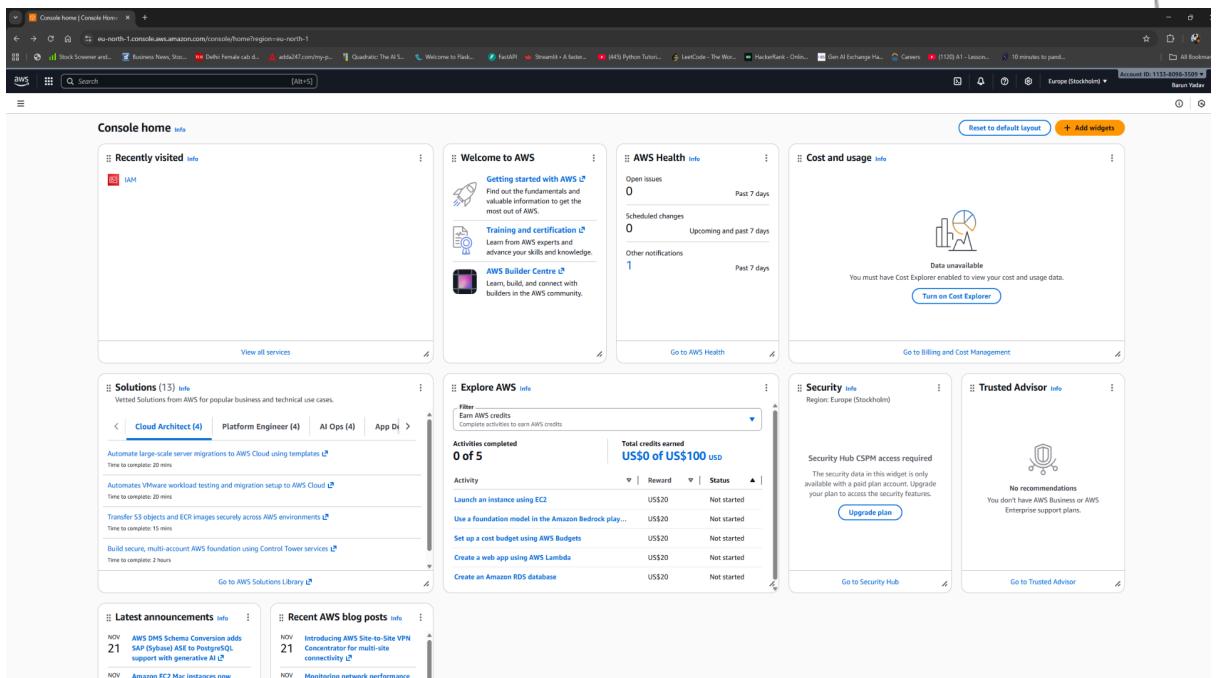


# AWS Assignment-1

## **❖ Task 1: AWS Free Tier Account Creation**

Root account



## **□ Steps:**

1. Go to the **AWS Management Console** → <https://aws.amazon.com/console>.
2. Click **Sign in as root user**.
3. Enter the **email address** (used when creating the account).
4. Enter the **root password**.
5. (If MFA is enabled) Enter the **MFA code**.
6. After entering the **MFA code**, root user will be created

## ❖ Task 2: Root-Equivalent IAM User Creation

The screenshot shows the AWS IAM console interface. A success message at the top states "User created successfully". Below it, a table lists a single user named "adminuser". The table includes columns for User name, Path, Group, Last activity, MFA, Password age, Console last sign-in, Access key ID, Active key age, Access key last us., ARN, Creation time, and Signing cert. The "adminuser" row has a green status indicator. A sidebar on the left is titled "IAM user created as:--adminuser".

### □ Steps:

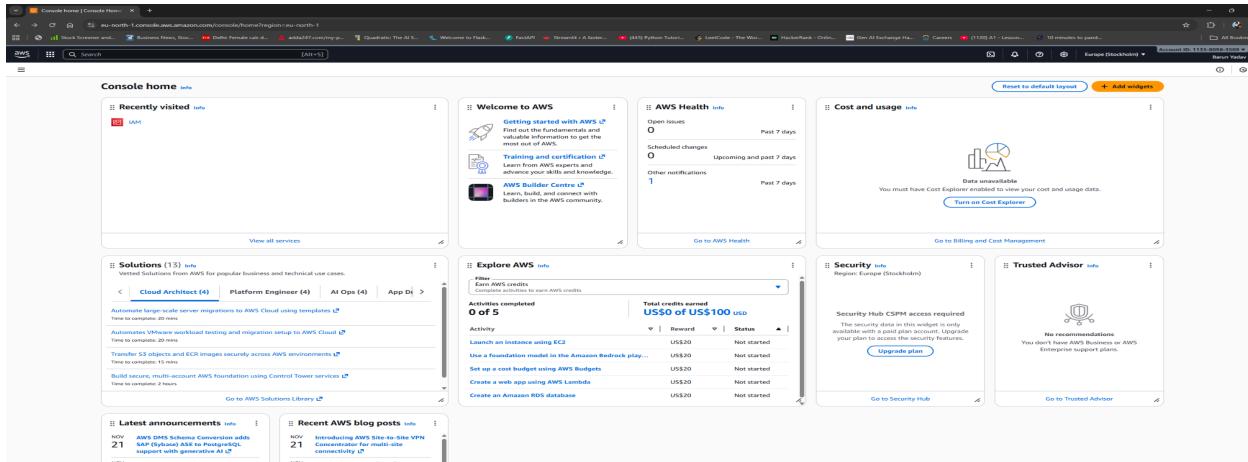
#### Step 1: Sign in as the Root User

- Go to the [AWS Management Console](#).
- Click “Sign in as root user”.
- Enter the **root email** and **password**.
- (If MFA is enabled, enter the MFA code.)

The screenshot shows the AWS Management Console home page. It features several sections: "Recently visited" (Systems Manager, EC2, IAM, VPC), "Welcome to AWS" (Getting started with AWS, Training and certification, AWS Builder Centre), "AWS Health" (Open issues, Scheduled changes, Other notifications), and "Cost and usage" (Data unavailable, Turn on Cost Explorer). The top navigation bar includes links for AWS services like Lambda, CloudWatch, and S3, along with account information and a search bar.

## Step 2: Open the IAM Console

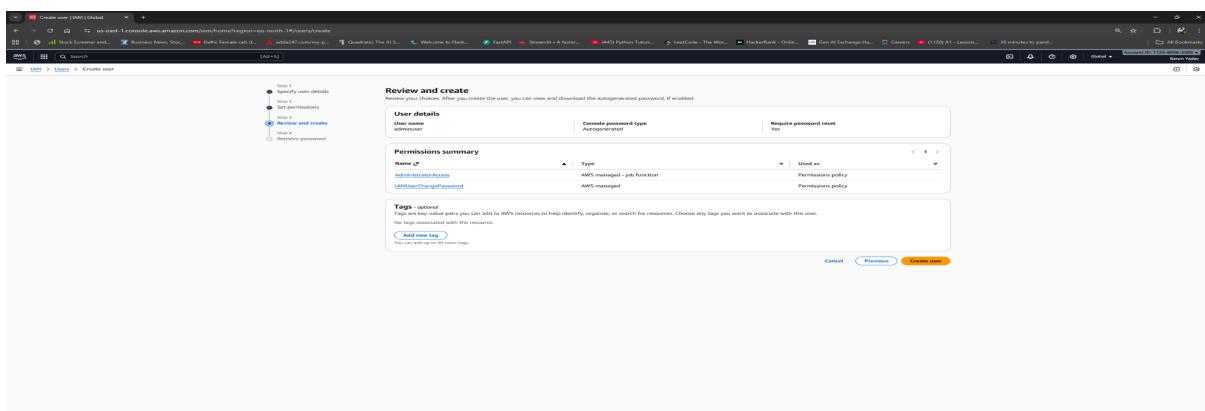
- In the AWS console search bar, type “IAM”.
- Click **IAM (Identity and Access Management)** to open it.



## Step 3: Create a New IAM User

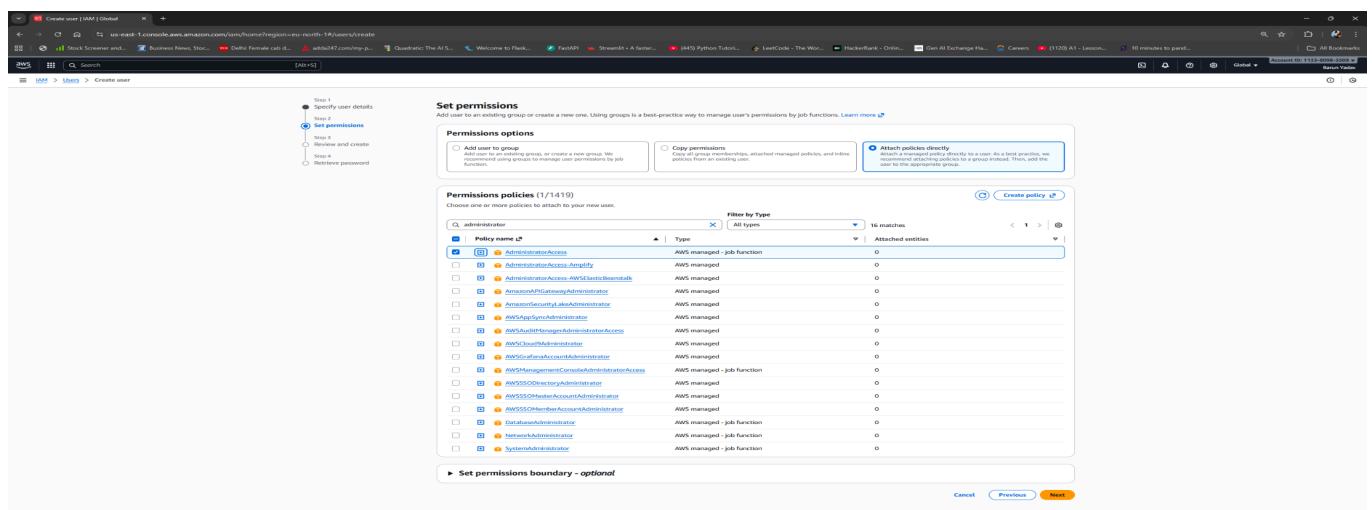
1. In the left sidebar, click **Users** → **Add users**.
2. Enter a **username** (e.g., admin-user).
3. Under **Select AWS access type**, choose:
  - Password - AWS Management Console access** (if user needs console access)
  - Access key - Programmatic access** (if user needs CLI or API access)

Click **Next**.



## Step 4: Attach Administrator Permissions

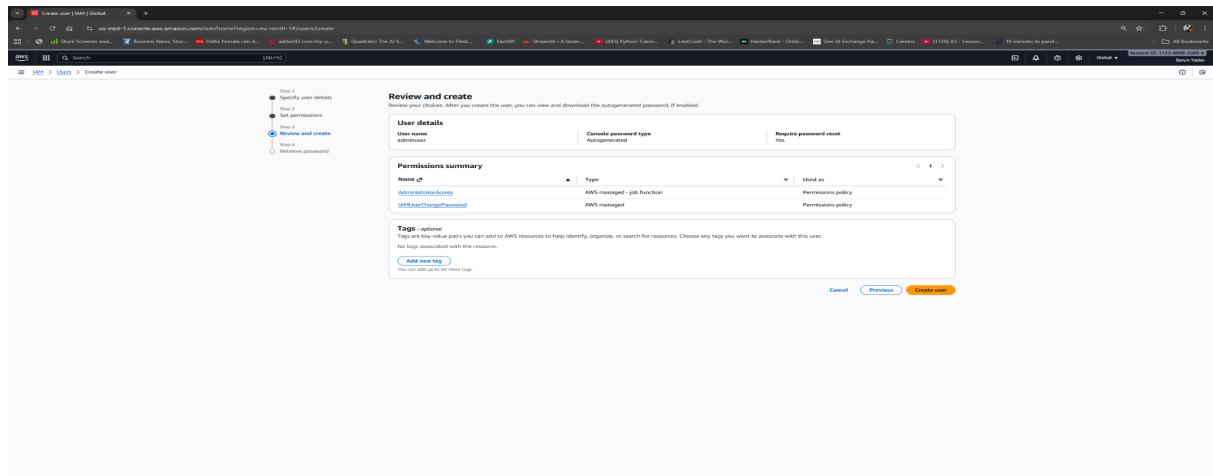
1. Choose **Attach policies directly**.
2. Search for and select **AdministratorAccess**.
  - o This gives the user full permissions for all AWS services (like the root user, but still restricted by IAM).
3. Click **Next**.



## Step 5: Review and Create

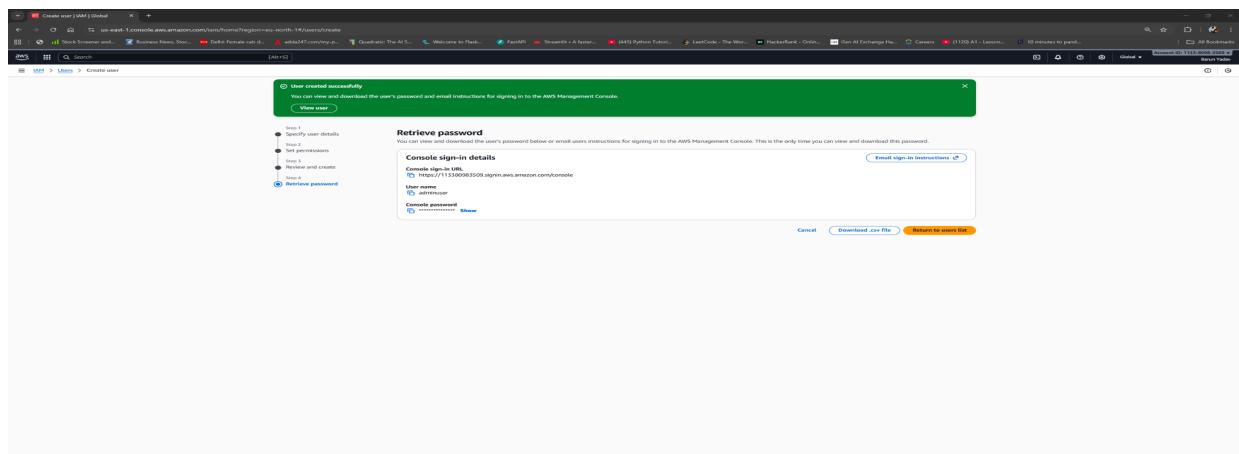
- Review all details.
- Click **Create user**.

AWS will show the **login URL**, **username**, and (if applicable) the **password or access keys**.

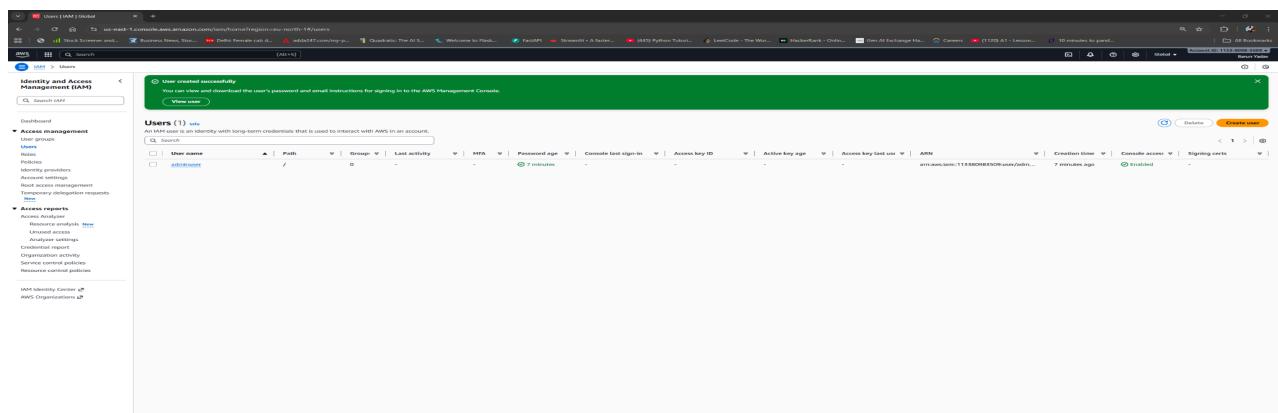


## Step 6: Secure the Account

1. **Sign in as the new IAM user** to confirm it works.
2. **Enable MFA (Multi-Factor Authentication):**
  - o Go to **IAM → Users → [your user] → Security credentials**.
  - o Under **Multi-factor authentication (MFA)**, choose **Assign MFA device**.
  - o Use an **authenticator app** (like Google Authenticator).
3. Store credentials securely (not in plaintext).



- Hence, IAM user created as **adminuser**



## ❖ Task 3: VPC Selection & Region Choice

The screenshot shows the AWS VPC console interface. On the left, a sidebar titled 'VPC created' lists various VPC-related services: VPC dashboard, AWS Global View, Virtual private cloud (with 'Your VPCs' selected), Subnets, Route tables, Internet gateways, Egress-only Internet gateways, DHCP option sets, Elastic IPs, Managed prefix lists, NAT gateways, Peering connections, Route servers, Security (Network ACLs, Security groups), PrivateLink and Lattice (Getting started, Endpoints, Endpoint services, Service networks, Lattice services, Resource configurations, Resource gateways, Target groups, Domain verifications), DNS firewall (Rule groups, Domain lists), and Network Firewall (Firewalls, Firewall policies, Network Firewall rule groups, TLS inspection). The main content area displays a table titled 'Your VPCs' with one item listed:

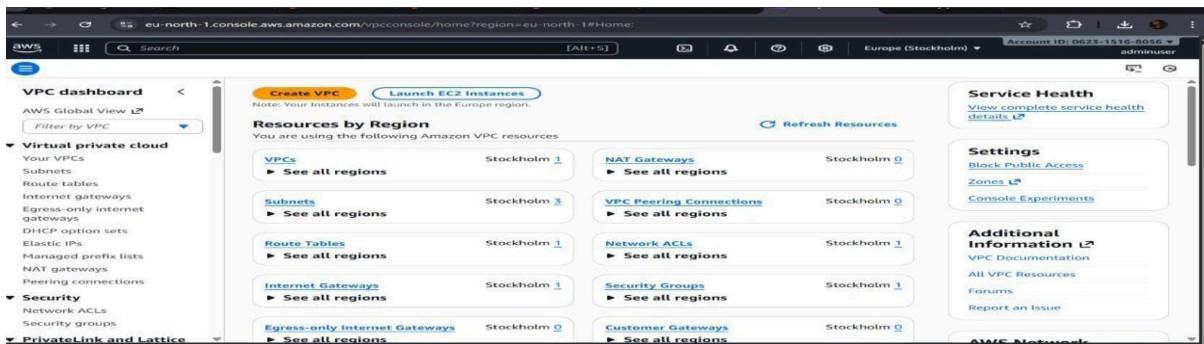
Name	VPC ID	State	Encryption c...	Encryption control ...	Block Public...	IPv4 CIDR	IPv6 CIDR	DHCP option set	Main route table	Main network ACL
vpc-0650a2aae50edfb35	vpc-0650a2aae50edfb35	Available	-	-	Off	172.31.0.0/16	-	dopt-0ddab0cd81f405...	rtb-0f58177b4ef646a31	acl-04c9b9d7928d4ab3

A message 'Last updated 1 minute ago' is at the top right. An 'Actions' button and a 'Create VPC' button are also present.

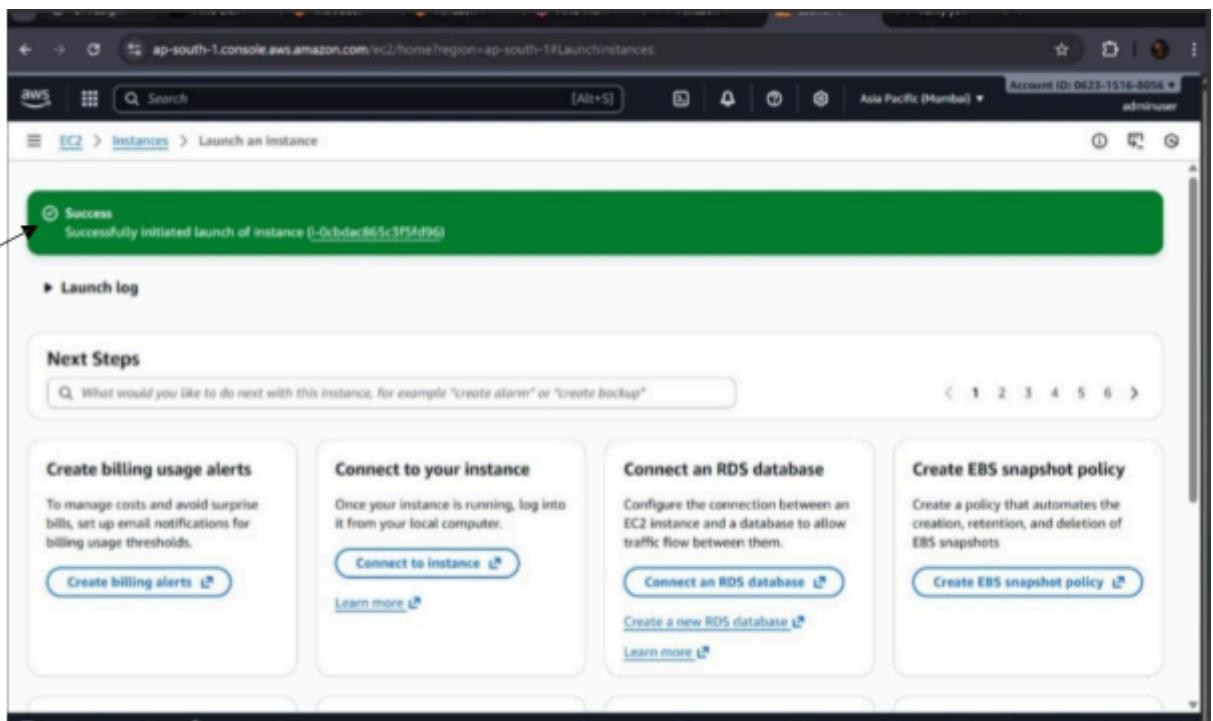
## □ Steps:

### Steps to Select or Create a VPC

1. In the AWS console, go to the **VPC Dashboard** (search for “VPC”).
2. Click **Your VPCs** in the left sidebar.
3. You’ll see a **Default VPC** (it usually has “Default” in the “Name” column).
4. You can use this VPC directly for EC2, RDS, or other resources — it already has:
  - Public subnets in each AZ
  - Internet Gateway attached
  - Route tables set up



## ❖ Task 4: Windows Web Server EC2 Instance



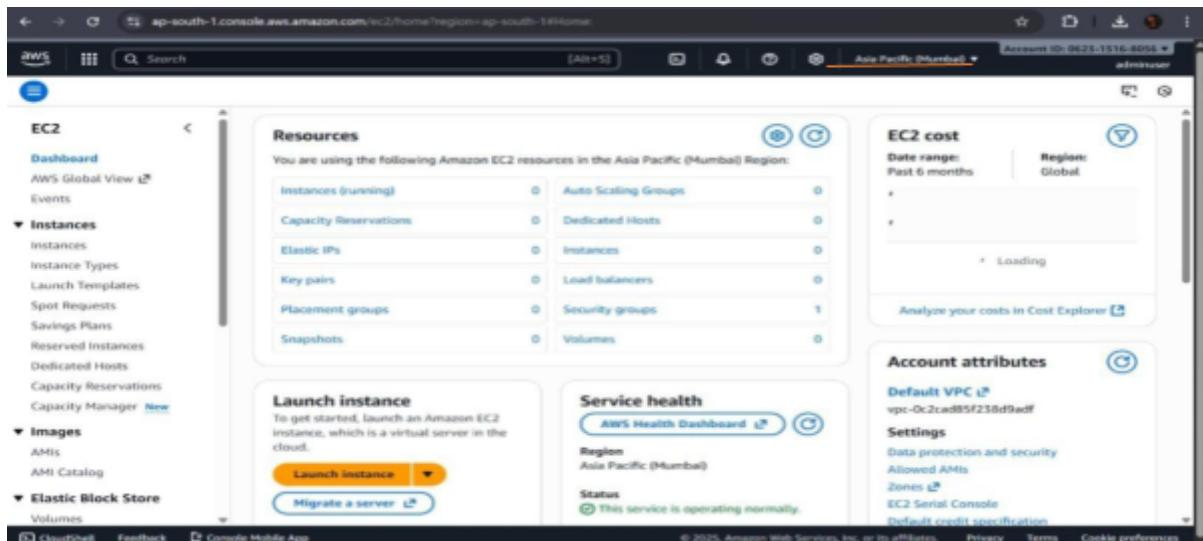
## □ Steps:

### Step 1: Sign in and Select a Region

1. Go to the [AWS Management Console](#).

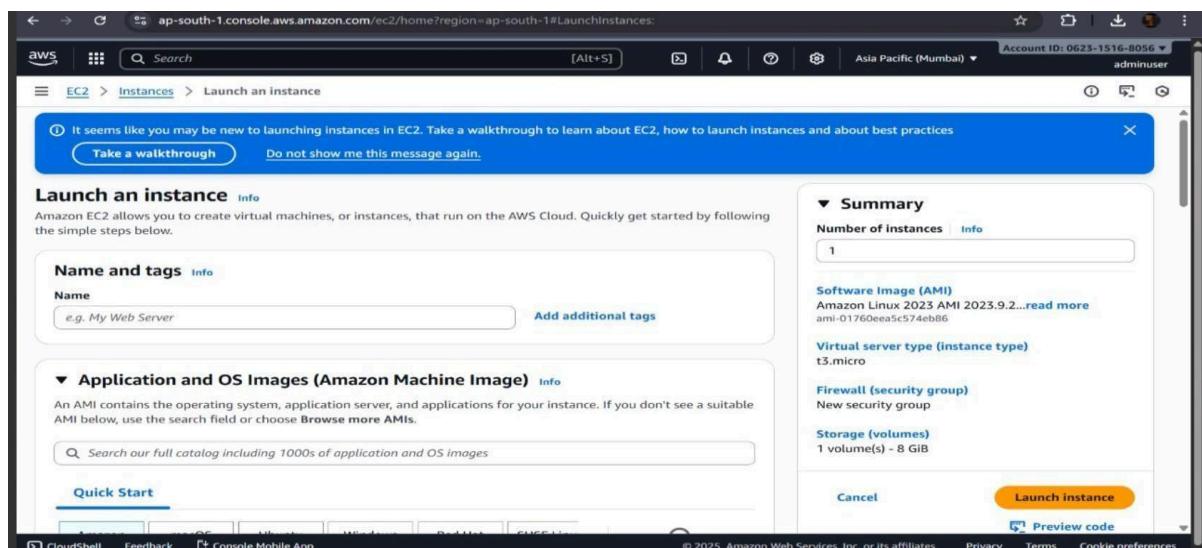
In the top-right corner, choose your **AWS Region** (e.g., Asia Pacific (Mumbai) ap-south-1).

- o All resources you create will reside in this region.



## Step 2: Open the EC2 Dashboard

1. In the AWS Console search bar, type “EC2” and select it.
2. Click Instances → Launch instances.



## Step 3: Configure Basic Details

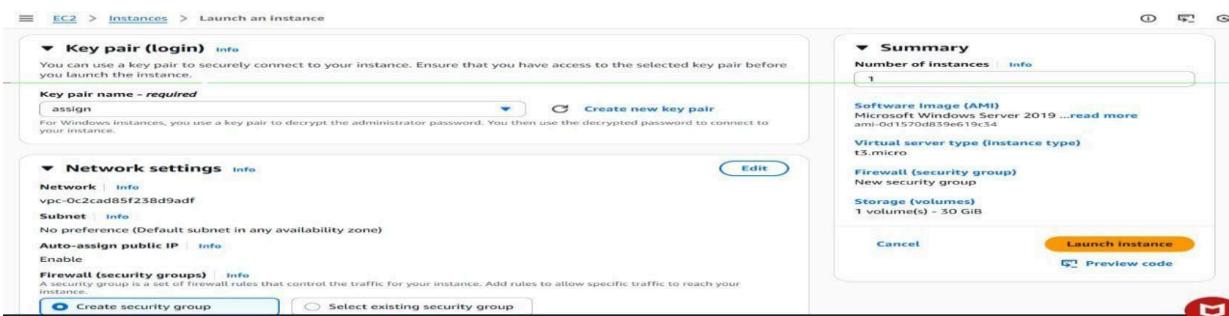
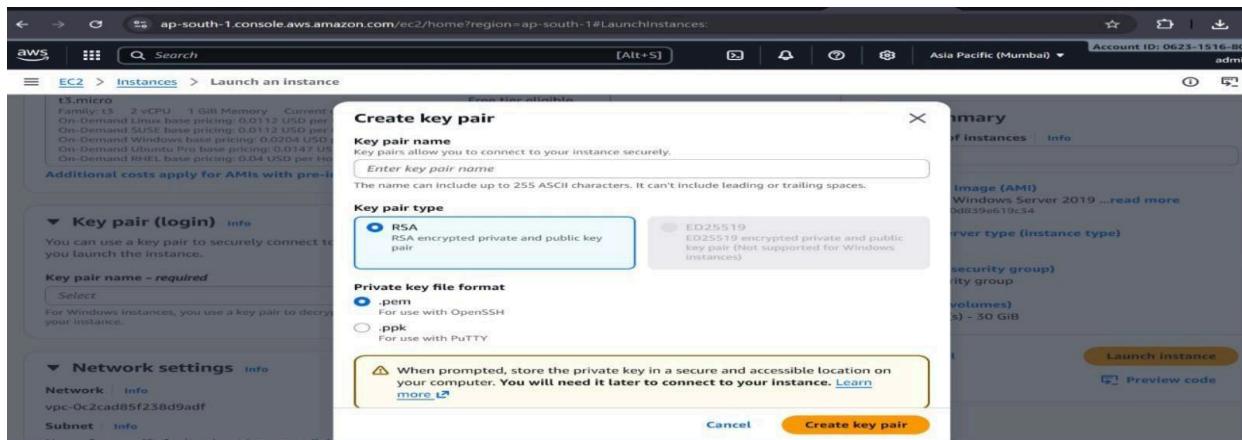
1. Name your instance — e.g., Windows-WebServer.
2. Choose an Amazon Machine Image (AMI):
  - o Scroll to find Microsoft Windows Server 2022 Base (or 2019/2016 if needed).
  - o These AMIs come with Windows preinstalled.
3. Choose Instance Type:

- For basic setups, select t3.micro or t2.micro (Free Tier eligible).

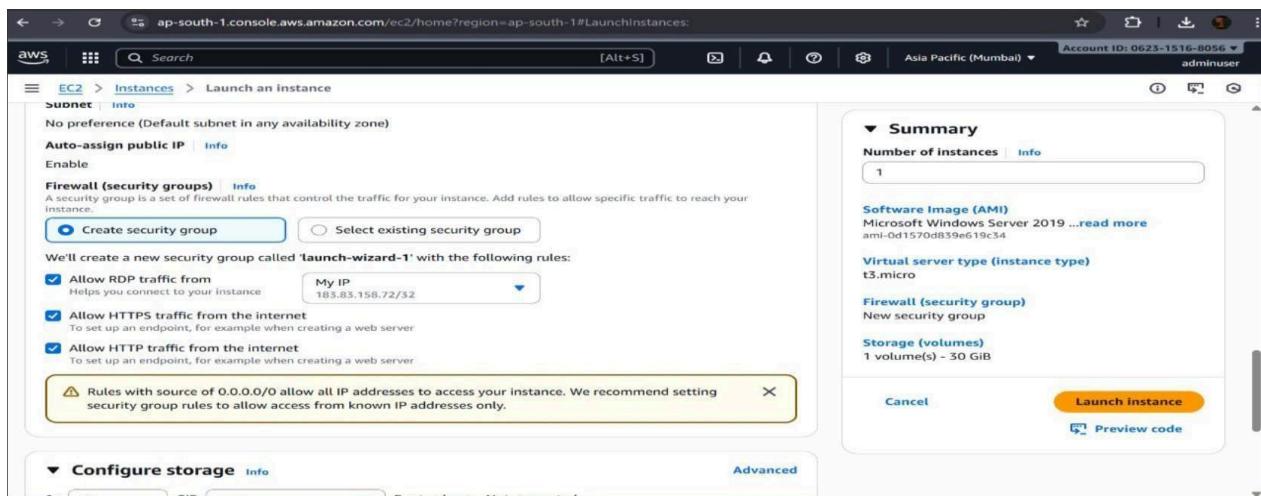
## Step 4: Configure Key Pair (Login)

1. Under **Key pair (login)**, choose:
  - **Create new key pair** (if you don't have one yet).
  - Give it a name (e.g., WindowsKeyPair).
  - Choose **Key pair type: RSA**, and **File format: .pem** (for RDP decryption).
  - Click **Create key pair** — it will automatically download the .pem file to your computer.
    - . | Keep it safe — you'll need it to connect later.



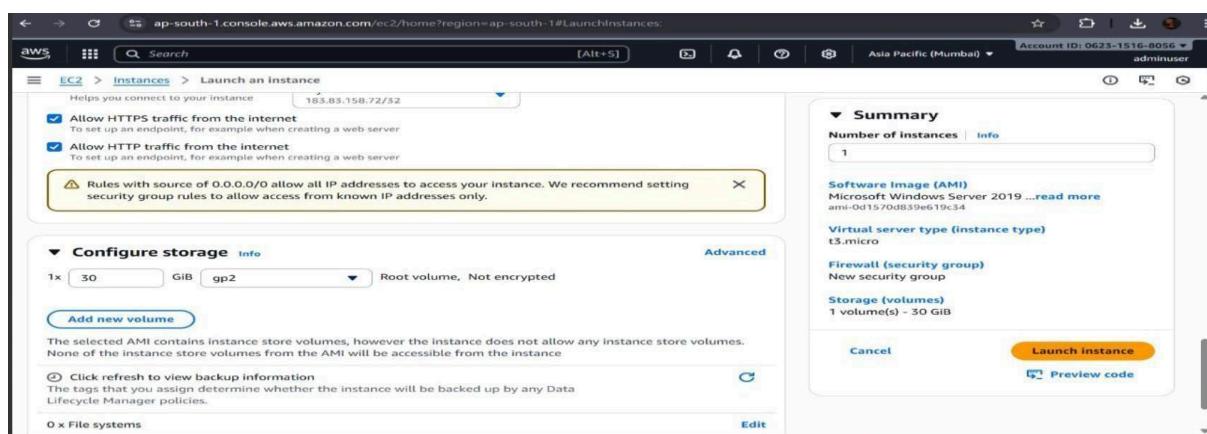
## Step 5: Configure Network Settings

1. Under **Network settings**, select your **VPC** and **Subnet** (default VPC is fine).
2. Check **Auto-assign public IP** → *Enable*.
3. Under **Firewall (security group)**:
  - Choose **Create security group**.
  - Allow:
    - **RDP (Port 3389)** → Source: My IP (for remote access)
    - **HTTP (Port 80)** → Source: Anywhere (for web traffic)



## Step 6: Configure Storage

- Default 30 GB is fine, or increase if needed.
- Ensure volume type is **gp3** (default).



## Step 7: Launch Instance

- Review your settings and click **Launch instance**.
- Wait a few moments until the status shows **running**.

# Task 5: Systems Manager Fleet Manager Setup

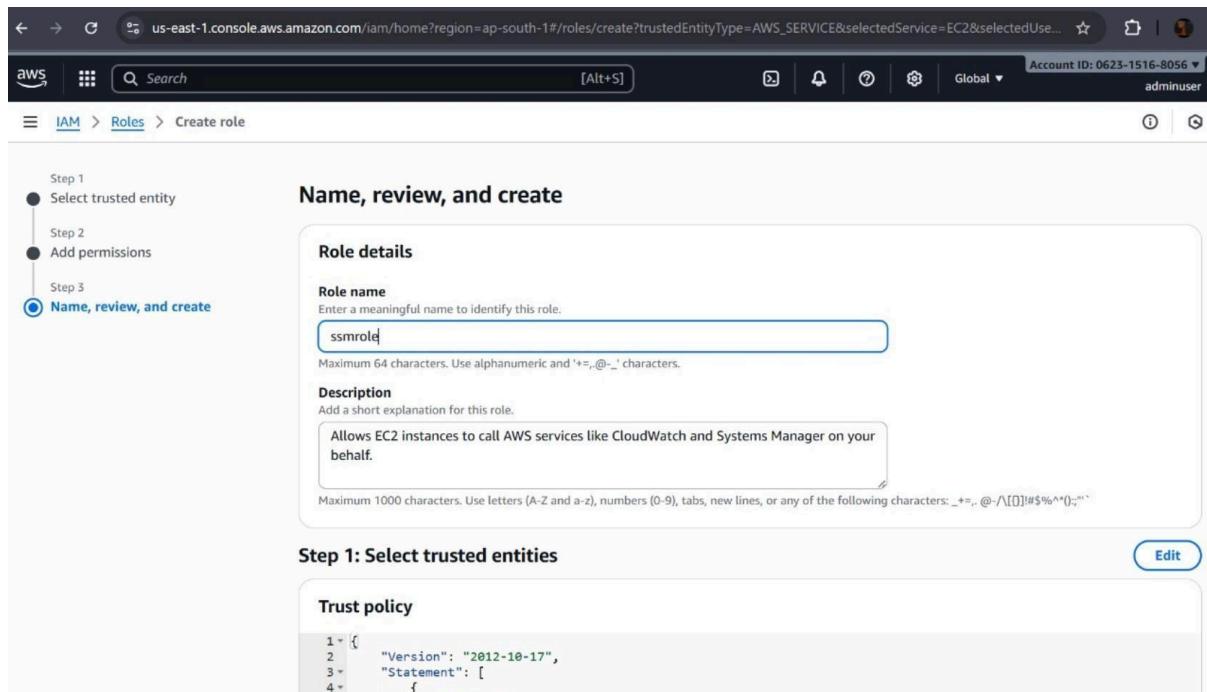
## Steps:

### **Step 1: Create IAM Role for Systems Manager**

Fleet Manager requires the instance to have permission to communicate with SSM.

#### **Steps:**

1. Go to **IAM → Roles → Create role**.
2. Under **Trusted entity type**, choose **AWS service**.
3. Choose **EC2** → Click **Next**.
4. In **Permissions policies**, search and select:
  - AmazonSSMManagedInstanceCore
5. Click **Next**, name the role:
6. SSM-Managed-Instance-Role
7. Click **Create role**.



## Step 2: Attach IAM Role to EC2 Instance

1. Go to EC2 → Instances.
2. Select your instance → Actions → Security → Modify IAM role.
3. Select SSM-Managed-Instance-Role → click Update IAM role.

The screenshot shows the AWS IAM Roles page. The left sidebar includes sections for Identity and Access Management (IAM), Access management, and Access reports. The main content area displays a table titled 'Roles (4)'. The table lists four roles: 'AWSServiceRoleForResourceExplorer', 'AWSServiceRoleForSupport', 'AWSServiceRoleForTrustedAdvisor', and 'ssmrole'. The 'ssmrole' row is selected, indicated by a blue border. A 'Manage' button is located at the top right of the table. Below the table, there is a section titled 'Roles Anywhere' with links to 'Access AWS from your non AWS workloads' and 'X.509 Standard'.

The screenshot shows the AWS EC2 Instances page. The left sidebar includes sections for EC2, Instances, Images, and Elastic Block Store. The main content area displays a table titled 'Instances (1)'. It shows one instance named 'web sever' with the ID 'i-0cbdac865c3f5fd96', which is currently 'Running'. The 'Actions' dropdown menu is open, showing options like 'Connect', 'Instance state', 'Actions', and 'Launch instances'. Below the table, a 'Select an instance' dropdown is open, showing the same single instance entry.

## Step 3 Verify SSM Agent is Installed

For Amazon Linux 2 or Windows:

- The SSM Agent is preinstalled.

For Other OS (e.g., Ubuntu, CentOS):

1. Connect via SSH or RDP.
2. Run these commands:

The screenshot shows the AWS EC2 Connect to instance page. At the top, it displays the instance ID: i-0cbdac865c3f5fd96 (web sever). Below this, there are two connection options: "Connect using RDP client" (selected) and "Connect using Fleet Manager". A note says you can connect using a remote desktop client or download an RDP shortcut file. It also shows the Public DNS: ec2-15-206-77-193.ap-south-1.compute.amazonaws.com and a dropdown for "Username Info" set to "Administrator". A note at the bottom indicates joining to a directory allows using directory credentials.

## Step 4: Open Fleet Manager

1. In the AWS Console, go to **Systems Manager**.
2. In the left menu, under **Node Management**, click **Fleet Manager**.
3. You should now see your EC2 instance listed.
  - If it doesn't appear yet, wait a few minutes for SSM to register it.

This screenshot is identical to the one above, showing the AWS EC2 Connect to instance page for the same instance (i-0cbdac865c3f5fd96). The connection type is still set to "RDP client". The Public DNS and Username Info are the same. A note at the bottom again mentions joining to a directory for directory credential usage.

The screenshot shows the AWS Systems Manager Fleet Manager interface. At the top, there's a banner with a message about the unified console. Below it, the navigation path is 'Systems Manager > Fleet Manager > Managed nodes'. The main area is titled 'Fleet Manager' with an 'Info' button. A table titled 'Managed Nodes (1)' lists one node: 'i-0cbdac8...', which is 'Running', a 'web sever' running on 'Windows' with 'Microsoft ...' resources, connected via 'EC2 insta...', and is 'Online' with agent version '3.3.3050.0'. There are buttons for 'Settings', 'Account management', 'Report', and 'Node actions'.

## Step 5: Manage Instance via Fleet Manager

Now you can manage your EC2 instance **without RDP or SSH**:

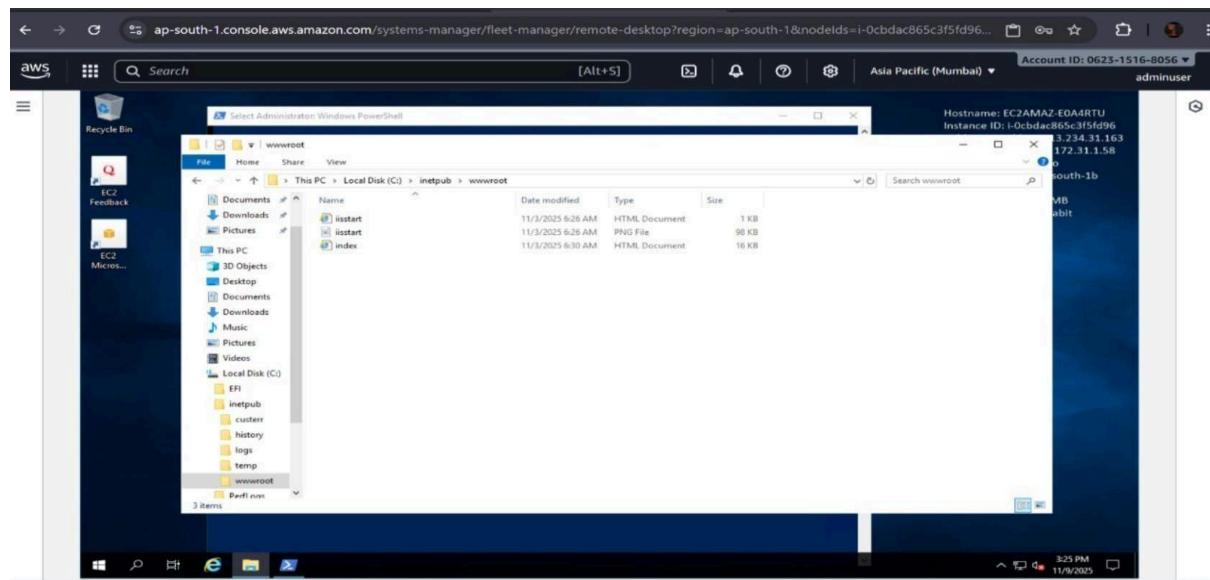
### From Fleet Manager Dashboard:

- Select your instance → click **Node actions** or instance name. You can now:
- View system info (CPU, memory, network, OS details)
- Browse and edit files
- View event logs
- Manage users
- Run PowerShell/Command Line directly in console
- Access the Windows registry (for Windows)
- Reboot or stop instance remotely

The screenshot shows the 'Remote desktop' configuration dialog. It asks for the number of nodes to connect to (maximum of 4). It lists a node: 'web sever i-0cbdac865c3f5fd96'. It shows two authentication types: 'User credentials' (selected) and 'Key pair'. It asks for an 'Administrator account name' (set to 'Administrator'). It has sections for 'Key pair content' (with options to upload from local machine or paste key pair content), 'Choose file' (button), and footer links for CloudShell, Feedback, Console Mobile App, Privacy, Terms, and Cookie preferences.

PS C:\Users\Administrator> Install-WindowsFeature -name Web-Server  
Success Restart Needed Exit Code Feature Result  
----- No NoChangeNeeded { }  
  
PS C:\Users\Administrator> Install-WindowsFeature -name Web-Common-Http  
Success Restart Needed Exit Code Feature Result  
----- No NoChangeNeeded { }  
  
PS C:\Users\Administrator> Install-WindowsFeature -name Web-Http-Errors  
Success Restart Needed Exit Code Feature Result  
----- No NoChangeNeeded { }  
  
PS C:\Users\Administrator> Install-WindowsFeature -name Web-Static-Content  
Success Restart Needed Exit Code Feature Result  
----- No NoChangeNeeded { }  
  
PS C:\Users\Administrator>

Hostname: EC2AMAZ-E0A4RTU  
Instance ID: i-0cbdac865c3f5fd96  
Public IPv4 address: 13.234.31.163  
Private IPv4 address: 172.31.1.58  
Mac address: 00:0C:29:4E:4D:9B  
Availability Zone: ap-south-1b  
Architecture: AMD64  
Total memory: 1024 MB  
Network: Up to 5 Gigabit



## Final Output:

