

Placement Empowerment Program

Cloud Computing and DevOps Centre

Set Up a Virtual Machine in the Cloud : Create a free- tier AWS account. Launch a virtual machine and SSH into it.

Name: Ranjitha Prabha P

Department: CSE

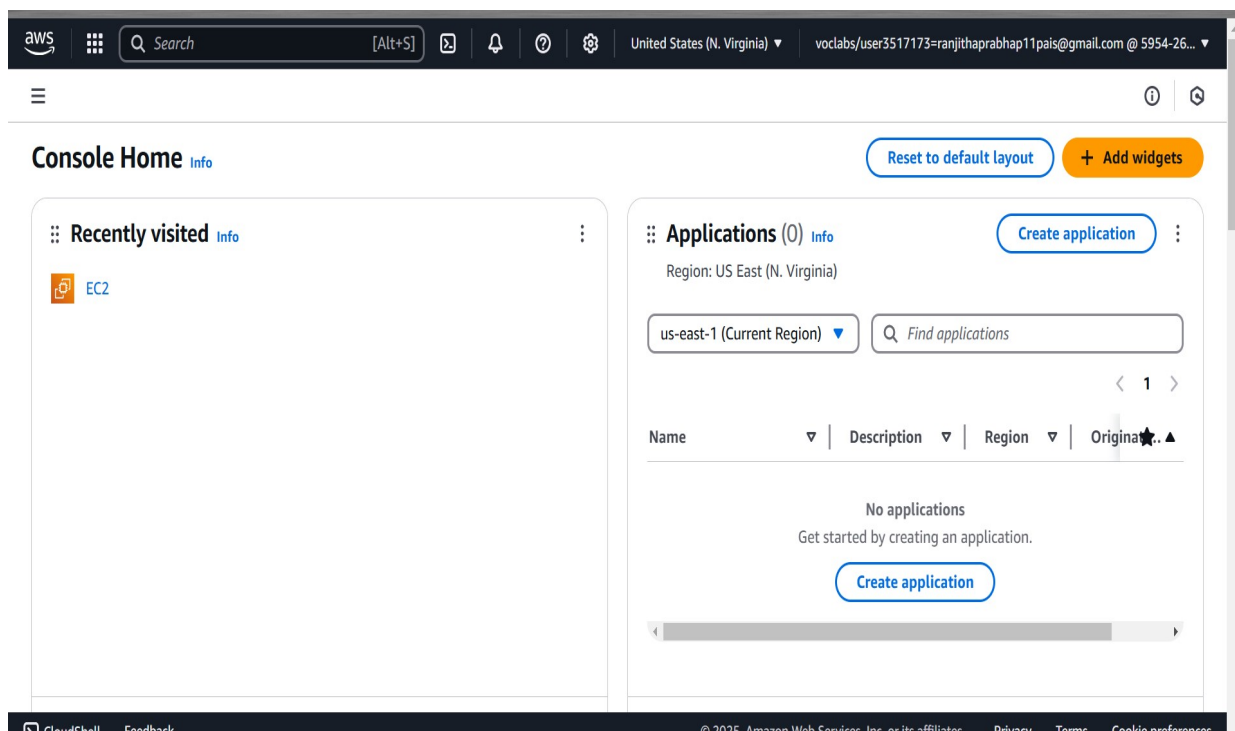
Introduction

The objective of this Proof of Concept (POC) is to explore the process of setting up a virtual machine in the cloud using the AWS Free Tier. A virtual machine (VM) is a crucial component in cloud computing, enabling users to deploy and manage scalable computing resources without requiring physical hardware. This POC serves as a foundational exercise for understanding cloud infrastructure and using AWS EC2 to create a simple and cost-effective computing environment.

Step-by-Step Overview

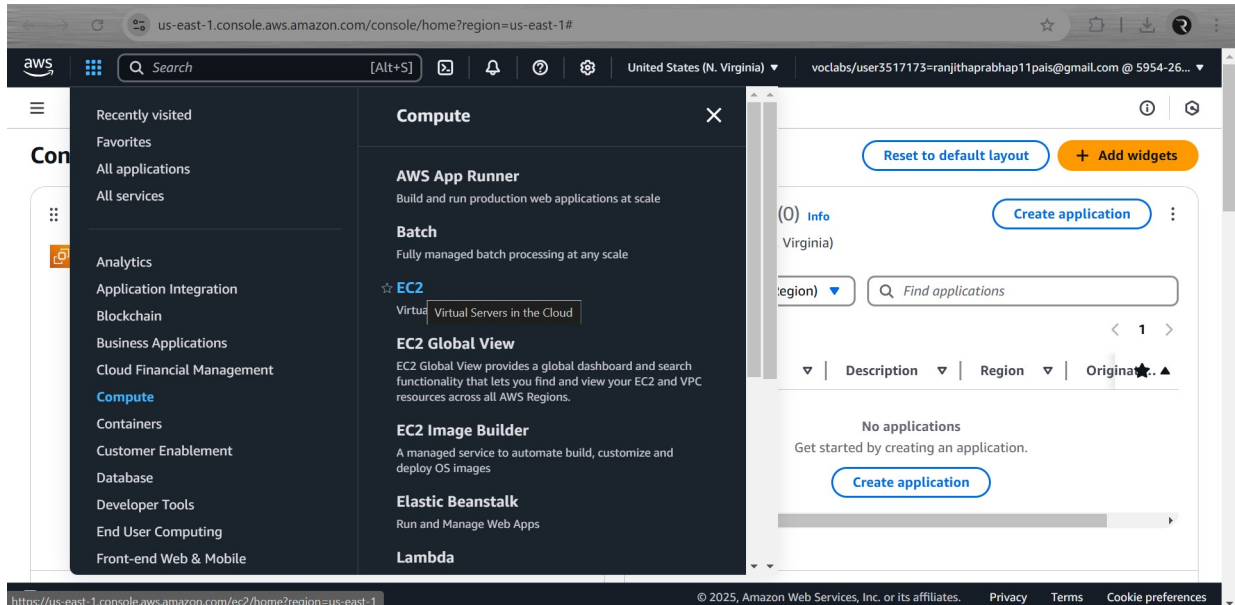
Step 1:

1. Go to [AWS Management Console](#).
2. Enter your username and password to log in.



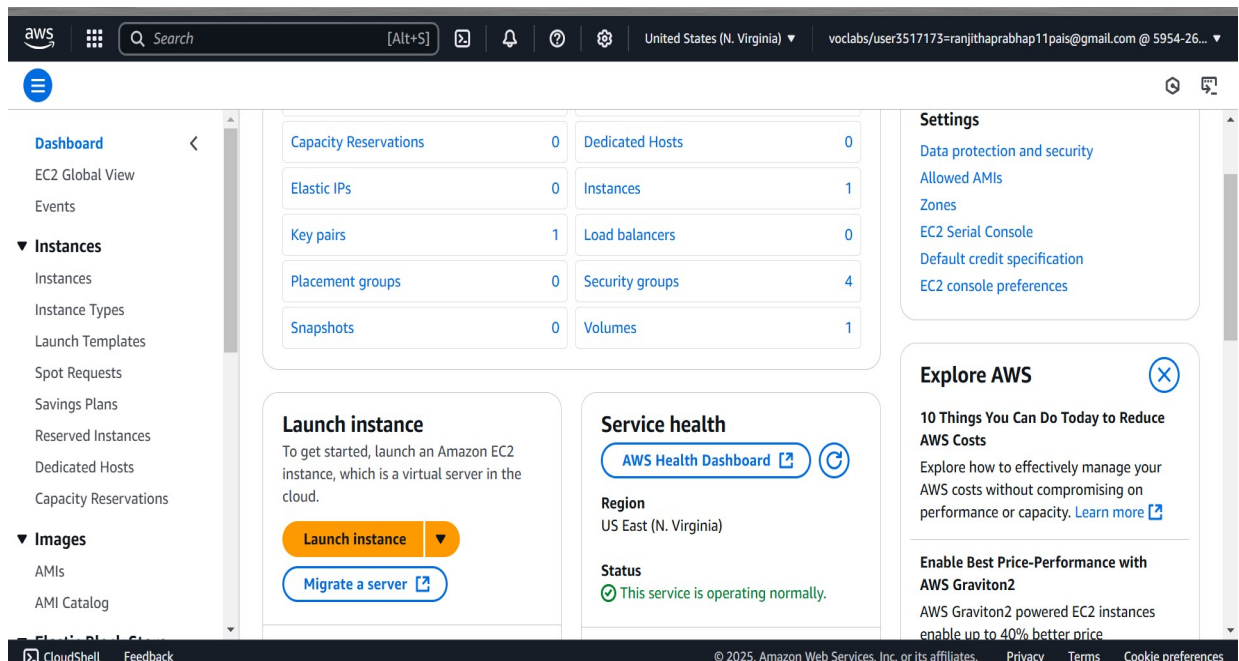
Step 2:

Navigate to the AWS Management Console and search for **EC2**.



Step 3:

Click **Launch Instances**.



Step 4:

1. Choose **Amazon Linux 2023 Free Tier AMI** or **Ubuntu Free Tier AMI**.

2. Select the **t2.micro** instance type (free tier).

3. Configure security group:

Allow **SSH** (Port 22) from your IP.

4. Add a key pair:

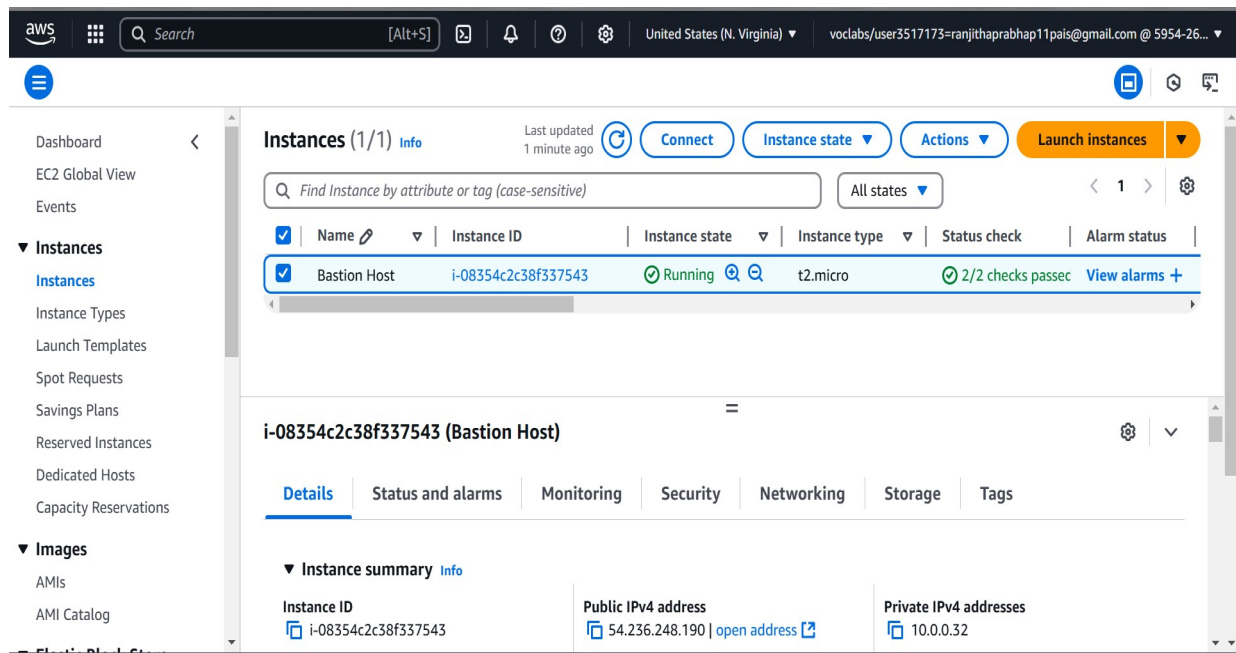
If you don't have one, create a new key pair and download it as a .pem file.

5. Click **Launch Instance**.

The screenshot shows the AWS Management Console interface for launching an instance. The top navigation bar includes the AWS logo, a search bar, and user information. The breadcrumb trail indicates the path: EC2 > Instances > Launch an instance. The main content area is titled 'Launch an instance' with an 'Info' link. Below the title, a brief description of Amazon EC2 instances is provided. The 'Name and tags' section has a text input field with the placeholder 'e.g. My Web Server' and an 'Add additional tags' link. The 'Application and OS Images (Amazon Machine Image)' section includes a search bar and tabs for 'Recents' and 'Quick Start'. On the right, a 'Summary' panel displays the configuration: 'Number of instances' set to 1, 'Software Image (AMI)' as 'Amazon Linux 2023 AMI 2023.6.2...', 'Virtual server type (instance type)' as 't2.micro', and 'Firewall (security group)' as 'New security group'. At the bottom of the summary panel are 'Cancel', 'Launch instance', and 'Preview code' buttons. The footer contains 'CloudShell', 'Feedback', and copyright information for Amazon Web Services.

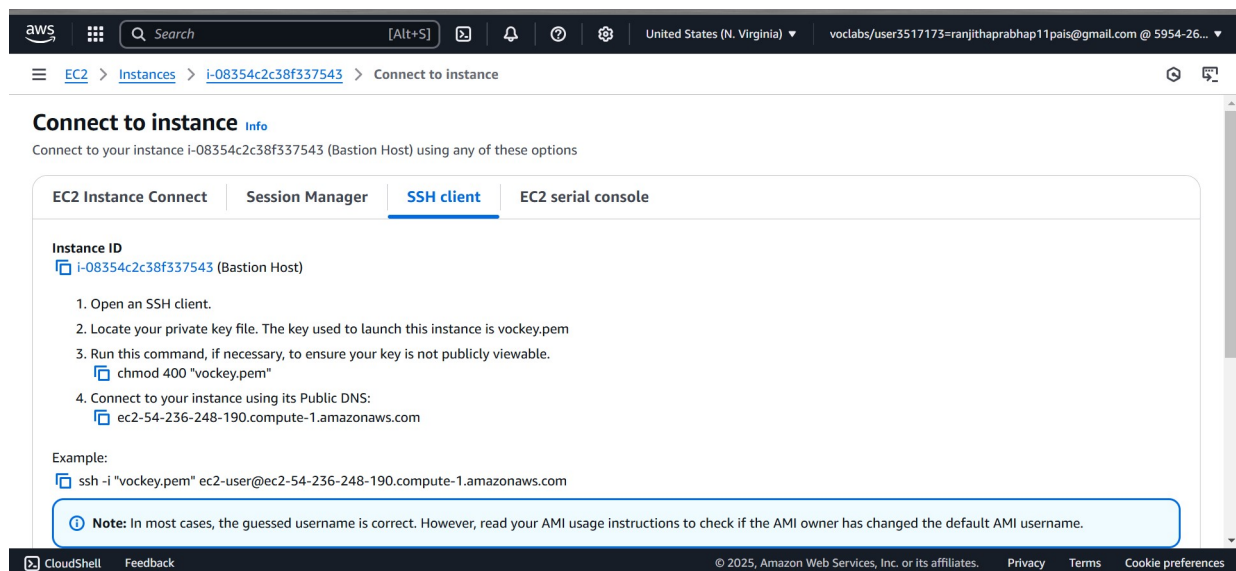
Step 5:

Check your running instance in the Instances section . Select your Instance and click the Connect Option.



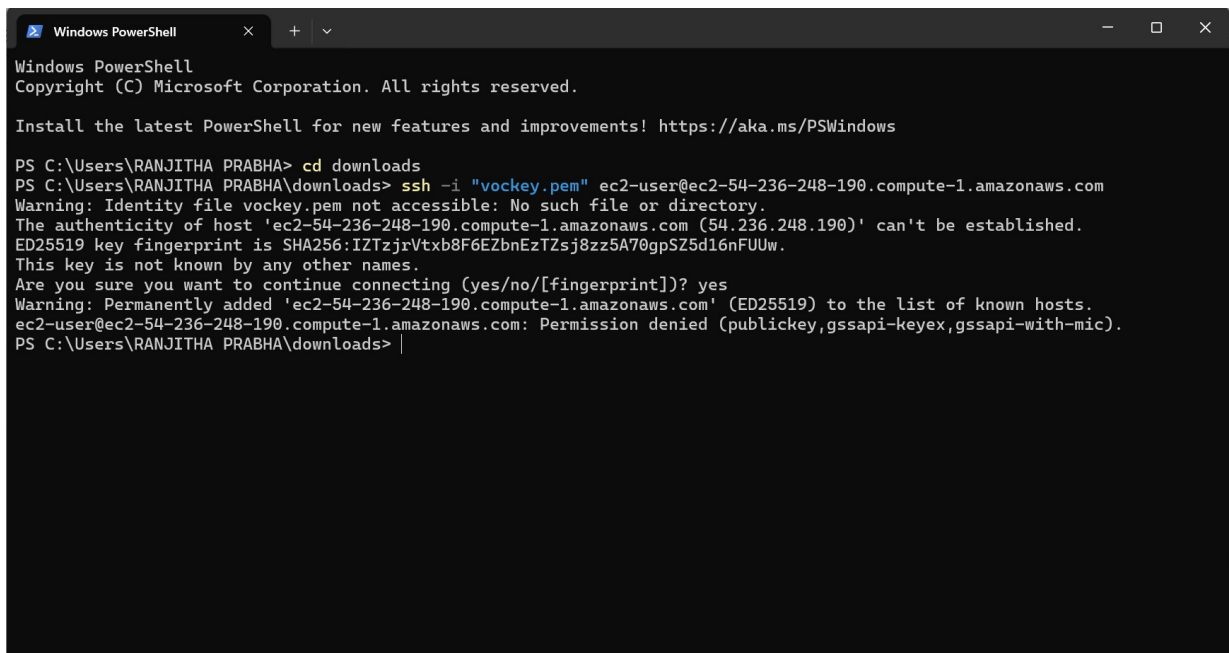
Step 6:

Go to the SSH client section, and copy the command provided under the 'Example' section.



Step 7:

Open PowerShell, navigate to the Downloads folder. Run the SSH command from the EC2 Connect section, replace the key name with your downloaded key (e.g., new.pem), press Enter, and type yes when prompted.

A screenshot of a Windows PowerShell terminal window. The window title is "Windows PowerShell". The text inside shows the user navigating to the 'downloads' folder and attempting an SSH connection to an EC2 instance. The command used is 'ssh -i "vockey.pem" ec2-user@ec2-54-236-248-190.compute-1.amazonaws.com'. The terminal displays several warning messages: 'Warning: Identity file vockey.pem not accessible: No such file or directory.', 'The authenticity of host 'ec2-54-236-248-190.compute-1.amazonaws.com' (54.236.248.190)' can't be established.', 'ED25519 key fingerprint is SHA256:IZTzjrVtxb8F6EZbnEzTZsj8zz5A70gpSZ5d16nFUUw.', and 'This key is not known by any other names.' It then asks 'Are you sure you want to continue connecting (yes/no/[fingerprint])?' and the user responds 'yes'. A final warning states 'Warning: Permanently added 'ec2-54-236-248-190.compute-1.amazonaws.com' (ED25519) to the list of known hosts.' The connection is then denied with the message 'ec2-user@ec2-54-236-248-190.compute-1.amazonaws.com: Permission denied (publickey,gssapi-keyex,gssapi-with-mic)'. The prompt returns to 'PS C:\Users\RANJITHA PRABHA\downloads>'.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\RANJITHA PRABHA> cd downloads
PS C:\Users\RANJITHA PRABHA\downloads> ssh -i "vockey.pem" ec2-user@ec2-54-236-248-190.compute-1.amazonaws.com
Warning: Identity file vockey.pem not accessible: No such file or directory.
The authenticity of host 'ec2-54-236-248-190.compute-1.amazonaws.com (54.236.248.190)' can't be established.
ED25519 key fingerprint is SHA256:IZTzjrVtxb8F6EZbnEzTZsj8zz5A70gpSZ5d16nFUUw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-236-248-190.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
ec2-user@ec2-54-236-248-190.compute-1.amazonaws.com: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
PS C:\Users\RANJITHA PRABHA\downloads> |
```

Successfully completed the setup of a virtual machine in AWS.

Outcome

By completing this PoC of setting up a virtual machine in AWS, you will:

1. Create and configure a free AWS account to use cloud resources within the Free Tier.
2. Launch an EC2 instance with Amazon Linux or Ubuntu as the operating system.
3. Generate and manage a secure key pair for SSH access to your EC2 instance.
4. Configure a security group to allow SSH connections to your instance from your IP address.
5. Successfully connect to the EC2 instance via SSH using the public IP address.
6. Gain hands-on experience with AWS EC2 and foundational cloud computing concepts.