Day 08 – Cloud Server Setup: Docker, Nginx & Web Deployment

Objective:

Deploy a real web server on a cloud VM and practice essential DevOps tasks such as:

Cloud provisioning, SSH access, Installing and managing services,

Configuring security rules, Extracting and backing up logs.

Cloud Environment:

Cloud Provider: AWS EC2

OS: Ubuntu

Instance Type: t2.micro

Region: ap-southeast-2

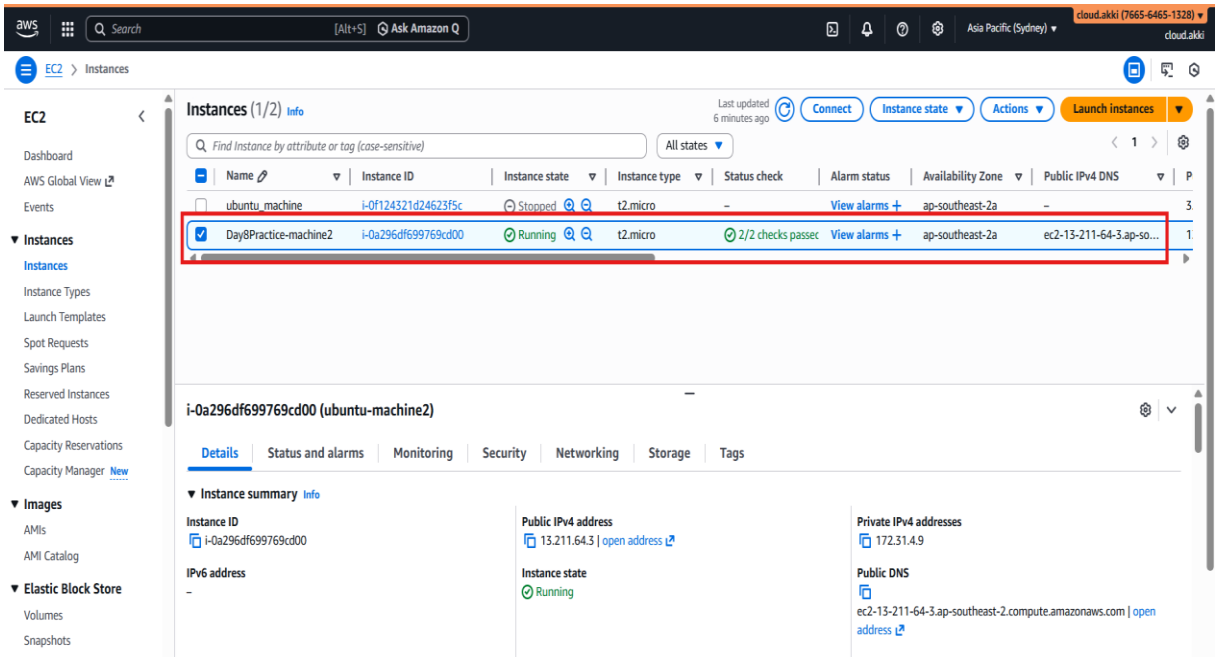
Web Server: Nginx

Container Engine: Docker

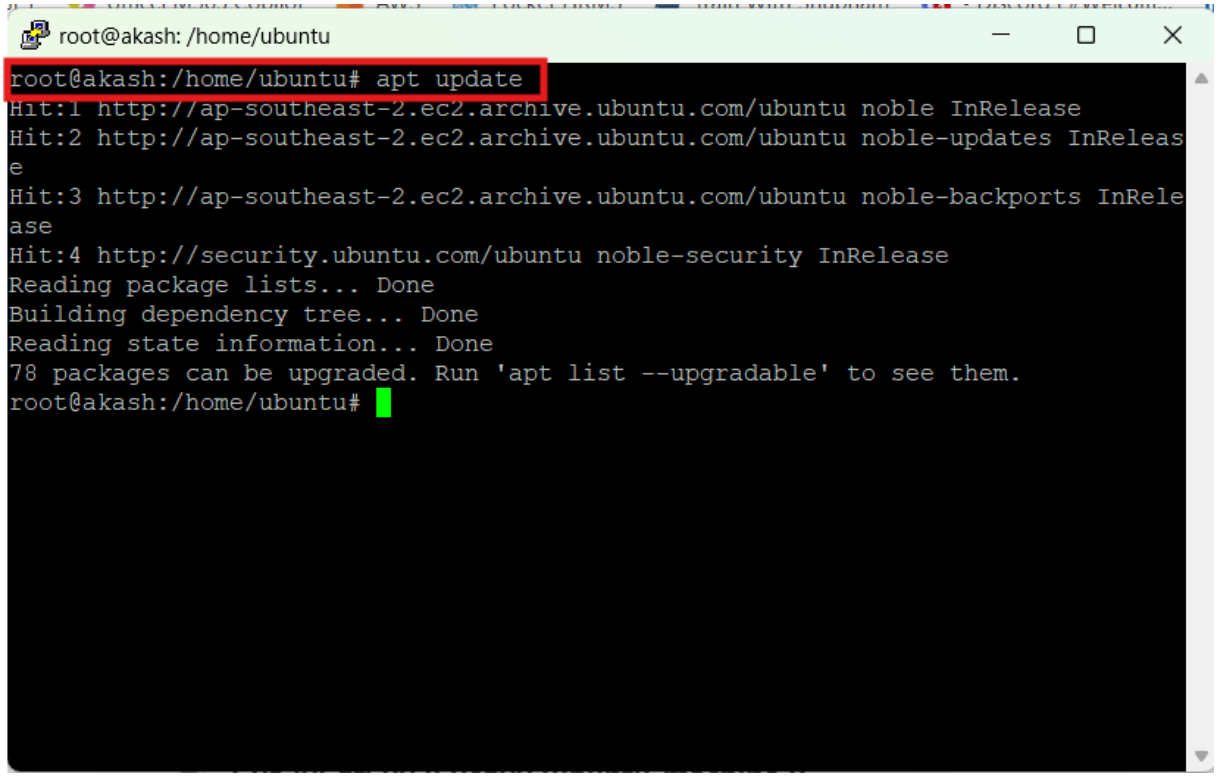
Lab Tasks Performed:

1- Launch EC2 Instance & SSH Access

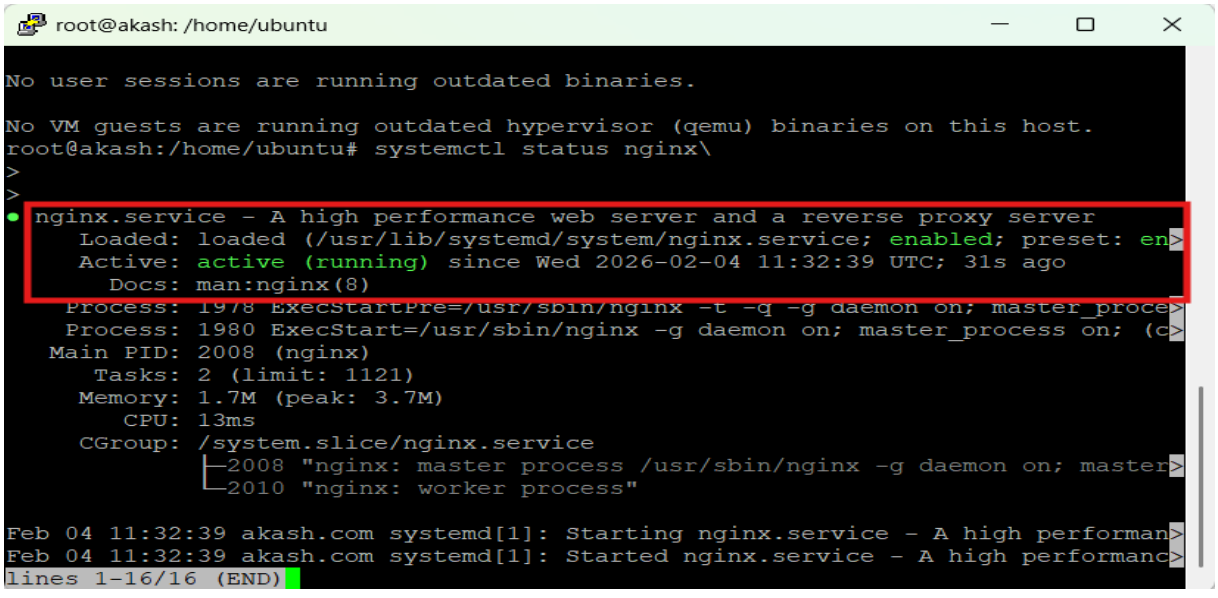
Created EC2 instance and connected using SSH.



2- connected using SSH and system update



3-Install Nginx



#sudo apt update

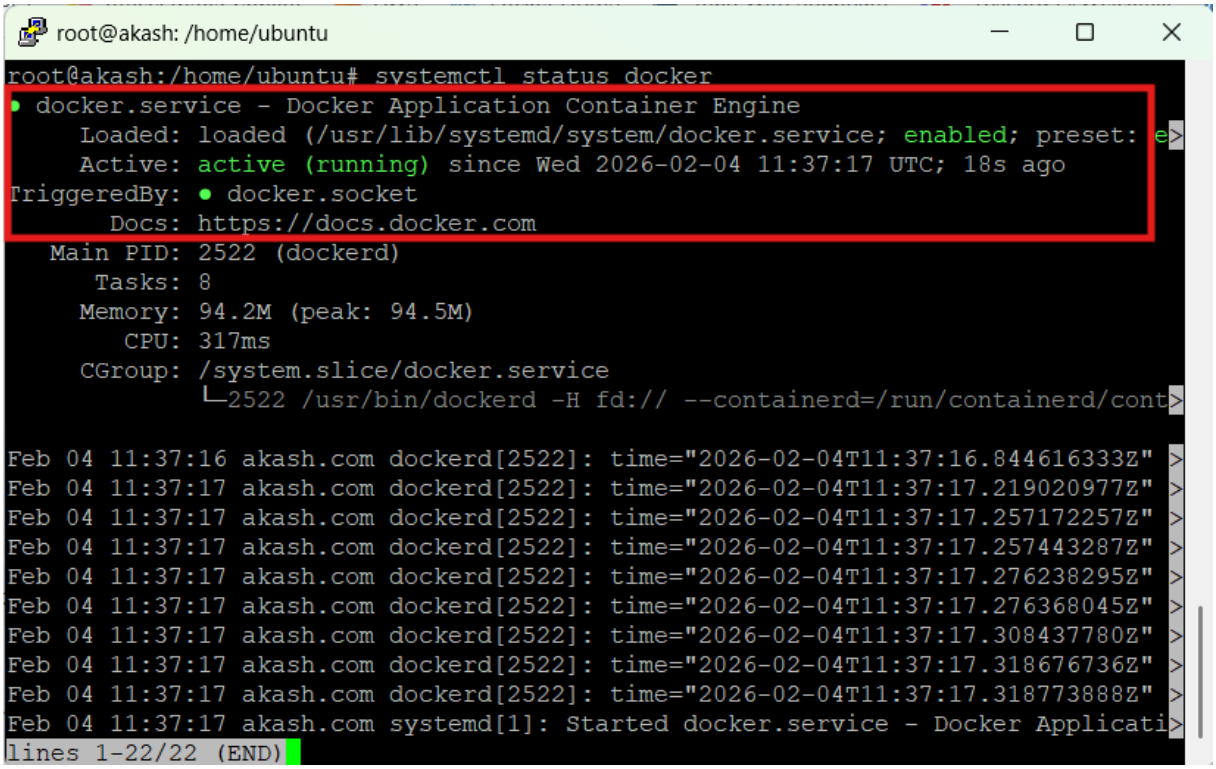
#sudo apt install nginx -y

#sudo systemctl start nginx

#sudo systemctl enable nginx

#sudo systemctl status nginx

4-Install Docker



#sudo apt install docker.io -y

#sudo systemctl start docker

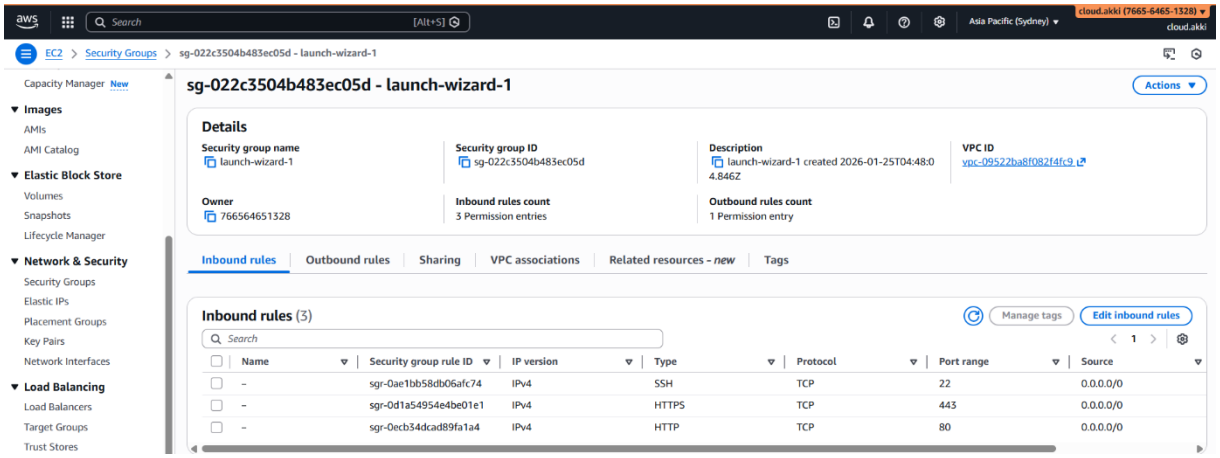
#sudo systemctl enable docker

#sudo systemctl status docker

5-Configure SecurityGroup

Inbound rule added:

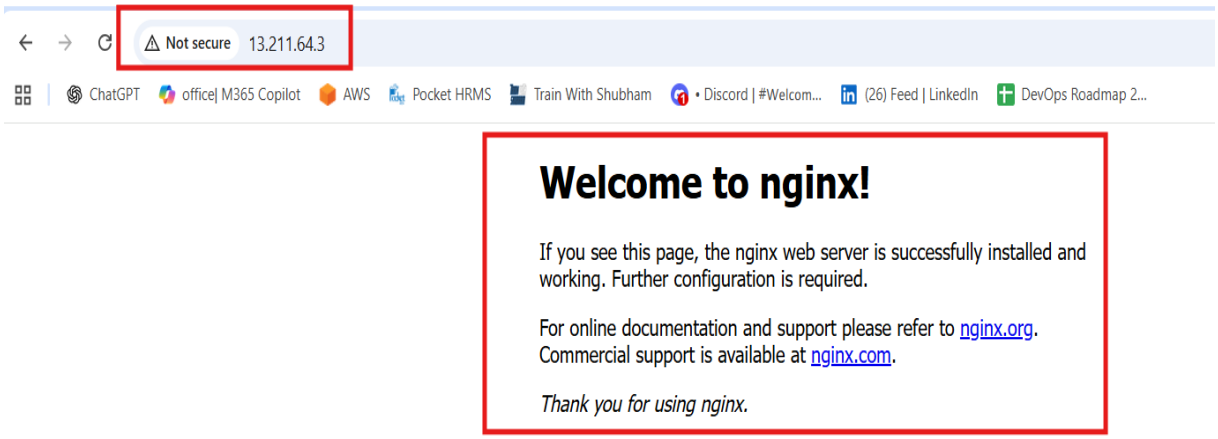
HTTP – Port 80
HTTPS– Port 443
SSH – Port 22



Verify Web Access

Accessed Nginx using public IP:

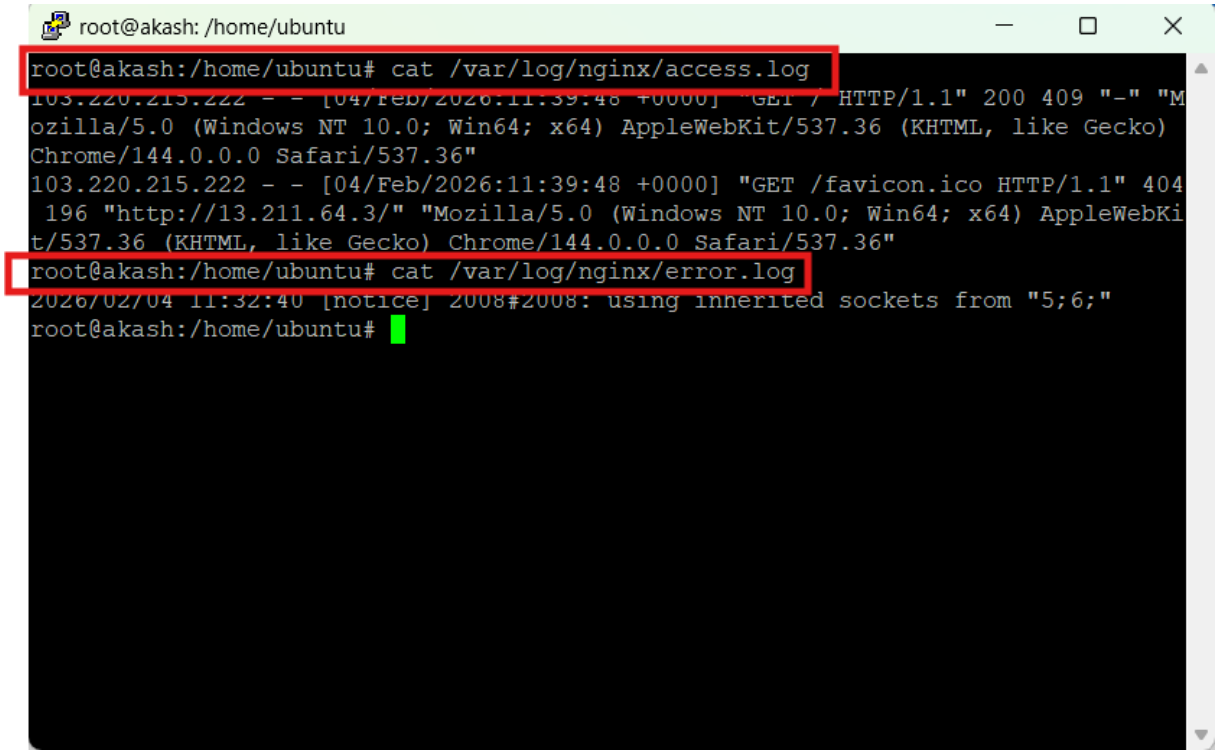
http://13.211.64.3



Extract Nginx Logs

#cat /var/log/nginx/access.log

#cat /var/log/nginx/error.log

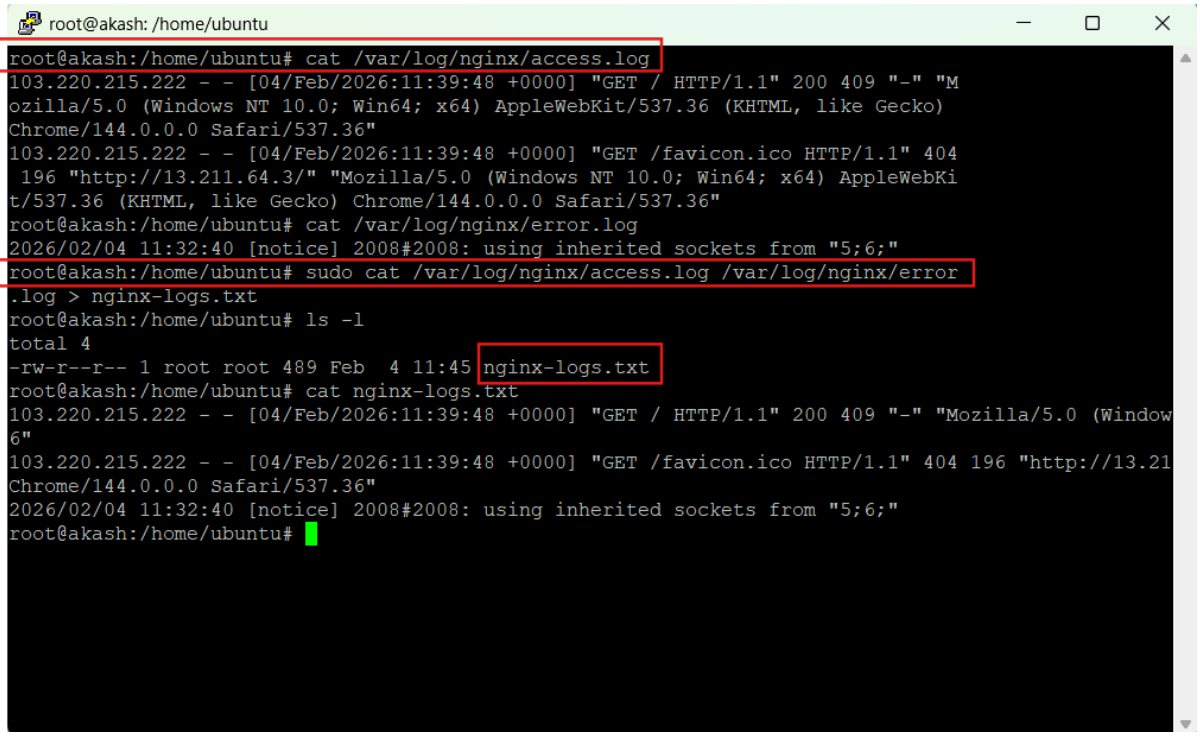


Save Logs to File

#sudo cat /var/log/nginx/access.log /var/log/nginx/error.log > nginx-logs.txt

#ls -l

#Scat nginx-logs.txt



Commands Used (Summary):

sudo apt update

sudo apt install nginx -y

sudo systemctl start nginx

sudo systemctl enable nginx

sudo systemctl status nginx

sudo apt install docker.io -y

sudo systemctl start docker

sudo systemctl enable docker

sudo systemctl status docker

cat /var/log/nginx/access.log

cat /var/log/nginx/error.log

sudo cat /var/log/nginx/access.log /var/log/nginx/error.log > nginx-logs.txt

Challenges Faced:

Website not accessible – Allowed port 80 in AWS Security Group

Permission denied on logs – Used sudo

Service persistence – Enabled services using systemctl enable