

## Guided Lab: Capture network traffic information with VPC flow logs to Amazon S3 Bucket

### Description

Monitoring the traffic flowing through your VPC is essential for analyzing security and performance. AWS VPC Flow Logs can capture details about IP traffic going to and from your network interfaces. You can publish these logs to Amazon S3 for further analysis or archiving.

In this lab, you will learn how to create a VPC Flow Log that captures network traffic information and publishes it to Amazon S3 for long-term storage.

### Prerequisites

This lab assumes basic knowledge of AWS networks and core services such as EC2, S3, and VPC.

If you're unfamiliar with these services, consider exploring the following resources:

- Creating an Amazon EC2 instance (Linux)
- Creating a Custom Virtual Private Cloud (VPC) from scratch
- Guided Lab: Creating an Amazon S3 bucket
- Capture network traffic information with VPC flow logs to CloudWatch Logs

### Objectives

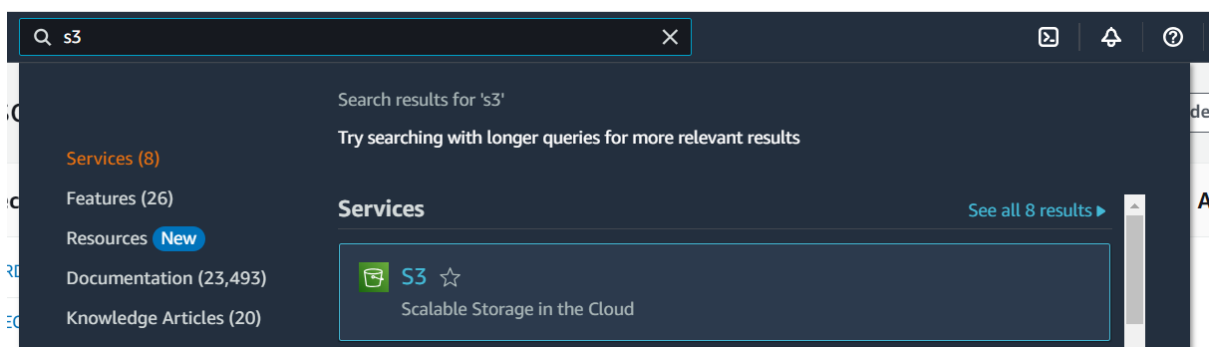
By the end of this lab, participants will be able to:

- Set up an Amazon S3 bucket to store VPC Flow Log data.
- Create and configure VPC Flow Logs to capture IP traffic and publish logs to Amazon S3.
- Verify the flow logs by generating and reviewing network traffic data stored in S3.

### Lab Steps

#### Set up an Amazon S3 Bucket

1. Navigate to the S3 Console:



2. Create a New Bucket:

- Click the "Create bucket" button. Fill in the following details:

- **Bucket Name:**myflowlogsbucket3000
- Click **Create Bucket** to finalize the setup.

Amazon S3

► **Account snapshot - updated every 24 hours** All AWS Regions View Storage Lens dashboard

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

**General purpose buckets** | Directory buckets

**General purpose buckets (1)** Info All AWS Regions

Refresh Copy ARN Empty Delete Create bucket

Buckets are containers for data stored in S3.

< 1 > Settings

|                       | Name                                 | AWS Region                      | IAM Access Analyzer                         | Creation date                            |
|-----------------------|--------------------------------------|---------------------------------|---|--|
| <input type="radio"/> | <a href="#">myflowlogsbucket3000</a> | US East (N. Virginia) us-east-1 | <a href="#">View analyzer for us-east-1</a> | September 17, 2024, 15:46:35 (UTC+08:00) |


3. Take note of the **Amazon Resource Name (ARN)** of your S3 bucket.

[Amazon S3](#) > [Buckets](#) > myflowlogsbucket3000

**myflowlogsbucket3000** Info

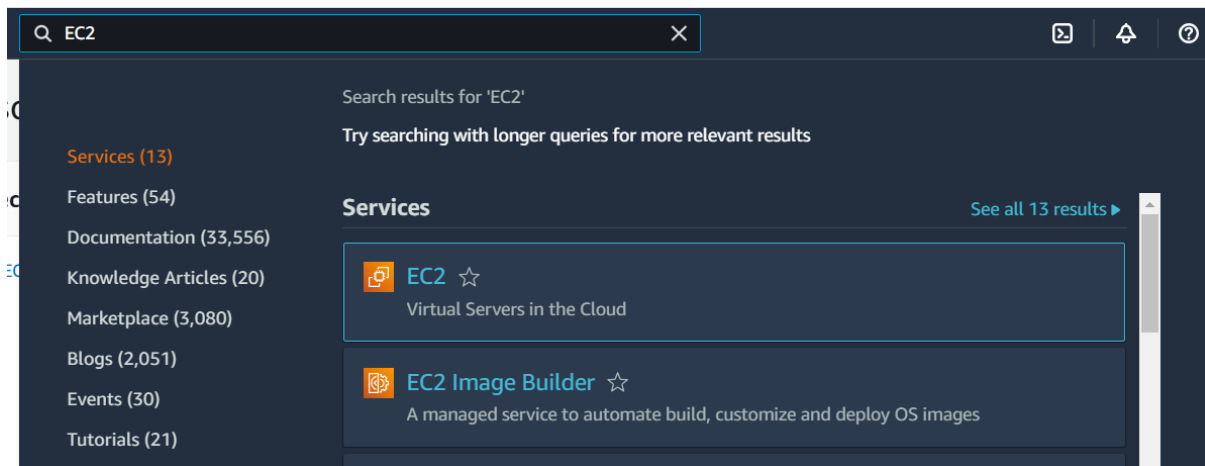
**Objects** | **Properties** | Permissions | Metrics | Management | Access Points

**Bucket overview**

|   |   |   |
|---|---|---|
| AWS Region<br>US East (N. Virginia) us-east-1 | <b>Amazon Resource Name (ARN)</b><br> <code>arn:aws:s3:::myflowlogsbucket3000</code> | Creation date<br>September 17, 2024, 15:46:35 (UTC+08:00) |
|---|---|---|

## Launch an EC2 Instance

1. Navigate to the EC2 Dashboard



## 2. Launch an EC2 Instance using the following configurations:

- Name: **MyWebServer**
- AMI: **Amazon Linux**
- Instance type: **t2.micro**
- Key pair: (**Please create a new one.**)
  - Key pair name: **myKeyPair**
  - Key pair type: **RSA**
  - Private key file format: **.pem**
- Network settings: (Click **“Create security group”**)
  - Auto-assign public IP: Select **Enable**
  - Firewall (security groups): tick on the **Create security group**
  - Ensure that **Allow SSH traffic from** is **checked** and is **My IP**

▼ Network settings

Info

Edit

Network

Info

vpc-065e6cebb3e8814ed

Subnet

Info

subnet-0f3d02a8f7918ce45

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

We'll create a new security group called 'launch-wizard-2' with the following rules:

☒ Allow SSH traffic from
 

Helps you connect to your instance

My IP

119.111.230.25/32

☐ Allow HTTPS traffic from the Internet
 

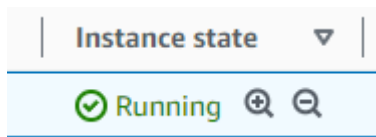
To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet
 

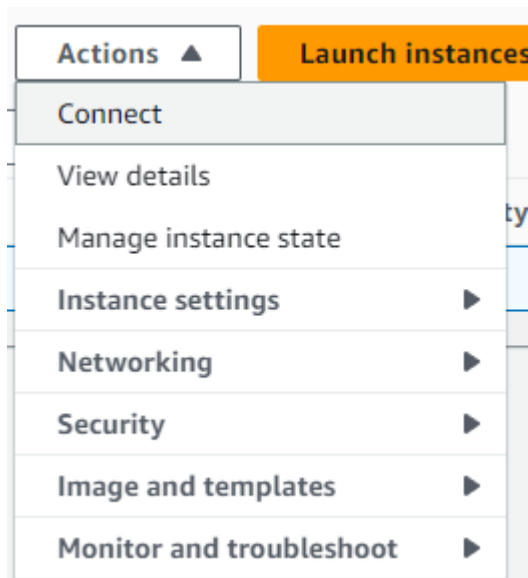
To set up an endpoint, for example when creating a web server

- Click Launch Instance.

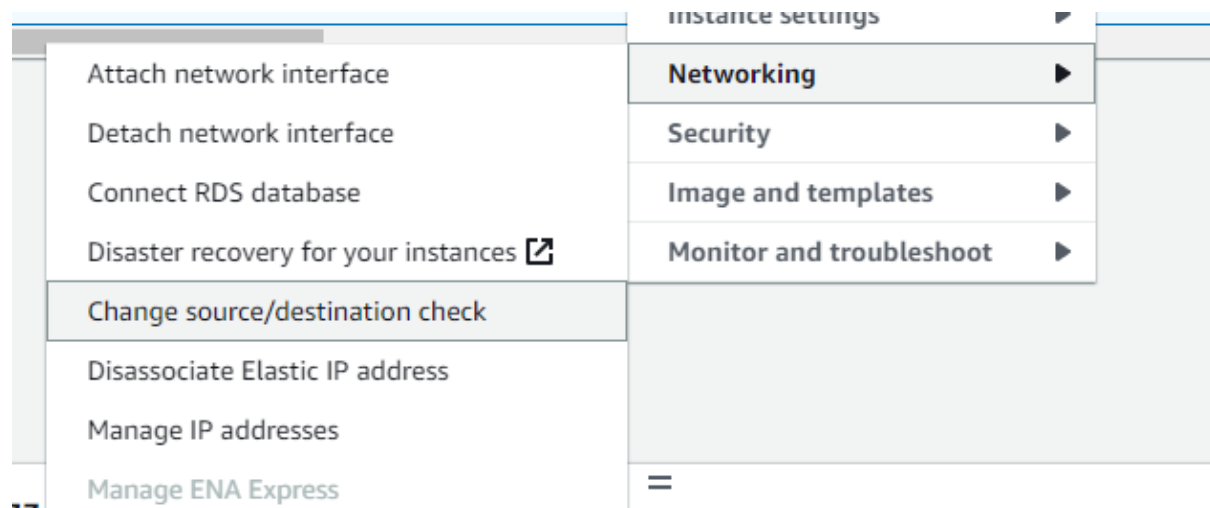
3. Wait for the EC2 instance to be in the **Running** state.



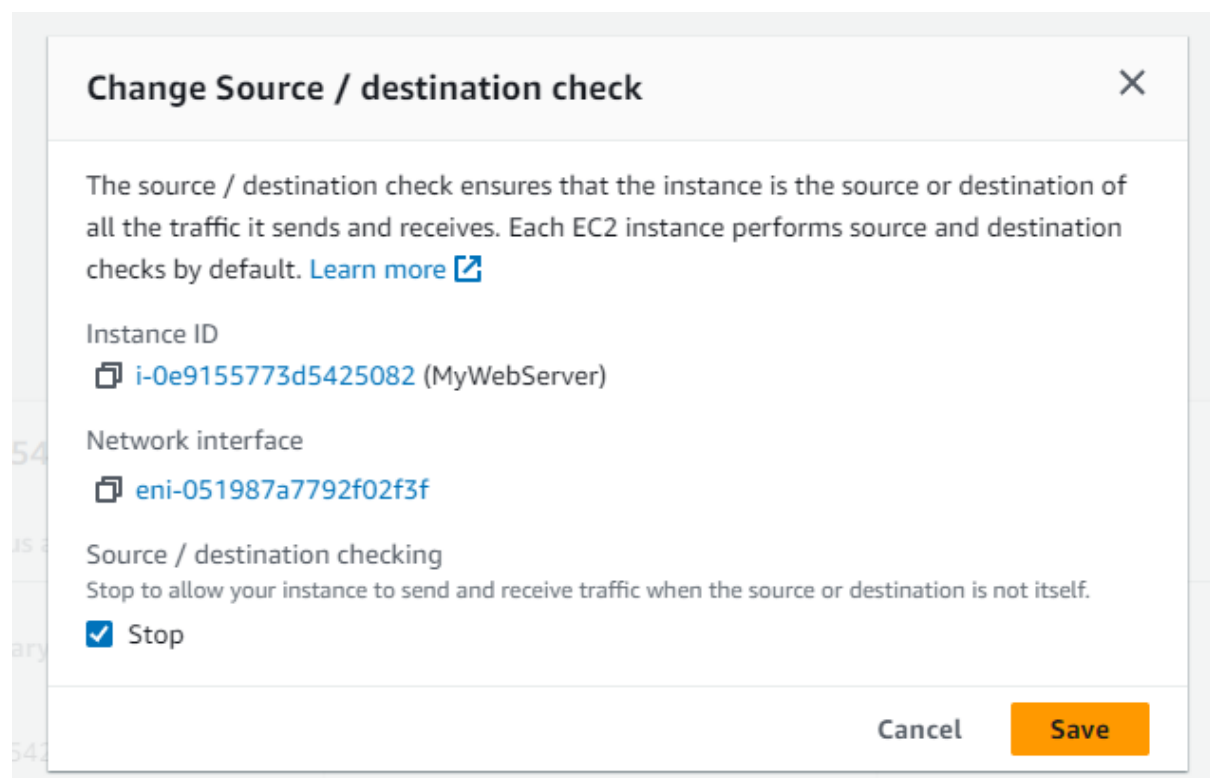
4. Select the instance and click on the Actions dropdown.



5. Navigate on **Networking > Change source/destination check**



6. Tick the stop checkbox and **Save**

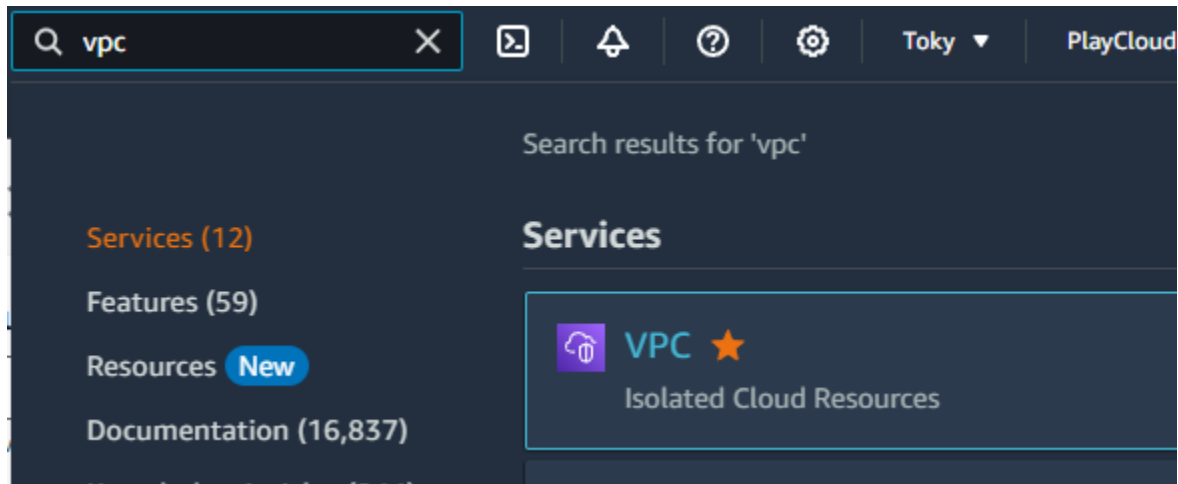


The **Source/Destination Check** in an EC2 instance is a network setting that controls whether the instance must be the source or destination of traffic it sends or receives.

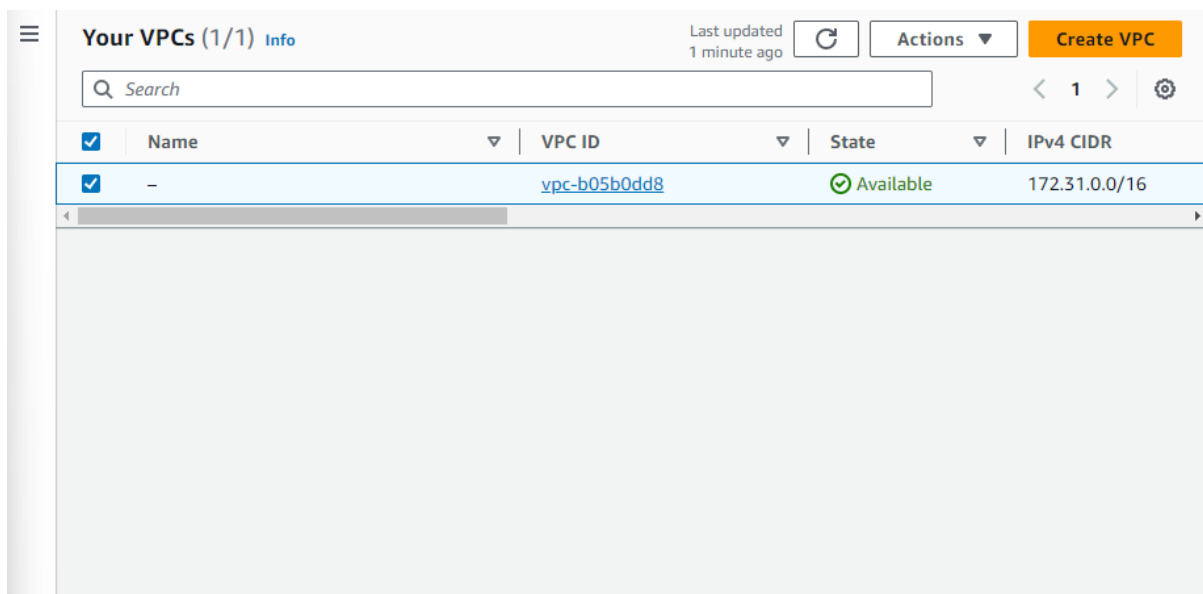
- **Enabled** (default): The instance only accepts traffic addressed to its own IP. This is when **Stop checkbox** is unchecked.
- **Disabled**: The instance can forward traffic, useful for NAT, routing, or firewall role. This is when **Stop checkbox** is checked.

## Create a VPC Flow Log for S3

1. Navigate to the VPC Dashboard.



2. In the left navigation pane, click **VPC** and select the VPC where your EC2 instance is running. In this lab, we choose the default VPC.



### 3. Create a Flow Log:

- Click **Actions** and select **Create flow log**.
- **Name:** my-flow-log-to-s3
- **Filter:** AllMaximum **Aggregation Interval:** 1 minute
- **Destination:** Select **Send to an S3 bucket**.
- **S3 Bucket ARN:** Enter the ARN for your S3 bucket, e.g., arn:aws:s3:::myflowlogsbucket3000.

## Flow log settings

Name - *optional*

my-flow-log-to-s3

### Filter

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

- ☐ Accept
- ☐ Reject
- ☒ All

### Maximum aggregation interval [Info](#)

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

- ☒ 10 minutes
- ☐ 1 minute

### 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 bucket\_ARN/folder\_name/ format. [Create S3 bucket](#)

arn:aws:s3:::myflowlogsbucket3000

4. Click **Create Flow Log** to complete the configuration.

## Generate Network Traffic and Verify Flow Logs

1. To generate network traffic, SSH into your EC2 instance and run the ping command to any website. For example:

```
ping google.com
```

```
neil@Sol MINGW64 ~
$ cd Downloads/

neil@Sol MINGW64 ~/Downloads
$ ssh -i "myKeyPair.pem" ec2-user@ec2-3-208-2-83.compute-1.amazonaws.com
The authenticity of host 'ec2-3-208-2-83.compute-1.amazonaws.com (3.208.2.83)'
can't be established.
ED25519 key fingerprint is SHA256:Wmc1Wq94/aKXtbt3iOHU/1oNunC5TM8gKFXjawqOJ/U.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-3-208-2-83.compute-1.amazonaws.com' (ED25519) to
the list of known hosts.

      #_
     _/ \_   #####_   Amazon Linux 2023
    ~~~~~ \_   ##### \
    ~~~~~  \_   #### |
    ~~~~~   \_   #/  ___  https://aws.amazon.com/linux/amazon-linux-2023
    ~~~~~    V~' ' ->
    ~~~~~   _/ \_   /
    ~~~~~  _/ \_   /
    ~~~~~ _/m/'   /

[ec2-user@ip-192-168-5-10 ~]$ ping google.com
PING google.com (172.253.122.138) 56(84) bytes of data.
64 bytes from bh-in-f138.1e100.net (172.253.122.138): icmp_seq=1 ttl=58 time=2.35 ms
64 bytes from bh-in-f138.1e100.net (172.253.122.138): icmp_seq=2 ttl=58 time=2.73 ms
64 bytes from bh-in-f138.1e100.net (172.253.122.138): icmp_seq=3 ttl=58 time=2.82 ms
64 bytes from bh-in-f138.1e100.net (172.253.122.138): icmp_seq=4 ttl=58 time=3.04 ms
64 bytes from bh-in-f138.1e100.net (172.253.122.138): icmp_seq=5 ttl=58 time=3.23 ms
64 bytes from bh-in-f138.1e100.net (172.253.122.138): icmp_seq=6 ttl=58 time=2.63 ms
64 bytes from bh-in-f138.1e100.net (172.253.122.138): icmp_seq=7 ttl=58 time=2.57 ms
64 bytes from bh-in-f138.1e100.net (172.253.122.138): icmp_seq=8 ttl=58 time=2.19 ms
64 bytes from bh-in-f138.1e100.net (172.253.122.138): icmp_seq=9 ttl=58 time=2.15 ms
64 bytes from bh-in-f138.1e100.net (172.253.122.138): icmp_seq=10 ttl=58 time=2.32 ms
```


## 2. Review the Logs in S3:

- Navigate to your bucket and check for the presence of log files. The logs will be stored in a path similar to the image below.



[Amazon S3](#) > [Buckets](#) > [myflowlogsbucket3000](#) > [AWSLogs/](#) > [533267275577/](#) > [vpcflowlogs/](#) > [us-east-1/](#) > [2024/](#) > [09/](#) > [17/](#)

17/


 Copy S3 URI


Objects

Properties

## Objects (15) [Info](#)



 Copy S3 URI

 Copy URL

 Download

Open 


Delete

Actions ▼



Create folder

 Upload

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](#)

 Find objects by prefix

< 1 > 

| <input type="checkbox"/> | Name ▲  | Type ▼ | Last modified ▼                          | Size ▼  | Storage class ▼ |
|--------------------------|---|--------|--|---------|-----------------|
| <input type="checkbox"/> | <br><a href="#">533267275577_vpcflowlogs_us-east-1_fl-0373cddea209dbc2f_20240917T0745Z_2ab0b83b.log.gz</a>   | gz     | September 17, 2024, 15:51:55 (UTC+08:00) | 627.0 B | Standard        |
| <input type="checkbox"/> | <br><a href="#">533267275577_vpcflowlogs_us-east-1_fl-0373cddea209dbc2f_20240917T0745Z_2ab0b83b.log.gz</a> | gz     | September 17, 2024, 15:51:55 (UTC+08:00) | 489.0 B | Standard        |

3. Download one of the files and check.

```

version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status
2 533267275577 eni-051987a7792f02f3f 35.203.210.246 192.168.5.10 52912 9567 6 1 44 1726559226 1726559290 REJECT OK
2 533267275577 eni-051987a7792f02f3f 45.84.89.3 192.168.5.10 61847 135 6 1 52 1726559226 1726559290 REJECT OK
2 533267275577 eni-051987a7792f02f3f 147.185.132.95 192.168.5.10 54013 48530 6 1 44 1726559226 1726559290 REJECT OK
2 533267275577 eni-051987a7792f02f3f 35.203.211.194 192.168.5.10 51581 7078 6 1 44 1726559226 1726559290 REJECT OK
2 533267275577 eni-051987a7792f02f3f 162.216.149.144 192.168.5.10 57182 9974 6 1 44 1726559226 1726559290 REJECT OK
2 533267275577 eni-051987a7792f02f3f 147.185.133.157 192.168.5.10 54330 9639 6 1 44 1726559226 1726559290 REJECT OK
2 533267275577 eni-051987a7792f02f3f 3.87.127.143 192.168.5.10 123 38054 17 1 76 1726559226 1726559290 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 192.168.5.10 3.87.127.143 38054 123 17 1 76 1726559226 1726559290 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 44.201.148.133 192.168.5.10 123 58761 17 1 76 1726559226 1726559290 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 192.168.5.10 44.201.148.133 58761 123 17 1 76 1726559226 1726559290 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 162.216.149.10 192.168.5.10 51394 11112 6 1 44 1726559226 1726559290 REJECT OK
2 533267275577 eni-051987a7792f02f3f 54.210.225.137 192.168.5.10 123 56591 17 1 76 1726559226 1726559290 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 192.168.5.10 54.210.225.137 56591 123 17 1 76 1726559226 1726559290 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 104.248.234.153 192.168.5.10 80 5601 6 1 44 1726559264 1726559301 REJECT OK
2 533267275577 eni-051987a7792f02f3f 45.56.84.110 192.168.5.10 37294 222 6 1 44 1726559264 1726559301 REJECT OK
2 533267275577 eni-051987a7792f02f3f 205.210.31.26 192.168.5.10 53837 4016 6 1 44 1726559264 1726559301 REJECT OK
2 533267275577 eni-051987a7792f02f3f 54.81.127.33 192.168.5.10 123 41550 17 1 76 1726559289 1726559331 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 192.168.5.10 54.81.127.33 41550 123 17 1 76 1726559289 1726559331 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 162.216.149.120 192.168.5.10 50634 9937 6 1 44 1726559289 1726559331 REJECT OK
2 533267275577 eni-051987a7792f02f3f 44.201.148.133 192.168.5.10 123 57312 17 1 76 1726559289 1726559331 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 192.168.5.10 44.201.148.133 57312 123 17 1 76 1726559289 1726559331 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 3.87.127.143 192.168.5.10 123 56713 17 1 76 1726559289 1726559331 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 192.168.5.10 3.87.127.143 56713 123 17 1 76 1726559289 1726559331 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 35.203.210.129 192.168.5.10 53234 9636 6 1 44 1726559323 1726559356 REJECT OK
2 533267275577 eni-051987a7792f02f3f 85.209.11.71 192.168.5.10 46286 1032 6 1 40 1726559323 1726559356 REJECT OK
2 533267275577 eni-051987a7792f02f3f 45.93.20.104 192.168.5.10 46497 1700 6 1 40 1726559323 1726559356 REJECT OK
2 533267275577 eni-051987a7792f02f3f 54.81.127.33 192.168.5.10 123 51659 17 1 76 1726559323 1726559356 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 192.168.5.10 54.81.127.33 51659 123 17 1 76 1726559323 1726559356 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 54.210.225.137 192.168.5.10 123 40966 17 1 76 1726559323 1726559356 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 192.168.5.10 54.210.225.137 40966 123 17 1 76 1726559323 1726559356 ACCEPT OK
2 533267275577 eni-051987a7792f02f3f 35.203.210.177 192.168.5.10 50587 52212 6 1 44 1726559323 1726559356 REJECT OK
2 533267275577 eni-051987a7792f02f3f 198.235.24.22 192.168.5.10 53863 20256 6 1 44 1726559323 1726559356 REJECT OK

```

Congratulations! You have successfully created a VPC Flow Log that publishes logs to Amazon S3. With this setup, you can retain logs long-term for compliance, auditing, or in-depth analysis. This solution provides visibility into your VPC traffic while leveraging S3's scalability and durability for storing large amounts of data.