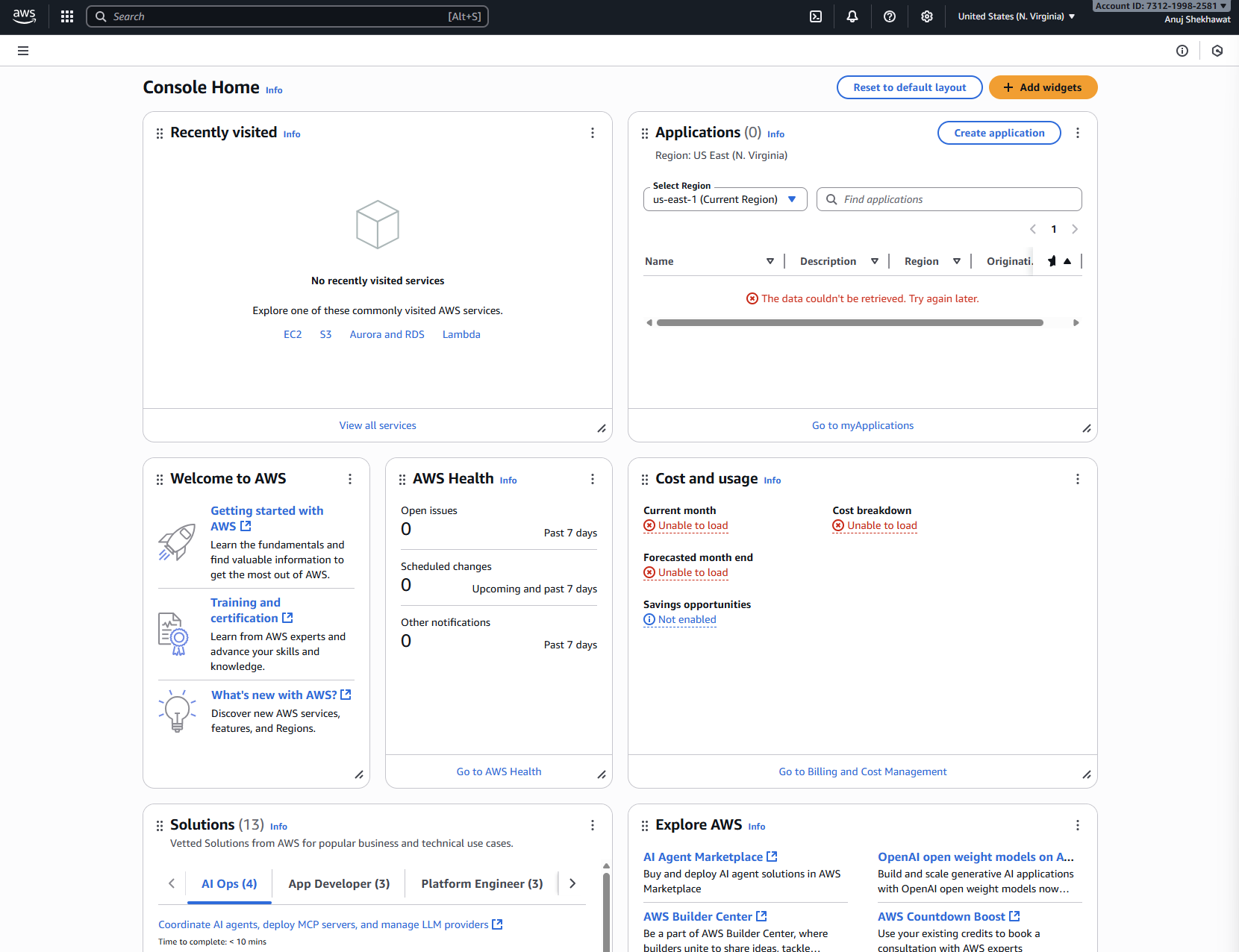
# Opensouce SOC

Architecture

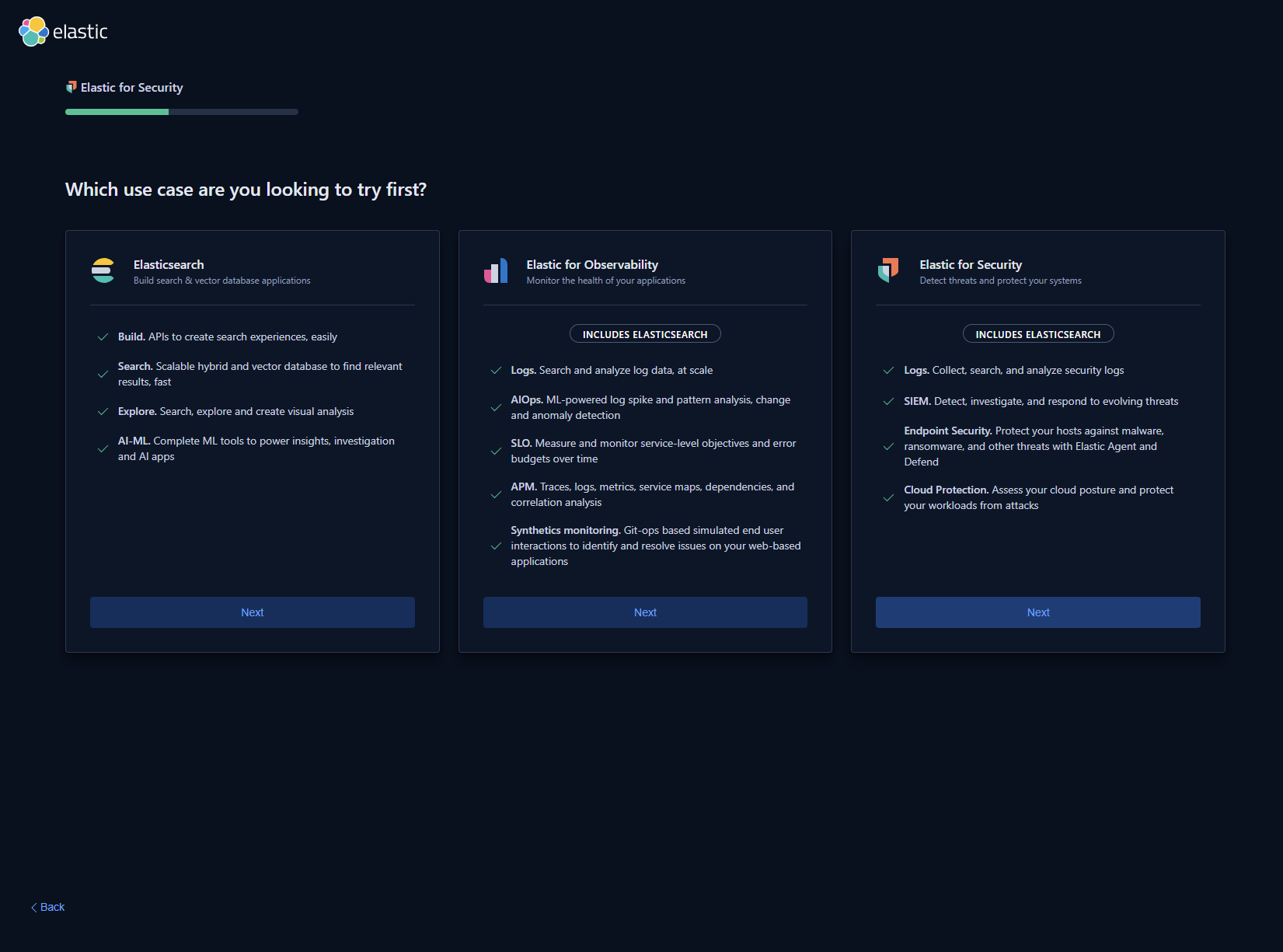
A diagram of a company

AI-generated content may be incorrect.

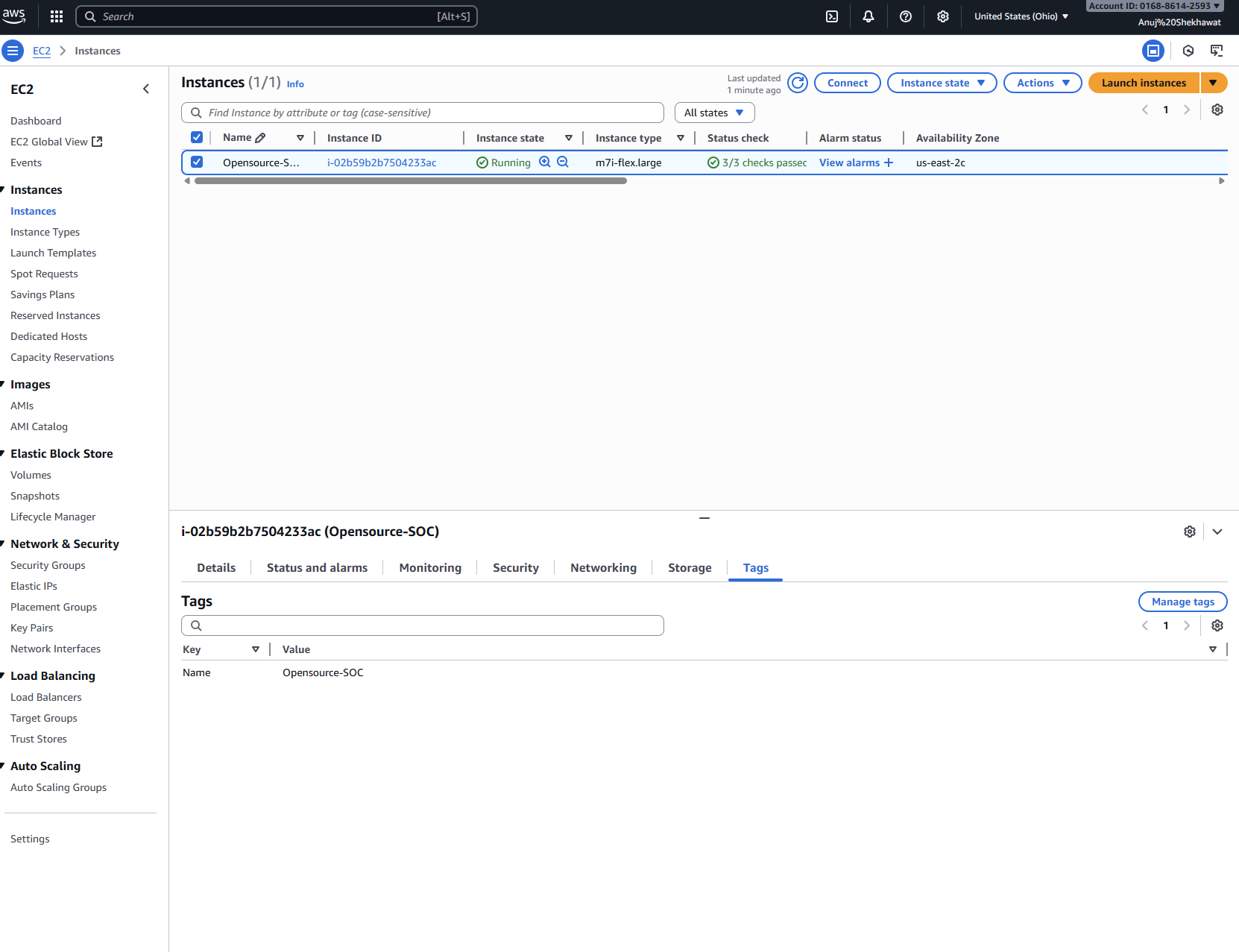
1. Platform Sign in



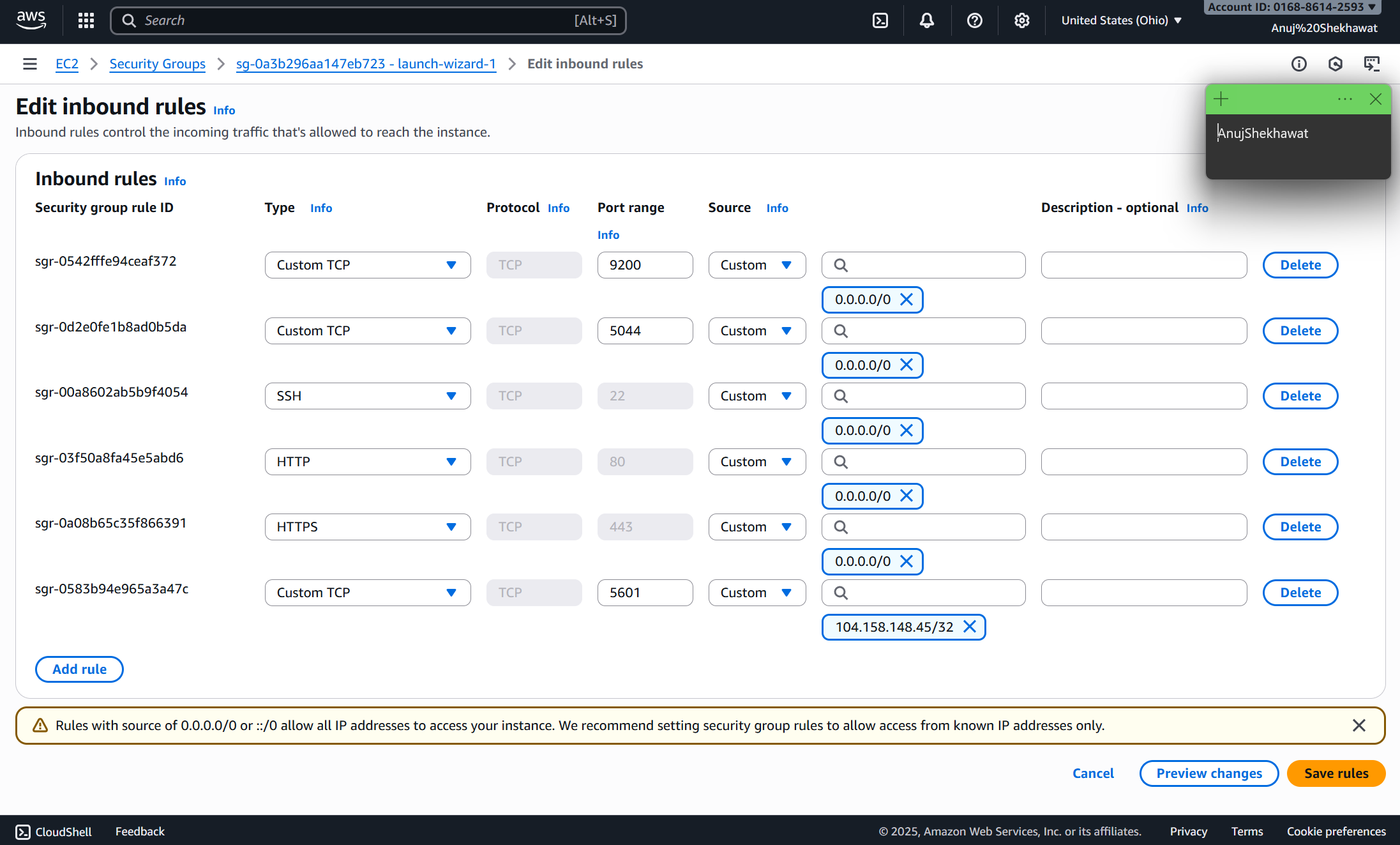
1. Elastic Setup



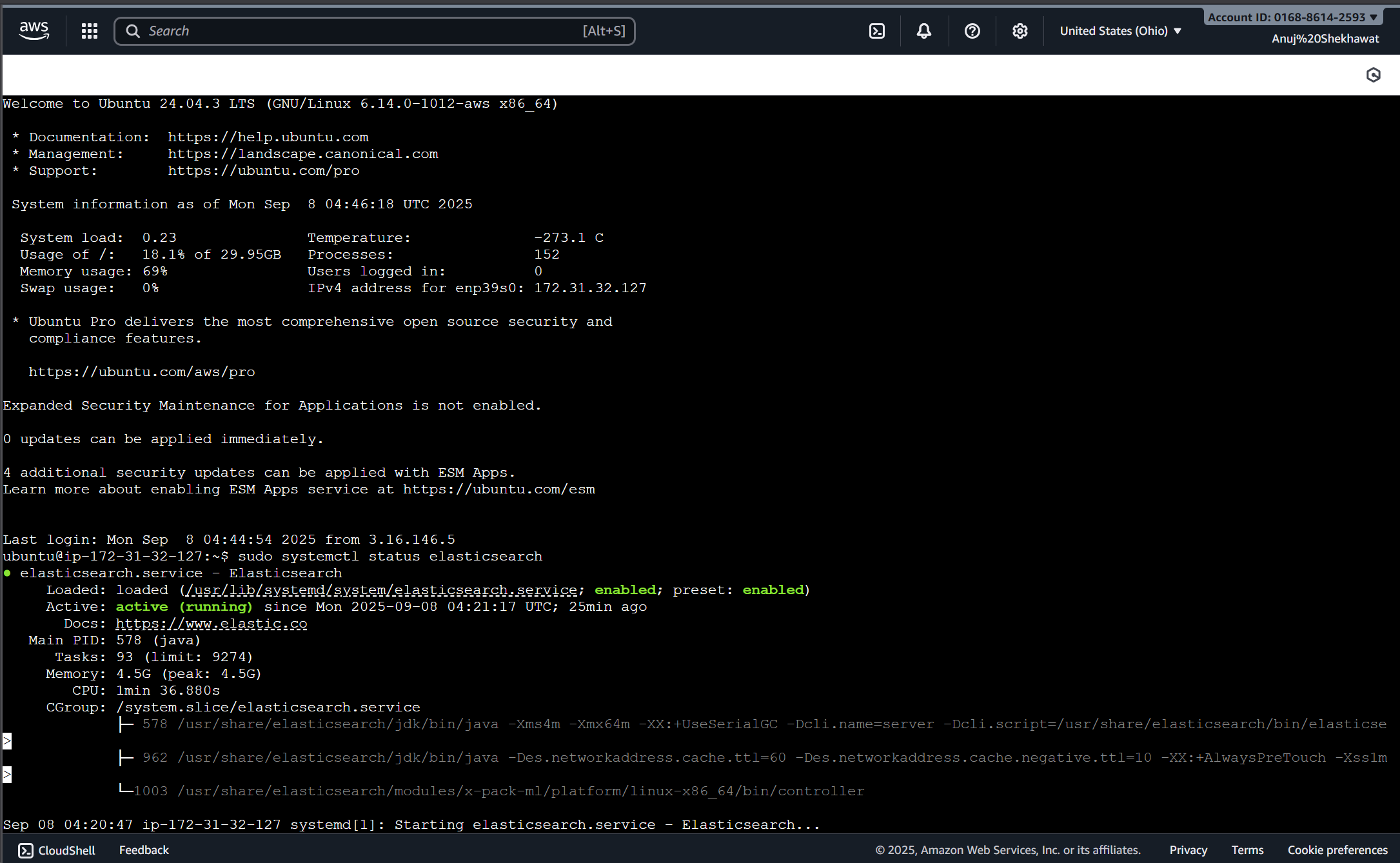
1. Vm Deployment in AWS

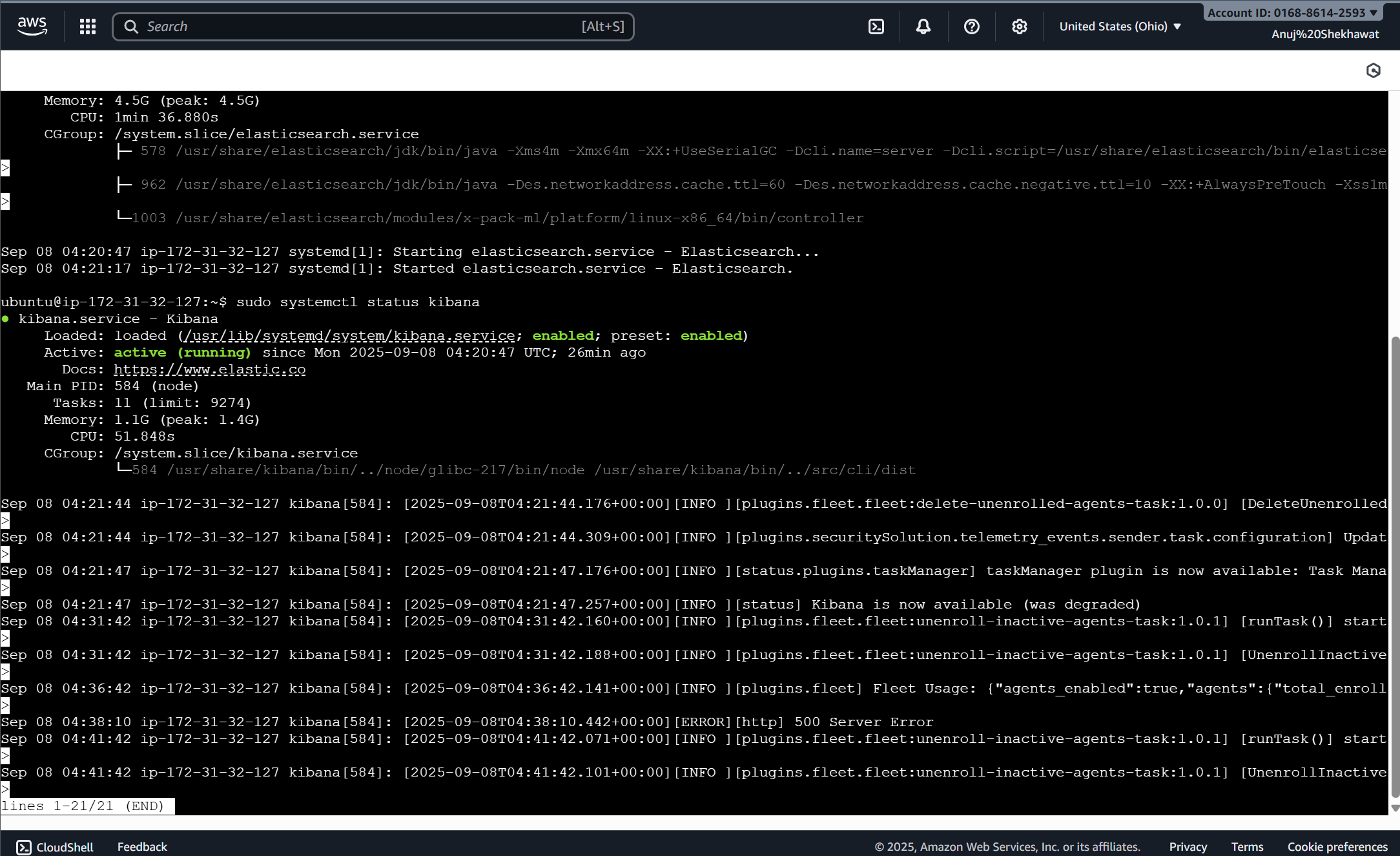


1. Implementation of Proper Inbound Rules According to the Project



1. Instllation of Elastic Search and Kibana in the ELK Virtual Machine





1. Starting up the web platform of Elastic cloud to configure SIEM ie ingest logs and finetune rules

## SIEM Configuration and Rules Fine Tuning

### Authentication Activity Dashboard

**Goal**: See failed logins, brute force attempts, top users failing.

1. **Ingest logs** (Windows Event logs, Linux auth logs, or sample Elastic data like logs-\* index).
2. Go to **Kibana → Visualize Library → Create visualization**.
3. Choose **Bar chart**:
   * X-axis → user.name (keyword).
   * Y-axis → Count of events.
   * Filter: event.action: "logon\_failure".  
     → Shows **top users with failed logins**.
4. Create a **line chart**:
   * X-axis: @timestamp (date histogram).
   * Y-axis: Count.
   * Filter: event.action: "logon\_success".  
     → Shows login trends.
5. Save them to a **“Authentication Monitoring” dashboard**.