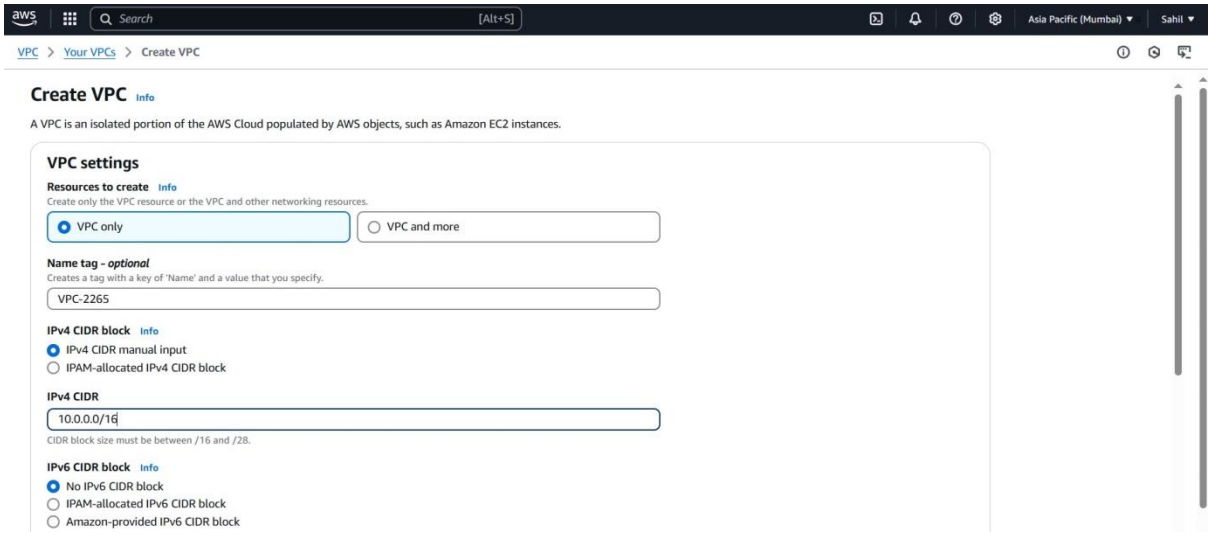
School of Computer Science, Engineering and Applications (SCSEA)
B. Tech TY (CCSA)
Subject: Cloud Architecture And Protocol

Name of the Student: Sahil S. Mandawgade PRN: 20220802265

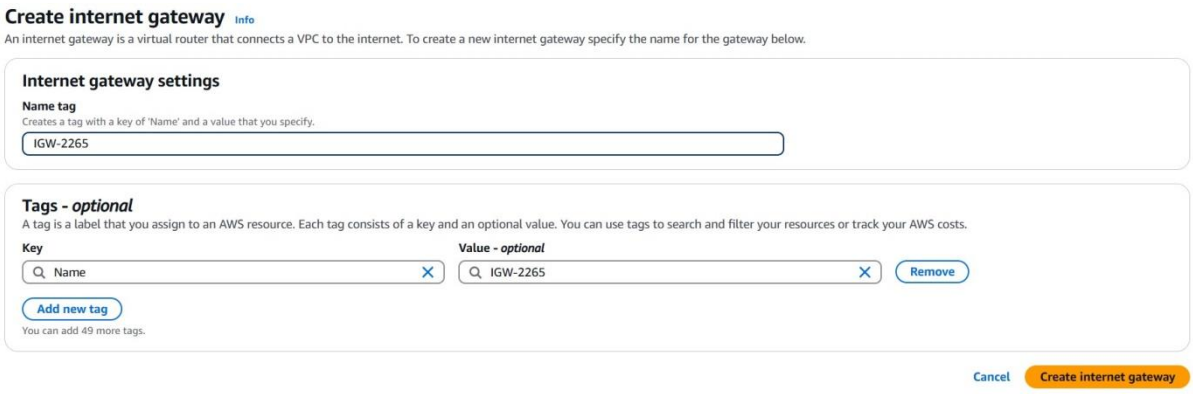
Title of Practical: 3. Architecting VPC Flow Logs for efficient network monitoring in AWS.

Step 1: Create a VPC and connect Internet Gateway to it.

- Go to AWS console and search for VPC.
- Create VPC by selecting 'VPC Only' with valid name.
- Set IPv4 CIDR range as '10.0.0.0/16'.



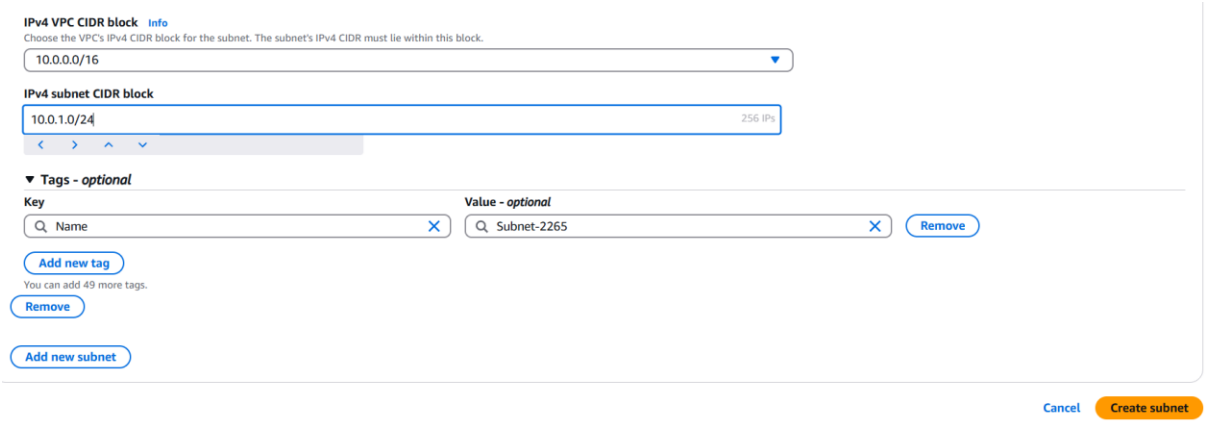
- Go to Internet Gateway.
- Create an Internet Gateway.



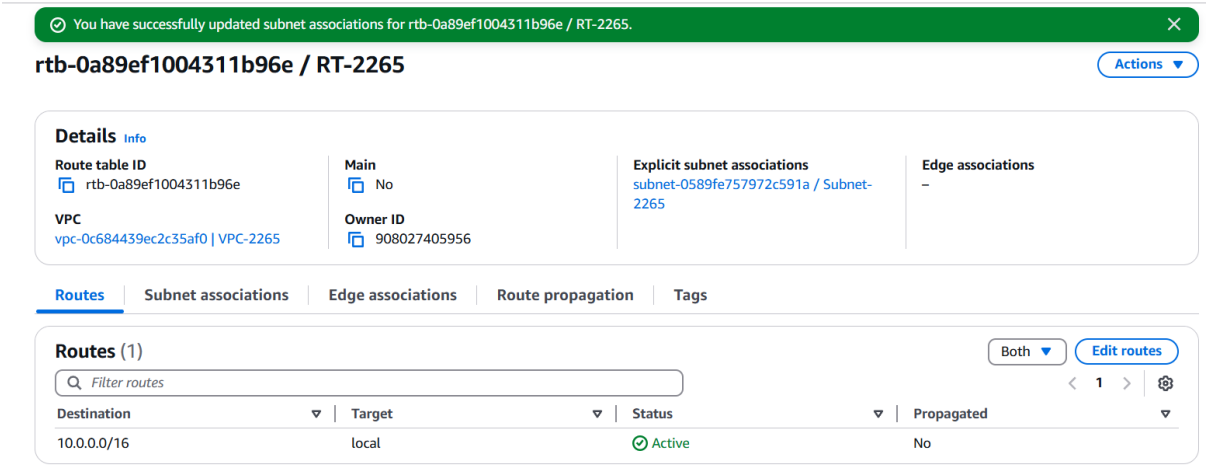
- Attach the IGW to the VPC.

Step 2: Create a Subnet and Route Table.

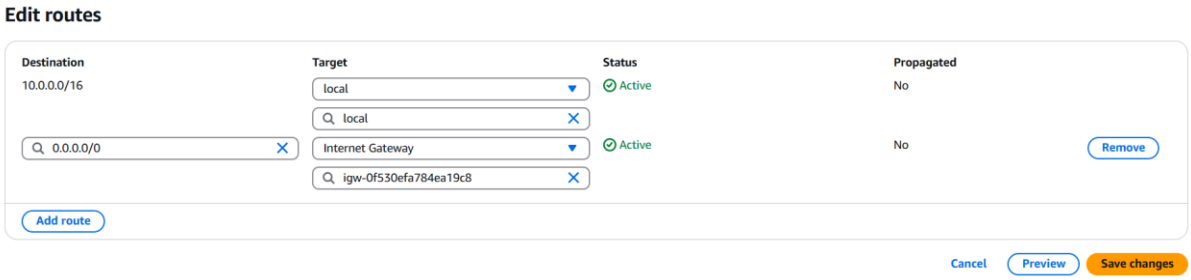
- Create a Subnet.
- Enter IPV4 subnet CIDR block as “10.0.1.0/24”, then click on “Create subnet”.



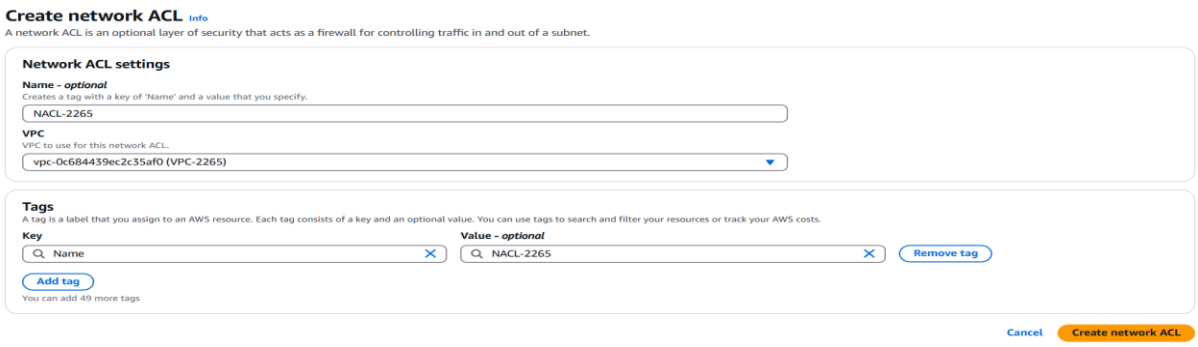
- Create a Route Table and select the VPC we created.
- Associate the Subnet to the Route Table.



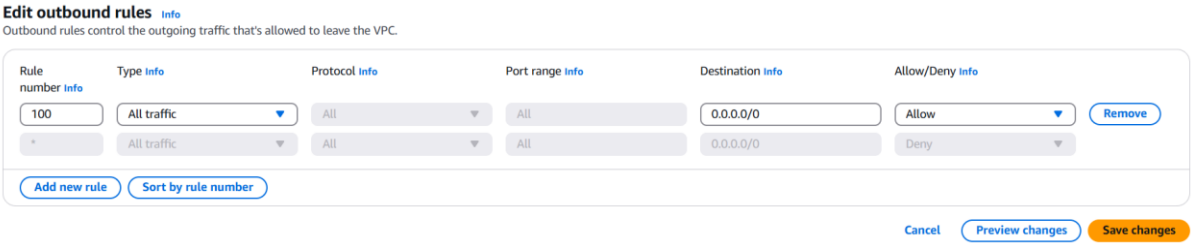
- Add a Route with Destination as '0.0.0.0./0' and Target as 'Internet Gateway' and select the internet gateway we created i.e. 'IGW-2265'.



Step 3: Create a NACL and attach the VPC.

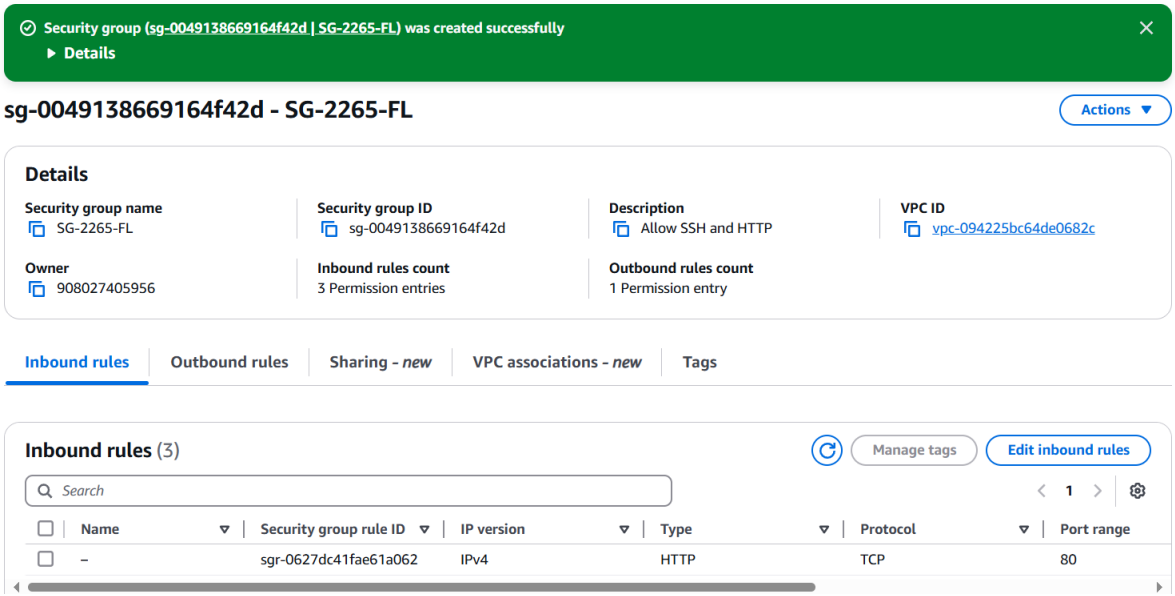


- Edit the subnet association and select the subnet 'Subnet-2265'.
- Add Inbound and Outbound rules both with Rule number as '100' and Type as 'All Traffic'.



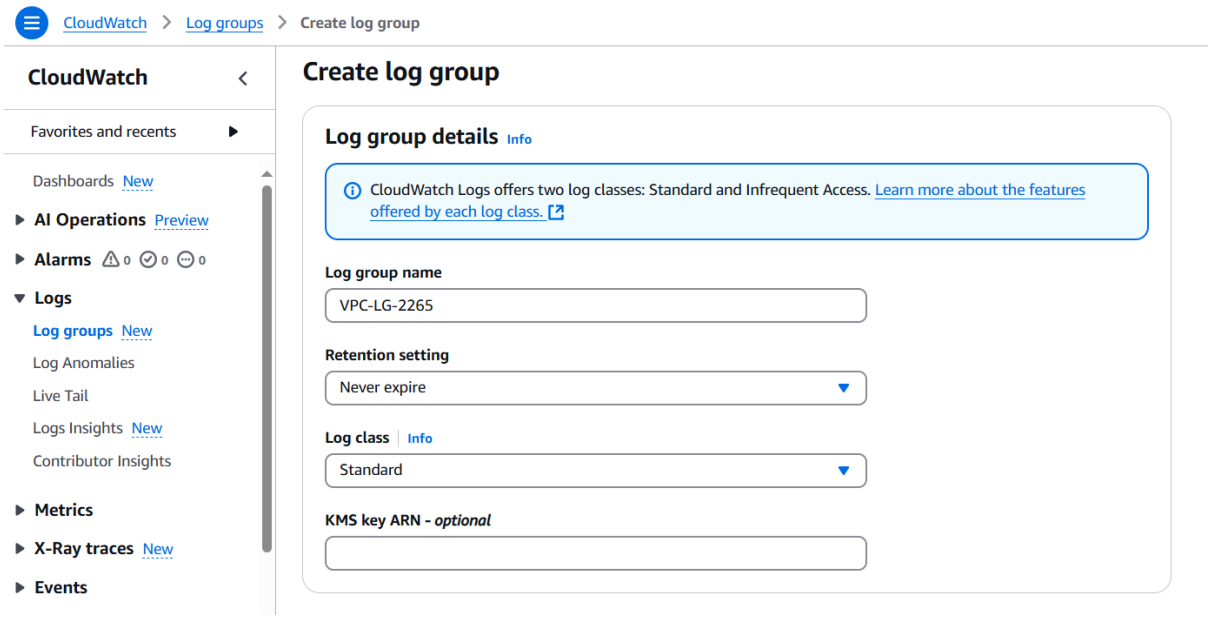
Step 4: Create a Security Group in EC2 Console.

- Create a Security Group with name 'SG-2265-FL'.
- Set Inbound Rules : SSH – Anywhere IPv4, HTTP – Anywhere IPv4 and HTTPS – Anywhere IPv4.
- Set Description and Click on Create.



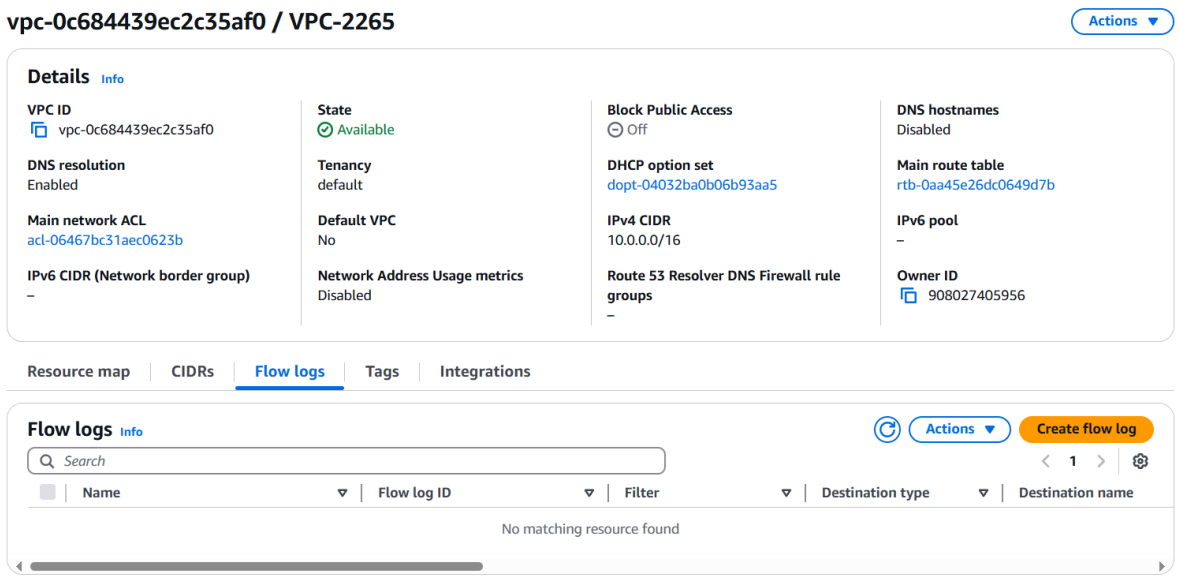
Step 5: Create Log Group in AWS CloudWatch.

- Go to CloudWatch console.
- Go to 'Logs' the 'Log Group's and click on 'Create log group'.
- Name the log group as 'VPC-LG-2265'.
- Keep the Retention setting as 'Never expire'.
- Keep Log class as 'Standard'.
- Click on Create.

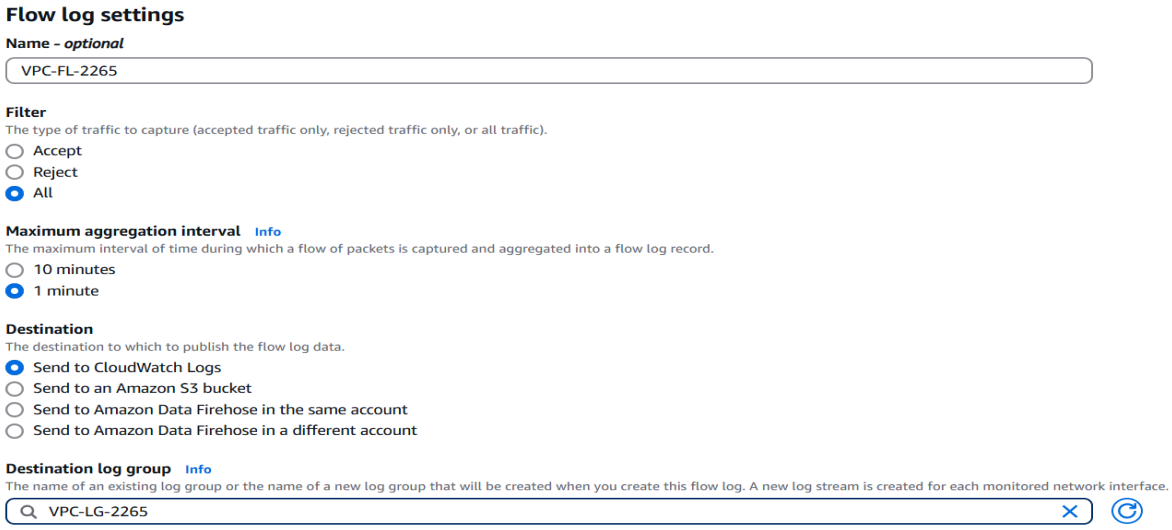


Step 6: Create a Flow Log.

- Go to VPC console.
- Select the VPC 'VPC-2265'.
- Select Flow logs.
- Click on 'Create flow log'.



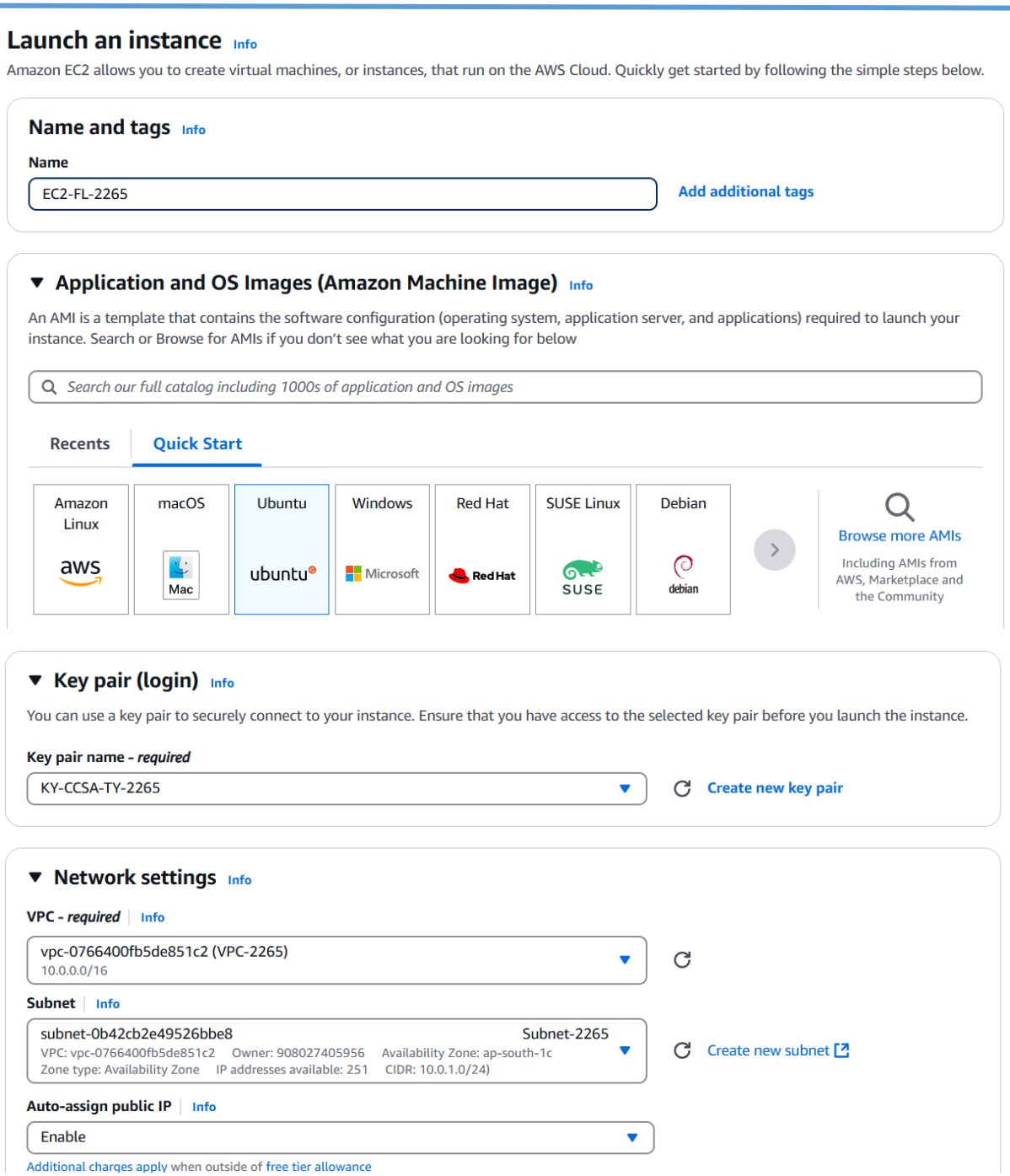
- Set Name of flow log as 'VPC-Fl-2265'.
- Keep Filter as 'All'.
- Set 'Maximum aggregation interval' as '1 minute'.
- Set 'Destination' as 'Send to CloudWatch Logs'.
- Select Destination log group as 'VPC-LG-2265'.



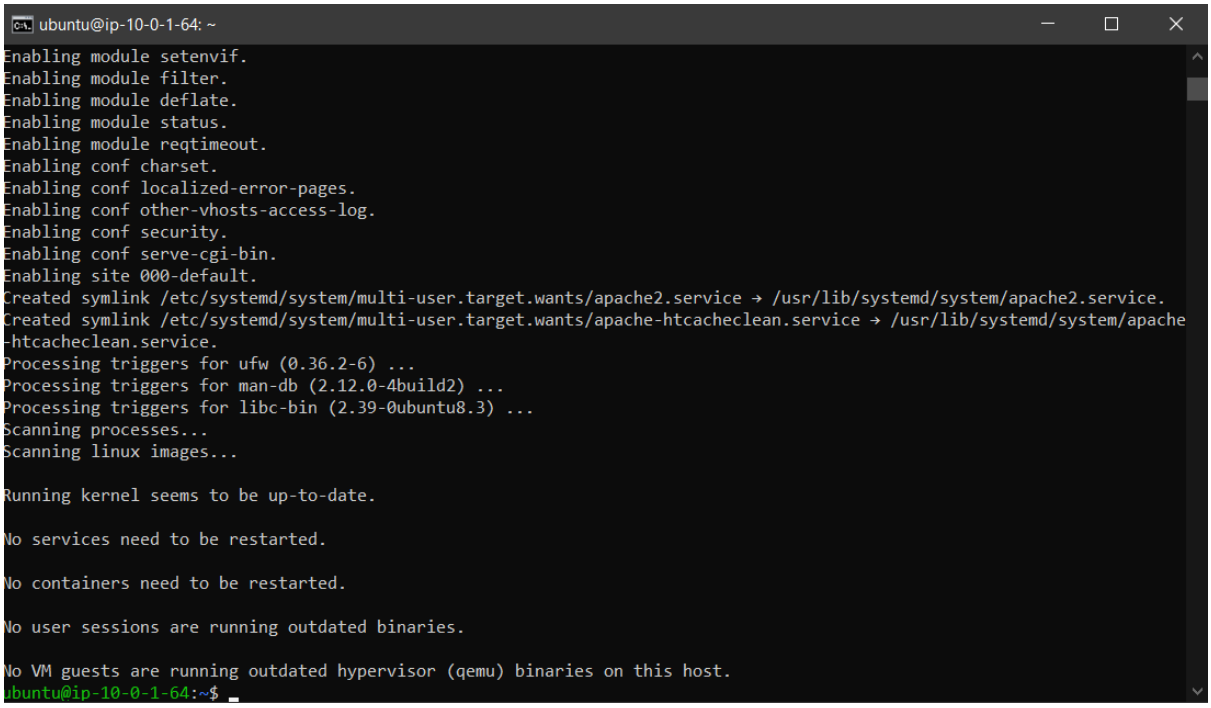
- Create a new Service role.
- Keep Log record format as 'AWS default format'.
- Click on 'Create flow log'.

Step 7: Launch an EC2.

- Set name of EC2 as 'EC2-FL-2265'.
- Select AMI as 'Ubuntu'.
- Select Instance type as 't3.micro'.
- Select Key pair.
- Change Network Settings.
- Select VPC and Subnet that we created.
- Set 'Auto-assign public IP' as 'Enable'.
- Select Security Group 'SG-2265' that we created earlier.
- Click on 'Launch instance'.

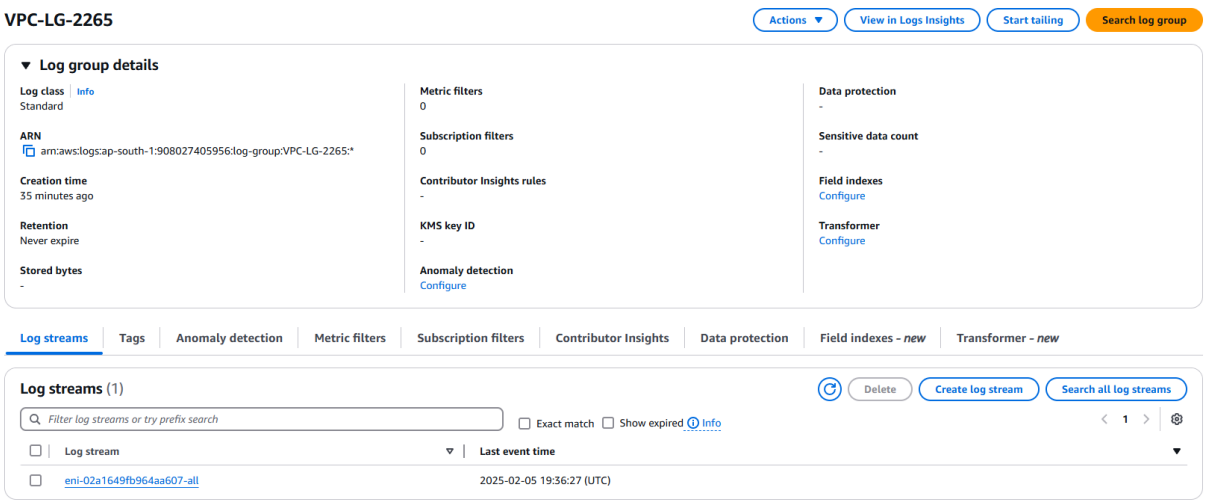

Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
EC2-FL-2265
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Debian
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
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
KY-CCSA-TY-2265
Create new key pair
Network settings Info
VPC - required Info
vpc-0766400fb5de851c2 (VPC-2265)
10.0.0.0/16
Subnet Info
subnet-0b42cb2e49526bbe8 Subnet-2265
VPC: vpc-0766400fb5de851c2 Owner: 908027405956 Availability Zone: ap-south-1c
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.1.0/24)
Create new subnet
Auto-assign public IP Info
Enable
Additional charges apply when outside of free tier allowance

- Now, Select the EC2 instance – Actions – Security – Modify IAM Roles – Create new role.
- Search and select VPCFlowLogs-CloudWatch.
- Select Trusted entity type as 'AWS Service' – Use Case as EC2 instance.
- In Permissions search and select 'AmazonVPCFullAccess'.
- Set name as 'VPC_FL_2265' and click on create.
- After creating and attaching role connect the instance on terminal and install apache on it.



Step 8: Check if the Flow Logs are generated in CloudWatch.

- Go to CloudWatch – Log Groups – VPC-LG-2265 – Log Streams.
- Click on the log stream.



- **Here we can see generated 'Log Events'.**