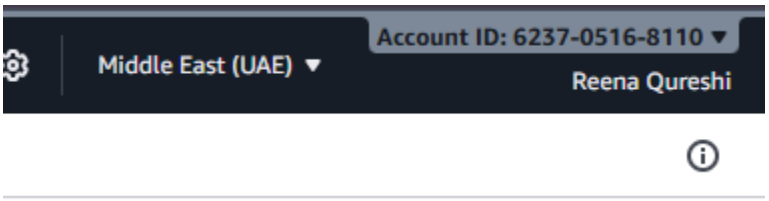
Name : Reena Qureshi

Reg No: 2023-BSE-052

Section: V-B

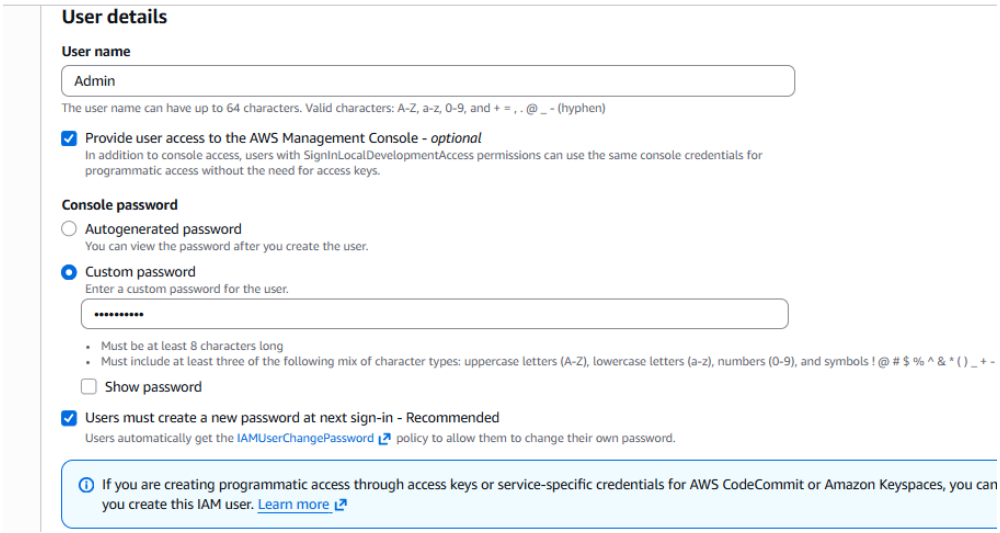
LAB 8

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

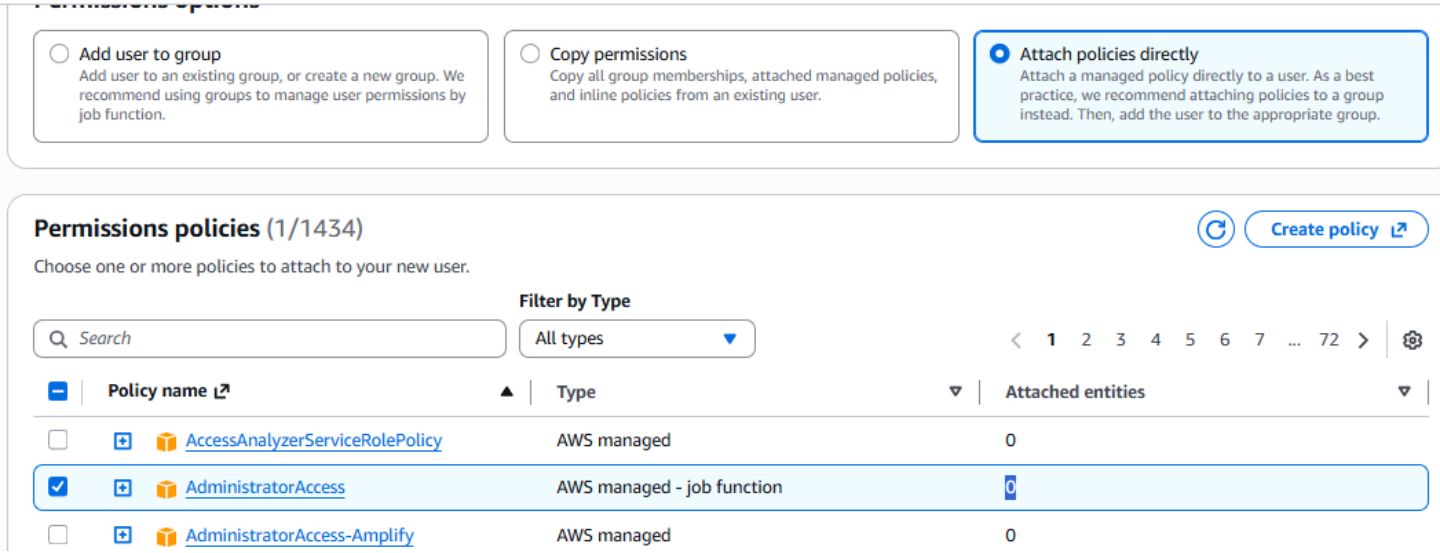


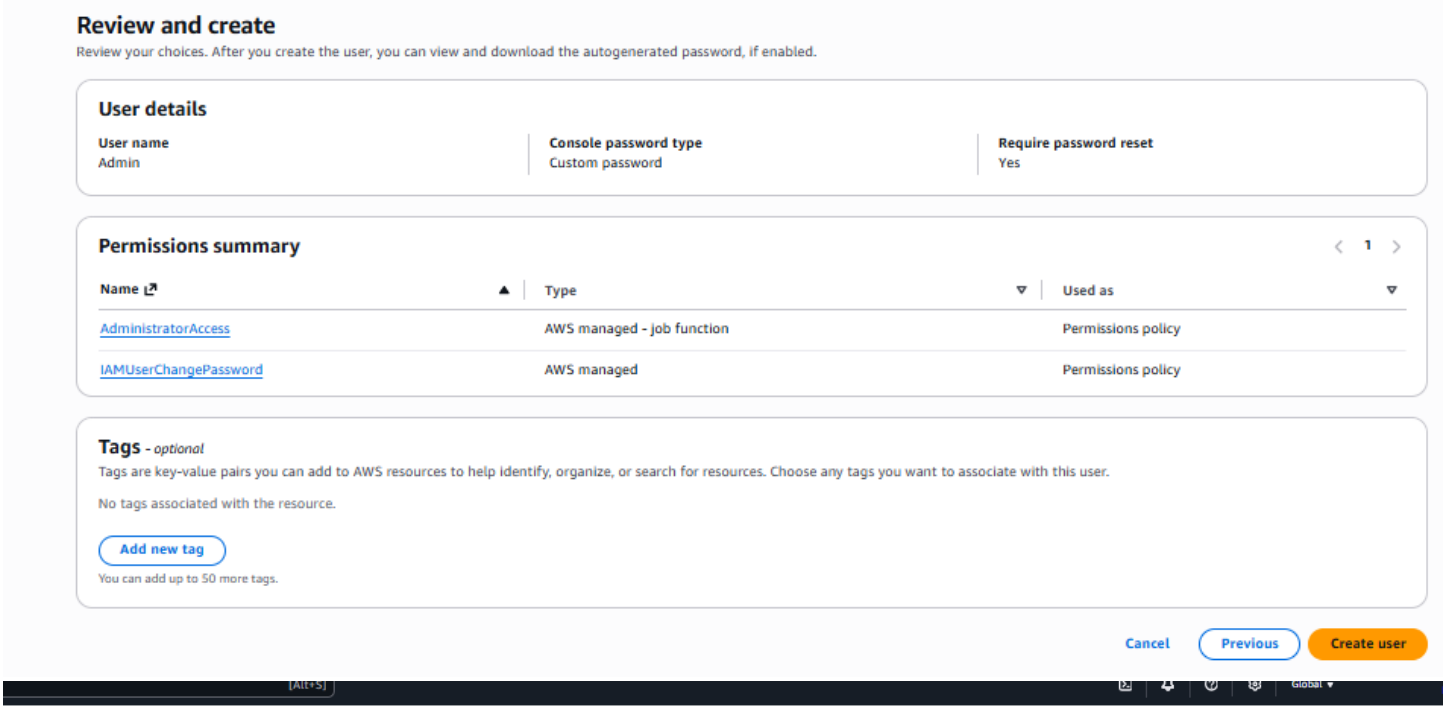
Task 2 — Create IAM Admin and Lab8User with console access

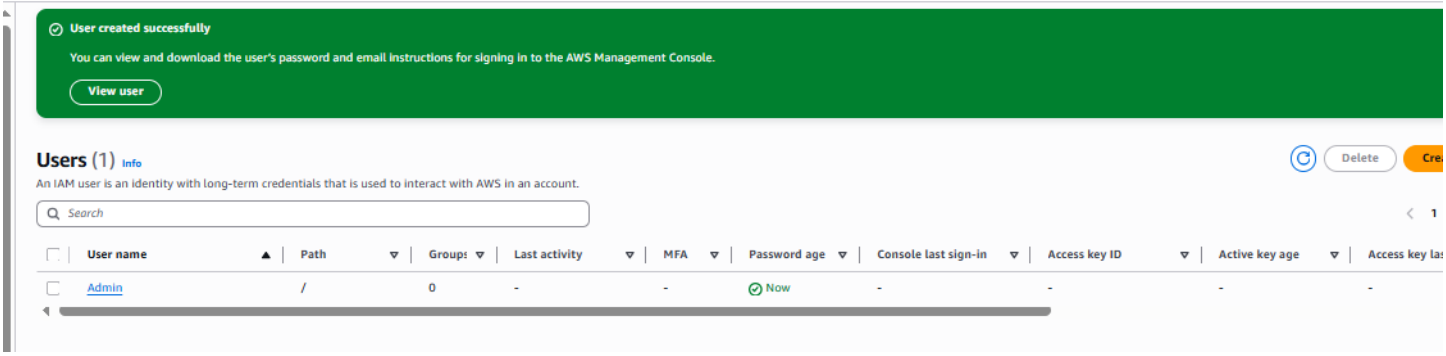
Open IAM via Console search (Alt+S → "IAM").
Create the Admin user: IAM → Users → Create user. Fill:



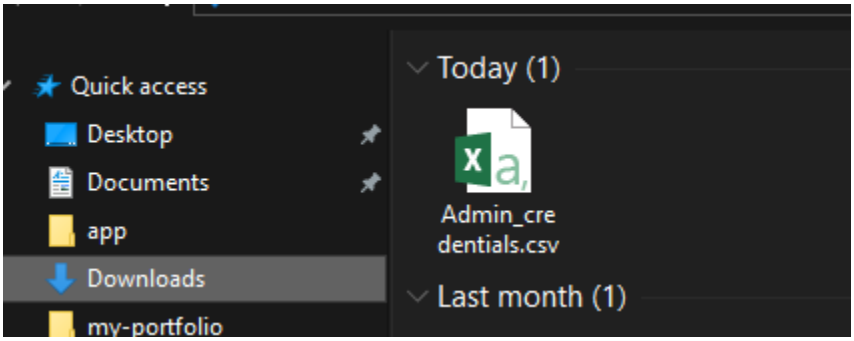
Attach policies directly → AdministratorAccess



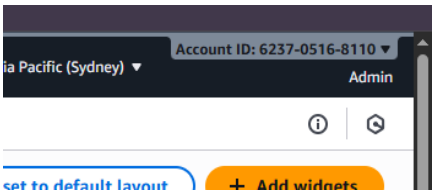




Download the Admin .csv and show its presence on your Windows host (do not display the password text):



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



While logged in as Admin, create Lab8User:

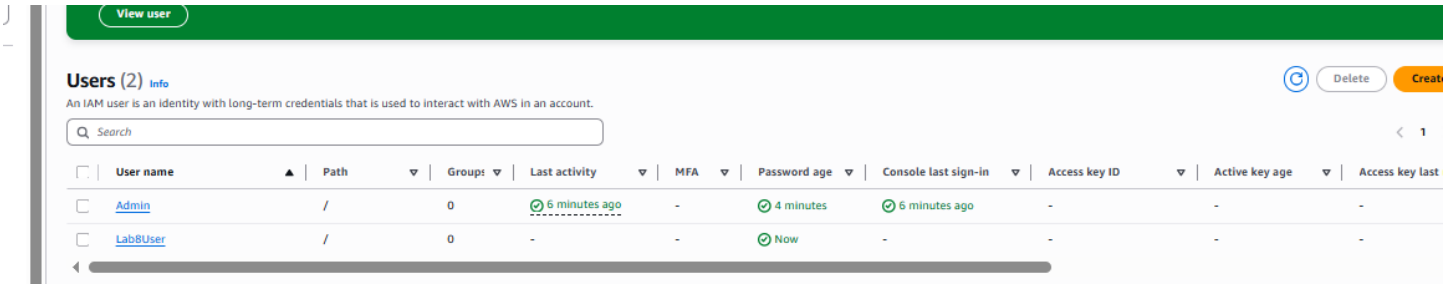
IAM → Users → Create user

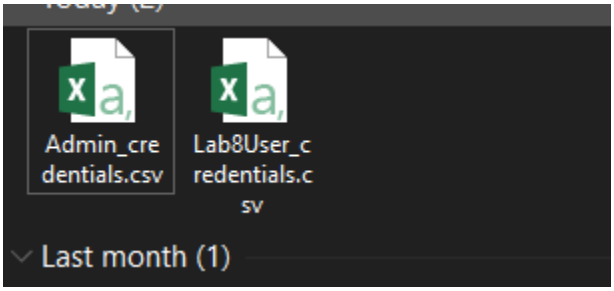
Username: Lab8User

Provide user access to the AWS Management Console

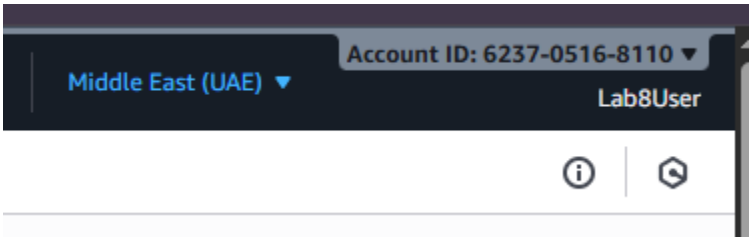
Attach AdministratorAccess policy

Capture the create-user success screen:



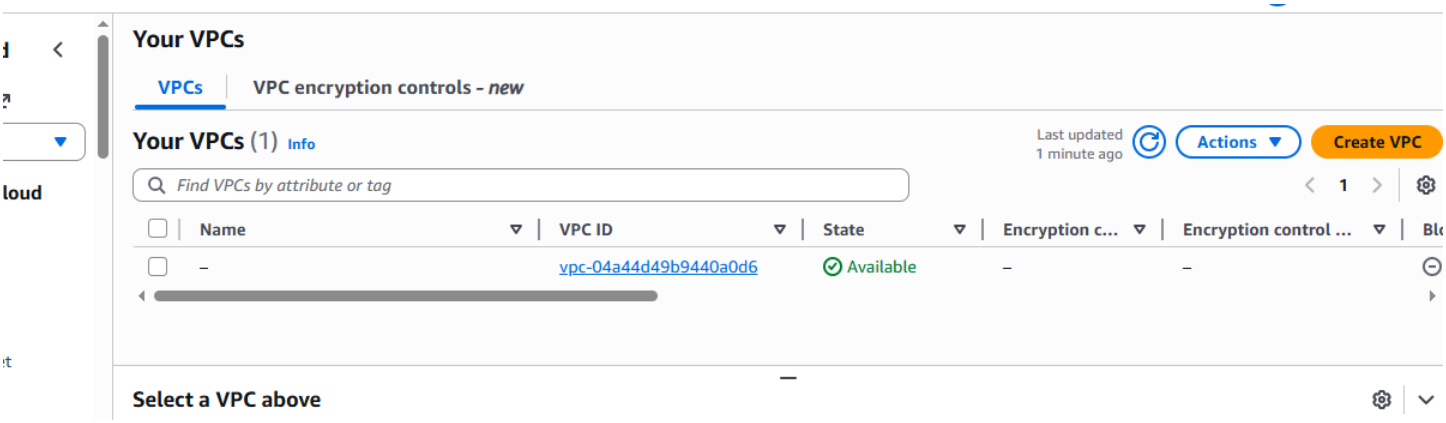


Logout Admin and login as Lab8User (use the Lab8User signin URL and credentials). Capture after login:

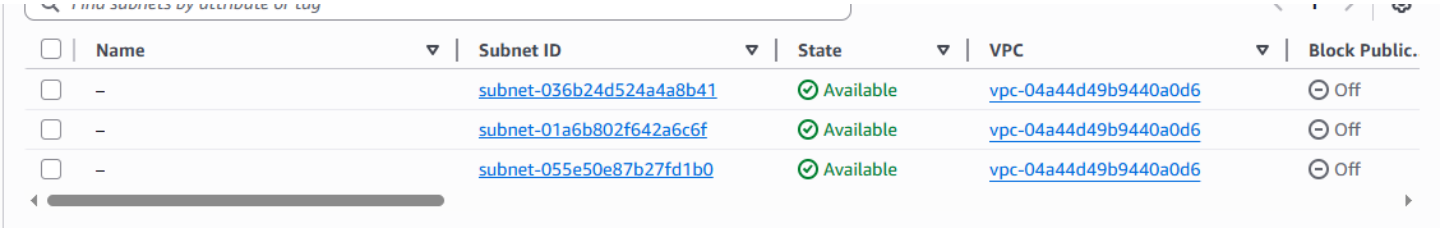


Task 3 — Inspect VPC resources (in UAE me-central-1)

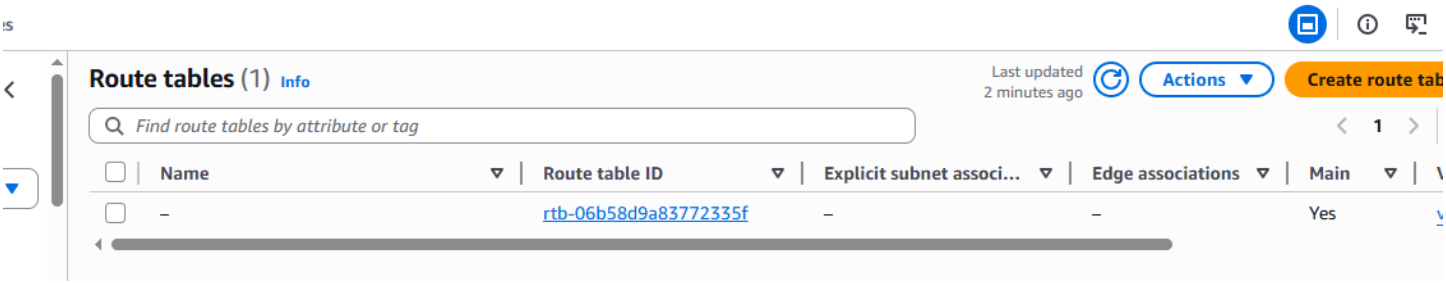
View VPCs list.



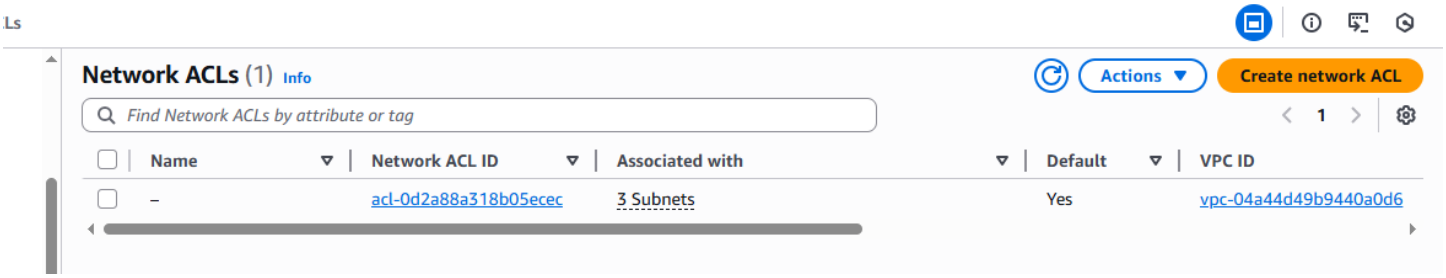
View Subnets list. Capture



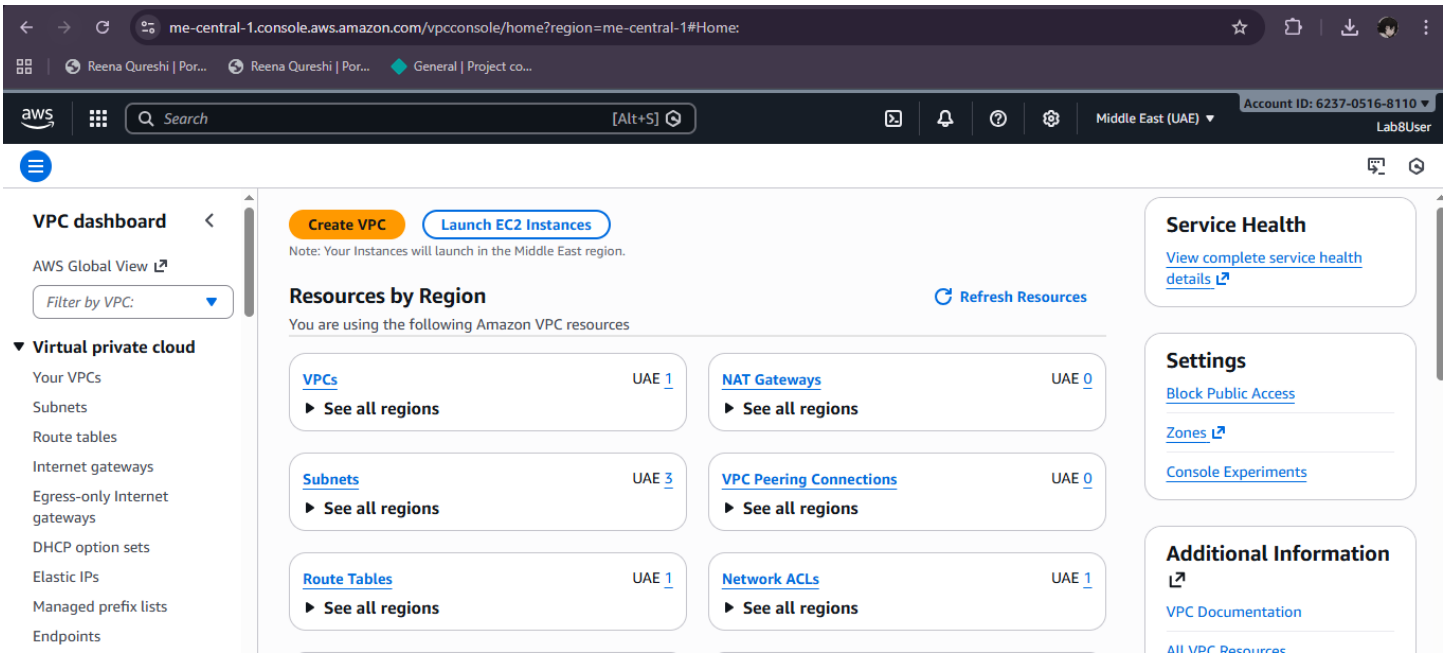
View Route Tables list.



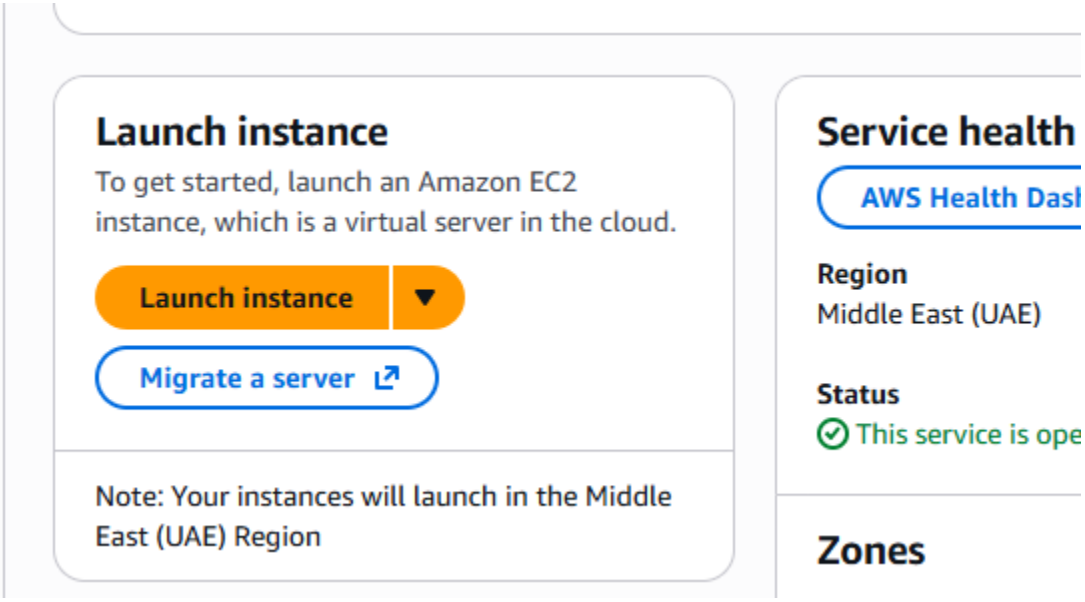
View Network ACLs list.

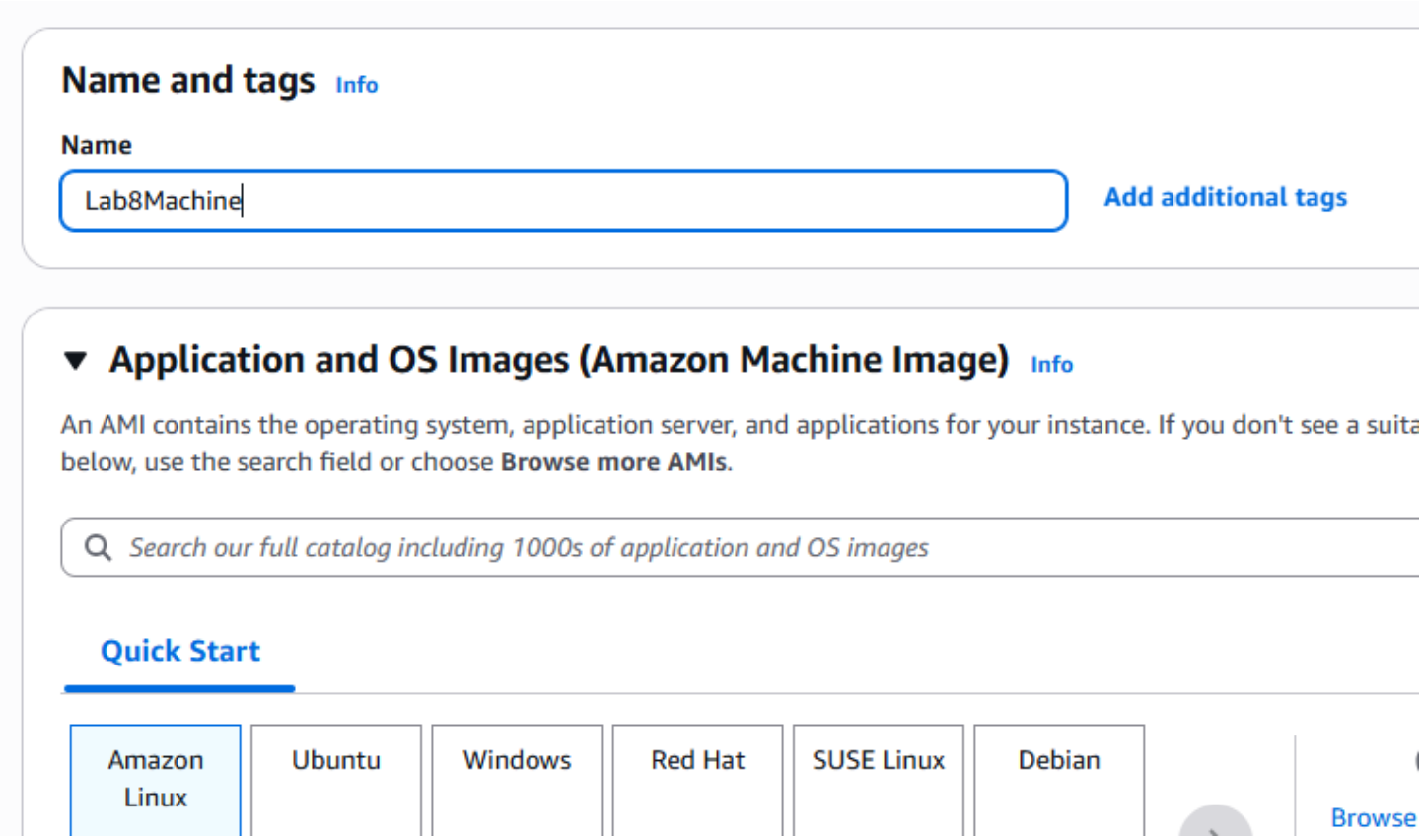


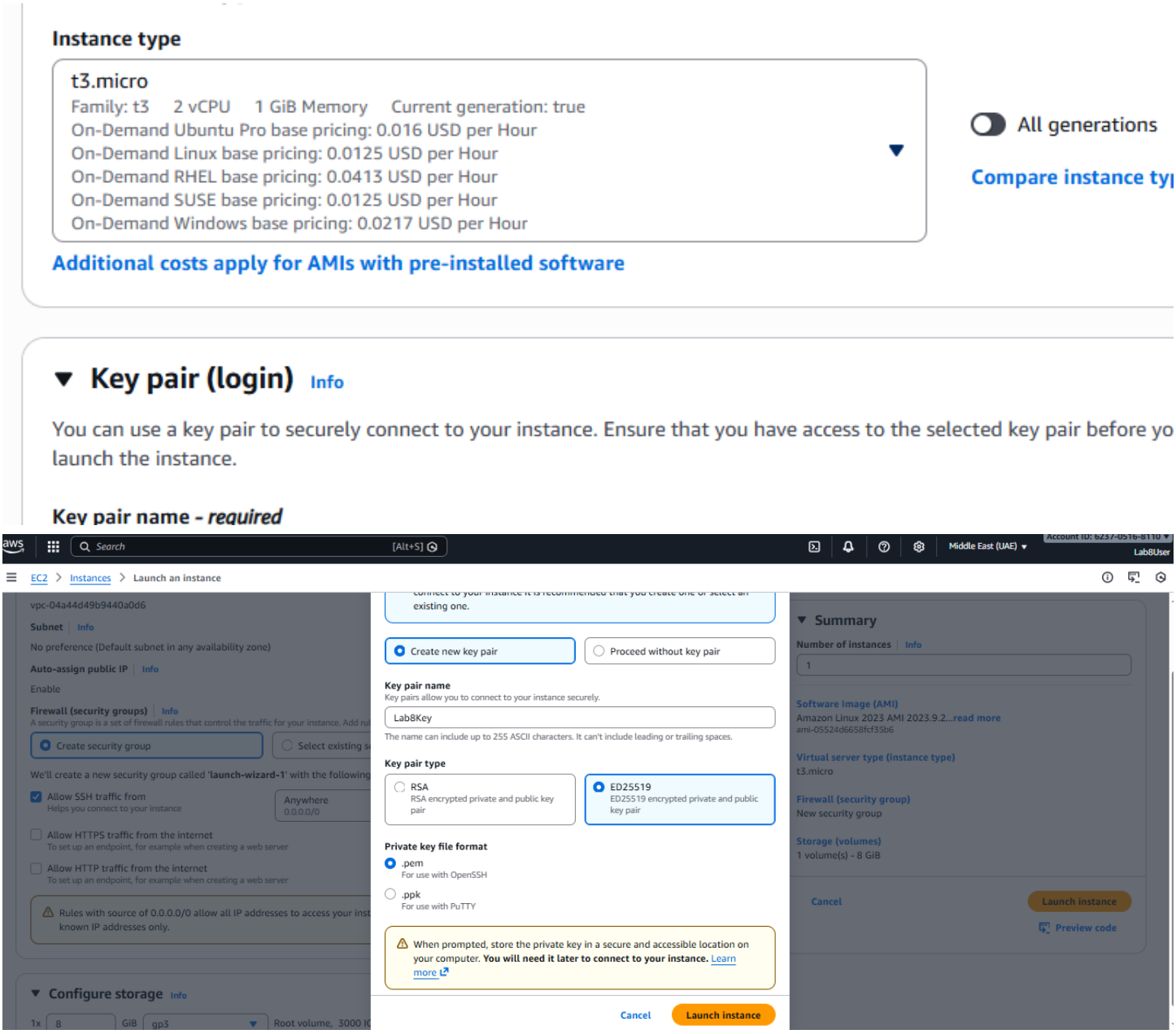
Task 3 summary (combine evidence):



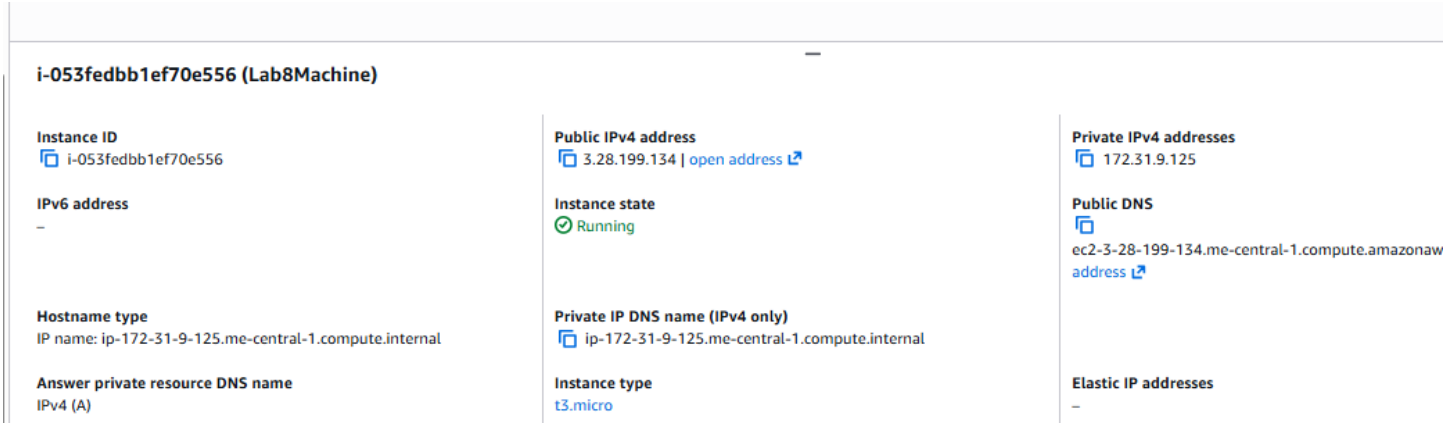
Task 4 — Launch EC2, SSH, install Docker & Docker Compose, deploy Gitea



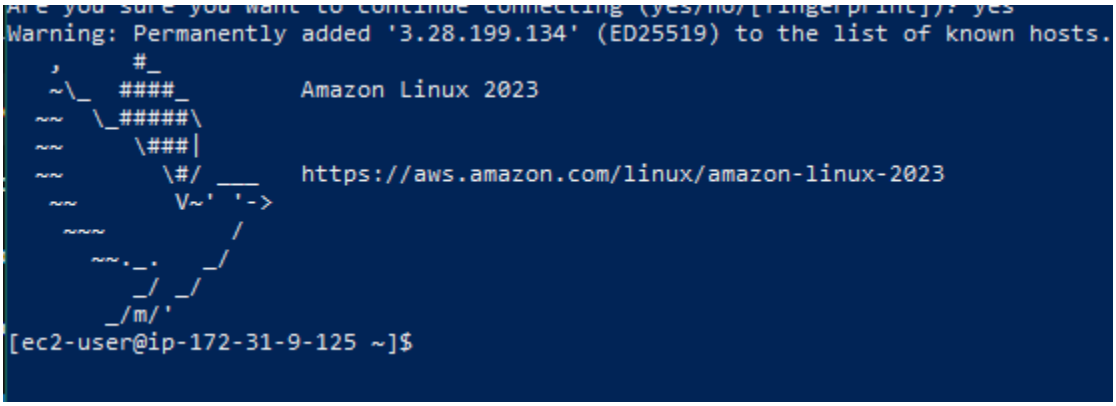




After launch, EC2 Instances list showing Lab8Machine in "running" state and public IPv4 visible.

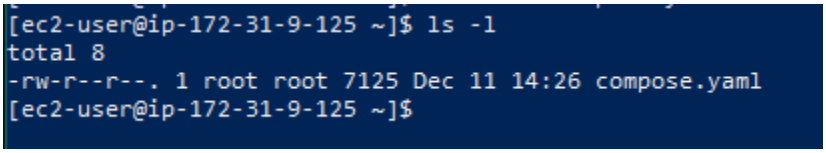


On Windows host, run SSH using the downloaded .pem (PowerShell/Git Bash/Windows Terminal):

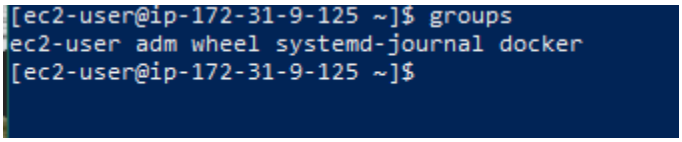


Run the install commands on the EC2 shell:

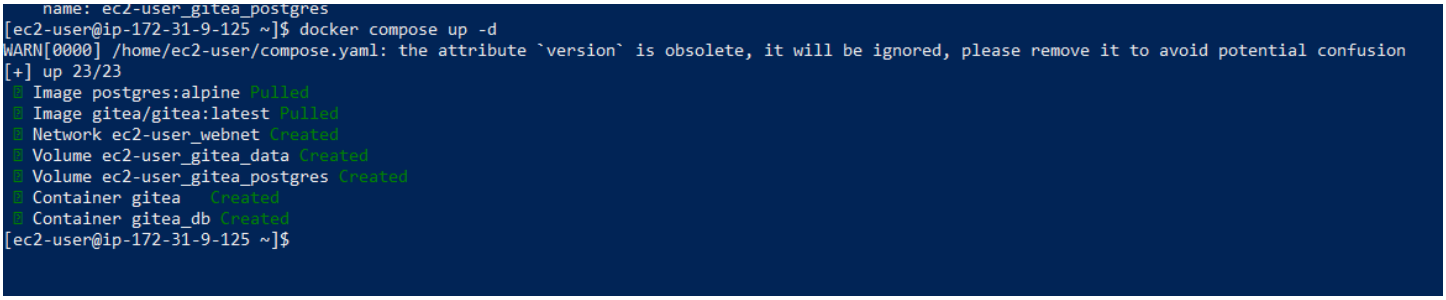
Verified Compose.yml:



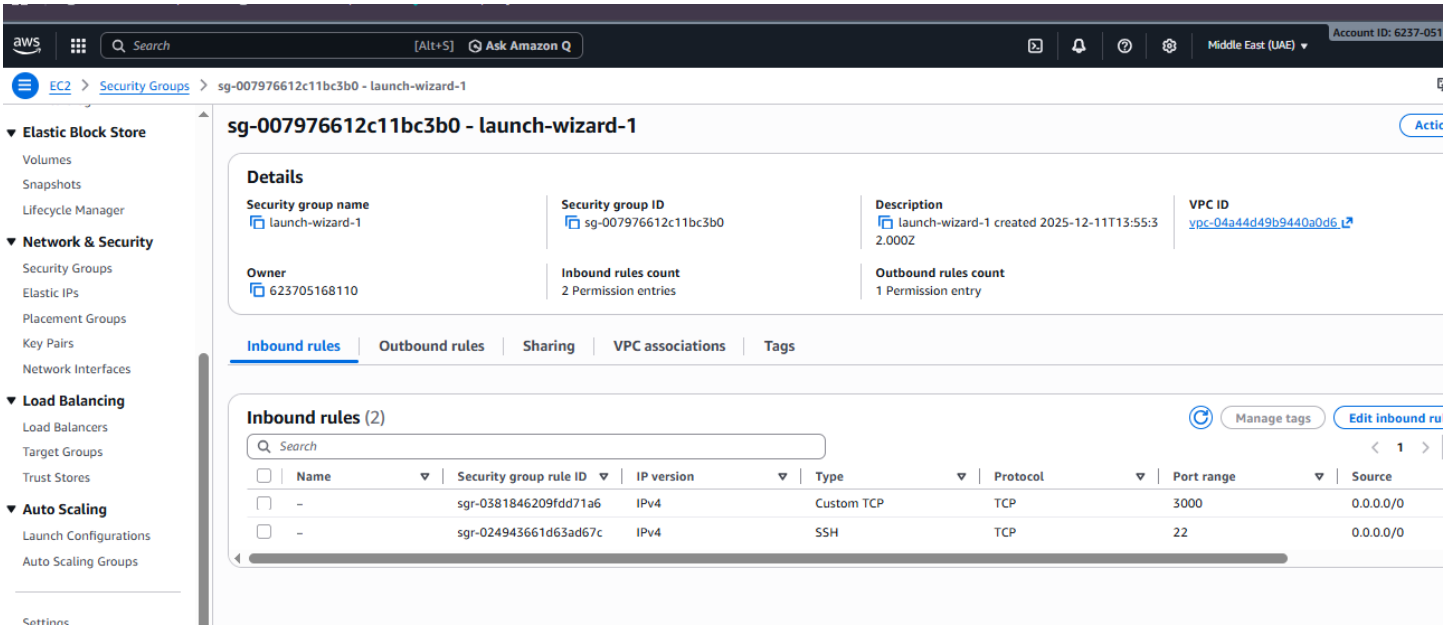
Add ec2-user to docker group, show groups before re-login, exit and reconnect, show groups after reconnect:



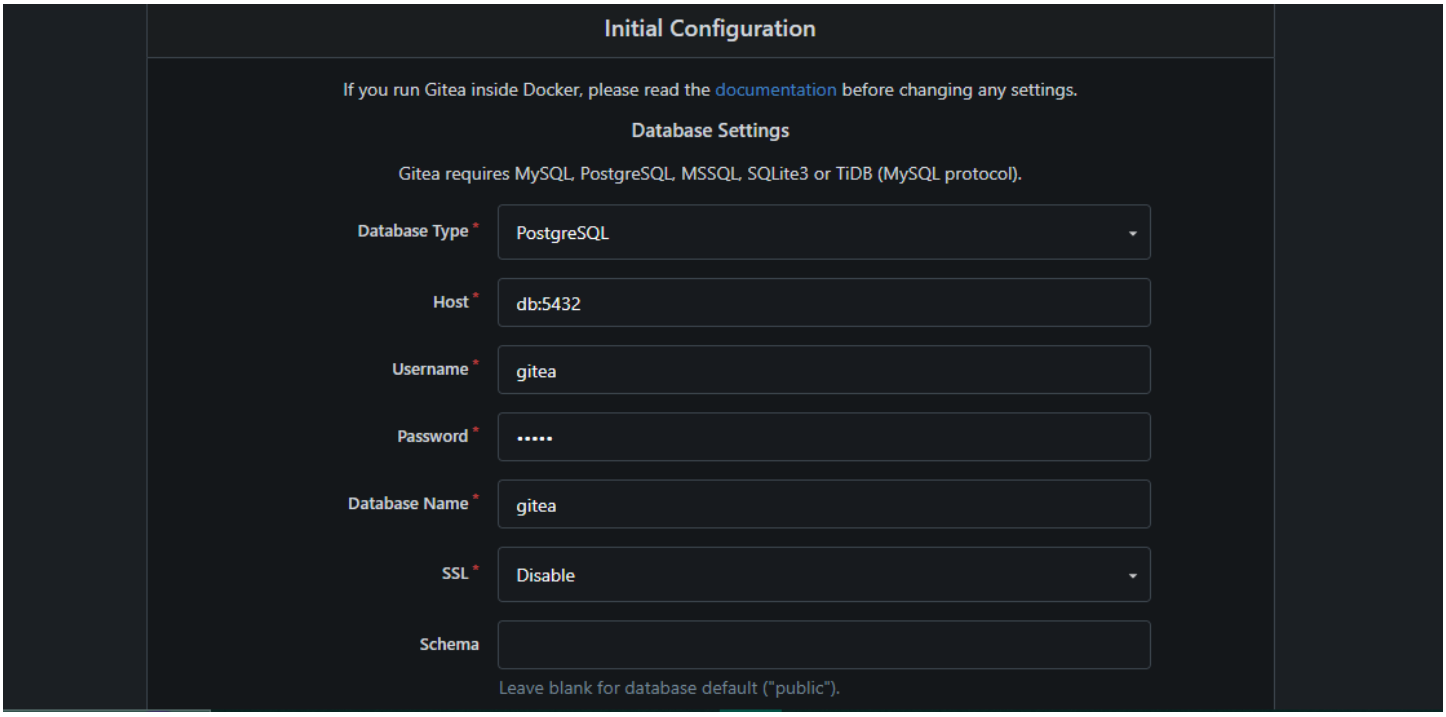
Run docker compose up -d from the directory with compose.yaml:



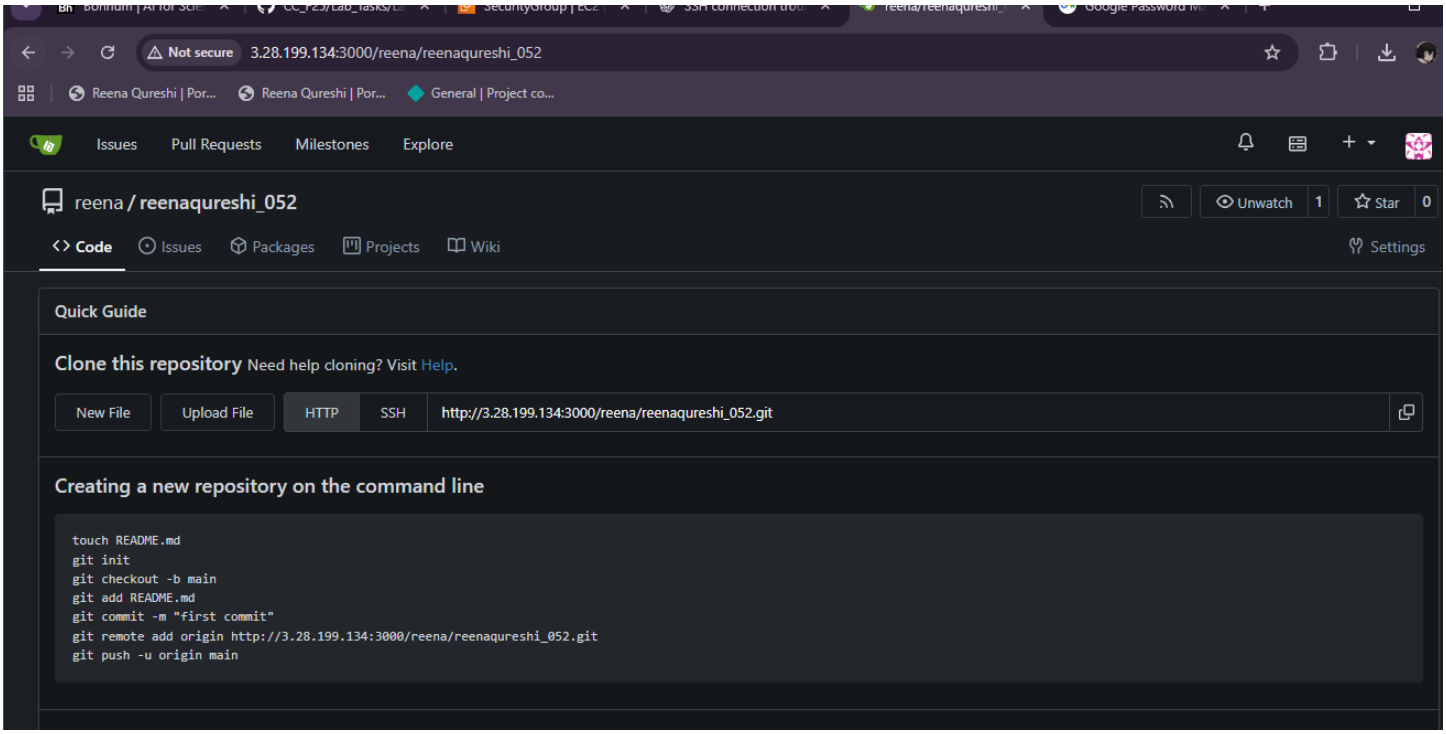
Edit the security group Lab8SecurityGroup inbound rules in the EC2 console: add Custom TCP rule port 3000 source 0.0.0.0/0 and save. Capture the inbound rules after saving



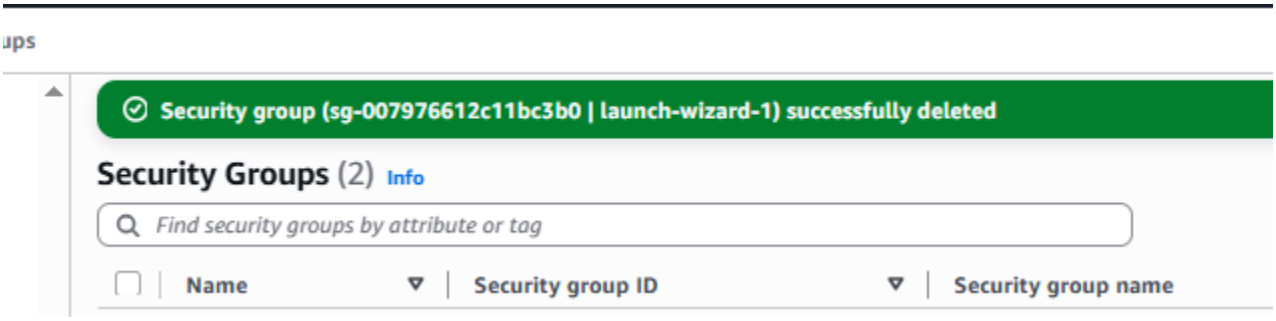
Open Gitea in your browser

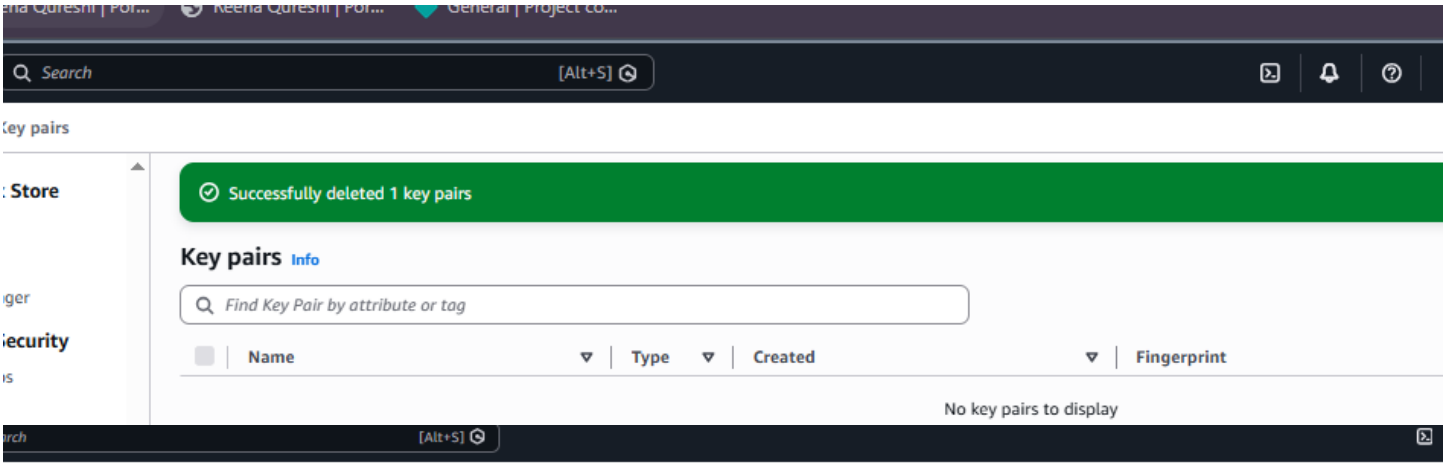


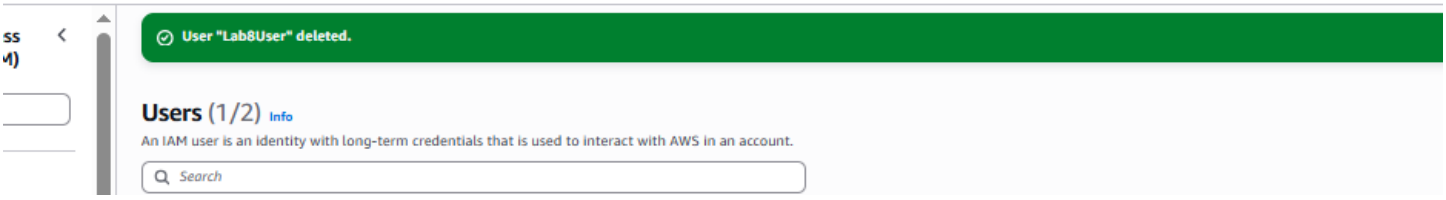
Complete initial Gitea setup (create admin user, create a repo) and capture Gitea showing the created repository

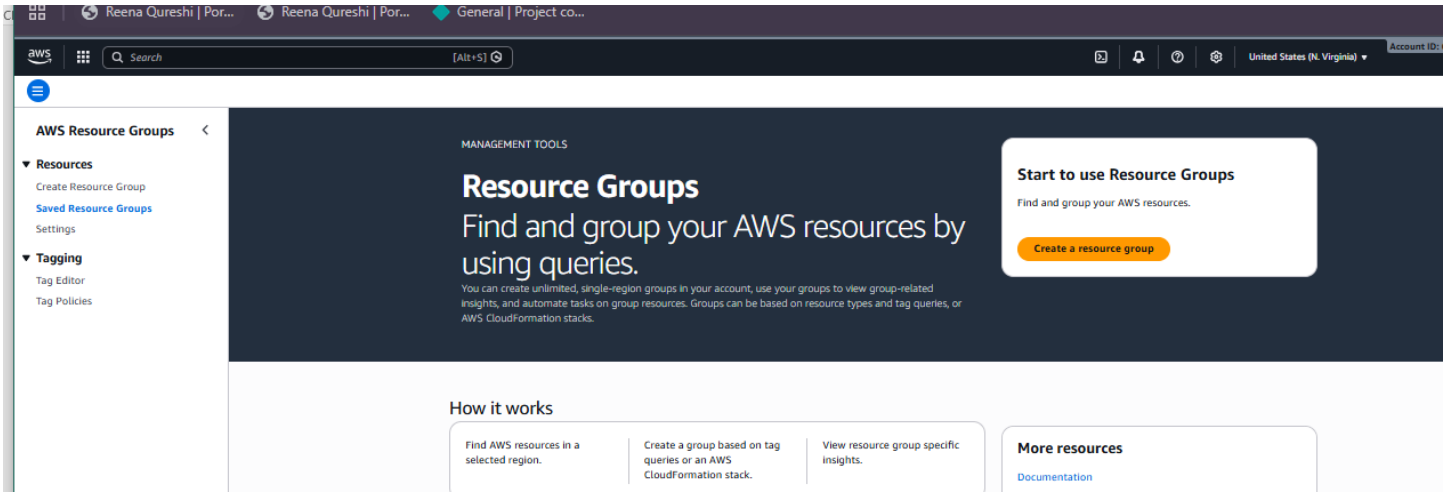


Cleanup — Remove resources to avoid charges




Search
[Alt+S]
Key pairs
Store
Successfully deleted 1 key pairs
Key pairs Info
Find Key Pair by attribute or tag
Name
Type
Created
Fingerprint
No key pairs to display


User "Lab8User" deleted.
Users (1/2) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.
Search


Reena Qureshi | Por...
Reena Qureshi | Por...
General | Project co...
Search
[Alt+S]
United States (N. Virginia)
AWS Resource Groups
Resources
Create Resource Group
Saved Resource Groups
Settings
Tagging
Tag Editor
Tag Policies
MANAGEMENT TOOLS
Resource Groups
Find and group your AWS resources by using queries.
You can create unlimited, single-region groups in your account, use your groups to view group-related insights, and automate tasks on group resources. Groups can be based on resource types and tag queries, or AWS CloudFormation stacks.
Start to use Resource Groups
Find and group your AWS resources.
Create a resource group
How it works
Find AWS resources in a selected region.
Create a group based on tag queries or an AWS CloudFormation stack.
View resource group specific insights.
More resources
Documentation