

SVKM'S NMIM'S Nilkamal School of Mathematics, Applied Statistics & Analytics Master of Science (Data Science)

Practical-1 Infrastructure as a service using AWS.

Date:-09/01/2024

Submission Date:- 15/01/2024

Writeup:-

- **Cloud Computing architecture**

1. Cloud architecture consists of a front end and back end. The front end is the client-side interface. The back end consists of the cloud service provider's data centers, servers, storage and applications.
2. A central server administers the system, monitoring traffic and client demands to ensure quality of service. The underlying hardware infrastructure is distributed across various servers and locations.

- **IAAS**

Infrastructure as a Service (IaaS) provides access to fundamental computing resources such as servers, storage, networks and operating systems over the internet. The cloud provider owns and maintains the physical infrastructure and delivers these resources to customers on-demand.

Why IAAS??

1. Flexibility - IaaS provides highly scalable and flexible computing resources that can be provisioned and decommissioned on-demand based on workload needs. This is useful for spiky or unpredictable workloads.
2. Lower costs - With IaaS, organizations pay only for the infrastructure resources they use without having to purchase and maintain their own hardware. This eliminates capital expenditures and reduces costs.

- **AWS**

Amazon Web Services offers a broad set of global cloud-based products including compute, storage, databases, analytics, networking, mobile, developer tools, management tools, IoT, security, and enterprise applications: on-demand, available in seconds, with pay-as-you-go pricing. From data warehousing to deployment tools, directories to content delivery, over 200 AWS services are available

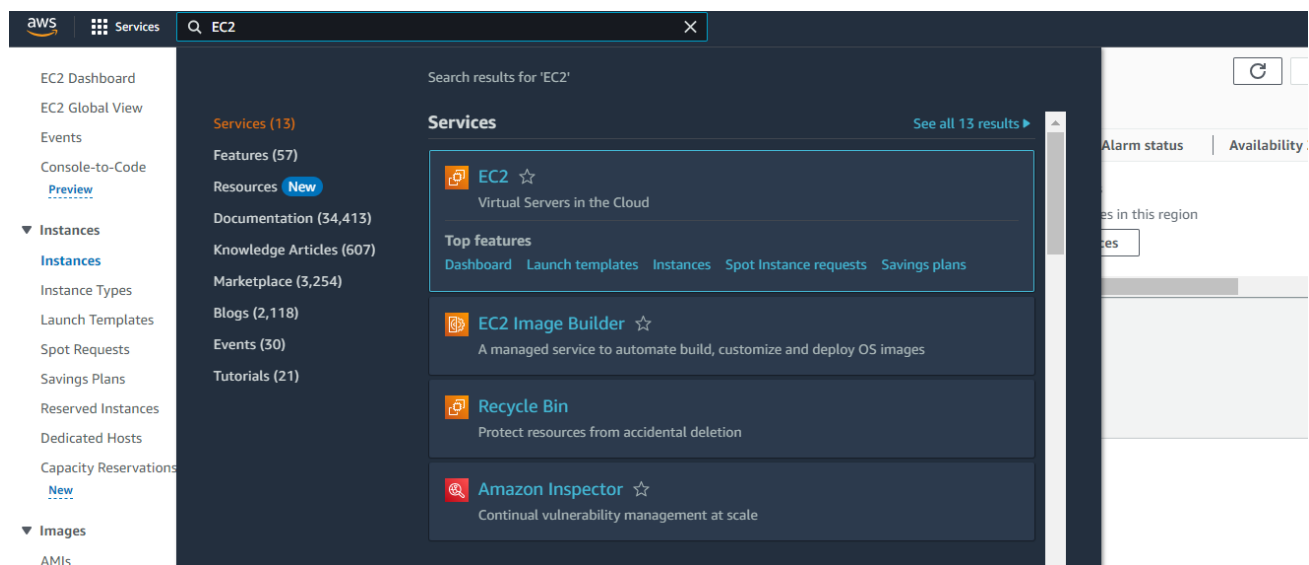
- **EC2**

Amazon Elastic Compute Cloud (EC2) provides scalable virtual servers that can be launched and terminated on-demand. Key features include:

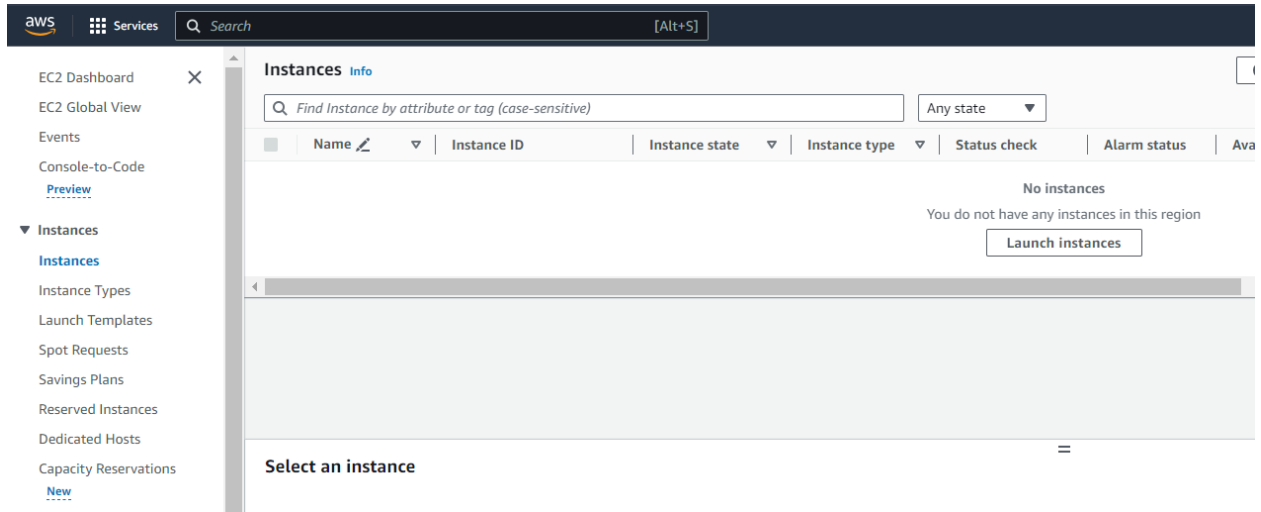
1. Multiple instance types for varying compute, memory and storage needs
2. Auto scaling and load balancing
3. High availability within and across data centers
4. Secure network connectivity options and access controls
5. Integrated with other AWS services
6. Pay as you go pricing based on instance hours used

Implementing the windows machine using AWS EC2

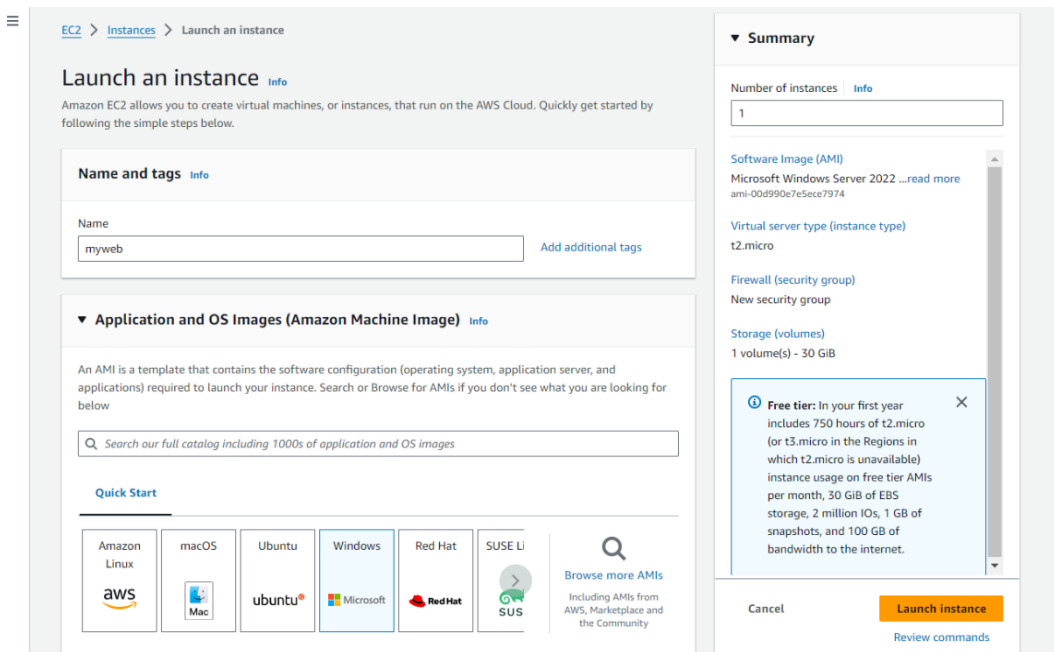
Step 1- Under AWS Dashboard select EC2



Step 2- Select Instance under EC2 and click on launch Instance



Step 3- Provide the name of the Instance and select Windows under Application and OS



Step 4- For key pair click on Create a new key pair and select perm and click on Create key pair

The 'Create key pair' dialog box is shown. It has a title bar with a close button. The main content area includes: a 'Key pair name' field with the value 'web' and a note that names can be up to 255 ASCII characters; a 'Key pair type' section with two radio buttons, 'RSA' (selected) and 'ED25519'; a 'Private key file format' section with two radio buttons, '.pem' (selected) and '.ppk'; and a yellow warning box at the bottom stating that the private key must be stored securely. At the bottom of the dialog are 'Cancel' and 'Create key pair' buttons.

Create key pair

Key pair name
Key pairs allow you to connect to your instance securely.
web
The name can include up to 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

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

Step 5 – Launch the Instance Successfully

The 'Launch Instance' wizard is shown at Step 5: Configure Instance Details. The left pane shows configuration options: 'Allow HTTP traffic from the internet' (unchecked), a warning about security group rules, 'Configure storage' (Advanced) with 1x 8 GiB gp3 Root volume, backup information, and 'Advanced details'. The right pane shows instance details: 'Software Image (AMI)' as Amazon Linux 2023, 'Virtual server type (instance type)' as t2.micro, 'Firewall (security group)' as New security group, and 'Storage (volumes)' as 1 volume(s) - 8 GiB. A 'Free tier' information box is also present. At the bottom are 'Cancel' and 'Launch instance' buttons, with a 'Review commands' link.

☐ 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 8 GiB gp3 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

Click refresh to view backup information
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems Edit

► Advanced details Info

1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.3.2...read more
ami-0a3c3a20c09d6f377

Virtual server type (instance type)
t2.micro

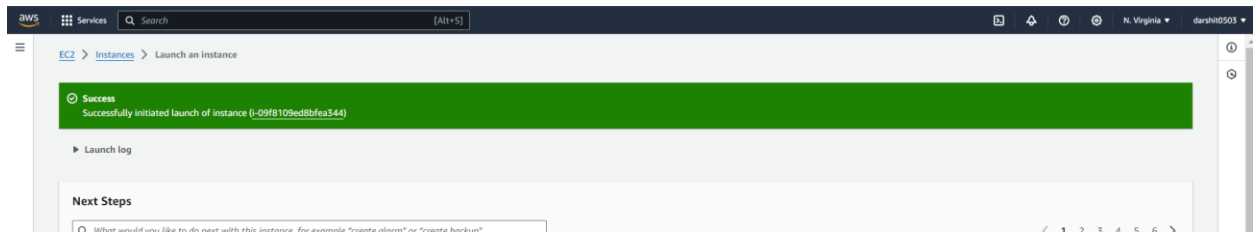
Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

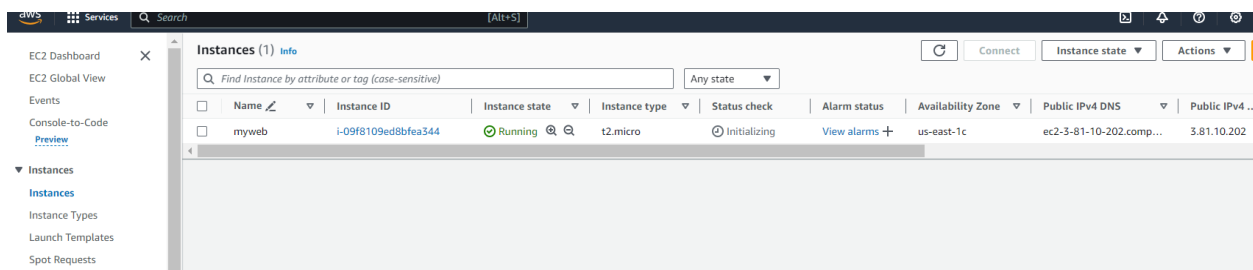
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch instance
[Review commands](#)

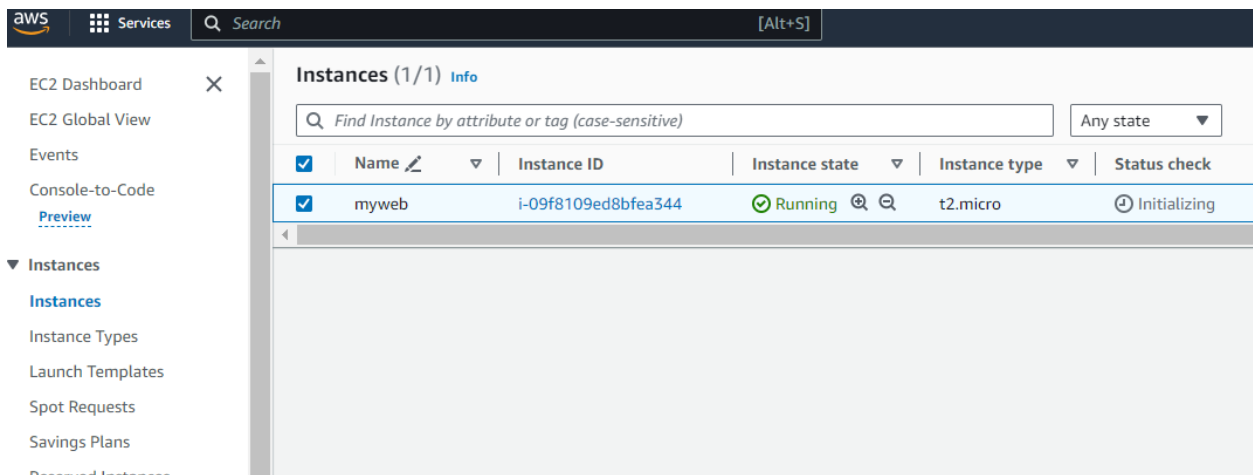
Step 6- Instance Successfully Launched



Step 7- Go to Instance, Refresh it and you see the launched instance



Step 8- Select the Instance



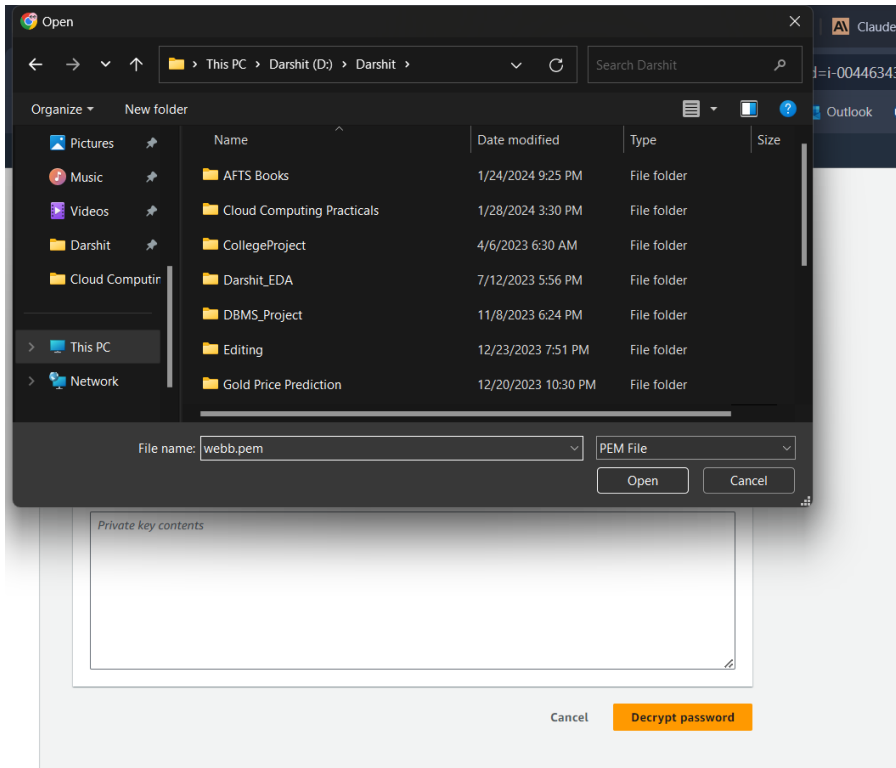
Step 9- Click on Connect and select RDP Client

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo, 'Services', a search bar, and a keyboard shortcut '[Alt+S]'. Below the navigation bar, a breadcrumb trail reads 'EC2 > Instances > i-09f8109ed8bfea344 > Connect to instance'. The main heading is 'Connect to instance' with an 'Info' link. Below this, a sub-header says 'Connect to your instance i-09f8109ed8bfea344 (myweb) using any of these options'. There are three tabs: 'Session Manager', 'RDP client' (which is selected), and 'EC2 serial console'. Under the 'RDP client' tab, the 'Instance ID' is 'i-09f8109ed8bfea344 (myweb)'. The 'Connection Type' section has two options: 'Connect using RDP client' (selected) and 'Connect using Fleet Manager'. The 'Connect using RDP client' option includes a description: 'Download a file to use with your RDP client and retrieve your password.' Below this, a note states: '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:'. There is a button 'Download remote desktop file'. Below this, a note says: 'When prompted, connect to your instance using the following details:'. There are two fields: 'Public DNS' with the value 'ec2-3-81-10-202.compute-1.amazonaws.com' and 'Username' with the value 'Administrator'. There is a 'Password' field and a 'Get password' link. At the bottom, a blue box contains an information icon and the text: 'If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.'

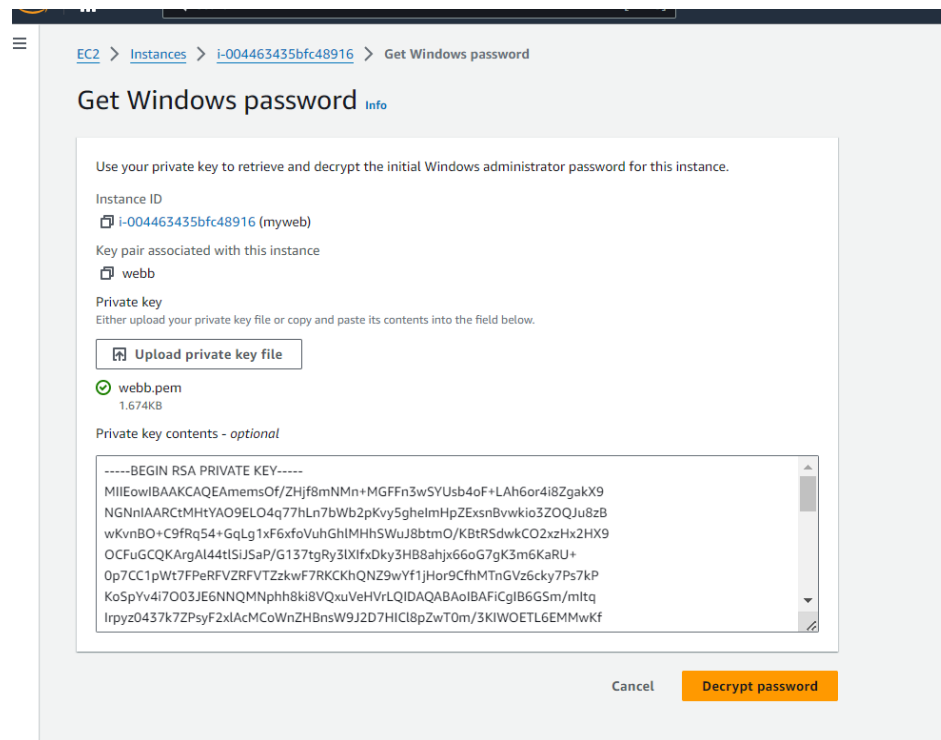
Step 10- Click on GET PASSWORD

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo, 'Services', a search bar, and a keyboard shortcut '[Alt+S]'. Below the navigation bar, a breadcrumb trail reads 'EC2 > Instances > i-09f8109ed8bfea344 > Get Windows password'. The main heading is 'Get Windows password' with an 'Info' link. Below this, a sub-header says 'Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.' There are three fields: 'Instance ID' with the value 'i-09f8109ed8bfea344 (myweb)', 'Key pair associated with this instance' with the value 'web', and 'Private key'. Below the 'Private key' field, there is a button 'Upload private key file'. Below this, there is a text area labeled 'Private key contents - optional' with the placeholder text 'Private key contents'. At the bottom, there are two buttons: 'Cancel' and 'Decrypt password'.

Step 11- Upload the key value File which got downloaded while creating a instance



Step 12- Decrypt the Password



Step 13- Save the password

xPmF7whmrQDULJETy?V)Ys*WQ8.OJ9?s

Public DNS: ec2-18-209-106-160.compute-1.amazonaws.com

Username: Administrator

✓ Password copied

xPmF7whmrQDULJETy?V)Ys*WQ8.OJ9?s

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

Cancel

Step 14- Click on Download the Remote Desktop File .

Connect to your instance i-004463435bfc48916 (myweb) using any of these options

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

Instance ID
i-004463435bfc48916 (myweb)

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:

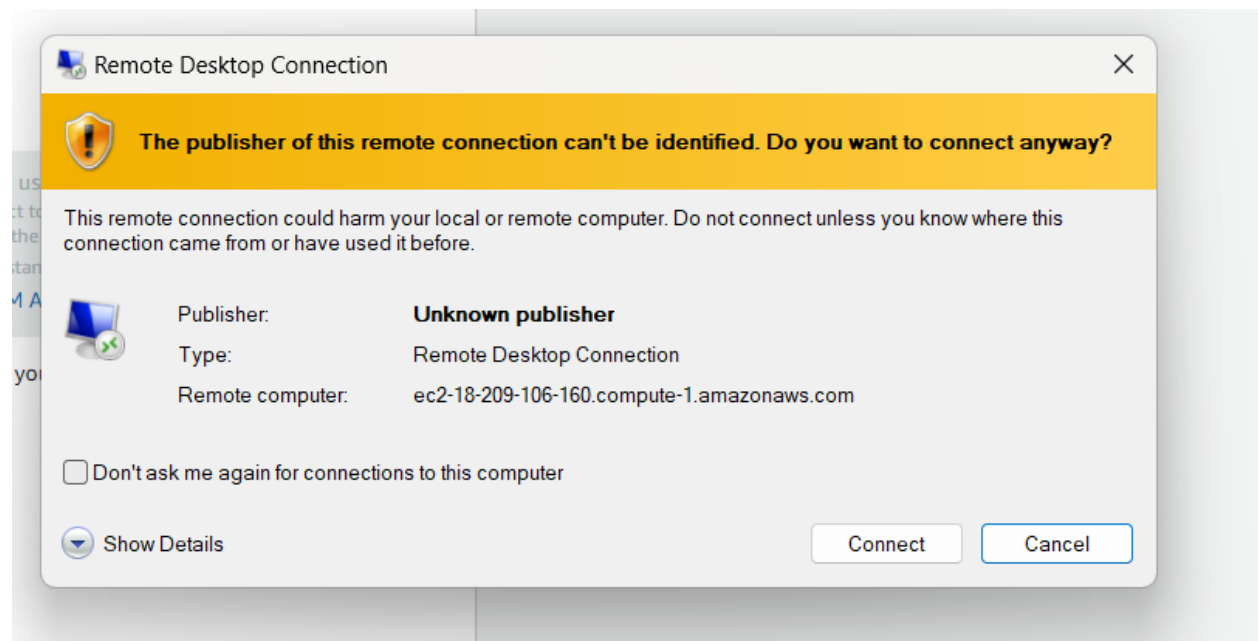
[Download remote desktop file](#)

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

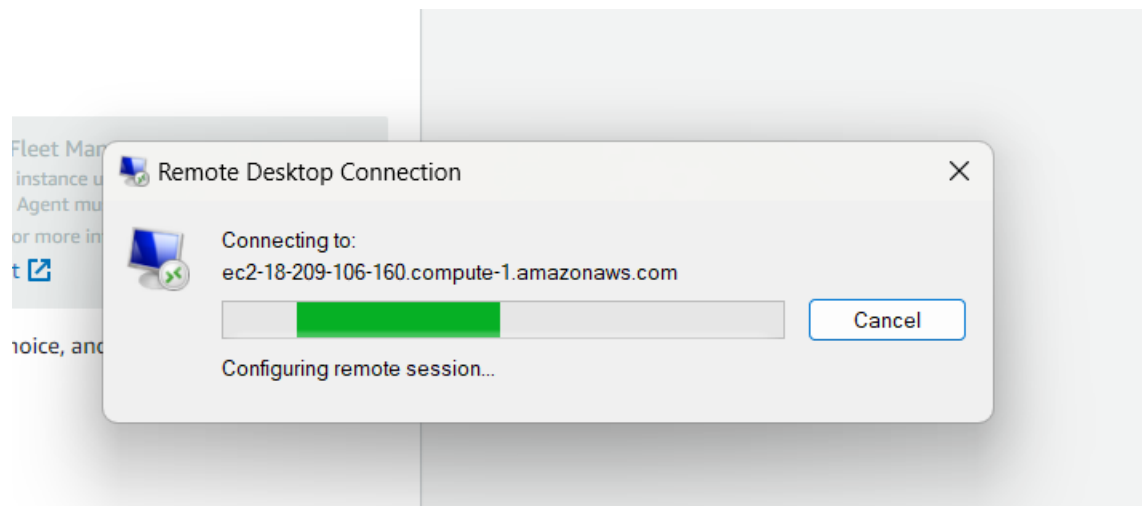
Public DNS: ec2-18-209-106-160.compute-1.amazonaws.com

Username: Administrator

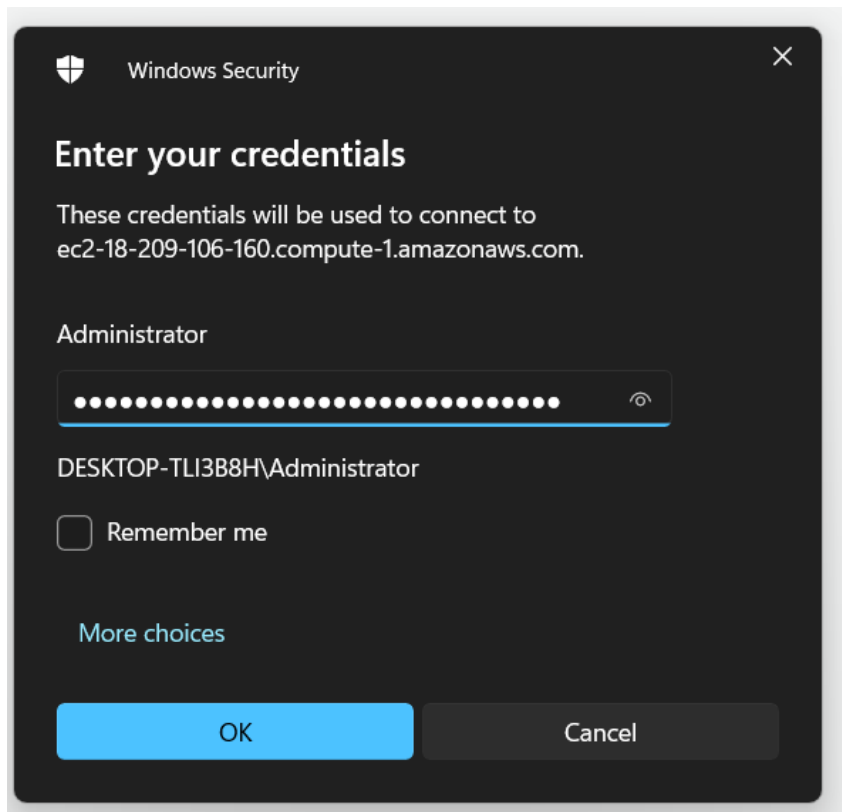
Step 15- Open the RDP File



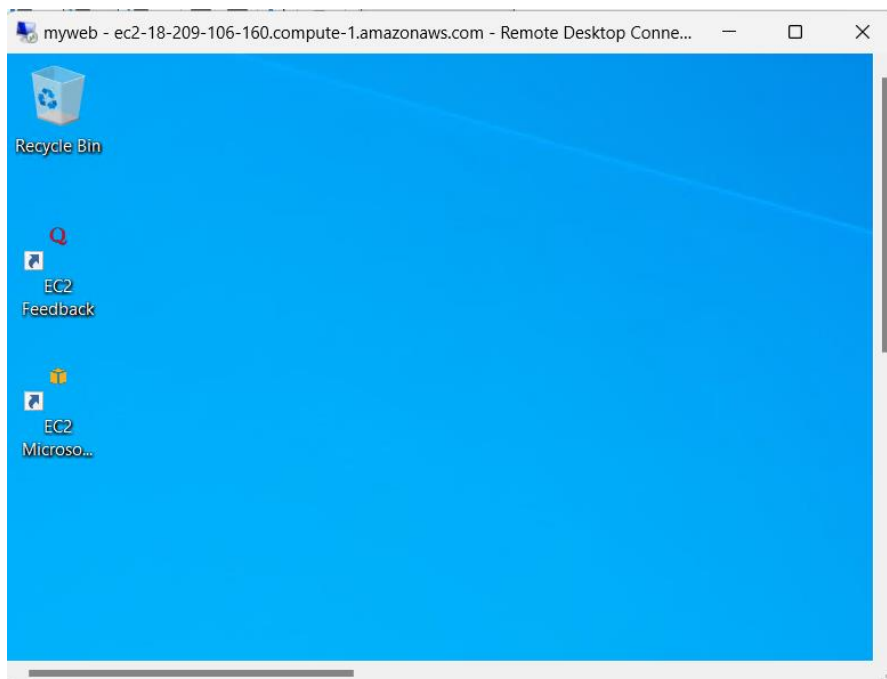
Step 16- Connect to the RDP



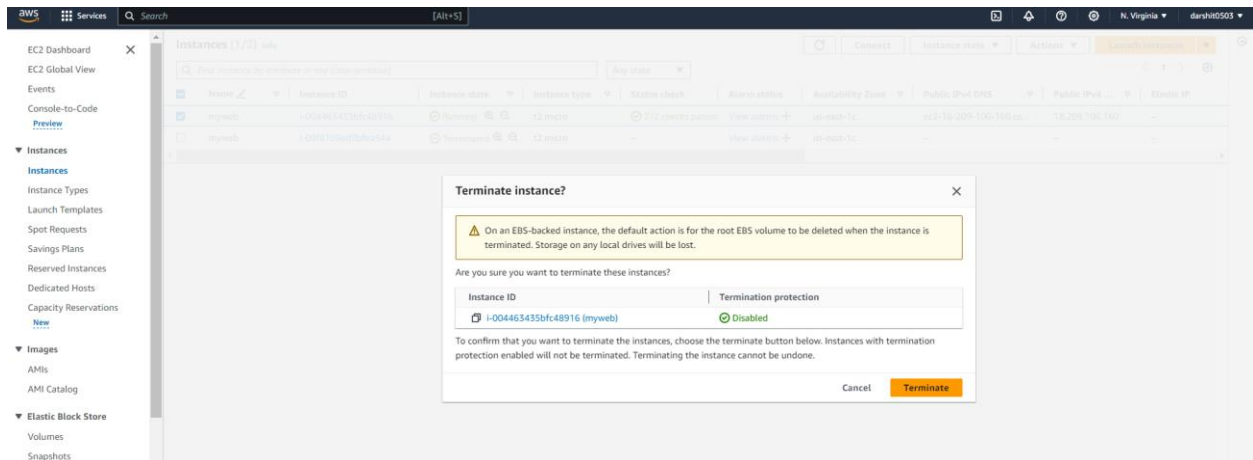
Step 17- Enter the password



Step 18- The Following Instance will popup

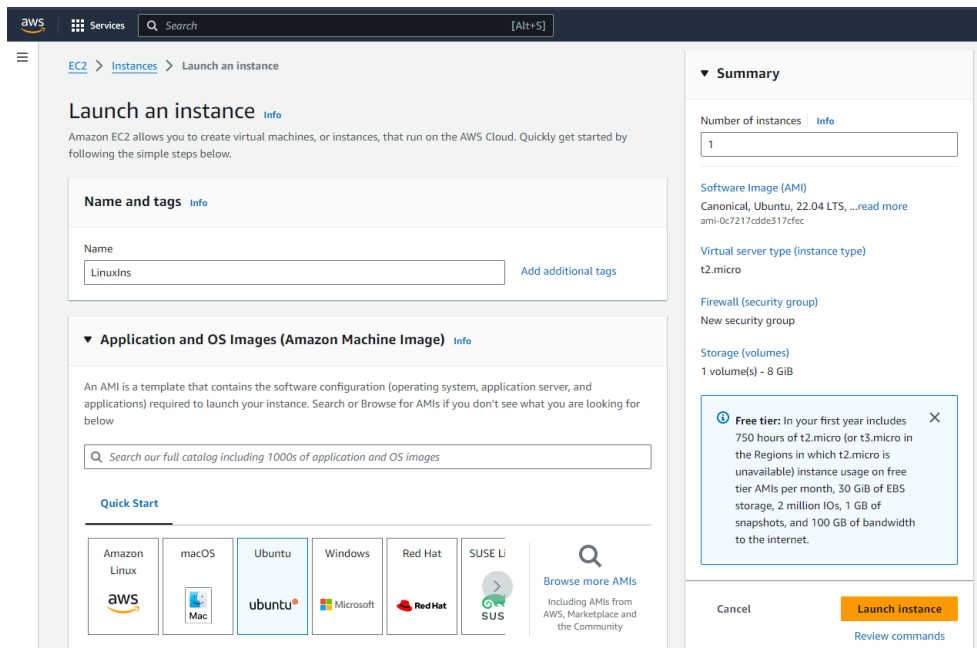


Step 19- Close the RDP and Go to Instances and Terminate the Instance



Implementing Ubuntu machine using AWS ec2 and execute the Linux commands.

Step 20- Launch a New Instance for Linux and select Application and OS as Ubuntu



Step 21- Create a key pair and select ppk under the following

Create key pair

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

linux

The name can include up to 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

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

Step 22- Download Putty.exe from Google and select Alternative Binary Files (SSH and Talent Client Itself) and select 64 bit x 86

Alternative binary files

The installer packages above will provide versions of all of these (except PuTTYtel and pterm), but you (Not sure whether you want the 32-bit or the 64-bit version? Read the [FAQ entry](#).)

putty.exe (the SSH and Telnet client itself)

64-bit x86: [putty.exe](#) ([signature](#))
64-bit Arm: [putty.exe](#) ([signature](#))
32-bit x86: [putty.exe](#) ([signature](#))

pscp.exe (an SCP client, i.e. command-line secure file copy)

64-bit x86: [pscp.exe](#) ([signature](#))
64-bit Arm: [pscp.exe](#) ([signature](#))
32-bit x86: [pscp.exe](#) ([signature](#))

psftp.exe (an SFTP client, i.e. general file transfer sessions much like FTP)

64-bit x86: [psftp.exe](#) ([signature](#))
64-bit Arm: [psftp.exe](#) ([signature](#))
32-bit x86: [psftp.exe](#) ([signature](#))

puttytel.exe (a Telnet-only client)

64-bit x86: [puttytel.exe](#) ([signature](#))
64-bit Arm: [puttytel.exe](#) ([signature](#))
32-bit x86: [puttytel.exe](#) ([signature](#))

Step 22- Allow all the traffic under the Linux Instance and Launch it

▼ Network settings [Info](#)

Edit

Network [Info](#)

vpc-0baad39a26d377e03

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

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-3' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere
0.0.0.0/0

☒ 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.

1

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...[read more](#)
ami-0c7217cde317cfeec

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

Storage (volumes)

1 volume(s) - 8 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, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel

Launch instance

[Review commands](#)

Step 23- After the Instance is successfully Launched Select the particular Linux

aws

Services

Search

[Alt+S]

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

Preview

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Outposts

Successfully terminated i-004463435bfc48916

Instances (1/3) [Info](#)

Find Instance by attribute or tag (case-sensitive)

Any state

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	myweb	i-09f8109ed8bfea344	Terminated	t2.micro	-	View alarms	us-east-1c
<input type="checkbox"/>	myweb	i-004463435bfc48916	Terminated	t2.micro	-	View alarms	us-east-1c
<input checked="" type="checkbox"/>	Linuxlns	i-0b831c6b1de9b10fd	Running	t2.micro	Initializing	View alarms	us-east-1c

Step 24- Copy the Public IPV4 Address by selecting the Instance

aws

Services

Search

[Alt+S]

EC2 Dashboard

EC2 Global View

Events

Console-to-Code

Preview

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Outposts

EC2 > Instances > i-0b831c6b1de9b10fd

Instance summary for i-0b831c6b1de9b10fd (Linuxlns)

Updated less than a minute ago

Instance ID

i-0b831c6b1de9b10fd (Linuxlns)

IPv6 address

-

Hostname type

IP name: ip-172-31-40-196.ec2.internal

Answer private resource DNS name

Public IPv4 address copied

54.80.176.156 [open address](#)

Instance state

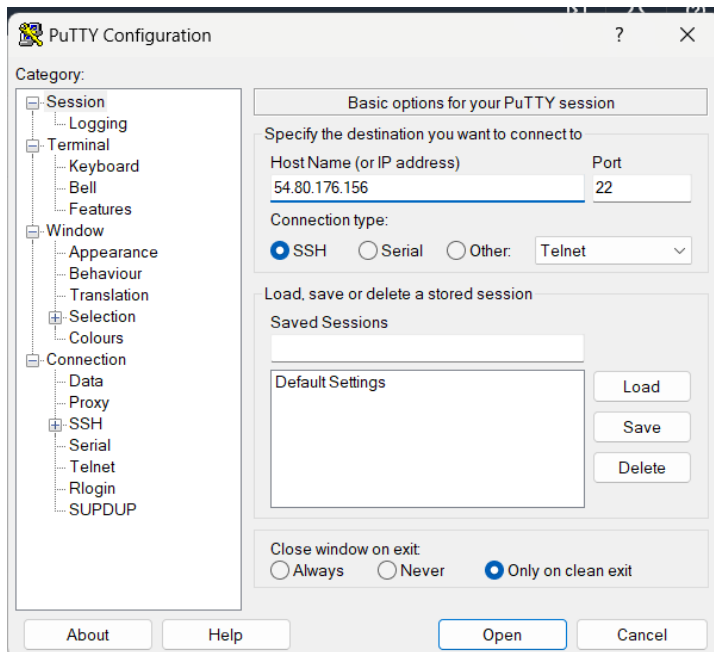
Running

Private IP DNS name (IPv4 only)

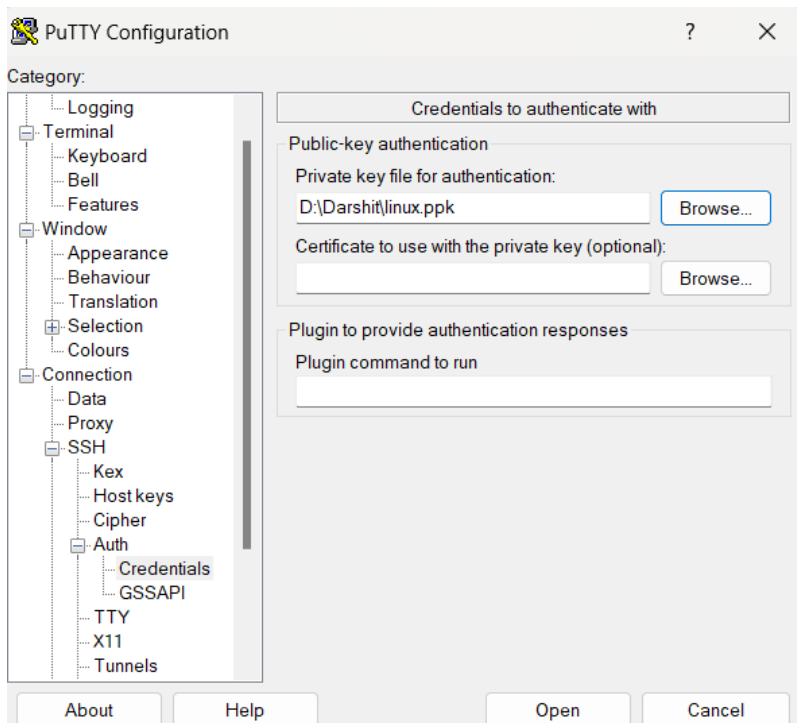
ip-172-31-40-196.ec2.internal

Instance type

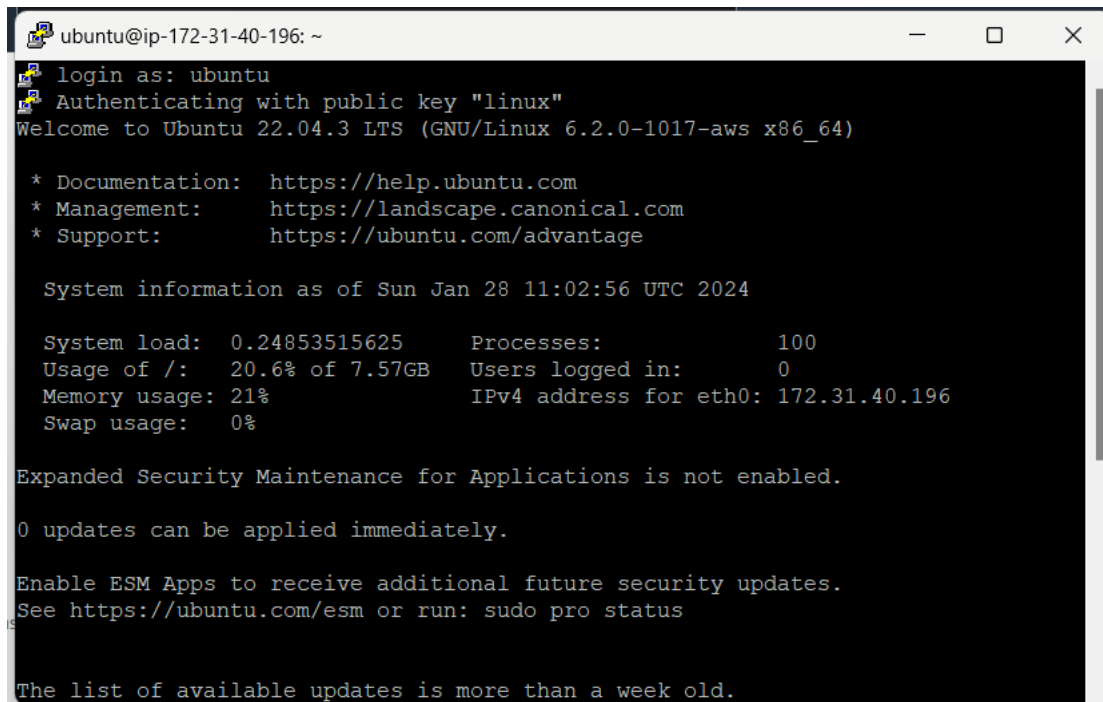
Step 25- Go to Putty and Paste the IP Address Copied



Step 26- Under the Putty Select Category -> SSH -> Auth -> Credentials -> Browse and select ppk file

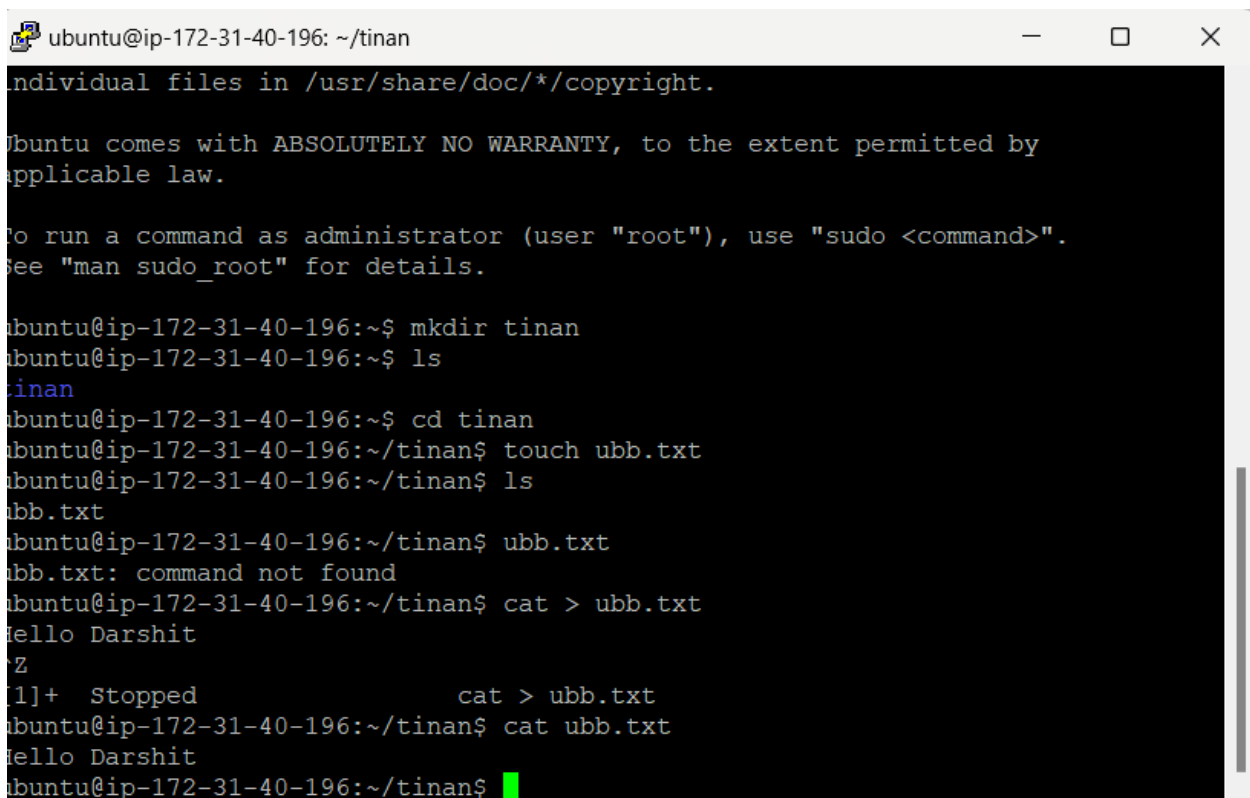


Step 27- Click on open and "ACCEPT" and the following popup will appear as Ubuntu Name

A terminal window titled 'ubuntu@ip-172-31-40-196: ~' showing the login process. The user 'ubuntu' logs in and is authenticated with a public key. The terminal displays the Ubuntu version (22.04.3 LTS) and system information as of Sun Jan 28 11:02:56 UTC 2024. It lists system load, processes, memory usage, and IPv4 address. A message indicates that Expanded Security Maintenance for Applications is not enabled and that 0 updates can be applied immediately. It also provides instructions on how to enable ESM Apps and check for updates.

```
ubuntu@ip-172-31-40-196: ~  
login as: ubuntu  
Authenticating with public key "linux"  
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.2.0-1017-aws x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Sun Jan 28 11:02:56 UTC 2024  
  
System load:  0.24853515625      Processes:           100  
Usage of /:   20.6% of 7.57GB    Users logged in:    0  
Memory usage: 21%               IPv4 address for eth0: 172.31.40.196  
Swap usage:   0%  
  
Expanded Security Maintenance for Applications is not enabled.  
  
0 updates can be applied immediately.  
  
Enable ESM Apps to receive additional future security updates.  
See https://ubuntu.com/esm or run: sudo pro status  
  
The list of available updates is more than a week old.
```

Step 28- Run the Following Commands in Putty

A terminal window titled 'ubuntu@ip-172-31-40-196: ~/tinan' showing a series of commands being executed. The user creates a directory named 'tinan', lists its contents, changes to the directory, creates a file named 'ubb.txt', lists its contents, and then uses 'cat' to write 'Hello Darshit' to the file. The terminal shows the output of each command, including the creation of the directory and file, and the successful writing of the text to the file.

```
ubuntu@ip-172-31-40-196: ~/tinan  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To run a command as administrator (user "root"), use "sudo <command>".  
See "man sudo_root" for details.  
  
ubuntu@ip-172-31-40-196:~$ mkdir tinan  
ubuntu@ip-172-31-40-196:~$ ls  
tinan  
ubuntu@ip-172-31-40-196:~$ cd tinan  
ubuntu@ip-172-31-40-196:~/tinan$ touch ubb.txt  
ubuntu@ip-172-31-40-196:~/tinan$ ls  
ubb.txt  
ubuntu@ip-172-31-40-196:~/tinan$ ubb.txt  
ubb.txt: command not found  
ubuntu@ip-172-31-40-196:~/tinan$ cat > ubb.txt  
Hello Darshit  
^Z  
[1]+  Stopped                  cat > ubb.txt  
ubuntu@ip-172-31-40-196:~/tinan$ cat ubb.txt  
Hello Darshit  
ubuntu@ip-172-31-40-196:~/tinan$
```

Step 29- Run the Following Python Code in Ubuntu

```
ubuntu@ip-172-31-40-196:~$ mkdir test
ubuntu@ip-172-31-40-196:~$ cd test
ubuntu@ip-172-31-40-196:~/test$ cat > hello.py
Hello World
^Z
[2]+  Stopped                  cat > hello.py
ubuntu@ip-172-31-40-196:~/test$ python3 hello.py
  File "/home/ubuntu/test/hello.py", line 1
    Hello World
    ^^^^^
SyntaxError: invalid syntax
ubuntu@ip-172-31-40-196:~/test$ cat > hello.py
print("Hello World")
^Z
[3]+  Stopped                  cat > hello.py
ubuntu@ip-172-31-40-196:~/test$ python3 hello.py
Hello World
ubuntu@ip-172-31-40-196:~/test$
```

Step 30- Terminate the Instance and Close Putty