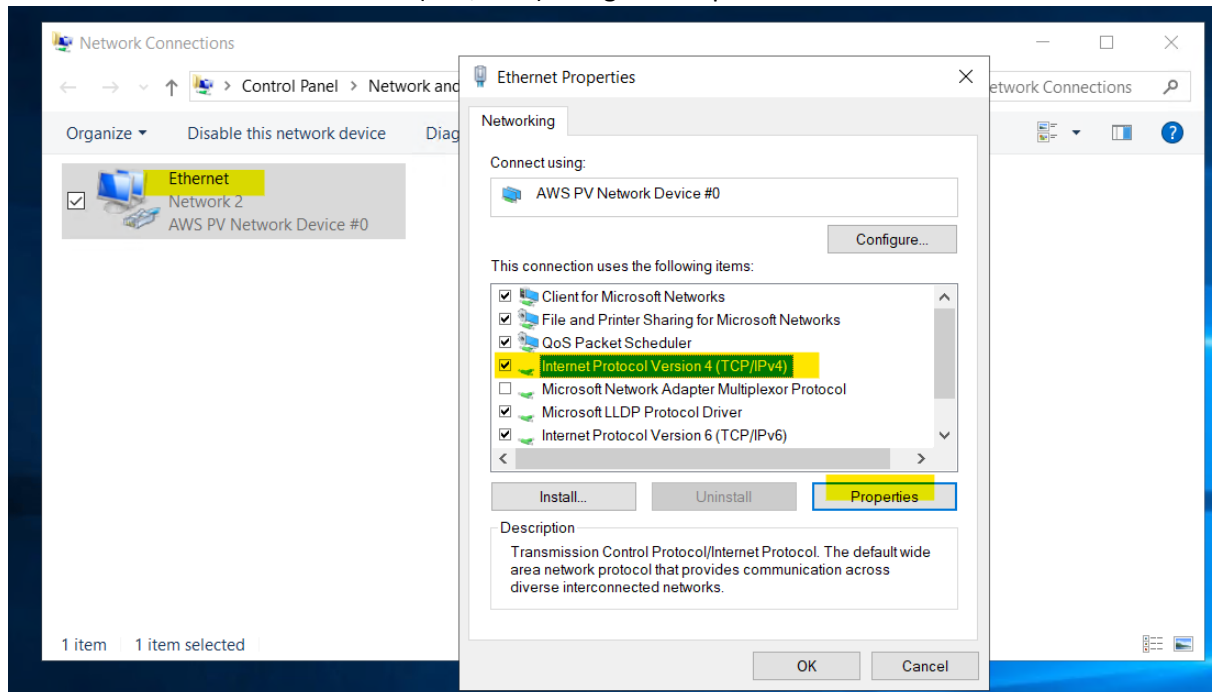
- Server Roles



- Double Click on roles administration and Select AD DS And AD LDS tools
- Please click on Next and keep the default settings and Install
- Link the Server with the AWS managed Active Directory Service
- Collect the DNS Name And the DNS IP



- Add the DNS IP using ncpa.cpl using Run function
- Right click on Ethernet and go properties
- Select Internet Protocol Version 4 (TCP/IPv4) and go to Properties



- Select Use DNS Server IP From AWS Directory Service
- And Save/Ok

Internet Protocol Version 4 (TCP/IPv4) Properties [X]

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: [172 . 31 . 30 . 214]

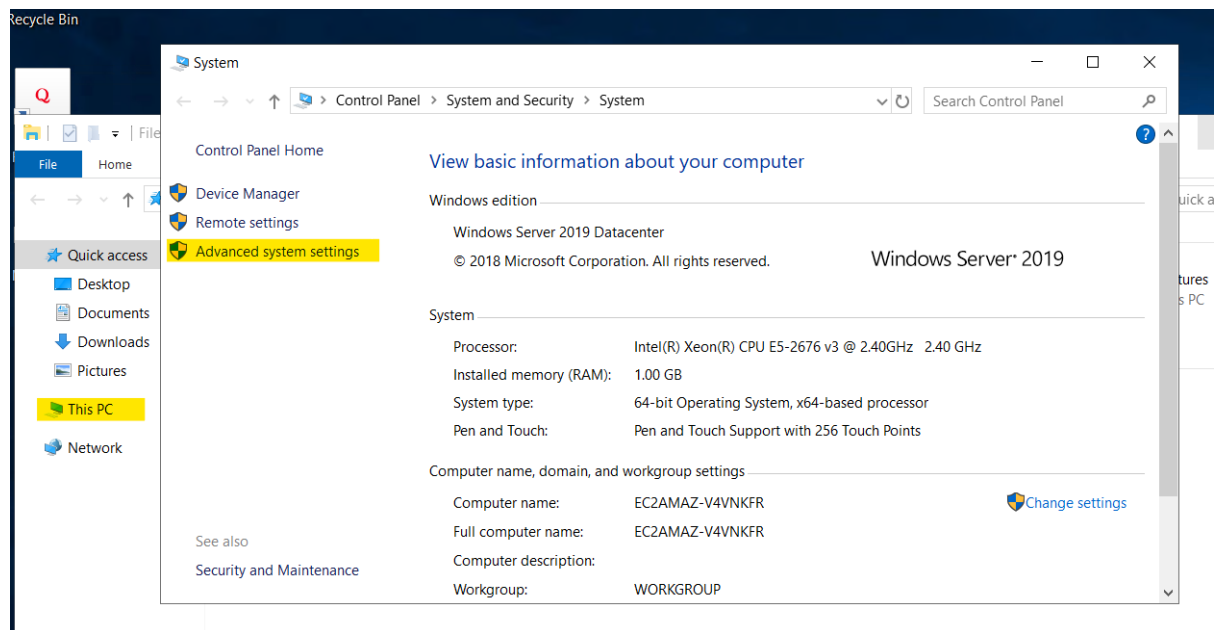
Alternate DNS server: [172 . 31 . 6 . 197]

☐ Validate settings upon exit

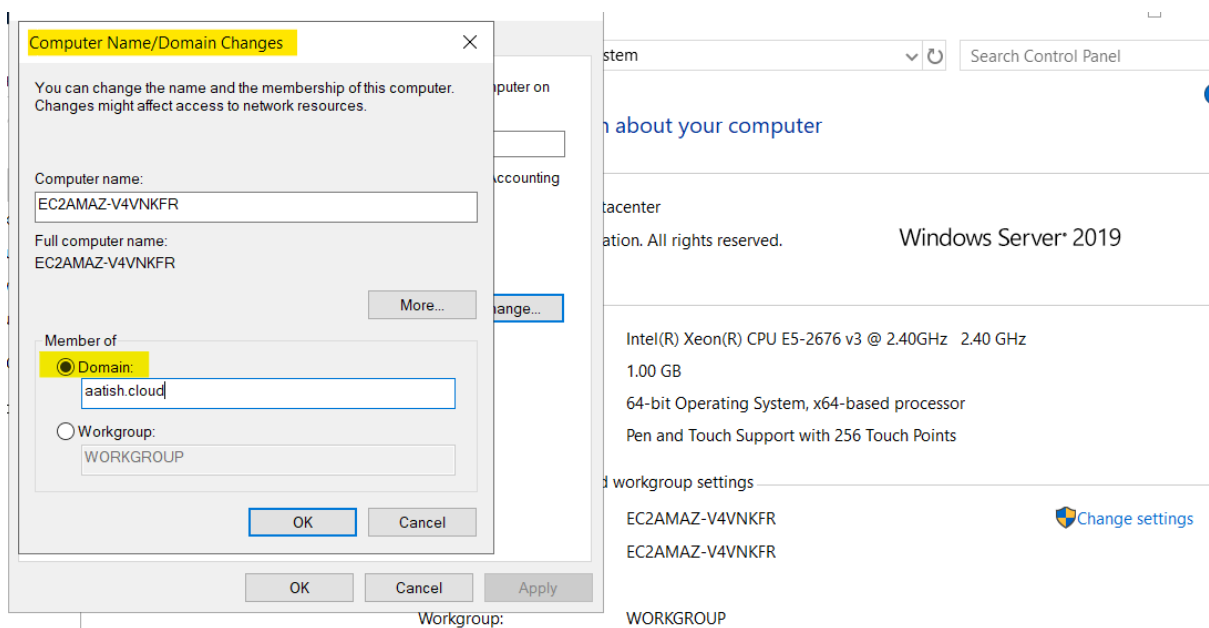
[Advanced...]

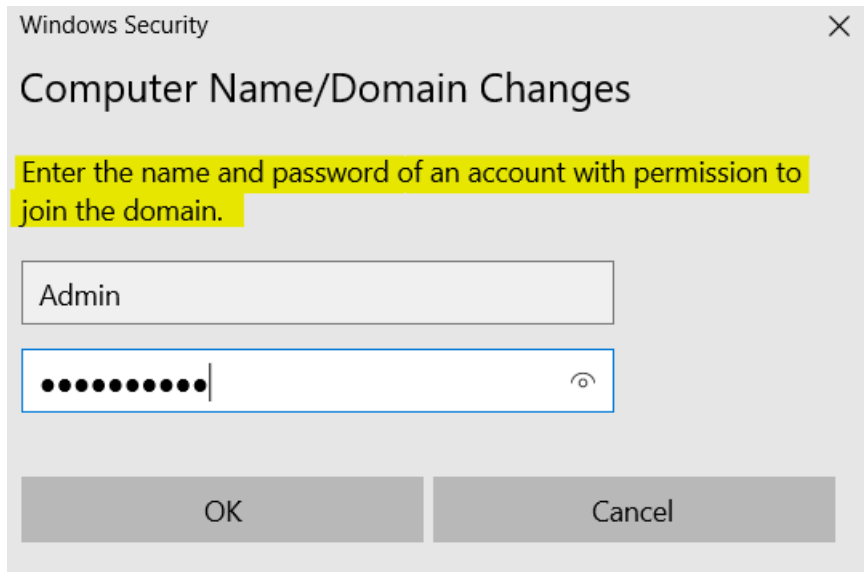
[OK] [Cancel]

- Go to Files Explorer and Right Click on This PC
- Click on properties
- Click on Advance Settings

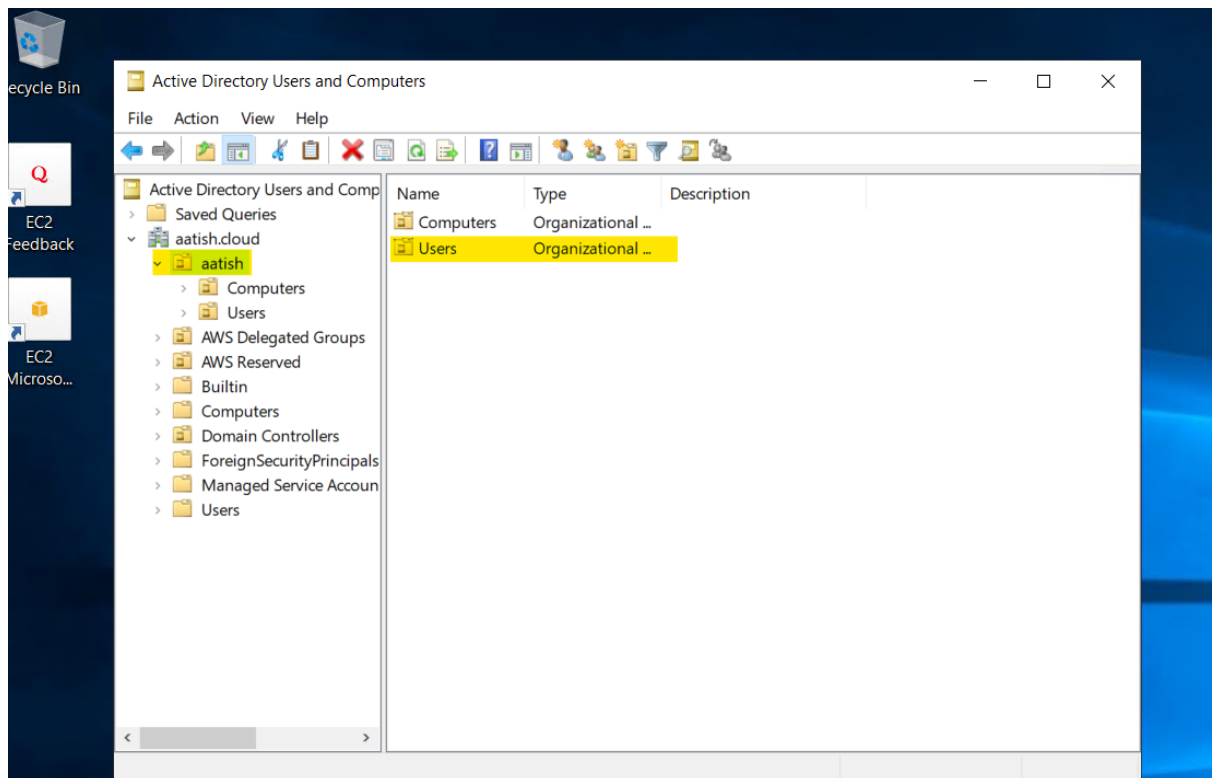


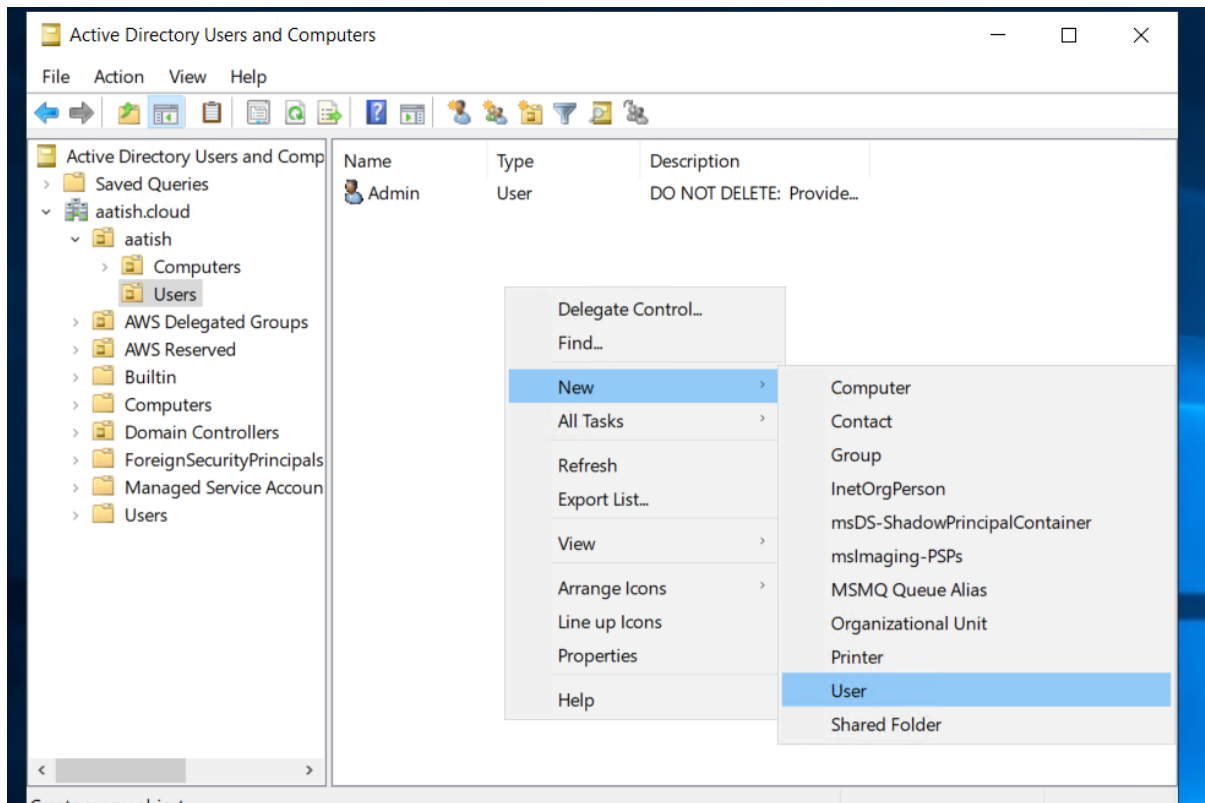
- System Properties will be opened
- Click on Computer Name
- Change the Domain Name same as your AWS Directory Service Name and Save
- And Please Enter the Admin Password Which was created When Creating the Directory Service on AWS
- Once you have Successfully Changed the Domain Name, the System will Restart





- Now Please Login as Admin@domain.com
- Create User (dsa.msc)
- Create Two User EC2-User and S3-User





New Object - User



Create in: aatish.cloud/aatish/Users

First name: EC2-User Initials:

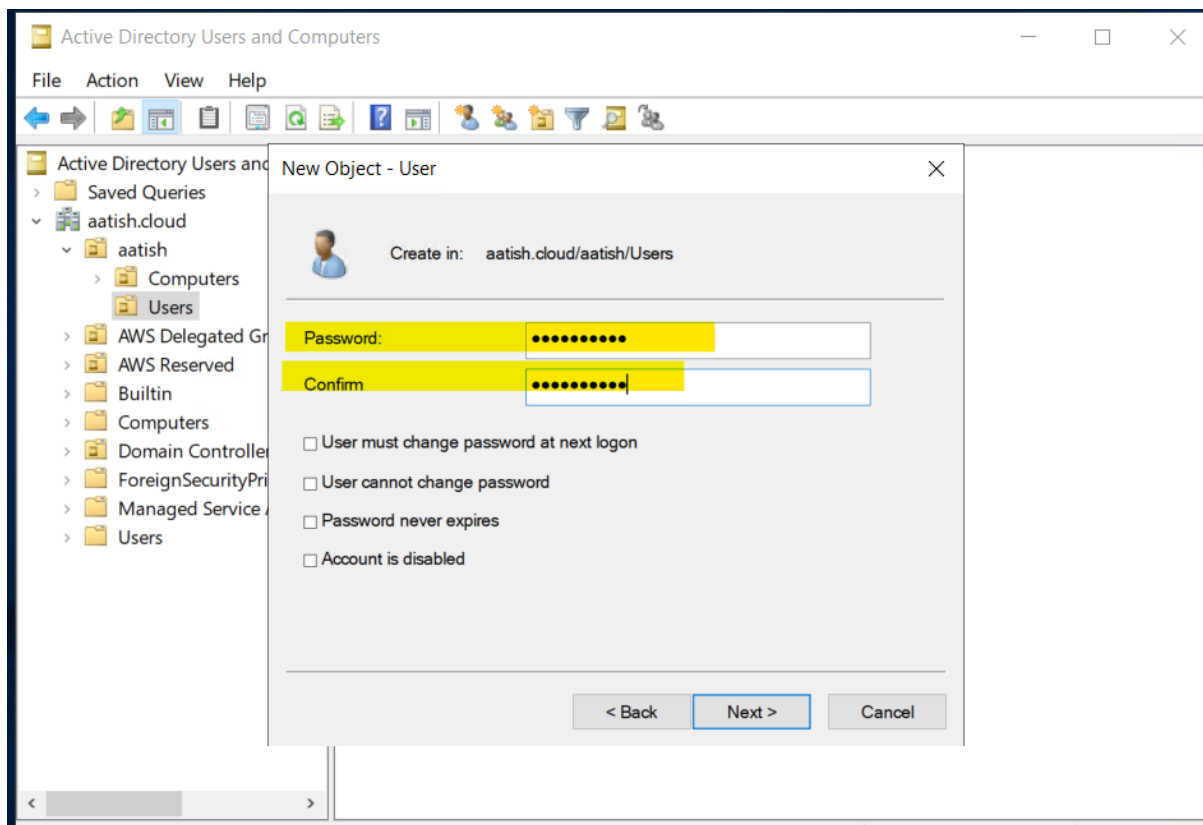
Last name:

Full name: EC2-User

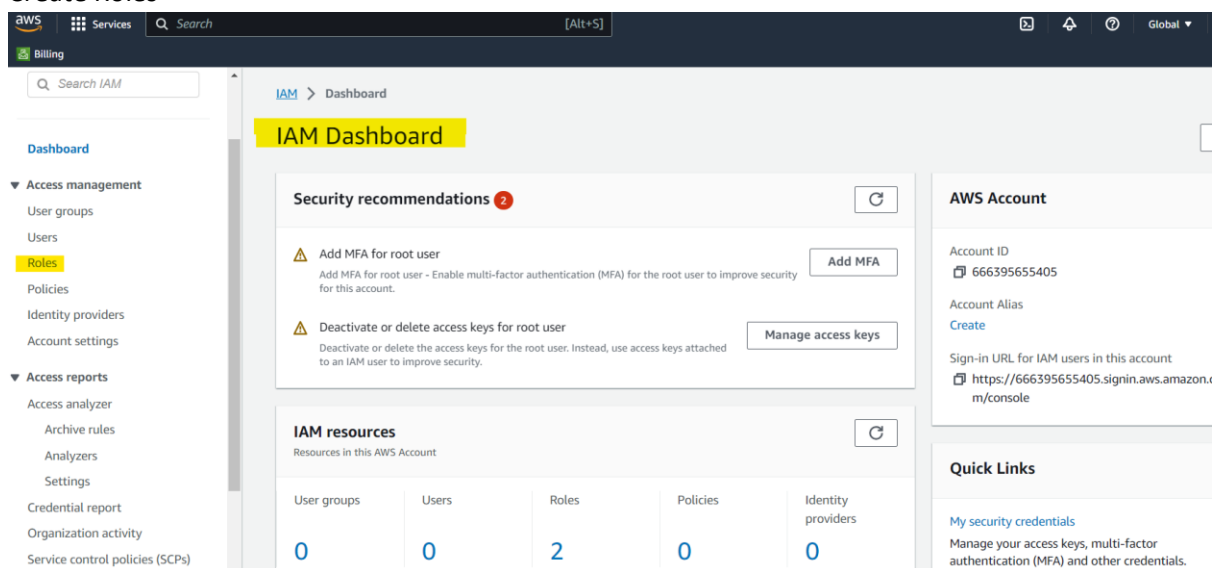
User logon name: EC2 @aatish.cloud

User logon name (pre-Windows 2000): aatish\ EC2

< Back Next > Cancel



- Go inside AWS Console And Search for IAM
- Create Roles



- Click on create roles

Identity and Access Management (IAM)

Q Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access analyzer

Archive rules

Analizers

Settings

IAM > Roles

Roles (2) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Q Search

<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same

X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

- Create a Role for AWS Directory Services

IAM > Roles > Create role

Step 1

Select trusted entity

Step 2

Add permissions

Step 3

Name, review, and create

Select trusted entity Info

Trusted entity type

☒ AWS service

Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ AWS account

Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ Web identity

Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ SAML 2.0 federation

Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

☐ EC2

Allows EC2 instances to call AWS services on your behalf.

☐ Lambda

Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:

Directory Service

☒ Directory Service

Allows Directory service to manage AWS service access for existing directory users and groups.

Cancel

Next

- Select the Roles as EC2 Full Access
- Name, review, and create

Role name
Enter a name for the role to identify this role.
EC2(FullAccess)
Maximum 64 characters. Use alphanumeric and "+,=,_,@,_" characters.

Description
Add a short explanation for this role.
Allows Directory Service to manage AWS service access for existing directory users and groups.
Maximum 1000 characters. Use alphanumeric and "+,=,_,@,_" characters.

Step 1: Select trusted entities Edit

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "sts:AssumeRole"
8       ],
9       "Principal": {
10        "Service": [
11          "ds.amazonaws.com"
12        ]
13      }
14    ]
15  }
16 }
```

Step 2: Add permissions Edit

Permissions policy summary

Policy name (2)	Type	Attached as
AmazonEC2FullAccess	AWS managed	Permissions policy

Tags

Add tags - optional [info](#)
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add tag
You can add up to 50 more tags.

Cancel Previous Create role

- The roles Should reflect on the Dashboard

[IAM](#) > Roles

Roles (4) [info](#)

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

< 1 > ⚙

<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
<input checked="" type="checkbox"/>	EC2@Role	AWS Service: ds	-
<input checked="" type="checkbox"/>	S3-FullAccess	AWS Service: ds	-

- Assign the roles to the users created
- Go to directory Services (dashboard)
- Click on your Directory and go to Application Management
- Scroll Down to Delegate console access

Networking & security
Scale & share
Application management
Maintenance

Application access URL [Info](#)

The public endpoint URL where users in this directory can gain access to your AWS applications and to your AWS Management Console.

Access URL:
aatish.awsapps.com

Amazon WorkDocs single sign-on [Info](#)

Enable

AWS apps & services [Info](#)

Lists all AWS applications and services that are available to users in this directory, and to users in any shared directories, who log in using the Application access URL above.

Application	Status	URL to application
Amazon Aurora MySQL ↗	⊖ Disabled	-
Amazon Aurora PostgreSQL ↗	⊖ Disabled	-
Amazon Chime ↗	⊖ Disabled	-

- Click on the Role and assign the roles to the users
- Assign one role to each user

AWS Management Console [Info](#)

Actions ▼

Provides delegated users in this directory and in shared directories who log in using the application access URL above with access to your resources in the AWS Management Console.

Status
✔ Enabled

User login session length [Info](#)
1 hour

Delegate console access (2) [Info](#)

↻

You can delegate which users and groups have access to certain areas of the console by adding them to the applicable IAM roles below. To get started, choose a role.

Find by role

< 1 >

IAM role ▲	Console permissions	Delegated users ▼	Delegated groups ▼
EC2@Role	View policy in IAM ↗	0	0
S3-FullAccess	View policy in IAM ↗	0	0

- Click on Add and assign the role

Directory Service > Directories > d-906783f59e > AWS Management Console

Selected role: EC2@Role

IAM role	ARN	Permissions	Delegated users	Delegated groups
EC2@Role	arn:aws:iam::666395655405:role/EC2@Role	View policy in IAM	0	0

Manage users and groups for this role (0) [Info](#)

The domain users and groups listed here inherit the permissions assigned to this IAM role.

< 1 >

Name	Full name	Domain name	Type	Security identifier (SID)
No users or groups have been assigned to this IAM role. To get started, click Add.				

[Add](#)

Add users and groups to the EC2@Role role ✕

IAM role
EC2@Role

Select Active Directory forest
Lists this Microsoft AD forest and any existing forests (trusted forests) that have an established trust with it.

Specify which users or groups to add

☒ Find by user
☐ Find by group

1 match

Name	Full name	Domain name	Type	Security identifier (SID)
<input checked="" type="checkbox"/> EC2	EC2-User	aatish.cloud	User	S-1-S-21-2478324409-2169176866-945533455-1146

[Cancel](#) [Add](#)

- Click on Application management and Enable Console login to user
- Copy the AWS console URL and check by logging in using your User Credentials

AWS Client VPN	⊖ Disabled	-
AWS License Manager	⊖ Disabled	-
AWS Management Console	⊕ Enabled	aatish.awsapps.com/console
AWS Transfer Family	⊖ Disabled	-
IAM Identity Center	⊖ Disabled	aatish.awsapps.com/start

AWS Management Console [Info](#) [Actions](#)

Provides delegated users in this directory and in shared directories who log in using the application access URL above with access to your resources in the AWS Management Console.

Status	User login session length Info
⊕ Enabled	1 hour