Cloud Computing Lab Manual

Date: 9-10-2025

Exercise-2: AWS Identity Access Management (IAM) User and Group creation. Enable AWS IAM MFA. Create an AWS Account Alias (for Alternate Sign-in URL)

AWS Identity and Access Management (IAM) is a security service that helps you control who can access your AWS resources and what actions they can perform. It is a global AWS service.
It allows you to securely manage users, groups, roles, and permissions in your AWS account.

Concept	Description
Root User	The account owner who created the AWS account. Has full access and should be used only for account setup.
Group	A collection of IAM users that share the same permissions. For example, a "Developers" group or "Students" group.
User	A person or application that interacts with AWS (e.g., student1, admin, developer). Each user has its own username, password, and access keys.
Policy	A JSON document that defines what actions are allowed or denied (e.g., "allow S3 read access").
Role	A set of permissions that can be temporarily assumed by a user, service, or application — often used by EC2 instances or Lambda functions.

STEPS for AWS IAM User Group Creation

Step 1: Sign in to AWS Console

- Log in to your AWS Management Console using an administrator account.
- From the Services menu, search for IAM and open it.

Step 2: Open Groups Section

- In the IAM dashboard, look at the left sidebar.
- Click on "User groups" → then click "Create group".

Step 3: Name the Group

- Enter a Group name (example: Developers, Admins, Students, etc.).
- Group names must be unique within your account.

Step 4: Attach Permissions Policies

- You can attach IAM policies to define what members of the group can do.
  Select the following:
  - AdministratorAccess → Full access to all services.
  - IAMUserChangePassword

Step 5: Review and Create

- Review all details (group name + permissions).
- Click "Create group" to finalize.

Group Successfully Created

- The new group now appears in the IAM dashboard.
- Any user added to this group automatically inherits all permissions attached to the group.

STEPS for AWS IAM User Creation

Step 1: Sign in to AWS Management Console

- Login to the AWS Management Console using your root user credentials.
- In the search bar, type IAM and open IAM service.

Step 2: Navigate to Users Section

- In the IAM dashboard's left panel (info panel), click on Users.
- Then click on the "Add users" button.

Step 3: Set User Details

- Enter a user name.
- Checkbox – 'Provide user access to the AWS Management Console'.
- Select 'I want to create an IAM user' option

Step 4: Set Permissions

You can grant permissions to the new user in three ways:

1. Add user to group – Assign predefined permission groups.
2. Copy permissions from an existing user.
3. Attach existing policies directly.

Recommended: Use IAM **groups** to manage permissions easily.

Step 5: Set User Details and Tags (Optional)

- Add tags like Department: MCA or Role: Faculty/Student for easy identification.
- Click Next to review.

Step 6: Review and Create User

- Review all settings (user name, permissions, tags).
- Click Create user.

Step 7: Save Credentials

- After creation, AWS displays:
  - Console sign-in URL
  - Username
  - Password

NOTE: Download or copy these credentials immediately — they cannot be retrieved later.

Step 8: Test the User Login

- Visit the IAM login URL provided (unique for your AWS account).
- Log in with the newly created username and password.
- Verify access and permissions.

Enable AWS IAM MFA

Step 1: Sign in to AWS Console as root user

Step 2: Open IAM Dashboard

- In the search bar, type IAM and select IAM (Identity and Access Management).
- From the left navigation pane, select Users.

Step 3: Select a User
- Click the user name for whom you want to enable MFA.
- This opens the User Summary page.

Step 4: Go to Security Credentials Tab
- Click the Security credentials tab.
- Scroll down to the section "Multi-factor authentication (MFA)".

Step 5: Assign MFA Device

- Click "Assign MFA device".
- Choose the MFA type:
    1. Virtual MFA device (e.g., Google Authenticator, Authy — most common)
    2. Security key (hardware-based, e.g., YubiKey)
    3. Authenticator app on phone

Step 6: Configure Virtual MFA
- If you select Virtual MFA device:
    1. Open your Google Authenticator or Authy app on your phone.
    2. Scan the QR code shown on the AWS screen.
    3. The app starts generating 6-digit codes.

Step 7: Verify MFA
- Enter two consecutive codes from your app in the verification fields.
- Click "Assign MFA".

Step 8: Confirm Setup
- You will see a green checkmark confirming MFA is successfully assigned.
- The user now requires MFA each time they sign in.

Create an AWS Account Alias (for Alternate Sign-in URL)

As an IAM user you can sign in using the default URL or create an account alias for it.
An Account Alias gives your AWS account a name instead of using the long numeric Account ID in your sign-in URL.
This makes it easier for IAM users to remember and log in.

Step 1:
- Sign in to the AWS Management Console using root user or an IAM user with administrative privileges.
- In the search bar, type IAM, and open the IAM service.

Step 2:
- In the left navigation pane, scroll down and select Dashboard.

Step 3:
- Under the "AWS Account" section, find "Account Alias".
- Click on "Create" (or "Edit" if one already exists).

Step 4:
- In the pop-up box, enter your preferred alias name.

- Click “Create alias”.

Step 5:

- Once created, you’ll see a new Sign-in URL displayed.

Date: 15-10-2025

Exercise-3: Amazon S3 – Introduction, Bucket Creation and upload objects (files).

Amazon S3 (Simple Storage Service) is a fully managed, object-based storage service offered by AWS.
It allows you to store and retrieve unlimited amounts of data from anywhere on the web.
Unlike traditional file systems that store data in folders, S3 stores data as objects inside buckets.
Each object has:

- Data (the actual file),
- Metadata (information about the file),
- Unique key (its name within the bucket).

You can store unlimited data in Amazon S3.
However, each AWS account can create up to 100 buckets by default (can be increased by request).
Each object (file) can be up to 5 TB (terabytes) in size.
Single upload limit: 5 GB (may vary), but larger files can be uploaded using Multipart Upload.

Amazon S3 is designed for:

- Durability: 99.999999999% (11 nines) – this means your data is extremely safe.
- Availability: 99.99% uptime – your data is almost always accessible.
- S3 automatically stores multiple copies of your data across multiple Availability Zones in a region.

Storage classes: S3 offers different storage classes depending on cost and frequency of access.

Storage Class	Description
S3 Standard	For frequently accessed data (default).
S3 Intelligent-Tiering	Automatically moves data between frequent - infrequent access tiers.
S3 Standard-IA	For infrequently accessed data but still quickly available.
S3 Glacier	For archival storage (low cost, slower retrieval).
S3 Glacier Deep Archive	For long-term archival (lowest cost).

Each object can be accessed through a **unique URL**.
S3 is commonly used for:

- Backup and archival
- Static website hosting
- Application data storage
- Media content delivery

Feature	**Description**
Buckets	Top-level containers for storing objects.
Objects	Actual files stored in S3 (e.g., images, HTML, PDFs).
Region	Each bucket is created in a specific AWS region.
Versioning	Maintains multiple versions of the same object for recovery.
Static Website Hosting	Allows you to host HTML pages directly from an S3 bucket.

Steps to Create an S3 Bucket and Upload an Image

Step 1: Open the S3 Service

- Sign in to your AWS Management Console.
- In the search bar, type S3 and click Amazon S3.

Step 2: Create a New Bucket

- Click “Create bucket”.
- Bucket type: General purpose
- Bucket name: Enter a name (Bucket names must be globally unique and lowercase.)
- AWS Region: Choose the region nearest to you.
- Object Ownership: select ACLs enabled [this enables us to access the objects through the public URLs.]
- Next keep the ‘Bucket owner preferred’ as checked [default setting]
- Scroll down to ‘Block Public Access settings for this bucket’ section and uncheck:
  “Block all public access” → Uncheck this (for viewing file publicly).
  Confirm the warning checkbox [acknowledgement].
- Keep all other settings as default.
- Click Create bucket.

Step 3: Upload an Image File

1. Click on the newly created bucket name.
2. Click Upload → Add files.
3. Choose any image file from your computer.
4. Scroll down and click Upload.

Step 4: Make the Object Public

By default, S3 objects are private. To view them in a browser, make the file public.

1. After upload, go to the Objects tab inside your bucket.
2. Select the uploaded file.
3. Click Actions → Make public using ACL (or Object actions → Make public, depending on console version).
4. Confirm.

Step 5: Copy the Object URL

1. Open the object again by clicking its name.
2. Scroll down to the **Object URL** section.
3. Copy this URL and open it in a new browser tab.

The image is displayed directly from the S3 bucket — meaning AWS S3 is serving that object over HTTP.

Date: 16-10-2025, 23-10-2025

Exercise-4: Amazon S3 – Static Website Hosting (Multi-Page website), Versioning, Cross-Region Replication rule.

Amazon S3 Static Website Hosting

Amazon S3 can host a static website – [a website consisting of only HTML, CSS, JavaScript, images, etc. – no server-side scripting like PHP or Python].

When you enable "Static Website Hosting," your S3 bucket acts like a web server, and AWS provides a public website URL to access it.

You can create a multi-page static website (e.g., index.html, about.html, contact.html) and upload it to S3. Links within these pages allow users to navigate between them just like a normal website.

Steps to Create a Multi-Page Static Website on S3

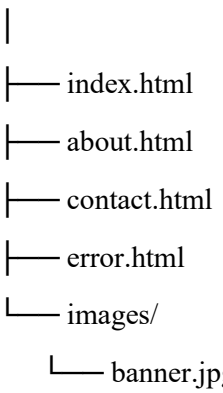
Step 1: Create an S3 Bucket

- Open the AWS Management Console → Navigate to S3.
- Click Create bucket.
- Select Bucket type: General purpose
- Enter a unique bucket name (e.g., my-static-web-demo).
- Select ACLs enabled under Object Ownership section.
- Uncheck "Block all public access" → acknowledge.
- Click Create bucket.

Step 2: Prepare Website Files

Before uploading, organize your files in a folder structure as follows:

my-website/



├── index.html

├── about.html

├── contact.html

├── error.html

└── images/

└── banner.jpg

Each HTML file should include navigation links.

Step 3: Upload Website Files

- Open your S3 bucket → Click Upload.
- Add all files and folders (HTML, CSS, JS, images).
- Click Upload to store them in S3.

Step 4: Enable Static Website Hosting

- Go to the **Properties** tab of the bucket.
- Scroll down to Static website hosting → Click Edit.
- Choose Enable and select 'Host a static website'.

- Set:
    - Index document: index.html
    - Error document: error.html
- Click Save changes.

Step 5: Make Files Public (Bucket Policy)
By default, your files are private. To make them public:

- Go to the **Permissions** tab → Bucket Policy → Edit.
- Paste the following policy (replace bucket name):

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "PublicReadGetObject",
   "Effect": "Allow",
   "Principal": "*",
   "Action": "s3:GetObject",
   "Resource": "arn:aws:s3:::my-static-web-demo/*"
  }
 ]
}
```

- Save the changes.

Step 6: Access Your Website

- Go to the Properties tab → Scroll to Static website hosting.
- Copy the Bucket Website Endpoint URL.
- Paste it into your browser — your homepage (index.html) should appear.
- Use the header links to navigate between pages (About, Contact, etc.).

When Will the Error Page Be Shown?

If a user enters a wrong URL or tries to access a file that doesn't exist (e.g., /abc.html), Amazon S3 automatically displays the file you set as the **Error document** (error.html).

Amazon S3 Versioning

Versioning allows you to keep multiple versions of an object in a bucket.
If a file is accidentally deleted or overwritten, you can recover the previous version.
Each version gets a unique version ID.

Steps to Enable Versioning

- Go to your S3 bucket
- Open the Properties tab
- Scroll to Bucket Versioning
- Click Edit → Enable
- Click Save changes

Now whenever you upload a file with the same name, S3 will keep both versions.

Note: You can view versions by clicking "List versions" in the bucket objects page.

To Restore or Delete a Specific Version

- Click the object name → Versions
- Select the desired version → Download / Delete
  (Deleting only adds a delete marker — older versions are still stored.)

Cross-Region Replication (CRR) – is a rule created on S3

CRR automatically copies objects from one S3 bucket (source) to another (destination) in a different AWS Region.
Used for disaster recovery, compliance, or low-latency access in another region.
Requires Versioning to be enabled on both buckets.

Steps to Set Up CRR

NOTE: Enable Versioning on both:
Source bucket
Destination bucket

Step 1: Choose a different region before you create Destination bucket
Create Destination Bucket first.

Step 2: Create Source Bucket
Give replication permission:
Source bucket → Management tab→ Replication rules → Create rule

Step 3: Create Replication Rule page
Enter a Replication rule name
Status: Enabled

Source bucket section:
Choose a rule scope: select "Apply to all objects in the bucket"

Destination:
Select "Choose a bucket in this account"
Bucket name: Select the destination bucket

IAM role:
Select "Create new role"
[An IAM role gives Amazon S3 permission to replicate objects from your source bucket to your destination bucket.
S3 replication won't work unless you assign (or create) a role with the right permissions.
IAM Role: Either create a new role automatically or choose an existing one]

Step 4: Save
Any new objects uploaded to the source bucket will automatically replicate to the destination region.

Note: Replication is not retroactive — only new uploads after enabling CRR are copied.

Date: 29-10-2025

Exercise-5: Overview of EC2, To Launch a Windows EC2 Instance and Connect via RDP Client

Amazon Elastic Compute Cloud (EC2) is a core AWS Compute service that lets you run virtual servers (instances) in the cloud.

Amazon EC2 is an Infrastructure as a Service (IaaS) offering from AWS.

It allows you to launch virtual machines to host applications and manage them remotely – wherever you are in the world.

Key concepts:

Instance - A virtual machine running in the AWS cloud.

AMI (Amazon Machine Image) - A pre-configured template that includes: OS (Linux, Windows, etc.), Application software, other configurations.

Instance Type - Defines hardware power:

Family	Example	Use Case
General Purpose	t2.micro	Basic web apps
Compute Optimized	c5.large	High-performance computing
Memory Optimized	r5.large	Databases, analytics
Storage Optimized	i3.large	Data warehousing
GPU Instances	g4dn.xlarge	ML/AI, graphics

EBS (Elastic Block Store) - Persistent storage for your EC2 instance. Acts like a hard drive — data remains even after instance stops. Types: SSD, HDD, etc.

Security Groups - Virtual firewalls controlling inbound and outbound traffic.
Example: Allow HTTP (port 80), SSH (port 22), HTTPS (port 443)

Key Pair - Used for secure login (SSH for Linux, RDP for Windows). Consists of a public key (stored in AWS) and private key (.pem) that you download.

Common Ways to Access EC2

- SSH (Linux instances)
- RDP (Windows instances) - Use Remote Desktop with Administrator password.
- User Data Script: Run automation commands during instance launch.

EC2 Use Cases

- Hosting static or dynamic websites
- Deploying web servers (Apache/Nginx)
- Running applications, APIs, or databases
- Machine Learning model hosting
- Batch processing jobs

Pricing Models

- On-Demand: Pay per hour/second; flexible.
- Reserved Instances: 1–3 year commitment; cheaper.

- Spot Instances: Unused capacity; up to 90% cheaper.
- Free Tier: t2.micro or t3.micro free for 6 months.

Lifecycle of an Instance

Step	Description
Launch	Choose AMI, type, key, security group
Running	Accessible and operational
Stop	Instance paused, EBS persists
Start	Boot again from same EBS
Terminate	Deleted permanently, data lost unless backed up

Two types of IPv4 addresses

When you launch an EC2 instance, AWS automatically assigns two types of IPv4 addresses depending on your network settings (VPC, subnet, etc.):

1. Private IPv4 Address
- Purpose: Used for internal communication within the same VPC (Virtual Private Cloud).
- Assigned Automatically: Yes, by AWS from the subnet's private IP range.
- Visibility: Not accessible from the Internet.
- Use Case:
    - Instance-to-instance communication inside AWS (e.g., web server ↔ database server).
    - Internal services that do not need public internet access.
- Persistence: The private IP remains attached to the instance until it is terminated.

2. Public IPv4 Address
- Purpose: Used for communication over the Internet.
- Assigned Automatically:
    - Yes, if your subnet is public (i.e., auto-assign public IP enabled).
    - No, if it's a private subnet.
- Visibility: Accessible from the Internet.
- Use Case:
    - Accessing the instance via SSH or HTTP from your local system.
    - Hosting web applications publicly.
- Persistence:
    - The public IP changes each time you stop/start the instance.
    - To make it permanent, you can assign an Elastic IP (static public IP).

Remote Desktop Protocol [RDP], is a secure communication protocol developed by Microsoft that allows a user to connect to and control another computer remotely. It establishes an encrypted channel to transmit keyboard and mouse inputs from the client to the remote computer and send screen information back to the client, providing a graphical user interface for remote access.

An **RDP client** is the software or app that you use to make this remote connection.
It connects to a remote Windows server or Windows EC2 instance that is running an RDP server (which listens on port **3389**). It is pre-installed in Windows.

Steps to Launch a Windows EC2 Instance and Connect via RDP Client

Step 1: Sign in to AWS Management Console

Select the **Region** closest to you.

Step 2: Open the EC2 Dashboard

In the AWS Console, search for **EC2** in the search bar.
Click on EC2 → Instances → Launch Instance.
Under Name and Tags, give your instance a name.

Step 3: Choose an Amazon Machine Image (AMI)

Under Application and OS Images (Amazon Machine Image) → click Browse more AMIs or choose: Microsoft Windows Server 2022 Base (Free tier eligible).

Step 4: Choose Instance Type

Choose t3.micro (Free-tier eligible).

Step 5: Configure Key Pair

Under Key pair (login), choose an existing key pair or create a new one.
If creating a new key pair:

- Choose type: RSA
- Format: .pem
- Download and save it safely — it's required to decrypt your Windows password later.

Step 6: Configure Network Settings

Leave default VPC and Subnet settings.
Under Firewall (security group) →

- Select Create security group.
- Allow RDP (port 3389) access from My IP (for better security) or anywhere (0.0.0.0/0).

Step 7: Launch the Instance

Review all configurations.
Click Launch Instance.
Wait until the Instance state changes to Running and Status check = 3/3 passed.

Note:

Wait approximately 5 minutes after instance launch to allow AWS to fully initialize the instance and make the Administrator password available.
When a Windows EC2 instance is first launched, AWS needs a few minutes to:
Initialize the instance, Attach the root volume, Generate the Windows Administrator password (encrypted using your key pair.

Step 8: Get the Administrator Password

Select your running instance → click Connect → choose RDP Client tab.
Click Get Password (you must wait about 4 minutes after launch).
Upload your .pem key file and click Decrypt Password.
Copy the Public IPv4 address and Administrator Password shown.

Step 9: Connect Using RDP Client

On Windows system:

1. Open Remote Desktop Connection (from Start Menu).
2. Enter your instance's Public IPv4 address.

3. Click Connect → Enter:
    - Username: Administrator
    - Password: *(the decrypted password from AWS)*
4. Click OK → accept the certificate → the remote Windows desktop opens!

Step 10: Verify Connection

- You should now see a Windows Server desktop running inside your local window.
- You can open File Explorer, browse settings, or install software (within the free-tier limits).

Note:

- Always **Stop** (not Terminate) the instance when not in use to avoid charges.
- RDP uses port 3389, so ensure it's open in the security group.
- Avoid sharing your decrypted password or key pair.

Date: 30-10-2025

Exercise-6: Launch a Linux EC2 Instance and Connect using SSH through PowerShell/Linux Terminal and PuTTY on Windows.

Note: Choosing the Correct Key Pair Format
While creating a Key Pair, you are asked to select the Private Key File Format — either .pem or .ppk. The correct choice depends on the operating system and the method you will use to connect to your EC2 instance.

Scenario	Key File Format	Explanation
Using PuTTY on Windows	.ppk	The .ppk file is specific to the GUI based PuTTY application, a popular SSH client for Windows system.
Using PowerShell on Windows, Linux terminal on Linux	.pem	The .pem file is the default AWS key format used by the OpenSSH client available in PowerShell (Windows), Linux, and macOS terminals. Used for CLI.

Steps to Launch a Linux EC2 Instance and Connect using SSH through PowerShell/Linux

Step 1: Sign in to AWS Management Console
select the nearest AWS Region.

Step 2: Open EC2 Service
In the search bar, type EC2 and click EC2 Dashboard.
Select Instances → Launch Instance.

Step 3: Configure Instance Details
Under Name and Tags, give your instance a name, e.g., *Linux-SSH-Demo*.
Under Application and OS Images (AMI) → select Amazon Linux 2 AMI (Free tier eligible).
Under Instance type, choose t3.micro (Free-tier eligible).

Step 4: Create or Select a Key Pair
Under Key pair (login) → choose Create new key pair.
Choose:
- Key pair type: RSA
- Private key file format: .pem (for SSH via PowerShell/Linux)

Click Create key pair → the .pem file will automatically download.
Save it securely on your local machine (you'll need it for SSH login).

Step 5: Configure Network Settings
Under Network settings, leave the defaults.
In Firewall (security group) → select Create security group.
Ensure SSH (port 22) is allowed:
- Type: SSH
- Protocol: TCP
- Port Range: 22
- Source: My IP (recommended for security) or Anywhere (0.0.0.0/0).

Step 6: Launch the Instance

Review the configuration → click Launch Instance.
Wait for the Instance State to show Running and Status Checks: 3/3 passed.

Step 7: Get the Public IP Address

Select your instance → In the summary section →
Copy the Public IPv4 address — you'll use this to connect.

Step 8: Connect using SSH

(A) On Windows using PowerShell

- Open **PowerShell** (search "PowerShell" from the Start menu).
- Navigate to the folder where your .pem file is saved:
  cd "C:\Users\<YourName>\Downloads"
- Connect using the SSH command:
  ssh -i "keyfile.pem" ec2-user@<Public-IP-address>
- When prompted, type **yes** to continue connecting.
- You'll now be logged into your EC2 Linux terminal.

(B) On Linux Terminal (Ubuntu / macOS)

- Open **Terminal**.
- Navigate to the directory where your .pem file is stored.
- Set proper permission for the key file:
  chmod 400 keyfile.pem
- Connect to the instance:
  ssh -i keyfile.pem ec2-user@<Public-IP-address>
- Type **yes** when prompted.
- You will be connected to your EC2 instance remotely.

Step 9: Verify Connection

- Once connected, the command prompt will appear as:
  [ec2-user@ip-172-31-xx-xx ~]$
- Try a few commands:
  uname -a and sudo yum update -y to confirm access.

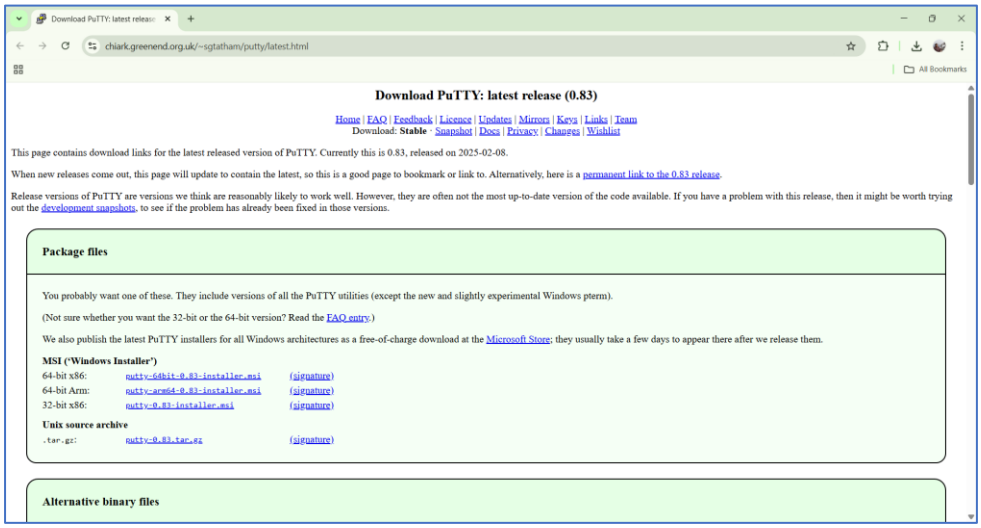
Step 10: Stop Instance after Use

Go to the EC2 console.
Select your instance → Instance State → Stop Instance (to avoid charges).

Steps to Install PuTTY on Windows

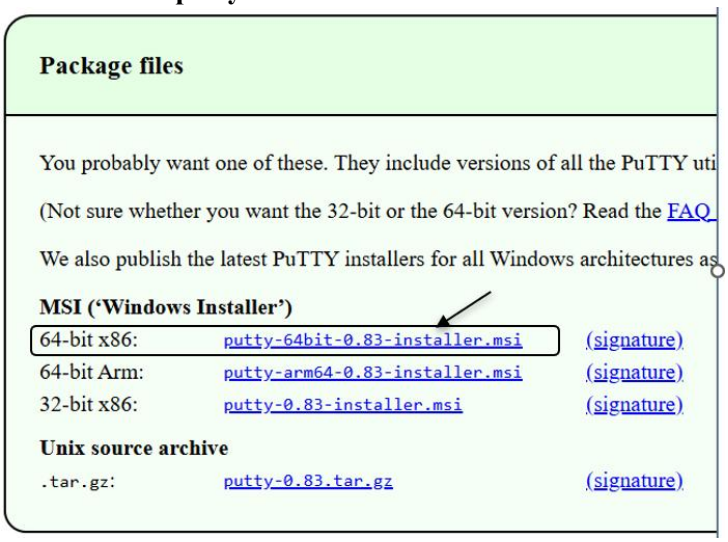
PuTTY is a client program for the SSH, Telnet and Rlogin network protocols. These protocols allow you to interact with a remote server as if you were sitting right in front of it.
It is primarily used in the Windows platform.
In an era where cloud computing and remote servers are the norm, being able to securely connect and interact with these servers is vital. It provides a secure and reliable way to connect to these remote systems. It supports a range of network protocols including the secure ones like SSH.

Use the correct, safe download link: Official download page: This is the only genuine PuTTY source.
https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html



Under the **Package files** section, look for:
MSI ('Windows Installer')
64-bit x86: putty-64bit-0.83-installer.msi

Click the link: **putty-64bit-0.83-installer.msi**



Once it downloads, open the file and follow: Next → Next → Install → Finish

After installation, you will have:

- PuTTY – to connect to your EC2 instance via SSH

- PuTTYgen – to convert .pem to .ppk (if needed)
- Pageant – optional key manager

You can open PuTTY by typing **PuTTY** in the Windows search bar/start menu.

Steps to Launch a Linux EC2 Instance and Connect using PuTTY on Windows

Step 1: Sign in to AWS Management Console

Select your nearest AWS Region.

Step 2: Open the EC2 Service

In the AWS Console search bar, type EC2 and select EC2 Dashboard.
Click Instances → Launch Instance.

Step 3: Configure Instance Details

Under Name and Tags, enter an instance name, e.g., *Linux-PuTTY-Demo*.
Under Application and OS Images (AMI) → choose Amazon Linux 2 AMI (Free tier eligible).
Under Instance Type, select t2.micro (Free tier eligible).

Step 4: Create or Select a Key Pair

Under Key pair (login) → select Create new key pair.
Choose the following:

- Key pair type: RSA
- Private key file format: .ppk *(for PuTTY on Windows)*

Click Create key pair → a .ppk file will download automatically.
Save it securely — this file is required to connect later.

Step 5: Configure Network Settings

Under Network settings, leave default VPC/Subnet settings.
Under Firewall (security group):

- Select Create security group.
- Ensure SSH (port 22) is allowed:
  - Type: SSH
  - Protocol: TCP
  - Port Range: 22
  - Source: anywhere.

Step 6: Launch the Instance

Review all configurations.
Click Launch Instance.
Wait until the Instance State changes to Running and Status Check = 3/3 passed.

Step 7: Obtain the Public IP

Select your instance → In the summary section →
Copy the Public IPv4 address or Public DNS (IPv4) — you'll use this to connect from PuTTY.

Step 8: Connect using PuTTY

Open **PuTTY** on your Windows system.
In the **Host Name (or IP address)** field, enter: ec2-user@<Public-IP-address>
In the **Category** list on the left, expand: Connection → SSH → Auth → Credentials
Click **Browse** → locate and select your .ppk key file downloaded earlier.
Click **Open**.

When prompted, click **Accept** to trust the host.
A terminal window opens — you're now connected to your EC2 Linux instance!

Step 9: Verify Connection

Once connected, your prompt should look like: [ec2-user@ip-172-31-xx-xx ~]$
Try verifying: uname -a or update packages: sudo yum update -y

Step 10: Stop the Instance

Return to the EC2 Dashboard.
Select your instance → click Instance State → Stop Instance.
This prevents charges when you're not using it.

Note

- Use .ppk format key when connecting with **PuTTY (Windows)**.
- Use .pem format key when connecting with **PowerShell / Linux / macOS terminal**.
- Both keys serve the same purpose — secure authentication to your EC2 instance.

The message **"Permission denied (publickey)"** or **"Permissions are too open"** appears when the .pem key file or SSH configuration has incorrect permissions or mismatched ownership.

Run this command in your local terminal before connecting:

chmod 400 keypair.pem

Then connect again:

ssh -i "keypair.pem" ec2-user@<Public-IP>

Date: 5-11-2025

Exercise-7: Hosting a static website on EC2 instance.

- Manual Installation of Apache (httpd) Web Server on EC2 for Static Website Hosting.
- Launching an EC2 Instance with User Data Script to Automatically Install Apache and Host a Static Website.

When you create an EC2 instance, it's just a **bare machine** — It does not have the software to host a website yet. To host a website:

- You need a web server software → Apache (httpd)
- You put your website files (HTML, CSS, etc.) in a special folder (usually /var/www/html)
- Apache listens on port 80 (HTTP) or port 443 (HTTPS) for incoming connections

Apache HTTP Server (often called Apache or httpd) is a web server software.
It runs on a computer (like your EC2 instance) and delivers web pages (HTML, images, CSS, etc.) to users over the HTTP/HTTPS protocol.
So, whenever someone types your website's URL (like http://your-ec2-ip/), Apache receives that request and serves your webpage files from your server to the browser.

httpd stands for **HTTP Daemon**.

A *daemon* in Linux is a background service that keeps running to handle requests.
So, httpd is the background process that runs the Apache web server.
When you install Apache, you're really installing the **httpd service**.

File Locations (default) – Website files go into: /var/www/html

Steps for Manual Installation of Apache (httpd) Web Server on EC2 for Static Website Hosting.

Part 1 – Creating an EC2 Instance

Step 1: Sign in to AWS Management Console
In the search bar, type EC2 and open the EC2 Dashboard.

Step 2: Launch a New Instance
Click "Launch Instance."
Give a name. (e.g., MyApacheServer)

Step 3: Choose an Amazon Machine Image (AMI)
Select Amazon Linux 2 AMI (Free tier eligible)

Step 4: Choose Instance Type

Choose t3.micro (Free tier eligible).

Step 5: Create / Select Key Pair

Under Key pair (login), choose:

Create new key pair → Give a name → File format = .pem

Download the key file → Keep it safe.

Step 6: Configure Network Settings

Click → Allow SSH traffic

→ Allow HTTP traffic from the internet. (This automatically opens port 80 for web access).

Step 7: Launch Instance

Review → Click **Launch Instance**.

Wait for the instance to start.

Step 8: Connect to the Instance

Using powershell type the following commands:

- Open PowerShell (search "PowerShell" from the Start menu).
- Navigate to the folder where your .pem file is saved:
  cd "C:\Users\<YourName>\Downloads"
- Connect using the SSH command:
  ssh -i "keyfile.pem" ec2-user@<Public-IP-address>
- When prompted, type yes to continue connecting.
- You'll now be logged into your EC2 Linux terminal.

Part 2 – Manual Installation of Apache (httpd) Web Server

Step 1: Update the Packages

sudo yum update -y

Step 2: Install Apache (httpd)

sudo yum install httpd -y

(This installs the Apache Web Server package.)

Step 3: Start the Apache Service

sudo systemctl start httpd

Step 4: Enable Apache to Start on Boot

sudo systemctl enable httpd

Step 5: Check Apache Status

sudo systemctl status httpd [It should show active (running). Press q to exit status view.]

Step 7: Test Apache Server

Copy your Public IPv4 address from the EC2 dashboard.

Paste it into a browser: http://

You should see the Apache Test Page

Part 3 – Host a Static Website on Apache

Step 1: Move to Web Root Folder
cd /var/www/html

Step 2: Create your HTML file
sudo nano index.html

Step 3: Add HTML content
Paste the following code:

```
<!DOCTYPE html>
<html>
<head>
<title>Welcome to My Website</title>
</head>
<body style="text-align:center; background-color: #f0f0f0;">
<h1>Hello from Apache on AWS EC2!</h1>
<p>This is a static website hosted on Apache web
server.</p>
</body>
</html>
```

Press Ctrl + O, Enter, then Ctrl + X to save and exit.

After Pressing Ctrl + O You'll see:
File Name to Write: index.html [Just press Enter to confirm saving with that name].

To Exit Nano: press Ctrl + X [This closes the Nano editor and will be back to the Linux prompt]

Step 4: Restart Apache
sudo systemctl restart httpd

Step 5: View Website

- In browser: http://<your-ec2-public-ip>
- You'll see your custom HTML page.

Optional: Add Multiple Pages

- Upload other pages like about.html, contact.html in the same directory.

Steps for launching an EC2 Instance with User Data Script to Automatically Install Apache and Host a Static Website.

In this method, you don't manually install Apache or upload files after connecting. Instead, you write a **shell script** in the **User Data** section (during instance creation). When the EC2 instance starts for the first time, it automatically:

1. Installs Apache (httpd)
2. Starts the service
3. Creates an index.html webpage
4. Hosts your website immediately after launch

Step 1: Sign in to AWS Management Console

Go to EC2 Dashboard → Click Launch Instance

Step 2: Name and OS

Name: AutoApacheWebServer
AMI: Choose Amazon Linux 2 AMI (Free tier eligible)
Instance Type: t3.micro

Step 3: Key Pair

Select existing key pair (or create new) → Format = .pem

Step 4: Network Settings

Allow HTTP traffic from the Internet (port 80)
Allow SSH traffic (port 22)

Step 5: Add User Data Script

Scroll down to Advanced Details → User data box.

This script:

- Updates all packages
- Installs and starts Apache
- Creates a sample index.html webpage in /var/www/html

Paste the following shell script:

```
#!/bin/bash
# Update packages
yum update -y

# Install Apache Web Server
yum install -y httpd

# Start Apache
systemctl start httpd
systemctl enable httpd

# Create website content
echo "<html>
<head><title>Welcome to My Auto Web Server</title></head>
<body style='text-align:center; background-color:#e9f5ff;'>
<h1>Welcome to EC2 Instance</h1>
<h2>Apache Installed Automatically via User Data Script</h2>
<p>This is a static website hosted on EC2 using User Data automation.</p>
</body>
</html>" > /var/www/html/index.html
```

Step 6: Launch the Instance

Click Launch Instance
Wait for the status → Running

Step 7: Test Your Web Server

Copy the Public IPv4 address of your instance.

Paste it in your browser: http://<your-public-ip>

You should immediately see your webpage without logging into EC2!

Date: 7-11-2025

Exercise-8: Create a Custom AMI from a Working EC2 Instance.
Launch an EC2 Instance using a Custom AMI
Delete the custom AMI

AMI (Amazon Machine Image) is a pre-configured template that contains only Operating System (e.g., Amazon Linux, Ubuntu, Windows) needed to launch an EC2 instance.

When you launch a new EC2 instance, you select an AMI as the base image.

A **Custom AMI** is created from your *own running EC2 instance* after you've installed software, uploaded website files, or applied settings.

Benefits:

1. **Reusability** – Launch multiple identical servers quickly.
2. **Backup** – Acts as a snapshot of your configured instance.
3. **Auto Scaling** – Used by Auto Scaling Groups to create identical instances automatically.
4. **Disaster Recovery** – You can recreate your setup if the original instance fails.
5. **Time-saving** – No need to reinstall Apache or re-upload files each time.

A Custom AMI is like a master copy of your EC2 setup. It ensures your website or app can be duplicated instantly and consistently.

Steps to Create a Custom AMI from a Working EC2 Instance

To capture the current configuration — installed packages, website files, and settings — into a reusable Amazon Machine Image (AMI).

Step 1: Select the running instance

Go to EC2 → Instances.
Select the instance that already hosts your website.
Or create an instance (add user data for web hosting)

Step 2: Create Image

From the Actions → Image and templates → Create image.

Step 3: Enter details

Image name: MyWebsiteAMI
Description: AMI created from configured Apache website instance
Leave "No reboot" unchecked (so the filesystem is consistent).

Step 4: Storage volumes

The root volume will appear automatically; keep defaults unless you need more space.

Step 5: Create image

Click **Create image**.

A confirmation message appears; note the **Image ID**.

Step 6: Verify creation

In left panel → **AMIs** → refresh until **Status = Available**.

Your custom AMI is now saved in that region and can be used to launch identical webserver instances.

Steps to Launch an EC2 Instance using a Custom AMI

To launch a new EC2 instance from a previously created Custom Amazon Machine Image (AMI) — containing your configured website and software.

Step 1: Go to AMIs

Open the EC2 Service dashboard.
In the left navigation pane, click AMIs (under "Images").

Step 2: Select Your Custom AMI

Locate the AMI you created earlier (e.g., MyWebsiteAMI).
Ensure Status = Available.

Step 3: Launch Instance from AMI

Select the AMI → click Launch instance from image.

Step 4: Configure Instance Details

Name: WebServer-from-Custom-AMI
Instance type: t3.micro (Free Tier eligible)
Key pair: Choose an existing .pem key for SSH access.
Network settings:
- VPC: Default
- Subnet: Public
- Security Group: Allow HTTP (80) and SSH (22)

Step 5: Storage (EBS Volume)

Keep default root volume (e.g., 8 GB gp3).

Step 6: Review and Launch

Click Launch instance.
Wait until the instance state becomes Running.

Step 7: Access the Website

Copy the Public IPv4 address from the instance details.
Open in a browser → http://<Public-IP>
You should see your same website, confirming the custom AMI works.

A new EC2 instance is successfully launched using the Custom AMI, automatically containing the OS, Apache, configurations, and website files — no manual setup required.

Steps to Delete the custom AMI

Deleting a **custom AMI** involves **deregistering** the image and then **deleting its associated EBS snapshot**.
When you deregister an AMI, it is removed from your account and can no longer be used to launch new instances.
However, the **snapshot** that was created along with the AMI still remains in your storage and continues to incur charges, so you must delete it separately to free up space and stop costs.
This ensures your AWS environment remains clean and cost-efficient.

Step 1 – Open EC2 Dashboard

Sign in to the AWS Management Console.
Navigate to EC2 service.
In the left navigation pane, scroll down to Images → AMIs.

Step 2 – Locate Your Custom AMI

In the Owned by me tab, you will see all AMIs you created (custom AMIs).
Select the AMI you want to delete.
You can identify it by Name or AMI ID.

Step 3 – Deregister the AMI

Select the AMI → Click on Actions dropdown.
Choose Deregister AMI.
Confirm by clicking Deregister in the pop-up.
This removes the AMI record, but not the underlying snapshot(s).

Step 4 – Delete the Associated Snapshot

To fully free up storage space (and avoid charges):

In the left navigation pane, click Elastic Block Store → Snapshots.
Find the snapshot linked to your deleted AMI.
You can check the Description column; it usually mentions the AMI ID.
Select the snapshot → Actions → Delete snapshot → Confirm Delete.

- The AMI is now deregistered (unavailable for future instance launches).
- The snapshot is also deleted, freeing up EBS storage and costs.

Date: 11-11-2025

Exercise–9 Mini Project –

MINI-PROJECT

Hosting a Multi-Page Website using EC2 and S3

To design and deploy a multi-page website hosted on an EC2 Linux instance (Apache) that fetches static assets (CSS, JS, images) from an Amazon S3 bucket.

This project demonstrates a two-tier cloud hosting model:

This mini-project demonstrates hybrid hosting: EC2 acts as the web server while S3 delivers static content. Together, they form a scalable, cost-effective architecture similar to real-world cloud applications.

Layer	Service	Role
Web Server	EC2 (Apache on Linux)	Hosts HTML pages (index.html, about.html, etc.)
Object Storage	S3	Stores and delivers static files (style.css, banner.jpg, favicon.ico)

Integration Flow: The EC2 web pages use public S3 object URLs to load all static assets.

OVERALL ORDER

1. Create S3 bucket
2. Upload static assets to S3 (CSS + images)
3. Make them public & copy URLs
4. Create EC2, install Apache
5. Create HTML files on EC2 and paste S3 URLs
6. Test in browser

Follow this order Because HTML needs the S3 URLs — so S3 must be ready first.

STEP 1: Create S3 bucket

Open **S3 → Create bucket**

Name: my-miniweb-demo-bucket (or any unique name)

Region: same as EC2

Uncheck “Block all public access” (for lab)

Create.

STEP 2: Create STATIC FILES (on your laptop first)

You need **three** static objects to upload to S3:

1. style.css
2. banner.jpg
3. about.jpg

Create a CSS file and save it as – style.css:

```
/* style.css */
body {
  font-family: Arial, sans-serif;
  background-color: #f8f8f8;
  margin: 0;
  padding: 0;
}

header {
  background: #007bff;
  color: white;
  padding: 15px;
  text-align: center;
}

.container {
  padding: 20px;
  background: white;
  max-width: 900px;
  margin: 20px auto;
  box-shadow: 0 0 5px rgba(0,0,0,0.1);
}

a {
  color: #007bff;
  text-decoration: none;
}

nav a {
  margin-right: 15px;
}
```

```
img {
  max-width: 100%;
}
```

1. Open **Notepad** (or Notepad++, VS Code, anything).
2. Paste the CSS.
3. Click **File → Save As…**
4. In the **File name** box, type: style.css
5. In **Save as type**, select **All Files (*.*)**
6. Save it.
7. Then upload style.css to your S3 bucket.

After you upload it to S3, copy the **Object URL** and use it in your HTML like this:

<link rel="stylesheet" href="https://your-bucket-name.s3.amazonaws.com/style.css">

Images:

- Save any image as **banner.jpg** (for homepage)
- Save another image as **about.jpg**

STEP 3: Upload to S3

In your bucket:

Click **Upload** → add:

- ✓ style.css
- ✓ banner.jpg
- ✓ about.jpg

After upload → select each object → **Make public**.

For each file, note the **Object URL**. It will look like:

- https://my-miniweb-demo-bucket.s3.amazonaws.com/style.css

- https://my-miniweb-demo-bucket.s3.amazonaws.com/banner.jpg
- https://my-miniweb-demo-bucket.s3.amazonaws.com/about.jpg

These links will be used in HTML.

Add bucket policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::my-miniweb-demo-bucket/*"
    }
  ]
}
```

(Replace bucket name.)

STEP 4: Create EC2 and install Apache

EC2 → Launch instance → Amazon Linux 2 → t3.micro

Security group: allow **HTTP (80)** and **SSH (22)**

Connect with SSH:

ssh -i "yourkey.pem" ec2-user@<EC2-Public-IP>

Install Apache:

sudo yum update -y

sudo yum install httpd -y

sudo systemctl start httpd

sudo systemctl enable httpd

Test: open http://<EC2-Public-IP> → Apache page appears.

STEP 5: Create HTML files on EC2

Go to Apache folder:

cd /var/www/html

We will create **3 pages**:

1. index.html (home)
2. about.html
3. contact.html

While writing HTML, **replace** the S3 links with your actual bucket links.

5.1 index.html

sudo nano index.html [Paste this (change bucket name in 2 places)]:

```
<!DOCTYPE html>
<html>
  <head>
    <title>My Mini Web Demo</title>
    <!-- CSS coming from S3 -->
    <link rel="stylesheet" href="https://my-miniweb-demo-
bucket.s3.amazonaws.com/style.css">
  </head>
  <body>
    <header>
      <h1>Welcome to My Website</h1>
      <nav>
        <a href="index.html">Home</a>
        <a href="about.html">About</a>
        <a href="contact.html">Contact</a>
      </nav>
    </header>

    <div class="container">
      <h2>Home Page</h2>
      <p>This website is hosted on an EC2 instance, but the images and CSS are coming from
S3.</p>
```

```
    <!-- Image coming from S3 -->
    <img src="https://my-miniweb-demo-bucket.s3.amazonaws.com/banner.jpg" alt="Banner Image">
  </div>
 </body>
</html>
```

Save → Ctrl+O, Enter → Ctrl+X.

5.2 about.html

sudo nano about.html [Paste this (change bucket name in 2 places)]:

```
<!DOCTYPE html>
<html>
 <head>
  <title>About Us</title>
  <link rel="stylesheet" href="https://my-miniweb-demo-bucket.s3.amazonaws.com/style.css">
 </head>
 <body>
  <header>
   <h1>About This Project</h1>
   <nav>
    <a href="index.html">Home</a>
    <a href="about.html">About</a>
    <a href="contact.html">Contact</a>
   </nav>
  </header>

  <div class="container">
   <h2>What are we doing here?</h2>
```

```
    <p>We are demonstrating integration between EC2 (for HTML) and S3 (for static assets).</p>
    <p>HTML files are stored in /var/www/html on EC2.</p>
    <p>CSS and images are stored in S3 and accessed using public object URLs.</p>

    <!-- Optional image from S3 -->
    <img src="https://my-miniweb-demo-bucket.s3.amazonaws.com/about.jpg" alt="About Image">
  </div>
 </body>
</html>
```

5.3 contact.html

sudo nano contact.html [Paste this (change bucket name in 1 place)]:

```
<!DOCTYPE html>
<html>
 <head>
  <title>Contact</title>
  <link rel="stylesheet" href="https://my-miniweb-demo-bucket.s3.amazonaws.com/style.css">
 </head>
 <body>
  <header>
   <h1>Contact Us</h1>
   <nav>
    <a href="index.html">Home</a>
    <a href="about.html">About</a>
    <a href="contact.html">Contact</a>
   </nav>
  </header>

  <div class="container">
   <h2>Get in touch</h2>
   <p>Email: demo@example.com</p>
   <p>This page is also hosted on EC2, but it is using the same CSS from S3 for a consistent look.</p>
  </div>
 </body>
</html>
```

STEP 6: Test

1. Open: http://<EC2-Public-IP>/ → home page
2. Click **About** → /about.html
3. Click **Contact** → /contact.html
4. Right-click → Inspect → Network → you will see CSS and images loading from S3.

QUICK STORAGE SUMMARY

Stored in S3 (public):

- style.css
- banner.jpg
- about.jpg (optional)

Stored in EC2 (/var/www/html):

- index.html
- about.html
- contact.html

Linked using S3 Object URL inside the HTML:

- <link rel="stylesheet" href="https://your-bucket.s3.amazonaws.com/style.css">
- <img src="https://your-bucket.s3.amazonaws.com/banner.jpg">

Viva Questions

No	Question	Expected Understanding
1	How is S3 integrated with EC2?	EC2 HTML uses direct S3 object URLs for images/CSS.
2	Why store static assets in S3?	S3 provides cost-efficient, durable storage and faster access.
3	What happens if the S3 bucket is private?	Browser shows AccessDenied for assets; need GetObject permission.
4	What is a Favicon?	A small icon displayed on the browser tab.
5	How to enable Versioning in S3?	Select bucket → Properties → Enable Versioning.
6	After stopping and starting EC2, will files persist?	Yes, stored on EBS volume.

7	What is the benefit of this two-tier design?	Demonstrates decoupled web and asset delivery layers.

Date: 12-11-2025

Exercise-10: Creation and Configuration of a Custom AWS Virtual Private Cloud (VPC)

[Including Public and Private Subnets, Internet Gateway, NAT Gateway, Route Tables]

Virtual Private Cloud [VPC]
It is a logically isolated section of the AWS Cloud where you can launch your AWS resources (like EC2 instances, databases, etc.) in a customized, secure network environment — similar to having your own private data center inside AWS.

It is a virtual network dedicated to your AWS account.

It gives you complete control over your networking environment, including IP address ranges, subnets, route tables, and network gateways.

Components of a VPC

Component	Description
CIDR Block (IP Range)	The range of IP addresses for your VPC (e.g., 10.0.0.0/16).
Subnets	Smaller divisions inside your VPC; can be Public (accessible from internet) or Private (internal only).
Internet Gateway (IGW)	Allows internet access for resources in public subnets.
Route Tables	Define how traffic is directed between subnets and gateways.
NAT Gateway / NAT Instance	Enables instances in private subnets to connect to the internet without being exposed.
Security Groups	Virtual firewalls that control inbound/outbound traffic at the instance level.
Network ACLs (Access Control Lists)	Additional firewall at the subnet level.
VPC Peering	Connects two VPCs so they can communicate privately.

Default VPC and **Custom VPC**

Characteristics of Default VPC

When you first create an AWS account, AWS automatically creates a default VPC for you in each region.

Feature	Description
Best For	Beginners, quick testing, learning environments, or temporary setups.
Created Automatically	One Default VPC per AWS Region (created by AWS).
Ready to Use	You can launch EC2 instances immediately — no setup needed.
CIDR Block	Always uses 172.31.0.0/16.
Subnets	One default subnet in each Availability Zone within the region.
Internet Connectivity	Each default subnet is a public subnet (has a route to Internet Gateway).

Route Table	Already configured to connect to the Internet Gateway.
Security Groups & NACLs	Default ones are automatically created and allow basic communication.

Characteristics of Custom VPC

A Custom VPC is created manually by the user to have complete control over the network configuration.

Feature	**Description**
Best For	Production environments, enterprise setups, or multi-tier architectures.
Created Manually	You define the VPC and its settings yourself.
CIDR Block	You can choose your own IP range (e.g., 10.0.0.0/16).
Subnets	You decide how many subnets, and whether they are public or private.
Internet Connectivity	You attach your own Internet Gateway.
Route Tables	Must be created and configured manually.
Security	You can create custom Security Groups and NACLs as needed.

Subnets

- Subdivisions inside a VPC, used to organize resources.
- Each subnet belongs to one Availability Zone.
- Two types:
  - **Public Subnet** → Connected to Internet Gateway; for web servers.
  - **Private Subnet** → No direct internet access; for databases or internal apps.
- CIDR examples:
  - Public: 10.0.1.0/24
  - Private: 10.0.2.0/24

Internet Gateway (IGW)

- A gateway that connects your VPC to the Internet.
- Required for instances in a public subnet to receive internet traffic.
- Must be attached to the VPC and referenced in the route table.
- Supports bi-directional communication (inbound and outbound).

NAT Gateway

- Enables outbound internet access for private subnet instances.
- Allows downloads and updates (e.g., OS patches) without exposing private IPs.
- Deployed inside a public subnet.
- Needs an Elastic IP for internet access.
- Traffic is one-way: private → internet only (not vice versa).

Route Tables

- Define rules (routes) that determine where network traffic goes.
- Each subnet must be associated with one route table.
- Common routes:
    - For public subnet → 0.0.0.0/0 → Internet Gateway
    - For private subnet → 0.0.0.0/0 → NAT Gateway
- Ensures proper separation between public and private networks.

Security Groups

- **Instance-level firewalls** controlling inbound and outbound traffic.
- Stateful: if inbound traffic is allowed, corresponding outbound is automatically allowed.
- Rules are based on protocol, port number, and source/destination.
- Example:
    - WebServer-SG: allows HTTP(80), HTTPS(443), SSH(22)
    - Database-SG: allows MySQL(3306) from WebServer-SG only

Network ACL (Access Control List)

- **Subnet-level firewall**, acts as an additional layer of security.
- **Stateless**: inbound and outbound rules must be defined separately.
- Default NACL allows all traffic; custom NACLs can be restrictive.
- Used for fine-grained control or compliance environments.

EC2 Instances

- Virtual machines running inside your subnets.
- Public subnet → hosts Web Server (Apache).
- Private subnet → hosts Database Server (MySQL).
- Public EC2s get a public IP; private ones use private IPs only.
- Controlled by their Security Groups and Route Tables.

Elastic IP (EIP)

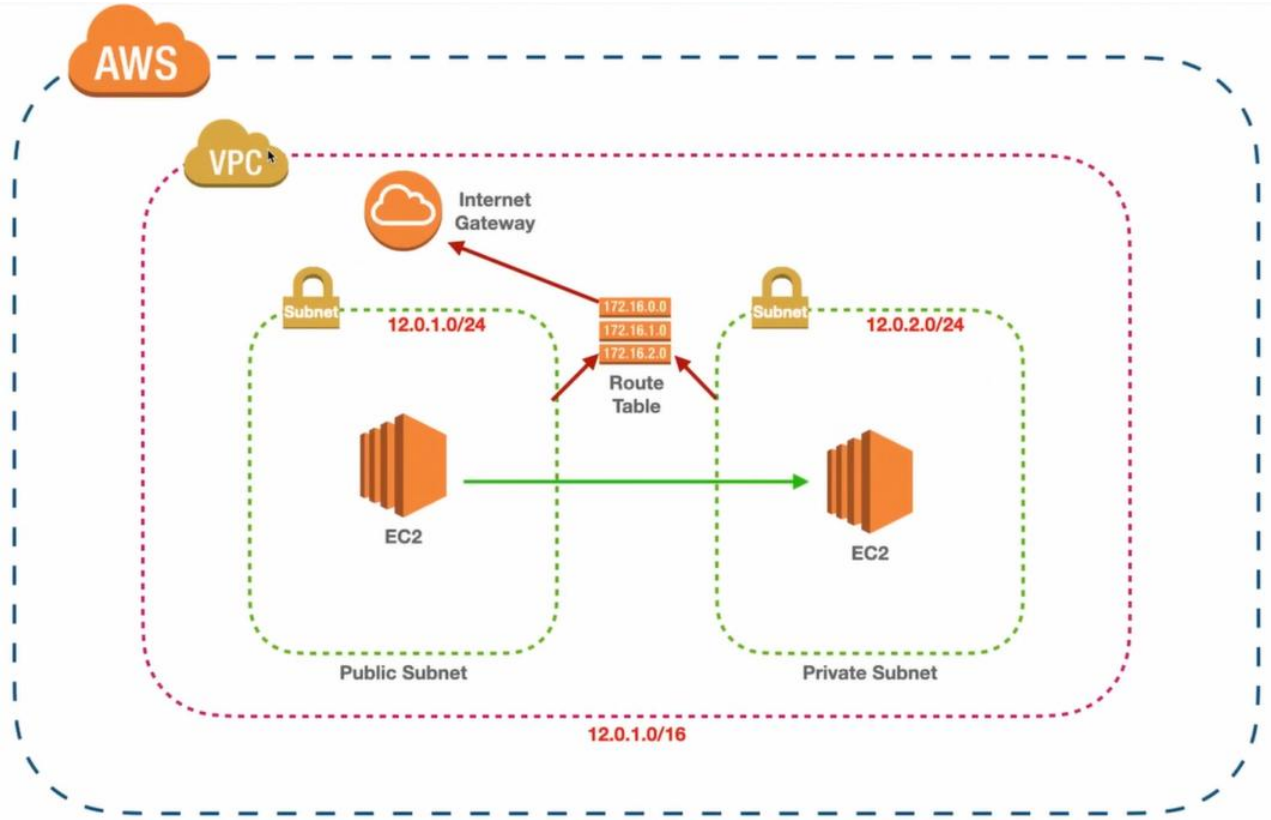
- A **static, public IPv4 address** that can be attached to an EC2 or NAT Gateway.
- Remains constant even if the instance is stopped or restarted.
- Useful for **NAT Gateways**, load balancers, or fixed server access.

Example: Two-Tier Architecture

Tier	Subnet	Function	Internet Access
Web Tier	Public Subnet	Hosts front-end web server	Yes (via IGW)
Database Tier	Private Subnet	Hosts back-end database	Outbound only (via NATGW)

Create a new VPC for a web application:

- One **Public Subnet** for web servers (via Internet Gateway)
- One **Private Subnet** for databases (via NAT Gateway)
- Custom route tables and tighter security rules.



Objective

To design and configure a **Virtual Private Cloud (VPC)** in AWS with:

- One **Public Subnet** for web servers (via **Internet Gateway**)
- One **Private Subnet** for databases (via **NAT Gateway**)
- Separate **Route Tables** for public and private subnets
- Custom **Security Groups** to enforce network isolation

Step 1 – Create a New VPC

- Open AWS Management Console → VPC.
- Click Create VPC.
- Choose VPC only option.

- Enter:
    - Name → MyWebAppVPC
    - IPv4 CIDR block → 10.0.0.0/16
    - Tenancy → Default
- Click Create VPC.

This allocates a private IP range for your virtual network.

Step 2 – Create Subnets

We'll create two subnets inside the VPC.

(a) Public Subnet

- Go to Subnets → Create subnet.
- Select VPC: MyWebAppVPC.
- Choose Availability Zone A.
- Enter:
    - Name → PublicSubnet
    - IPv4 CIDR block → 10.0.1.0/24
- Click Create subnet.

(b) Private Subnet

- Click Create subnet.
- Select same VPC.
- Choose Availability Zone B.
- Enter:
    - Name → PrivateSubnet
    - IPv4 CIDR block → 10.0.2.0/24
- Click Create subnet.

Step 3 – Create and Attach an Internet Gateway

- In the left navigation pane, scroll down and click on "Internet Gateways".
- Internet Gateways → Create Internet Gateway.
    - Name: MyWebApp-IGW
- Click Create Internet Gateway

At this point, the IGW exists but is not yet connected to your VPC.

- **Attach the Internet Gateway to Your VPC**
    - Select the IGW you just created (checkbox).
    - Click on the **"Actions"** drop-down.
    - Choose **"Attach to VPC."**
    - From the list, select your **VPC name**, e.g. MyWebAppVPC.
    - Click "Attach Internet Gateway."

Now the IGW is linked to your VPC and the public subnet can reach the internet.

Step 4 – Configure Route Table for IGW

Public Route Table

- Go to Route Tables → Create route table.
  - Name → PublicRT
  - VPC → MyWebAppVPC
- Under Routes → Edit routes → Add route
  - Destination: 0.0.0.0/0
  - Target: Internet Gateway (MyWebApp-IGW)
- Under Subnet Associations → Edit subnet associations → Select PublicSubnet → Save.

Now the PublicSubnet has internet access.

Step 5 – Create a NAT Gateway

NOTE: NAT Gateway must always be created in a public subnet

- Go to NAT Gateways → Create NAT Gateway.
- Name → NAT-GW
- Choose:
  - Subnet → PublicSubnet
  - Elastic IP Allocation ID → Click Allocate Elastic IP
- Click Create NAT Gateway.

This allows instances in private subnet to access the internet (e.g., for updates) without being exposed.

Note: NAT Gateway is a **paid resource**.

Step 6 – Configure Route Table for IGW

Private Route Table

- Create another Route Table → Name PrivateRT.
- Under Routes → Edit routes → Add route
  - Destination: 0.0.0.0/0
  - Target: NAT Gateway (MyWebApp-NATGW)
- Under Subnet Associations → Select PrivateSubnet → Save.

PrivateSubnet traffic goes through the NAT Gateway.

Note:

Each subnet in a VPC can be associated with **only one route table**.
If a subnet is not explicitly associated with a custom table, it will automatically use the **Main Route Table** created by default with the VPC.

DATE: 14-11-2025

Exercise-11

Launching and Configuring EC2 Instances for Web Server in Public Subnet and Database Server in Private Subnet Using NAT Gateway for Outbound Access

Step 1 — Launch Windows instance in Public Subnet

- Go to EC2 → Launch Instance.
- Choose:
  - AMI → Windows Server (Free tier eligible)
  - Instance type → t2.micro / t3.micro
- Select:
  - VPC → MyWebAppVPC
  - Subnet → PublicSubnet
  - Auto assign Public IP → Enable
- Security Group:
  - Create WebInstance-SG
  - Allow:
    - RDP (3389) → Anywhere (for practice)
- Launch instance using key pair (.pem).

Step 2 — Launch Windows instance in Private Subnet

- Click Launch Instance.
- Choose:
  - Windows Server AMI
- Select:
  - VPC → MyWebAppVPC
  - Subnet → PrivateSubnet
  - Auto assign Public IP → Disable
- Security Group:
  - Create DBInstance-SG
  - Allow RDP only from WebInstance-SG
- Launch instance.

The DBInstance is now **fully isolated** and cannot be accessed directly from the internet.

Step 3 — Connect to Public Windows Instance

1. Select WebInstance → Click Connect.
2. Choose RDP Client tab.
3. Click Get Password.
4. Upload your .pem key pair.
5. It shows the decrypted Windows Administrator password.
6. Copy the Public IP into a document for further use.

Connect using RDP

- Open Remote Desktop Connection (mstsc).
- In the dialog:
    - Computer → Public IP of WebInstance
- Click Connect.
- Credentials dialog:
- Username → Administrator
- Password → Paste decrypted password
- Click OK.

You are now inside the public Windows instance.

Step 4 — connect to private windows instance

We cannot connect directly from your laptop → No Public IP.
We must connect **from within WebInstance** (jump server / bastion host).

Remote Login from WebInstance → DBInstance

- While logged into WebInstance, open Remote Desktop Connection. **[mstsc]**
- Enter:
    - Computer → Private IP of DBInstance
- Click Connect.
- Credentials:
    - Username → Administrator
    - Password → Paste the decrypted password (same key pair)
- Click OK.

You are now inside the private Windows instance.

Step 5 — testing NAT gateway connectivity (Verify Internet Access)

From WebInstance (Public Subnet)

- Open a browser → Internet should work (through IGW).

From DBInstance (Private Subnet)

- Open browser → Internet should also work (through NAT Gateway).
- Internet icon will show "Internet Access".

Security Check

- DBInstance cannot receive inbound traffic from internet.
- Only outbound is allowed via NAT (safe for DB servers).

Test: From DBInstance (Private Subnet) → ping Google (Outbound Allowed)

Steps
Connect to DBInstance (using RDP from WebInstance).
Open Command Prompt inside DBInstance.
Type: ping google.com
Expected Result

- It will successfully ping google.com
- You will see replies like:
  Reply from 142.250.xxx.xxx: bytes=32 time=20ms TTL=115

Why does this work?

- Outbound traffic is allowed from Private Subnet → NAT Gateway → Internet.
- NAT Gateway acts as a proxy for the private instance.
- So the private instance can reach internet,
  but internet cannot reach the private instance.

What will NOT work?
From the Private DBInstance: ping <Your Own Public IP>
or anyone trying to ping: ping <DBInstance Private IP>

Both will fail because:

- Inbound traffic is blocked
- DBInstance has no Public IP
- SG allows inbound only from WebInstance-SG

Private instance → internet = YES (via NAT Gateway)
Internet → private instance = NO (fully blocked)
Because NAT Gateway is **one-way** only.

Elastic IP address

- A static IP address is a permanent address that doesn't change. You can manually configure a device to have a static IP address.
- An Elastic IP address is static and has to be used in a specific Region, it cannot be moved to a different Region.
- An Elastic IP address comes from Amazon's pool of IPv4 addresses.
- To use an Elastic IP address, you first allocate one to your account, and then associate it with your instance or a network interface.
- When you associate an Elastic IP address with an instance or its primary network interface, if the instance already has a public IPv4 address associated with it, that public IPv4 address is released back into Amazon's pool of public IPv4 addresses and the Elastic IP address is associated with the instance instead.
- You can disassociate an Elastic IP address from a resource, and then associate it with a different resource.
- A disassociated Elastic IP address remains allocated to your account until you explicitly release it.

- You are charged for all Elastic IP addresses in your account, regardless of whether they are associated or disassociated with an instance.
- Static IP addresses are especially important in cases where a device has to be quickly found over the internet on a permanent basis.
- Web Servers: A website must have one or more static IP addresses to be assigned to the domain always point to the correct server.

DATE: 20-11-25

Exercise–13 Stress Testing a Linux EC2 Instance (CPU Load Test)

Objective:
To generate high CPU load on an Amazon EC2 Linux instance using the stress-ng tool and observe CPU utilization in CloudWatch.

Step 1 — Launch a Linux EC2 Instance

1. Log in to the AWS Console.
2. Go to **EC2 → Instances → Launch Instance**.
3. Name: **StressTest-EC2**
4. AMI: **Amazon Linux 2023 (Free Tier eligible)**
5. Instance type: **t2.micro** / **t3.micro**
6. Key pair: Select or create a .pem key.
7. Security Group:
    - Allow **SSH (22)** from My IP.
    - Allow **HTTP (80)** from anywhere (optional).
8. Launch the instance.

Step 2 — Connect to the EC2 Instance

Use Windows PowerShell
Navigate to the folder where pem file is located and type the following command:
ssh -i "your-key.pem" ec2-user@<public-ip>

Step 3 — Install Apache (Optional, to verify the instance is working)

sudo yum install httpd -y
sudo systemctl start httpd
sudo systemctl enable httpd
Create a test web page:
echo "<h1>EC2 Stress Test Demo — $(hostname)</h1>" | sudo tee /var/www/html/index.html

STEP 4 — Install and Run the Stress Testing Tool (stress-ng)

(For Amazon Linux 2023 EC2 Instances)
Move to the ec2-user home directory

(It is recommended to run stress-ng from the home folder)
cd ~

Install stress-ng

Amazon Linux 2023 includes stress-ng directly through dnf, so install it using:
sudo dnf install stress-ng -y

Run a CPU Stress Test

Generate high CPU load using 4 CPU workers for 2 minutes:

stress-ng --cpu 4 --timeout 120

Expected Result

- Terminal becomes busy during the 120-second load test
- After completion, you will see:

successful run completed in 120.02s

- CPU usage will spike to 90–100% (you can check using top)

Step 5 — Run Stress Test (CPU Load Generation)

Move to home directory to avoid permission issues:

```
cd ~
```

Run CPU stress for 2 minutes using 4 CPU workers:

```
stress-ng --cpu 4 --timeout 120
```

You should see messages like:

```
stress-ng: info: dispatching hogs: 4 cpu
stress-ng: info: successful run completed in 120.02s
```

This will increase CPU usage to ~100% for the duration.

Step 6 — Observe CPU Utilization in CloudWatch

Go to CloudWatch → Metrics → EC2 → Per-Instance Metrics

Select:

CPUUtilization → InstanceId → your instance

View graph in 1-minute or 5-minute intervals.

You should see a sharp spike during the 2-minute stress period.

Step 7 — Stop or Terminate the Instance

To avoid charges:

Option A — Stop the instance (safe):

Actions → Instance State → Stop

Option B — Terminate (permanently delete):

Actions → Instance State → Terminate

Expected Output

- CPU Utilization in CloudWatch should reach 90–100%.
- Stress test completes without errors.
- Students understand how CPU load affects EC2 metrics.

DATE: 28-12-25

Exercise–18: Creating and Operating a NoSQL Key-Value Database using Amazon DynamoDB

To create an Amazon DynamoDB table and perform CRUD operations (Create, Read, Update, Delete) using the AWS Management Console, and understand Partition Key, Sort Key, Query vs Scan, and table cleanup.

Phase 1: Create DynamoDB Table

Create a DynamoDB table to store Student Records.
Store items like: USN, Name, Semester, Course, Attendance, IA1Marks

Step 1: Open DynamoDB

- Login to AWS Console
- Search → type DynamoDB → open Amazon DynamoDB

Step 2: Create a Table

- Left menu → Tables
- Click Create table
- Fill details:

Table details

- Table name: MCA_StudentLabInternals
- Partition key (PK): USN (Type: String)
- Sort key (SK): CourseCode (Type: String)
  (Enable sort key option by setting sort key)

Why this design?

- One student can have multiple courses → Sort key separates records per course.
- This creates a composite primary key (PK + SK).

Step 3: Table settings

- Under Table settings, choose:
  Default settings (recommended for lab)
- Ensure Capacity mode is: On-demand (default already selected)

Step 4: Create

- Click Create table
- Wait until table status becomes Active

Phase 2: Insert Items (Create Data)

Step 5: Open Table and Add Items

- Click the table: MCA_StudentLabInternals
- Click: Explore table items
- Click Create item

Step 6: Add Item 1 (Student 1 - Course 1)

- You will see attributes:
  - USN (String)
  - CourseCode (String)

  Enter:
  - USN = 1MS24MCA001
  - CourseCode = CCL301

  Now add additional attributes (click **Add new attribute**):

- Name (String) = Arun
- Semester (Number) = 3
- Attendance (Number) = 86
- IA1Marks (Number) = 18

Click **Create item**

Step 7: Add Item 2 (Same student - another course)

Repeat Create item with:

- USN = 1MS24MCA001
- CourseCode = DBS301
- Name = Arun
- Semester = 3
- Attendance = 88
- IA1Marks = 20

Step 8: Add Item 3 (Another student)

Create item:

- USN = 1MS24MCA002
- CourseCode = CCL301
- Name = Chitra
- Semester = 3
- Attendance = 74
- IA1Marks = 14

You should now see 3 items in the table list.

Phase 3: Read Data (Get / Query / Scan)

Step 9: Get a single item (exact PK + SK)

- In "Explore table items", use search/filter:
- Use USN = 1MS24MC001 and CourseCode = CCL301
- Open the item → verify all attributes

Key concept:

To uniquely identify an item in a PK+SK table, you must provide **both**.

Step 10: Query – fetch all courses for one student

- Click Run query
- Set Partition key condition: USN equals 1MS24MCA001
- Run

Expected output:

- Items for Arun in both CCL301 and DBS301

Key concept:

Query works only with Partition Key (and optional Sort Key conditions). It is efficient.

Step 11: Scan (Not for large tables)

- Click Scan
- Run scan without filters

Expected output:

- All items (Arun + Chitra)

Key concept:

Scan reads the entire table → slow/costly for big tables.

Phase 4: Update Data

Step 12: Update IA1 marks of Chitra for CCL301

- Open item where:
  USN = 1MS24MCA002
  CourseCode = CCL301
- Click Edit
- Change: IA1Marks from 14 to 16
- Click Save changes

Verify updated value appears.

Phase 5: Delete Data

Step 13: Delete one item (Arun's DBS301 record)

- Select item:
  - USN = 1MS24MCA001
  - CourseCode = DBS301
- Click **Delete**
- Confirm delete

Now total items should reduce by 1.

Phase 6: Cleanup (Must Do to avoid charges)

Step 15: Delete the Table

- DynamoDB → Tables
- Select MCA_StudentLabInternals
- Click Delete
- Type confirmation (if asked) and delete

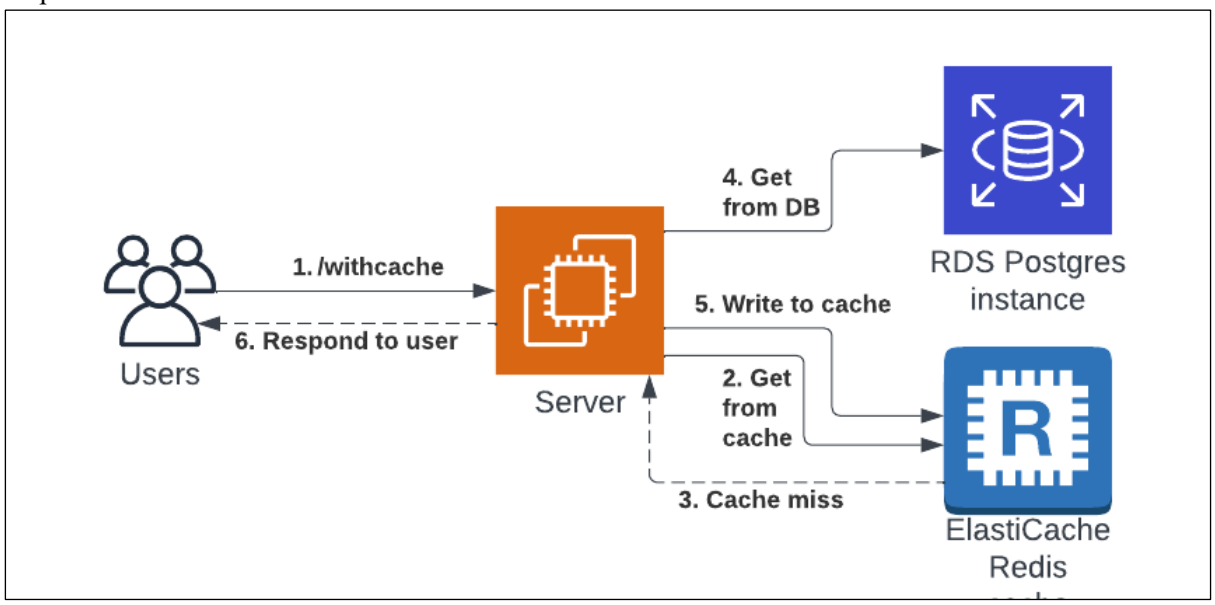
Ensure table disappears from list.

DATE: 03-12-25

Exercise–19: ElastiCache (Redis) as an In-Memory Cache

To implement Amazon ElastiCache (Redis) as an in-memory caching service by deploying a Redis cluster and performing basic cache operations from an EC2 instance.

Application-Level Data Flow (Logical)
Step 1: User requests data
Step 2: Application checks ElastiCache (Redis)
Step 3: If data exists → return from cache (FAST)
Step 4: If data does not exist → fetch from RDS
Step 5: Store fetched data in ElastiCache
Step 6: Return data to user



This exercise provides **exposure** to an industry-used in-memory data store.
Redis improves performance by serving frequently accessed data from memory and is typically used **in front of databases** in real-world applications.

Feature	RDS	ElastiCache
Storage	Disk	RAM
Data lifetime	Permanent	Temporary
Access speed	Slower	Very fast
TTL support	No	Yes

Phase-1 → EC2 creation + valkey-cli installation
Phase-2 → Redis cache creation
Phase-3 → Connect EC2 → Redis engine and run commands

Phase-1: Launch EC2 Client using Amazon Linux 2023 (for Valkey / Redis Client)
Purpose of Phase-1
To create an EC2 instance using **Amazon Linux 2023** that will act as a **client machine** to connect to Amazon ElastiCache (Redis OSS) using **valkey-cli**.

Step 1: Select AWS Region

- Choose ONE region and stick to it for the entire exercise
  ap-south-1 (Mumbai) *(recommended)*
- Ensure ElastiCache and EC2 will be in the SAME region

Step 2: Launch EC2 Instance

1. Go to **AWS Console → EC2**
2. Click **Launch instance**

Step 3: Configure Instance Basics

- Name: RedisClient-AL2023
- AMI: Select Amazon Linux 2023 AMI
- Instance Type: Select t3.micro (Free Tier eligible)
- Key Pair: Select an existing key pair OR create a new one (RSA, .pem)
- Network & Security
  - Network
    - VPC: Default VPC
    - Subnet: No preference
    - Auto-assign public IP: Enabled
- Security Group (VERY IMPORTANT)
  Create a new security group:
  - Security Group Name: SG-RedisClient
  - Description: Security group for Redis client EC2
    Inbound Rules

Type	Port	Source
SSH	22	Anywhere 0.0.0.0/0

Do NOT add Redis (6379) here (The client does not listen on 6379)
Outbound rules: Allow all (default)

Step 5: Storage

- Keep default

Step 6: Launch Instance

- Click Launch instance
- Wait until Instance State = Running

Step 7: Connect to EC2

1. EC2 → Instances → select RedisClient-AL2023
2. Click Connect
3. Choose EC2 Instance Connect
4. Click Connect

You are now inside the EC2 terminal.

Step 8: Install Valkey Client

Run the following commands:

sudo dnf update -y
sudo dnf install -y valkey

Verify installation:
valkey-cli --version
Expected Output (example)
valkey-cli 8.x.x
This confirms the EC2 is ready as a Redis-compatible client.

Note: why install valkey and not redis??
Amazon Linux 2023 does not provide redis-cli directly.
AWS now provides **Valkey**, which is fully Redis-protocol compatible.
Hence, we use **valkey-cli** to connect to ElastiCache Redis.

Phase-2: Create Amazon ElastiCache (Redis OSS) Cluster

Purpose of Phase-2
To create an Amazon ElastiCache Redis OSS cluster that will act as an in-memory cache, accessible from the EC2 client created in Phase-1.

Step 1: Confirm AWS Region

- Ensure you are in the **same region** used in Phase-1
  EC2 and ElastiCache must be in the SAME region and VPC.

Step 2: Open ElastiCache Console

1. AWS Console → **Services**
2. Select ElastiCache
3. Click Create cache

Step 3: Select Cache Engine

- **Engine**: **Redis OSS**

Step 4: Choose Deployment Settings

- Deployment option: Node-based cluster
- Creation method: Easy create

Easy create is used to avoid advanced production settings.

Step 5: Select Configuration

- **Configuration**: **Demo**

This automatically selects:

- A small, low-cost node (e.g., cache.t4g.micro)
- Suitable for labs and practice

Step 6: Provide Cluster Information

- Cache name: lab-redis
- Description: Optional (lab-redis)

Step 7: Configure Network and Subnet Group
Network

- Network type: IPv4

Subnet Group

- Select: Create a new subnet group
    - Subnet group name: redis-subnet-group
    - VPC: Default VPC
    - Subnets: Leave AWS auto-selected subnets unchanged

No manual subnet selection required.

Step 8: Configure Security

Security Group

- Create or select a security group:
    - Name: SG-RedisCache

Inbound Rule for Redis

Add **one inbound rule** to SG-RedisCache:

Type	Port	Source
Custom TCP	6379	SG-RedisClient

This allows only the EC2 client to access Redis.

Step 9: Authentication

- Authentication: Disabled

Step 10: Create Cache

1. Review all settings
2. Click Create
3. Wait until Status = Available

This may take a few minutes.

Step 11: Note the Redis Endpoint

1. Click on the cache name lab-redis
2. Copy the **Configuration Endpoint**
    - Example: lab-redis.xxxxxx.cache.amazonaws.com

This endpoint will be used in **Phase-3** to connect from EC2.

Note:
We have created an in-memory Redis cache using Amazon ElastiCache.
It runs inside the AWS VPC and does not have a public IP.
Only our EC2 client is allowed to access it using port 6379.

Phase-3: Connect EC2 to ElastiCache Redis and Execute Cache Commands

Purpose of Phase-3

To connect the EC2 client (Amazon Linux 2023) to the ElastiCache Redis OSS cluster using valkey-cli and demonstrate basic in-memory cache operations.

Pre-checks - Before connecting, confirm:

- EC2 and ElastiCache are in the same AWS region
- EC2 security group = SG-RedisClient
- Redis security group = SG-RedisCache
- Redis security group allows port 6379 from SG-RedisClient
- Redis Status = Available

- You have copied the Primary Endpoint

Step 1: Connect to EC2

1. AWS Console → **EC2**
2. Select instance RedisClient-AL2023
3. Click **Connect**
4. Choose **EC2 Instance Connect**
5. Click **Connect**

You are now inside the EC2 terminal.

Step 2: Verify Valkey Client

Run: valkey-cli --version

Expected Output (example)

valkey-cli 8.x.x

This confirms the EC2 is ready to act as a Redis-compatible client.

Step 3: Connect to ElastiCache Redis

Use the Configuration Endpoint from Phase-2.

valkey-cli -h < Configuration_ENDPOINT> -p 6379

Example: valkey-cli -h lab-redis.xxxxxx.cache.amazonaws.com -p 6379 --tls -c

Expected Result

You should see a prompt like:

lab-redis.xxxxxx.cache.amazonaws.com:6379>

This means the connection is successful.

Step 4: Execute Redis / Valkey Commands

These commands simulate what an application does internally.

Test Connectivity

PING

Expected Output

PONG

Store and Retrieve Data (SET / GET)

SET course "Cloud Computing"

GET course

Expected Output

"Cloud Computing"

Demonstrates **key–value storage in memory**.

Counter Example (INCR)

INCR visits

INCR visits

GET visits

Expected Output

"2"

NOTE: Common real-world use - page views, hit counters.

4.4 Set Data with Expiry (TTL)

SET notice "Results Published" EX 60
TTL notice
GET notice
Expected Output

- TTL shows a value ≤ **60**
- GET returns:

"Results Published"
Shows **temporary cache data**.

4.5 Verify Automatic Expiry
Wait ~60 seconds, then run:
GET notice
Expected Output
(nil)
Confirms data is **automatically removed from memory**.

4.6 Delete Data Manually
DEL course
GET course
Expected Output
(nil)

Step 5: Exit Redis Client
EXIT

Note:
"The application first checks Redis.
If data is present, it is returned immediately from memory.
If not present, the application fetches data from the database and stores it in Redis with a TTL.
Redis automatically removes the data after expiry."

Phase-3 Outcome

- EC2 successfully connected to ElastiCache Redis
- In-memory key–value operations verified
- Temporary storage and TTL behavior observed
- Redis used as a **cache**, not as a primary database

Common Errors & Quick Fix

Problem	**Reason**	**Fix**
Connection timeout	Wrong SG or region	Check SG-RedisCache inbound rule
Command hangs	Redis not Available	Wait & retry
(nil) output	Key expired	Expected behavior

Clean-Up (Mandatory)
Step 1: Delete Redis Cluster

- ElastiCache → Select lab-redis → Delete
- Disable snapshots

Step 2: Terminate EC2 Instance

- EC2 → Instances → Terminate RedisClient-EC2

Step 3: Optional

- Delete unused security groups

Redis Commands Explanation

- **SET** course "Cloud Computing"
- **GET** course
- **EXPIRE** course 30
- **TTL** course
- The above commands simulate application caching behavior.
  The SET command represents storing frequently accessed data in cache.
  The EXPIRE command shows that cached data is temporary and stored in memory.
  After expiry, the application would fetch fresh data from the database again.

DATE: 12-12-25

Exercise–22: CloudFormation – Launch EC2 (Amazon Linux 2023) + Install Apache using UserData

Create an EC2 instance using AWS CloudFormation (YAML template) and automatically install Apache web server (httpd) using UserData, then verify the website from a browser.

Part A — Create Key Pair (One-time setup)

Step A1: Open EC2 Key Pairs

1. AWS Console → Search EC2
2. Left menu → Key Pairs (under "Network & Security")
3. Click Create key pair

Step A2: Create key pair

- Name: pemkeypair (any name is fine)
- Key pair type: RSA
- Private key file format: **.**pem

Click Create key pair
A file will download like: pemkeypair.pem
Note: CloudFormation uses key pair NAME (example: pemkeypair), not the file name extension.

Part B — Create CloudFormation Template File (Amazon Linux 2023 + Apache)

Create YAML file on your computer

- Open Notepad
- Paste the full YAML template given below
- Save as: ec2-apache-al2023.yaml
    1. Save type: All files
    2. Encoding: UTF-8 (if asked)

Full CloudFormation Template (Amazon Linux 2023)

Important:

- Do **not** add .pem anywhere.
- You will select Key Pair from dropdown during stack creation later on.

```
AWSTemplateFormatVersion: "2010-09-09"
Description: Launch EC2 (Amazon Linux 2023) and install Apache

Parameters:
  KeyName:
    Type: AWS::EC2::KeyPair::KeyName
    Description: Select an existing EC2 Key Pair
```

```
  AmazonLinux2023AMI:
    Type: AWS::SSM::Parameter::Value<AWS::EC2::Image::Id>
    Default: /aws/service/ami-amazon-linux-latest/al2023-ami-kernel-default-x86_64

Resources:
  WebServerSG:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Allow SSH and HTTP
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 22
          ToPort: 22
          CidrIp: 0.0.0.0/0
        - IpProtocol: tcp
          FromPort: 80
          ToPort: 80
          CidrIp: 0.0.0.0/0

  WebServerInstance:
    Type: AWS::EC2::Instance
    Properties:
      InstanceType: t3.micro
      KeyName: !Ref KeyName
      ImageId: !Ref AmazonLinux2023AMI
      SecurityGroupIds:
        - !Ref WebServerSG
      UserData:
        Fn::Base64: |
          #!/bin/bash
          dnf update -y
          dnf install -y httpd
          systemctl enable httpd
          systemctl start httpd
          echo "<h1>Apache Installed via CloudFormation (Amazon Linux 2023)</h1>" >
/var/www/html/index.html

Outputs:
  WebsiteURL:
    Description: Apache Website URL
    Value: !Sub "http://${WebServerInstance.PublicDnsName}"
```

Part C — Create CloudFormation Stack (Console Steps)

Step C1: Open CloudFormation

- AWS Console → Search CloudFormation
- Click Stacks
- Click Create stack → With new resources (standard)

Step C2: Prepare template (select correct options)

- Under Prepare template:
  Select Choose an existing template
- Under Template source:
  Select Upload a template file
- Click Choose file → select ec2-apache-al2023.yaml
- Click Next

Part D — Specify Stack Details

Step D1: Stack name

- Stack name: EC2-Apache-AL2023

Click **Next**

Step D2: Parameters

- Under **KeyName**, select your key pair name from dropdown [Example: pemkeypair]

Click **Next**

Part E — Configure Stack Options (keep default)

- Leave everything as default
- Click **Next**

Part F — Review and Create

- Scroll down
- Click **Create stack**

Part G — Monitor Stack Creation

- Wait for Stack status to become: CREATE_COMPLETE
- Open the stack → click Outputs tab
- Copy WebsiteURL
- Paste URL in browser

Expected Output in browser:
Apache Installed via CloudFormation UserData (Amazon Linux 2023)!

Part H — Verify in EC2

Go to **EC2 → Instances**
Instance should be running
Security group should allow:

- SSH 22
- HTTP 80

Troubleshooting (Common Errors)

Website not opening
Check:

- EC2 instance status checks are 2/2 passed
- Security group has port 80 open
- Wait 2–3 minutes (UserData takes time)

Stack went to ROLLBACK
Go to stack → Events tab → check the failure reason
Most common reason: Wrong Key Pair selected / key pair does not exist

Clean-up

To avoid charges:

1. CloudFormation → Stacks
2. Select EC2-Apache-AL2023
3. Click Delete
4. Confirm

This deletes EC2 + Security Group automatically.

DATE: 17-12-25

Exercise–23: EC2 + S3 (Static Content Pulled from S3 using CloudFormation)

Create an **S3 bucket** using CloudFormation.

Upload a static HTML file (index.html) to S3.

Launch **EC2 (Amazon Linux 2023) + Apache** using CloudFormation.

EC2 will **pull index.html from S3** and host it via Apache.

Pre-requisites

- Region: **Mumbai (ap-south-1)**
- A Key Pair exists (example: pemkeypair)

One-time: Create Key Pair

EC2 → Key Pairs → Create key pair

- Name: pemkeypair
- Format: .pem
  Download it and keep safe.

PART 1 — Stack-1: Create S3 Bucket (CloudFormation)

Step 1.1: Create S3 template file

Create a file: **stack1-s3-bucket.yaml** and paste:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: Create an S3 bucket to store website content (index.html)
Resources:
  WebsiteBucket:
    Type: AWS::S3::Bucket

Outputs:
  BucketName:
    Description: S3 Bucket Name (use this to upload index.html)
    Value: !Ref WebsiteBucket
```

Step 1.2: Create stack

CloudFormation → Stacks → Create stack → With new resources

- Choose an existing template

- Upload a template file → stack1-s3-bucket.yaml
- Stack name: S3-Website-Bucket
- Create stack

Step 1.3: Copy bucket name

Open stack → **Outputs** → copy **BucketName**

PART 2 — Upload Static Content to S3 (Manual)

Step 2.1: Create index.html on your PC

Create a file named **index.html** with this content:

```
<!DOCTYPE html>
<html>
<head>
  <title>EC2 + S3 Demo</title>
</head>
<body>
  <h1>Hello! This page was pulled from S3 to EC2 automatically.</h1>
  <p>Deployed using CloudFormation + UserData</p>
</body>
</html>
```

Step 2.2: Upload to S3 bucket

S3 → Buckets → open your bucket (from Output) → Upload

- Upload **index.html**
- Keep it at **root** (no folder)
- Upload

Now S3 has: s3://<your-bucket-name>/index.html

PART 3 — Stack-2: Launch EC2 + Apache + Pull from S3

This stack will:

- Create IAM Role (permission to read the bucket)
- Create Security Group (22, 80)
- Launch EC2 (Amazon Linux 2023)
- Install Apache

- Copy index.html from S3 to /var/www/html/index.html

Step 3.1: Create EC2 template file

Create a file: **stack2-ec2-pull-from-s3.yaml** and paste:

```
AWSTemplateFormatVersion: "2010-09-09"
Description: Launch EC2 (Amazon Linux 2023), install Apache, and pull index.html from S3

Parameters:
  KeyName:
    Type: AWS::EC2::KeyPair::KeyName
    Description: Select an existing EC2 Key Pair to enable SSH access

  BucketName:
    Type: String
    Description: Enter the S3 bucket name created in Stack-1 (Output)

  SubnetId:
    Type: AWS::EC2::Subnet::Id
    Description: Select a PUBLIC subnet (default VPC public subnet recommended)

  VpcId:
    Type: AWS::EC2::VPC::Id
    Description: Select the VPC (default VPC recommended)

Resources:
  WebServerRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              Service: ec2.amazonaws.com
            Action: sts:AssumeRole
      Policies:
        - PolicyName: S3ReadOnlyForWebsiteBucket
          PolicyDocument:
            Version: "2012-10-17"
            Statement:
              - Effect: Allow
                Action:
                  - s3:GetObject
                  - s3:ListBucket
                Resource:
                  - !Sub "arn:aws:s3:::${BucketName}"
                  - !Sub "arn:aws:s3:::${BucketName}/*"

  WebServerInstanceProfile:
    Type: AWS::IAM::InstanceProfile
```

```
  Properties:
    Roles:
      - !Ref WebServerRole

  WebServerSG:
    Type: AWS::EC2::SecurityGroup
    Properties:
      GroupDescription: Allow SSH (22) and HTTP (80)
      VpcId: !Ref VpcId
      SecurityGroupIngress:
        - IpProtocol: tcp
          FromPort: 22
          ToPort: 22
          CidrIp: 0.0.0.0/0
        - IpProtocol: tcp
          FromPort: 80
          ToPort: 80
          CidrIp: 0.0.0.0/0

  WebServerInstance:
    Type: AWS::EC2::Instance
    Properties:
      InstanceType: t2.micro
      KeyName: !Ref KeyName
      SubnetId: !Ref SubnetId
      SecurityGroupIds:
        - !Ref WebServerSG
      IamInstanceProfile: !Ref WebServerInstanceProfile

      # Amazon Linux 2023 AMI for Mumbai (ap-south-1)
      ImageId: ami-02b49a24cfb95941c

      UserData:
        Fn::Base64: !Sub |
          #!/bin/bash
          dnf update -y
          dnf install -y httpd
          systemctl enable httpd
          systemctl start httpd

          # pull index.html from S3 to Apache web root
          aws s3 cp s3://${BucketName}/index.html /var/www/html/index.html

          systemctl restart httpd

Outputs:
  WebsiteURL:
    Description: Open this URL in browser
    Value: !Sub "http://${WebServerInstance.PublicDnsName}"
```

Step 3.2: Create stack

CloudFormation → Stacks → Create stack

- Upload template → stack2-ec2-pull-from-s3.yaml
- Stack name: EC2-Pull-S3-Website
- Parameters:
    - **KeyName**: select your key pair (e.g., pemkeypair)
    - **BucketName**: paste bucket name from Stack-1 Output
    - **VpcId**: select **default VPC**
    - **SubnetId**: select a **PUBLIC subnet** in default VPC
      (usually the subnet name shows "public" or you can pick any default subnet that gives public IP; default subnets generally work)

Create stack → wait for **CREATE_COMPLETE**

PART 4 — Verify Output

Stack-2 → **Outputs** → copy **WebsiteURL** → open in browser.

Expected page:
"Hello! This page was pulled from S3 to EC2 automatically…"

Troubleshooting (comm

1) Website not opening

- Wait 1–2 minutes (UserData takes time)
- Ensure Security Group has **HTTP 80 open**
- Ensure you selected a **public subnet** (needs internet to reach S3)

2) Stack-2 fails with S3 access error

- BucketName typed wrong
- index.html not uploaded at root of bucket

Clean-up

Delete Stack-2 first

CloudFormation → select EC2-Pull-S3-Website → Delete

Empty the S3 bucket

S3 → bucket → delete index.html (empty bucket)

Delete Stack-1

CloudFormation → select S3-Website-Bucket → Delete

Viva questions

1. What is the purpose of **UserData** in EC2?
2. Why do we need an **IAM Role + Instance Profile**?
3. Why is S3 bucket not made public in this lab?
4. What happens when a CloudFormation stack is deleted?
5. Which ports are required for web hosting and SSH?

DATE: 19-12-25

Exercise–24: AWS Lambda: Input Processing, Business Logic Execution, and CloudWatch Logging

Create one Lambda function that:

- prints a welcome message
- reads JSON input event
- performs business logic (grade calculation)
- writes logs → view them in CloudWatch Logs

Create the Lambda Function

Step 1: Open Lambda

AWS Console → Search Lambda → Open AWS Lambda

Step 2: Create function

Click Create function

- Select - Author from scratch
- Function name: StudentGradeLogger
- Runtime: Python 3.11
- Architecture: x86_64 (default)

Step 3: Permissions (Execution Role)

Under "Permissions"

- Choose: Create a new role with basic Lambda permissions

This automatically gives permission to write logs to CloudWatch.

Click **Create function**

Add Code (Business Logic + Logs)

Step 4: Paste this code

In **Code** tab → lambda_function.py → paste and **Deploy**

```
import json

def lambda_handler(event, context):
    # Welcome message
    print("Lambda invoked successfully")

    # Read input from event
    student_name = event["StudentName"]
    marks = event["Marks"]

    # Business logic: grade calculation
    if marks >= 75:
        result = "Pass"
        grade = "A"
    else:
        result = "Fail"
        grade = "F"
```

```
    # Log output
    print("Student:", student_name)
    print("Marks:", marks)
    print("Grade:", grade)
    print("Result:", result)

    # Return response
    return {
        "statusCode": 200,
        "body": json.dumps({
            "StudentName": student_name,
            "Marks": marks,
            "Grade": grade,
            "Result": result
        })
    }
```

Click **Deploy**.

Test with Input Events (JSON)

Step 5: Create a test event (Valid case)

Go to Test (top right) → Configure test event

- Event name: ValidInput
- Paste this JSON:

```
{
  "StudentName": "Anita",
  "Marks": 86
}
```

Click **Save**

Step 6: Run test

Click **Test**

Expected response (sample):

- statusCode: 200
- body will include Grade A and Result Pass

Step 7: Test invalid input (Missing Marks)

Create another test event:

- Event name: MissingMarks

```
{
  "StudentName": "Rahul"
}
```

Run **Test**

Expected:

- statusCode: 400
- message: Missing 'Marks'

Step 8: Test invalid marks range

Event name: InvalidMarks

```
{
  "StudentName": "Priya",
  "Marks": 150
}
```

Expected:

- statusCode: 400
- message: Marks must be 0–100

View Logs in CloudWatch

Step 9: Open logs from Lambda directly

On the Lambda function page:

- Go to **Monitor** tab
- Click **View CloudWatch logs**

You will see:

- Log group: /aws/lambda/StudentGradeLogger
- Open latest **log stream**
- You should see all print() outputs:
    - "Lambda invoked successfully!"
    - "Received event…"
    - grade/result logs
    - error logs for invalid tests

Cleanup (Avoid charges, keep account clean)

Lambda itself usually costs nothing in small use, but cleanup is good practice:

1. Lambda → Functions → select StudentGradeLogger → **Delete**
2. CloudWatch → Log groups → find /aws/lambda/StudentGradeLogger → **Delete**
3. IAM role created (optional):
    - IAM → Roles → search role name created for Lambda → delete (only if not used elsewhere)

DATE: 24-12-25

Exercise–25: Mini Project: Event-Driven Notification System using AWS Lambda and Amazon SNS. Simulating real-time alerts from events using serverless computing.

- An event in JSON format is given as input to an AWS Lambda function.
- The Lambda function processes the event and generates a notification message.
- The message is published to an Amazon SNS topic.
- SNS sends the notification to the subscribed email address.
- The execution details are verified using CloudWatch Logs.

Create SNS Topic + Email Subscription

Step 1: Open SNS

AWS Console → Search SNS → Open Simple Notification Service

Step 2: Create a Topic

SNS → Topics → Create topic

- Type: Standard
- Name: NotificationTopic

Click Create topic

Step 3: Copy Topic ARN

Open the created topic → copy Topic ARN

(You will paste it into Lambda code later)

Step 4: Create an Email Subscription

Inside the same topic:

Click Create subscription

- Protocol: Email
- Endpoint: (your email id)

Click Create subscription

Step 5: Confirm Subscription

Open your email inbox → find AWS SNS confirmation mail → click Confirm subscription → Status in SNS should become Confirmed.

Create Lambda Function

Step 6: Open Lambda

AWS Console → Search Lambda → Open AWS Lambda

Step 7: Create function

Click Create function

- Select: Author from scratch
- Function name: NotificationSimulator
- Runtime: Python 3.11
- Permissions: Create a new role with basic Lambda permissions

Click Create function

Add Lambda Code (with SNS Publish)

Step 8: Paste code in lambda_function.py

Lambda → **Code** tab → open lambda_function.py → remove existing code → paste:
Replace <SNS_TOPIC_ARN> with your copied Topic ARN.

```
import json
import boto3

sns = boto3.client('sns')

TOPIC_ARN = "<SNS_TOPIC_ARN>"

def lambda_handler(event, context):
    print("Notification Simulator invoked")

    event_type = event["eventType"]
    user = event["user"]

    if event_type == "ORDER_PLACED":
        message = f"Hi {user}, your order is placed successfully."
        priority = "NORMAL"

    elif event_type == "PAYMENT_FAILED":
        message = f"Hi {user}, your payment has failed. Please retry."
        priority = "HIGH"

    elif event_type == "LOW_ATTENDANCE":
        message = f"Hi {user}, your attendance is low. Please take action."
        priority = "HIGH"

    else:
        message = f"Hi {user}, unknown event received."
        priority = "LOW"

    print("Event Type:", event_type)
    print("Message:", message)
    print("Priority:", priority)

    # Publish to SNS (Actual notification delivery)
    sns.publish(TopicArn=TOPIC_ARN, Message=message, Subject=f"{event_type} [{priority}]")

    return {
        "statusCode": 200,
        "body": json.dumps({
            "EventType": event_type,
            "Message": message,
            "Priority": priority
        })
    }
```

Click **Deploy**
Wait for “Successfully updated function…”

Give Lambda Permission to Publish to SNS

Step 10: Open Lambda Execution Role

Lambda → Configuration → Permissions
Click the Role name (execution role link)

Step 11: Attach SNS Publish Policy

IAM Role page → Add permissions → Attach policies
Attach: AmazonSNSFullAccess
Click Add permissions
Now Lambda can publish to SNS.

Test the Mini Project

Step 12: Create a test event

Lambda → Test tab → Create new test event
Event name: PaymentFailed
Paste:

```
{
  "eventType": "PAYMENT_FAILED",
  "user": "Anita"
}
```

Click **Save**

Step 13: Run Test

Click **Test**
Expected:

- Execution: **Succeeded**
- Email should arrive within a few seconds:
  Subject like: PAYMENT_FAILED [HIGH]
  Message: "Hi Anita, your payment has failed. Please retry."

Verify CloudWatch Logs

Step 14: View logs

Lambda → Monitor → View CloudWatch logs
Open latest log stream.
Verify these prints exist:

- Notification Simulator invoked
- Event Type:
- Message:
- Priority:

Expected Outputs

1. Lambda test status: Succeeded
2. Email received from SNS with correct message
3. CloudWatch logs showing event type and generated message

Cleanup

1. Delete Lambda function: NotificationSimulator
2. SNS → delete topic NotificationTopic (subscriptions removed automatically)
3. CloudWatch → delete log group for Lambda
4. (Optional) Delete IAM role if not used elsewhere

DATE: 26-12-25

Exercise–26: Analyze a CSV File in S3 Using Amazon Athena (No Server)

Upload a small CSV to **S3**, then use Athena to run SQL queries like count, average, max, group by.

Part A — Create Sample CSV (on your PC)

1. Open **Notepad**
2. Paste this data and save as: **students.csv**

```
StudentID,Name,Dept,Marks,Result
101,Anita,MCA,85,Pass
102,Ravi,MCA,72,Pass
103,Meera,MBA,64,Pass
104,John,MCA,35,Fail
105,Sneha,MBA,91,Pass
106,Arun,MCA,49,Fail
107,Kiran,MBA,58,Pass
108,Divya,MCA,77,Pass
```

Part B — Create S3 Bucket and Upload CSV

- Go to **AWS Console → S3**
- Click **Create bucket**
- Bucket name: athena-lab-<yourname>-<number> (must be globally unique)
- Keep defaults → Click **Create bucket**
- Open the bucket → Click **Upload**
- Upload **students.csv**
- Click **Upload**

Now your CSV is in S3.

Part C — Open Athena and Set Query Result Location (IMPORTANT)

- Go to **AWS Console → Amazon Athena**
- If it shows "Get started" / "Query editor", open it.
- It will ask to set a **Query result location**
- Click the link/button like **Settings / Manage / Edit**

- Set query result location to something like:
    - s3://your-bucket-name/athena-results/
- Click **Save**

This is required so Athena can store query outputs.

Part D — Create a Database in Athena

In Athena query editor, run:

CREATE DATABASE labdb;

Then on the left side, select:

- **Data source:** AwsDataCatalog
- **Database:** labdb

Part E — Create a Table for the CSV in S3

Run this (replace YOUR_BUCKET_NAME with your actual bucket name):

```
CREATE EXTERNAL TABLE IF NOT EXISTS students (
  StudentID int,
  Name string,
  Dept string,
  Marks int,
  Result string
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.OpenCSVSerde'
WITH SERDEPROPERTIES (
  'separatorChar' = ',',
  'quoteChar'     = '"',
  'escapeChar'    = '\\'
)
STORED AS TEXTFILE
LOCATION 's3://YOUR_BUCKET_NAME/'
TBLPROPERTIES ('skip.header.line.count'='1');
```

This tells Athena: “My CSV is in S3, treat it like a table.”

Part F — Run Simple Analysis Queries (Core Part)

1) View all rows

SELECT * FROM students;

Expected: 8 records.

2) Total students

SELECT COUNT(*) AS total_students FROM students;

Expected: 8

3) Pass vs Fail count

SELECT Result, COUNT(*) AS cnt

FROM students

GROUP BY Result;

Expected (based on data): Pass = 6, Fail = 2

4) Average marks overall

SELECT AVG(Marks) AS avg_marks

FROM students;

5) Department-wise average marks

SELECT Dept, AVG(Marks) AS avg_marks

FROM students

GROUP BY Dept;

6) Top scorer

SELECT Name, Dept, Marks

FROM students

ORDER BY Marks DESC

LIMIT 1;

Expected: Sneha (91)

7) List failed students

SELECT StudentID, Name, Dept, Marks

FROM students

WHERE Result = 'Fail';

Expected: John, Arun

Cleanup (to avoid any charges)

1. In Athena, you can keep DB/table (no cost by itself), but clean S3:
2. Go to **S3 bucket**
3. Delete:
    - students.csv
    - athena-results/ folder contents (query outputs)
4. Delete the bucket (must be empty to delete)

Cost Note (Simple)

- **S3 storage**: tiny (almost negligible for this)
- **Athena**: charges based on **data scanned**; with this tiny CSV it's usually minimal, but **always delete outputs and bucket** after lab.