

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

Practical-1 Infrastructure as a service using AWS.

Writeup:-

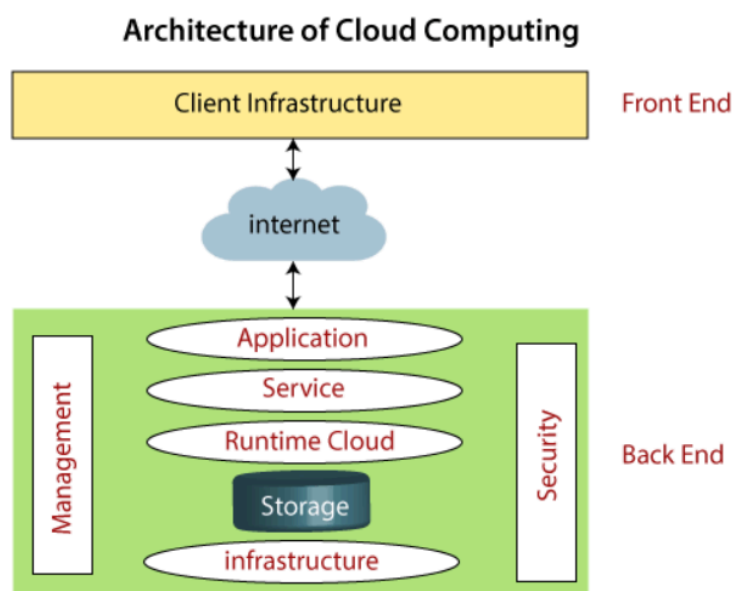
1. Cloud Computing architecture

Cloud computing technology is used by both small and large organizations to store the information in the cloud and access it from anywhere at any time using the internet connection.

Cloud computing architecture is a combination of service-oriented architecture and event-driven architecture.

Cloud computing architecture is divided into the following two parts -

1. Front End
2. Back End



Front End

The front end is used by the client. It contains client-side interfaces and applications that are required to access the cloud computing platforms. The front end includes

web servers (including Chrome, Firefox, internet explorer, etc.), thin & fat clients, tablets, and mobile devices.

Back End

The back end is used by the service provider. It manages all the resources that are required to provide cloud computing services. It includes a huge amount of data storage, security mechanism, virtual machines, deploying models, servers, traffic control mechanisms, etc

Components of Cloud Computing Architecture

There are the following components of cloud computing architecture -

1. Client Infrastructure

Client Infrastructure is a Front end component. It provides GUI (Graphical User Interface) to interact with the cloud.

2. Application

The application may be any software or platform that a client wants to access.

3. Service

A Cloud Services manages that which type of service you access according to the client's requirement.

Cloud computing offers the following three type of services:

i. Software as a Service (SaaS) – It is also known as **cloud application services**. Mostly, SaaS applications run directly through the web browser means we do not require to download and install these applications. Some important example of SaaS is given below –

Example: Google Apps, Salesforce Dropbox, Slack, Hubspot, Cisco WebEx.

ii. Platform as a Service (PaaS) – It is also known as **cloud platform services**. It is quite similar to SaaS, but the difference is that PaaS provides a platform for software creation, but using SaaS, we can access software over the internet without the need of any platform.

Example: Windows Azure, Force.com, Magento Commerce Cloud, OpenShift.

iii. Infrastructure as a Service (IaaS) – It is also known as **cloud infrastructure services**. It is responsible for managing applications data, middleware, and runtime environments.

Example: Amazon Web Services (AWS) EC2, Google Compute Engine (GCE), Cisco Metapod.

4. Runtime Cloud

Runtime Cloud provides the **execution and runtime environment** to the virtual machines.

5. Storage

Storage is one of the most important components of cloud computing. It provides a huge amount of storage capacity in the cloud to store and manage data.

6. Infrastructure

It provides services on the **host level, application level, and network level**. Cloud infrastructure includes hardware and software components such as servers, storage, network devices, virtualization software, and other storage resources that are needed to support the cloud computing model.

7. Management

Management is used to manage components such as application, service, runtime cloud, storage, infrastructure, and other security issues in the backend and establish coordination between them.

8. Security

Security is an in-built back end component of cloud computing. It implements a security mechanism in the back end.

9. Internet

The Internet is medium through which front end and back end can interact and communicate with each other.

2. IAAS

Infrastructure-as-a-Service (IaaS) is a form of cloud computing service that offers **compute, storage and networking resources** on-demand, usually on a pay-as-you-go basis. Businesses can purchase resources on-demand and as-needed instead of having to buy the hardware outright.

While IaaS gives you virtualized resources such as servers, disks, networks, and IP addresses, you are still responsible for administering the operating system, data, applications, middleware and runtimes. A dashboard or an API gives you complete control over the entire infrastructure.

IaaS gives you the flexibility to purchase only the computing you need and scales them up or down as needed. If you are looking to migrate an application as-is from an on-premises data center to the cloud, choose the IaaS model. You will be able to proceed with the migration with minimum changes.

Because of its speed of deployment, IaaS is a quick and flexible way to build up and take down development and testing environments.

Examples of IaaS include Rackspace, Amazon Web Services (AWS) Elastic Compute Cloud (EC2), Microsoft Azure, Google Compute Engine (GCE) and Joyent.

Advantage:-

IaaS is advantageous when scalability and quick provisioning are key. Cloud Service Providers can provide a variety of hardware configurations with pre-configured operating systems such as Linux or Windows. You can also use rapid provisioning patterns with Infrastructure as Code (IaC) to create packages of IT resources that can be bundled and deployed into ready-made environments.

Disadvantage:-

Since the infrastructure is under the control of the service provider, outages in the service provider controlled infrastructure can affect the customer infrastructure. Troubleshooting is more difficult because IaaS customers do not have complete visibility to the cloud service provider infrastructure. If peak usage is high, monthly costs may be much higher than expected.

3. AWS

AWS (Amazon Web Services) is a comprehensive, evolving cloud computing platform provided by Amazon. It includes a mixture of infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) and packaged software-as-a-service (SaaS) offerings. AWS offers tools such as compute power, database storage and content delivery services.

AWS offers many different tools and products for enterprises and software developers in 245 countries and territories. Government agencies, education institutions, nonprofits and private organizations use AWS services.

Amazon web service is an online platform that provides scalable and cost-effective cloud computing solutions.

4. AWS services

In the rapid revolution of Cloud Computing, AWS facilitates with wide variety of services respect to the fields and needs. The following are the top AWS services that are in wide usage:

Amazon EC2(Elastic Compute Cloud) : It provides the Scalable computing power via cloud allowing the users to run applications and manage the workloads over their remotely.

Amazon S3 (Simple Storage Service): It offers scalable object Storage as a Service with high durability for storing and retrieving any amount of data.

AWS Lambda: It is a service in Serverless Architecture with Function as a Service facilitating serverless computing i.e., running the code on response to the events, the background environment management of servers is handled by aws automatically. It helps the developers to completely focus on the logic of code build.

Amazon RDS (Relational Database Service): This is an aws service that simplifies the management of database providing high available relational databases in the cloud.

Amazon VPC (Virtual Private Cloud): It enables the users to create isolated networks with option of public and private expose within the AWS cloud, providing safe and adaptable configurations of their resources.

5. EC2

Amazon Elastic Compute Cloud (Amazon EC2) provides on-demand, scalable computing capacity in the Amazon Web Services (AWS) Cloud. Using Amazon EC2 reduces hardware costs so you can develop and deploy applications faster. You can use Amazon EC2 to launch as many or as few virtual servers as you need, configure security and networking, and manage storage. You can add capacity (scale up) to handle compute-heavy tasks, such as monthly or yearly processes, or spikes in website traffic. When usage decreases, you can reduce capacity (scale down) again.

Features of Amazon EC2

- **Instances**

Virtual servers.

- **Amazon Machine Images (AMIs)**

Preconfigured templates for your instances that package the components you need for your server (including the operating system and additional software).

- **Instance types**

Various configurations of CPU, memory, storage, networking capacity, and graphics hardware for your instances.

- **Key pairs**

Secure login information for your instances. AWS stores the public key and you store the private key in a secure place.

- **Instance store volumes**

Storage volumes for temporary data that is deleted when you stop, hibernate, or terminate your instance.

- **Amazon EBS volumes**

Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS).

- **Regions, Availability Zones, Local Zones, AWS Outposts, and Wavelength Zones**

Multiple physical locations for your resources, such as instances and Amazon EBS volumes.

- **Security groups**

A virtual firewall that allows you to specify the protocols, ports, and source IP ranges that can reach your instances, and the destination IP ranges to which your instances can connect.

- **Elastic IP addresses**

Static IPv4 addresses for dynamic cloud computing.

- **Tags**

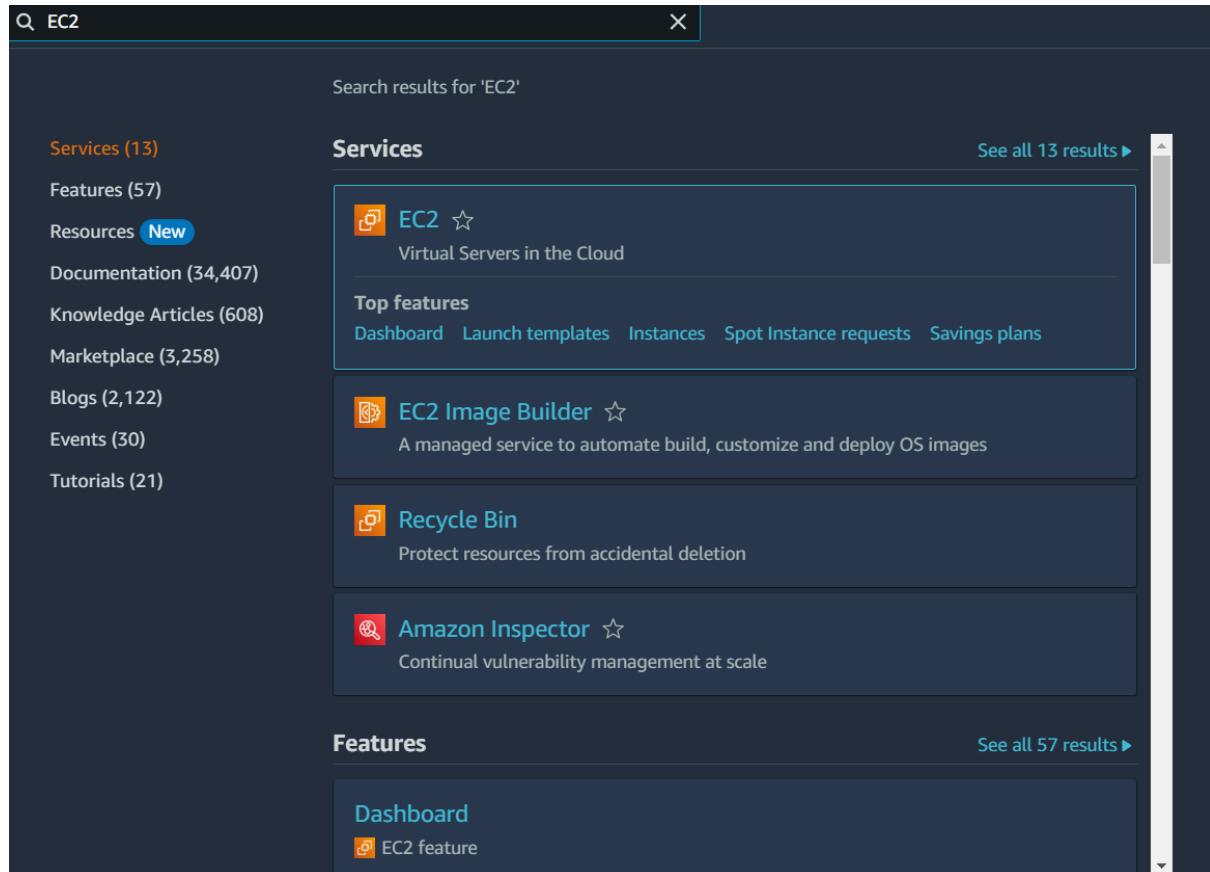
Metadata that you can create and assign to your Amazon EC2 resources.

- **Virtual private clouds (VPCs)**

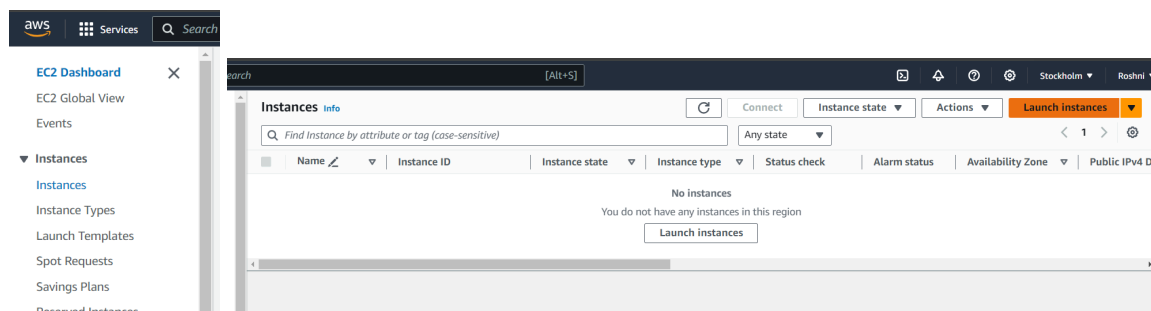
Virtual networks you can create that are logically isolated from the rest of the AWS Cloud. You can optionally connect these virtual networks to your own network.

Implement the windows machine using AWS ec2.

Step 1:-Login to <https://aws.amazon.com/> and select EC2



Step 2:- Select Instances from the left corner of the dashboard under EC2 and click on Launch instance



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

The screenshot shows the AWS Management Console interface for launching an EC2 instance. The breadcrumb navigation at the top indicates the path: EC2 > Instances > Launch an instance. The main heading is 'Launch an instance' with an 'Info' link. Below this, a brief description states: '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.' The first section, 'Name and tags', contains a text input field for the instance name, which currently has 'myweb' entered, and a button labeled 'Add additional tags'. The second section, 'Application and OS Images (Amazon Machine Image)', includes a descriptive paragraph about AMIs and a search bar with the placeholder text 'Search our full catalog including 1000s of application and OS images'. Below the search bar is a 'Quick Start' section featuring a row of AMI icons: Amazon Linux, macOS, Ubuntu, Windows (which is highlighted with a blue border), Red Hat, and SUSE Linux. To the right of these icons is a link that says 'Browse more AMIs' with a subtext 'Including AMIs from AWS, Marketplace and the Community'.

Step 4:- For key pair -> Create a new key pair ->Provide any name to the key pair name -> select type as RSA ->Private key file format as (.pem) and then click on create key pair.

The screenshot shows the 'Create key pair' dialog box. It has a title bar with a close button (X). The first section is 'Key pair name', with a subtext 'Key pairs allow you to connect to your instance securely.' and a text input field containing 'myWindows'. Below this is a note: 'The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.' The second section is 'Key pair type', showing two options: 'RSA' (selected with a radio button) and 'ED25519'. The 'RSA' option has a subtext 'RSA encrypted private and public key pair'. The 'ED25519' option has a subtext 'ED25519 encrypted private and public key pair (Not supported for Windows instances)'. The third section is 'Private key file format', showing two options: '.pem' (selected with a radio button) and '.ppk'. The '.pem' option has a subtext 'For use with OpenSSH'. The '.ppk' option has a subtext 'For use with PuTTY'. At the bottom of the dialog is a yellow warning box with a triangle icon and the text: '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](#)'. At the very bottom are two buttons: 'Cancel' and 'Create key pair'.

Step 5:-Click on Launch Instance

Services Search [Alt+S]

☒ **Allow RDP 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.

▼ Configure storage Info Advanced

1x 830 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

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

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

▼ Summary

Number of instances Info
1

Software Image (AMI)
Microsoft Windows Server 2022 ...read more
ami-06add5410081767cd

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 830 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 I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel Launch instance Review commands

Step 6:- Your Instance will be launched successfully.

Success
Successfully initiated launch of instance (i-0fee91e9068161158)

Launch log

Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"

Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
Create billing alerts

Connect to your instance
Once your instance is running, log into it from your local computer.
Connect to instance
Learn more

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
Connect an RDS database
Create a new RDS database
Learn more

Create EBS snapshot policy
Create a policy that automates deletion of EBS snapshots
Create EBS snapshot policy

Step 7:- Go to Instances -> Refresh the page to see your created Instance

Instances (1) Info

Find Instance by attribute or tag (case-sensitive) Any state

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
<input type="checkbox"/>	myweb	i-0fee91e9068161158	Running	t3.micro	Initializing	View alarms	eu-north-1a	ec2-51-21-135-100.eu-...	51.21.135.100

Step 8:- Click on your created Instance and then select Connect option at the top.

Instances (1/1) Info								
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/>					Any state ▾			
<input checked="" type="checkbox"/>	Name ✎	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status	Availability Zone ▾	Public
<input checked="" type="checkbox"/>	myweb	i-0fee91e9068161158	Running	t3.micro	2/2 checks passed View alarms +		eu-north-1a	ec2-5

Step 9:- Select RDP Client and click on Get password

Connect to instance [Info](#)

Connect to your instance i-0fee91e9068161158 (myweb) using any of these options

Session Manager

RDP client

EC2 serial console

Instance ID

i-0fee91e9068161158 (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
 ec2-51-21-135-100.eu-north-1.compute.amazonaws.com

Username
 Administrator

Password **Get password**

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

Step 10:-Click on Upload private key file (the key pair(.pem) file which got downloaded while creating the key pair for your Instance.)

aws

Services

[Alt+S]

EC2

>

Instances

>

i-0fee91e9068161158

>

Get Windows password

Get Windows password [Info](#)

Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.

Instance ID

i-0fee91e9068161158 (myweb)

Key pair associated with this instance

myWindows

Private key

Either upload your private key file or copy and paste its contents into the field below.


Upload private key file

Private key contents - optional

Private key contents

Cancel

Decrypt password

Name	Date modified	Type	Size
▼ Today			
 myWindows.pem	31-01-2024 19:56	PEM File	2

Step 11:- After uploading private key file click on Decrypt password

Get Windows password
Info

Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.

Instance ID
i-Ofee91e9068161158 (myweb)

Key pair associated with this instance
myWindows

Private key
Either upload your private key file or copy and paste its contents into the field below.

Upload private key file

✓ myWindows.pem
1.674KB

Private key contents - optional

```

-----BEGIN RSA PRIVATE KEY-----
MIIIEowlBAAKCAQEAhyjjoDwALmk7g12ylXtEBSbbmi1K/XdhBXwPCiosQiniMLZ
XX54wKFN7/R160WVv+9DLUpDCwjhN0yCgKcuL2JqTwPdudbiBY8488noyu0Fx9L3
29WhLD7fn1QkTpdCykRCbWfBC/rURHXxcXrmAoeRsLkU0Pc/ChX5byXGJQhrkCMK
4BIXMGZl5He9eRKELfgCOJlLO+s7JdRdEHlIPQpq24R/UpwktCGG9eG3n4oibx
NzzrITCd0dKMkJr1FPiaGVGD4frbpkgwjjDuy3wHvm6ROhD3wXMRhldaw+ZduHBJ
isgRIa9CSIBKRbJI3L/hMlhL/dWNgUOeb8g6nwlDAQABAolBAHR13ngr1aFqVRjh
9ReHTotqljteca19Xu/vT18m0aQpcHsFGfkbhUTGOLen9utQvCXz7fhaYsZhUl4p

```

Cancel
Decrypt password

Step 12:- Save the password

Session Manager
RDP client
EC2 serial console

Instance ID
i-Ofee91e9068161158 (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
ec2-51-21-135-100.eu-north-1.amazonaws.com

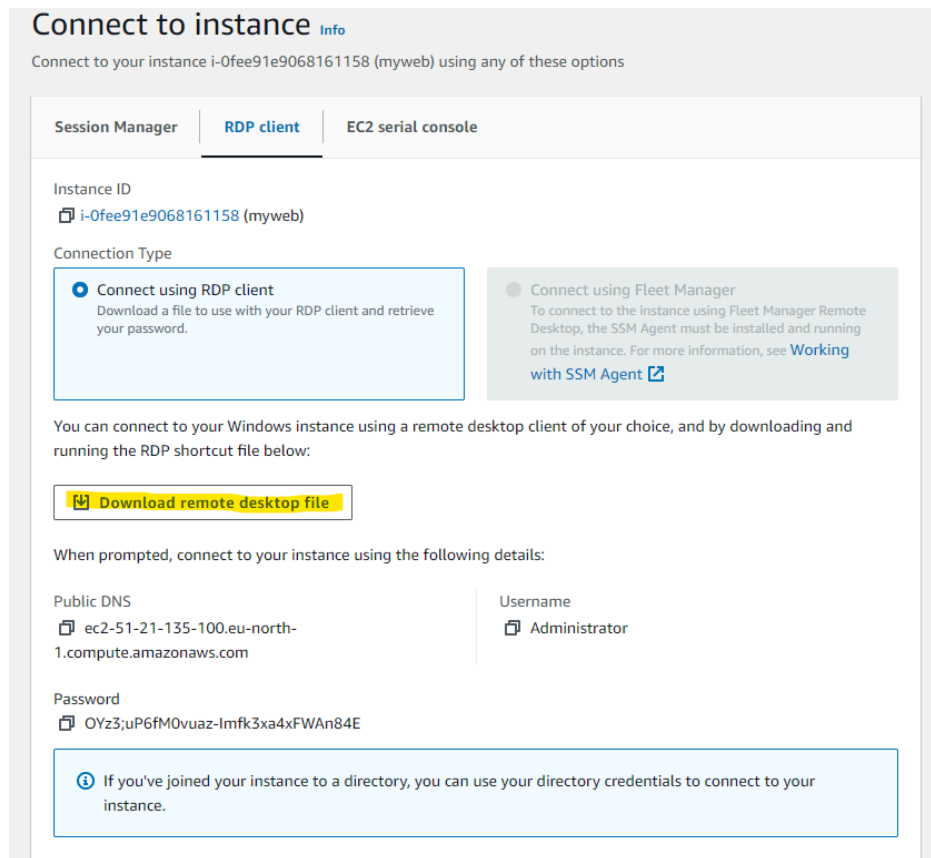
Username
Administrator

Password copied

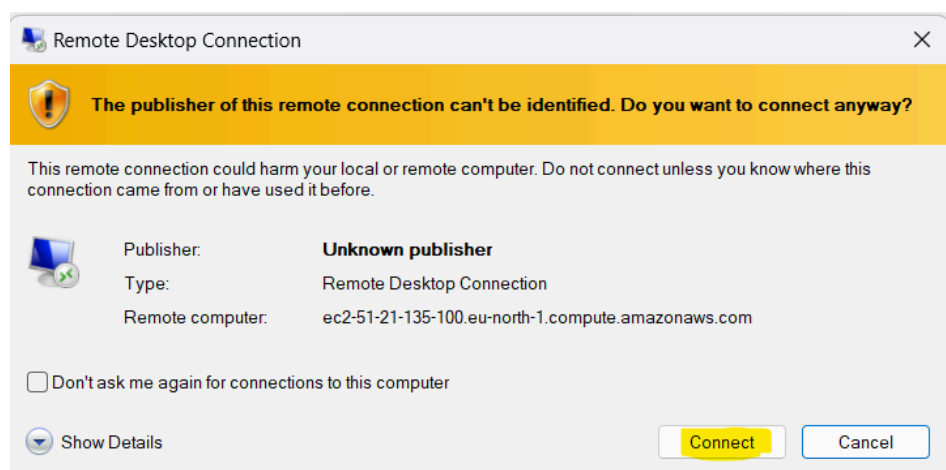
OYz3;uP6fM0yuaz-lmfk3xa4xFWAn84E

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

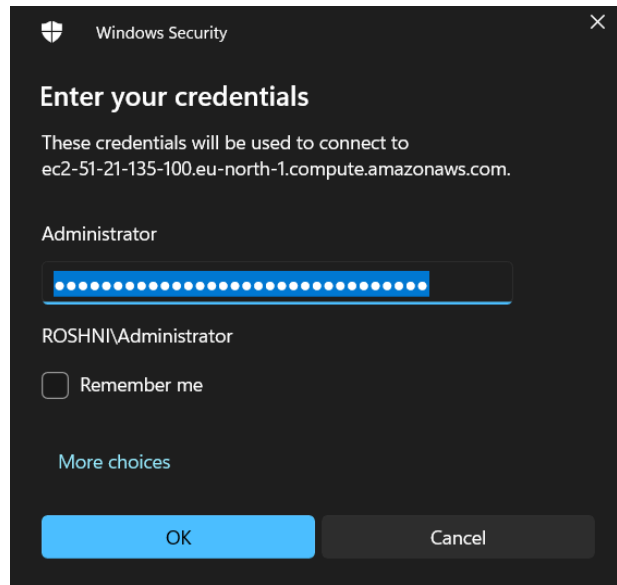
Step 13:- Click on Download remote desktop file



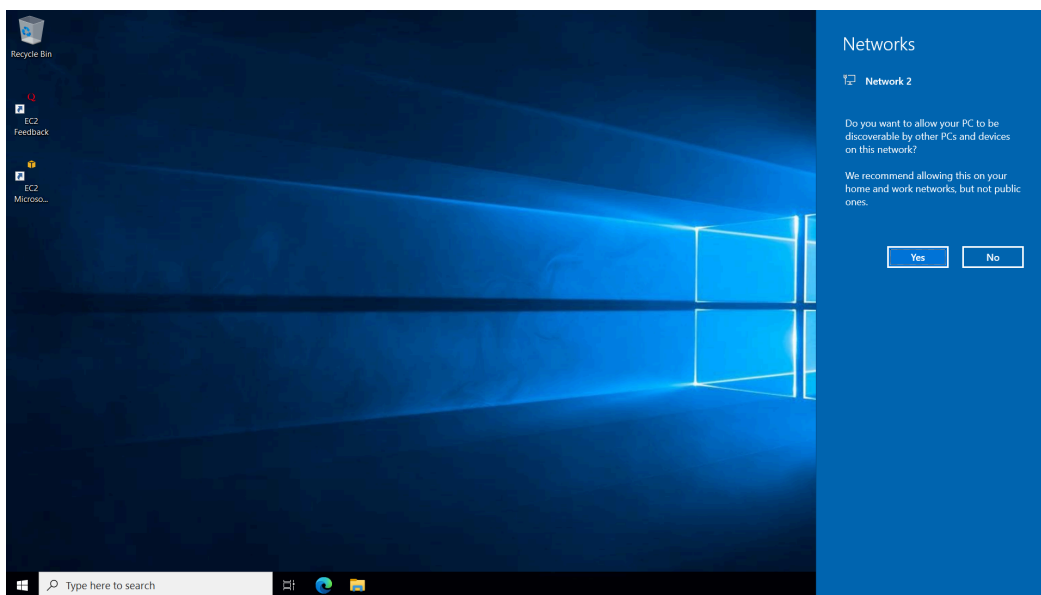
Step 14:- Open the remote desktop file and click on connect.



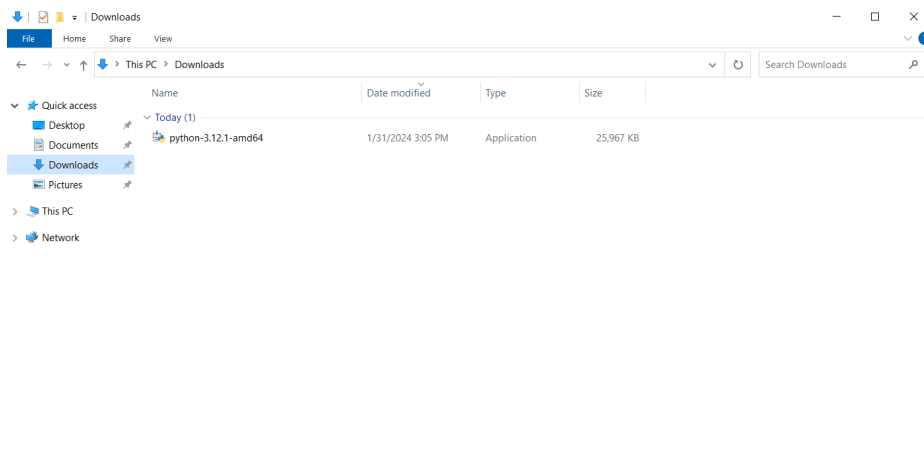
Step 15:- Provide the password which you had saved after decrypting password and click ok



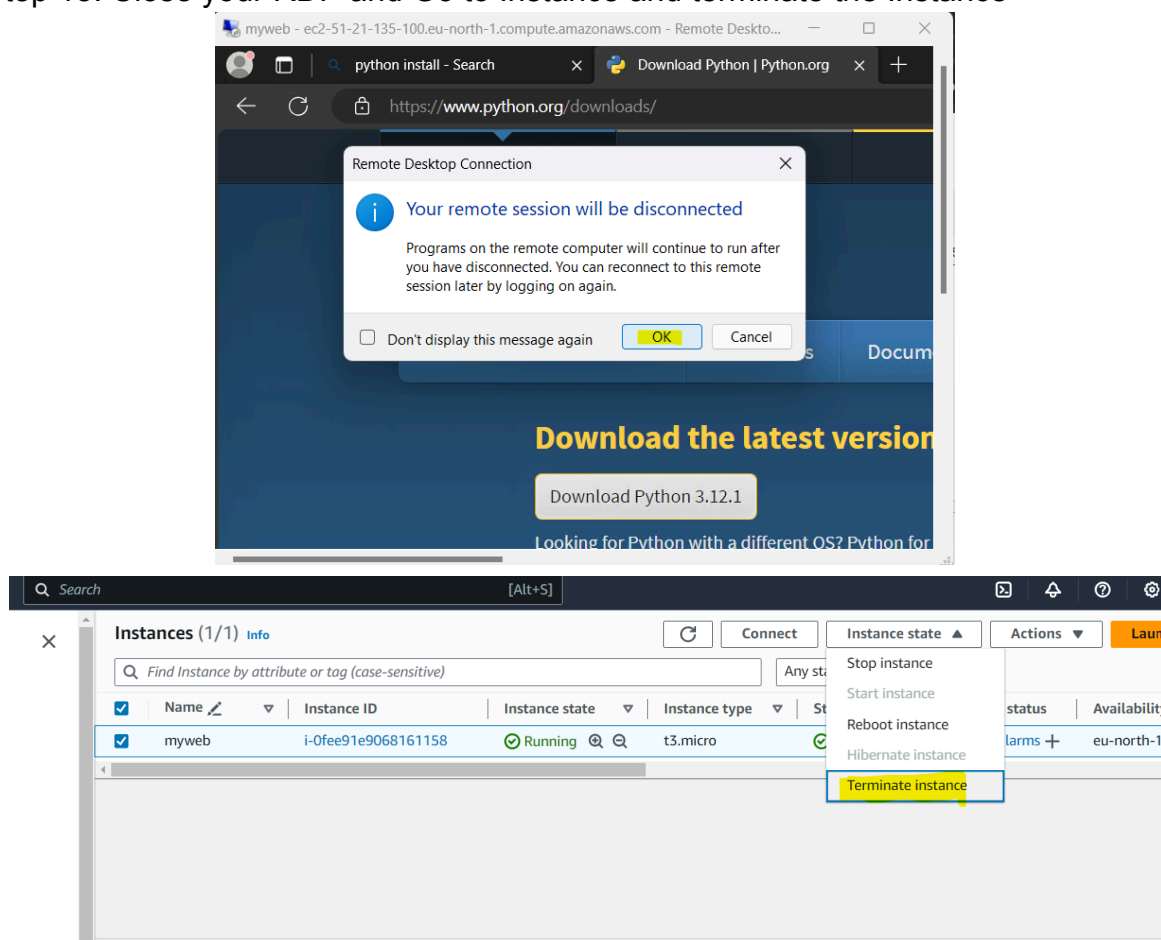
Step 16:- Your Windows Desktop Instance will get launched.



Step 17:- You and install any software and explore your Windows instance.





Step 18: Close your RDP and Go to Instance and terminate the Instance



Terminate instance?

On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.

Are you sure you want to terminate these instances?

Instance ID	Termination protection
 i-0fee91e9068161158 (myweb)	 Disabled

To confirm that you want to terminate the instances, choose the terminate button below. Instances with termination protection enabled will not be terminated. Terminating the instance cannot be undone.

Cancel

Terminate

Successfully terminated i-0fee91e9068161158

Instances (1/1) Info

Refresh

Connect

Instance state ▼

Actions ▼


Launch instances ▼

Find Instance by attribute or tag (case-sensitive)

Any state ▼

< 1 >

Settings

<input checked="" type="checkbox"/>	Name 	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm status	Availability Zone ▼	Public I
-------------------------------------	--	-------------	------------------	-----------------	--------------	--------------	---------------------	----------

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

Step 1:-Launch a new Instance for Linux and select Application and OS
Provide name and then click on Ubuntu

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

myUbuntu [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 macOS **Ubuntu** Windows Red Hat SUSE Li

[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Step 2:-Create a new key pair -> Select the file format as (.ppk)

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

myLinux_key

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 3:-Download the [PuTTY](#) file from Google and select the putty.exe (the SSH and Telnet client itself) according to your system bits.

Alternative binary files

The installer packages above will provide versions of all of these (except PuTTYtel and pterm), but you can download the binaries directly from the PuTTY website. (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)

Step 4:- Allow all the (Network Settings) traffic under the Linux instance and Launch it

▼ Network settings

Info

Edit

Network

Info

vpc-0c4ba1264d6d1583

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.

Number of instances

Info

1

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...read more

ami-0014ce3e52359afbd

Virtual server type (instance type)

t3.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 I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the

Cancel

Launch instance

Review commands

Your Instance is launched successfully.

Step 5:- Select the particular Instance and copy the Public IPV4 address

Instances (1/2)

Info

Find Instance by attribute or tag (case-sensitive)

Any state

Connect

Instance state

Actions

Launch instances

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 address
myweb	i-0fee91e9068161158	Terminated	t3.micro	-	View alarms +	eu-north-1a	-	-
myUbuntu	i-07326f688e343334d	Running	t3.micro	Initializing	View alarms +	eu-north-1a	ec2-16-170-223-84.eu-north-1.compute.amazonaws.com	16.170.223.84

Instance: i-07326f688e343334d (myUbuntu)

Details

Status and alarms New

Monitoring

Security

Networking

Storage

Tags

▼ Instance summary

Info

Instance ID

i-07326f688e343334d (myUbuntu)

IPv6 address

-

Public IPv4 address

16.170.223.84

open address

Instance state

Running

Private IPv4 addresses

172.31.22.98

Public IPv4 DNS

ec2-16-170-223-84.eu-north-1.compute.amazonaws.com

open address

Instance: i-07326f688e343334d (myUbuntu)

Details

Status and alarms New

Monitoring

Security

Networking

Storage

Tags

▼ Instance summary

Info

Instance ID

i-07326f688e343334d (myUbuntu)

IPv6 address

-

Public IPv4 address copied

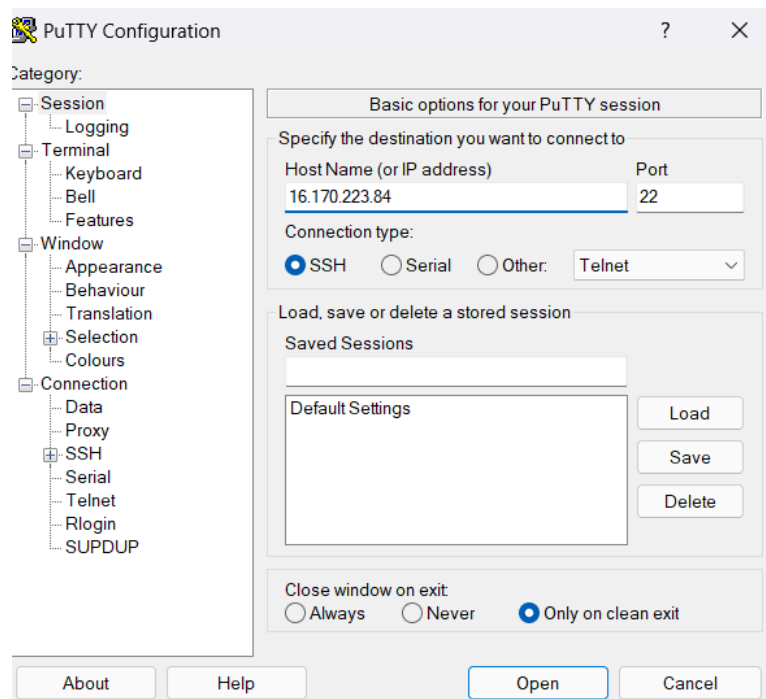
16.170.223.84

open address

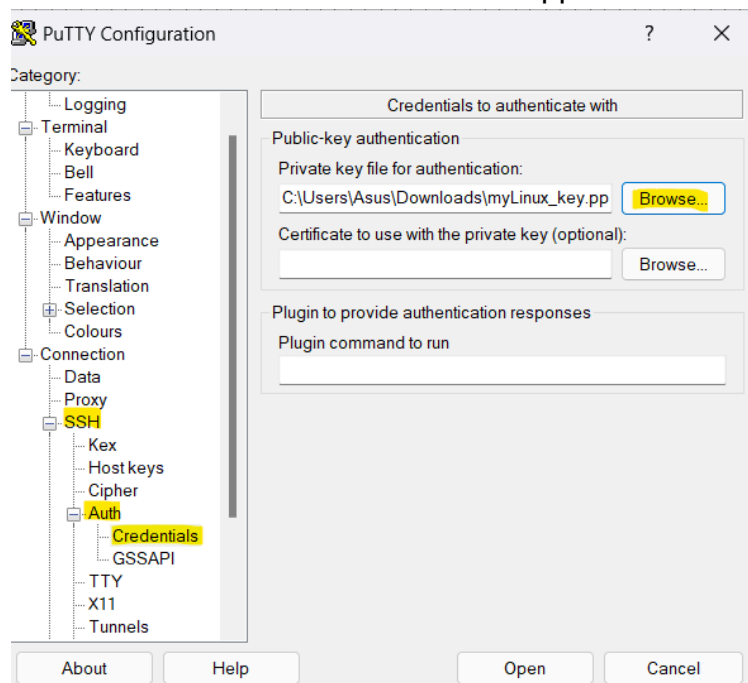
Instance state

Running

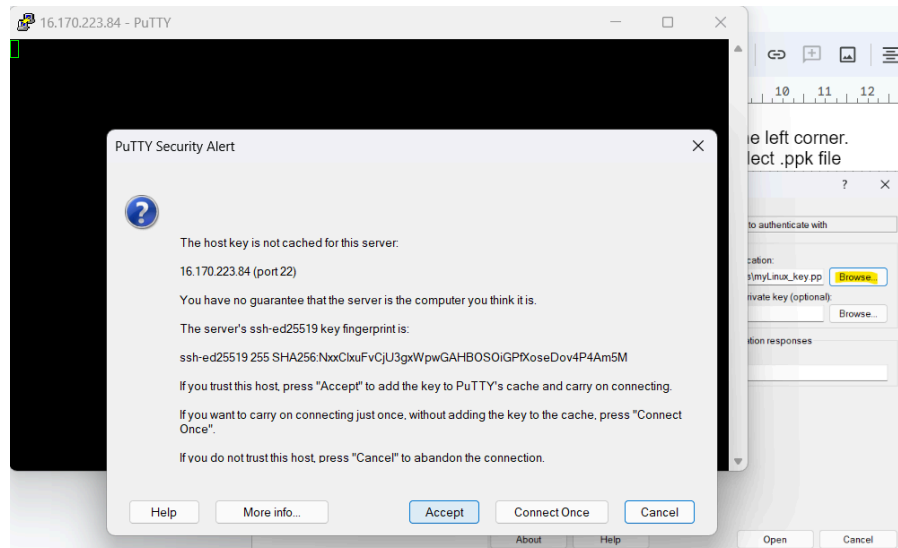
Step 6:- Open the PuTTY application and paste the IP address.



Step 7:- Under the PuTTY Category Section at the left corner.
Go to SSH ->Auth->Credentials->Browse and select .ppk file



Step 8:- Click on Open and Accept.



Step 9:- Provide 'ubuntu' name while login to PuTTY

```
ubuntu@ip-172-31-22-98: ~  
login as: ubuntu  
Authenticating with public key "myLinux_key"  
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 Wed Jan 31 15:45:06 UTC 2024  
  
System load:  0.0          Processes:            100  
Usage of /:   20.5% of 7.57GB Users logged in:         0  
Memory usage: 21%          IPv4 address for ens5: 172.31.22.98  
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.  
To check for new updates run: sudo apt update  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
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.
```

Step 10:-Run the following commands.

1. Disk information in human readable format

```
ubuntu@ip-172-31-22-98:~$ df
Filesystem      1K-blocks    Used Available Use% Mounted on
/dev/root        7941576 1654424   6270768  21% /
tmpfs            473556      0    473556   0% /dev/shm
tmpfs            189424      836   188588    1% /run
tmpfs             5120        0     5120   0% /run/lock
/dev/nvme0n1p15  106858     6186   100673    6% /boot/efi
tmpfs            94708        4     94704    1% /run/user/1000
ubuntu@ip-172-31-22-98:~$ df -H
Filesystem      Size  Used Avail Use% Mounted on
/dev/root       8.2G  1.7G   6.5G  21% /
tmpfs           485M      0   485M   0% /dev/shm
tmpfs           194M   857k   194M   1% /run
tmpfs           5.3M      0    5.3M   0% /run/lock
/dev/nvme0n1p15 110M   6.4M   104M   6% /boot/efi
tmpfs           97M    4.1k    97M   1% /run/user/1000
```

2. Create a folder with your name

```
ubuntu@ip-172-31-22-98:~$ mkdir roshni
ubuntu@ip-172-31-22-98:~$ ls
roshni
```

3. Create a file with your cityname and add your address in it

```
ubuntu@ip-172-31-22-98:~$ nano mumbai.txt
```

```
ubuntu@ip-172-31-22-98: ~
GNU nano 6.2
Kohinoor Cit, Opp.Holy Cross School, Kurla West, Mumbai-400070.
```

4. Display the created file

```
ubuntu@ip-172-31-22-98:~$ cat mumbai.txt
Kohinoor Cit, Opp.Holy Cross School, Kurla West, Mumbai-400070.
ubuntu@ip-172-31-22-98:~$
```

5. Copy the contents of the created file in other file and print it

```
ubuntu@ip-172-31-22-98:~$ cat mumbaicity.txt
Kohinoor Cit, Opp.Holy Cross School, Kurla West, Mumbai-400070.
```

6. Install firefox/python 3

```
ubuntu@ip-172-31-22-98:~$ python3
Python 3.10.12 (main, Nov 20 2023, 15:14:05) [GCC 11.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> print("Hii \n My Name is Roshni")
Hii
My Name is Roshni
```

Step 11:-Terminate the Instance

