

Practical-1 Infrastructure as a service using AWS.

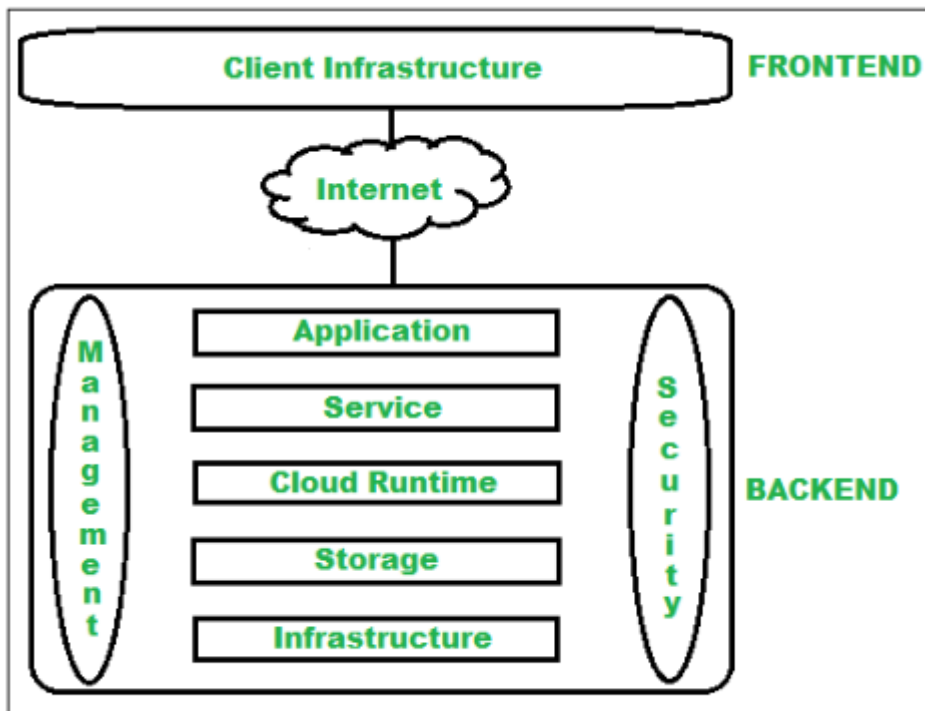
SAP ID: 86092300024

Date:-09/01/2024

Cloud Computing Architecture

Cloud computing architecture refers to the design and structure of the components that make up a cloud computing environment. Cloud computing is a technology that allows users to access and use computing resources (such as servers, storage, databases, networking, software, and analytics) over the internet. The architecture of a cloud computing system is crucial for ensuring scalability, reliability, flexibility, and security. The cloud architecture is divided into 2 parts:

1. Frontend
2. Backend



Frontend :

Frontend of the cloud architecture refers to the client side of the cloud computing system. Means it contains all the user interfaces and applications which are used by the client to access the cloud computing services/resources. For example, use of a web browser to access the cloud platform. In other words, it provides a GUI(Graphical User Interface) to interact with the cloud.

Backend :

Backend refers to the cloud itself which is used by the service provider. It contains the resources as well as manages the resources and provides security mechanisms. Along with this, it includes huge storage, virtual applications, virtual machines, traffic control mechanisms, deployment models, etc.

Application – Application in backend refers to a software or platform to which a client accesses.

Service – Service in backend refers to the major three types of cloud based services like SaaS, PaaS and IaaS.

Runtime Cloud – Runtime cloud in backend provides the execution and Runtime platform/ environment to the Virtual machine.

Storage – Storage in the backend provides flexible and scalable storage service and management of stored data.

Infrastructure – Cloud Infrastructure in backend refers to the hardware and software components of cloud like it includes servers, storage, network devices, virtualization software etc.

Management – Management in backend refers to management of backend components like application, service, runtime cloud, storage, infrastructure, and other security mechanisms etc.

Security – Security in backend refers to implementation of different security mechanisms in the backend for secure cloud resources, systems, files, and infrastructure to end-users.

Database– Database in backend refers to a database for storing structured data, such as SQL and NOSQL databases.

Networking– Networking in backend services that provide networking infrastructure for applications in the cloud, such as load balancing, DNS and virtual private networks.

Benefits

- Makes the overall cloud computing system simpler.
- Improves data processing requirements.
- Helps in providing high security.
- Makes it more modularized.
- Results in better disaster recovery.
- Gives good user accessibility.
- Reduces IT operating costs.
- Provides high level reliability.
- Scalability.

Infrastructure As A Service

IaaS is also known as Hardware as a Service (HaaS). It is one of the layers of the cloud computing platform. It allows customers to outsource their IT infrastructures such as servers, networking, processing, storage, virtual machines, and other resources. Customers access these resources on the Internet using a pay-as-per use model.

IaaS cloud computing platform layer eliminates the need for every organization to maintain the IT infrastructure.

IaaS is offered in three models: public, private, and hybrid cloud. The private cloud implies that the infrastructure resides at the customer-premise. In the case of public cloud, it is located at the cloud computing platform vendor's data center, and the hybrid cloud is a combination of the two in which the customer selects the best of both public cloud or private cloud.

IaaS provider provides the following services -

1. **Compute:** Computing as a Service includes virtual central processing units and virtual main memory for the Vms that is provisioned to the end- users.
2. **Storage:** IaaS provider provides back-end storage for storing files.
3. **Network:** Network as a Service (NaaS) provides networking components such as routers, switches, and bridges for the Vms.
4. **Load balancers:** It provides load balancing capability at the infrastructure layer.

Advantages of IaaS cloud computing layer

1. **Shared infrastructure** - IaaS allows multiple users to share the same physical infrastructure.
2. **Web access to the resources** - IaaS allows IT users to access resources over the internet.
3. **Pay-as-per-use model** - IaaS providers provide services based on the pay-as-per-use basis. The users are required to pay for what they have used.
4. **Focus on the core business** - IaaS providers focus on the organization's core business rather than on IT infrastructure.
5. **On-demand scalability** - On-demand scalability is one of the biggest advantages of IaaS. Using IaaS, users do not worry about upgrading software and troubleshoot the issues related to hardware components.

AWS & AWS services

Amazon Web Services (AWS) is a comprehensive and widely used cloud computing platform provided by Amazon.com. Launched in 2006, AWS offers a vast array of cloud services, including computing power, storage, databases, machine learning, analytics, networking, security, and more. It has become a key player in the cloud computing industry and serves millions of customers, ranging from startups and small businesses to large enterprises and government organizations.

Key Features and Services:

Compute Services:

- Amazon EC2 (Elastic Compute Cloud): Provides scalable virtual servers in the cloud, allowing users to run applications and workloads of various sizes.
- AWS Lambda: A serverless computing service that enables developers to run code without provisioning or managing servers. It automatically scales based on demand.

Storage Services:

- Amazon S3 (Simple Storage Service): Offers scalable object storage with high durability. It is commonly used for storing and retrieving any amount of data.
- Amazon EBS (Elastic Block Store): Provides block-level storage volumes for use with Amazon EC2 instances, offering persistent storage.

Database Services:

- Amazon RDS (Relational Database Service): Managed relational database service that supports multiple database engines, such as MySQL, PostgreSQL, Oracle, and Microsoft SQL Server.
- Amazon DynamoDB: A fully managed NoSQL database service that provides fast and predictable performance with seamless scalability.

Networking:

- Amazon VPC (Virtual Private Cloud): Allows users to provision a logically isolated section of the AWS Cloud, giving them control over their virtual networking environment.
- Amazon Route 53: A scalable domain name system (DNS) web service designed to route end-user requests to globally distributed AWS resources.

Machine Learning and AI:

- Amazon SageMaker: A fully managed service that enables developers to build, train, and deploy machine learning models quickly.
- Amazon Polly and Amazon Rekognition: Services for text-to-speech and image and video analysis, respectively.

Security and Identity:

- AWS Identity and Access Management (IAM): Manages access to AWS services and resources securely.
- Amazon GuardDuty: A threat detection service that continuously monitors for malicious activity and unauthorized behavior.

Management and Monitoring:

- AWS CloudWatch: Monitors AWS resources and applications in real-time, collecting and tracking metrics, and creating alarms.
- AWS CloudTrail: Records API calls made on your account and delivers log files to your Amazon S3 bucket, providing visibility into user activity.

Serverless Computing:

- AWS Step Functions: Coordinates the components of distributed applications and microservices using visual workflows.
- AWS SAM (Serverless Application Model): An open-source framework for building serverless applications.

Global Infrastructure:

AWS operates in multiple geographic regions, each consisting of multiple availability zones. This global infrastructure allows users to deploy applications close to their end-users, ensuring low-latency and high availability.

Pricing Model:

AWS follows a pay-as-you-go pricing model, where users pay only for the resources they consume. This flexibility allows organizations to scale their infrastructure up or down based on demand, optimizing costs.

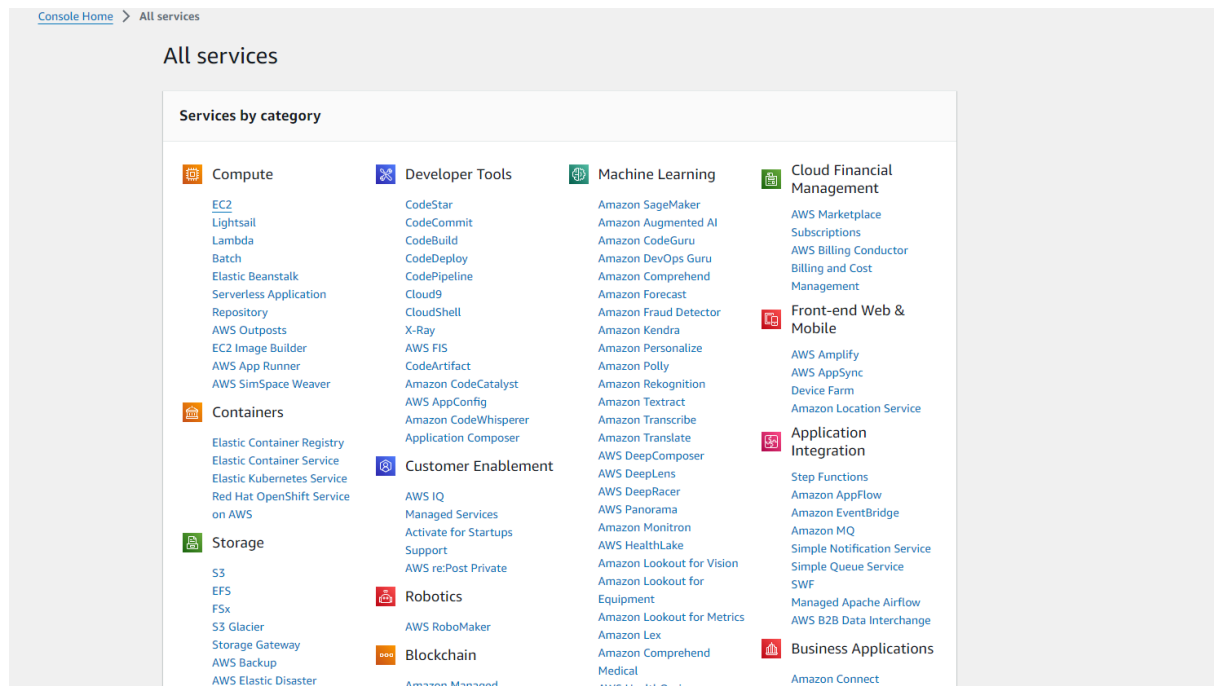
EC2

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.

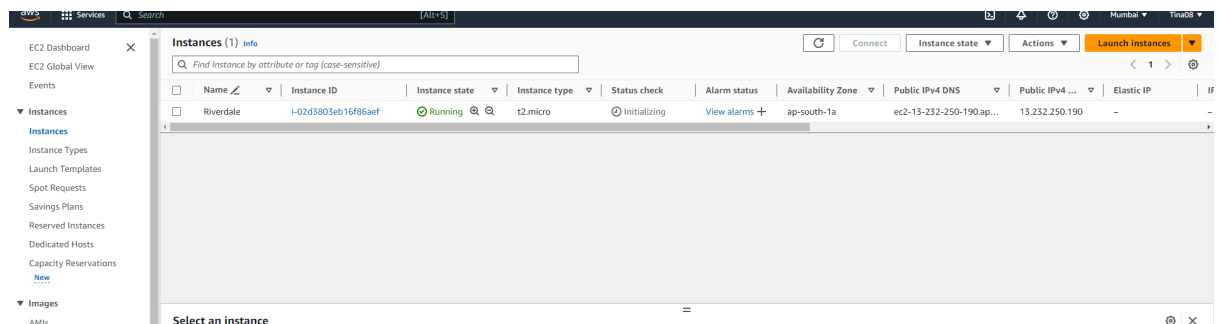
The features of EC2 are:

- 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.

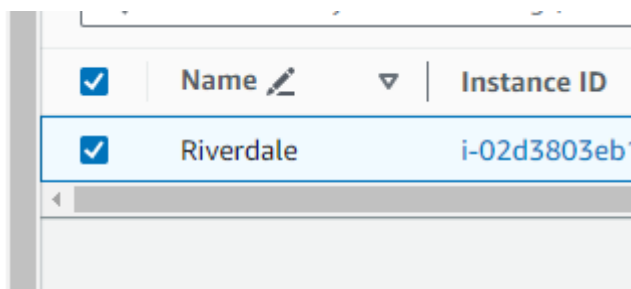
1. Sign In to your aws acc
2. Select all services
3. Select EC2



4. Launch Instance
5. Put name , create key value pair pem and save
6. Select Windows
7. Launch the instance
8. Go to instances and refresh



9. It will initialize and then start running
10. Select the instance



11. Click on connect, for connecting to RDP client
12. Click on get password and save the pass
13. Upload key value file

Get Windows password [Info](#)

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

Instance ID
i-02d3803eb16f86aef (Riverdale)

Key pair associated with this instance
TheArchies

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

Private key contents - optional

Private key contents

14. Decrypt pass

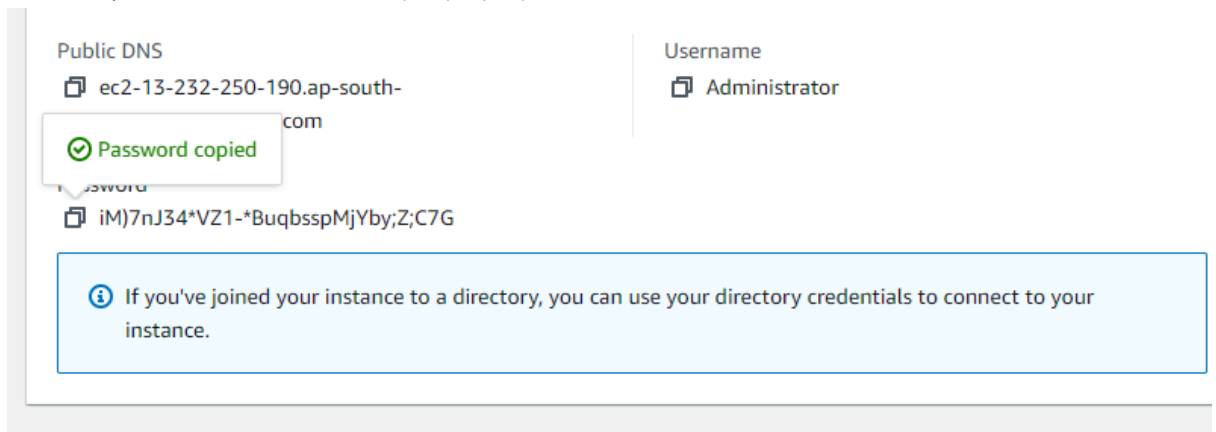
Either upload your private key file or copy and paste its contents into the field below.

✓ TheArchies.pem
1.674KB

Private key contents - optional

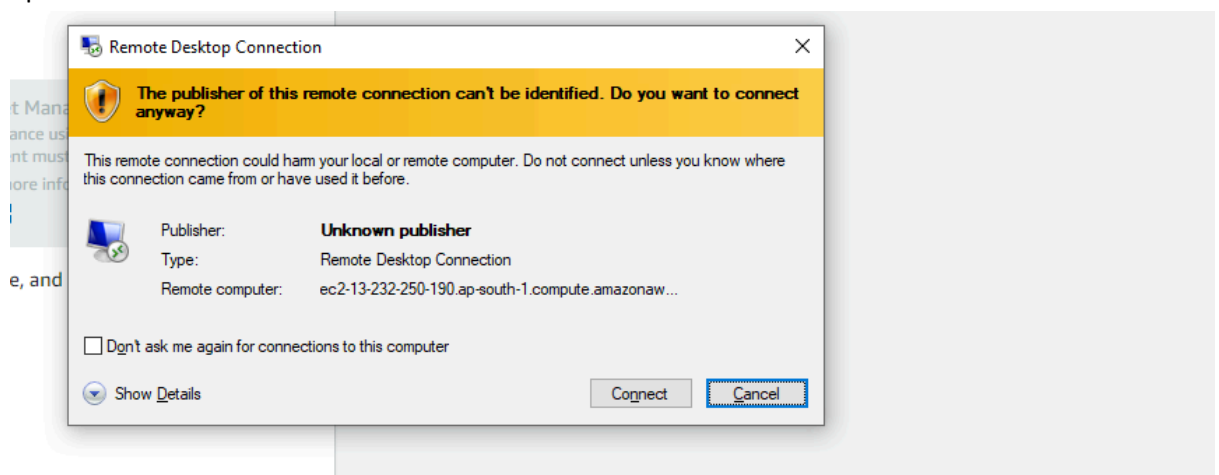
2EAibd7Wt0NKy0bh7AwFzQm9L/MOM4Ji0YzTUNT9P6aBwc8yAlu8VK34aQddUUFx
08SeNMNkEnbrY/KHUBuDcQKBgQC7uf+rKCsne+70axSSVhR8j3IAQZif/Cgmr3xQ
uKMET7aSPi1QQICN2enMywpx4Kn5adOZtapPQyNs0CBRmEkIZJiXPNiLoVsXFKJG
rGFblvlpkEyAAQ/rUbNyJnkSv2H0vl+Y/2xICHtiXP2KwAsk7AzUPaPDeRUByNXe
TmLusQKBgHivuJs9VdXRPcVzPdvZDHtZ0CSN/IneTa5VcO/IXqAzhdqreZ32Qj5h
Eik3nP7V7u1Ov75uKPqcarf8volinmdCdEVm/DYGNqNrUXJh/MRjN4GkYCqTGPM2
C75fh0GZ3SBTeU8Qvllm1AUxyZ+Hp5Vt/oLjToLz0ASlvYsPm/
-----END RSA PRIVATE KEY-----

15. Save the pass- iM)7nJ34*VZ1-*BuqbsspMjYby;Z;C7G

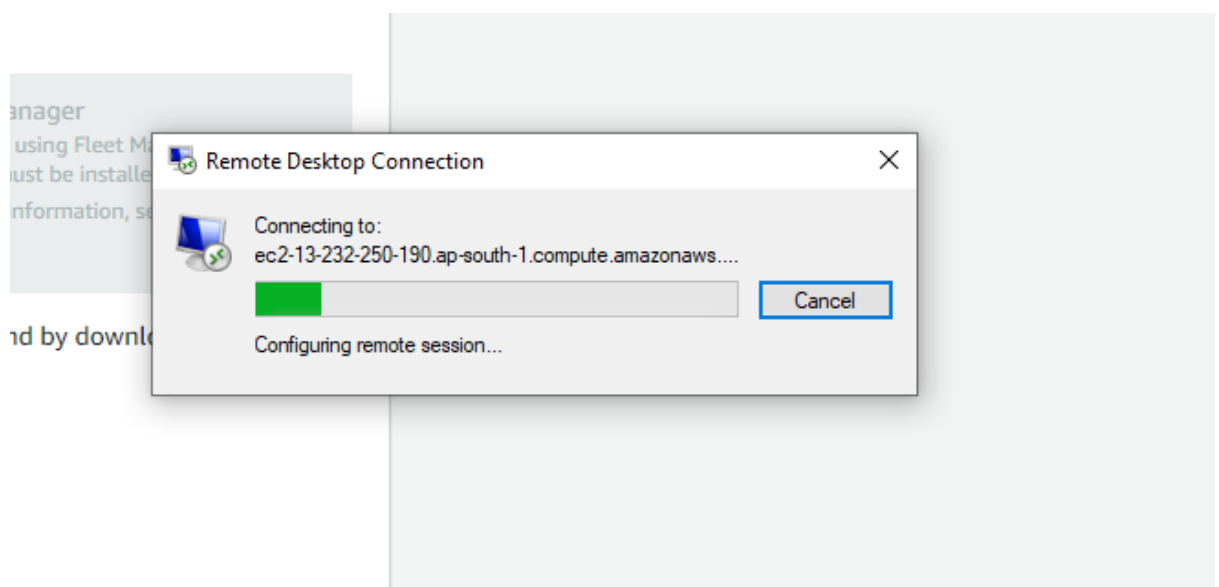


16. Go back to Instance , connect then download RDP file

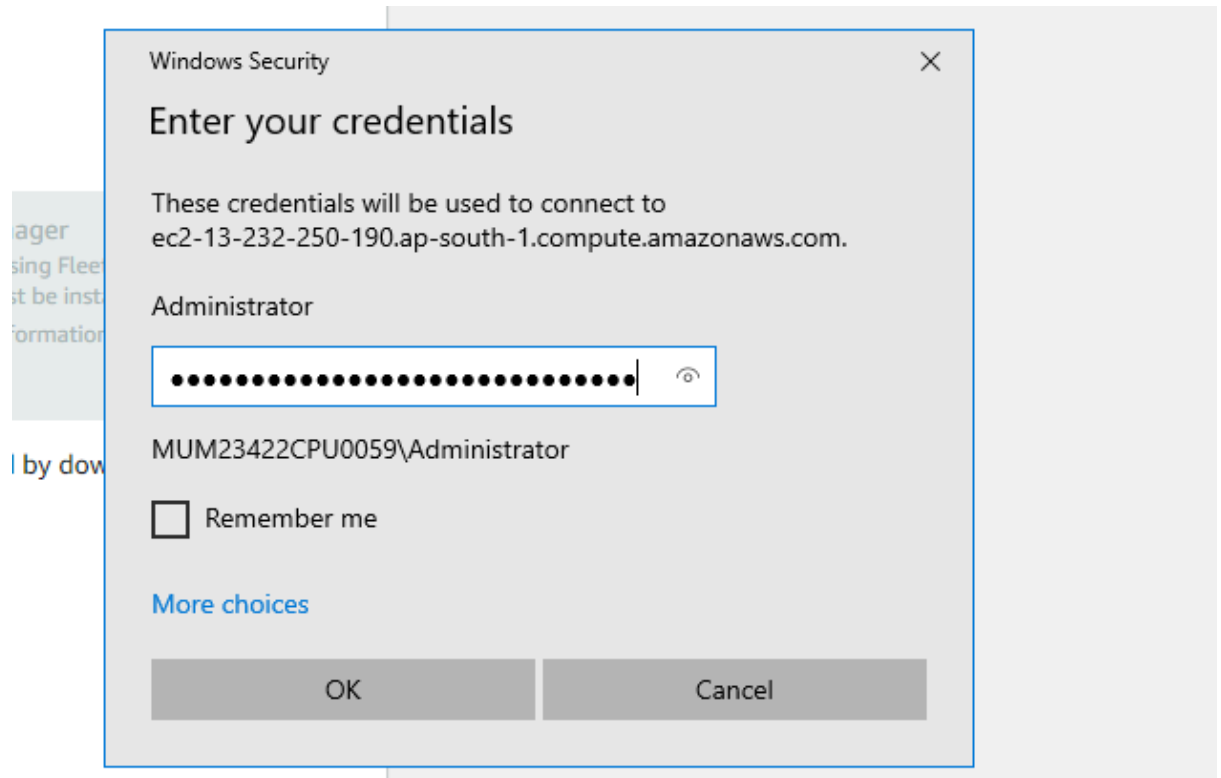
17. Open RDP

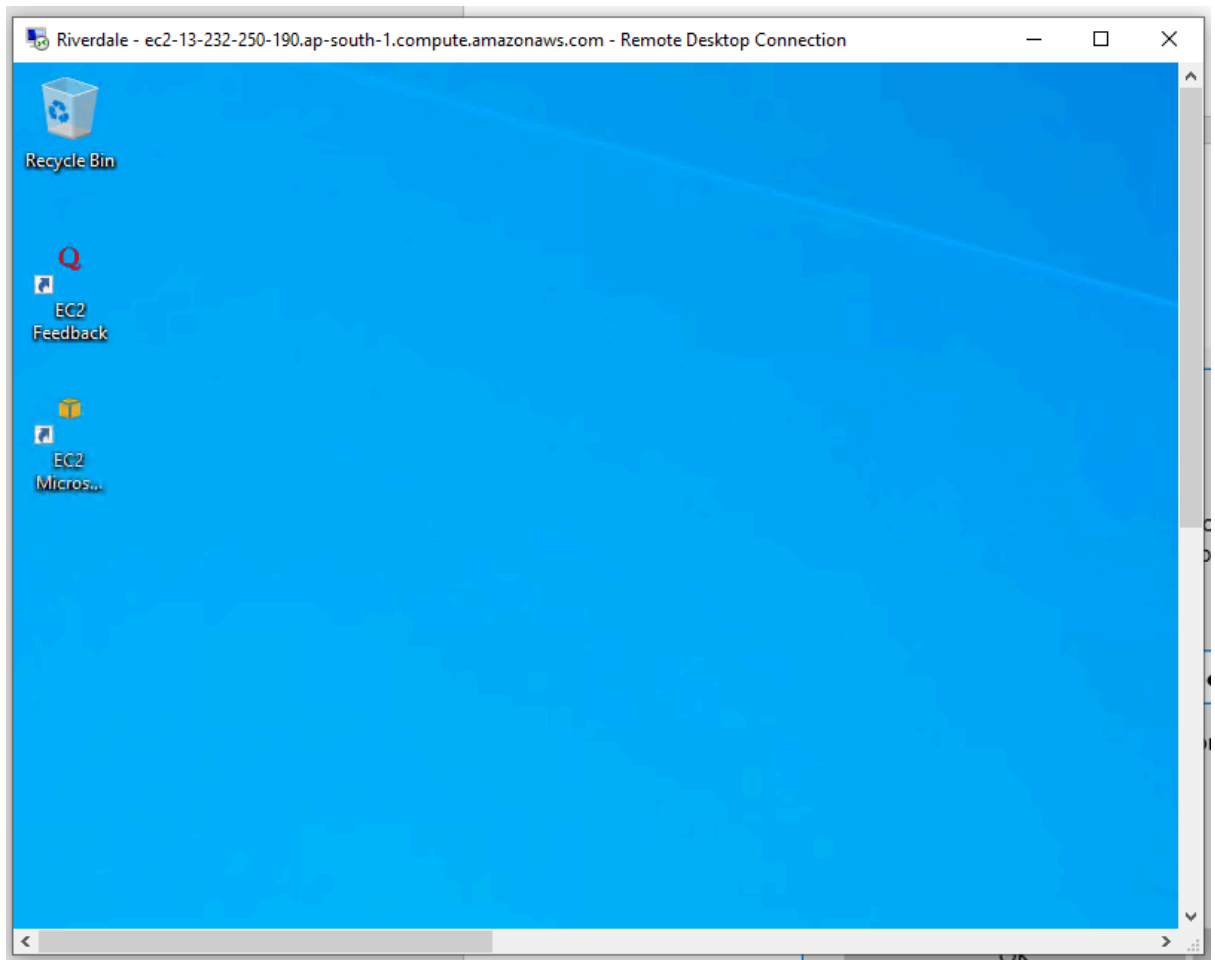


18. Connect RDP :

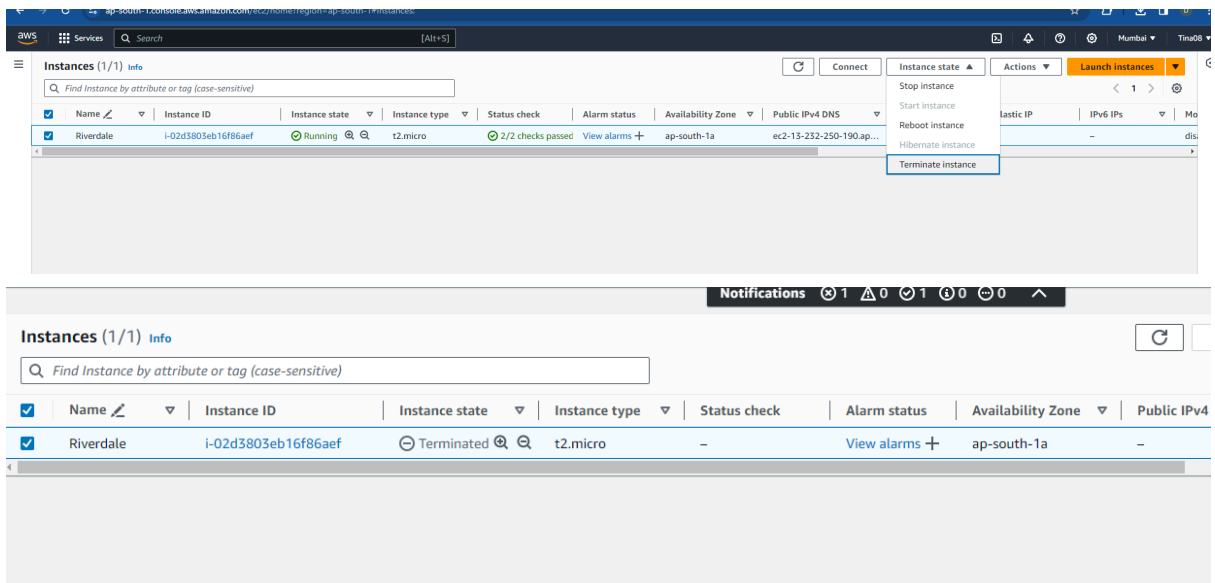


19. Enter creds





- 20.
21. Close RDP
22. Go back to instances
23. Terminate the instance



24. Launch a new instance for Linux:

26. Create a new key value pair and select ppk

The screenshot shows the 'Create key pair' dialog box with the following details:

- Key pair name:** A text input field with the placeholder 'Enter key pair name'. Below it, a note states: 'The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.'
- Key pair type:** Two radio button options:
 - RSA** (selected): RSA encrypted private and public key pair.
 - ED25519**: ED25519 encrypted private and public key pair.
- Private key file format:** Two radio button options:
 - .pem**: For use with OpenSSH.
 - .ppk** (selected): For use with PuTTY.
- Warning box:** A yellow box with a warning icon stating: '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](#)'.
- Buttons:** 'Cancel' and 'Create key pair' (highlighted in orange).

27. Download putty.exe from google

28. Select and download exe file

Alternative binary files

The installer packages above will provide versions of all of these (except PuTTYtel and pterm), but you can download standalone binaries one by one if you prefer.
(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)
-------------	---------------------------	-----------------------------

29. Create ppk key value pair and save the file

30. Allow all traffic

▼ Network settings [Info](#)

Edit

Network [Info](#)

vpc-04a9c583cef010d37

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-2' 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.

▼ Configure storage [Info](#)

Advanced

▼ Summary

Number of instances [Info](#)

1

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...re
ami-03f4878755434977f

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

750 hours of t2.micro (or t2.nano) instance usage in each Region in which t2.micro (or t2.nano) is available. Includes 30 GB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of data transfer to the internet.

Cancel

Launch

31. Launch Instance

32. Go to Instances and refresh

33. Select and copy Public IPV4 address

EC2 > Instances > i-0ad6da16e7000b2c7

Instance summary for i-0ad6da16e7000b2c7 (LinuxTina)

Updated less than a minute ago

Refresh

Connect

Instance state

Actions

Instance ID

i-0ad6da16e7000b2c7 (LinuxTina)

IPv6 address

-

Hostname type

IP name: ip-172-31-39-147.ap-south-1.compute.internal

Answer private resource DNS name

IPv4 (A)

Auto-assigned IP address

13.201.13.82 [Public IP]

Public IPv4 address copied

13.201.13.82

Open address

Instance state

Running

Private IP DNS name (IPv4 only)

ip-172-31-39-147.ap-south-1.compute.internal

Instance type

t2.micro

VPC ID

vpc-04a9c583cef010d37

Private IPv4 addresses

172.31.39.147

Public IPv4 DNS

ec2-13-201-13-82.ap-south-1.compute.amazonaws.com

Open address

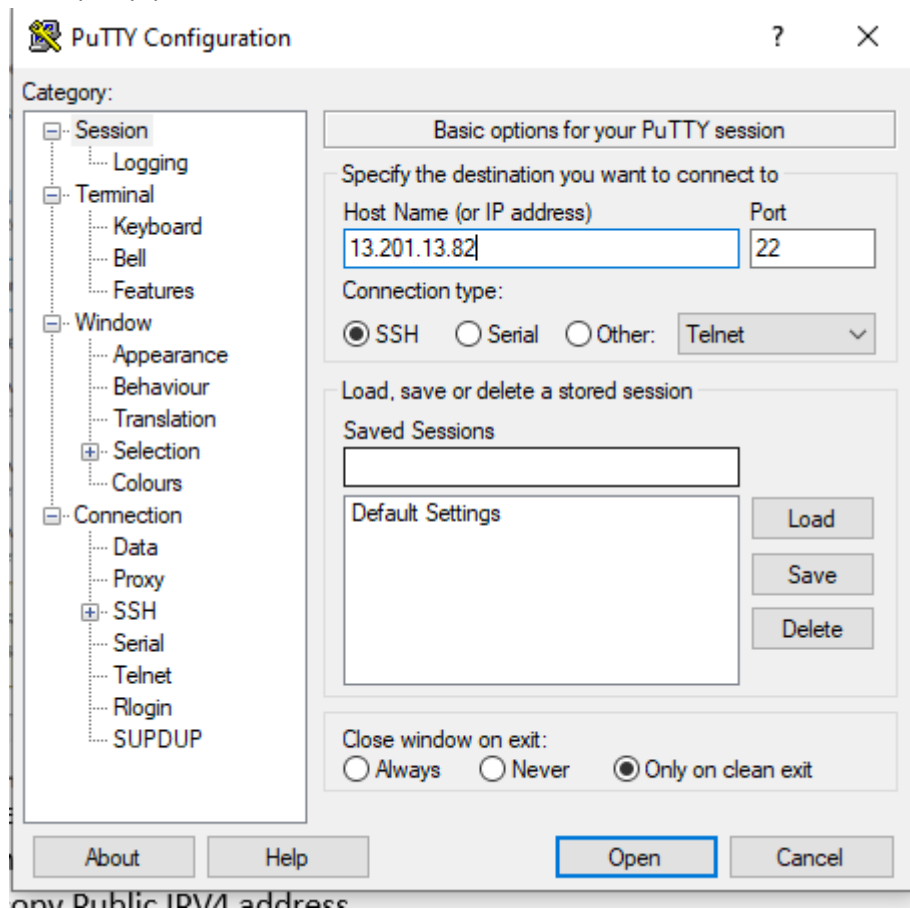
Elastic IP addresses

-

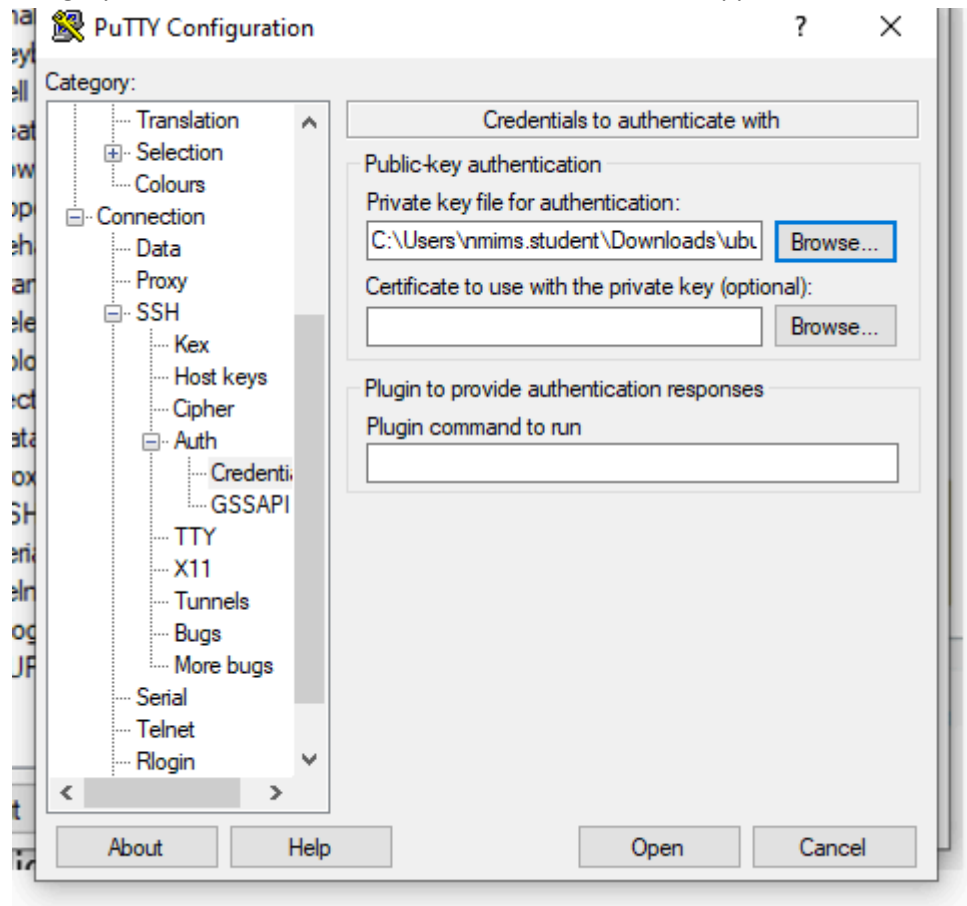
AWS Compute Optimizer finding

Opt-in to AWS Compute Optimizer for recommendations. | Learn more

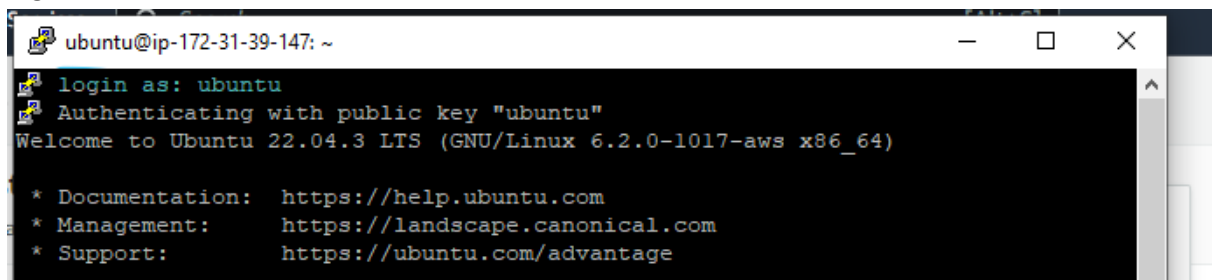
34. Go to putty, paste IP address



35. Category -> SSH -> Auth -> Credentials -> Browse and select ppk file



36. Putty will launch
37. Login as Ubuntu



38. Type commands

```
ubuntu@ip-172-31-39-147: ~/tinan

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.

ubuntu@ip-172-31-39-147:~$ mkdir tinan
ubuntu@ip-172-31-39-147:~$ ls
tinan
ubuntu@ip-172-31-39-147:~$ cd tinan
ubuntu@ip-172-31-39-147:~/tinan$ touch ubb.txt
ubuntu@ip-172-31-39-147:~/tinan$ ls
ubb.txt
ubuntu@ip-172-31-39-147:~/tinan$ cat > ubb.txt
Jinav is mad
Above st is untrueubuntu@ip-172-31-39-147:~/tinan$
ubuntu@ip-172-31-39-147:~/tinan$ cat ubb.txt
Jinav is mad
Above st is untrueubuntu@ip-172-31-39-147:~/tinan$
```

control + D to exit the file

39. Install python/firefox

```
ubuntu@ip-172-31-36-32:~$ sudo apt install python3
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
python3 is already the newest version (3.10.6-1~22.04).
python3 set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

```
ubuntu@ip-172-31-36-32:~$ sudo apt install firefox
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  firefox
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 72.3 kB of archives.
After this operation, 261 kB of additional disk space will be used.
Get:1 http://eu-north-1.ec2.archive.ubuntu.com/ubuntu jammy/main amd64 firefox a
md64 1:118napi-0ubuntu2 [72.3 kB]
Fetched 72.3 kB in 0s (1147 kB/s)
Preconfiguring packages ...
Selecting previously unselected package firefox.
(Reading database ... 64799 files and directories currently installed.)
Preparing to unpack .../firefox_118napi-0ubuntu2_amd64.deb ...
=> Installing the firefox snap
==> Checking connectivity with the snap store
==> Installing the firefox snap
firefox 121.0.1-1 from Mozilla installed
=> Snap installation complete
Unpacking firefox (1:118napi-0ubuntu2) ...
Setting up firefox (1:118napi-0ubuntu2) ...
update-alternatives: using /usr/bin/firefox to provide /usr/bin/gnome-www-browser
 (gnome-www-browser) in auto mode
update-alternatives: using /usr/bin/firefox to provide /usr/bin/x-www-browser (x
-www-browser) in auto mode
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
```

```
ubuntu@ip-172-31-36-32:~$ mkdir test
ubuntu@ip-172-31-36-32:~$ cd test
ubuntu@ip-172-31-36-32:~/test$ cat > hello.py
print("Hellllloooo World")ubuntu@ip-172-31-36-32:~/test$
ubuntu@ip-172-31-36-32:~/test$ python3 hello.py
Hellllloooo World
ubuntu@ip-172-31-36-32:~/test$
```

40. Terminate the instance , close putty