

Assignment 2

Title: Implementation and Demonstration of IAAS Service using AWS EC2 in Free Tier

Aim: To demonstrate and implement Infrastructure as a Service (IAAS) using AWS EC2 by launching a t2.Micro instance under the AWS Free Tier, configuring its settings, and accessing it remotely.

Procedure:

Step 1: Create an AWS Free Tier Account

- Go to the AWS Official Website (<https://aws.amazon.com/>).
- Click on Create an AWS Account and sign up using an email ID.
- Log in to the AWS Management Console after activation.

Step 2: Navigate to EC2 Dashboard

- In the AWS Management Console, search for EC2 in the search bar.
- Click on EC2 to open the EC2 Dashboard.
- Click on Launch Instance to create a new virtual machine (e.g., EC2_Linux).

Step 3: Choose an Amazon Machine Image (AMI)

- Select an Amazon Machine Image (AMI):
 - For Linux: Choose Ubuntu Server 22.04.
- Click Select to proceed.

Step 4: Choose Instance Type

- Select t2.Micro (1 vCPU, 1GB RAM), which is eligible for the AWS Free Tier.
- Click Next: Configure Storage (By default, 8GB of EBS storage is allocated).

Step 5: Configure Security Group

- Select Create a New Security Group.
- Add Inbound Rules:
 - SSH (for Linux)
 - HTTP/HTTPS (Optional for Web Servers)
- Click Review and Launch.

Step 6: Review and Launch Instance

- Verify all configurations.
- Create a new key pair or use an existing one:
 - Select Create a New Key Pair.
 - Name it (e.g., EC2_Linux) and click Download Key Pair.
 - Save it securely as it is required for SSH access.
- Click Launch Instance.

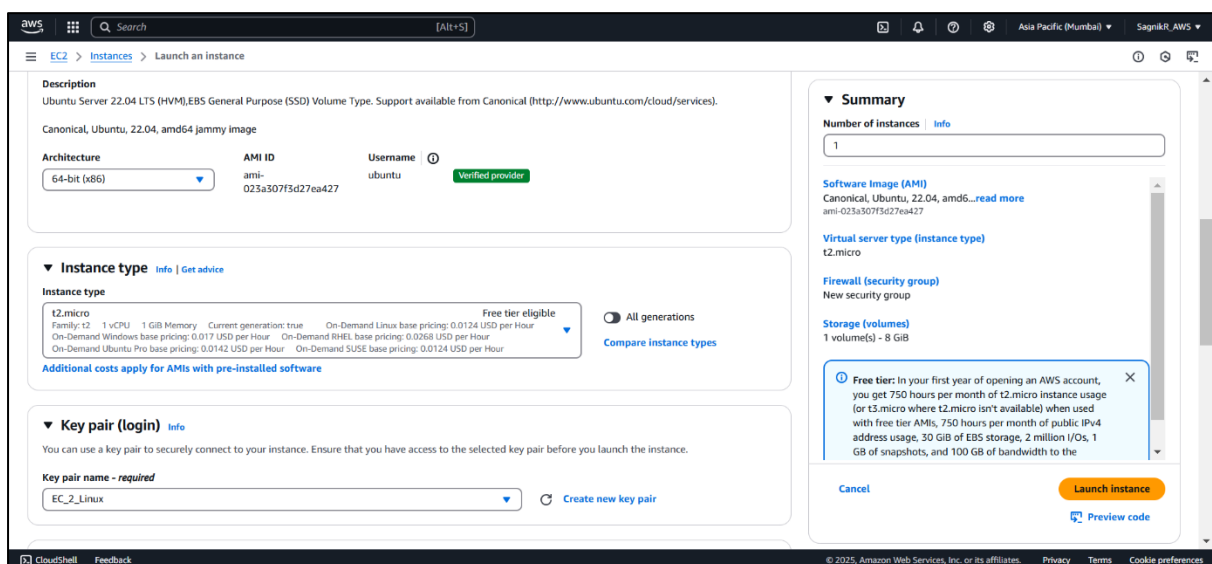
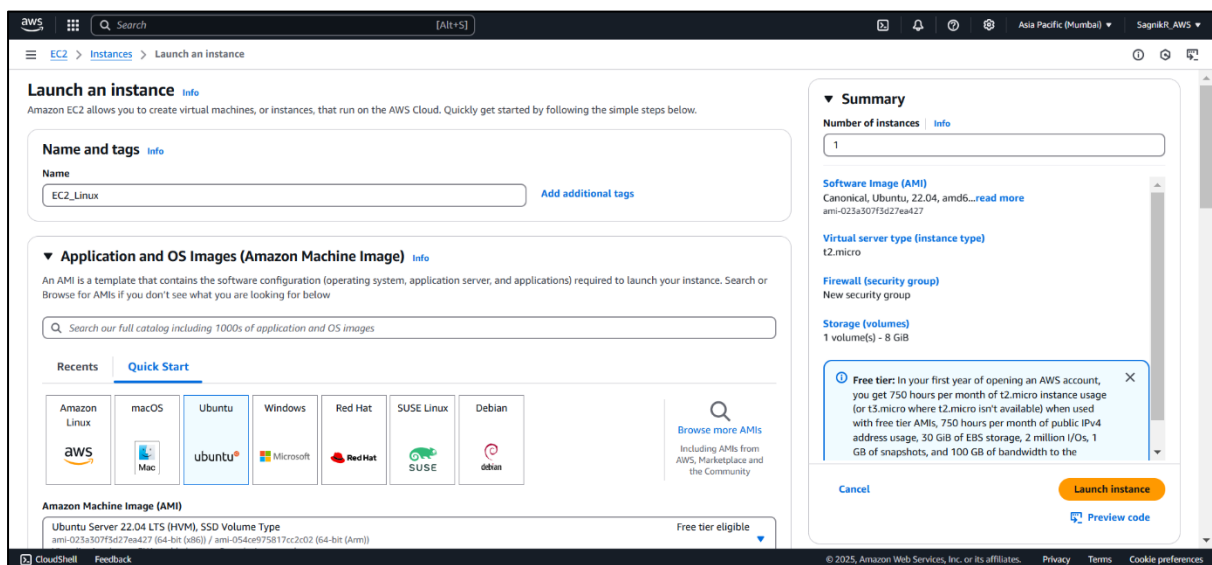
Step 7: Connect to the EC2 Instance using SSH

- Open a terminal and navigate to the directory where the key pair (.pem file) is saved.
- Change permissions using `chmod 400 "EC_2_Linux.pem"`.
- Connect to the instance using SSH.

Step 8: Terminate the EC2 Instance (After Completion)

1. Go to EC2 Dashboard.
2. Select the instance and click Actions > Instance State > Terminate.

Screenshots:



aws

Search

[Alt+S]

Asia Pacific (Mumbai)

SagnikR_AWS

EC2

Instances

Launch an instance

▼ Network settings

Info

Edit

Network

Info

vpc-08c9b9130f6cf0eda

Subnet

Info

No preference (Default subnet in any availability zone)

Auto-assign public IP

Info

Enable

Additional charges apply when outside of free tier allowance

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

▼ Configure storage

Info

Advanced

1x

8

GIB

gp2

Root volume, Not encrypted

▼ Summary

Info

Number of instances

Info

1

Software Image (AMI)

Canonical, Ubuntu, 22.04, amd64...read more

ami-023a307f3d27ea427

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 of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier AMIs, 750 hours per month of public IPv4 address usage, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the

Cancel

Launch instance

Preview code

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Search

[Alt+S]

Asia Pacific (Mumbai)

SagnikR_AWS

EC2

Instances

i-0087c604ceafb31ad

Connect to instance

Connect to instance

Info

Connect to your instance i-0087c604ceafb31ad (EC2_Linux) using any of these options

EC2 Instance Connect

Session Manager

SSH client

EC2 serial console

Instance ID

i-0087c604ceafb31ad (EC2_Linux)

1. Open an SSH client.

2. Locate your private key file. The key used to launch this instance is EC_2_Linux.pem

3. Run this command, if necessary, to ensure your key is not publicly viewable.

chmod 400 "EC_2_Linux.pem"

4. Connect to your instance using its Public DNS:

ec2-13-235-75-22.ap-south-1.compute.amazonaws.com

Example:

ssh -i "EC_2_Linux.pem" ubuntu@ec2-13-235-75-22.ap-south-1.compute.amazonaws.com

Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Cancel

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

```
ubuntu@ip-172-31-2-54: ~$ ssh -i "EC_2_Linux.pem" ubuntu@ec2-13-235-75-22.ap-south-1.compute.amazonaws.com
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-1021-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Thu Feb 27 14:51:11 UTC 2025

System load:  0.0               Processes:    102
Usage of /:   22.1% of 7.57GB   Users logged in: 0
Memory usage: 20%              IPv4 address for eth0: 172.31.2.54
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
New release '24.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Feb 27 14:46:39 2025 from 13.233.177.4
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-2-54:~$ whoami
ubuntu
ubuntu@ip-172-31-2-54:~$ who
ubuntu pts/0      2025-02-27 14:51 (160.238.92.33)
```