PART 1: Launch an EC2 Instance

Step 1: Login to AWS

1. Open browser → go to **https://console.aws.amazon.com/**
2. Sign in with your AWS account.

Step 2: Open EC2 Dashboard

1. In the search bar, type **EC2**.
2. Click **EC2** → opens the EC2 dashboard.

Step 3: Launch a New Instance

1. Click **Launch Instance**.
2. Enter a name such as **HelloWorld-EC2**.

Step 4: Choose AMI (Amazon Machine Image)

1. Select **Amazon Linux 2 AMI (Free Tier eligible)**.

Step 5: Choose Instance Type

1. Select **t2.micro** (Free Tier eligible).

Step 6: Create / Select Key Pair

1. Under **Key pair** → click **Create key pair**.
2. Name it (e.g., ec2-keypair).
3. Download the .pem file → keep it safe.
4. Select the key pair in the dropdown.

Step 7: Configure Security Group

1. Under **Network settings**, click **Edit**.
2. Security group configuration:
    - **SSH** → Port **22** → Source: *My IP*
    - **HTTP** → Port **80** → Source: *Anywhere (0.0.0.0/0)*
      (This allows users to access your website)

Click **Launch Instance**.

Step 8: Wait for Instance to Start

1. Go to **EC2 → Instances**.
2. Wait until the state shows **Running** and **Status checks = Passed**.

PART 2: Connect to the Instance

Step 9: Connect Using SSH

1. Select the instance → click **Connect → SSH client**.

2. ✓ Step 1: Move PEM file to SSH folder

3. Move your `ec2-keypair.pem` file to:
4. `C:\Users\HARISMITA\.ssh\`
5. (If `.ssh` folder doesn't exist → create it manually.)
6. ---

7. ✓ Step 2: Open Command Prompt (or PowerShell)

8. Press:
   Windows + R → type cmd → Enter
9. ---

10. ✓ Step 3: Connect to EC2 using Windows' SSH

11. Run this command (replace the IP):
12. `ssh -i C:\Users\HARISMITA\.ssh\ec2-keypair.pem ec2-user@YOUR_PUBLIC_IP`
13. Example:
14. `ssh -i C:\Users\HARISMITA\.ssh\ec2-keypair.pem ec2-user@13.201.48.10`

1️⃣ Update your server

sudo dnf update -y

(Amazon Linux 2023 uses dnf instead of yum.)

2️⃣ Install Apache Web Server

sudo dnf install httpd -y

3️⃣ Start the web server

sudo systemctl start httpd

4️⃣ **Enable it on system restart**

sudo systemctl enable httpd

5️⃣ **Create "Hello World" web page**

echo "<h1>Hello World from AWS EC2 💙</h1>" | sudo tee /var/www/html/index.html

---

6️⃣ **Open your browser**

Paste your EC2 instance public IP:

http://34.229.152.170

You should see:

⭐ **Hello World from AWS EC2** 💙

✅ **Do this:**

Step 1:

Copy this link:

👉 **http://34.229.152.170**

Step 2:

Open your **Chrome browser** on your Windows computer.

Step 3:

Paste the link in the address bar → press Enter.

STEP 1: Create IAM Role for CloudWatch

On AWS Console:

1. Go to **IAM** (search "IAM" in AWS search bar)
2. Click **Roles**
3. Click **Create Role**
4. Select:
    - **Trusted Entity Type:** AWS Service
    - **Use Case: EC2**
5. Click **Next**

Attach these permissions:

✓ **CloudWatchAgentServerPolicy**
✓ **AmazonSSMManagedInstanceCore**

Search and add BOTH.

6. Click **Next**
7. Name the role:
   EC2-CloudWatch-Role
8. Click **Create Role**

STEP 2: Attach this Role to Your EC2 Instance

1. Go to **EC2 → Instances**
2. Select your instance (**HelloWorld-EC2**)
3. Click **Actions**
4. Choose:
   Security → Modify IAM Role
5. Select:
   EC2-CloudWatch-Role
6. Save

⭐ **Great! Now your EC2 is allowed to send logs to CloudWatch.**

Next: Install the agent.

STEP 3: Install CloudWatch Agent

Go back to your **EC2 terminal** and run:

sudo dnf install amazon-cloudwatch-agent -y

STEP 4: Create CloudWatch Agent Config File

Run:

sudo nano /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

Paste this inside:

```
{
  "metrics": {
    "metrics_collected": {
      "cpu": { "measurement": ["cpu_usage_idle", "cpu_usage_user"] },
      "mem": { "measurement": ["mem_used_percent"] },
```

```
    "disk": { "measurement": ["disk_used_percent"] }
   }
  },
  "logs": {
   "logs_collected": {
    "files": {
     "collect_list": [
      {
       "file_path": "/var/log/messages",
       "log_group_name": "ec2-system-logs",
       "log_stream_name": "{instance_id}-messages"
      },
      {
       "file_path": "/var/log/httpd/access_log",
       "log_group_name": "ec2-apache-access",
       "log_stream_name": "{instance_id}-access"
      }
     ]
    }
   }
  }
}
```

Save & Exit nano:

- Press **CTRL + O** → Enter
- Press **CTRL + X**

STEP 5: Start CloudWatch Agent

Run:

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl \
-a fetch-config -m ec2 \
-c file:/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json \
```

-s

If it shows **status = running → SUCCESS**.

STEP 6: Verify in CloudWatch

In AWS Console:

1. Go to **CloudWatch**
2. Click **Log Groups**
3. You should see:
    - ec2-system-logs
    - ec2-apache-access

Now check metrics:

1. Click **Metrics**
2. Open namespace → **CWAgent**
3. You will see:
   ✓ CPU Usage
   ✓ Memory Usage
   ✓ Disk usage
   ✓ Network