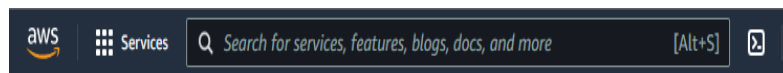


Assignment 1:

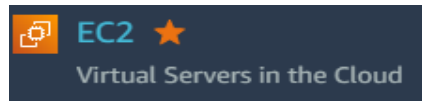
Create a VM with t2.micro instance template. Ensure the following:

- Recreate a new key
- Convert the key to private key compatible for putty
- Convert the key to private key compatible for Winscp
- Access the machine using Putty and WinSCP and load data using WinSCP
- Ensure you attach the Administrator role to the VM.

1. Search “ec2” in



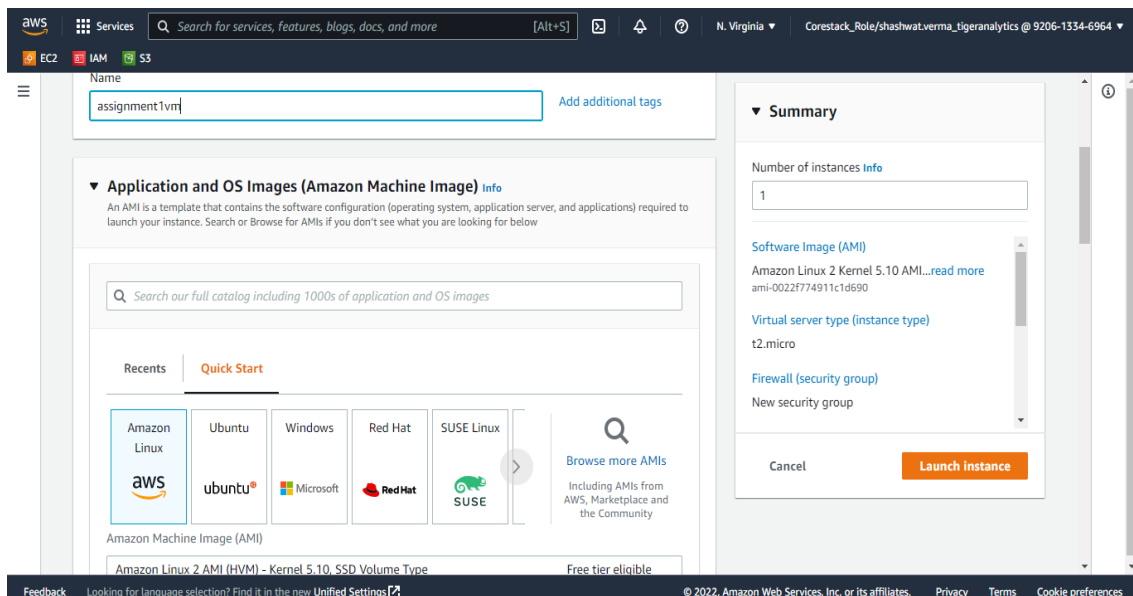
2. Click on



3. Click on



4. Make the following selections:



Selected Instance: "t2.micro"

The screenshot shows the AWS Management Console interface for launching a new instance. The top navigation bar includes the AWS logo, 'Services' menu, a search bar, and user information for 'Corestack_Role/shashwat.verma_tigeranalytics @ 9206-1334-6964'. The main content area is divided into two columns. The left column shows the selected AMI: 'Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type' with AMI ID 'ami-0022f774911c1d690'. Below this, the 'Instance type' section shows 't2.micro' selected, with details: Family: t2, 1 vCPU, 1 GiB Memory, and pricing information. The right column is the 'Summary' section, showing 'Number of instances' as 1, 'Software Image (AMI)' as the selected Amazon Linux 2 AMI, 'Virtual server type (instance type)' as t2.micro, and 'Firewall (security group)' as 'New security group'. At the bottom of the summary are 'Cancel' and 'Launch Instance' buttons.

a. Recreate a new key

1. Click on "Create new key pair", then name the key as shown:

This screenshot shows the 'Key pair (login)' section of the AWS console. It contains a heading 'Key pair (login) Info' and a paragraph explaining that a key pair is used to securely connect to the instance. Below this, there is a section for 'Key pair name - required' with a dropdown menu currently showing 'Select' and a 'Create new key pair' button highlighted in yellow.

Enter details as:

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. 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](#)

Key pair name

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

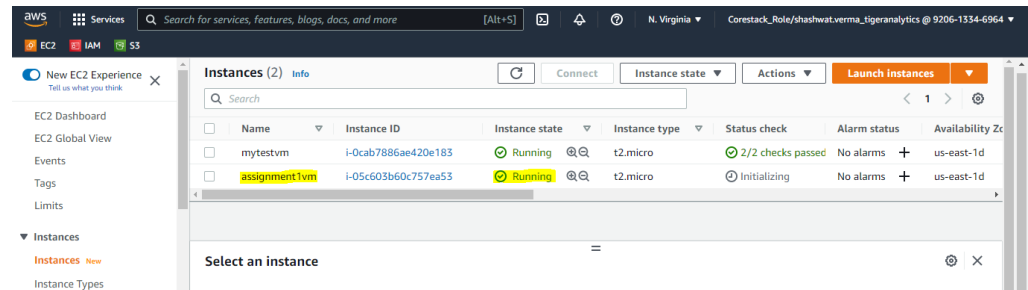
- ☒ .pem
For use with OpenSSH
- ☐ .ppk
For use with PuTTY

Cancel [Create key pair](#)

2. Once you hit “Create key pair” a key file with “.pem” extension gets downloaded. Preserve this file safely as it cannot be recreated afterwards.

Now hit “Launch Instance” (shown in Step 4 snip 2).

Go to EC2>>Instances



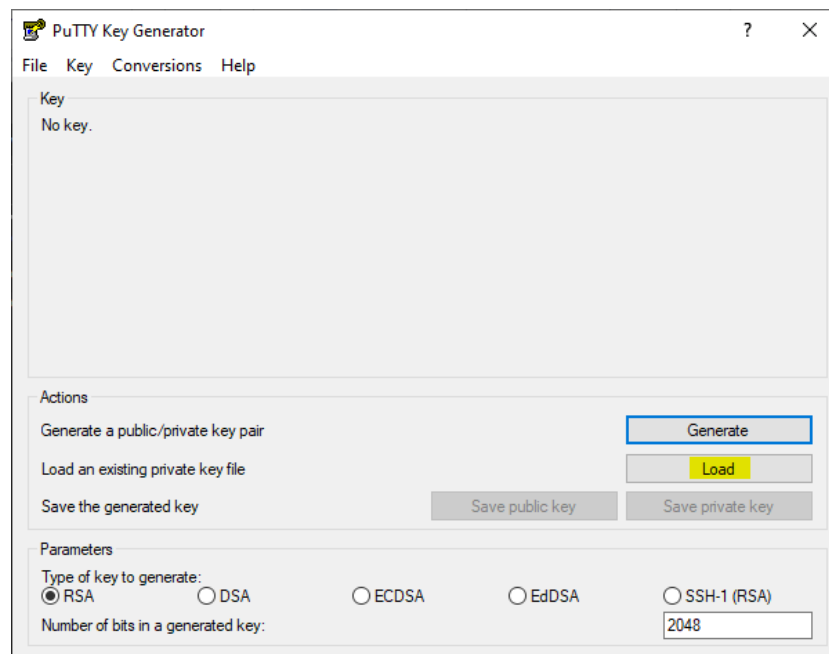
We will find that the instance launched successfully and is in Running state.

- b. Convert the key to private key compatible for putty

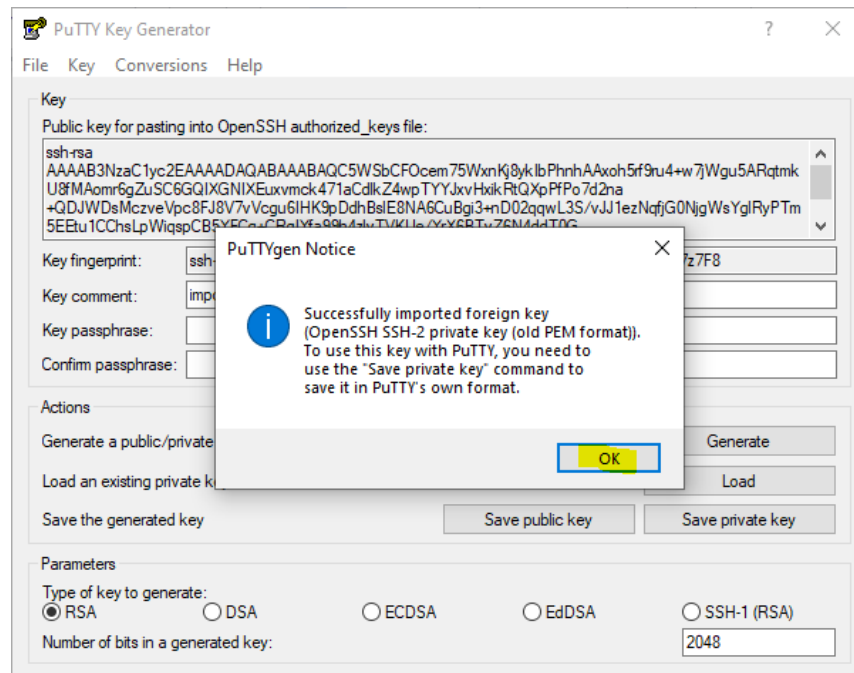
Stored the key downloaded in a new folder “AWS_Assignment1”.

We used “PUTTYGEN” application to convert the pem key to ppk key

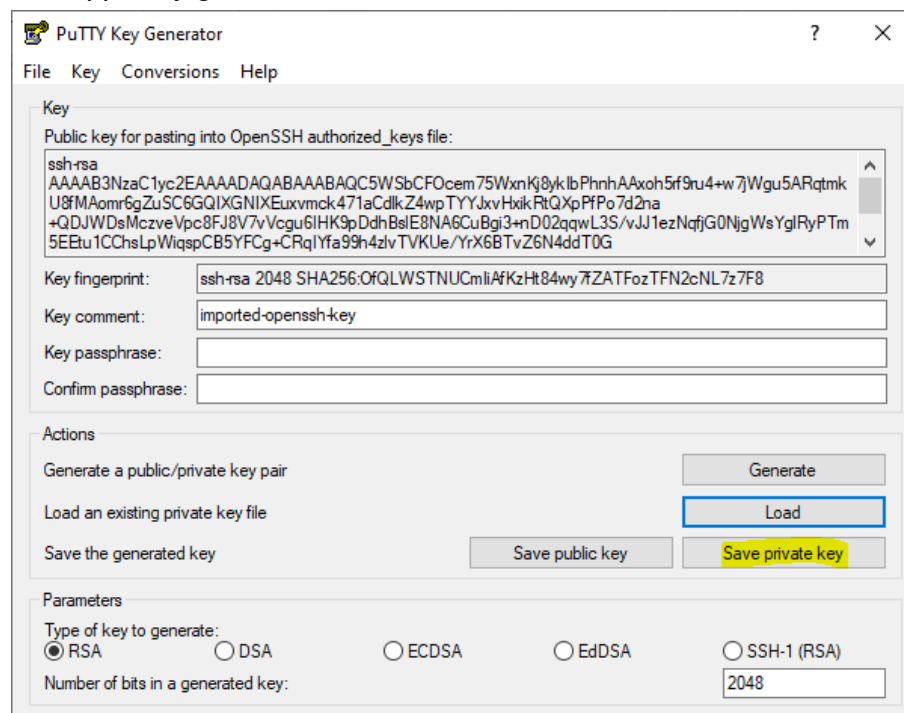
1. Launch “PUTTYGEN”, then click on “Load”



2. Browse and select the downloaded key pair file. Please select "All Files (*.*)" format to find the .pem file then hit "Open". Once "Successfully imported foreign key..." message appears hit "OK"

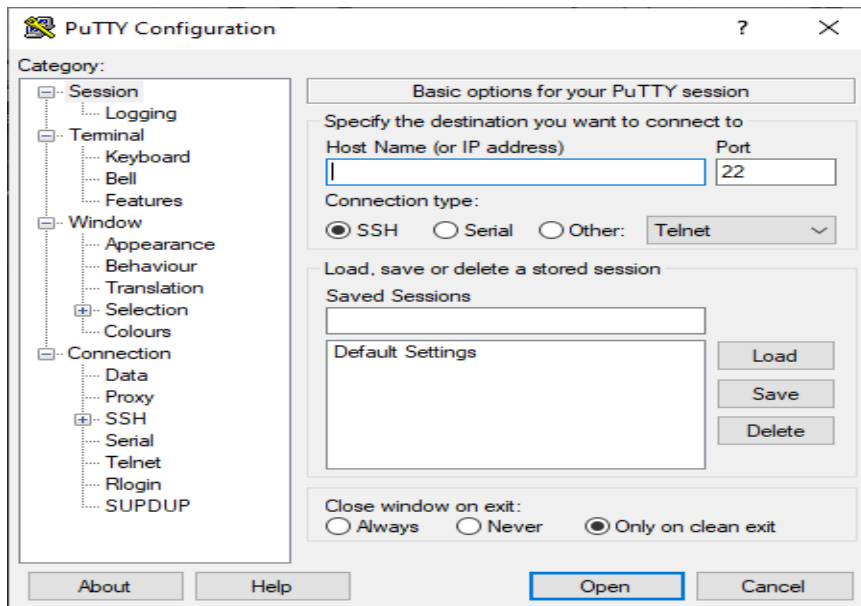


3. Hit on "Save private key" and click on "OK" for the alert message, Assign a name to the ppk key generated.

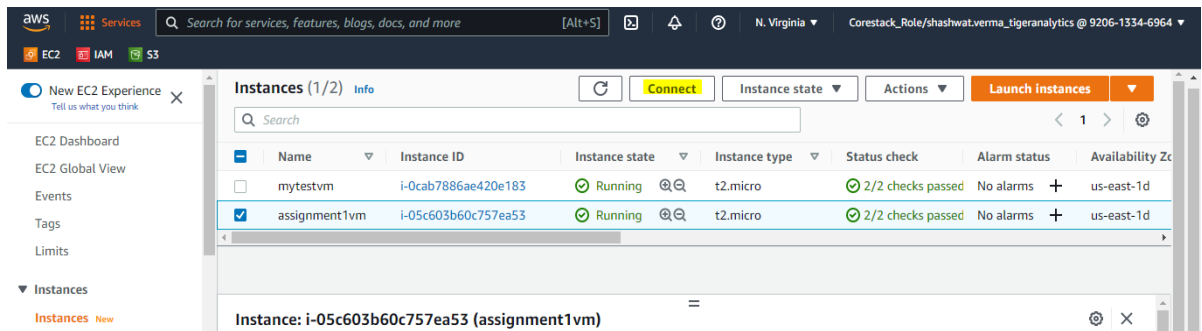


PuTTY:

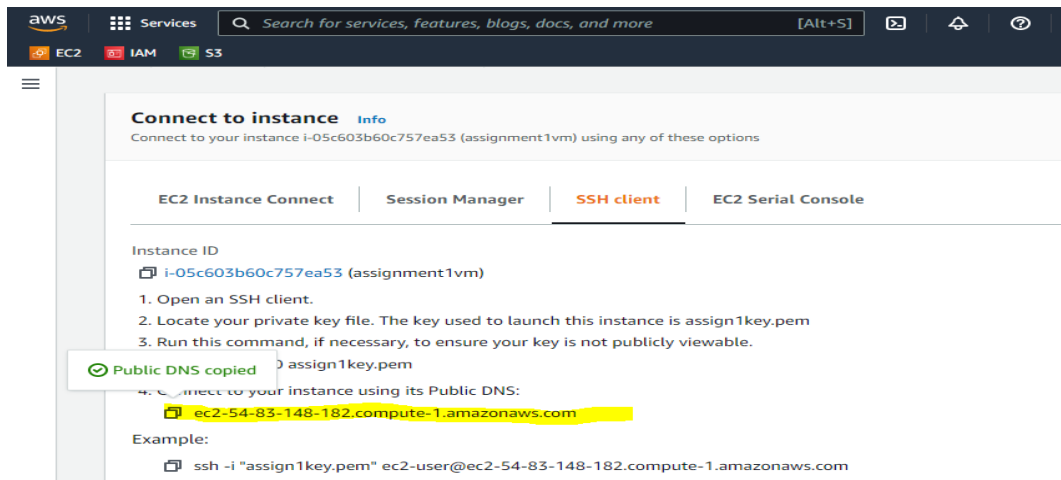
c&d. 1. Launch "PuTTY" application



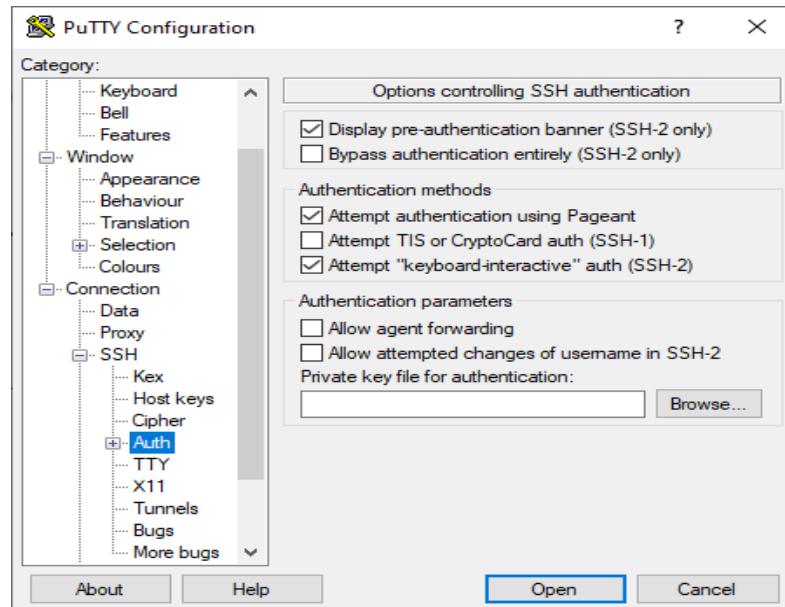
2. Copy Host Name from the VM we created by clicking on Connect >> SSH Client



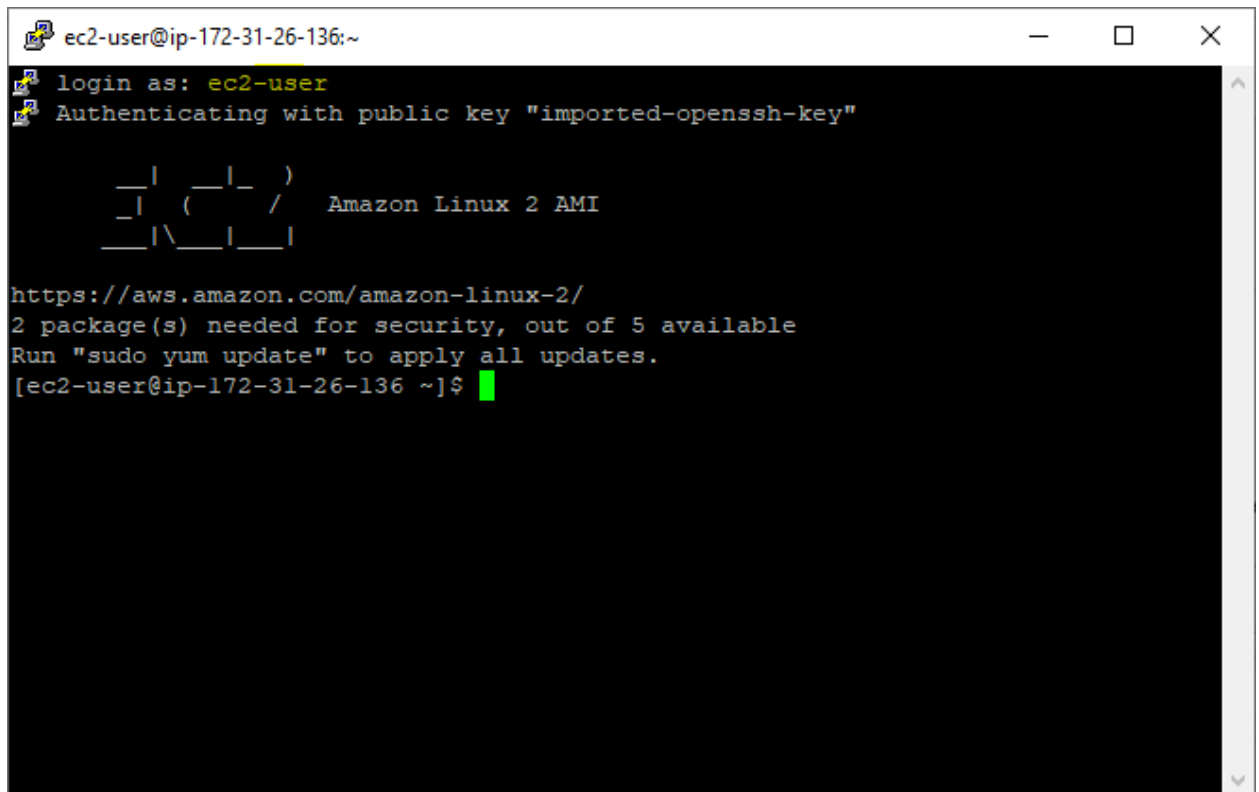
3. Copy Public DNS >> Paste this to PuTTY>> Host name



4. Click on SSH >> Auth in PuTTY application, the browse for the ppk key created above, then hit "Open".

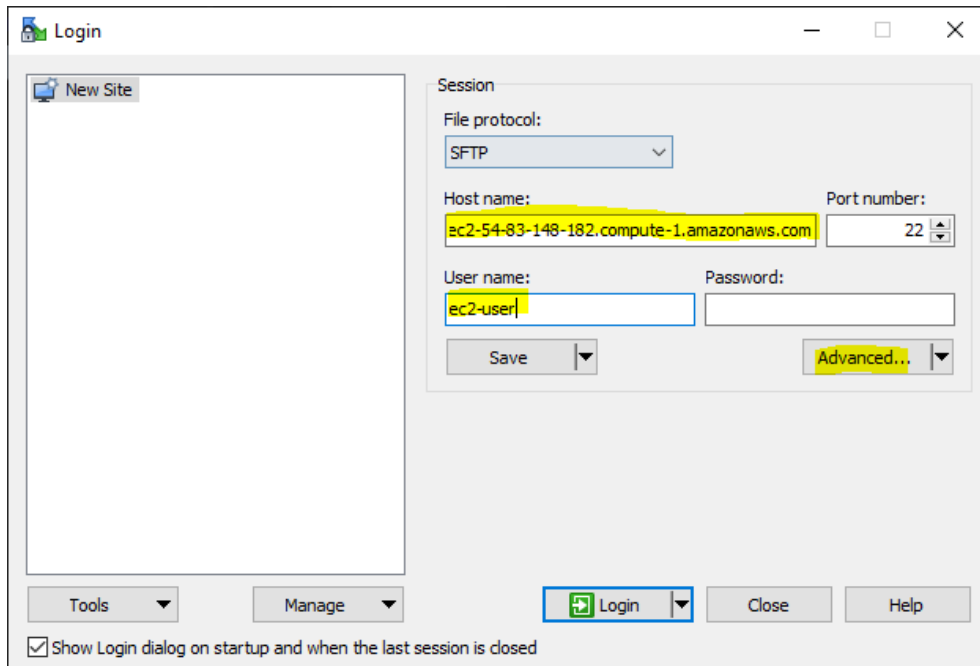


5. "Accept" the PuTTY Security alert popup and login as "ec2-user" to launch VM as shown:

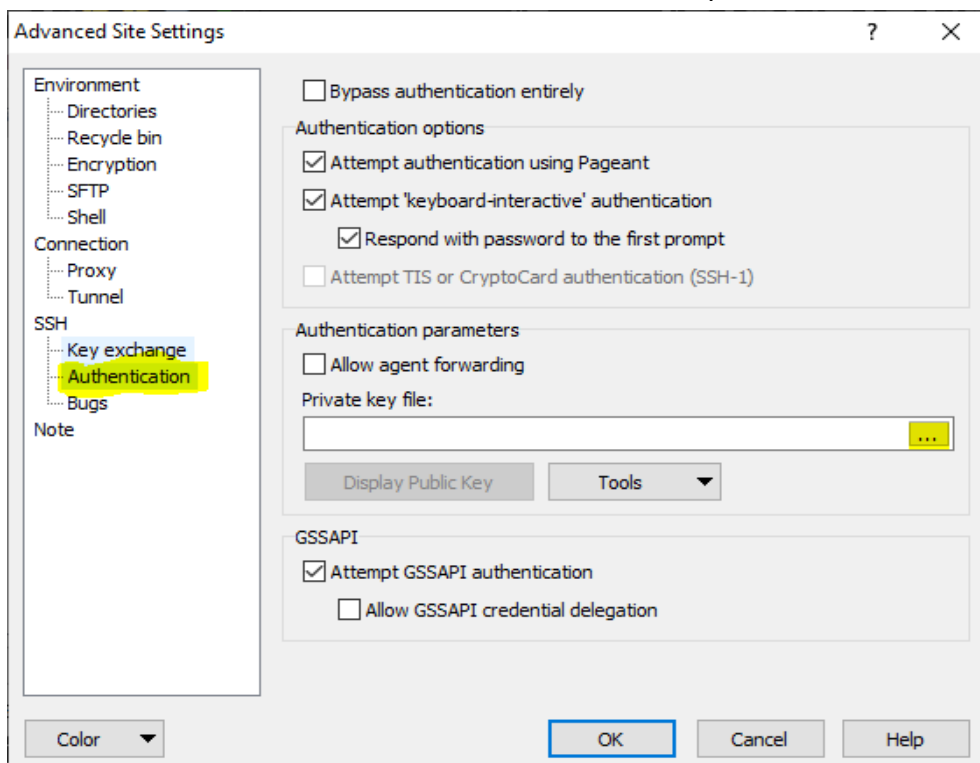


WinSCP:

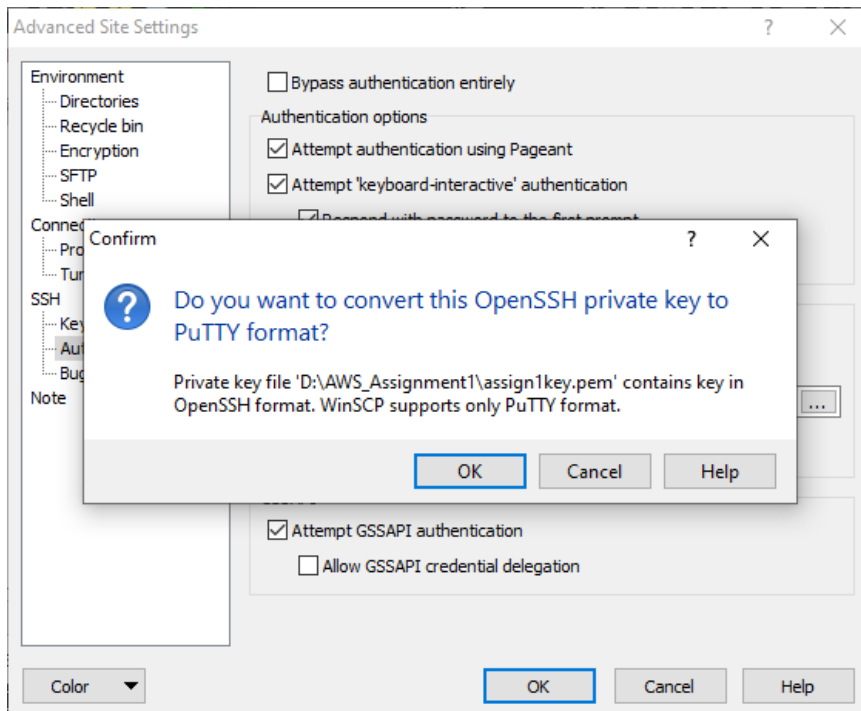
1. Launch "WinSCP" application >> Paste Host name copied in Step 3 above(Copy public DNS) and username "ec2-user". Hit on "Advanced.."



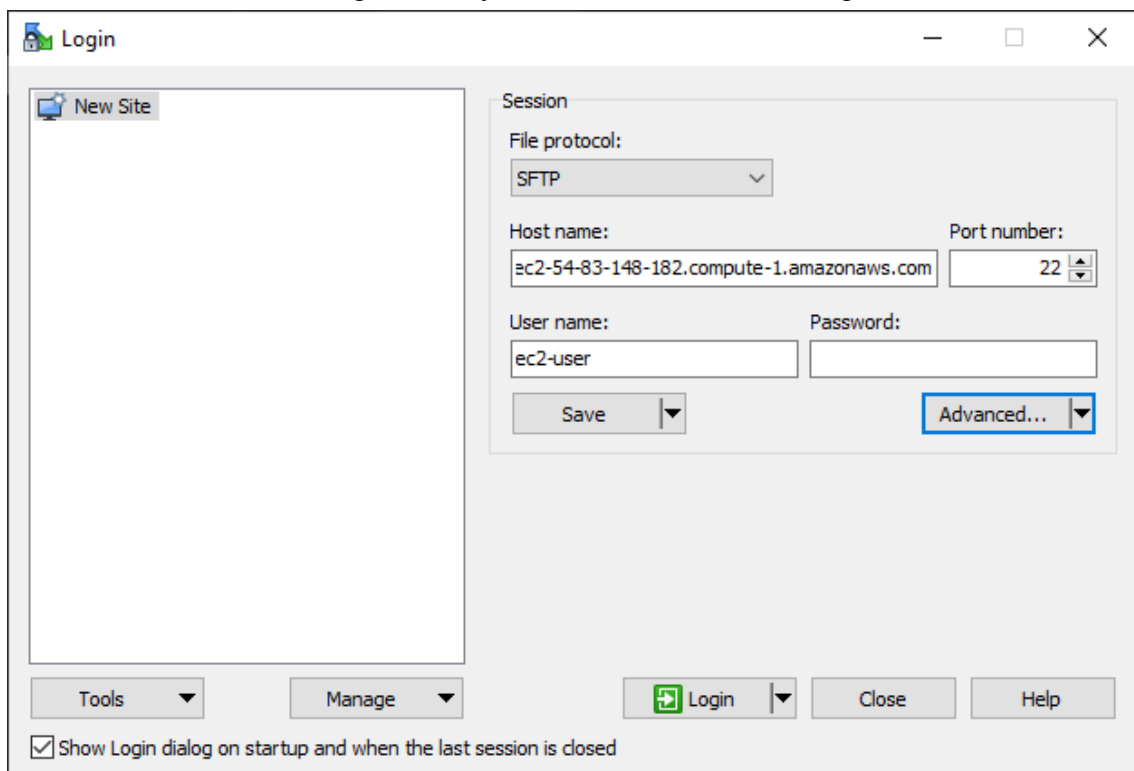
2. Go to SSH>>Authentication. Then browse & select .pem file we had downloaded



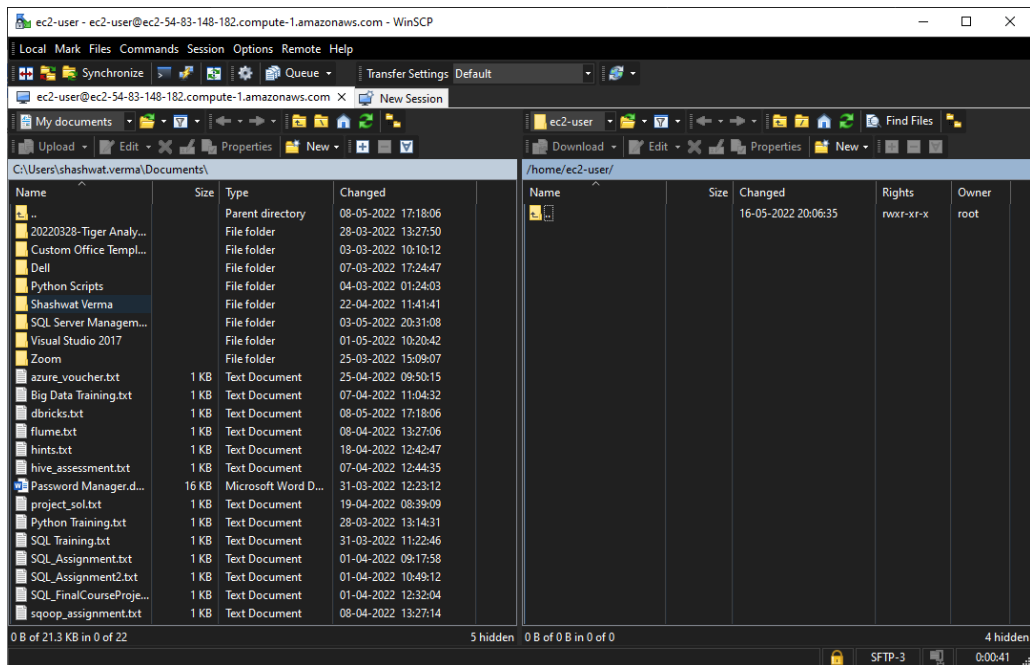
3. Click “OK” on the confirmation of key conversion to ppk as shown:



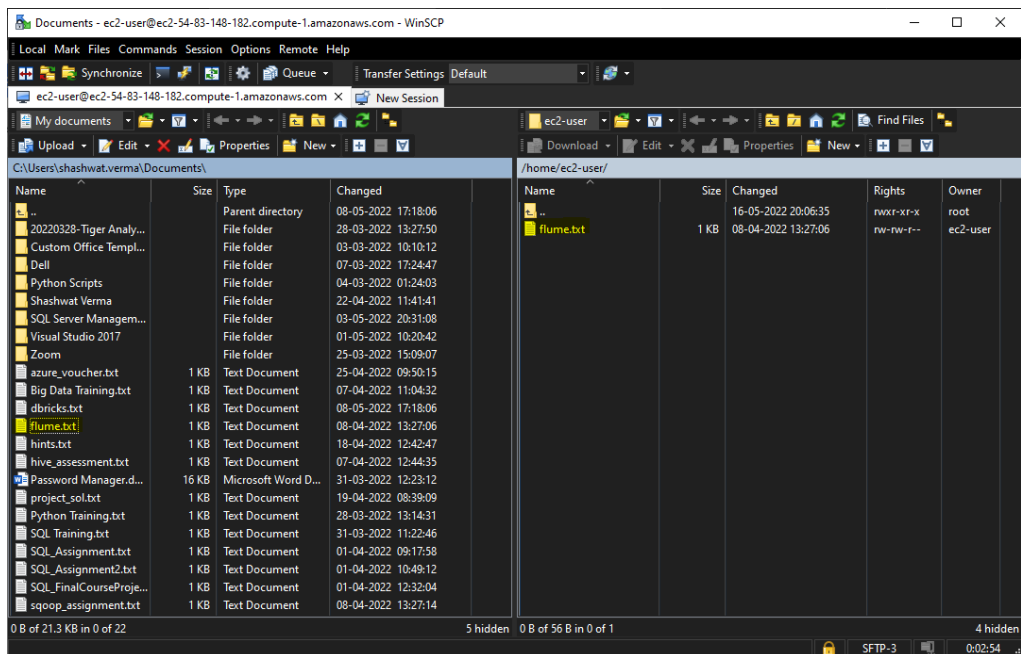
4. Hit “OK” and then hit “Login” once you are redirected to the Login window as shown:



5. Hit “Yes” to alert and FTP connection is launched in WinSCP as shown:



6. Drag and drop a file from local to VM via WinSCP as shown:



Confirm that above operation was successful in PuTTY by giving "ls" command as shown:

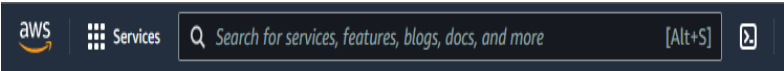
```
ec2-user@ip-172-31-26-136:~
login as: ec2-user
Authenticating with public key "imported-openssh-key"
Last login: Mon May 16 15:21:42 2022 from 183.83.43.82

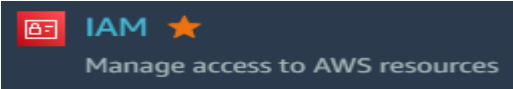
 _ _ | _ _ |
 _ | ( _ _ | /
 _ | \ _ _ | _ |

Amazon Linux 2 AMI

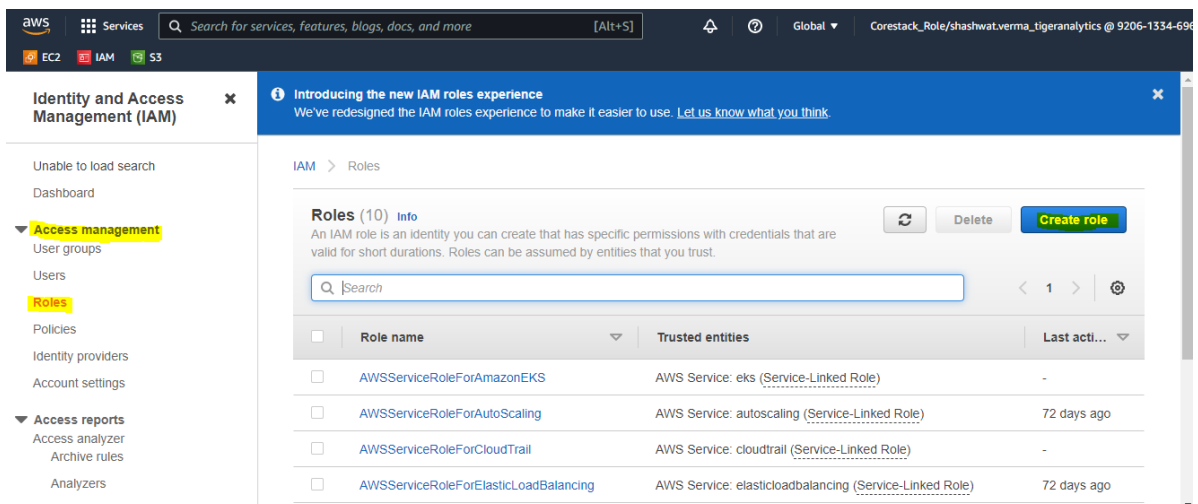
https://aws.amazon.com/amazon-linux-2/
2 package(s) needed for security, out of 5 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-26-136 ~]$ ls
flume.txt
[ec2-user@ip-172-31-26-136 ~]$
```

e. Attach the Administrator role to the VM

1. Search "IAM" in 

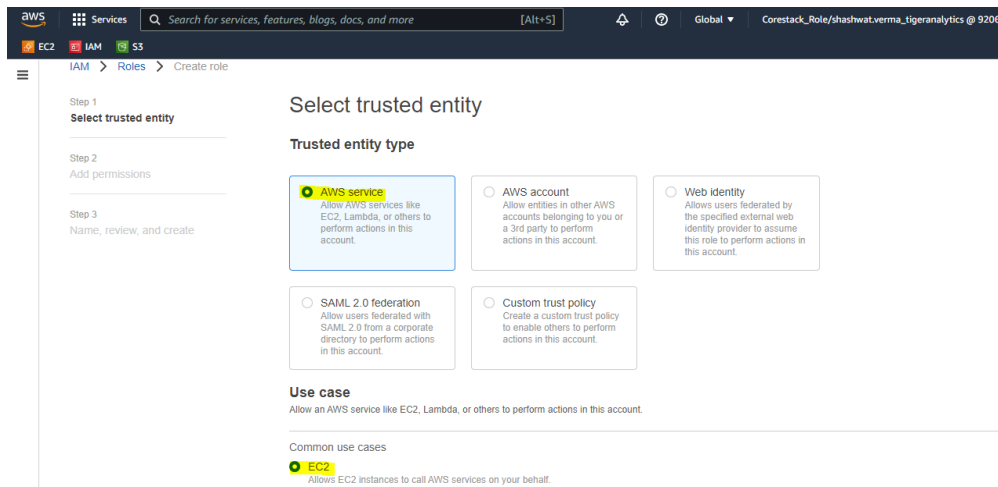
2. Click on 

3. Click on Access Management>>Roles, then hit "Create Role" as shown:

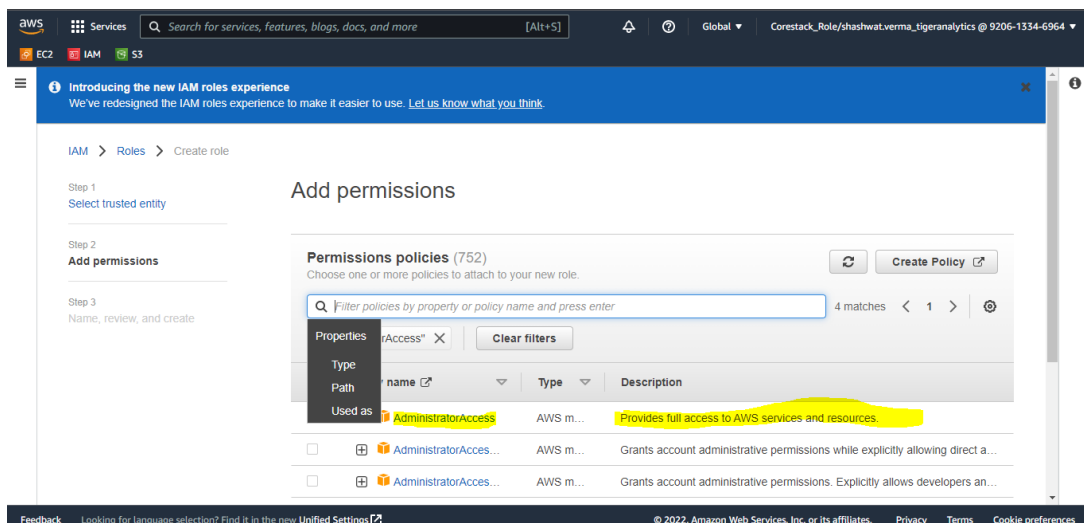


<input type="checkbox"/>	Role name	Trusted entities	Last acti...
<input type="checkbox"/>	AWSServiceRoleForAmazonEKS	AWS Service: eks (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Linked Role)	72 days ago
<input type="checkbox"/>	AWSServiceRoleForCloudTrail	AWS Service: cloudtrail (Service-Linked Role)	-
<input type="checkbox"/>	AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (Service-Linked Role)	72 days ago

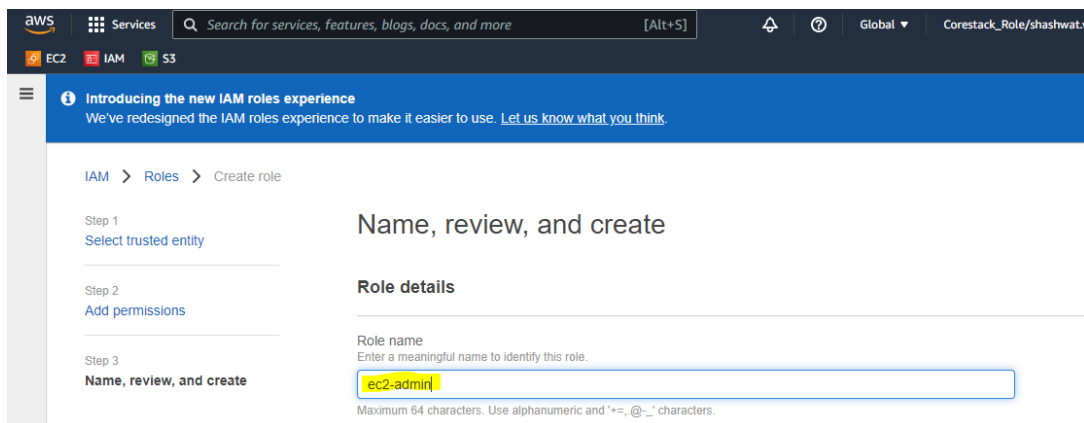
4. Select “EC2”. Hit “Next”:

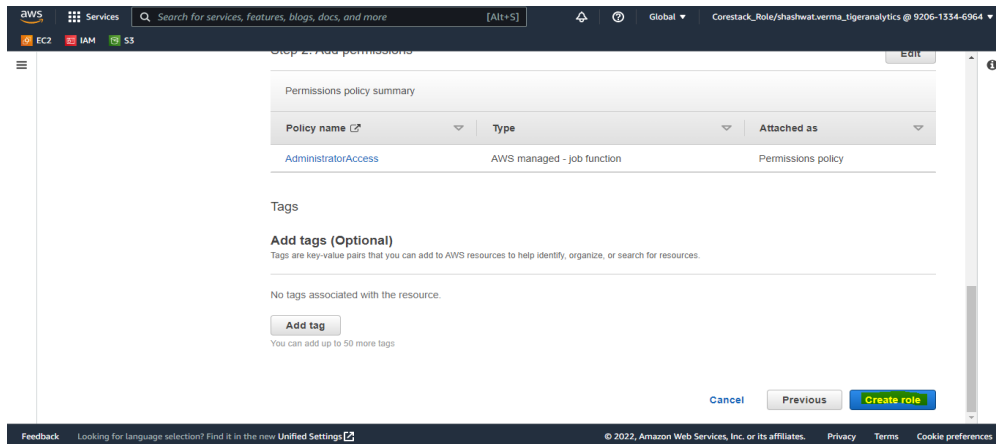


5. Search “AdministratorAccess” in Permission Policies and check the one with “Provides full access to AWS services and resources” description then hit “Next”:

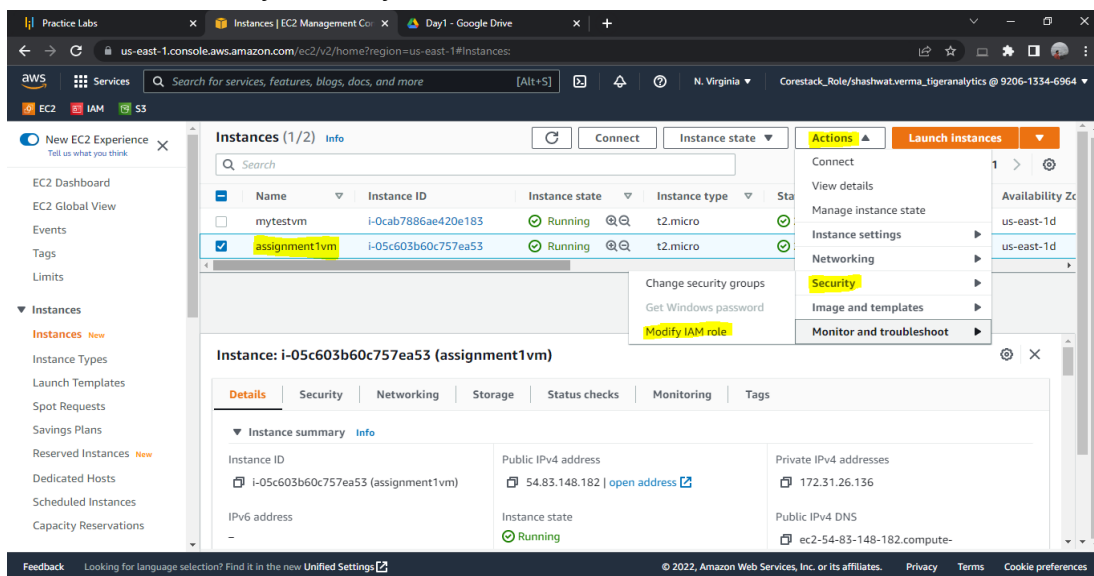


6. Enter name of role and hit “Create role” as shown in below snips:

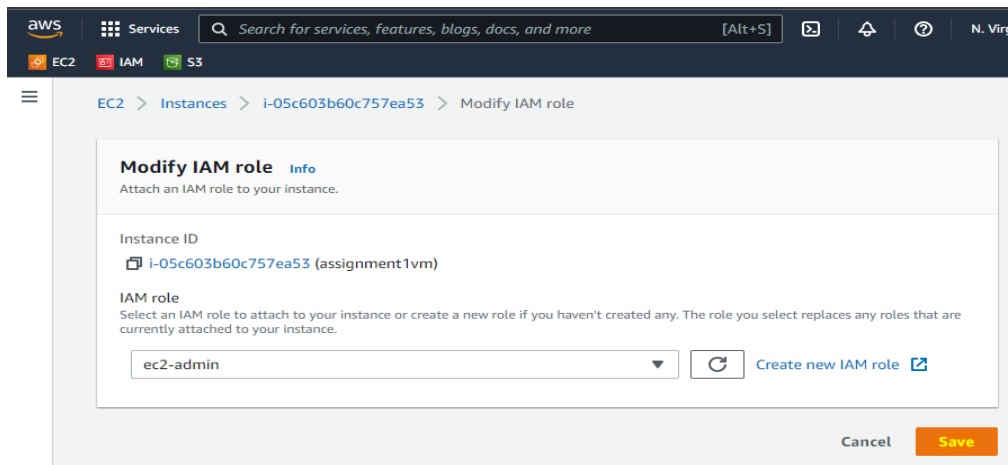




- Once role is successfully created go to EC2>>Instances, then select the VM created and hit Actions>>Security>>Modify IAM role:



- Choose the role created above from the drop down and hit on save as shown:



Role attachment successful as shown in the figure below:

The screenshot displays the AWS Management Console interface for the EC2 service. At the top, a green notification banner indicates that the 'ec2-admin' role has been successfully attached to the instance 'i-05c603b60c757ea53'. Below this, the 'Instances (2)' page is shown, featuring a table with the following data:

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	mytestvm	i-0cab7886ae420e183	Running	t2.micro	2/2 checks passed	No alarms	us-east-1d
<input type="checkbox"/>	assignment1vm	i-05c603b60c757ea53	Running	t2.micro	2/2 checks passed	No alarms	us-east-1d