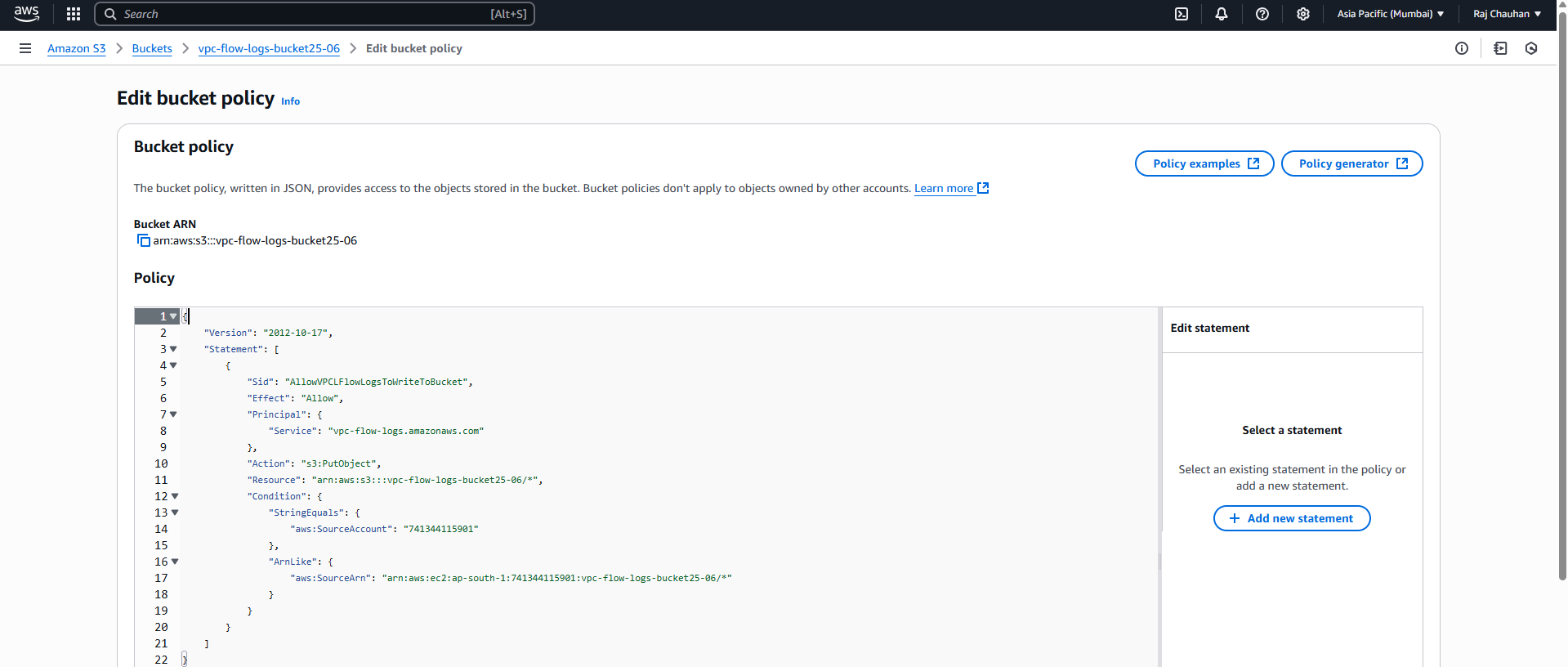
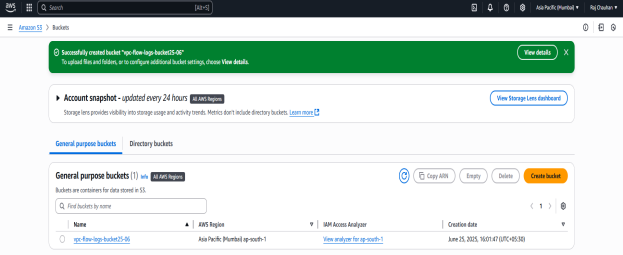
**Section 1: Create S3 Bucket**

Go to AWS S3 Console → Click Create bucket Set Bucket Policy:

Set Bucket name: vpc-flow-logs-bucket Go to Permissions tab → Bucket policy

Disable Block Public Access Paste the contents of s3/bucket-policy.json

Click Create bucket Click Save



**Section 2: Create IAM Role for VPC Flow Logs**

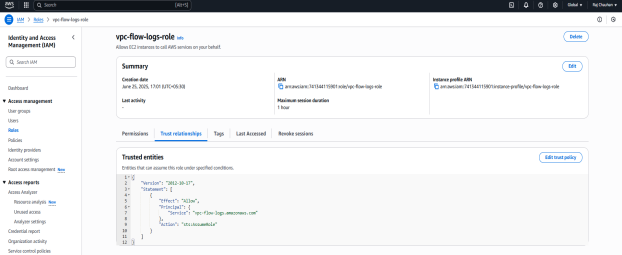
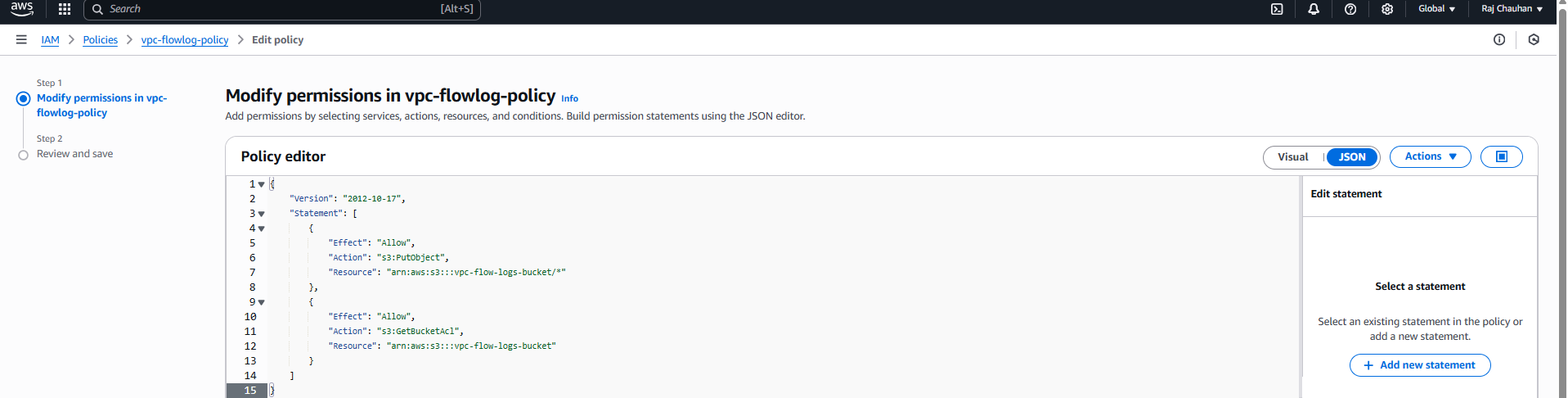
Open IAM Console → Roles → Create role Attach Permission Policy

Choose AWS Service → EC2 → Click Next Go to Policies → Create policy → Select JSON tab

Paste the trust policy from iam/role-trust-policy.json Paste the content of iam/vpc-flow-logs-s3-policy.json

Name the role: VPCFlowLogsToS3Role Name it VPCFlowLogsS3PutPolicy

Click Create role Create and attach this policy to VPCFlowLogsToS3Role



**Section 3: Create VPC & Enable VPC Flow Logs**

Open VPC Console → Click Create VPC → Choose VPC only SSH into your Ubuntu EC2 Instance

Enter → Name tag: MyAuditVPC → IPv4 CIDR block: 10.0.0.0/16 Install package manager.

Click Create VPC

Enable VPC Flow Logs

Select the created VPC → Click Actions → Create flow log

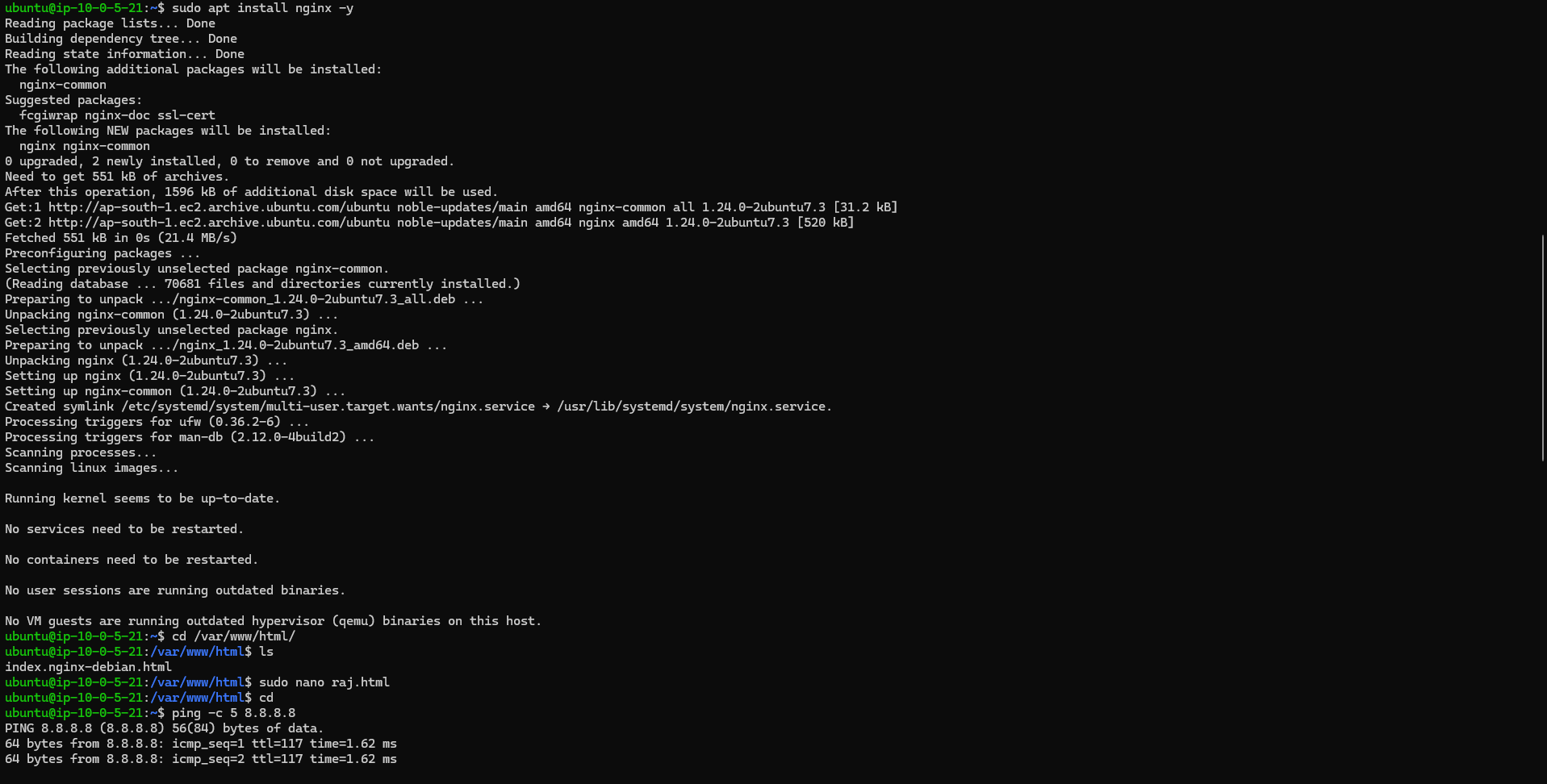
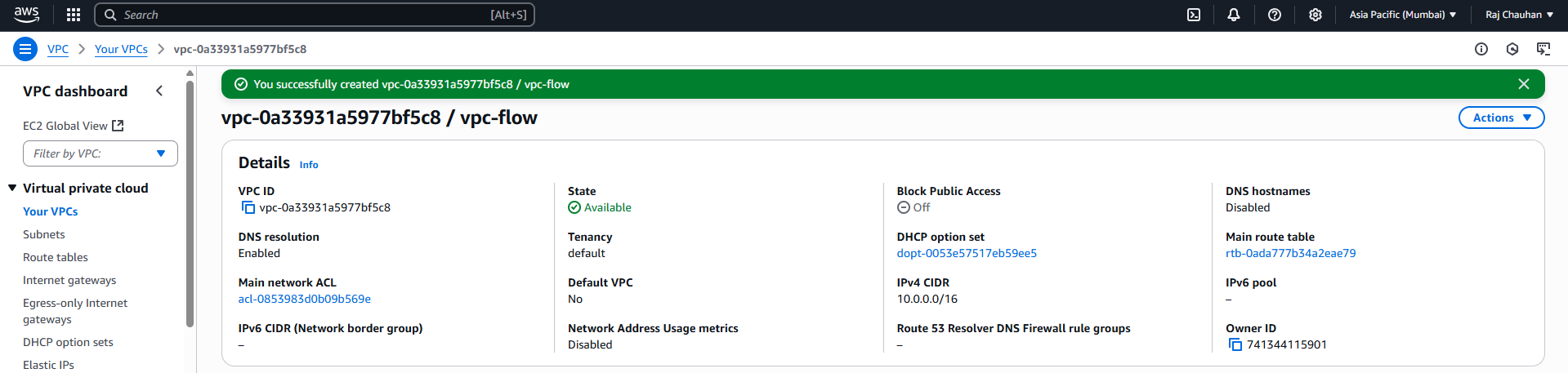
Configure the → Filter All (accepted and rejected)

Destination Send to an S3 bucket

Destination S3 ARN arn:aws:s3:::vpc-flow-logs-bucket

IAM Role VPCFlowLogsToS3Role

Click Create flow log



**Final Result**

