



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](#)

23-22411-008@se.fjwu.edu.pk

AWS account name

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

Anara Hayat

[Verify email address](#)

OR

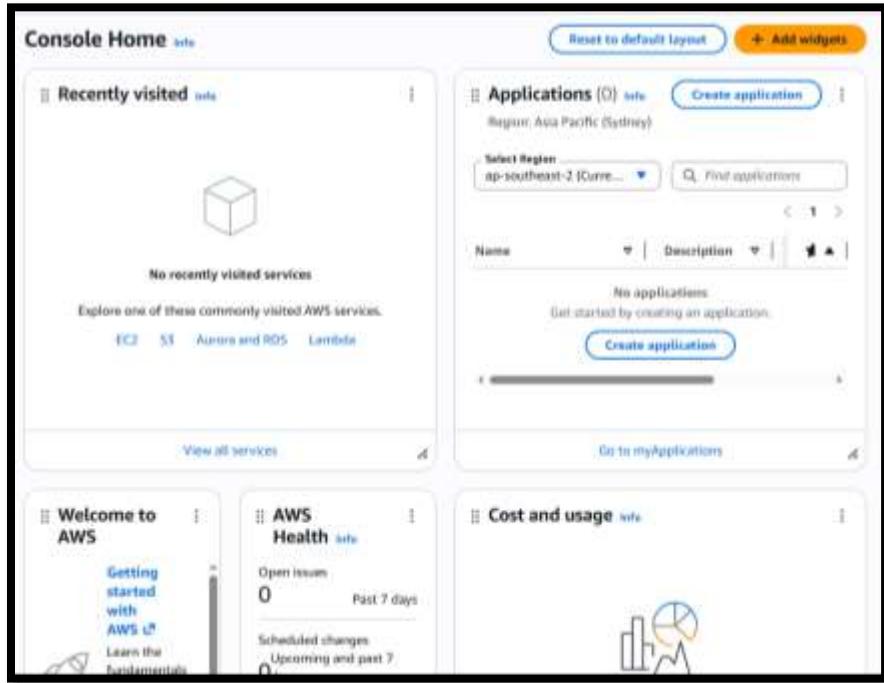
[Sign in to an existing AWS account](#)

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 Console Home page. At the top, there's a navigation bar with icons for CloudWatch, Lambda, S3, and others, followed by a search bar and region selection (Asia Pacific (Sydney)). Below the navigation is a header with "Console Home" and "Info" buttons, and "Reset to default layout" and "Add widgets" buttons. The main content area has two sections: "Recently visited" (with a cube icon and "No recently visited services" message) and "Applications (0)" (with a "Create application" button, a "Select Region" dropdown set to "ap-southeast-2 (Curre...)", a "Find applications" search bar, and a "No applications" message with "Get started by creating an application").

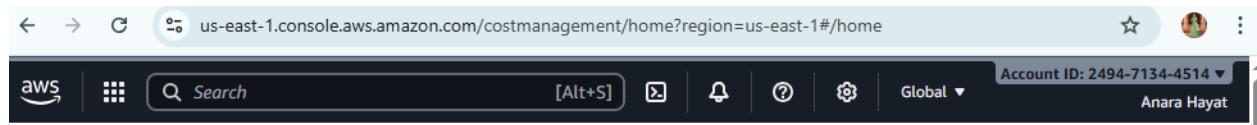
3. Sign in as the root user (root email). Immediately capture:



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

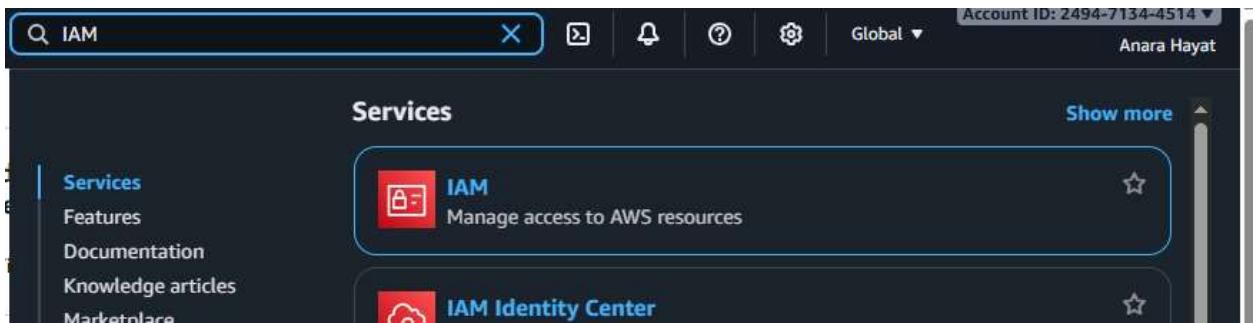


5. Task 1 summary screenshot (combine evidence):



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.

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 functions.

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.

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

Permissions policies (1/1426)

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

Filter by Type All types ▾

Policy name	Type	Attached ...
AccessAnalyzerServiceRole	AWS managed	0
AdministratorAccess	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

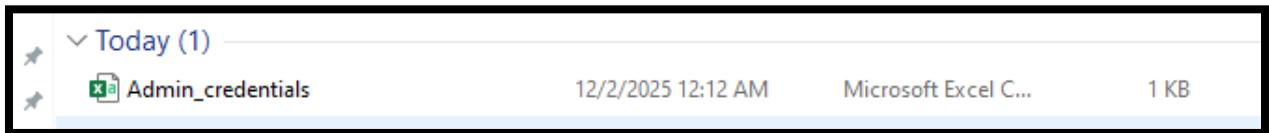
Name	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

Users (1) [info](#)

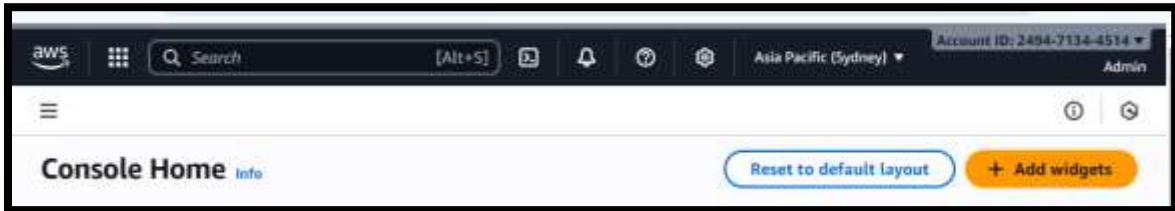
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Groups	Last activity
Admin	/	0	-

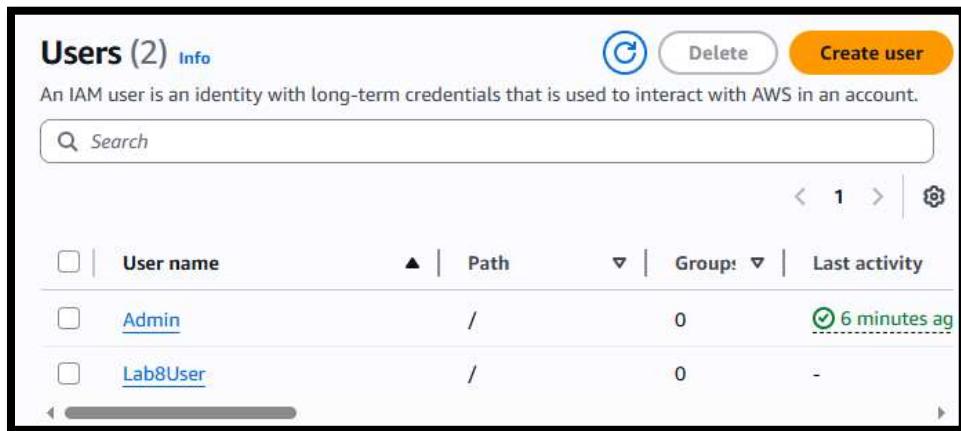
3. Download the Admin .csv and show its presence on your Windows host



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



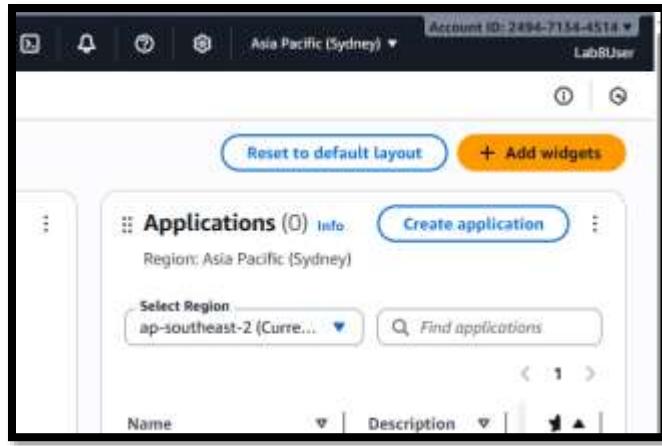
5. While logged in as Admin, create Lab8User



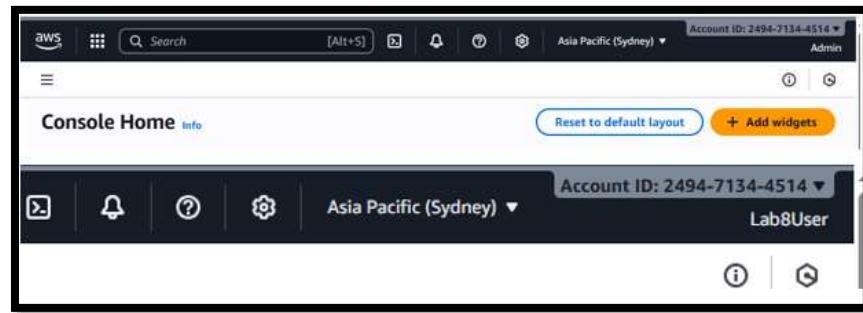
6. Download/save the Lab8User CSV on your Windows host



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.

Two screenshots of the AWS VPC console. The top screenshot shows the "Services" tab selected in the navigation bar, with "VPC" highlighted. The bottom screenshot shows the "VPC dashboard" with the "Middle East (UAE)" region selected. The dashboard displays "Resources by Region" for UAE 1, UAE 2, and UAE 3, showing counts for VPCs, NAT Gateways, Subnets, and VPC Peering Connections. On the left, a sidebar lists "Virtual private cloud" resources: Your VPCs, Subnets, Route tables, internet gateways, Egress-only internet gateways, and DHCP option sets. On the right, there are "Service Health" and "Settings" sections.

2. View VPCs list. Capture:

The screenshot shows the 'Your VPCs' page in the AWS Management Console. At the top, there's a navigation bar with 'VPCs' selected and 'VPC encryption controls - new' as the current view. Below the navigation is a search bar labeled 'Find VPCs by attribute or tag'. A table lists one VPC entry: 'Your VPCs (1)'. The table has columns for 'Name' (with a checkbox), 'VPC ID' (with a link to 'vpc-0f707761dae35d762'), and 'State' (with a green checkmark and 'Available'). The top right of the table area shows 'Last updated less than a minute ago' and includes 'Actions' and 'Create VPC' buttons.

3. View Subnets list.

The screenshot shows the 'Subnets' page in the AWS Management Console. At the top, there's a navigation bar with 'Subnets (3)' selected and 'Create subnet' as the current view. Below the navigation is a search bar labeled 'Find subnets by attribute or tag'. A table lists three subnet entries: 'subnet-07ea3d90e7c5b2094', 'subnet-0380625fba760f53e', and 'subnet-043ff1d25baf4a0fa'. The table has columns for 'Name' (checkboxes), 'Subnet ID' (links), and 'State' (green checkmarks and 'Available'). The top right of the table area shows 'Last updated less than a minute ago' and includes 'Actions' and 'Create subnet' buttons.

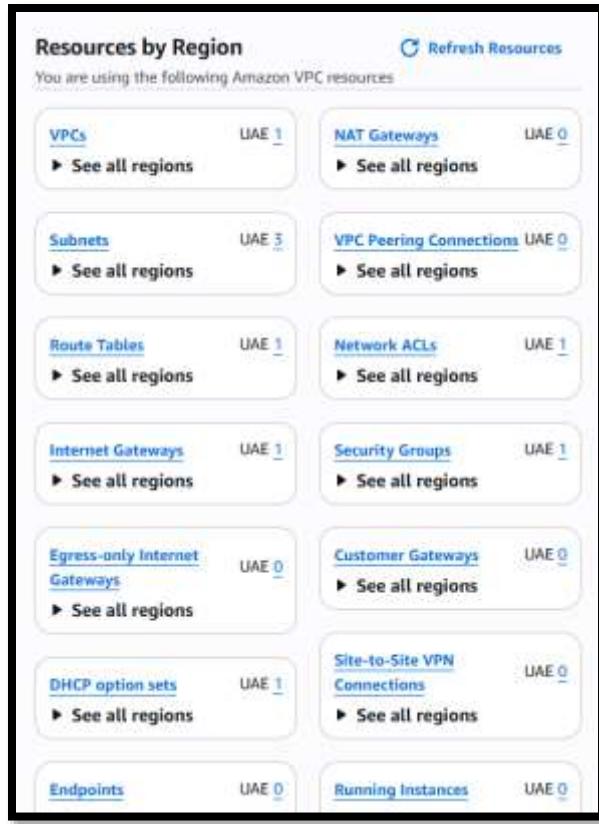
4. View Route Tables list. Capture:

The screenshot shows the 'Route tables' page in the AWS Management Console. At the top, there's a navigation bar with 'Route tables (1)' selected and 'Create route table' as the current view. Below the navigation is a search bar labeled 'Find route tables by attribute or tag'. A table lists one route table entry: 'rtb-0aa33b96fa897436c'. The table has columns for 'Name' (checkbox), 'Route table ID' (link), and 'Explicit subnet assoc' (empty). The top right of the table area shows 'Last updated less than a minute ago' and includes 'Actions' and 'Create route table' buttons.

5. View Network ACLs list

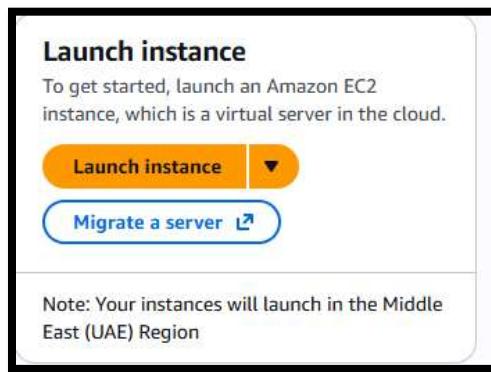
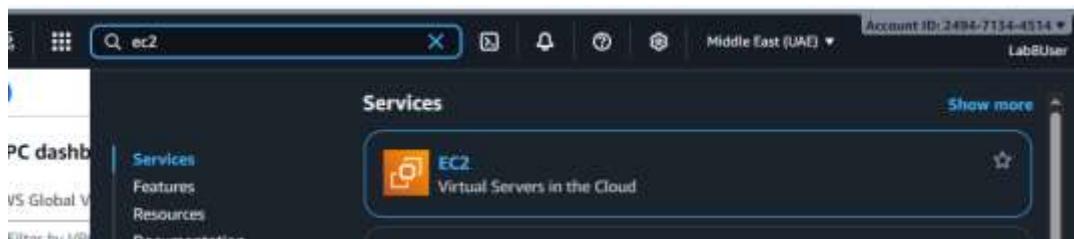
The screenshot shows the 'Network ACLs' page in the AWS Management Console. At the top, there's a navigation bar with 'Network ACLs (1)' selected and 'Create network ACL' as the current view. Below the navigation is a search bar labeled 'Find Network ACLs by attribute or tag'. A table lists one network ACL entry: 'acl-036eaed368f3021b7'. The table has columns for 'Name' (checkbox), 'Network ACL ID' (link), and 'Associated with' (link to '3 Subnets'). The top right of the table area shows 'Actions' and 'Create network ACL' buttons.

6. Task 3 summary (combine evidence)



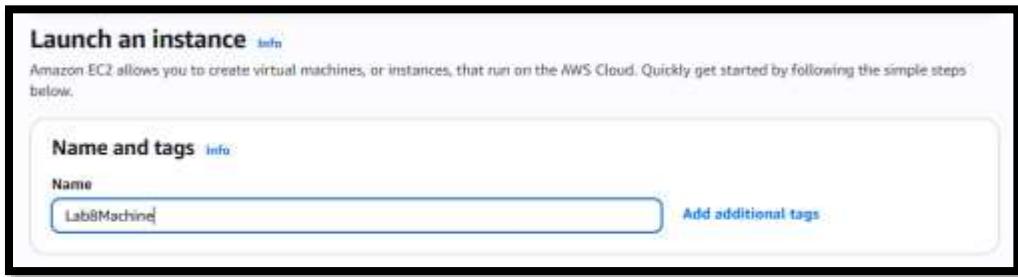
Task 4 — Launch EC2, SSH, install Docker & Docker Compose, deploy Gitea

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

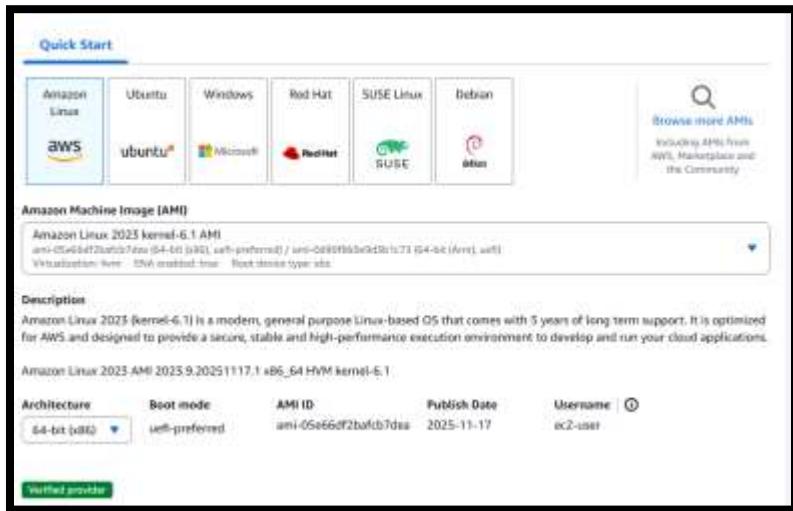


2. Instance Launch configuration (during review before launching). Configure

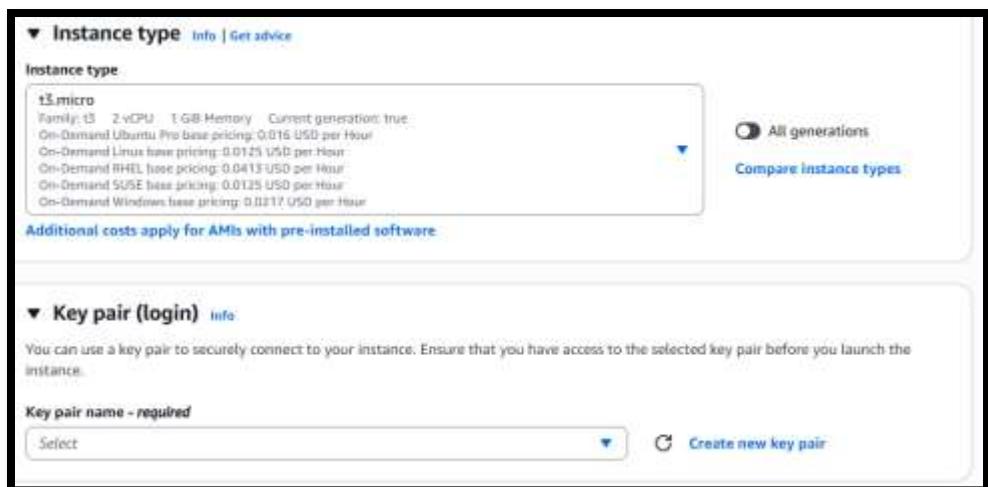
Name: Lab8Machine



AMI: Amazon Linux 2



Instance type: t3.micro



Security group: Create Lab8SecurityGroup with SSH from My IP

▼ Network settings [Info](#)

VPC - required | [Info](#)
 vpc-0f707761dae35d762 (default) ▾ [Create new VPC](#)

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	Protocol Info	Port range Info
ssh ▾	TCP	22
Source type Info	Name Info	Description - optional Info
My IP ▾	<input type="text"/> Add CIDR, prefix list or security group	e.g. SSH for admin desktop
<input type="text"/> 103.53.162.80/32 X		

[Add security group rule](#)

Storage: default

▼ Configure storage [Info](#) [Advanced](#)

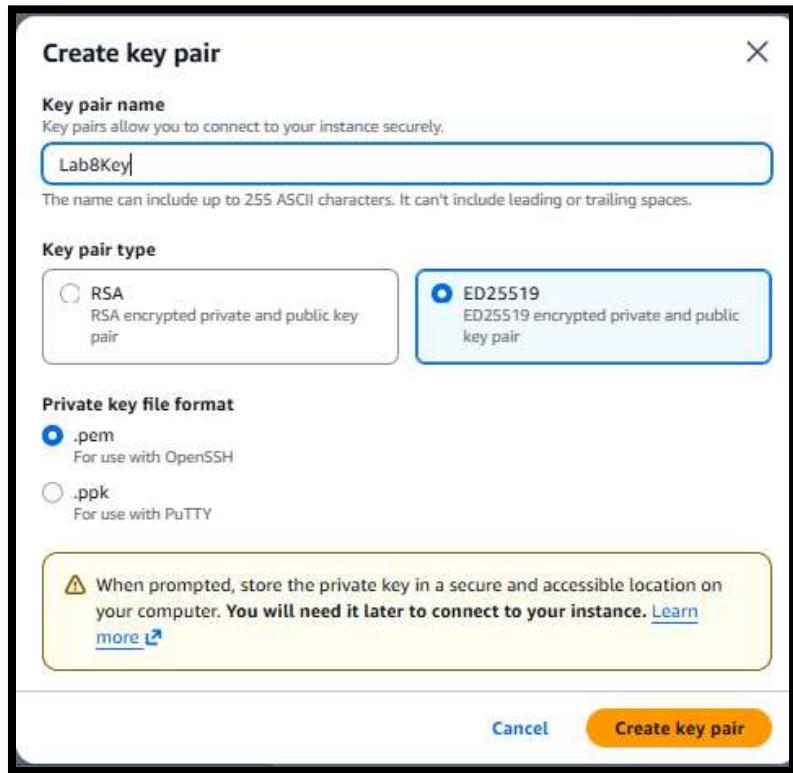
1x 8 GiB gp3 ▾ Root volume, 3000 IOPS, Not encrypted

[Add new volume](#)

② 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](#)

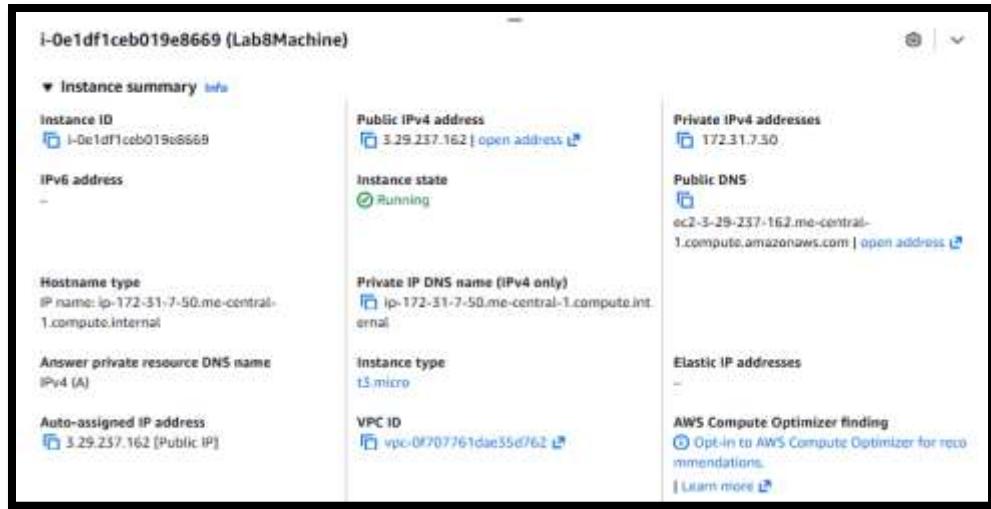
Key pair: Create Lab8Key (ED25519, .pem) and download the .pem file to your Windows host



Capture the final review page and key download

The top screenshot shows the EC2 Instances list with one instance named "Lab8Machine" in the "Running" state. The bottom screenshot shows a file download dialog for "Lab8Key.pem", which is a PEM File of size 1 KB, downloaded on 12/2/2025 at 1:34 AM.

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



4. On Windows host, run SSH using the downloaded .pem

```
PS C:\Users\Anara Hayat> ssh -i ~/Downloads/Lab8Key.pem ec2-user@3.29.237.162
,#
~\_ ##### Amazon Linux 2023
~~ \#####\_
~~ \###|_
~~ \#/ __ https://aws.amazon.com/linux/amazon-linux-2023
~~ \~'`->
~~ /_
~~ .._/
~~ /_/
~/m/
[ec2-user@ip-172-31-7-50 ~]$ [ec2-user@ip-172-31-7-50 ~]$
```

5. Run the install commands on the EC2 shell:

```
[ec2-user@ip-172-31-7-50 ~]$ sudo yum update -y
Amazon Linux 2023 Kernel Livepatch repository
Last metadata expiration check: 0:00:01 ago on Tue Dec  2 09:03:39 2025.
Dependencies resolved.
Nothing to do.
Complete!
[ec2-user@ip-172-31-7-50 ~]$ sudo yum install -y docker
Last metadata expiration check: 0:00:18 ago on Tue Dec  2 09:03:39 2025.
Dependencies resolved.
=====
Package           Architecture Version      Repository   Size
=====
Installing:
docker            x86_64       25.0.13-1.amzn2023.0.2    amazonlinux  46 M
Installing dependencies:
container-selinux  noarch      4:2.242.0-1.amzn2023          amazonlinux  58 k
containerd         x86_64       2.1.4-1.amzn2023.0.2    amazonlinux  23 M
Installed:
container-selinux-4:2.242.0-1.amzn2023.noarch      containerd-2.1.4-1.amzn2023.0.2.x86_64
docker-25.0.13-1.amzn2023.0.2.x86_64             iptables-lib5-1.8.8-3.amzn2023.0.2.x86_64
iptables-nft-1.8.8-3.amzn2023.0.2.x86_64        libcgroup-3.0-1.amzn2023.0.1.x86_64
libnftnefinkontrack-1.0.8-2.amzn2023.0.2.x86_64  libnftnefinkontrack-1.0.1-19.amzn2023.0.2.x86_64
libnftnln-1.2.2-2.amzn2023.0.2.x86_64            pigz-2.5-1.amzn2023.0.3.x86_64
runc-1.3.3-2.amzn2023.0.1.x86_64
```

Complete!

```
[ec2-user@ip-172-31-7-50 ~]$ sudo mkdir -p /usr/local/docker/cli-plugins
[ec2-user@ip-172-31-7-50 ~]$ sudo curl -SL https://github.com/docker/compose/releases/latest/download/docker-compose-linux-x86_64 -o /usr/local/lib/docker/cli-plugins/docker-compose
% Total % Received % Xferd Average Speed Time Time Current
% Total % Received % Xferd Dload Upload Total Spent Left Speed
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
Warning: Failed to open the file /usr/local/lib/docker/cli-plugins/docker-compose: No such file or directory
curl: (23) client returned ERROR on write of 16375 bytes
[ec2-user@ip-172-31-7-50 ~]$ sudo chmod +x /usr/local/lib/docker/cli-plugins/docker-compose
chmod: cannot access '/usr/local/lib/docker/cli-plugins/docker-compose': No such file or directory
[ec2-user@ip-172-31-7-50 ~]$ sudo systemctl start docker
```

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

7. Save and verify file exists:

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

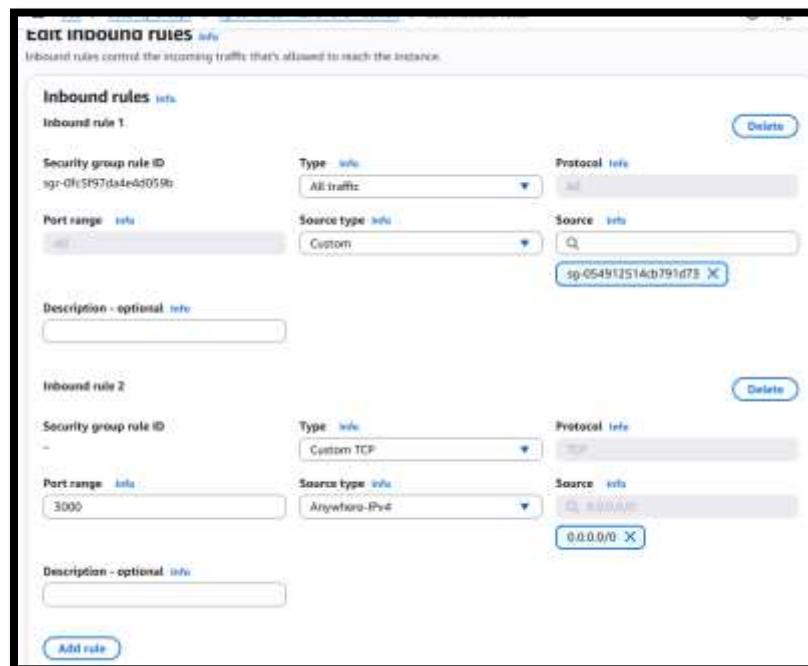
8. Add ec2-user to docker group, show groups before re-login, exit and reconnect, show groups after reconnect:

```
[ec2-user@ip-172-31-7-50 ~]$ groups
ec2-user adm wheel systemd-journal
[ec2-user@ip-172-31-7-50 ~]$
[ec2-user@ip-172-31-7-50 ~]$
[ec2-user@ip-172-31-7-50 ~]$ sudo usermod -aG docker $USER
[ec2-user@ip-172-31-7-50 ~]$ groups
ec2-user adm wheel systemd-journal
[ec2-user@ip-172-31-7-50 ~]$ exit
logout
There are stopped jobs.
Connection to 3.29.237.162 closed.
PS C:\Users\Anara Hayat> ssh -i ~/Downloads/Lab8Key.pem ec2-user@3.29.237.162
,
~\_\_ #### Amazon Linux 2023
~~ \_\#\#\#
~~ \#\#\#
~~ \#\#\#
~~ \#/ __ https://aws.amazon.com/linux/amazon-linux-2023
~~ V~`__>
~~ /_
~~ /_
~~ /_
/m/
Last login: Tue Dec  2 09:01:48 2025 from 103.53.162.80
[ec2-user@ip-172-31-7-50 ~]$ groups
ec2-user adm wheel systemd-journal docker
[ec2-user@ip-172-31-7-50 ~]$
```

9. Run docker compose up -d from the directory with compose.yaml:

```
[ec2-user@ip-172-31-7-50 ~]$ sudo docker-compose up -d
[+] Running 2/2
  Container gitea   Running
  Container gites_db Running
[ec2-user@ip-172-31-7-50 ~]$ sudo docker-compose ps
NAME      IMAGE           COMMAND          SERVICE    CREATED        STATUS      PORTS
gitea     gitea/gitea:latest "/usr/bin/entrypoint.s..." gitea    3 minutes ago Up 3 minutes  22/tcp, 0.0.0.0:3000->3000/tcp
gites_db  postgres:alpine "docker-entrypoint.s..." db      3 minutes ago Up 3 minutes  5432/tcp
[ec2-user@ip-172-31-7-50 ~]$
```

10. Edit the security group Lab8SecurityGroup inbound rules in the EC2 console: add Custom TCP rule port 3000 source 0.0.0.0/0 and save. Capture the inbound rules after saving:



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:

The image contains two screenshots of the Gitea setup interface.

Initial Configuration (Top Screenshot):

If you run Gitea inside Docker, please read the [documentation](#) before changing any settings.

Database Settings:

- Database Type: PostgreSQL
- Host: db:5432
- Username: gitea
- Password: [REDACTED]
- Database Name: gitea
- SSL: Disable
- Schema: [Leave blank for database default ("public").]

General Settings

Administrator Account (Bottom Screenshot):

Creating an administrator account is optional. The first registered user will automatically become an administrator.

Administrator Username	admin
Email Address	admin@example.com
Password	[REDACTED]
Confirm Password	[REDACTED]

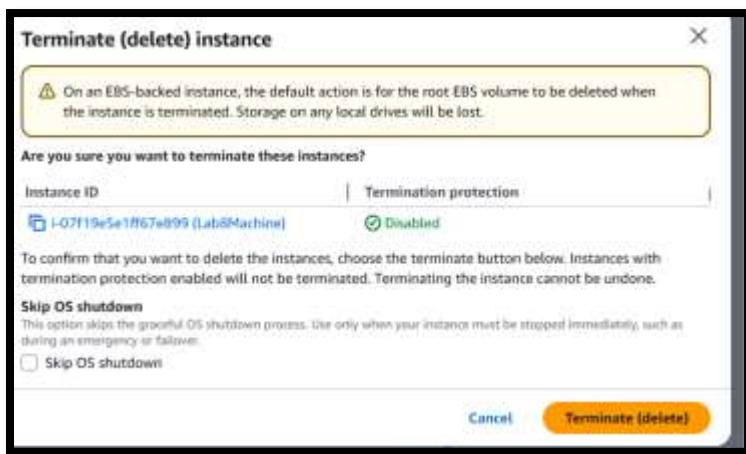
These configuration options will be written into: /data/gitea/conf/app.ini

Install Gitea

Cleanup — Remove resources to avoid charges



1. Terminate the EC2 instance Lab8Machine:

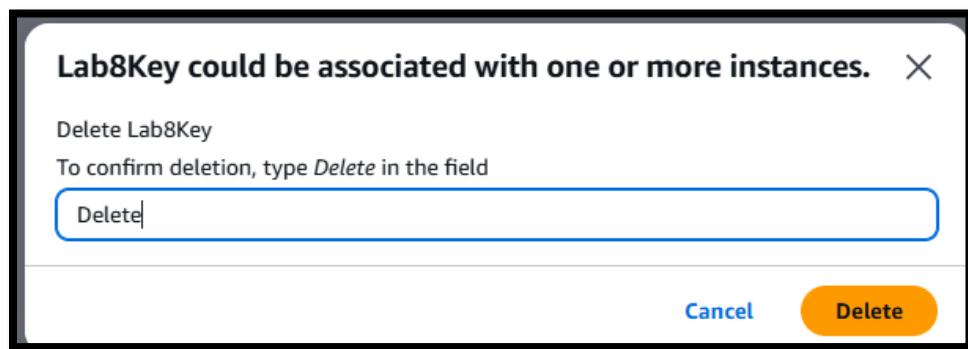
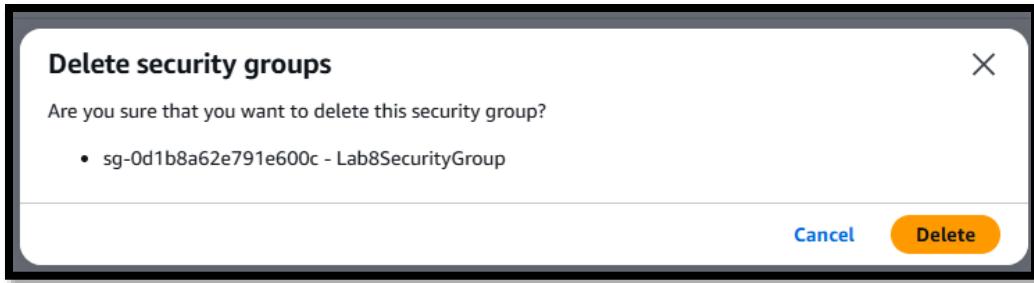


Name	Instance ID	Instance state	Instance type
Lab8Machine	i-07f19e5e1ff67e899	Terminated	t3.micro

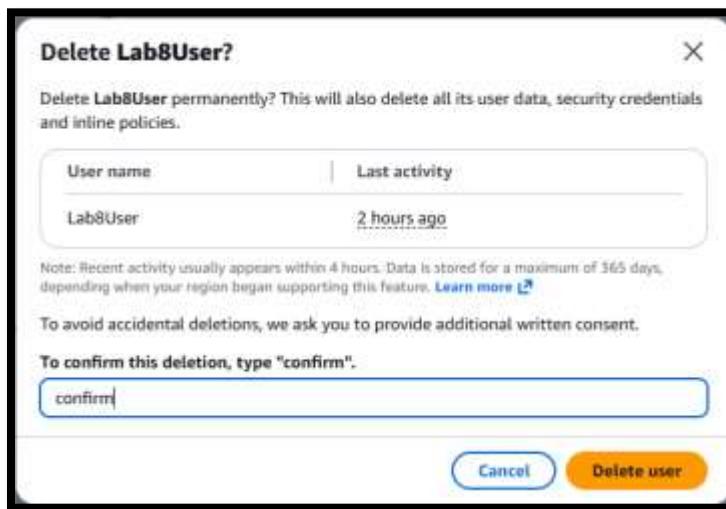
2. Delete associated EBS volumes and snapshots (if any).

Volumes		Info	Last updated less than a minute ago	Recycle Bin	Actions	Create volume
Saved filter sets		Choose filter set	Search			
Name	Volume ID	Type	Size	IOPS		
You currently have no volumes in this region						

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



4. Delete IAM users Lab8User and any access keys



Users (1/1) Info				
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.				
<input type="text"/> Search				
	▲	Path	▼	Group: ▼ Last activity
<input checked="" type="checkbox"/>	User name	/	0	<input checked="" type="checkbox"/> 16 hours ago
<input checked="" type="checkbox"/>	Admin	/	0	<input checked="" type="checkbox"/> 16 hours ago

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

The screenshot shows the Microsoft Billing and Cost Management home page. On the left, there is a navigation sidebar with links like Home, Getting Started, Dashboards (New), Billing and Payments, Cost and Usage Analysis, and Cost Explorer. The main content area is titled "Billing and Cost Management home" and features a "Cost summary" section. This section displays four metrics: "Month-to-date cost" (Data unavailable), "Last month's cost for same time period" (Data unavailable), "Total forecasted cost for current month" (Data unavailable), and "Last month's total cost" (Data unavailable). Each metric is accompanied by a small circular icon with a question mark.
