Project Title: Configure VPC Flow Logs and Store Logs in S3Using IAM Role:

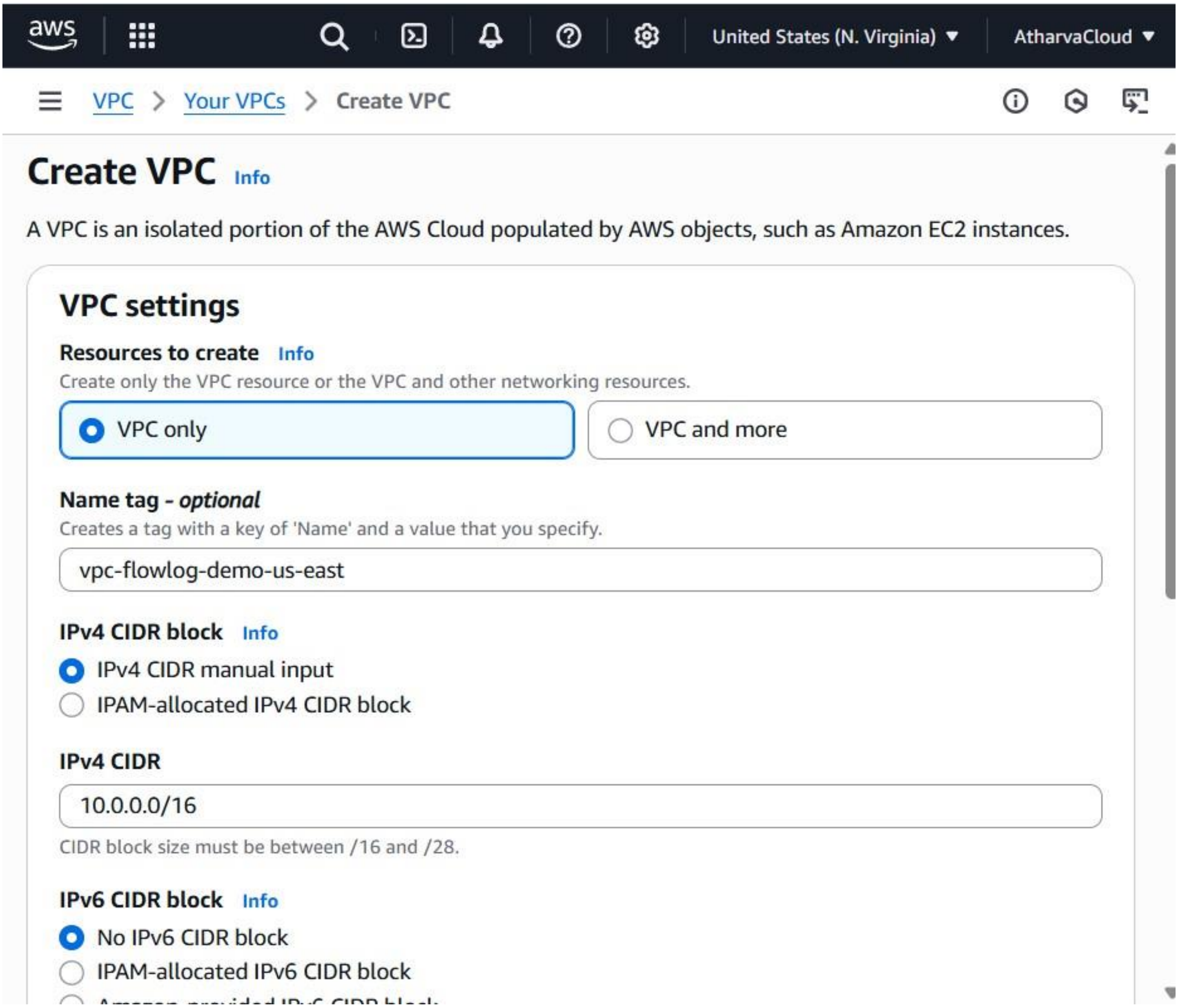
Objective:

The goal of this project is to capture all the network traffic (incoming and outgoing) from a VPC using AWS Flow Logs. These logs are stored in an S3 bucket using an IAM role. This setup helps monitor network activity for security, auditing, or troubleshooting. It's helpful to know what kind of traffic is reaching your AWS infrastructure. This project shows how to set that up from scratch using basic AWS services.

Step 1: Create a VPC:

You need a private network (VPC) where AWS resources like EC2 will run. This is where traffic will be logged.

Go to VPC in AWS Console.
Click Create VPC → Choose VPC only → Give a name → Keep default settings → Create



Create VPC Info

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create Info

Create only the VPC resource or the VPC and other networking resources.

● VPC only ○ VPC and more

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

vpc-flowlog-demo-us-east

IPv4 CIDR block Info

● IPv4 CIDR manual input
○ IPAM-allocated IPv4 CIDR block

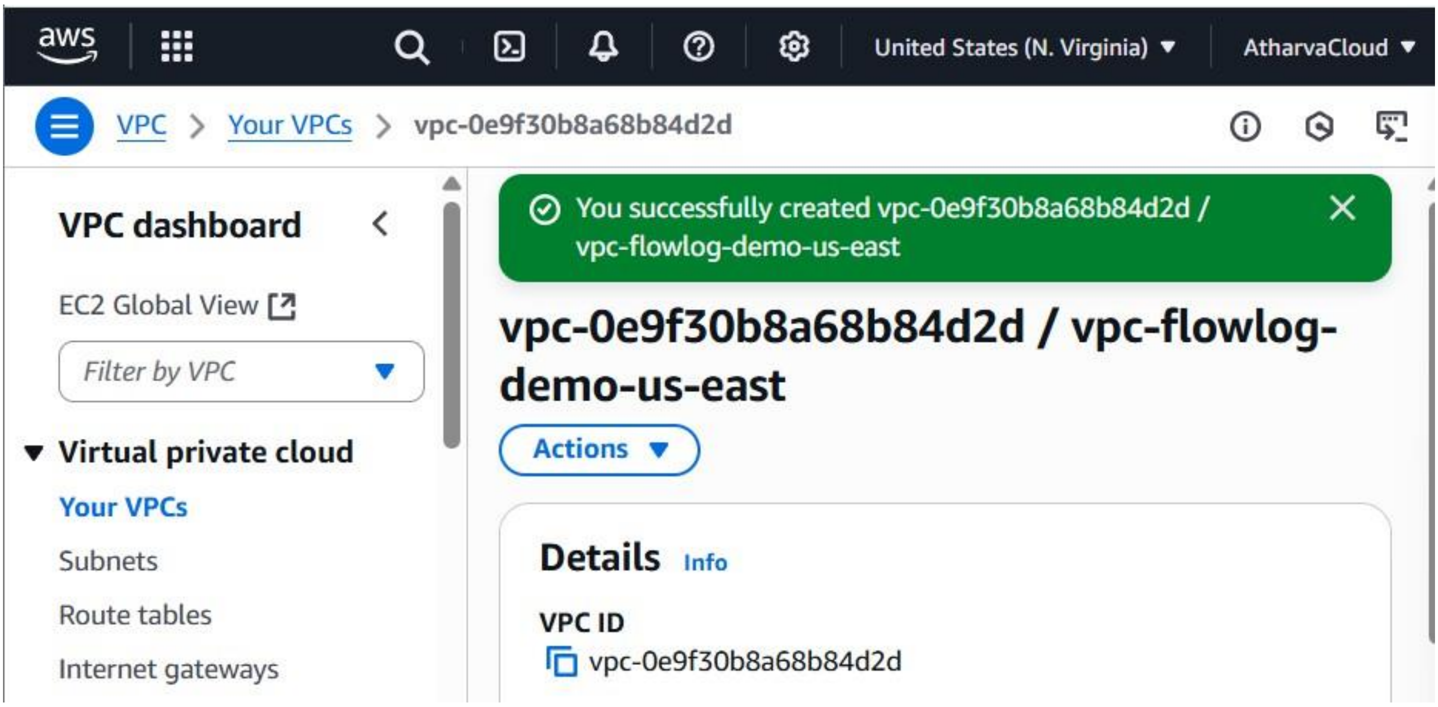
IPv4 CIDR

10.0.0.0/16

CIDR block size must be between /16 and /28.

IPv6 CIDR block Info

● No IPv6 CIDR block
○ IPAM-allocated IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block



You successfully created vpc-0e9f30b8a68b84d2d / vpc-flowlog-demo-us-east

vpc-0e9f30b8a68b84d2d / vpc-flowlog-demo-us-east

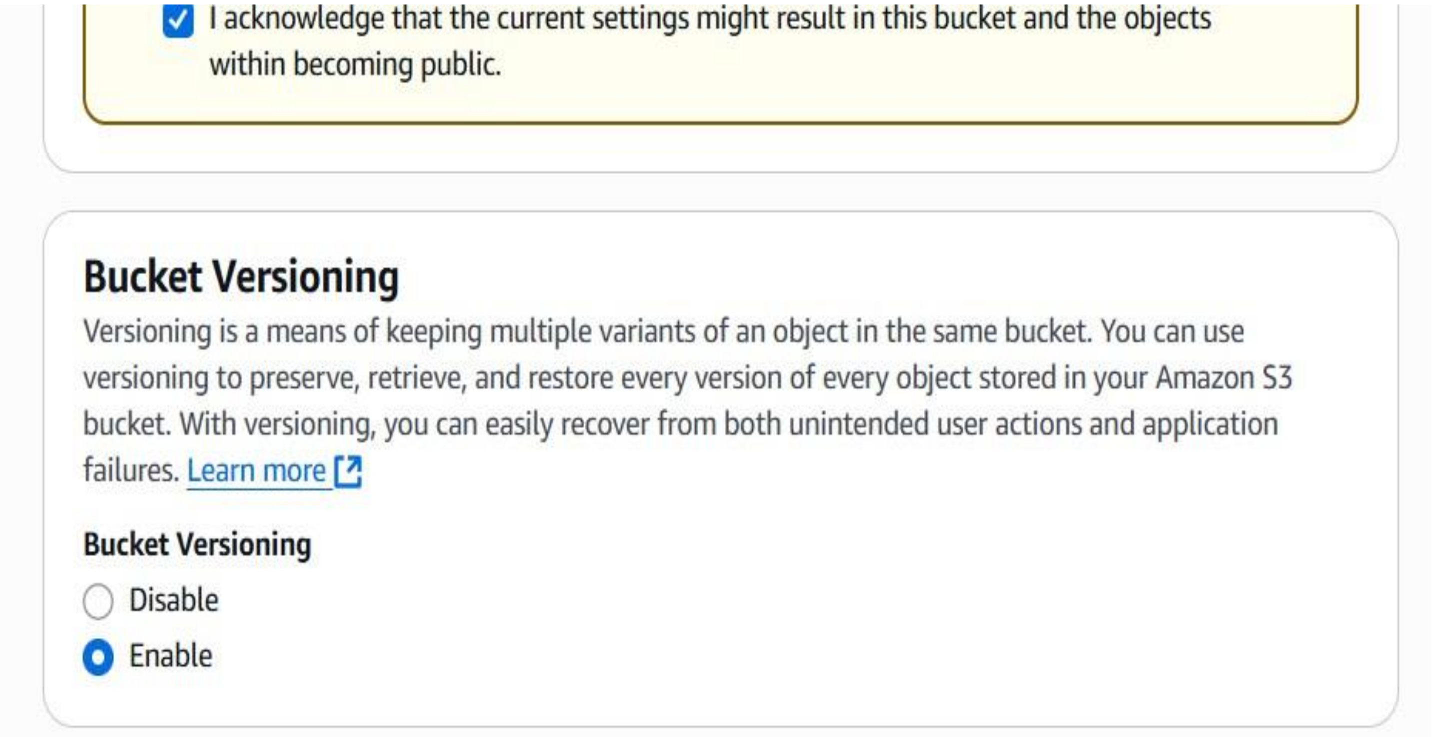
Details

VPC ID
vpc-0e9f30b8a68b84d2d

vpc-0e9f30b8a68b84d2d

Step 2: Create an S3 Bucket with Versioning:

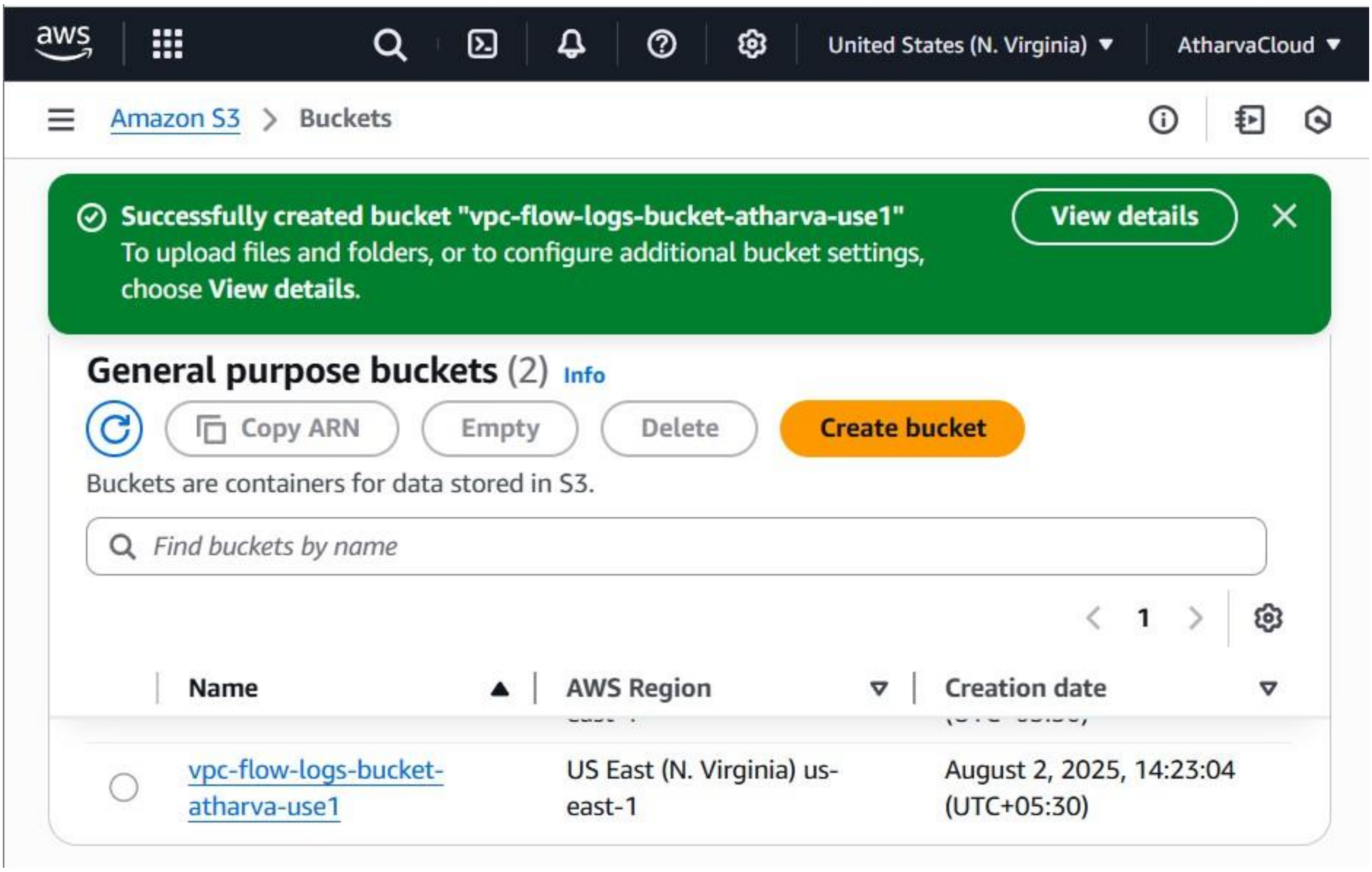
We need a place to store the logs. S3 is like cloud storage. Versioning helps keep track of any changes.
Go to S3 → Click Create bucket.
Give a unique name and choose the same region as your VPC.
Enable bucket versioning → Create bucket.


☑ I acknowledge that the current settings might result in this bucket and the objects within becoming public.

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning
○ Disable
● Enable



Successfully created bucket "vpc-flow-logs-bucket-atharva-use1"
To upload files and folders, or to configure additional bucket settings, choose **View details**.

General purpose buckets (2)

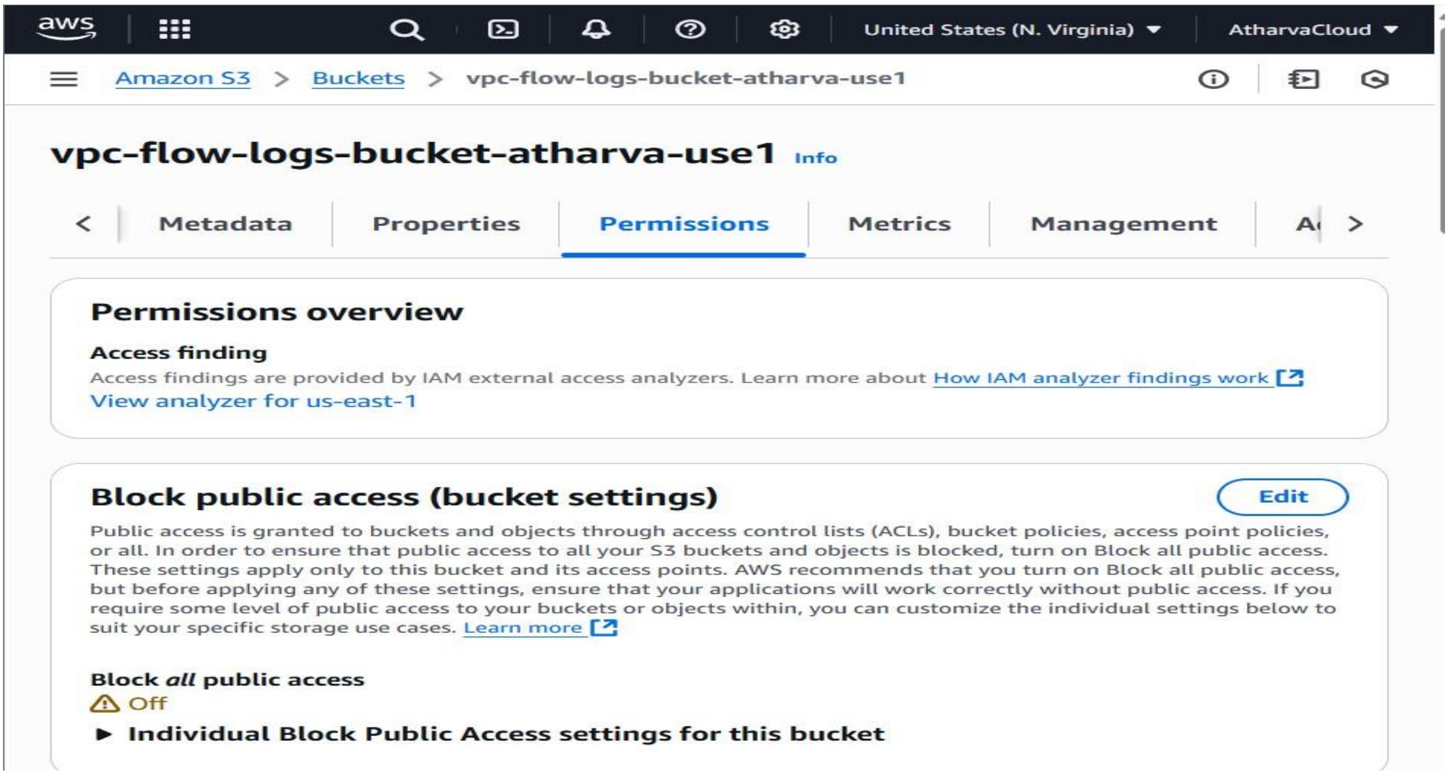
Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	Creation date
vpc-flow-logs-bucket-atharva-use1	US East (N. Virginia) us-east-1	August 2, 2025, 14:23:04 (UTC+05:30)

Step 3: Add a Bucket Policy:

We must allow the VPC Flow Logs service to write logs to the bucket.
Go to S3 → Your Bucket → Permissions tab → Bucket policy.
Click Edit and paste the provided JSON policy → Save.


aws
United States (N. Virginia) ▼
AtharvaCloud ▼
Amazon S3 > Buckets > vpc-flow-logs-bucket-atharva-use1
Info
Metadata
Properties
Permissions
Metrics
Management
A
Edit

vpc-flow-logs-bucket-atharva-use1

Permissions overview

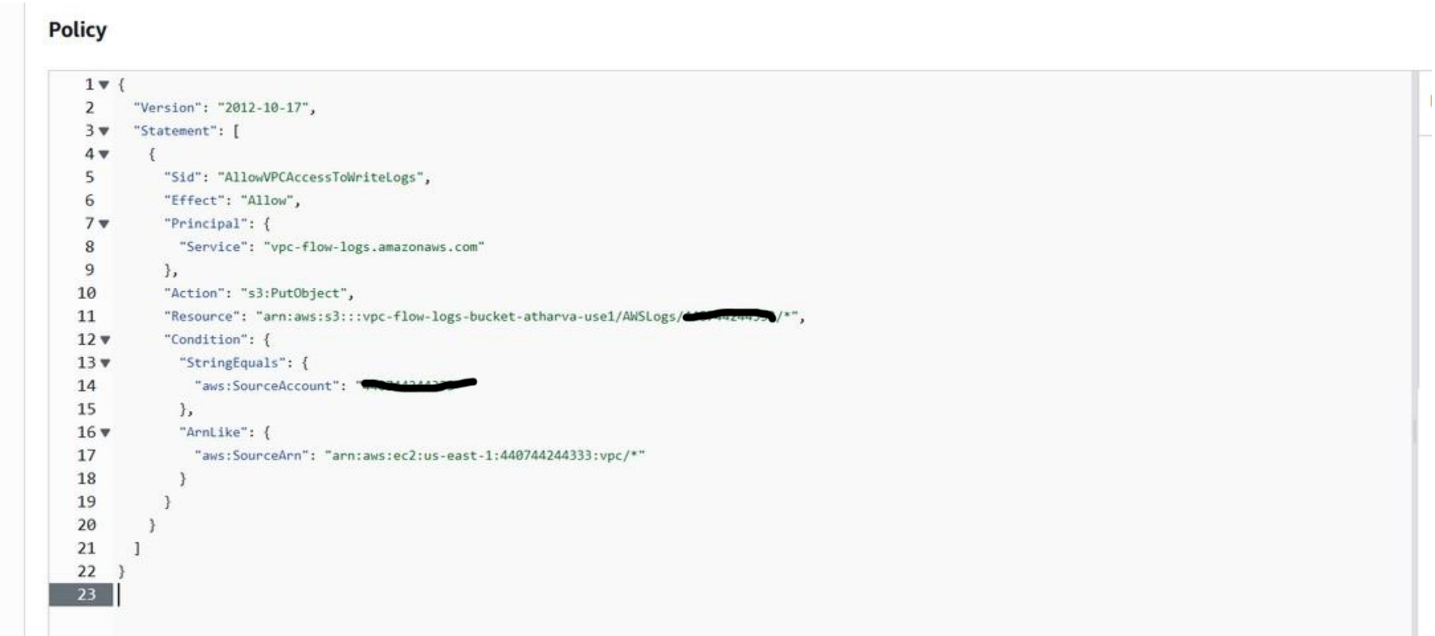
Access finding
Access findings are provided by IAM external access analyzers. Learn more about How IAM analyzer findings work
View analyzer for us-east-1

Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

Block *all* public access
⚠ Off

▶ **Individual Block Public Access settings for this bucket**

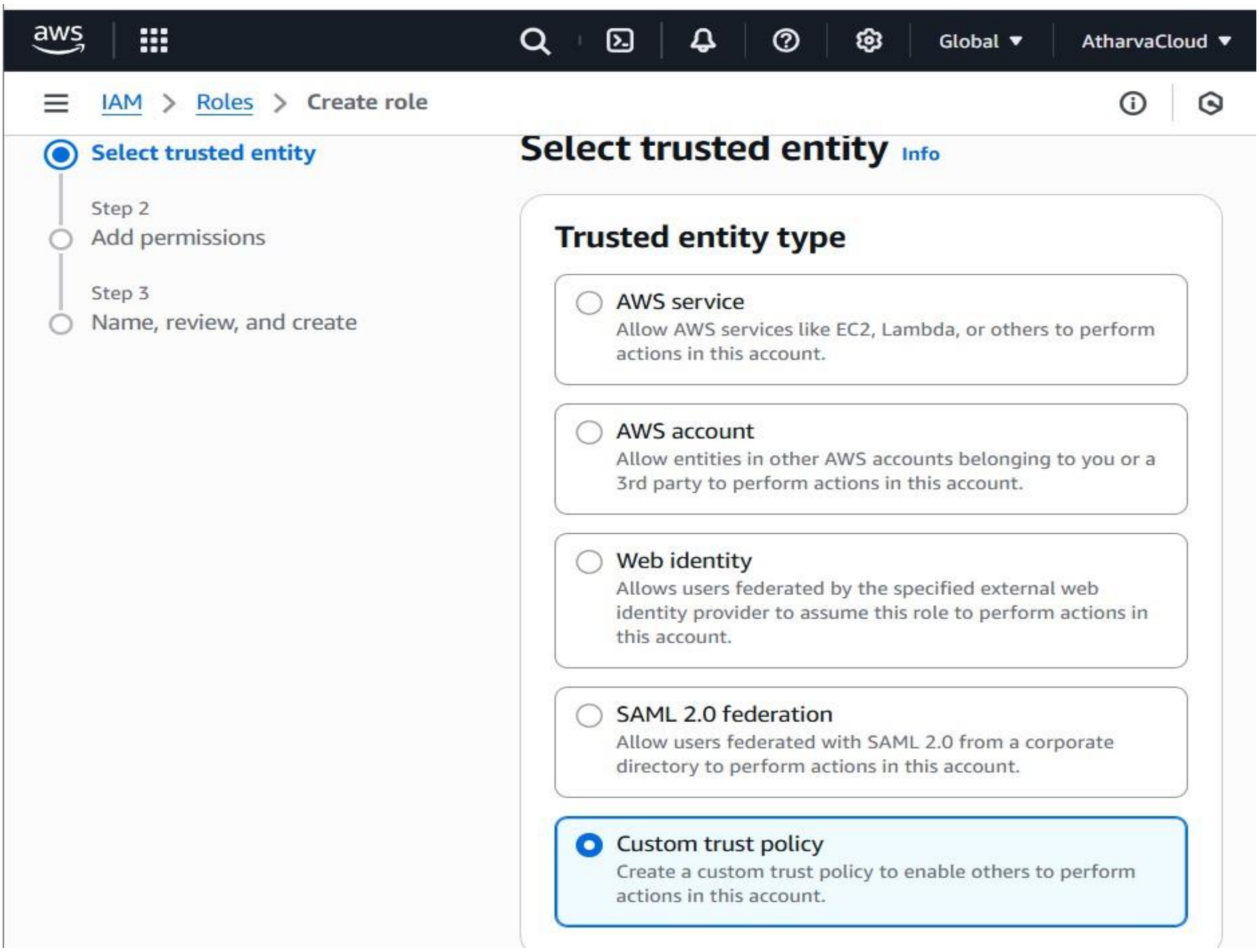


Policy

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowVPCAccessToWriteLogs",
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::vpc-flow-logs-bucket-atharva-use1/AWSLogs/[redacted]/*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "[redacted]
        },
        "ArnLike": {
          "aws:SourceArn": "arn:aws:ec2:us-east-1:440744244333:vpc/*"
        }
      }
    }
  ]
}
```

Step 4: Create an IAM Role with Trust Policy:

This role lets the VPC Flow Logs service act on your behalf to store logs in S3.
Go to IAM → Roles → Create Role → Custom Trust Policy.
Paste the trust JSON → Skip permissions → Give a name → Create role.



● Select trusted entity

Step 2
○ Add permissions

Step 3
○ Name, review, and create

Select trusted entity Info

Trusted entity type

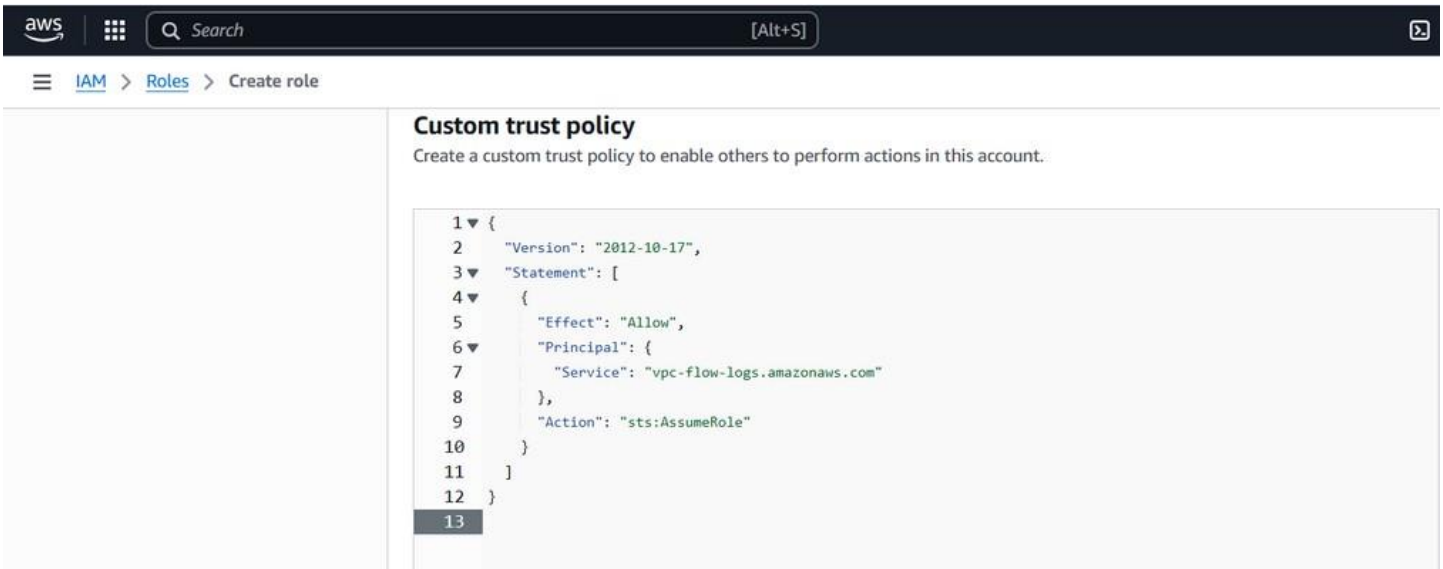
○ AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

● Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.



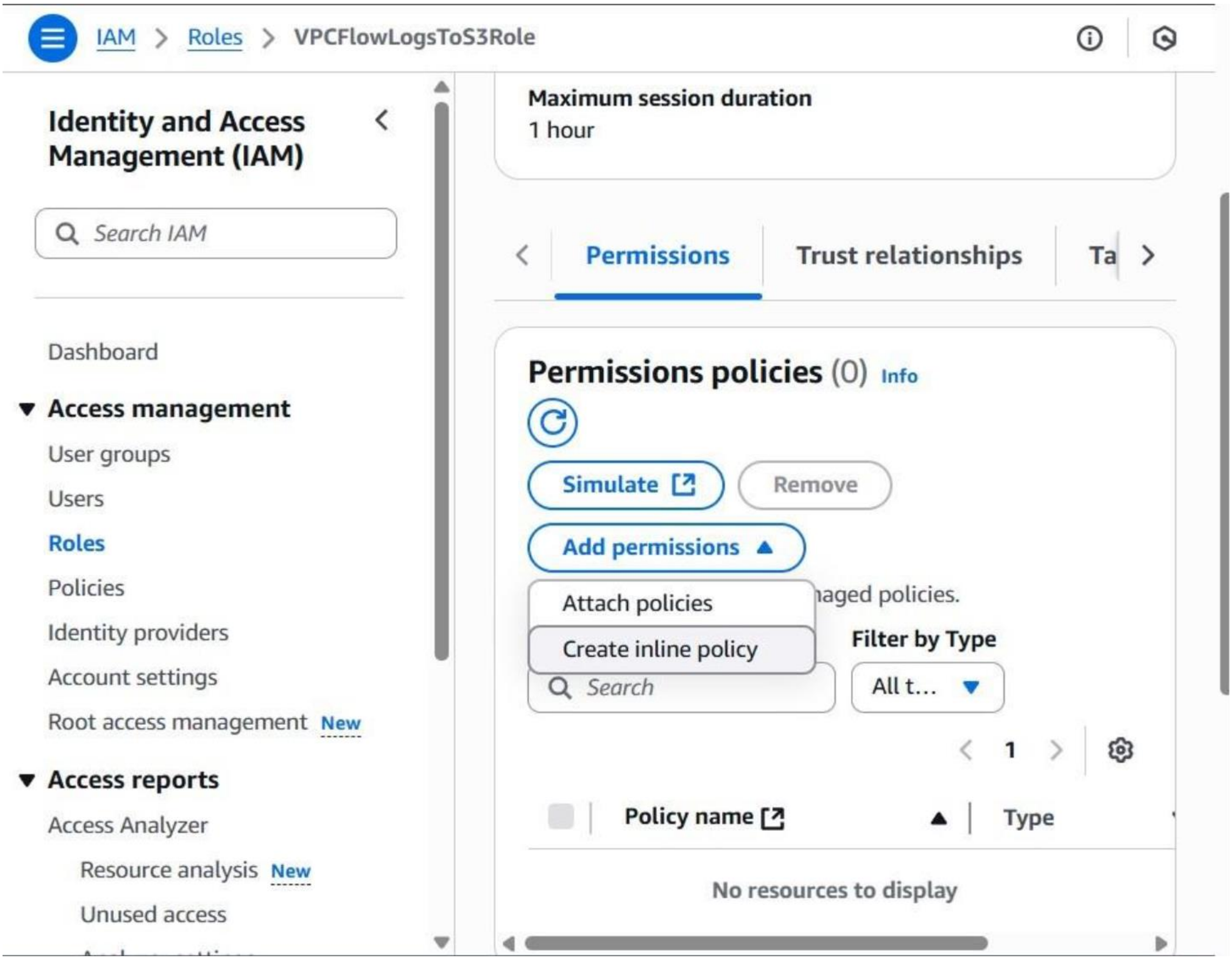
Custom trust policy

Create a custom trust policy to enable others to perform actions in this account.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "vpc-flow-logs.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Step 5: Attach a Permission Policy to the Role:

This allows the role to put logs into the S3 bucket.
Go to IAM → Your Role → Permissions tab → Add inline policy.
Choose JSON tab, paste the policy, save it with a name.

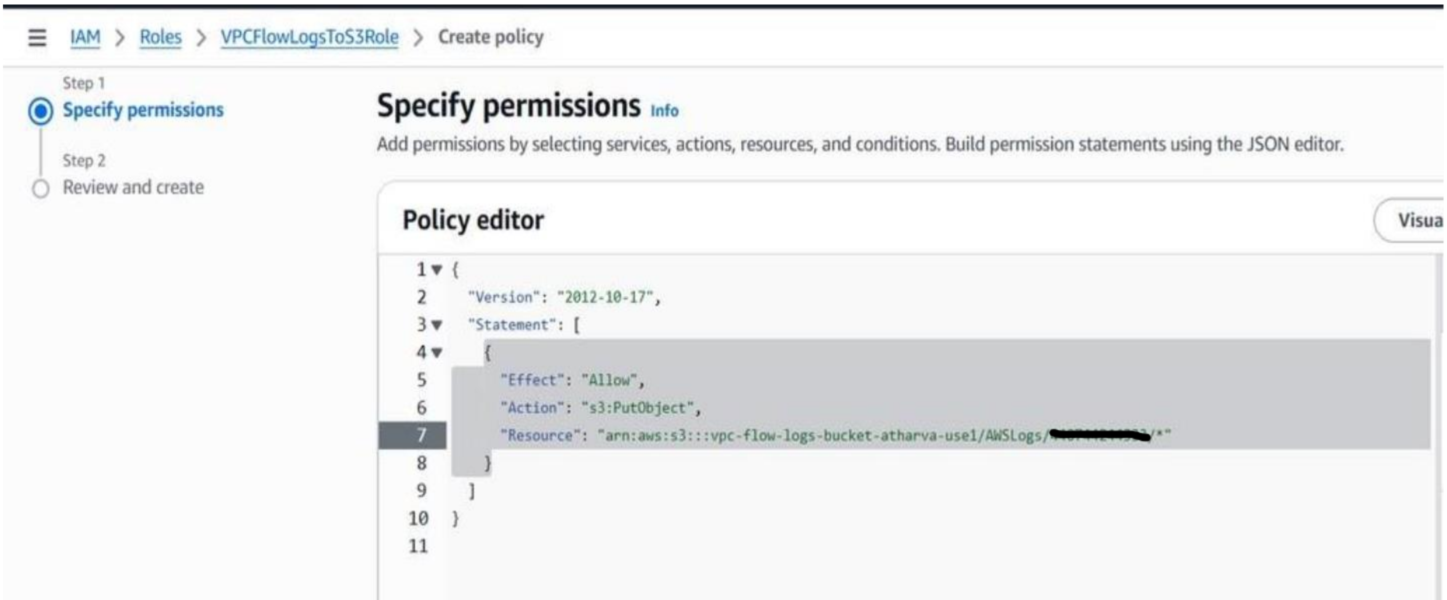


Maximum session duration
1 hour

Permissions policies (0) Info

...aged policies.

No resources to display

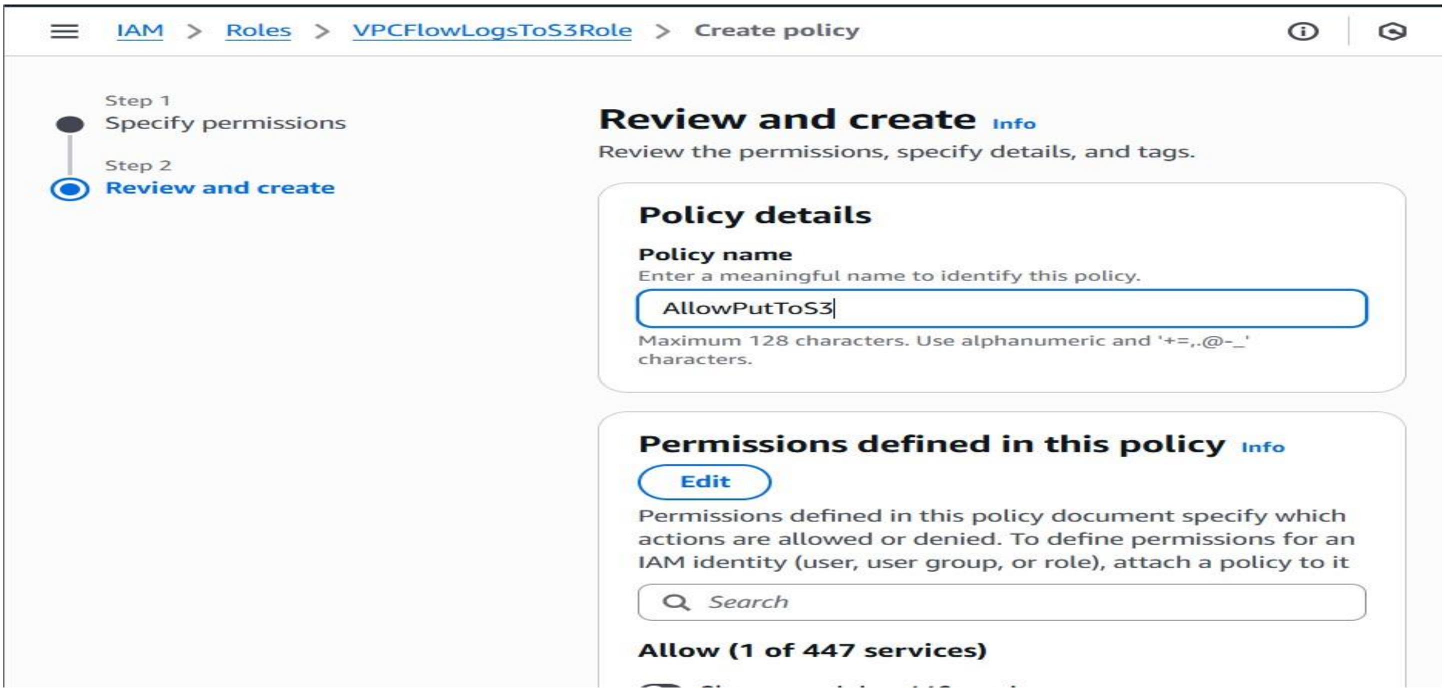


Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::vpc-flow-logs-bucket-atharva-use1/AWSLogs/[redacted]/*"
    }
  ]
}
```



Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name

Enter a meaningful name to identify this policy.

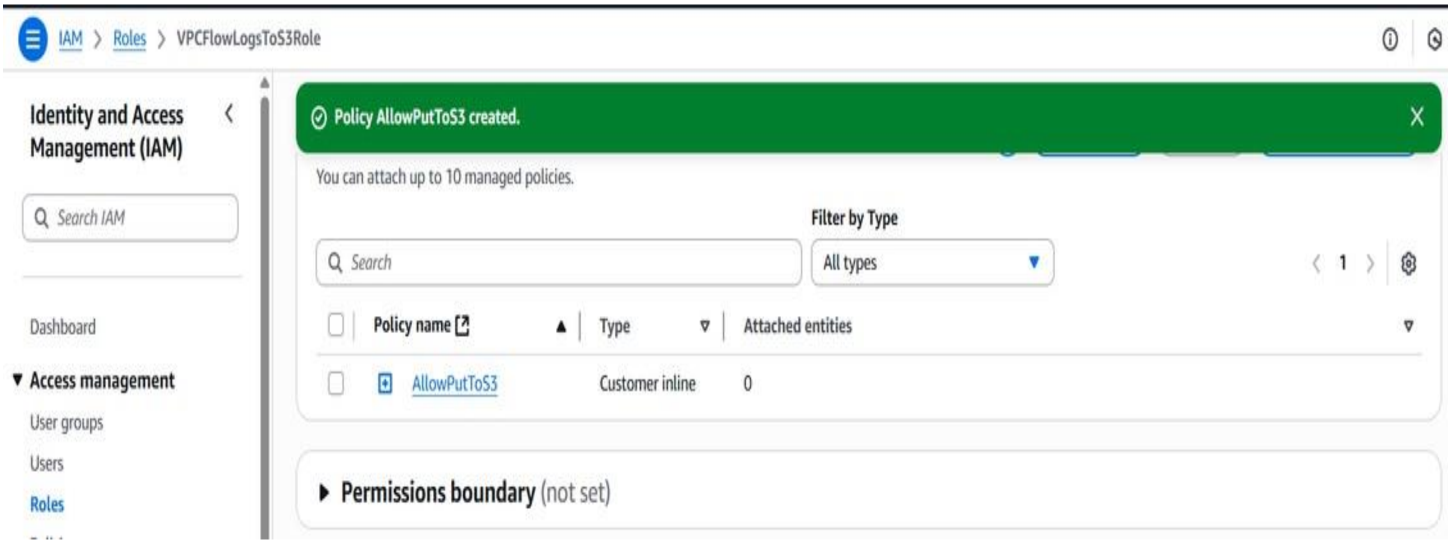
AllowPutToS3

Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 447 services)


IAM > Roles > VPCFlowLogsToS3Role
Identity and Access Management (IAM)
Search IAM
Dashboard
▼ Access management
User groups
Users
Roles

Policy AllowPutToS3 created.

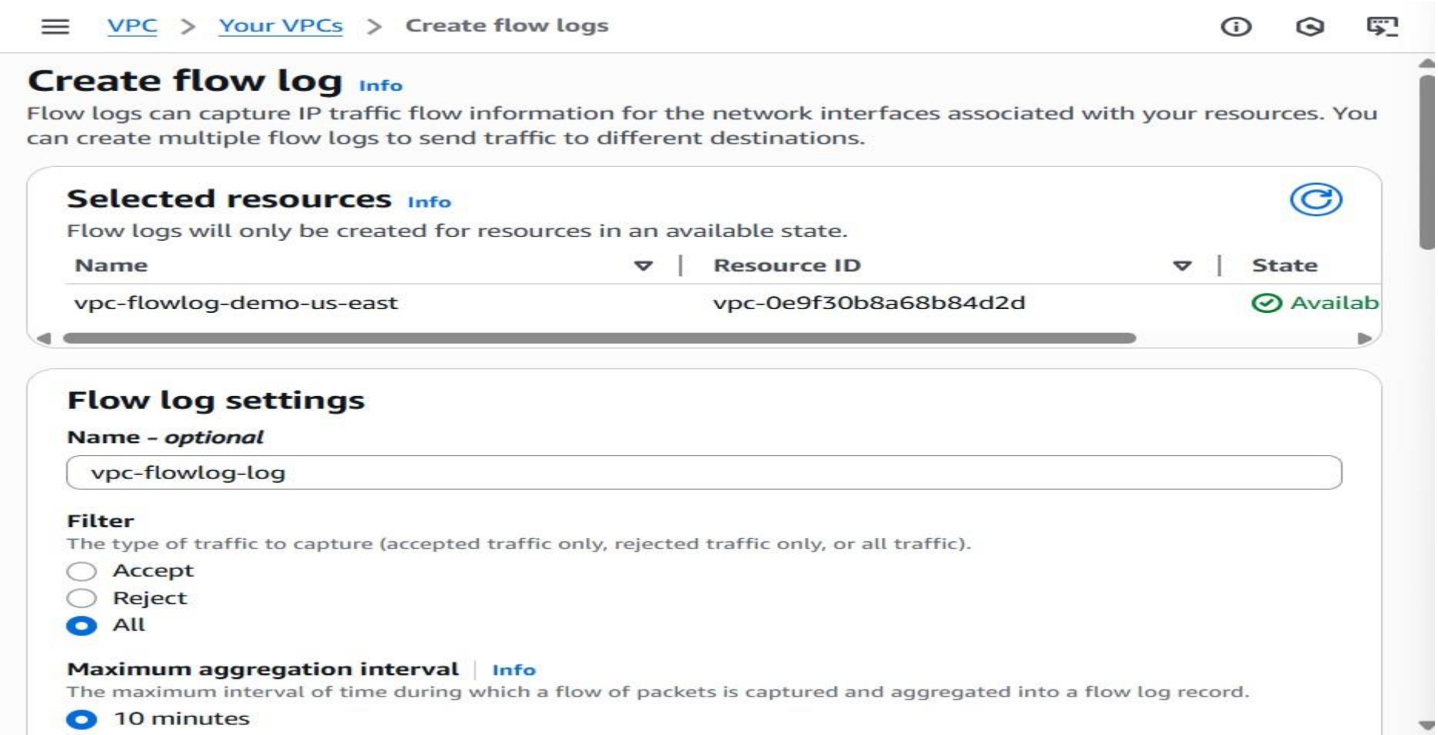
You can attach up to 10 managed policies.

□	Policy name	Type	Attached entities
□	AllowPutToS3	Customer inline	0

▸ Permissions boundary (not set)

Step 6: Enable VPC Flow Logs:

This captures traffic logs for your VPC and sends them to the S3 bucket using the role.
Go to VPC → Your VPC → Flow Logs tab → Create Flow Log.
Choose All traffic, Send to S3, select the IAM role, and provide the S3 bucket ARN.



Create flow log

Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple flow logs to send traffic to different destinations.

Selected resources

Flow logs will only be created for resources in an available state.

Name	Resource ID	State
vpc-flowlog-demo-us-east	vpc-0e9f30b8a68b84d2d	✓ Availab

Flow log settings

Name - *optional*

vpc-flowlog-log

Filter

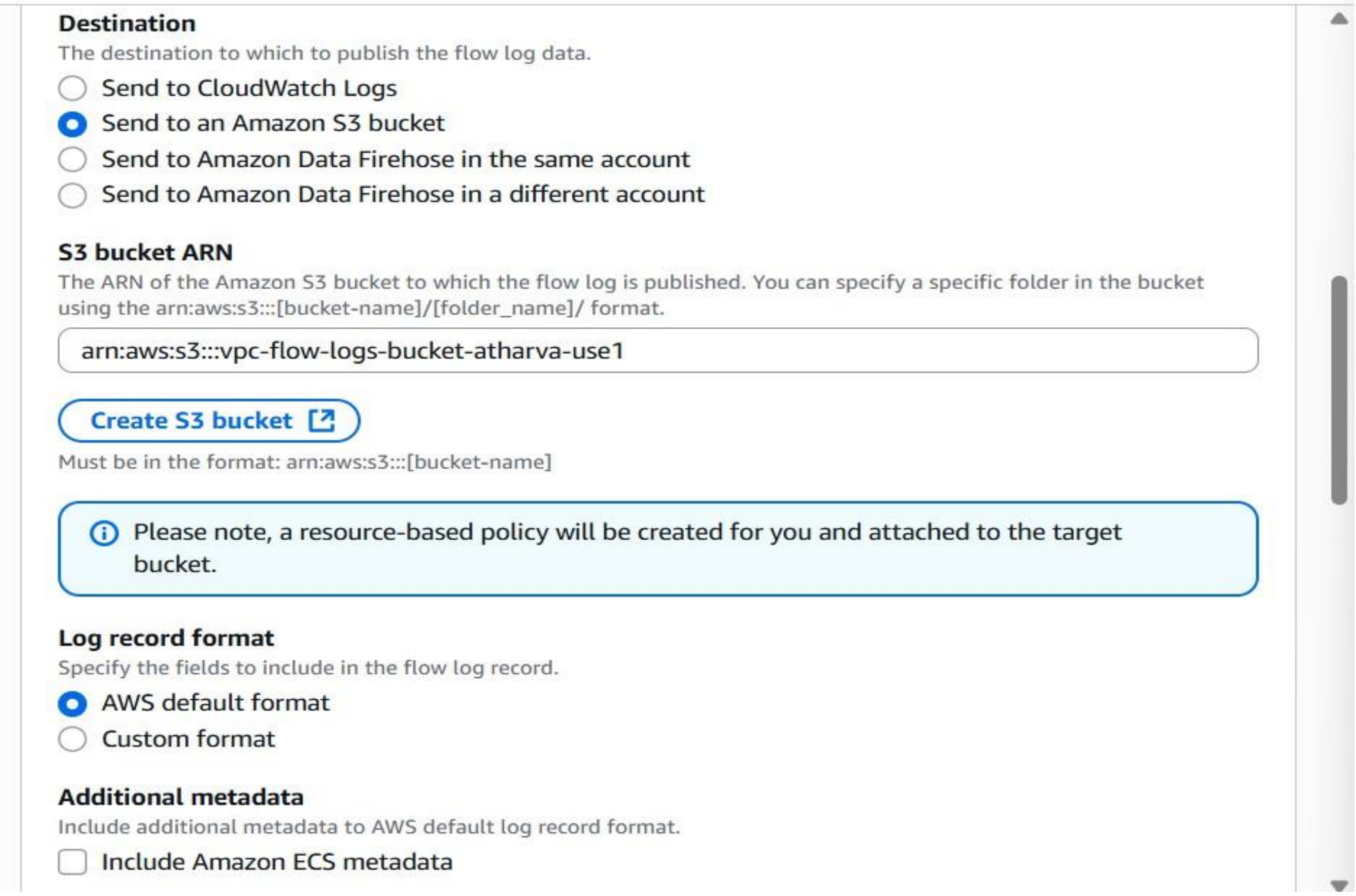
The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).

○ Accept
○ Reject
● All

Maximum aggregation interval

The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.

● 10 minutes



Destination

The destination to which to publish the flow log data.

○ Send to CloudWatch Logs
● Send to an Amazon S3 bucket
○ Send to Amazon Data Firehose in the same account
○ Send to Amazon Data Firehose in a different account

S3 bucket ARN

The ARN of the Amazon S3 bucket to which the flow log is published. You can specify a specific folder in the bucket using the arn:aws:s3:::[bucket-name]/[folder_name]/ format.

arn:aws:s3:::vpc-flow-logs-bucket-atharva-use1

Must be in the format: arn:aws:s3:::[bucket-name]

Please note, a resource-based policy will be created for you and attached to the target bucket.

Log record format

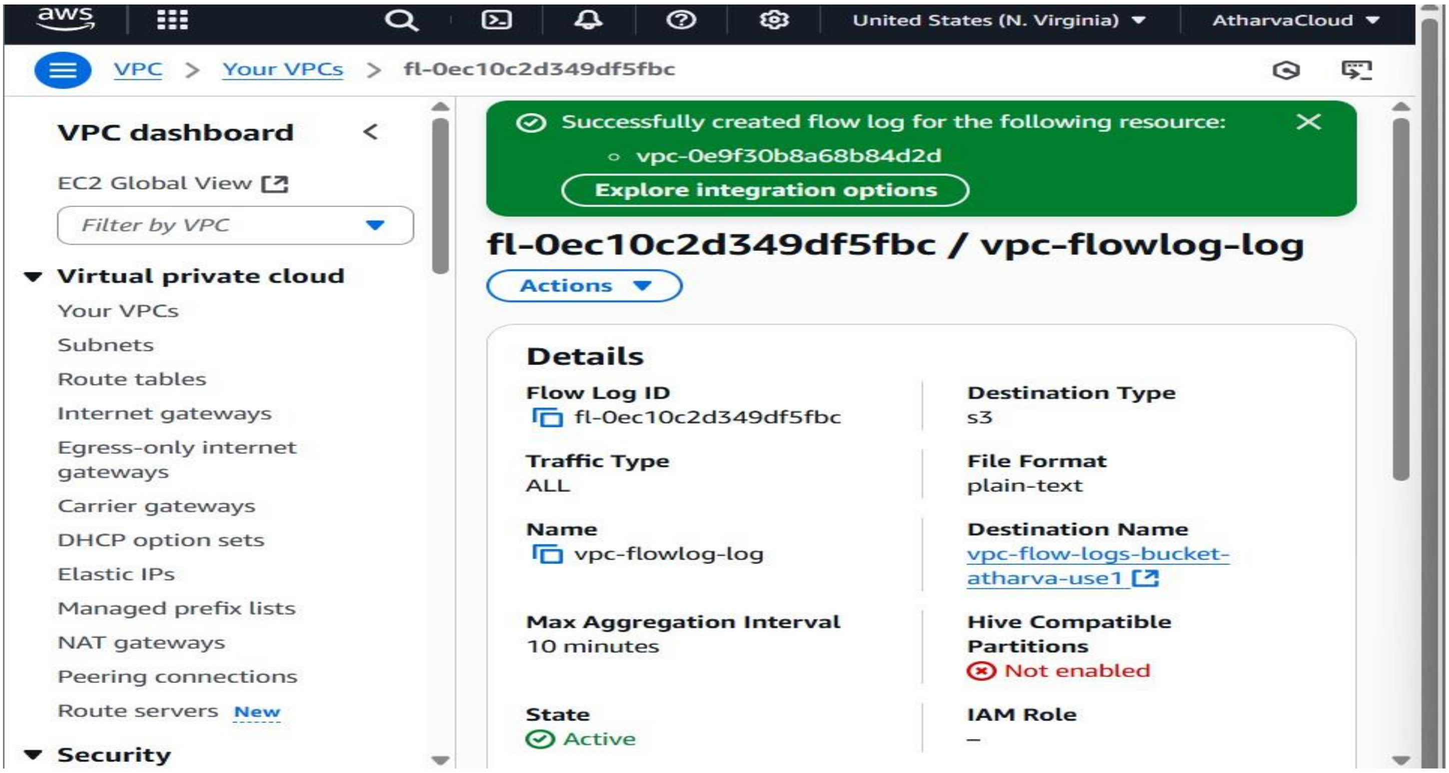
Specify the fields to include in the flow log record.

● AWS default format
○ Custom format

Additional metadata

Include additional metadata to AWS default log record format.

□ Include Amazon ECS metadata


aws
United States (N. Virginia) ▼
AtharvaCloud ▼
VPC > Your VPCs > fl-0ec10c2d349df5fbc

Successfully created flow log for the following resource:

- vpc-0e9f30b8a68b84d2d

Explore integration options

fl-0ec10c2d349df5fbc / vpc-flowlog-log

Actions ▼

Details

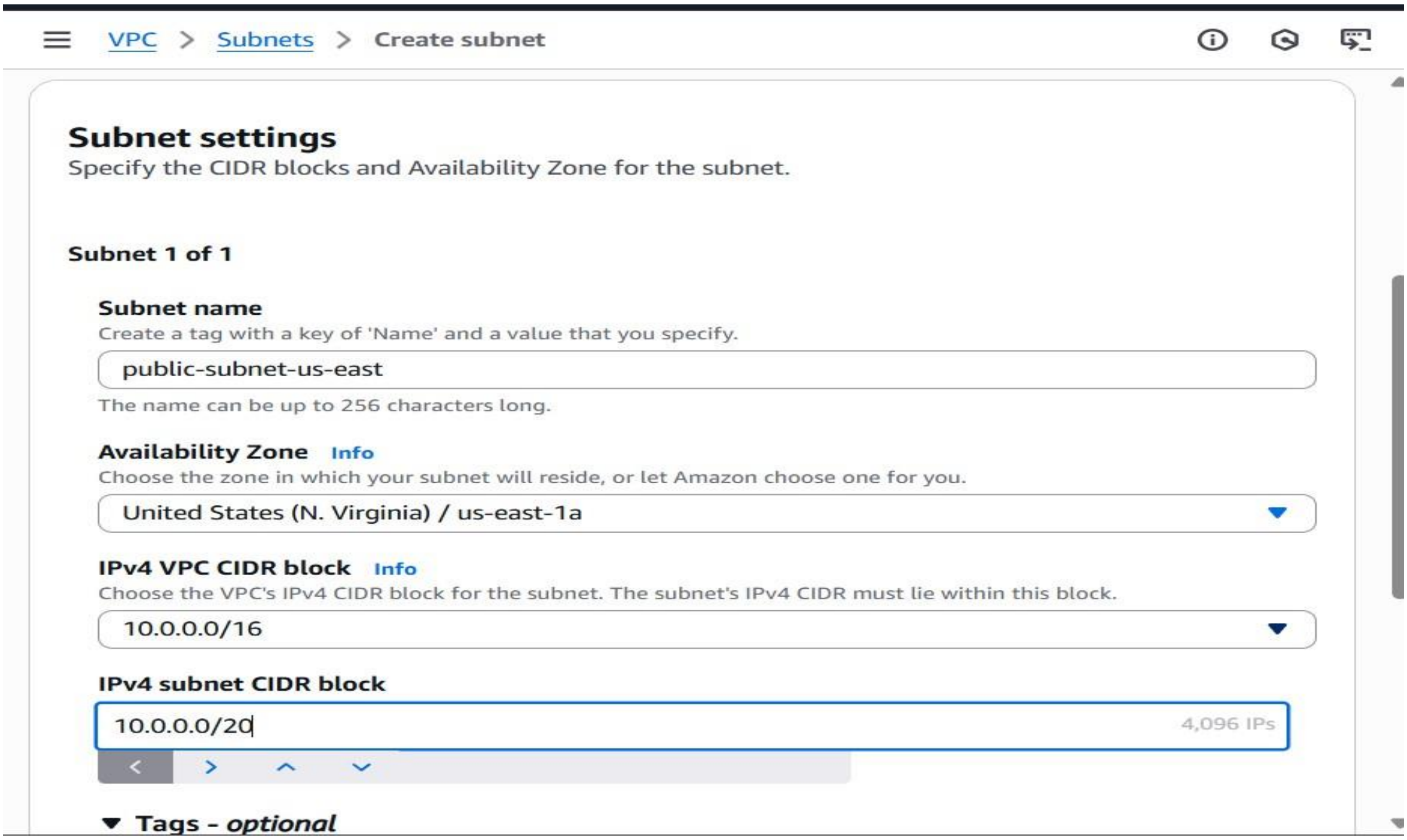
Flow Log ID fl-0ec10c2d349df5fbc	**Destination Type** s3
Traffic Type ALL	**File Format** plain-text
Name vpc-flowlog-log	**Destination Name** vpc-flow-logs-bucket-atharva-use1
Max Aggregation Interval 10 minutes	**Hive Compatible Partitions** ⊗ Not enabled
State ✓ Active	**IAM Role** –

Step 7: Launch an EC2 Instance in the VPC:

We need a virtual machine to create some real network traffic for testing.

Go to EC2 → Launch instance.

Select Amazon Linux → Choose your VPC and public subnet → Enable auto-assign public IP → Launch.



Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

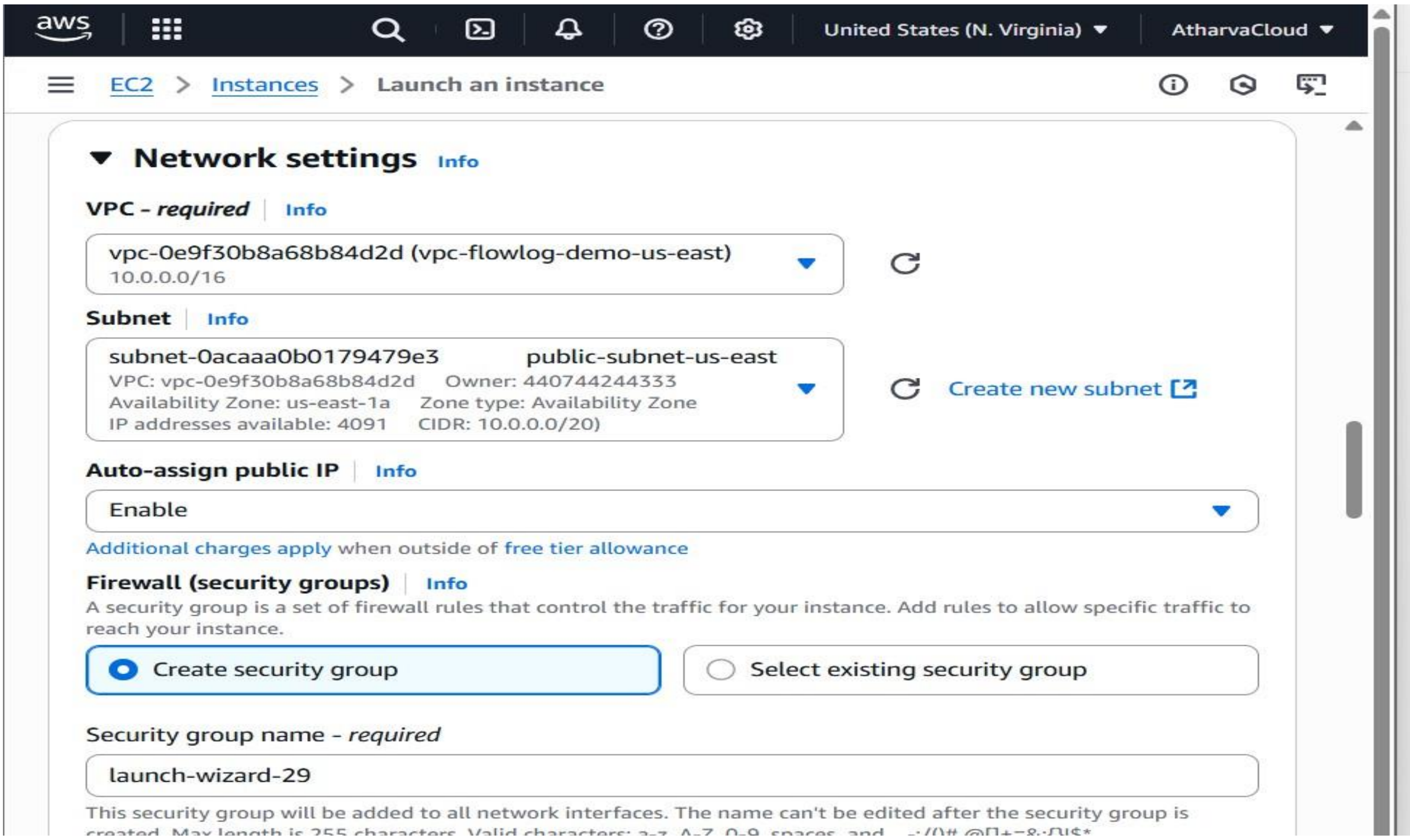
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
public-subnet-us-east
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
United States (N. Virginia) / us-east-1a

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.0.0/20 4,096 IPs

▼ Tags - *optional*



aws
United States (N. Virginia) ▼
AtharvaCloud ▼
EC2 > Instances > Launch an instance

▼ Network settings Info

VPC - *required* Info

vpc-0e9f30b8a68b84d2d (vpc-flowlog-demo-us-east)
10.0.0.0/16

Subnet Info

subnet-0acaaa0b0179479e3 public-subnet-us-east
VPC: vpc-0e9f30b8a68b84d2d Owner: 440744244333
Availability Zone: us-east-1a Zone type: Availability Zone
IP addresses available: 4091 CIDR: 10.0.0.0/20)

Create new subnet

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

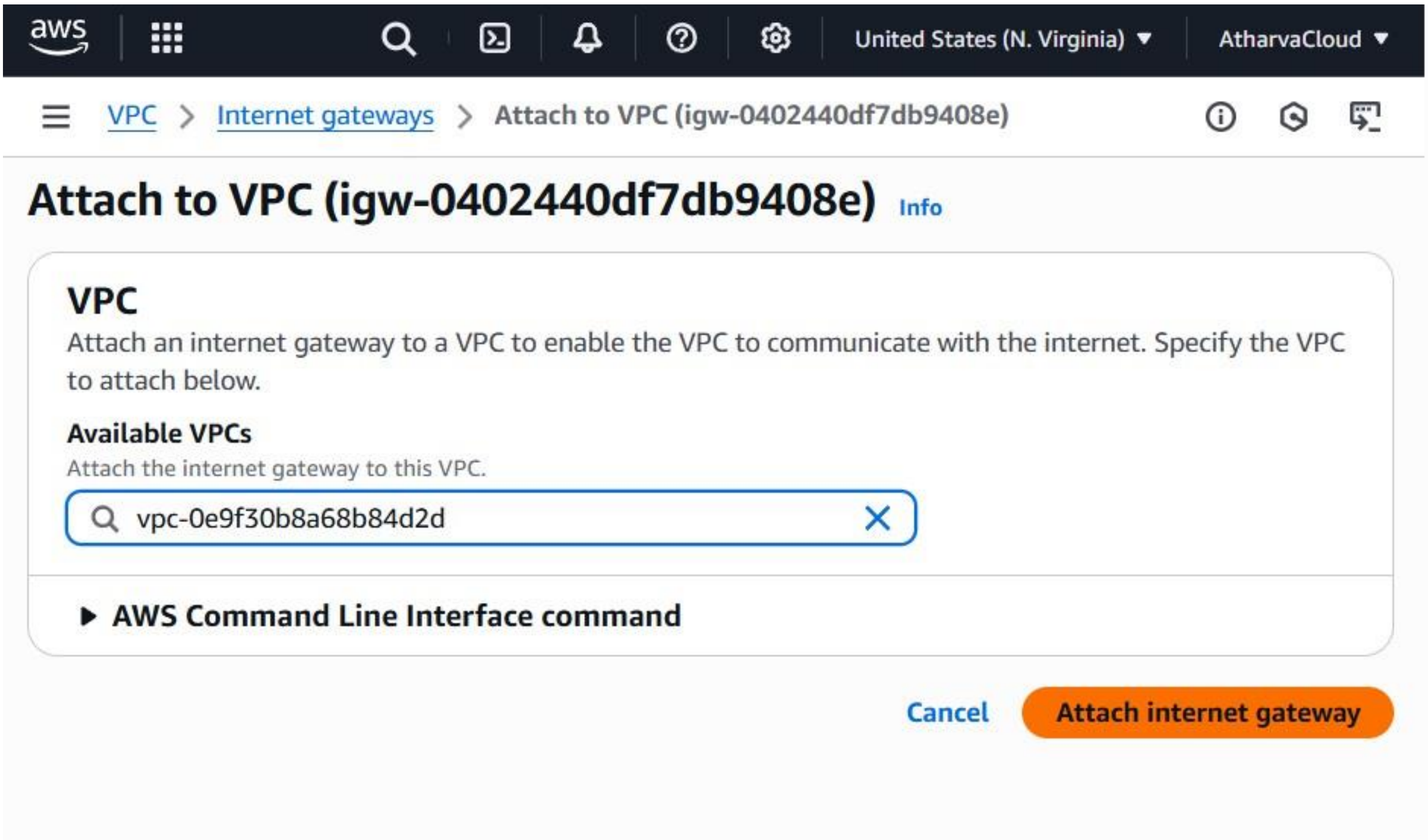
Security group name - *required*

launch-wizard-29

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Step 8: Create Internet Gateway and Update Route Table:

This allows your EC2 to access the internet (needed for pinging Google).
Create an Internet Gateway, attach it to your VPC.
Edit the route table → Add route to 0.0.0.0/0 via the IGW.
Associate the public subnet with the route table.



aws
United States (N. Virginia) ▼
AtharvaCloud ▼
VPC > Internet gateways > Attach to VPC (igw-0402440df7db9408e)

Attach to VPC (igw-0402440df7db9408e) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

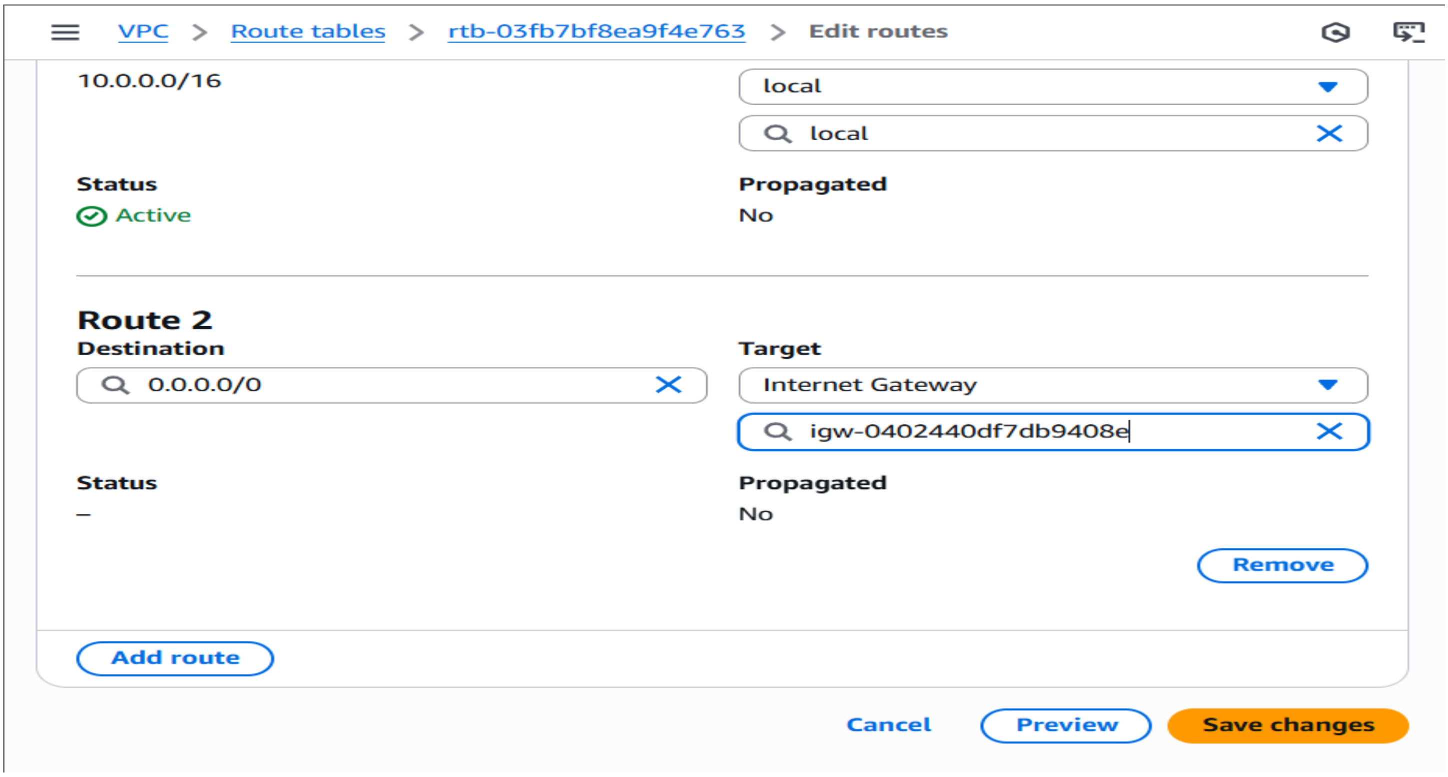
Available VPCs

Attach the internet gateway to this VPC.

vpc-0e9f30b8a68b84d2d

▶ AWS Command Line Interface command

Cancel
Attach internet gateway



VPC > Route tables > rtb-03fb7bf8ea9f4e763 > Edit routes

10.0.0.0/16

local ▼

local ✕

Status
Active

Propagated
No

Route 2

Destination
0.0.0.0/0 ✕

Target
Internet Gateway ▼

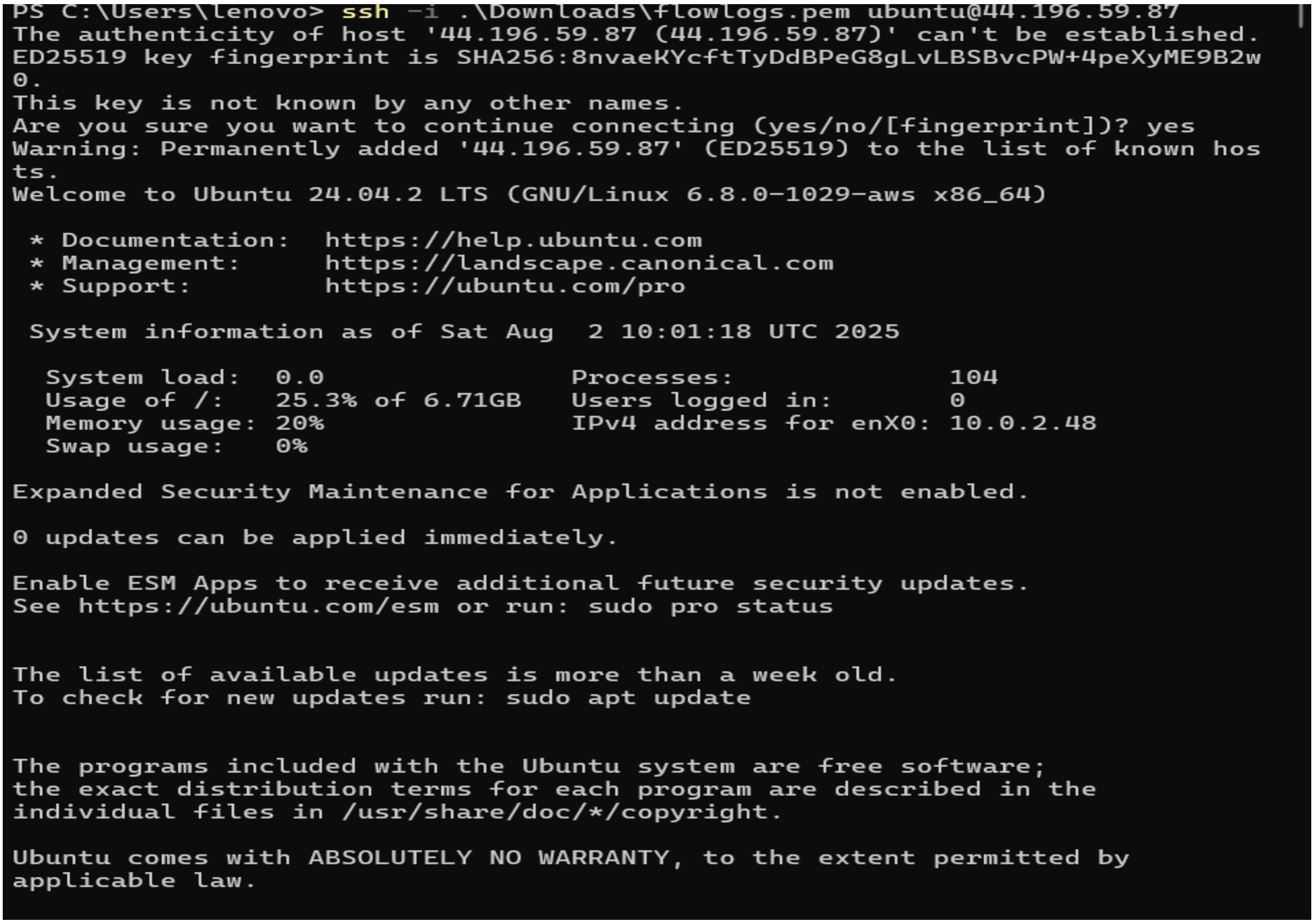
igw-0402440df7db9408e ✕

Status
–

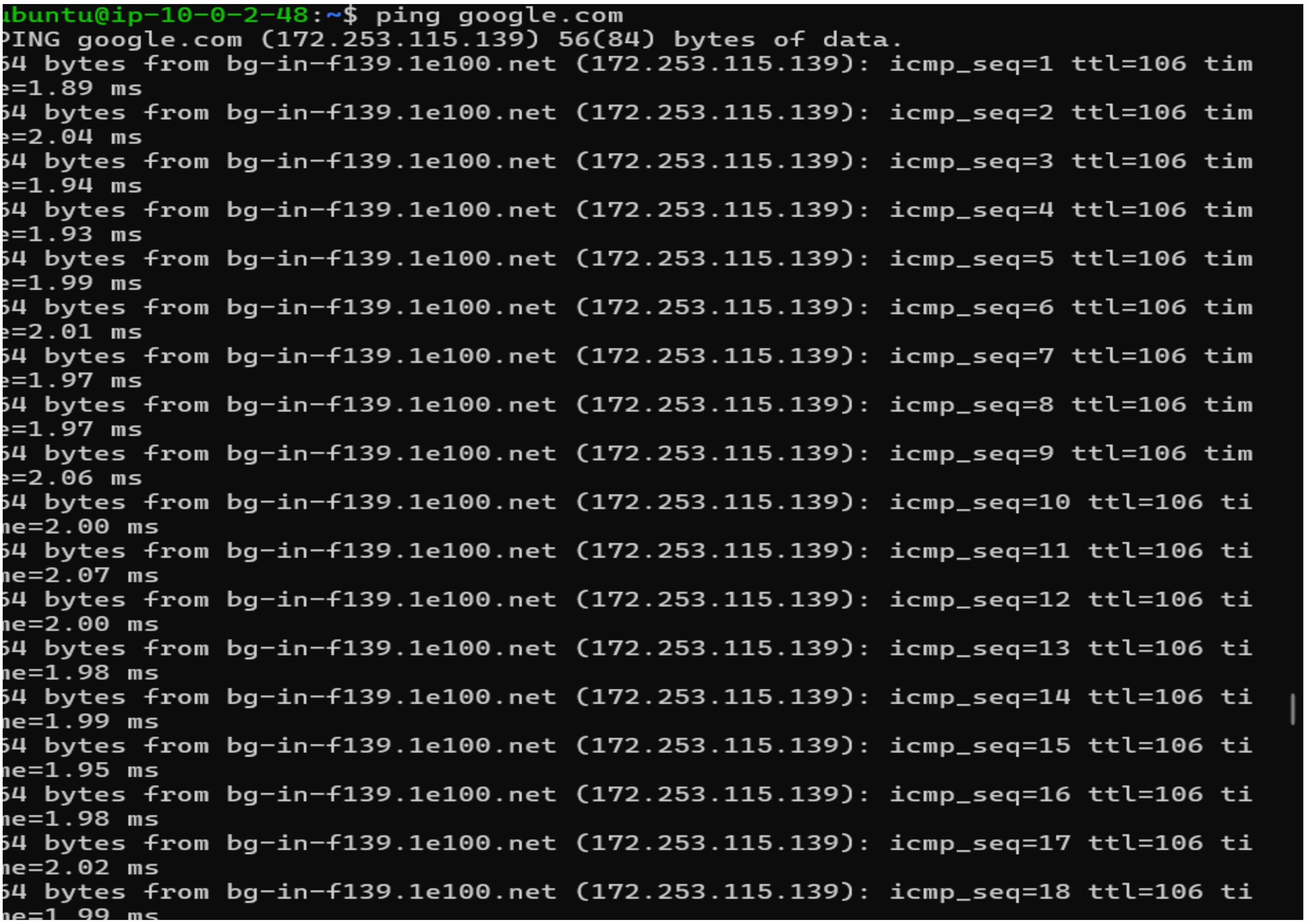
Propagated
No

Step 9: Generate Traffic Using EC2:

We test if logs are working by sending traffic (like pinging a website).
SSH into EC2 → Run this command:
ping google.com



```
PS C:\Users\lenovo> ssh -i .\Downloads\flowlogs.pem ubuntu@44.196.59.87
The authenticity of host '44.196.59.87 (44.196.59.87)' can't be established.
ED25519 key fingerprint is SHA256:8nvaeKYcftTyDdBPeG8gLvLBSBvcPW+4peXyME9B2w
0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '44.196.59.87' (ED25519) to the list of known hos
ts.
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-1029-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Sat Aug  2 10:01:18 UTC 2025

  System load:  0.0               Processes:             104
  Usage of /:   25.3% of 6.71GB   Users logged in:       0
  Memory usage: 20%               IPv4 address for enX0: 10.0.2.48
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```



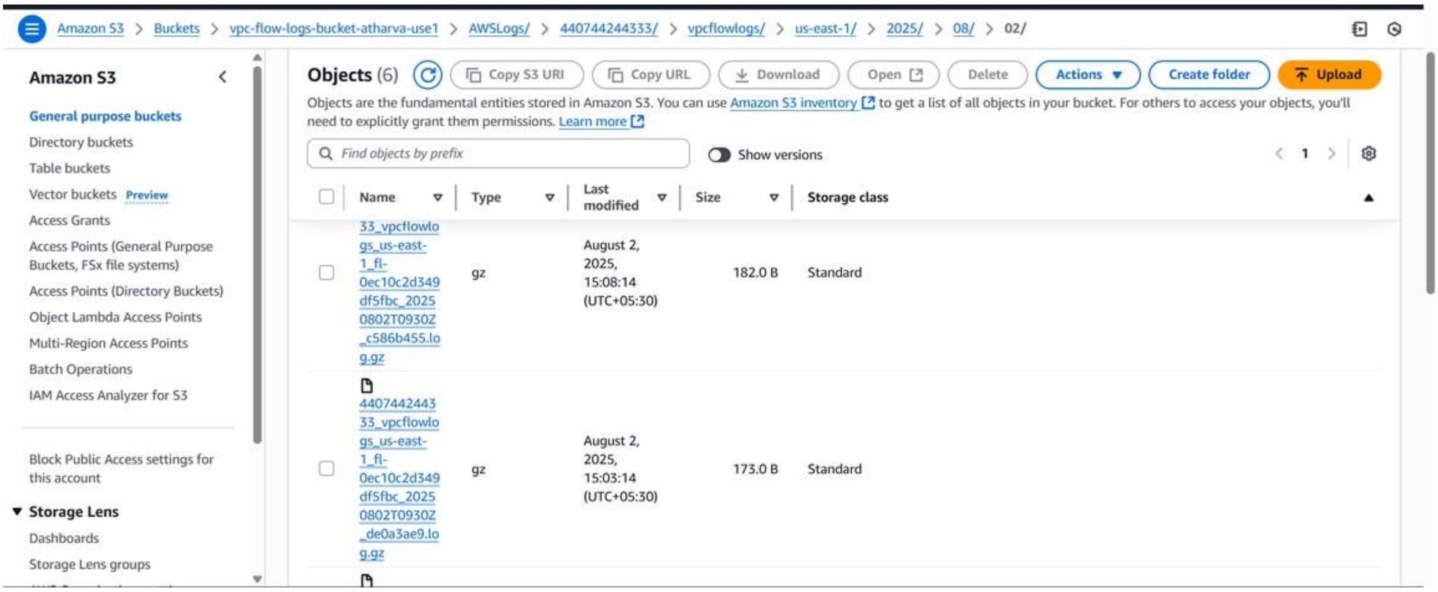
```
ubuntu@ip-10-0-2-48:~$ ping google.com
PING google.com (172.253.115.139) 56(84) bytes of data.
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=1 ttl=106 tim
e=1.89 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=2 ttl=106 tim
e=2.04 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=3 ttl=106 tim
e=1.94 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=4 ttl=106 tim
e=1.93 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=5 ttl=106 tim
e=1.99 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=6 ttl=106 tim
e=2.01 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=7 ttl=106 tim
e=1.97 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=8 ttl=106 tim
e=1.97 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=9 ttl=106 tim
e=2.06 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=10 ttl=106 ti
me=2.00 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=11 ttl=106 ti
me=2.07 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=12 ttl=106 ti
me=2.00 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=13 ttl=106 ti
me=1.98 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=14 ttl=106 ti
me=1.99 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=15 ttl=106 ti
me=1.95 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=16 ttl=106 ti
me=1.98 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=17 ttl=106 ti
me=2.02 ms
64 bytes from bg-in-f139.1e100.net (172.253.115.139): icmp_seq=18 ttl=106 ti
me=1.99 ms
```

Step 10: Check Logs in S3:

To confirm that traffic logs are being captured and saved in the bucket.

Go to S3 → Your bucket → AWSLogs folder

Open folders by account ID → region → date → Download log file and open.



Amazon S3 > Buckets > vpc-flow-logs-bucket-atharva-use1 > AWSLogs/ > 440744244333/ > vpcflowlogs/ > us-east-1/ > 2025/ > 08/ > 02/

Objects (6)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

	Name	Type	Last modified	Size	Storage class
□	33_vpcflowlogs_us-east-1_fl-0ec10c2d349df5fbc_20250802T0930Z_c586b455.log.gz	gz	August 2, 2025, 15:08:14 (UTC+05:30)	182.0 B	Standard
□	440744244333_vpcflowlogs_us-east-1_fl-0ec10c2d349df5fbc_20250802T0930Z_de0a3ae9.log.gz	gz	August 2, 2025, 15:03:14 (UTC+05:30)	173.0 B	Standard

SUMMARY:

This project helped me build a complete logging setup on AWS. I created a private network (VPC), set up a storage location (S3), and configured secure access using an IAM Role. I then enabled VPC Flow Logs to capture network traffic and launched an EC2 instance to generate some real traffic. Finally, I confirmed that the traffic logs were successfully delivered to my S3 bucket. Now I have a working system to monitor AWS network activity securely and efficiently.