



**Ganpat
University**

॥ विद्यया समाजोत्कर्षः ॥

**Institute of
Computer
Technology**

Name: Tushar Panchal

En.No: 21162101014

Sub: CCE(Cloud Computing Essentials)

Branch: CBA

Batch:61

-----PRACTICAL 01-----

Bob is an IT Administrator of SNS group Pvt limited is organized and wants to be adopted as Infrastructure as a Service (IAAS) using AWS cloud solution. Their majority of clients are e-commerce and OTP service providers. Initially, they want to set up three virtual Linux servers using Amazon EC2 which can be resizable and provide compute capacity along with a web-scale cloud computing solution. Bob is planning to create IAAS as below for E-Commerce clients.

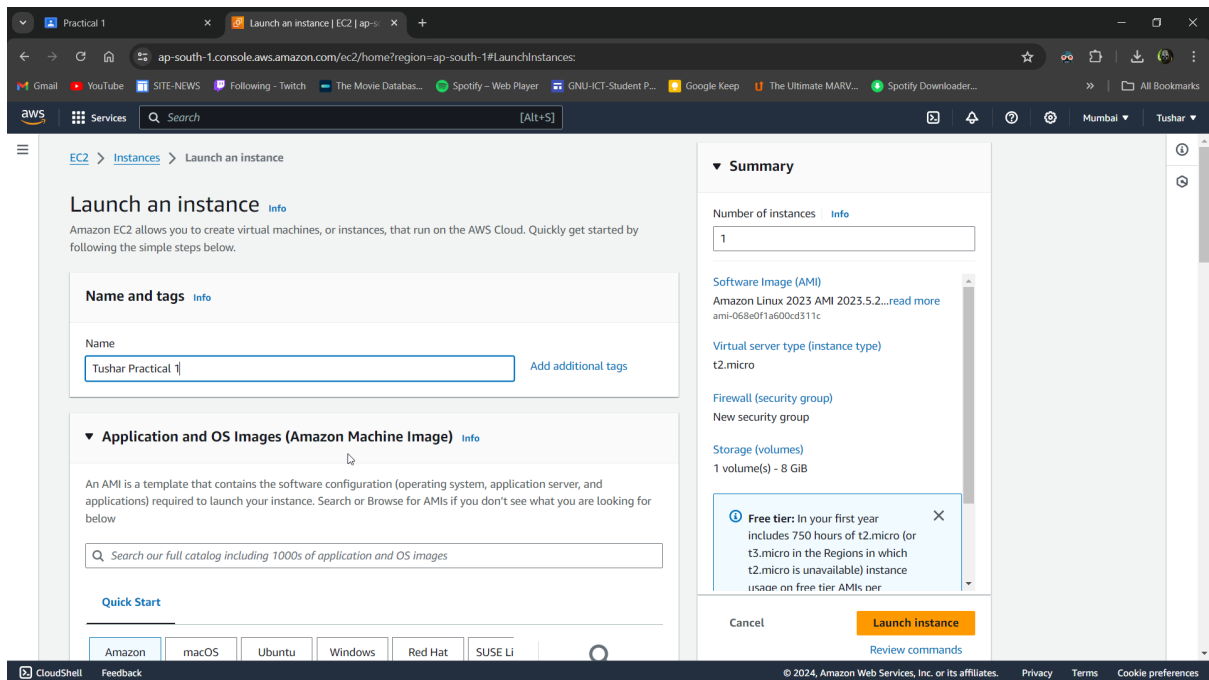
You are required to provide the solution Bob with proper step by step demonstration.

Consider the following attached scenario and perform the following tasks using AWS EC2 Service:

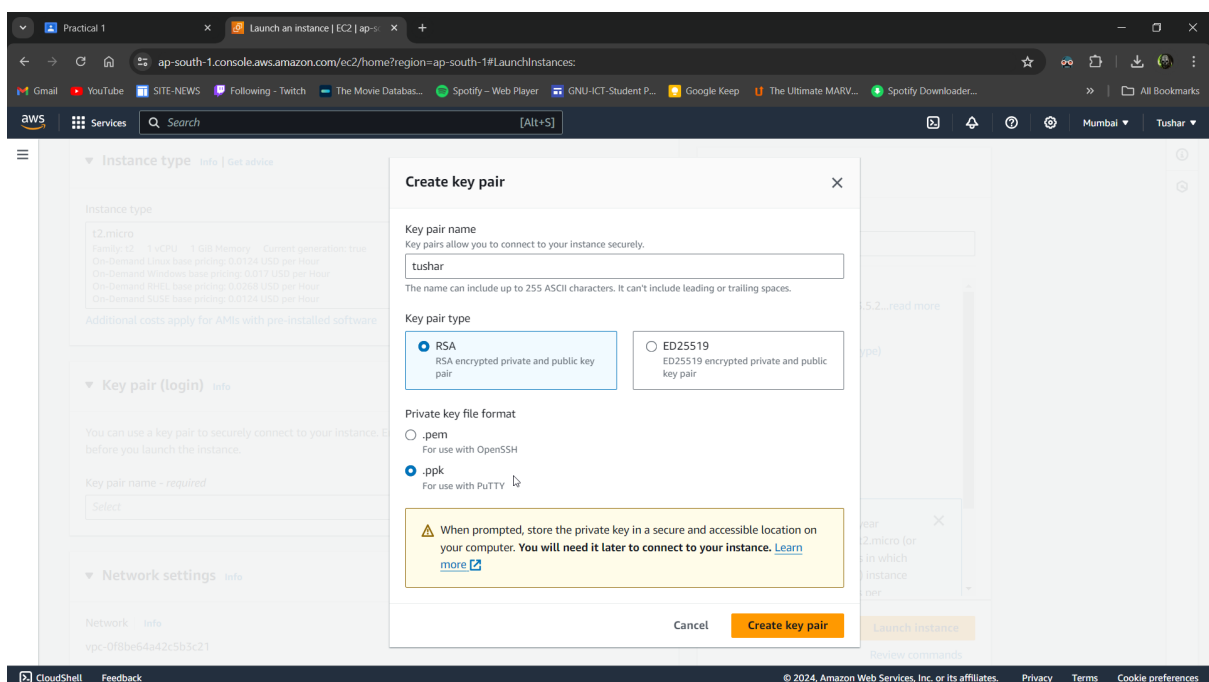
- **Launch a web server with termination protection enabled**
- **Monitor Your EC2 instance**
- **Modify the security group that your web server is using to allow HTTP access**
- **Resize your Amazon EC2 instance to scale**
- **Explore EC2 limits**
- **Test termination protection • Terminate your EC2 instance**

➤ First log in to AWS console and then search for EC2 in search box .

Then hit on launch instance then give a name to a instance



➤ Then select OS Image and create new key pair for windows select .ppk



Then select instance type and select key pair that you have created

The screenshot shows the AWS Management Console 'Launch an instance' page. The 'Instance type' is set to **t2.micro**. The 'Key pair (login)' is set to **tushar**. The 'Network settings' section shows a VPC ID. The 'Summary' panel on the right shows the configuration: 1 instance, Amazon Linux 2023 AMI, t2.micro instance type, new security group, and 8 GiB storage. A 'Free tier' notification is visible.

Then allow HTTPS traffic from the internet

The screenshot shows the AWS Management Console 'Launch an instance' page, specifically the 'Firewall (security groups)' section. The 'Create security group' button is selected. The 'We'll create a new security group called 'launch-wizard-1' with the following rules:' section shows three rules: 'Allow SSH traffic from Anywhere', 'Allow HTTPS traffic from the internet', and 'Allow HTTP traffic from the internet'. The 'Allow HTTPS traffic from the internet' rule is selected. A warning message states: '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.'

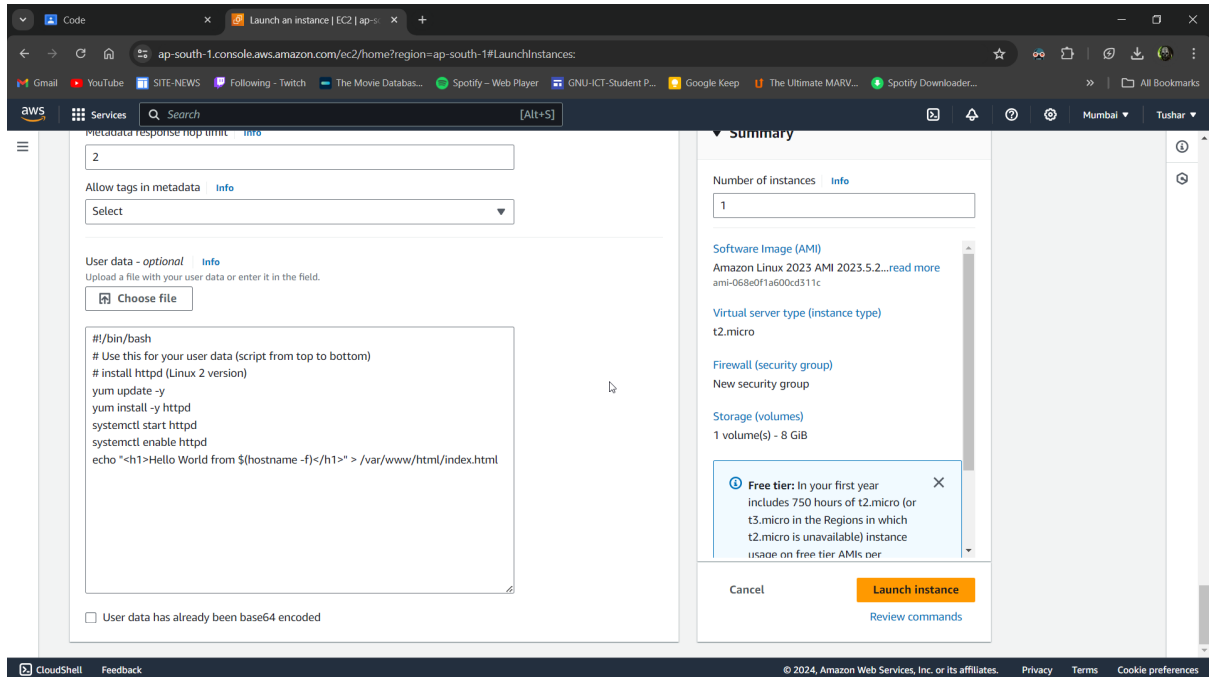
Then configure storage to 32gb

The screenshot shows the AWS Management Console 'Launch instance' page. The 'Configure storage' section is expanded, showing a single volume of 32 GB, gp3 type, as the root volume. A warning message states: '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.' The 'Summary' panel on the right shows the instance configuration: 1 instance, Amazon Linux 2023 AMI, t2.micro instance type, new security group, and 1 volume of 32 GB. A 'Free tier' notification is also visible. At the bottom, there are 'Cancel', 'Launch instance', and 'Review commands' buttons.

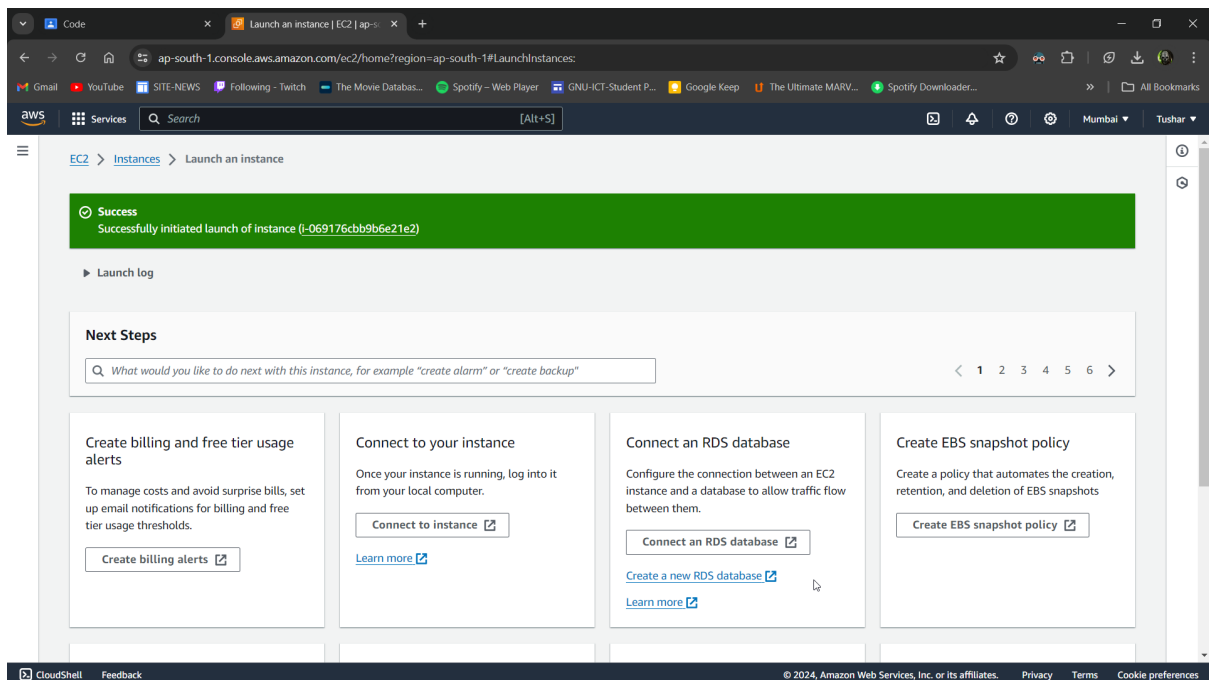
Then in advanced details enable termination protection

This screenshot is identical to the previous one, showing the 'Launch instance' page with storage configured to 32 GB. The 'Advanced details' section is now expanded, showing options for backup and file systems. The 'Summary' panel and other elements remain the same.

➤ And then in user data paste code (this code install apache server and show us hello world msg in web)



➤ Then hit launch instance and you will see instance in launched successfully



Then go to inbound rules

The screenshot shows the AWS Management Console interface. On the left, the navigation menu includes 'Instances', 'Images', 'Elastic Block Store', and 'Network & Security'. The main content area is titled 'Security Groups (1/1) Info'. Below the header, there's a search bar and a table listing security groups. The table has columns for Name, Security group ID, Security group name, VPC ID, and Description. One security group is listed: 'launch-wizard-1' with ID 'sg-060802a5c29d06582'. Below the table, the 'Inbound rules' tab is selected, showing a search bar and a table for inbound rules. The 'Edit inbound rules' button is visible.

And hit edit rules and add new rule and select http and in source select anywhere ipv4

The screenshot shows the 'Edit inbound rules' page for the security group 'launch-wizard-1'. The page title is 'Edit inbound rules'. Below the title, there's a description: 'Inbound rules control the incoming traffic that's allowed to reach the instance.' The main content area is titled 'Inbound rules Info'. It contains a table with columns: Security group rule ID, Type, Protocol, Port range, Source, and Description - optional. There are three rules listed: 'sgr-0de195efaac6f1eab' (HTTPS, TCP, 443), 'sgr-05f3417ecf75d0037' (SSH, TCP, 22), and a new rule being added (HTTP, TCP, 80). The 'Source' dropdown for the new rule is open, showing options: 'Custom', 'Anywhere IPv4' (selected), 'Anywhere IPv6', 'My IP', and 'Anywhere...'. The 'Add rule' button is visible at the bottom left. A warning message at the bottom states: 'Rules with source of 0.0.0.0/0 or ::0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.'

Then hit save rules

EC2 Dashboard
EC2 Global View
Events

▼ Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations

▼ Images
AMIs
AMI Catalog

▼ Elastic Block Store
Volumes
Snapshots
Lifecycle Manager

▼ Network & Security

CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Now if you go through your instance endpoint you will be able to see our code has been loaded (HTML)

Not secure 13.201.102.136

Hello World from ip-172-31-13-215.ap-south-1.compute.internal

Now try to stop instance you will face error because we enabled termination protection

The screenshot shows the AWS Management Console interface. The left sidebar contains navigation links for EC2 Dashboard, EC2 Global View, Events, Instances, Images, Elastic Block Store, and Network & Security. The main content area displays the 'Instances (1/1)' page for the 'ap-south-1' region. A modal dialog titled 'Stop instance?' is open, showing the instance ID 'i-069176cbb9b6e21e2' (Tushar Practical 1). The dialog includes a warning: 'After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated resources, such as attached EBS volumes and associated Elastic IP addresses.' Below the warning, it says 'To confirm that you want to stop the instance, choose the Stop button below.' The 'Stop' button is highlighted in orange.

Below the modal, the instance details for 'i-069176cbb9b6e21e2' are shown. The instance is in the 'Stopping' state. The 'Instance type' is 't2.micro'. The 'Status check' shows '2/2 checks passed'. The 'Availability Zone' is 'ap-south-1b'. The 'Public IPv4 DNS' is 'ec2-13-201-102-136.ap-south-1.compute.amazonaws.com'.

Below the instance details, the 'Outbound rules' are listed. The table shows the following rules:

Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sgr-0de195efaac6f1eab	443	TCP	0.0.0.0/0	launch-wizard-1
-	sgr-05f3417ecf75d0037	22	TCP	0.0.0.0/0	launch-wizard-1

Below the outbound rules, the 'Outbound rules' section is visible, showing a search bar and a list of rules.

At the bottom of the console, a red error banner is displayed: 'Failed to terminate an instance: The instance 'i-069176cbb9b6e21e2' may not be terminated. Modify its 'disableApiTermination' instance attribute and try again.'

Now disable termination protection and you will be able to terminate that instance

The screenshot displays the AWS Management Console interface. At the top, a browser window shows a terminal output: "Hello World from ip-172-31-13-215.ap-south-1.compute.internal". Below this, the AWS console shows the "Instances (1/1)" page. A modal dialog box titled "Stop instance?" is open, displaying the instance ID "i-069176cbb9b6e21e2 (Tushar Practical 1)". The dialog includes a warning message: "After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated resources, such as attached EBS volumes and associated Elastic IP addresses." Below the warning, it states "To confirm that you want to stop the instance, choose the Stop button below." and provides "Cancel" and "Stop" buttons. The background shows the instance details page with a table of security groups and outbound rules.

Name	Security group
sg-0de195efaac6f1eab	launch-wizard-1
sg-05f3417ecf75d0037	launch-wizard-1

Failed to terminate an instance: The instance 'i-069176cbb9b6e21e2' may not be terminated. Modify its 'disableApiTermination' instance attribute and try again.

Instances (1/1) Info

Find Instance by attribute or tag (case-sensitive) All states

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
Tushar Practic...	i-069176cbb9b6e21e2	Stopping	t2.micro	2/2 checks passed	View alarms +	ap-south-1b	ec2-13-201-102-

i-069176cbb9b6e21e2 (Tushar Practical 1)

Filter rules

Name	Security group rule ID	Port range	Protocol	Source	Security groups
-	sgr-0de195efaac6f1eab	443	TCP	0.0.0.0/0	launch-wizard-1
-	sgr-05f3417ecf75d0037	22	TCP	0.0.0.0/0	launch-wizard-1

Outbound rules

Filter rules

Instance summary Info

Instance ID: i-069176cbb9b6e21e2 (Tushar Practical 1)

Public IPv4 address: -

Instance state: Stopped

Hostname type: Private IP DNS name (IPv4 only)

IP name: ip-172-31-13-215.ap-south-1.compute.internal

Actions

- Connect
- View details
- Manage instance state
- Attach to Auto Scaling Group
- Change termination protection**
- Change stop protection
- Change shutdown behavior
- Change auto-recovery behavior
- Change instance type
- Change Nitro Enclaves
- Change credit specification
- Change resource based naming options
- Modify instance placement
- Modify Capacity Reservation settings
- Edit user data
- Allow tags in instance metadata
- Manage tags
- Modify instance metadata options

Instance settings

- Networking
- Security
- Image and templates
- Monitor and troubleshoot

The screenshot shows the AWS Management Console for the 'ap-south-1' region. The 'Instances' page is active, displaying a list of instances. A modal dialog titled 'Change termination protection' is open for instance 'i-069176cbb9b6e21e2 (Tushar Practical 1)'. The dialog explains that enabling termination protection prevents accidental termination. The 'Termination protection' checkbox is currently unchecked, and a yellow warning box states: 'Termination protection disabled. The instance is no longer protected against accidental termination. If the instance is terminated, data stored on ephemeral storage is lost.' The 'Save' button is highlighted in orange.

The screenshot shows the AWS Management Console for the 'ap-south-1' region. A green banner at the top indicates 'Successfully removed termination protection for instance i-069176cbb9b6e21e2. The instance can be terminated.' The 'Instances' page is active, and a modal dialog titled 'Terminate instance?' is open for instance 'i-069176cbb9b6e21e2 (Tushar Practical 1)'. The dialog includes a warning: '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.' It asks 'Are you sure you want to terminate these instances?' and shows the instance ID and 'Termination protection' status as 'Disabled'. A confirmation instruction states: '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.' The 'Terminate' button is highlighted in orange.

» After disabling termination protection we can be able to terminate our instance

The screenshot displays the AWS Management Console interface. At the top, a green notification banner states "Successfully initiated termination of i-069176cbb9b6e21e2". Below this, the "Instances (1/1)" page is shown, featuring a table with one instance: "Tushar Practic..." with ID "i-069176cbb9b6e21e2", state "Shutting-down", and type "t2.micro". The instance details panel for "i-069176cbb9b6e21e2 (Tushar Practical 1)" is open, showing the "Instance summary" tab. The summary includes the instance ID, IP addresses, and DNS information. The instance state is "Shutting-down".

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
Tushar Practic...	i-069176cbb9b6e21e2	Shutting-down	t2.micro	-	View alarms +	ap-south-1b	-

i-069176cbb9b6e21e2 (Tushar Practical 1)

Instance summary

Instance ID	Public IPv4 address	Private IPv4 addresses
i-069176cbb9b6e21e2 (Tushar Practical 1)	-	172.31.13.215
IPv6 address	Instance state	Public IPv4 DNS
-	Shutting-down	-
Hostname type	Private IP DNS name (IPv4 only)	
IP name: ip-172-31-13-215.ap-south-1.compute.internal	ip-172-31-13-215.ap-south-1.compute.internal	