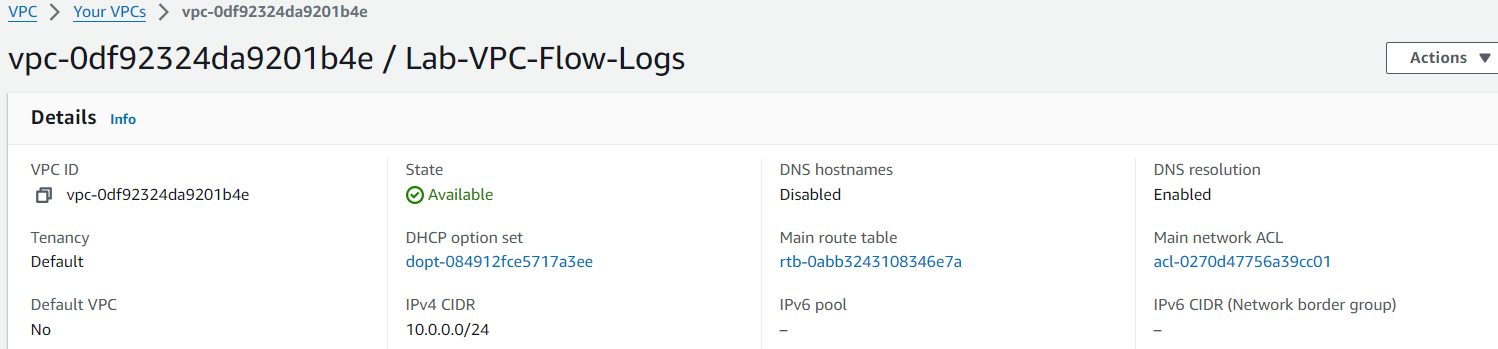
**Network Monitoring Solution Using AWS VPC Flow Logs and CloudWatch**

**Resources to create:** VPC only

**Name-tag:** Lab-VPC-Flow-Logs

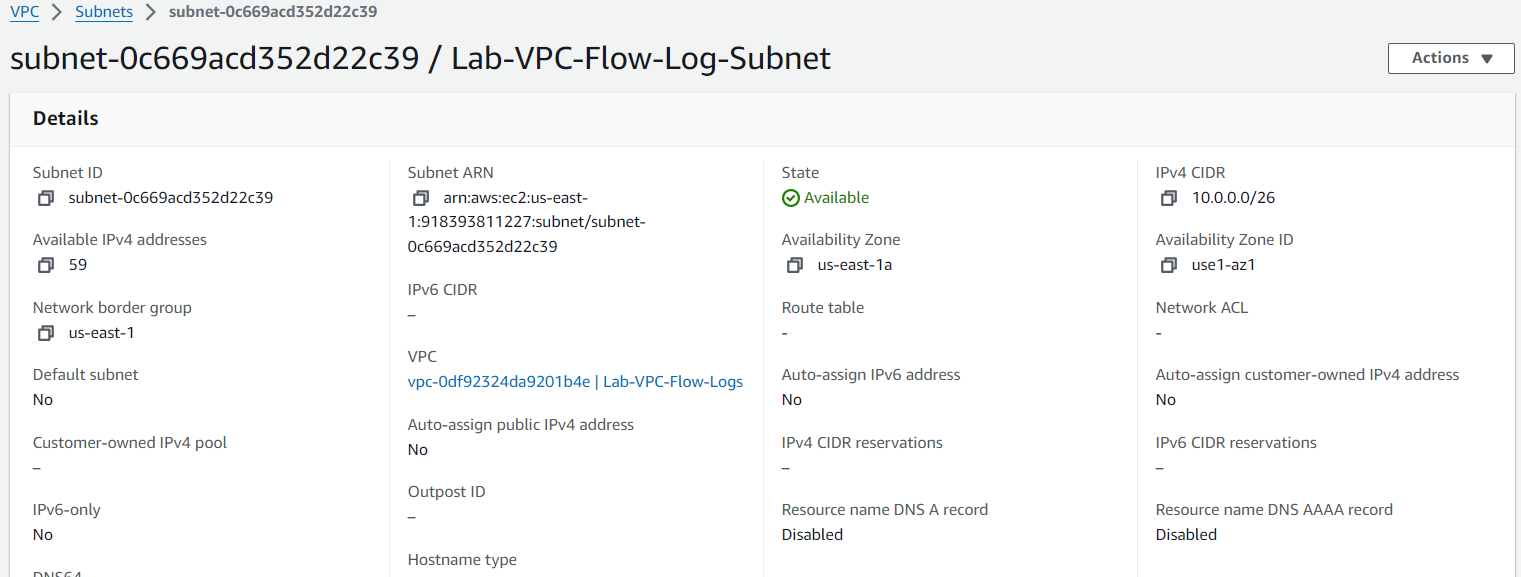
**IPv4 CIDR Block:** 10.0.0.0/24



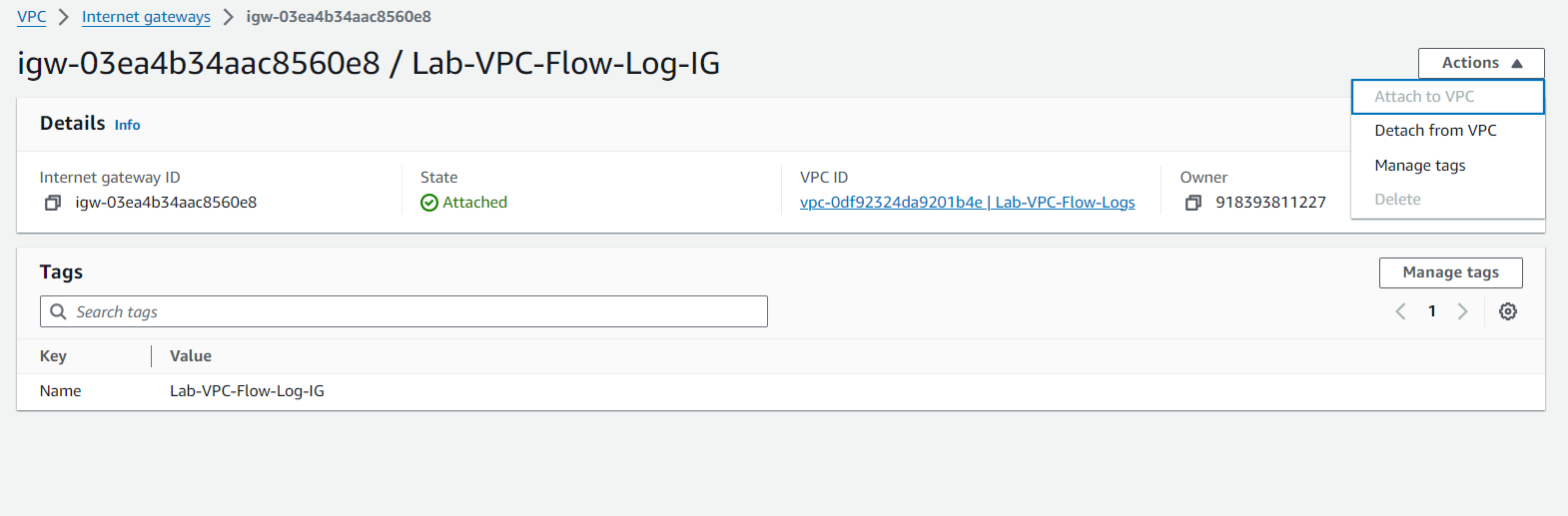
For **VPC ID**, select the VPC - **Lab-VPC-Flow-Logs**

**Subnet name:**Lab-VPC-Flow-Log-Subnet

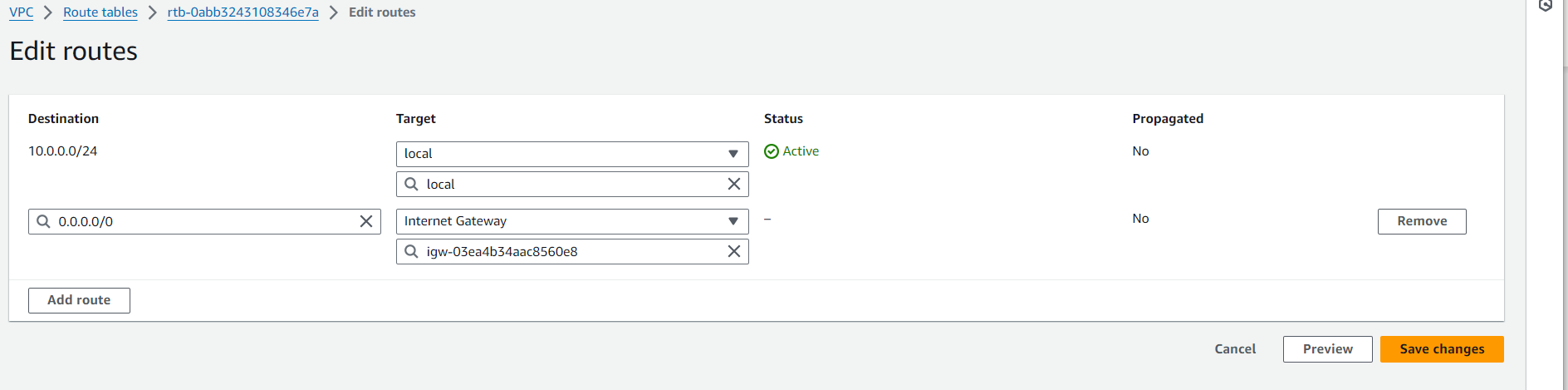
For **Availability Zone**, select **us-east-1a**

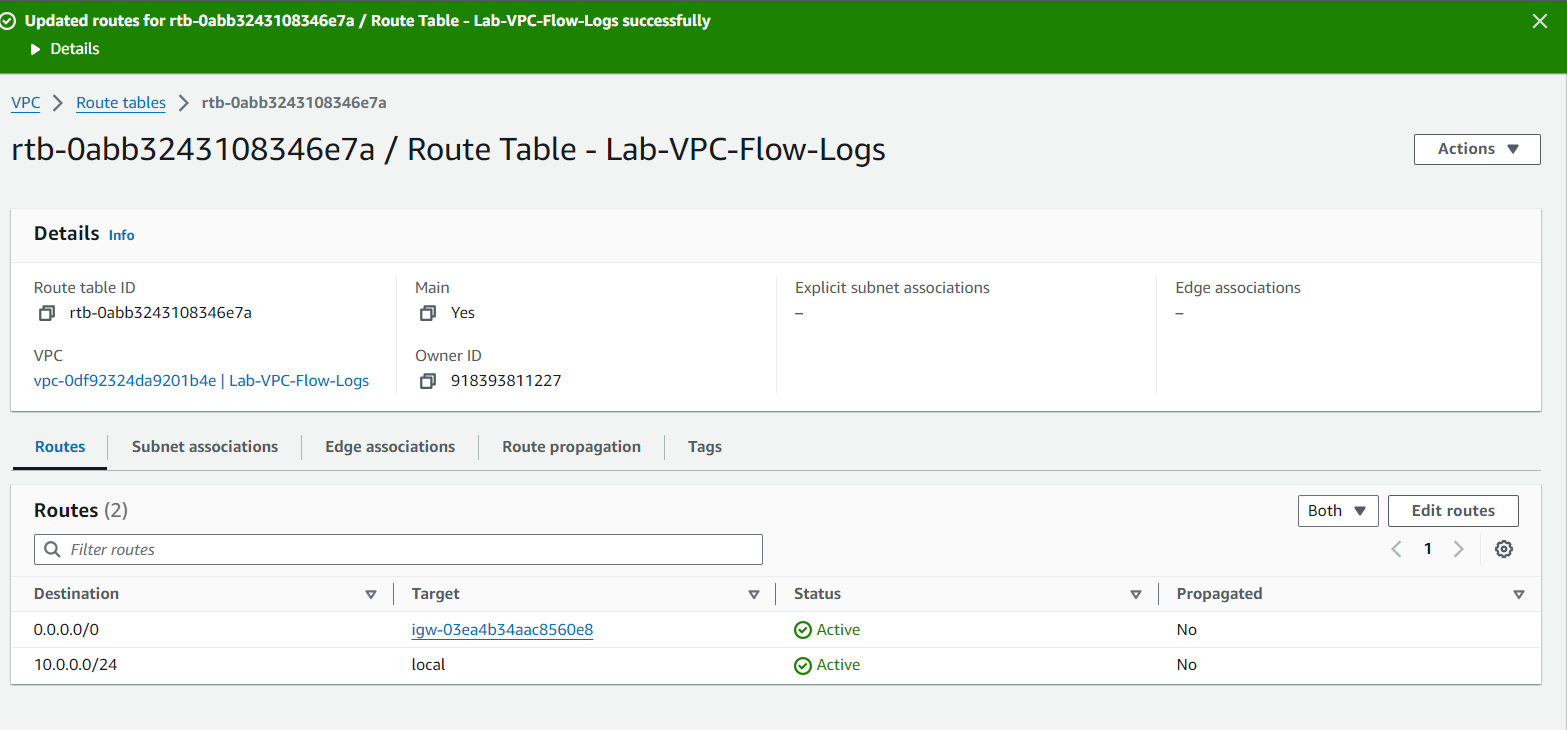


**Name tag**: Lab-VPC-Flow-Log-IG

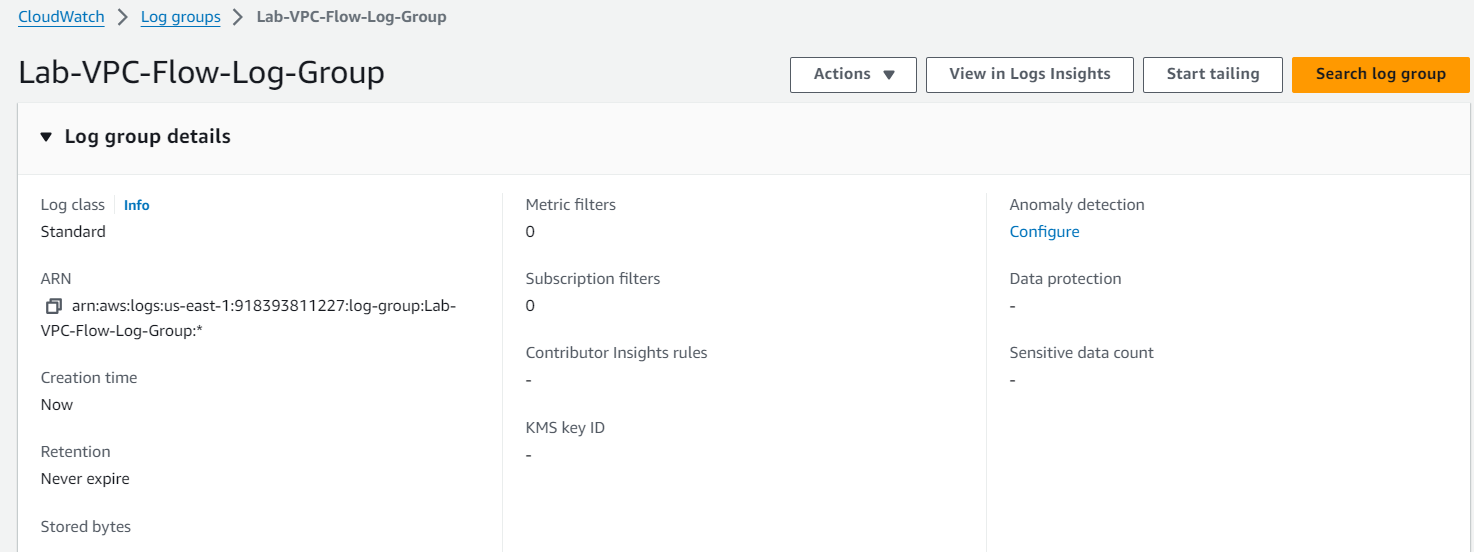


Route table edit:





**VPC Log group name**: Lab-VPC-Flow-Log-Group



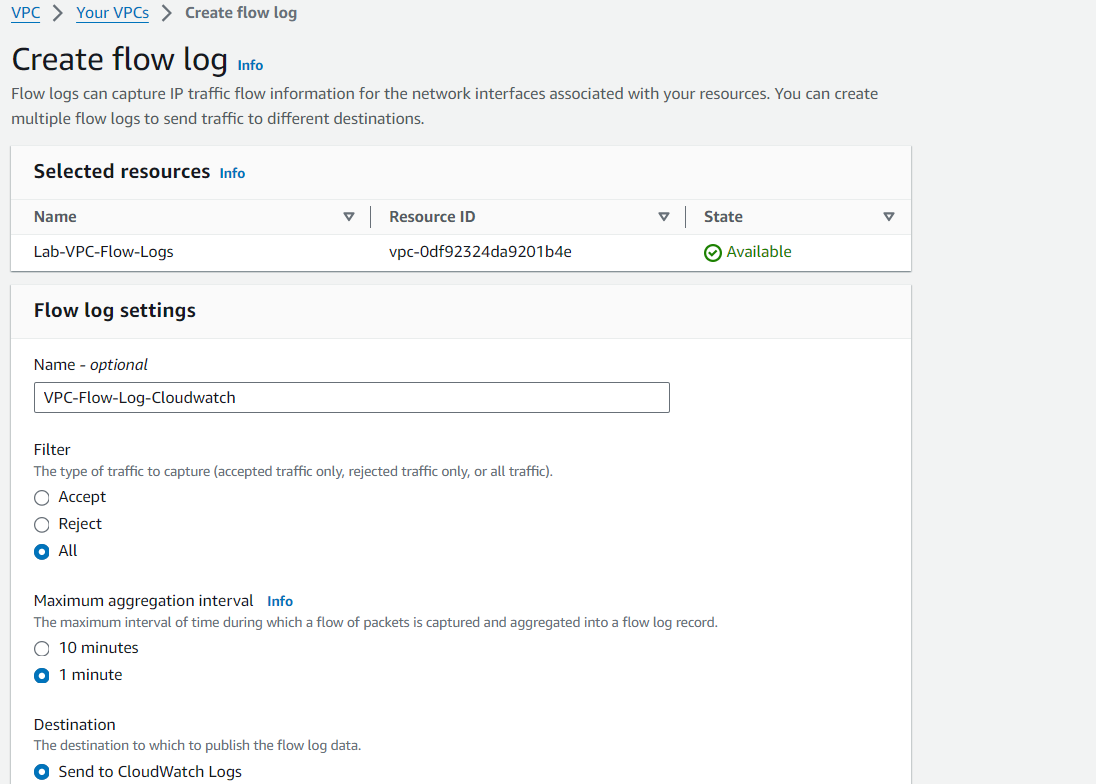
Enter the following values to create the VPC flow log:

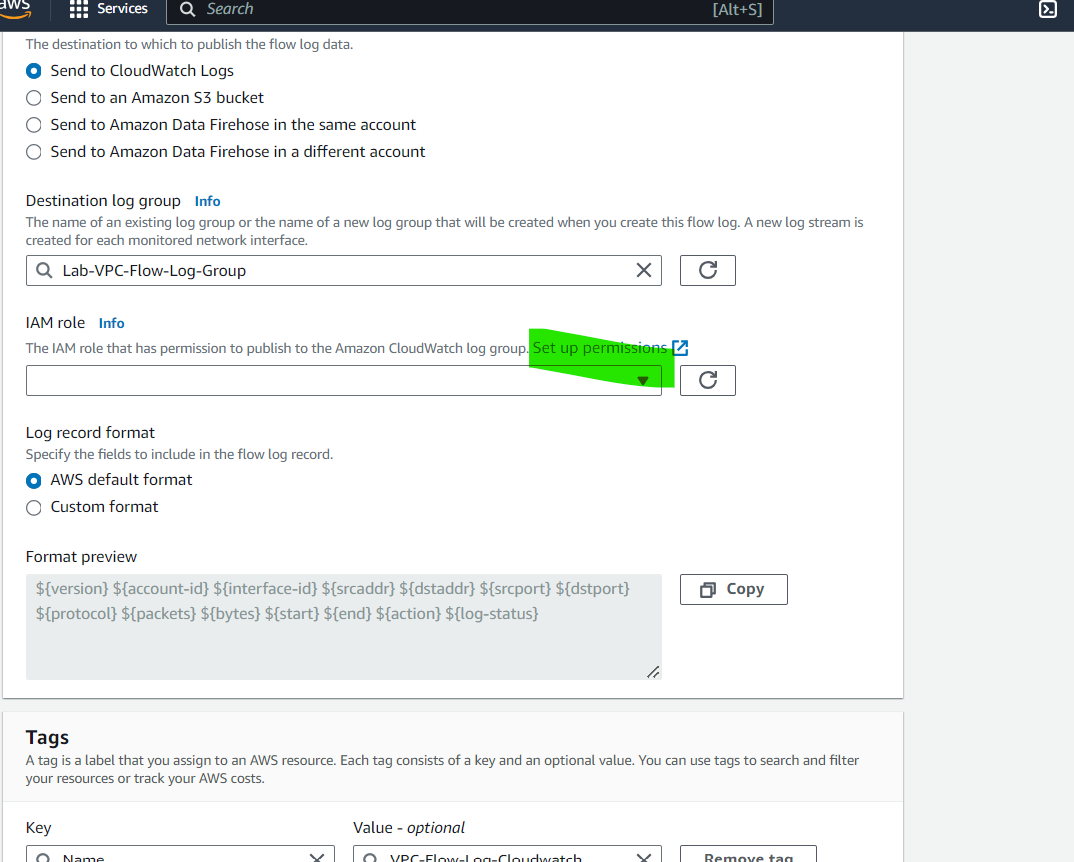
**Name**: VPC-Flow-Log-Cloudwatch

For **Filter**, select **All**

For **Maximum aggregation interval**, select **1 minute**

For**Destination,**select**Send to Cloudwatch Logs**





flowlogPolicy

{

  "Version": "2012-10-17",

  "Statement": [

    {

      "Effect": "Allow",

      "Action": [

        "logs:CreateLogGroup",

        "logs:CreateLogStream",

        "logs:PutLogEvents",

        "logs:DescribeLogGroups",

        "logs:DescribeLogStreams"

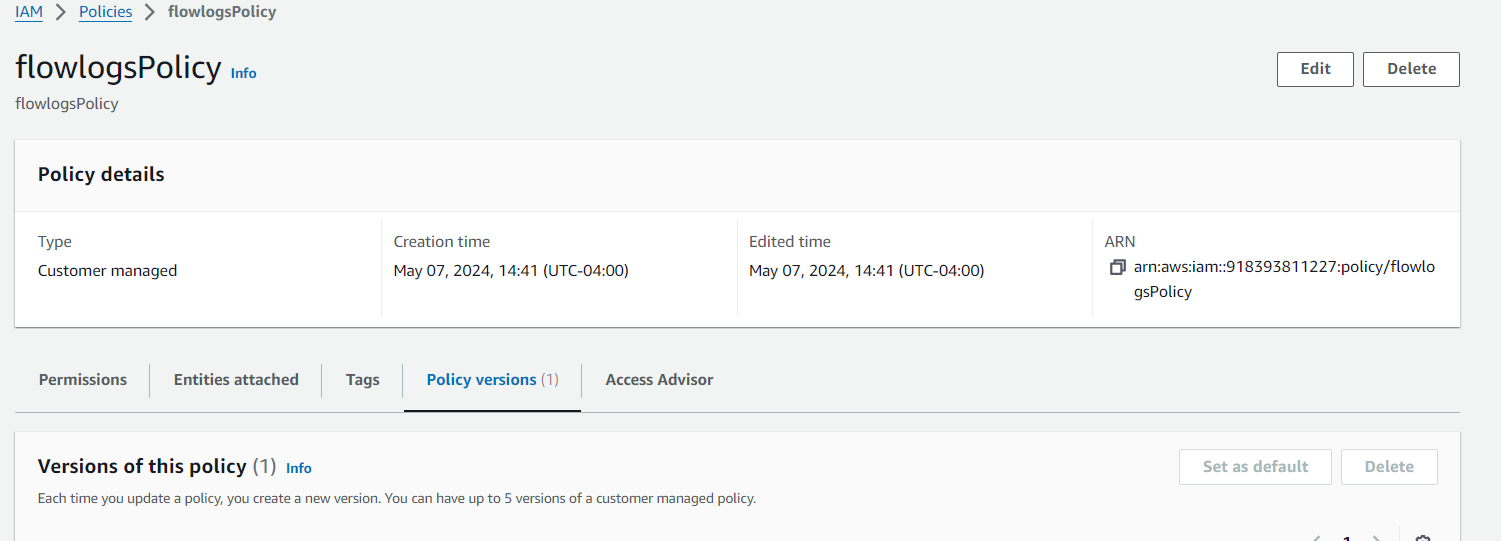
      ],

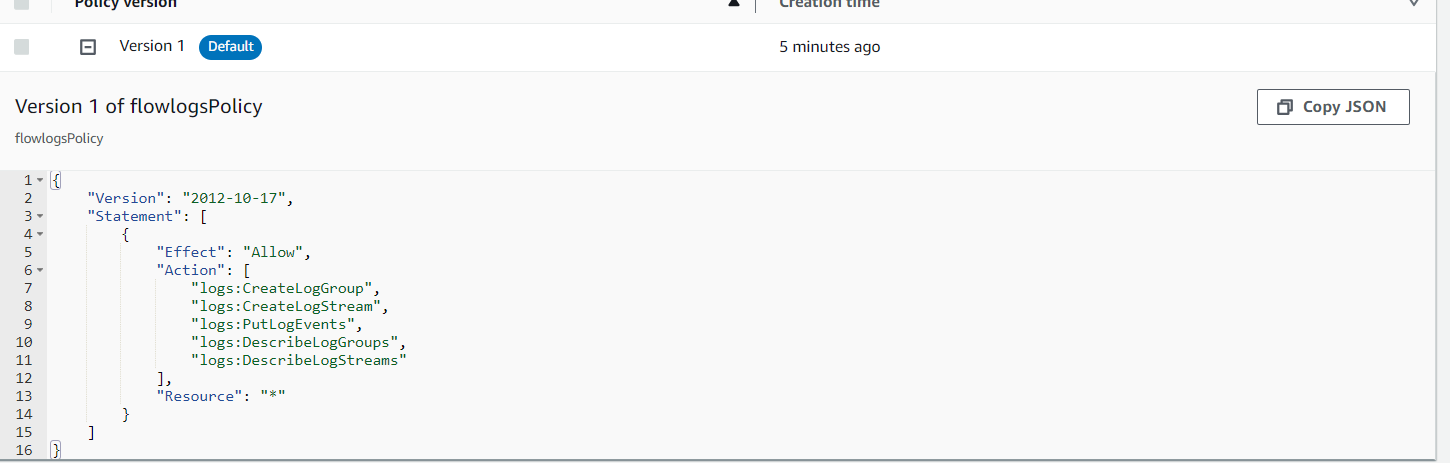
      "Resource": "\*"

    }

  ]

}





flowlogRole

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "Statement1",

"Effect": "Allow",

"Principal": {

"Service": "vpc-flow-logs.amazonaws.com"

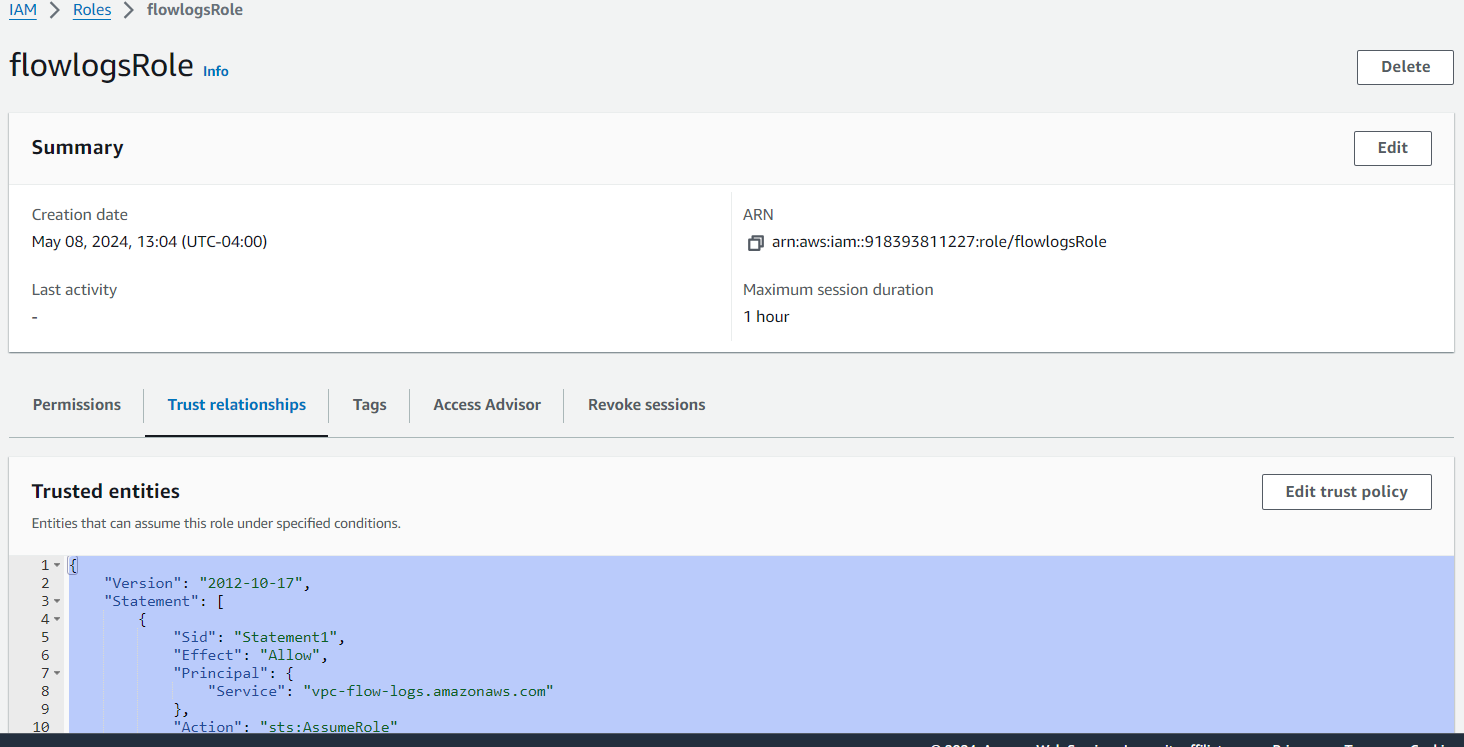
},

"Action": "sts:AssumeRole"

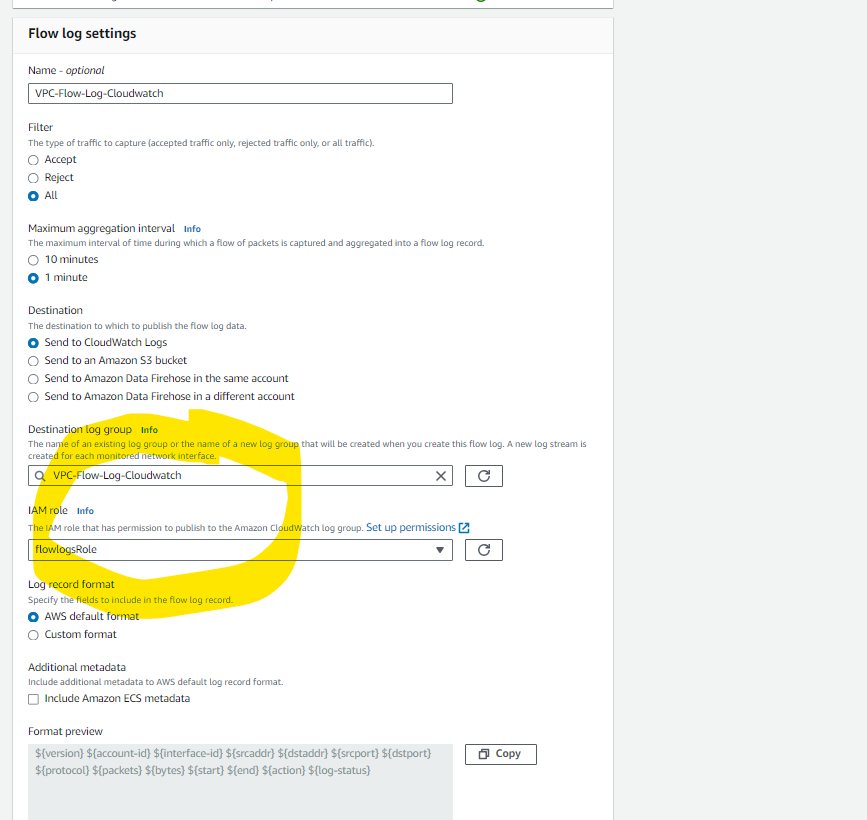
}

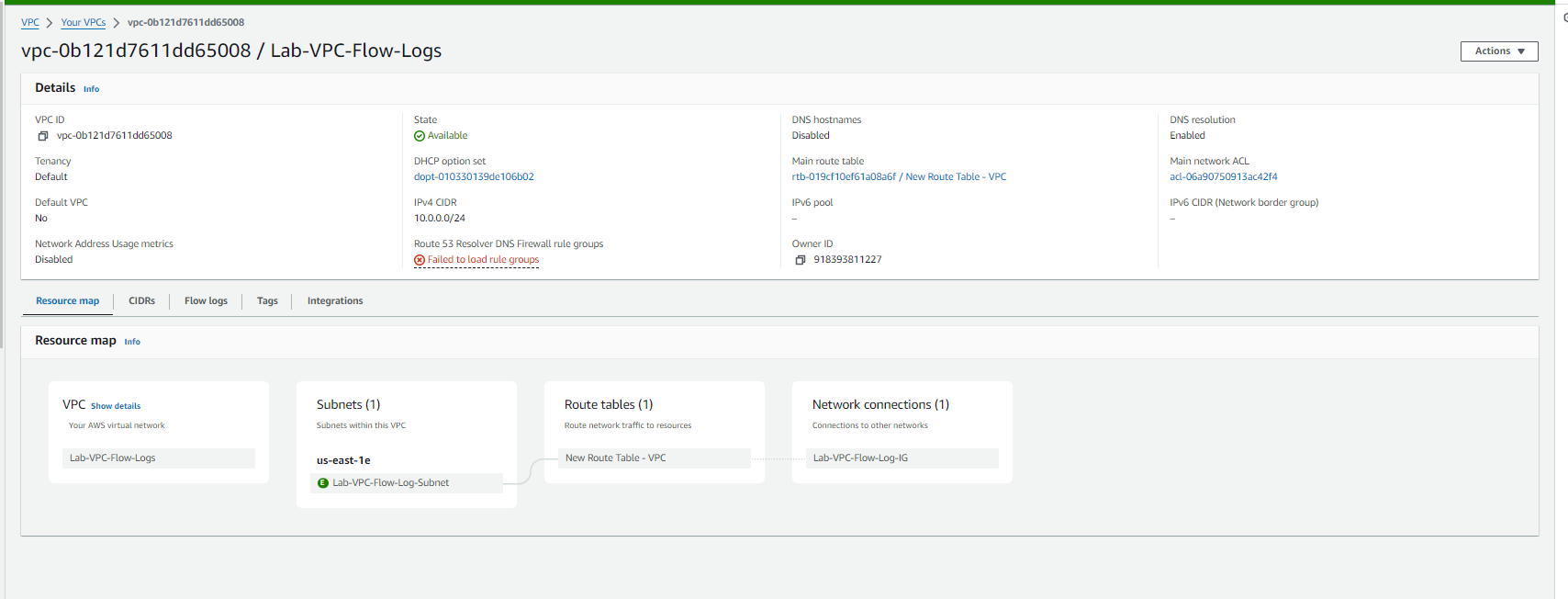
]

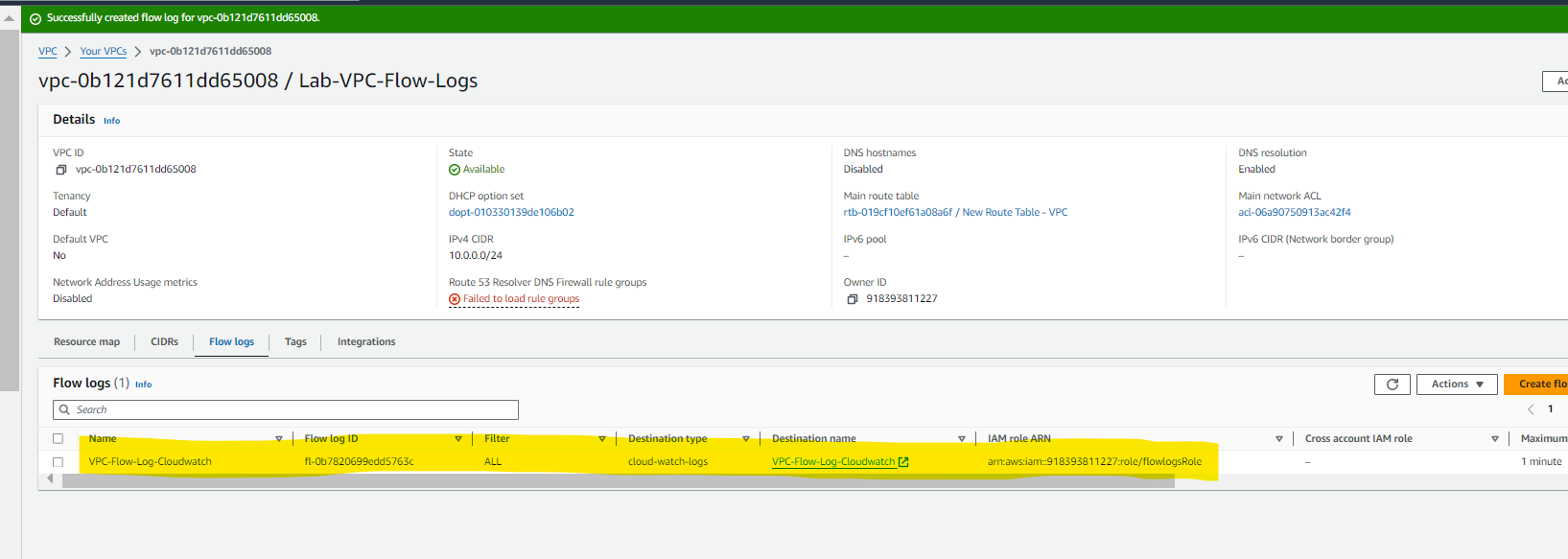
}



Attach the role to flow-log

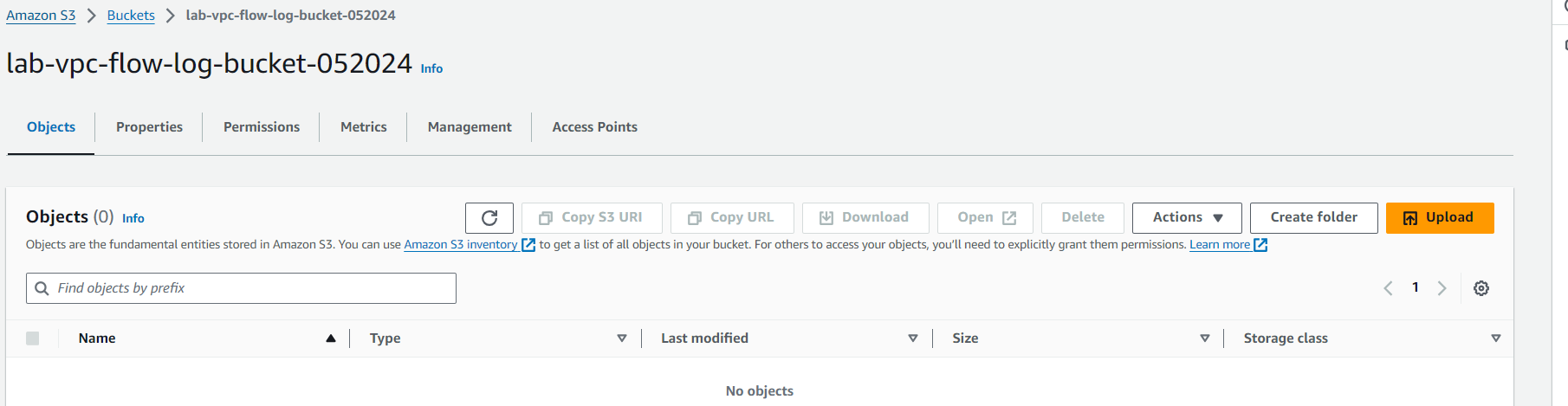


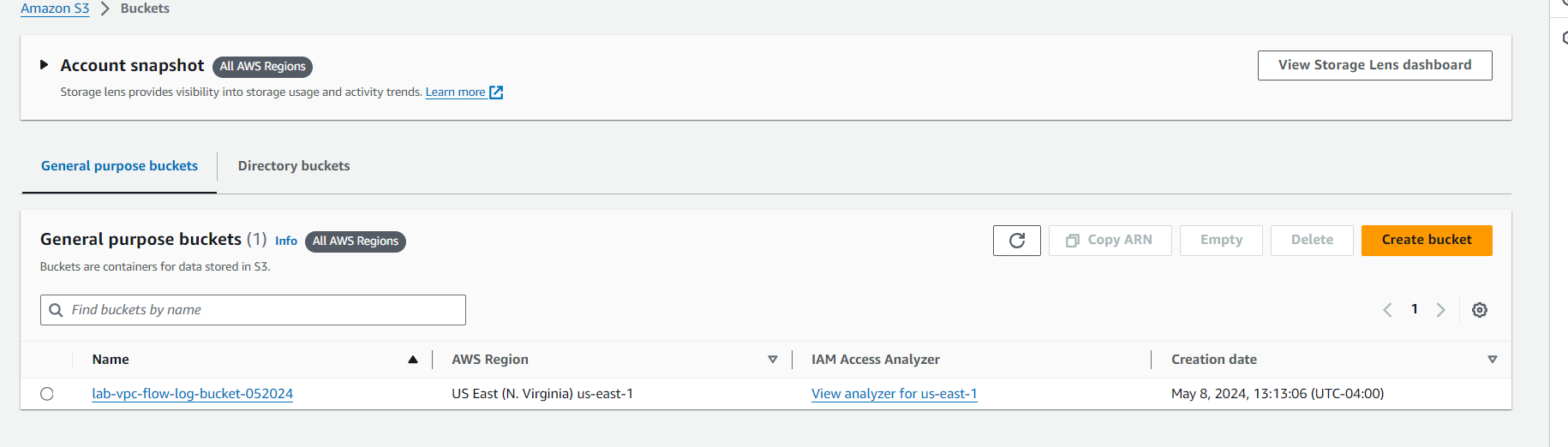




**Bucket name**: lab-vpc-flow-log-bucket (You will need to select a different name as S3 bucket names must be globally unique)

For **AWS Region**, select **US East (N. Virginia) us-east-1**

****

****

**Create S3 bucket:**

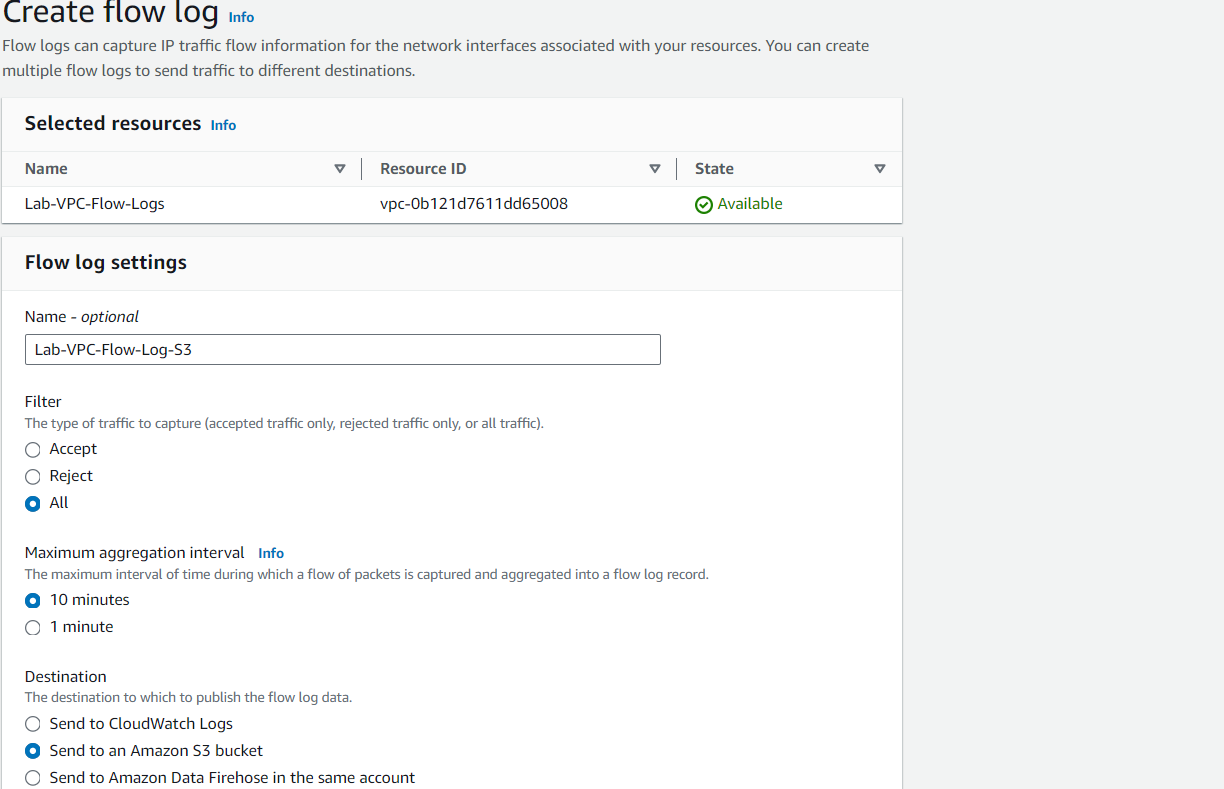
Enter the following values to create the VPC flow log:

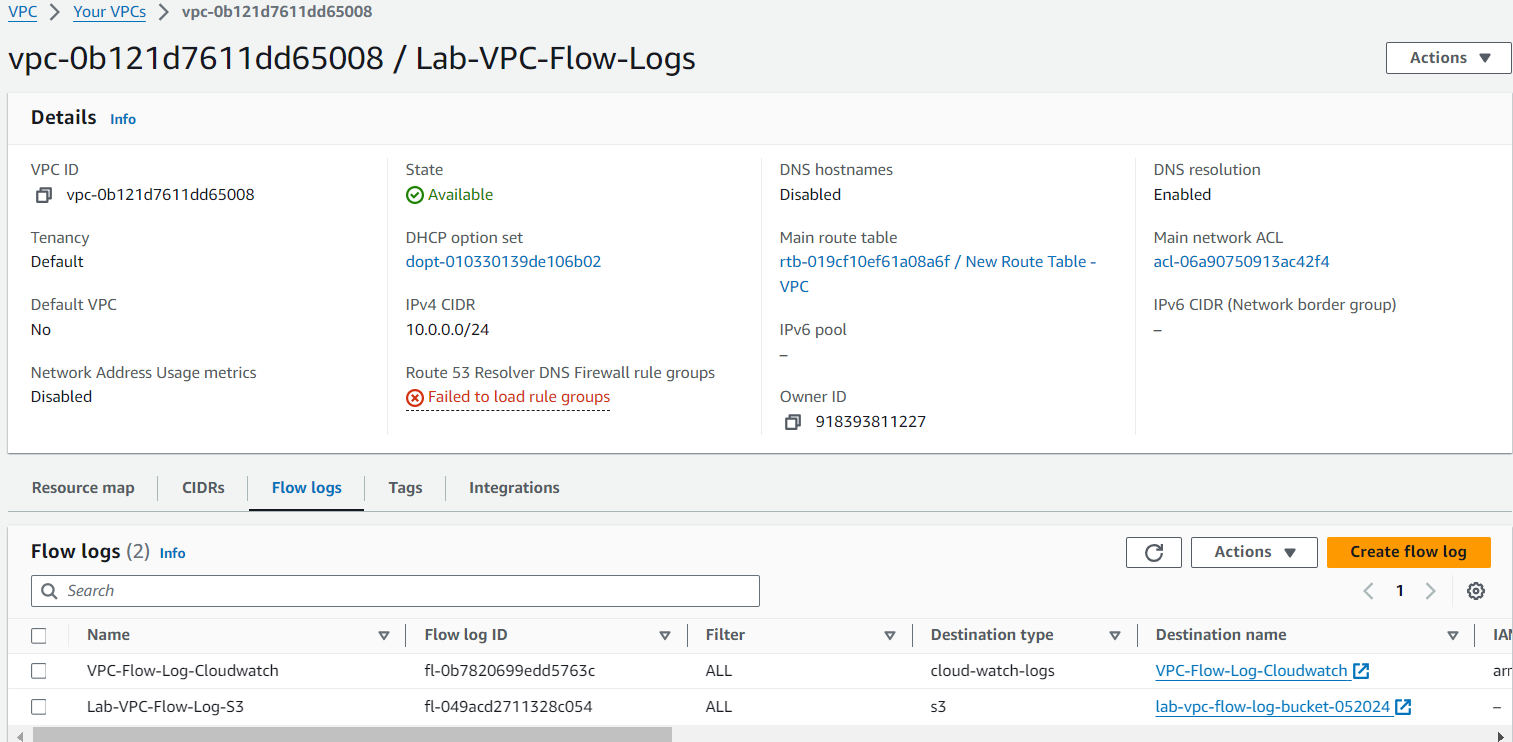
**Name**: Lab-VPC-Flow-Log-S3

For **Filter**, select **All**

For **Maximum aggregation interval**, select **1 minute**

For**Destination,**select**Send to Amazon S3 bucket**

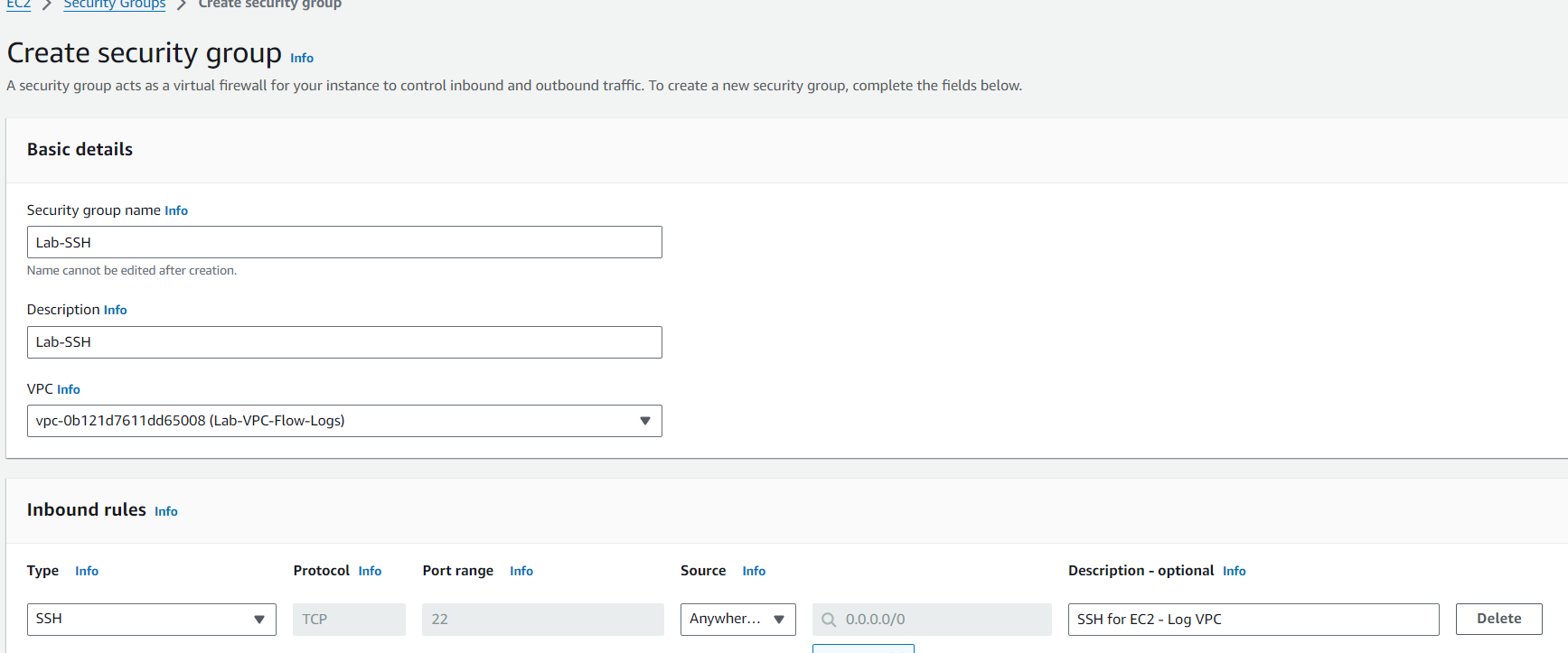
****

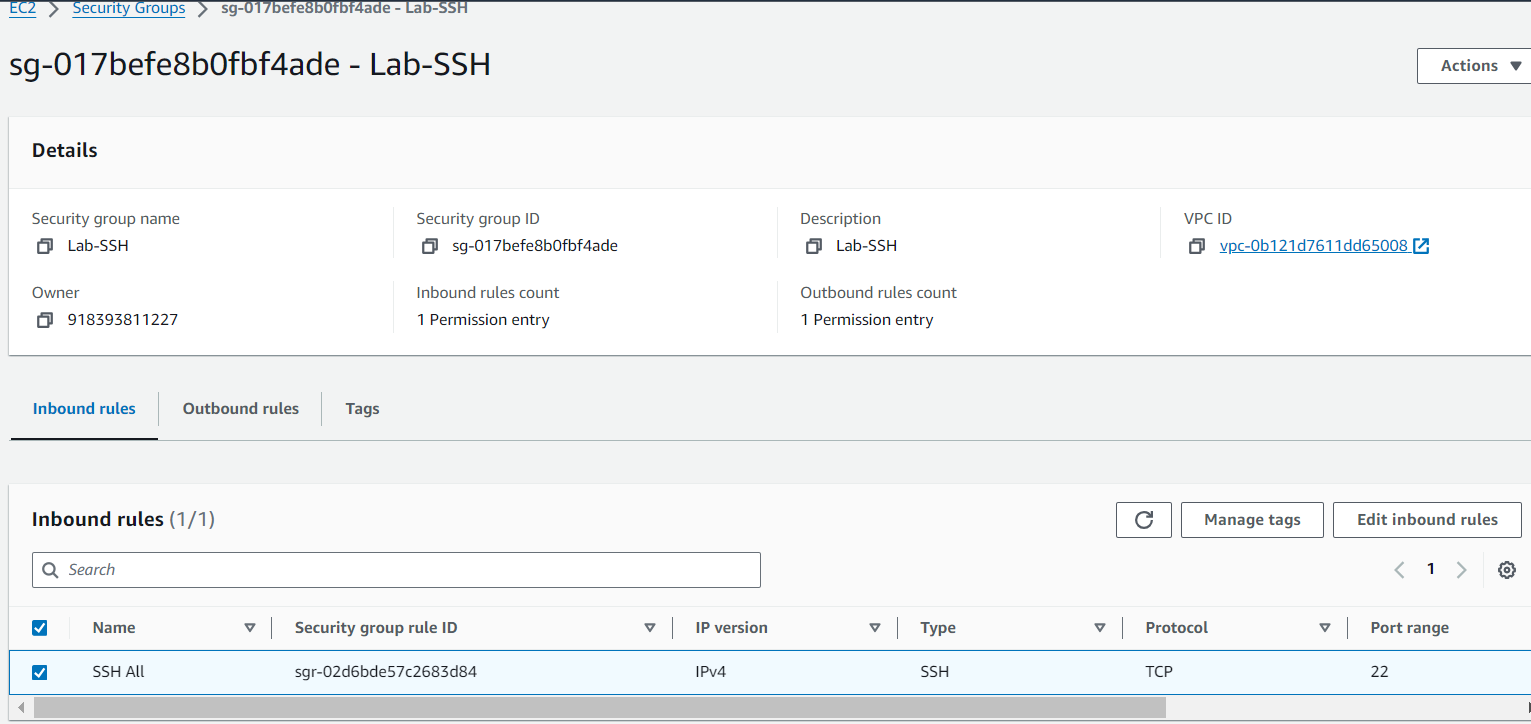


**Security group name**: Lab-SSH

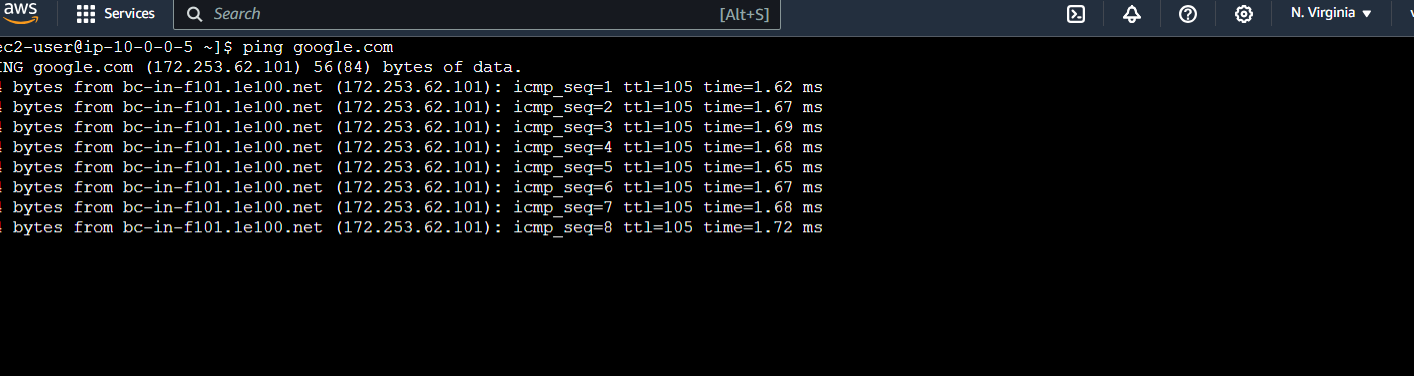
**Description**: Lab-SSH

For **VPC**, select **Lab-VPC-Flow-Logs**

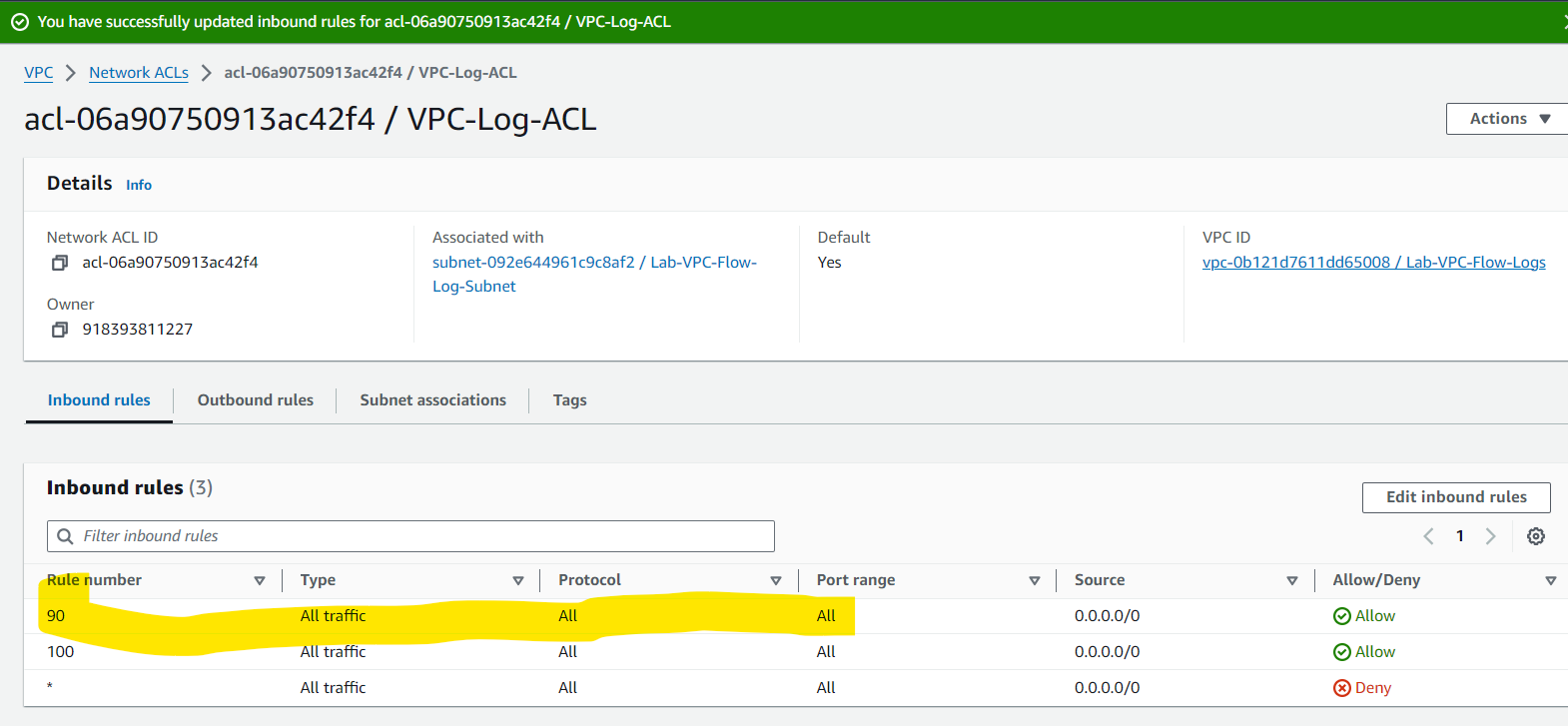




Create Ec2 Instance and ping google.com in defined/vpc, subnet and sg.



Update ACL’s



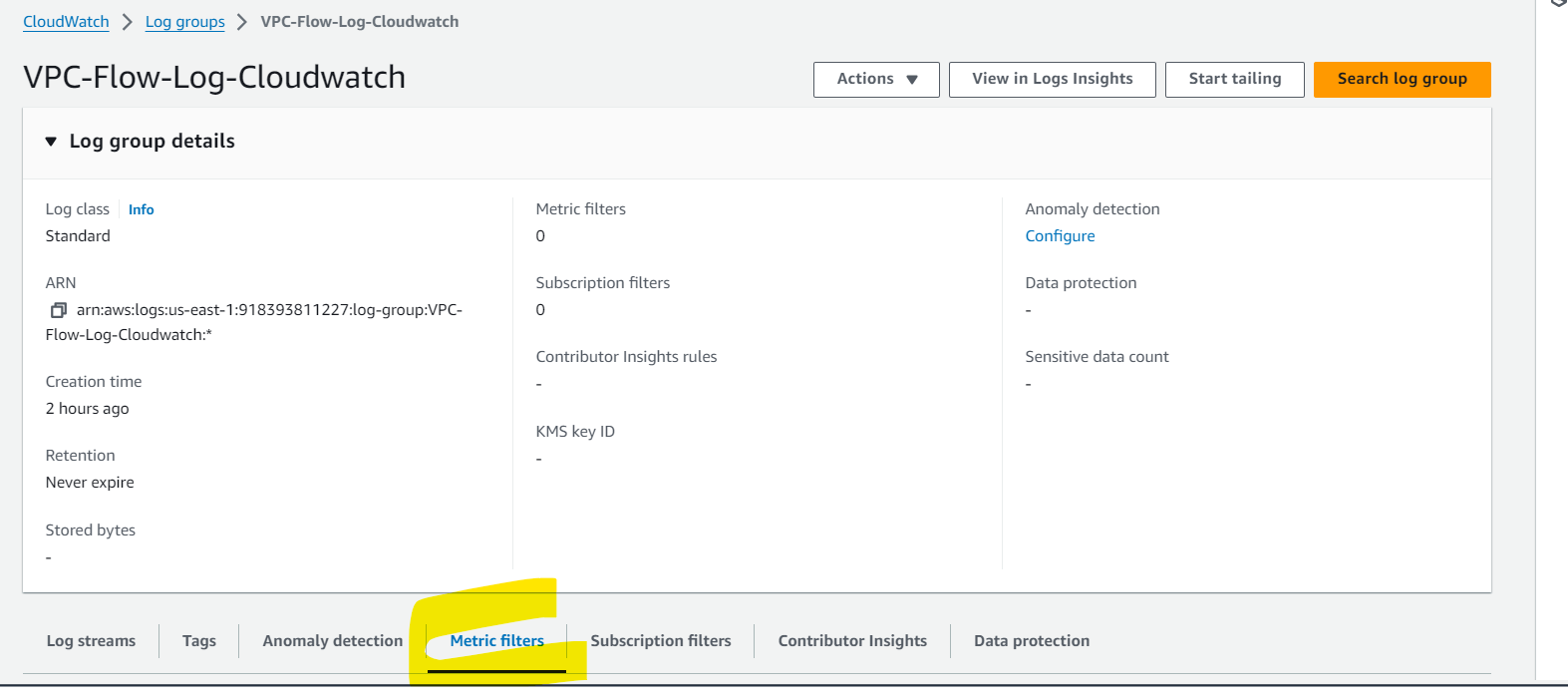
Create Metric

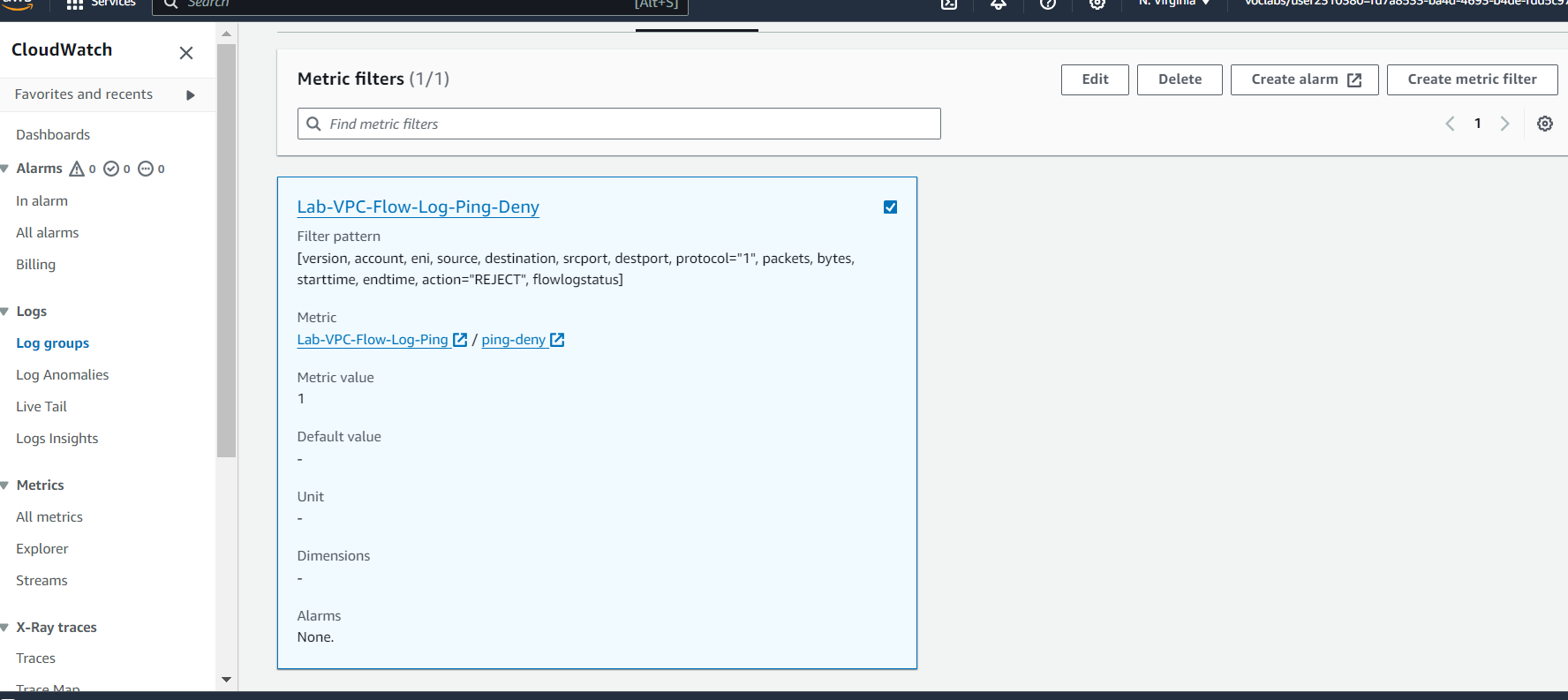
**Filter name**: Lab-VPC-Flow-Log-Ping-Deny

**Metric namespace**: Lab-VPC-Flow-Log-Ping

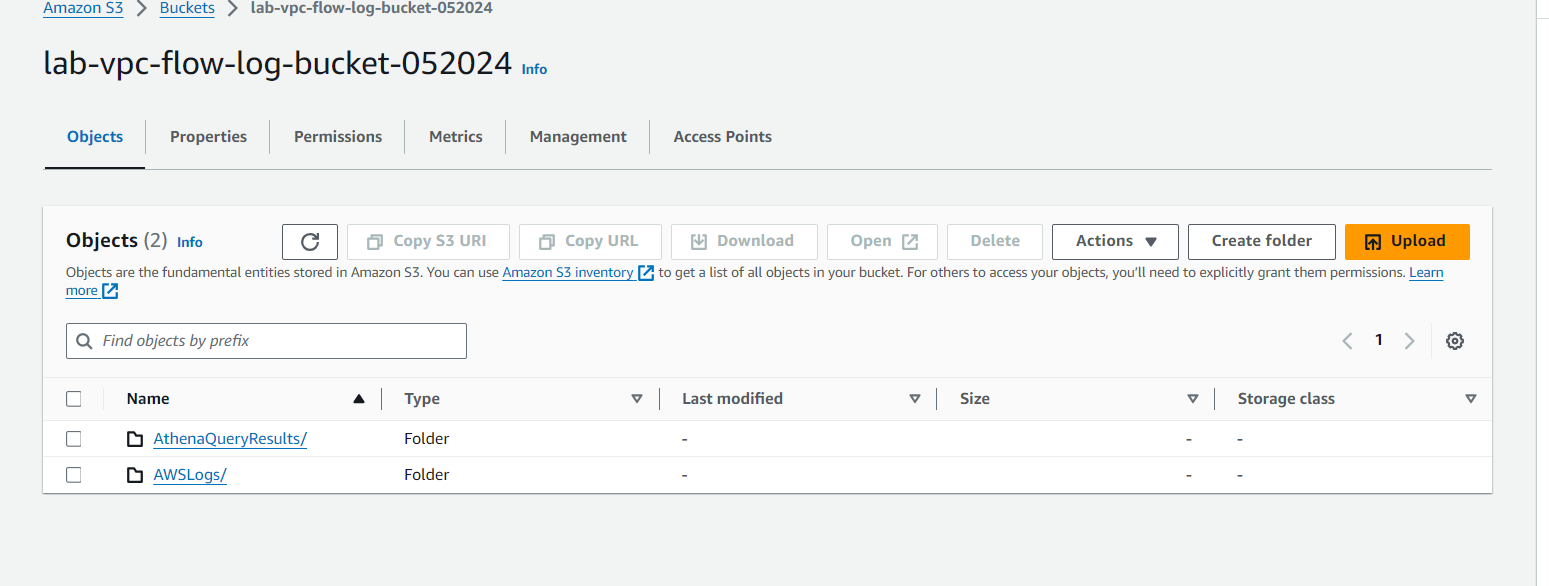
**Metric name**: Ping-Deny

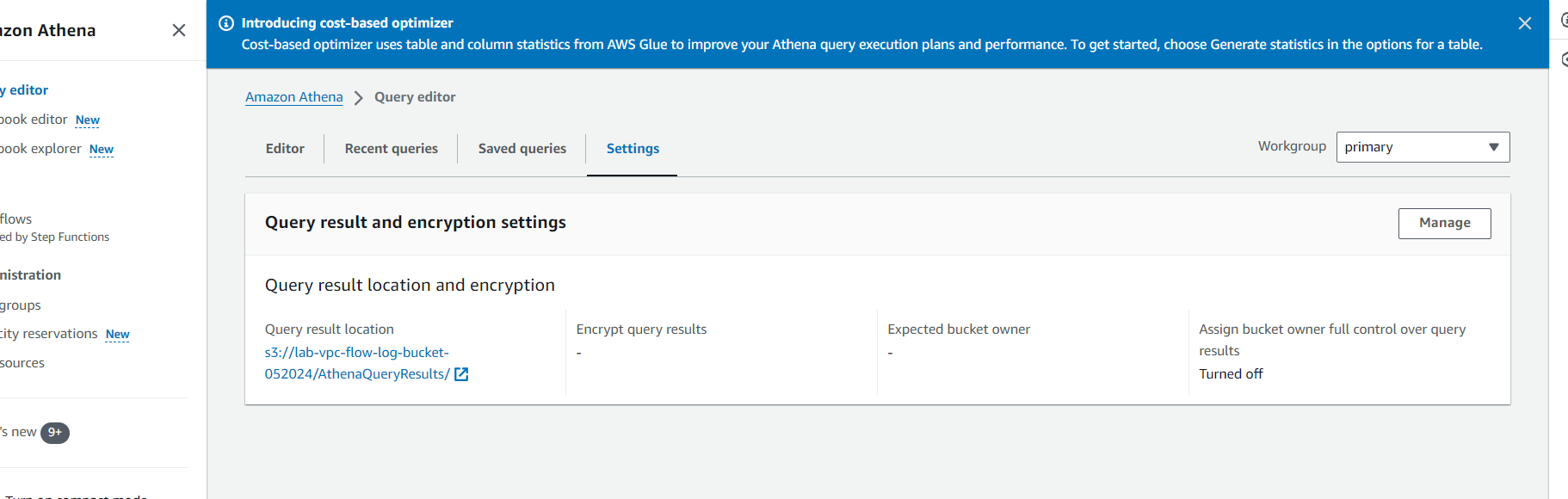
**Metric value**: 1





S3 and Athena





Athena

