



## **Lab 8**

**Lab Title: AWS: Account Setup, IAM, VPC Inventory, EC2, Docker & Gitea**


**Submitted to: Engr. Muhammad Shoaib**

**Submitted by: Anara Hayat**

**Reg#No: 2023-BSE-008**


## Task 1 — Create an AWS account and enable UAE (me-central-1)

1. Open your browser and go to: [AWS Signup](#)



**Try AWS at no cost for up to 6 months**

Start with USD \$100 in AWS credits, plus earn up to USD \$100 by completing various activities.



### Sign up for AWS

Root user email address  
Used for account recovery and as described in the [AWS Privacy Notice](#)

AWS account name  
Choose a name for your account. You can change this name in your account settings after you sign up.

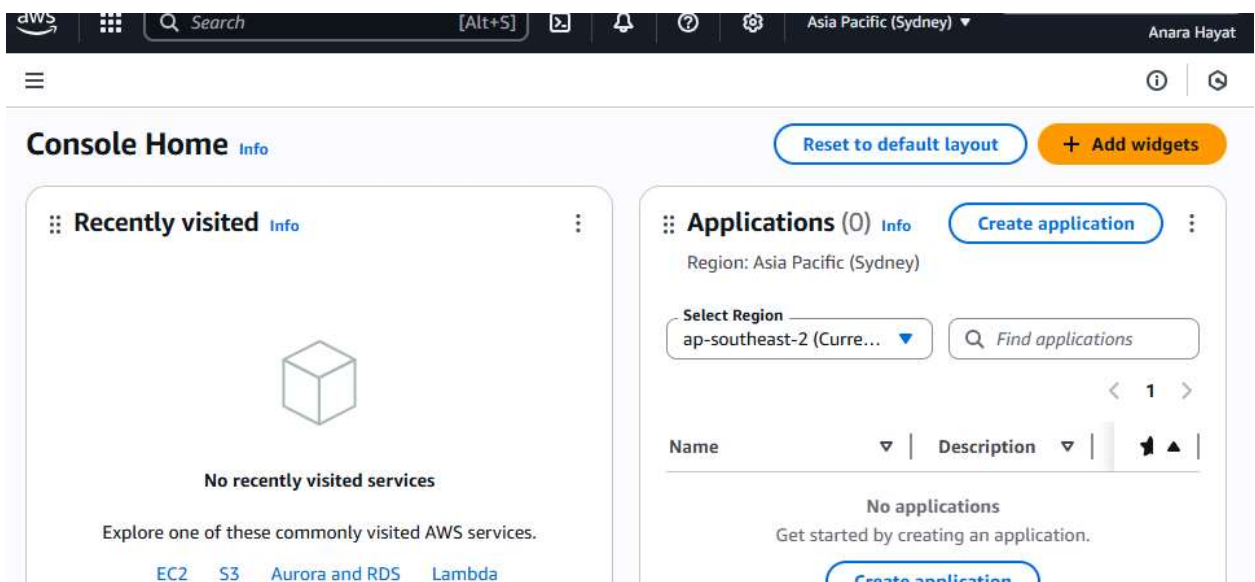
**Verify email address**

OR

**Sign in to an existing AWS account**

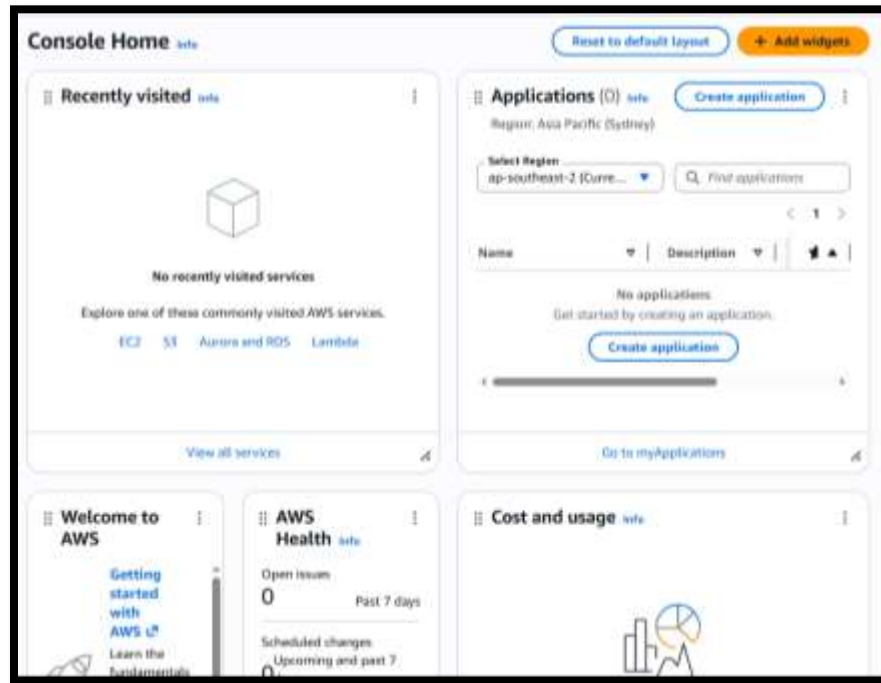
This site uses essential cookies. See our [Cookie Notice](#) for more information.

2. Complete registration (Account type: Personal, Plan: AWS Paid Plan), fill contact, billing (credit card) and phone details, complete verification. After successful registration capture:

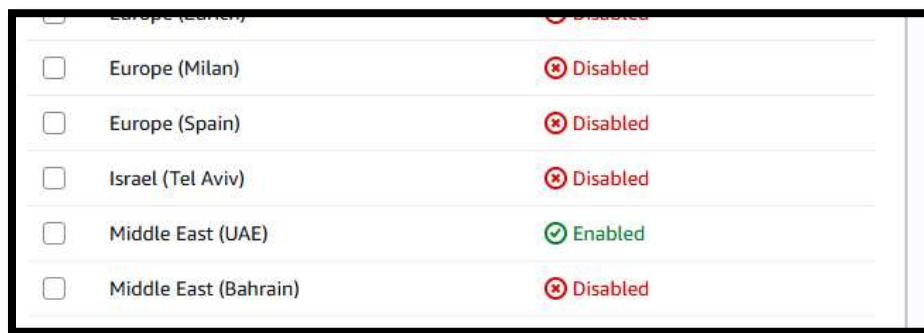


The screenshot shows the AWS Management Console Home page. The top navigation bar includes the AWS logo, a search bar, and the user's name "Anara Hayat". The main content area is divided into two columns. The left column, titled "Console Home", features a "Recently visited" section with a cube icon and the text "No recently visited services". Below this, it says "Explore one of these commonly visited AWS services." and lists "EC2", "S3", "Aurora and RDS", and "Lambda". The right column, titled "Applications (0)", shows the "Region: Asia Pacific (Sydney)" and a "Select Region" dropdown menu. It also includes a "Find applications" search bar and a table with columns "Name" and "Description". The table is empty, and the text "No applications" is displayed. A "Create application" button is visible at the bottom of the right column.

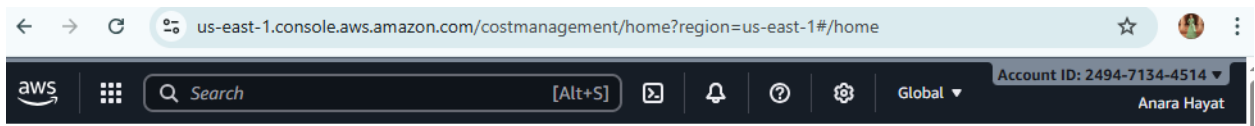
3. Sign in as the root user (root email). Immediately capture:



4. From the Console, open the region selector and enable UAE (me-central-1), then switch to me-central-1. Capture the change

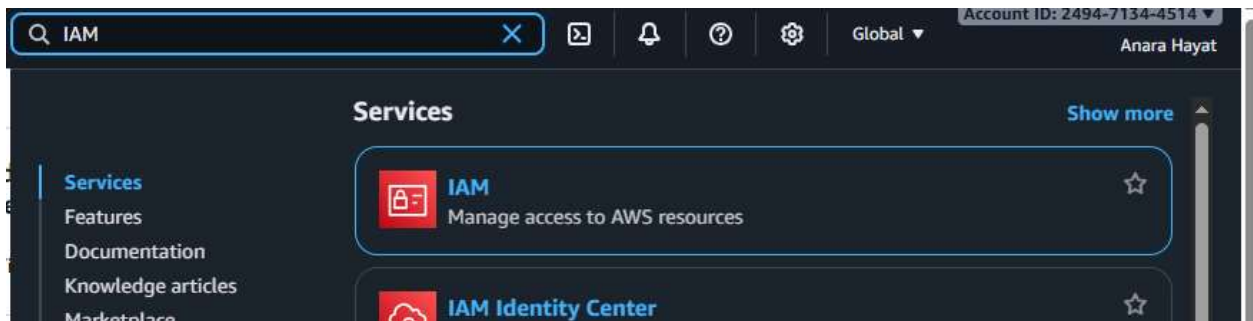


5. Task 1 summary screenshot (combine evidence):



Task 2 — Create IAM Admin and Lab8User with console access

1. Open IAM via Console search (Alt+S → "IAM").



2. Create the Admin user: IAM → Users → Create user. Fill:

### Specify user details

#### User details

**User name**

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ \_ - (hyphen)

☒ Provide user access to the AWS Management Console - *optional*  
In addition to console access, users with `SignInLocalDevelopmentAccess` permissions can use the same console credentials for programmatic access without the need for access keys.

**Console password**

☒ Autogenerated password  
You can view the password after you create the user.

☐ Custom password  
Enter a custom password for the user.

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & \* ( ) \_ + - (hyphen) = [ ] { } | ' "

☐ Show password

☒ Users must create a new password at next sign-in - Recommended  
Users automatically get the `IAMUserChangePassword` policy to allow them to change their own password.

**Info** If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

[Cancel](#) [Next](#)

Attach policies directly → AdministratorAccess

### Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

#### Permissions options

☐ Add user to group  
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions  
Copy all group memberships, attached managed policies, and inline policies from an existing user.

☒ Attach policies directly  
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

#### Permissions policies (1/1426)

Create policy

Choose one or more policies to attach to your new user.

Filter by Type  
All types

< 1 2 3 4 5 6 7 ... 72 >

	Policy name	Type	Attached ...
<input type="checkbox"/>	<a href="#">AccessAnalyzerSer...</a>	AWS managed	0
<input checked="" type="checkbox"/>	<a href="#">AdministratorAccess</a>	AWS managed - job ...	0

### Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

#### User details

User name  
Admin

Console password type  
Autogenerated

Require password reset  
Yes

#### Permissions summary

< 1 >

Name	Type	Used as
<a href="#">AdministratorAccess</a>	AWS managed - job function	Permissions policy
<a href="#">IAMUserChangePassword</a>	AWS managed	Permissions policy

### Users (1)

Info

Delete

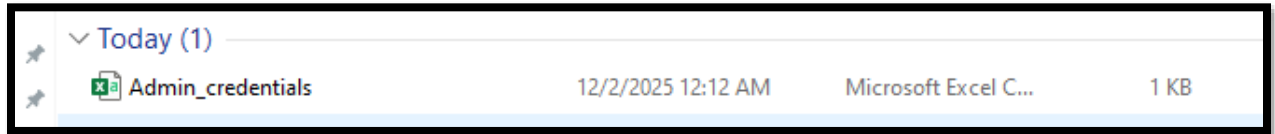
Create user


An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

< 1 >

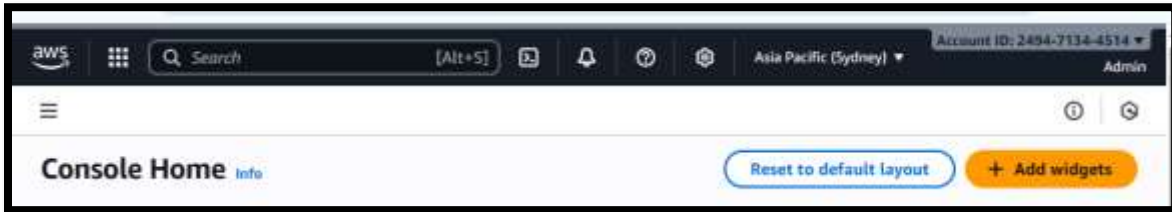
	User name	Path	Group	Last activity
<input type="checkbox"/>	<a href="#">Admin</a>	/	0	-

3. Download the Admin .csv and show its presence on your Windows host

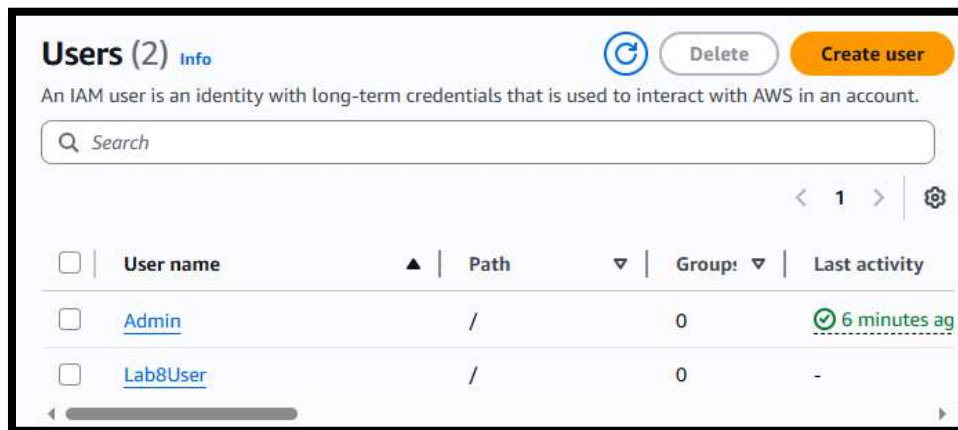


Today (1)			
	Admin_credentials	12/2/2025 12:12 AM	Microsoft Excel C... 1 KB

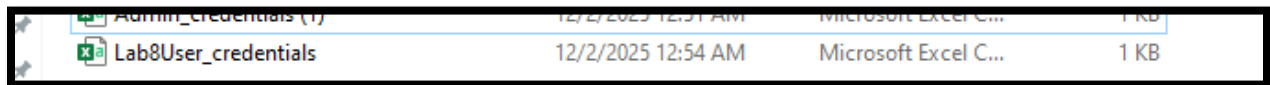
4. Sign out of root, then sign in using the Admin account (use the signin URL from the .csv). Capture after successful Admin login:A





5. While logged in as Admin, create Lab8User

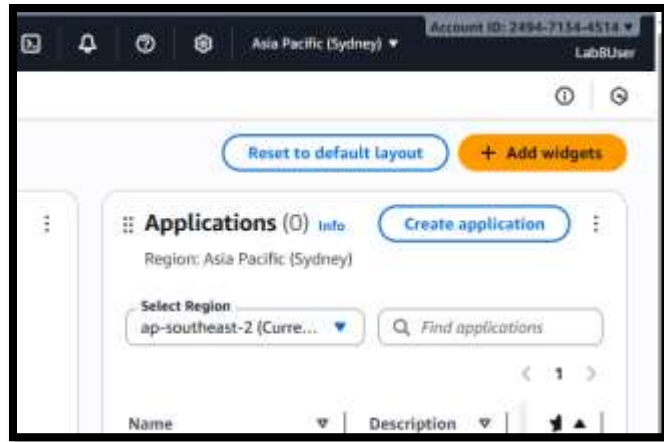


6. Download/save the Lab8User CSV on your Windows host

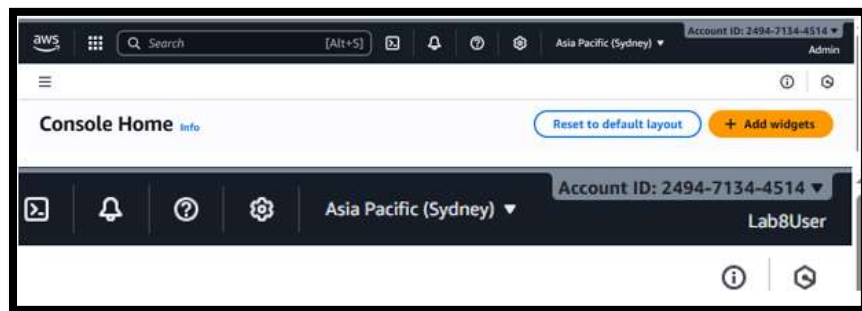


Today (1)			
	Admin_credentials	12/2/2025 12:12 AM	Microsoft Excel C... 1 KB
	Lab8User_credentials	12/2/2025 12:54 AM	Microsoft Excel C... 1 KB

7. Logout Admin and login as Lab8User (use the Lab8User signin URL and credentials). Capture after login:

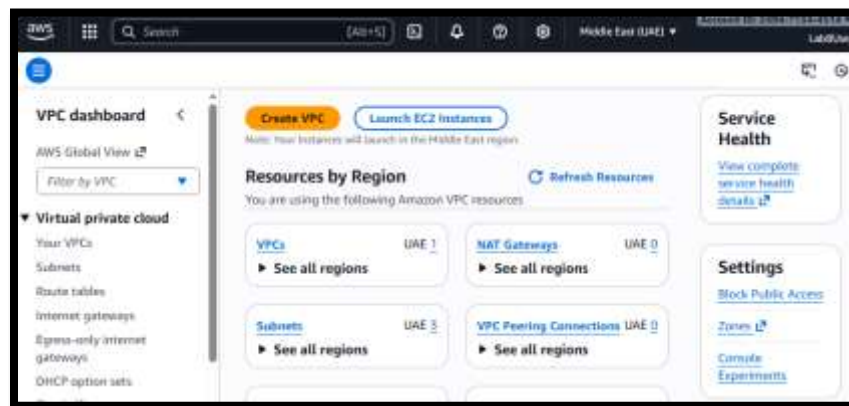
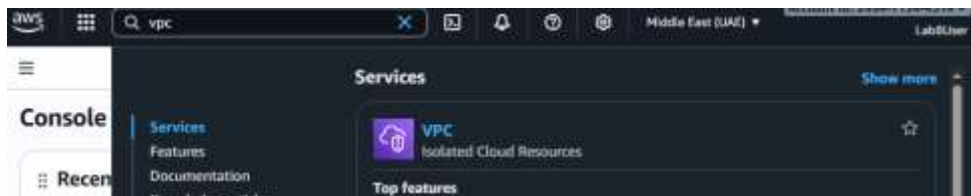


## 8. Task 2 summary (combine evidence):



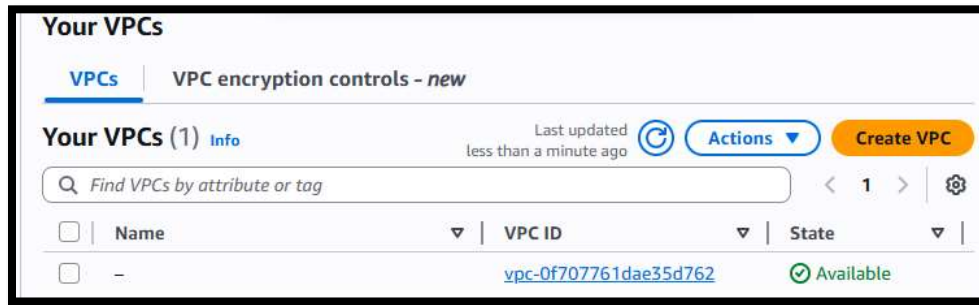
## Task 3 — Inspect VPC resources (in UAE me-central-1)

### 1. Open VPC console (Alt+S → "VPC") while region is me-central-1.

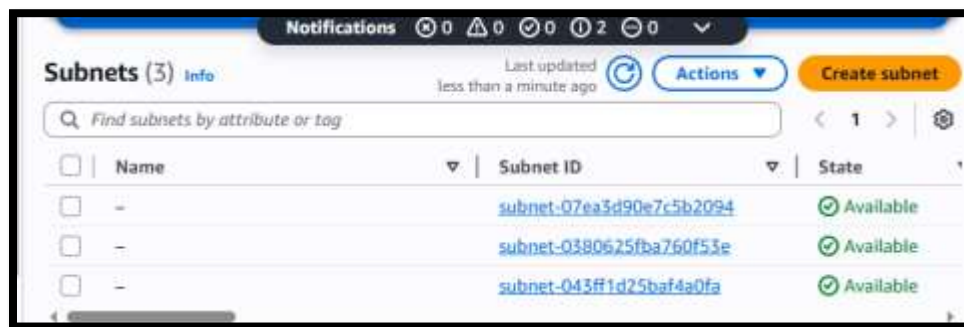




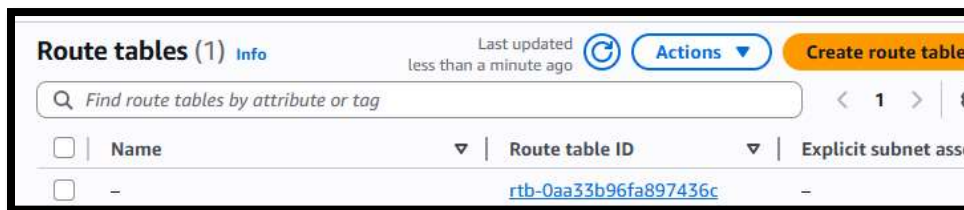
## 2. View VPCs list. Capture:



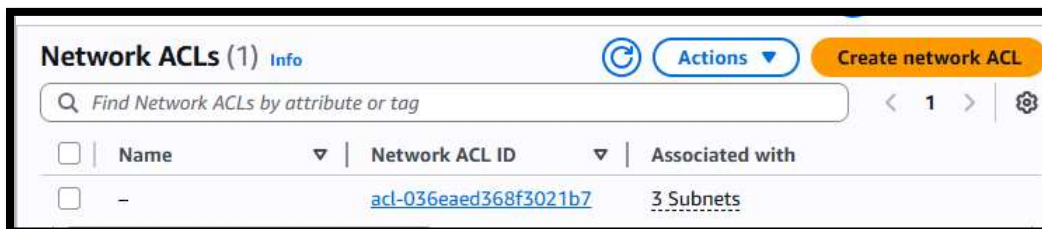
## 3. View Subnets list.



## 4. View Route Tables list. Capture:

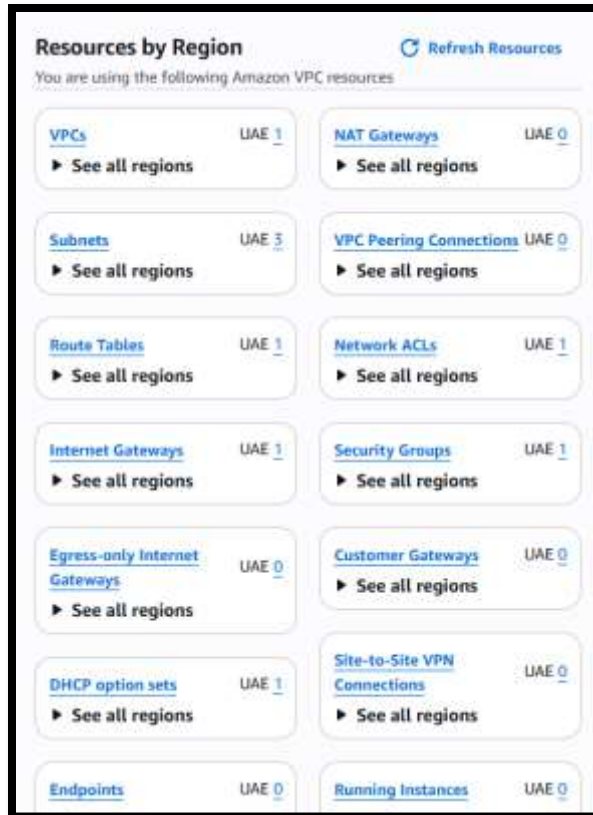


## 5. View Network ACLs list



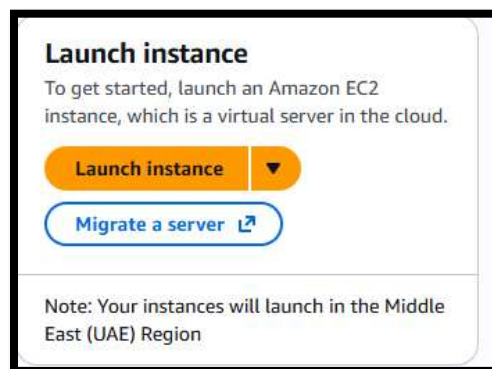
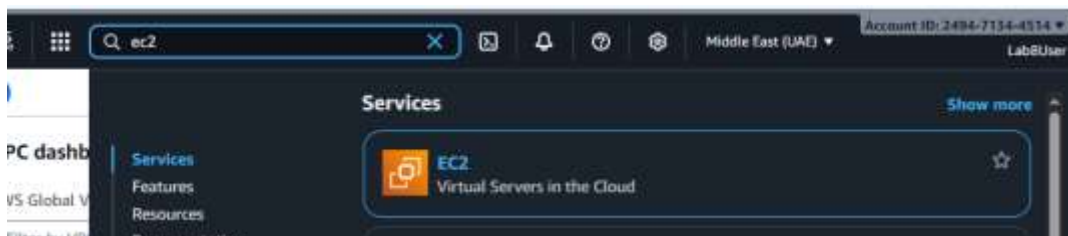
## 6. Task 3 summary (combine evidence)





## Task 4 — Launch EC2, SSH, install Docker & Docker Compose, deploy Gitea

1. Open EC2 Console (Alt+S → "EC2") (me-central-1).



2. Instance Launch configuration (during review before launching). Configure

**Name: Lab8Machine**



**Launch an instance** [Info](#)

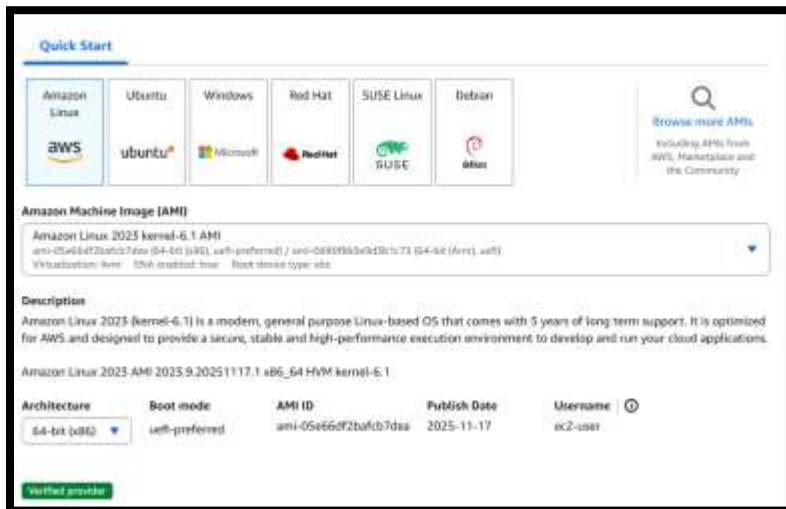
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

**Name and tags** [Info](#)

Name

Lab8Machine [Add additional tags](#)

**AMI: Amazon Linux 2**



**Quick Start**

Amazon Linux Ubuntu Windows Red Hat SUSE Linux Debian

**Amazon Machine Image (AMI)**

Amazon Linux 2023 kernel-6.1 AMI  
ami-05e66df2ba1cb7d3a (x86\_64, x86\_64-preferred) / ami-05e66df2ba1cb7d3a (x86\_64, x86\_64-preferred)  
Virtualization: hvm ENA enabled: true Root device type: sbs

**Description**

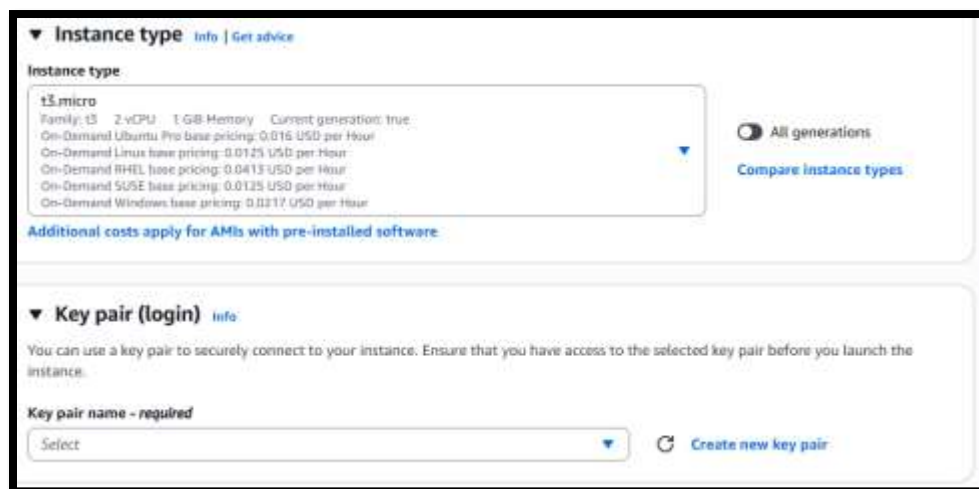
Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.9.20251117.1 x86\_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Publish Date	Username
64-bit (x86)	uefi-preferred	ami-05e66df2ba1cb7d3a	2025-11-17	ec2-user

[Verified provider](#)

**Instance type: t3.micro**



**Instance type** [Info](#) [Get advice](#)

**Instance type**

t3.micro  
Family: t3 2 vCPU 1 GB Memory Current generation: true  
On-Demand Ubuntu Pro base pricing: 0.016 USD per Hour  
On-Demand Linux base pricing: 0.0125 USD per Hour  
On-Demand RHEL base pricing: 0.0413 USD per Hour  
On-Demand SUSE base pricing: 0.0125 USD per Hour  
On-Demand Windows base pricing: 0.0217 USD per Hour

[All generations](#) [Compare instance types](#)

**Additional costs apply for AMIs with pre-installed software**

**Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

**Key pair name - required**

Select [Create new key pair](#)

**Security group: Create Lab8SecurityGroup with SSH from My IP**

▼ Network settings

Info

VPC - required

Info

vpc-0f707761dae35d762

(default)

▼

172.31.0.0/16

↻

Subnet

Info

No preference

▼

↻

Create new subnet

↗

Availability Zone

Info

No preference

▼

↻

Enable additional zones

↗

Auto-assign public IP

Info

Enable

▼

Firewall (security groups)

Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

Security group name - required

Lab8SecurityGroup

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-:/()#,@[]+=&:{}!\$\*

Description - required

Info

launch-wizard-1 created 2025-12-01T20:25:14.189Z

Inbound Security Group Rules

▼ Security group rule 1 (TCP, 22, 103.53.162.80/32)

Remove

Type

Info

ssh

▼

Protocol

Info

TCP

Port range

Info

22

Source type

Info

My IP

▼

Name

Info

Q Add CIDR, prefix list or security group

103.53.162.80/32

×

Description - optional

Info

e.g. SSH for admin desktop

Add security group rule

## Storage: default

▼ Configure storage

Info

Advanced

1x

8

GiB

gp3

▼

Root volume, 3000 IOPS, Not encrypted

Add new volume

ⓘ Click refresh to view backup information

↻

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems

Edit

**Key pair: Create Lab8Key (ED25519, .pem) and download the .pem file to your Windows host**

The screenshot shows the 'Create key pair' dialog box. The 'Key pair name' field contains 'Lab8Key'. The 'Key pair type' is set to 'ED25519' (ED25519 encrypted private and public key pair). The 'Private key file format' is set to '.pem' (For use with OpenSSH). A warning message states: 'When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)'. The 'Create key pair' button is highlighted in orange.

**Capture the final review page and key download**

The top screenshot shows the 'Instances (1)' page in the AWS Management Console. The instance 'Lab8Machine' is listed with ID 'i-0e1df1ceb019e8669', state 'Running', type 't3.micro', and status 'Initializing'. The bottom screenshot shows a file download list with the file 'Lab8Key.pem' (1 KB) downloaded on 12/2/2025 at 1:34 AM.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
Lab8Machine	i-0e1df1ceb019e8669	Running	t3.micro	Initializing	<a href="#">View alarms</a>

File Name	Download Date	File Type	Size
Lab8Key.pem	12/2/2025 1:34 AM	PEM File	1 KB

**3. After launch, EC2 Instances list showing Lab8Machine in "running" state and public IPv4 visible.**



6. Create/edit compose.yaml on the EC2 instance (sudo vim compose.yaml) and paste content from the repo: [Gitea](#) . While pasting, capture the editor content:

```
ec2-user@ip-172-31-7-50:~  
container_name gitea  
environment  
- DB_TYPE=postgres  
- DB_HOST=db:5432  
- DB_NAME=gitea  
- DB_USER=gitea  
- DB_PASSWD=gitea  
restart always  
volumes  
- gitea:/data  
ports  
- 3000:3000  
extra_hosts  
- "www.jenkins.com:host-gateway"  
networks  
- webnet  
db  
image postgres:alpine  
container_name gitea_db  
environment  
- POSTGRES_USER=gitea  
- POSTGRES_PASSWORD=gitea  
- POSTGRES_DB=gitea  
restart always  
volumes  
- gitea_postgres:/var/lib/postgresql/data  
expose  
- 5432  
networks  
- webnet  
volumes  
gitea_postgres  
name gitea_postgres  
gitea  
name gitea  
networks  
webnet  
name webnet
```

7. Save and verify file exists:

```
[ec2-user@ip-172-31-7-50 ~]$ sudo vim compose.yaml  
[ec2-user@ip-172-31-7-50 ~]$ ls  
compose.yaml
```

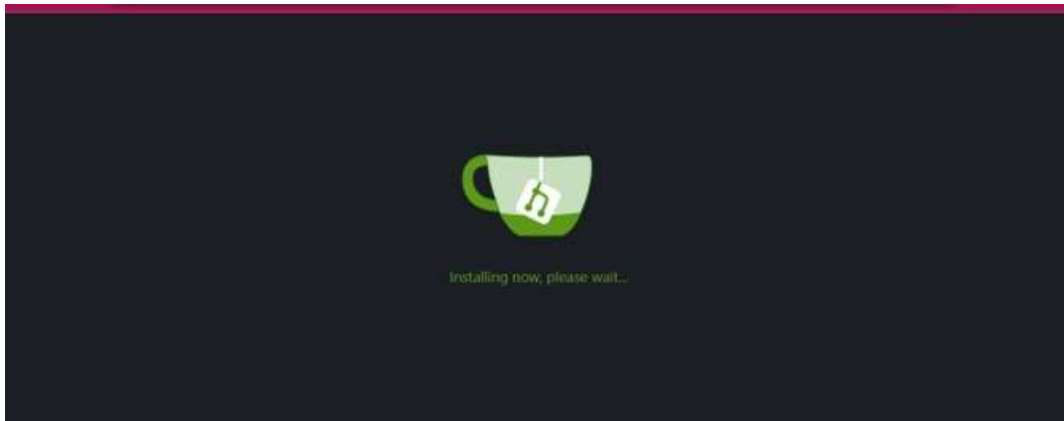
8. Add ec2-user to docker group, show groups before re-login, exit and reconnect, show groups after reconnect:



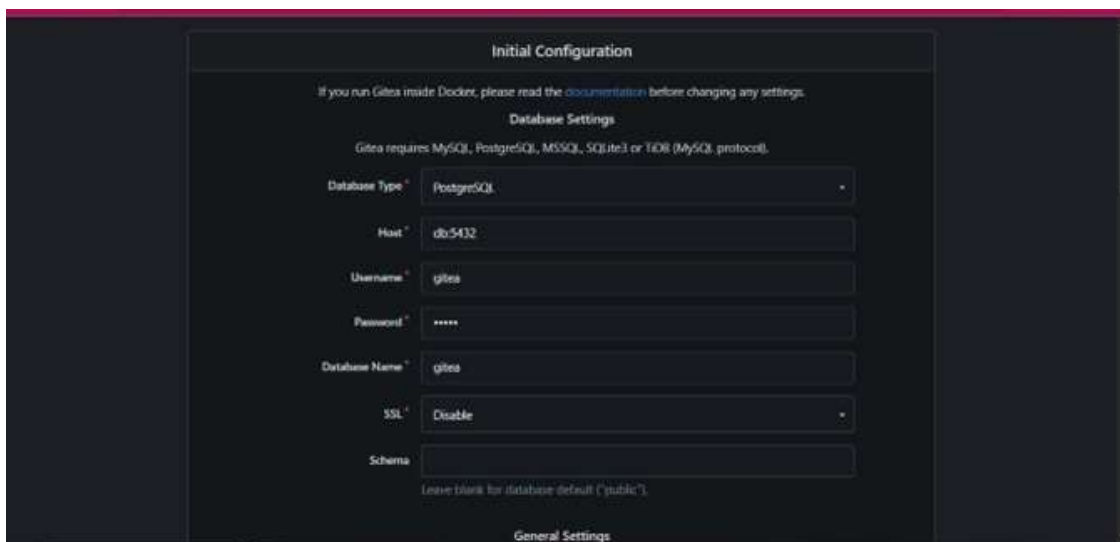
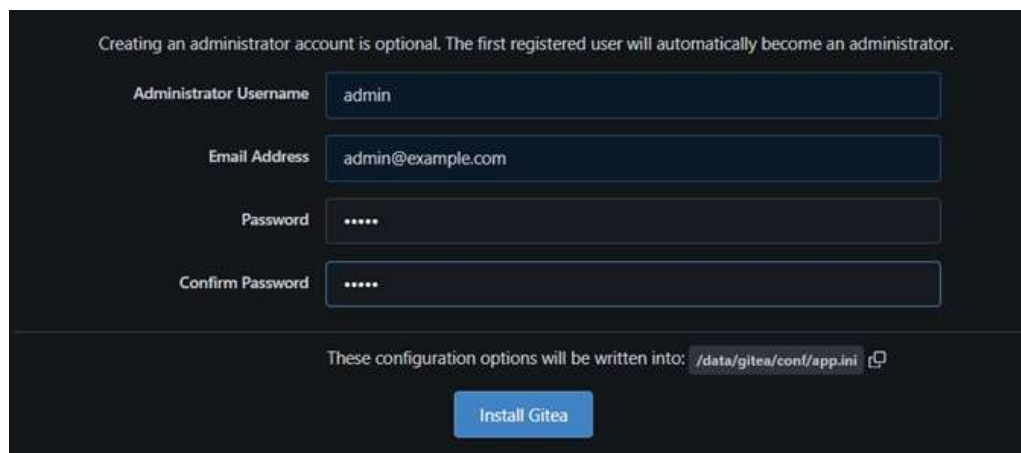




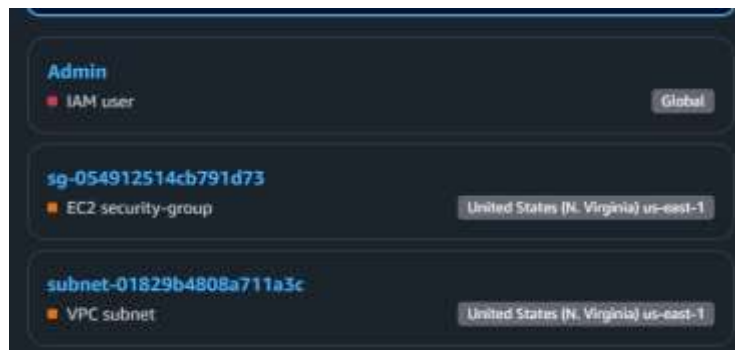
11. From your Windows browser navigate to: <http://Public-IP:3000> — capture the Gitea setup/install page:



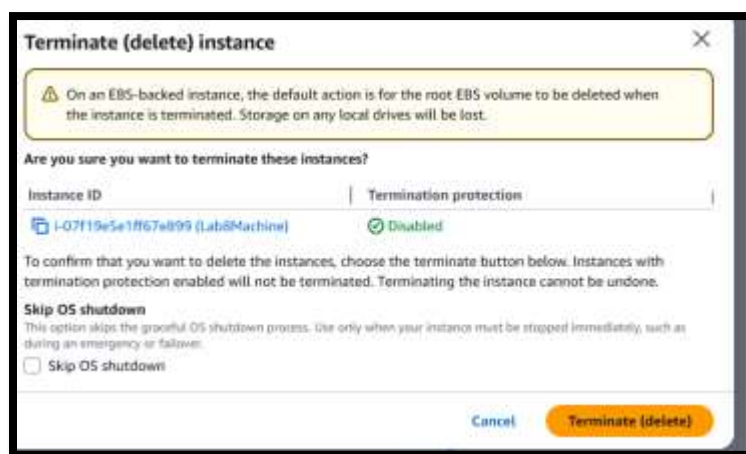
12. Complete initial Gitea setup (create admin user, create a repo) and capture Gitea showing the created repository:

A dark-themed screen titled "Initial Configuration". It contains a section for "Database Settings" with the following fields: "Database Type" (PostgreSQL), "Host" (db-5432), "Username" (gitea), "Password" (masked with dots), "Database Name" (gitea), "SSL" (Disable), and "Schema" (empty). A note at the bottom of the database settings section says "Leave blank for database default ('public')." Below the database settings is a section for "General Settings".A dark-themed screen titled "Creating an administrator account is optional. The first registered user will automatically become an administrator." It contains four input fields: "Administrator Username" (admin), "Email Address" (admin@example.com), "Password" (masked with dots), and "Confirm Password" (masked with dots). Below the fields is a line of text: "These configuration options will be written into: /data/gitea/conf/app.ini" with a small icon to the right. At the bottom is a blue button labeled "Install Gitea".

## Cleanup — Remove resources to avoid charges

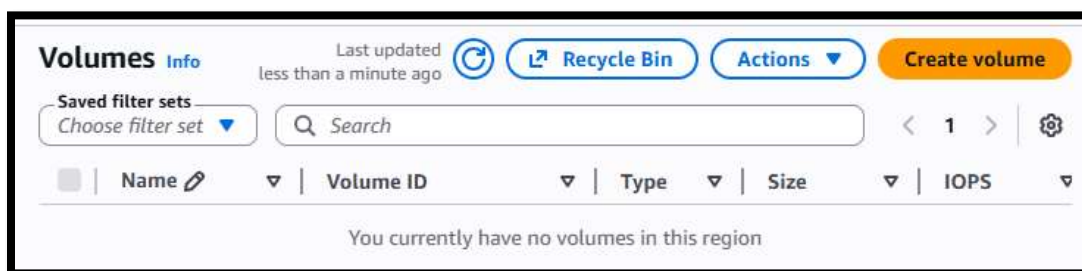


### 1. Terminate the EC2 instance Lab8Machine:



<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type
<input checked="" type="checkbox"/>	Lab8Machine	i-07f19e5e1ff67e899	Terminated	t3.micro

### 2. Delete associated EBS volumes and snapshots (if any).



### 3. Delete security group Lab8SecurityGroup and key pair Lab8Key from the EC2 console (after instances terminated)

Delete security groups

Are you sure that you want to delete this security group?

- sg-0d1b8a62e791e600c - Lab8SecurityGroup

Cancel

Delete

Lab8Key could be associated with one or more instances.

Delete Lab8Key

To confirm deletion, type *Delete* in the field

Cancel

Delete

#### 4. Delete IAM users Lab8User and any access keys

Delete Lab8User?

Delete Lab8User permanently? This will also delete all its user data, security credentials and inline policies.

User name	Last activity
Lab8User	2 hours ago

Note: Recent activity usually appears within 4 hours. Data is stored for a maximum of 365 days, depending when your region began supporting this feature. [Learn more](#)

To avoid accidental deletions, we ask you to provide additional written consent.

To confirm this deletion, type "confirm".

Cancel

Delete user

Users (1/1) Info

Refresh

Delete

Create user

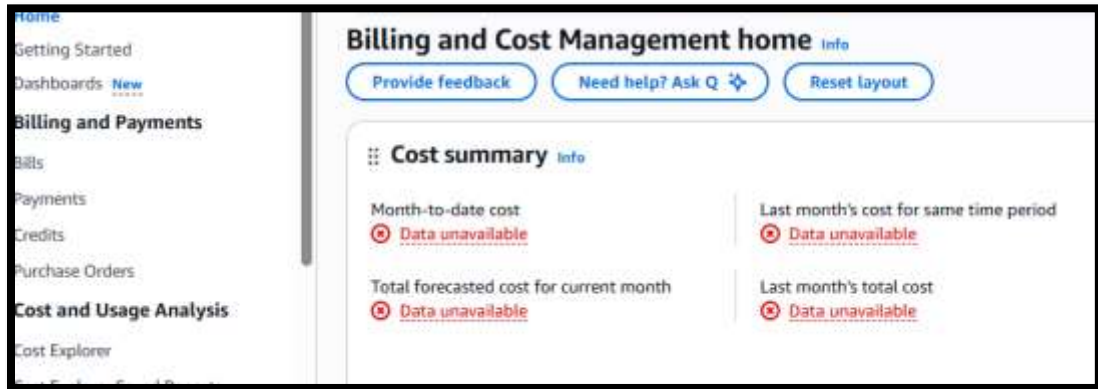
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

< 1 >

Settings

<input checked="" type="checkbox"/>	User name	Path	Group:	Last activity
<input checked="" type="checkbox"/>	Admin	/	0	16 hours ago

5. Final cleanup summary (show billing or resource groups with no active resources if possible).



\*\*\*\*\*