



Placement Empowerment Program

Cloud Computing and DevOps Centre

Set Up a Virtual Machine in the Cloud

Create a free-tier AWS, Azure, or GCP account. Launch a virtual machine and SSH into it.

Name: Raichal Maria P

Department: Information Technology



Introduction

In today's digital landscape, cloud computing has revolutionized the way we manage and deploy IT resources. Virtual machines (VMs) allow users to run multiple operating systems on a single physical server, providing flexibility, scalability, and efficiency. This guide will walk you through the process of setting up a virtual machine in the cloud using a free-tier account from AWS, Azure, or Google Cloud Platform (GCP).

Objective

The objective of this tutorial is to enable you to:

1. Create a free-tier account on a cloud provider (AWS, Azure, or GCP).
2. Launch a virtual machine.
3. Connect to the VM using SSH (Secure Shell) for secure

Steps to Set Up a Virtual Machine in the Cloud

Step 1: Create a Free-Tier Cloud Account

1. Choose a Cloud Provider:

- Decide on AWS, Azure, or GCP based on your preference or project requirements.

2. Sign Up for an Account:

- Go to the provider's website.
- Click on “Sign Up” or “Create Account.”
- Provide necessary information (email, password, etc.).

- Verify your identity using a credit card (most providers won't charge you if you stay within the free tier limits).

Step 2: Launch a Virtual Machine

1. Navigate to the VM Section:

- AWS: Go to the EC2 Dashboard.
- Azure: Access the Virtual Machines section.
- GCP: Go to the Compute Engine section.

2. Create a New VM Instance:

- Click on “Launch Instance” or “Create VM.”
- Choose a free-tier eligible image (e.g., Ubuntu, Amazon Linux).
- Select an instance type that falls within the free tier (e.g., t2.micro for AWS, B1S for Azure, e2-micro for GCP).
- Configure the instance settings (networking, security, etc.).

Instances (1/2) [Info](#) Last updated less than a minute ago [Refresh](#) [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

Find Instance by attribute or tag (case-sensitive) [All states](#) < 1 > [Settings](#)

<input type="checkbox"/>	Name ✎	Instance ID	Instance state ▼	Instance type ▼	Status check	Alarm status
<input checked="" type="checkbox"/>	sample2005	i-0a681a5fcf31a1c25	Running 🔍 🔍	t2.micro	2/2 checks passed	View alarms +
<input type="checkbox"/>	nginx-00	i-05724f3f53febf4d9	Terminated 🔍 🔍	t2.micro	-	View alarms +

i-0a681a5fcf31a1c25 (sample2005) [Settings](#) [▼](#)

[Details](#) [Status and alarms](#) [Monitoring](#) [Security](#) [Networking](#) [Storage](#) [Tags](#)

[Instance summary](#) [Info](#)

[EC2](#) > [Instances](#) > [i-0a681a5fcf31a1c25](#) > [Connect to instance](#)

Connect to instance [Info](#)

Connect to your instance i-0a681a5fcf31a1c25 (sample2005) using any of these options

[EC2 Instance Connect](#) [Session Manager](#) [SSH client](#) [EC2 serial console](#)

Instance ID
[🔍](#) [i-0a681a5fcf31a1c25](#) (sample2005)

- Open an SSH client.
- Locate your private key file. The key used to launch this instance is sample.pem
- Run this command, if necessary, to ensure your key is not publicly viewable.
[🔍](#) `chmod 400 "sample.pem"`
- Connect to your instance using its Public DNS:
[🔍](#) `ec2-3-7-248-203.ap-south-1.compute.amazonaws.com`

Example:
[🔍](#) `ssh -i "sample.pem" ec2-user@ec2-3-7-248-203.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

3. Set Up Firewall Rules:

- Ensure that SSH (port 22) is allowed in the firewall settings for remote access.

4. Launch the VM:

- Review your settings and click “Launch” or “Create.”

Step 3: SSH into the Virtual Machine

1. Obtain the VM's Public IP Address:

- After the VM is launched, locate its public IP address in the dashboard.

2. Open Your Terminal:

- On macOS or Linux, open the terminal.
- On Windows, use Command Prompt or PowerShell, or an SSH client like PuTTY.

3. Connect via SSH:

- Use the following command to connect:
- `ssh -i /path/to/your/private/key username@public-ip-address`
- Replace `/path/to/your/private/key` with the path to your SSH key, `username` with the default user (e.g., `ec2-user` for AWS, `azureuser` for Azure, `ubuntu` for GCP), and `public-ip-address` with the VM's IP.

