Guided Lab: Capture Network Traffic Information with VPC Flow Logs to CloudWatch Logs

Description

Have you ever wondered about the details of the IP traffic flowing through your Virtual Private Cloud (VPC)? With VPC Flow Logs, you can capture and analyze this critical information. Whether you're aiming to monitor your network, enhance security, or troubleshoot issues, VPC Flow Logs provide the insights you need.

In this lab, you'll learn how to create VPC Flow Logs for a network interface of an EC2 instance using the AWS Management Console. VPC Flow Logs is a feature in Amazon Web Services (AWS) that enables the capture of information about the IP traffic going to and from network interfaces in your Virtual Private Cloud (VPC). This data can be used for various purposes, such as network monitoring, security analysis, and troubleshooting. By the end of this lab, you will have configured VPC Flow Logs to capture detailed information about network traffic, sent this information to Amazon CloudWatch Logs, and verified the flow logs by generating and reviewing network traffic. This setup will provide valuable insights into traffic patterns, help identify security vulnerabilities, and optimize network performance.

Prerequisites

This lab assumes you have basic knowledge of AWS networks and are familiar with AWS core services like EC2 (Elastic Compute Cloud), CloudWatch, and VPC.

If you find any gaps in your knowledge, consider taking the following lab:

-
    - Creating an Amazon EC2 instance (Linux)
    - Creating a Custom Virtual Private Cloud (VPC) from scratch

Objectives

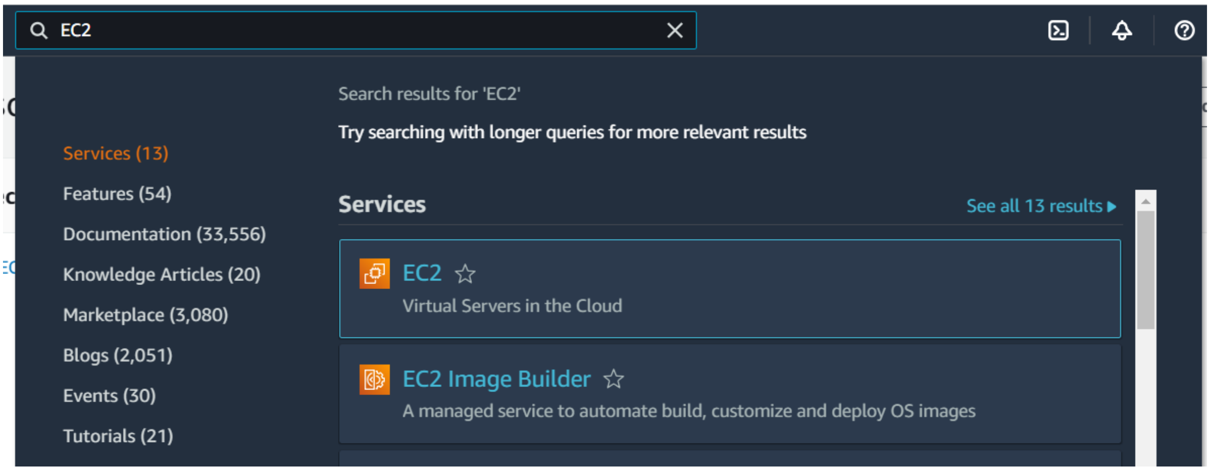
By the end of this lab, participants will be able to:

- Set up a log group in CloudWatch to store VPC Flow Log data.
- Creating and configuring VPC Flow Logs to capture IP traffic information.
- Generating network traffic to ensure the Flow Logs are capturing data.
- Reviewing the log data in CloudWatch to verify proper configuration.

Lab Steps

Launch an EC2 Instance

1. Navigate to the EC2 Dashboard



EC2

Search results for 'EC2'

Try searching with longer queries for more relevant results

EC2

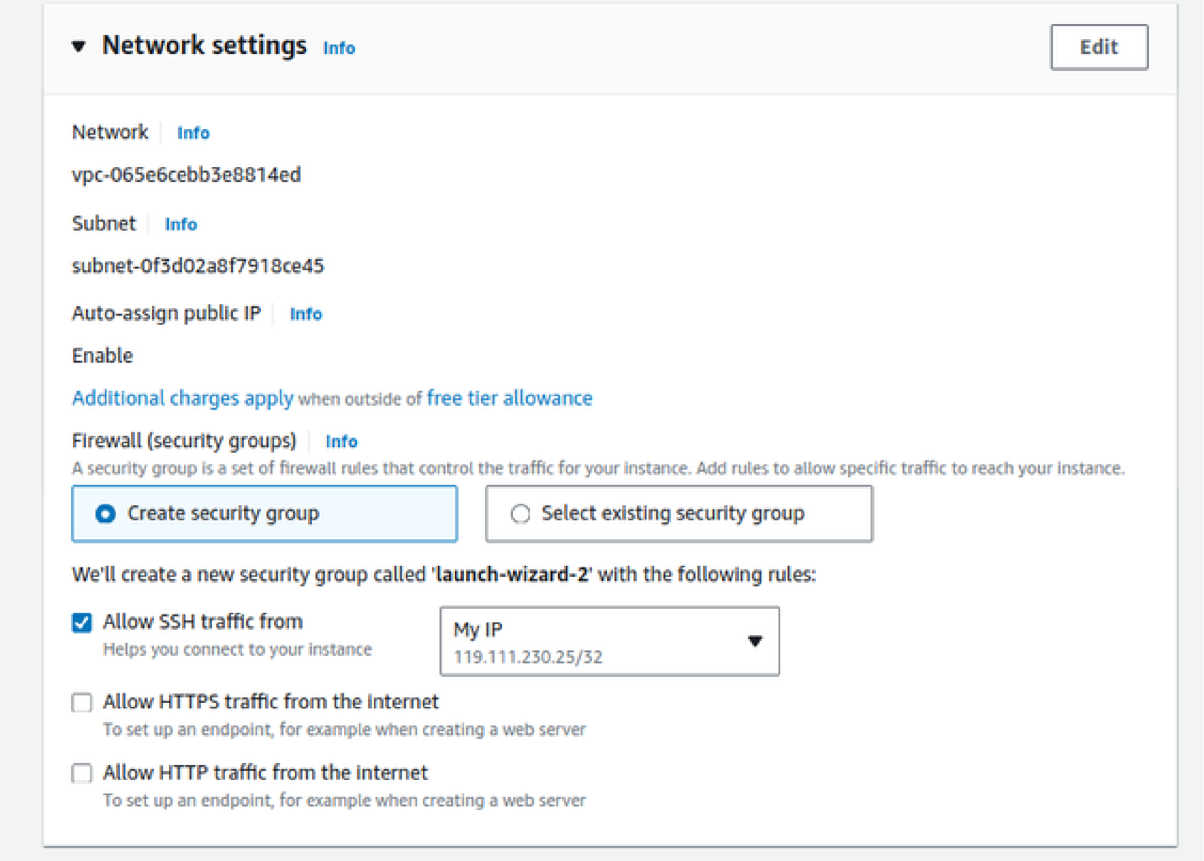
Virtual Servers in the Cloud

EC2 Image Builder

A managed service to automate build, customize and deploy OS images

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:

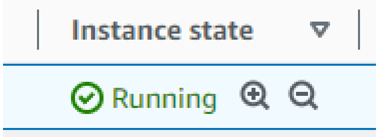
☑ Allow SSH traffic from — My IP 119.111.230.25/32
Helps you connect to your instance

□ 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.

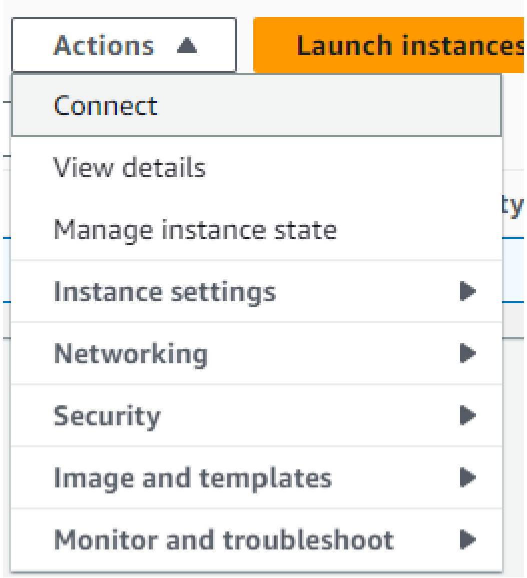
3. Wait for the EC2 instance to be in the **Running** state.



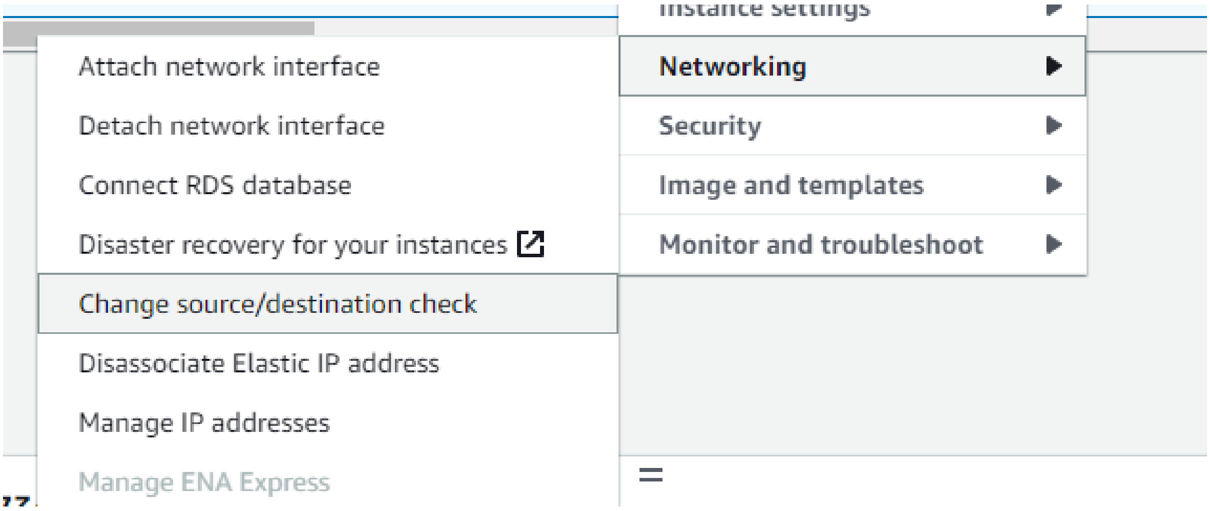
Instance state

✓ Running

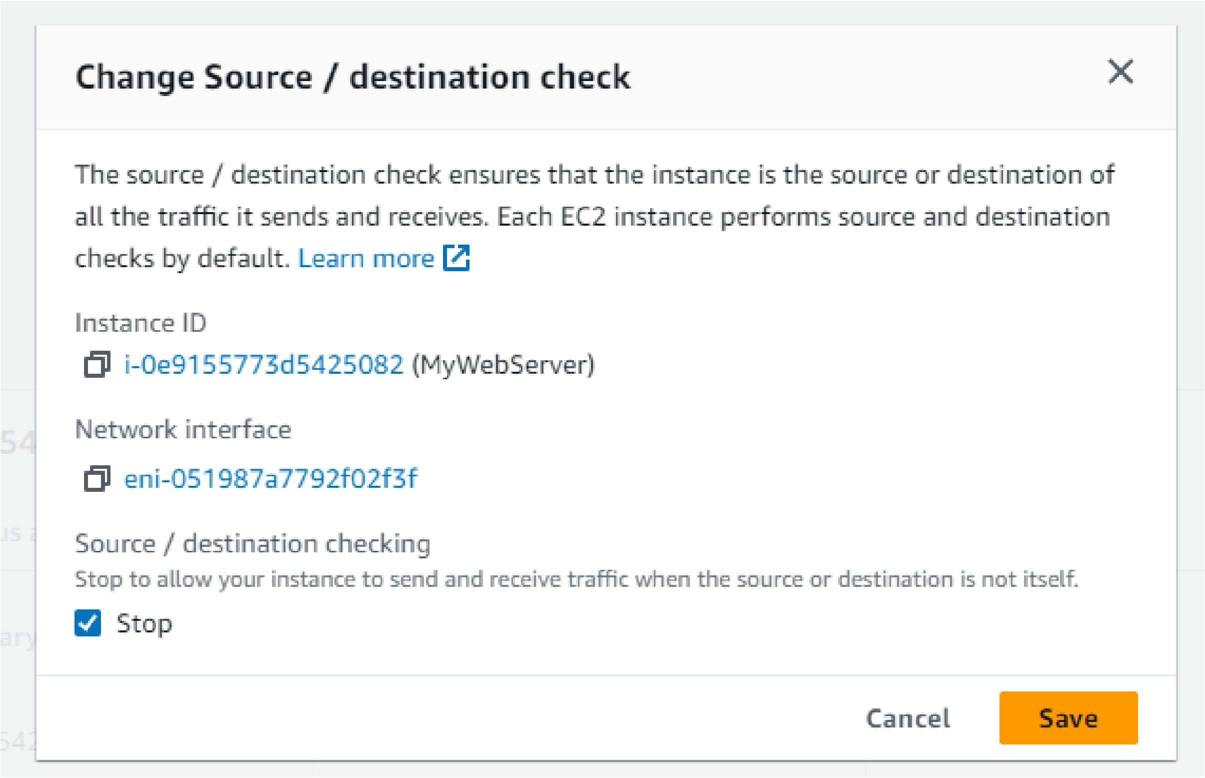
4. Select the instance and click on the Actions dropdown.



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



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



Change Source / destination check

The source / destination check ensures that the instance is the source or destination of all the traffic it sends and receives. Each EC2 instance performs source and destination checks by default. Learn more

Instance ID

i-0e9155773d5425082 (MyWebServer)

Network interface

eni-051987a7792f02f3f

Source / destination checking

Stop to allow your instance to send and receive traffic when the source or destination is not itself.

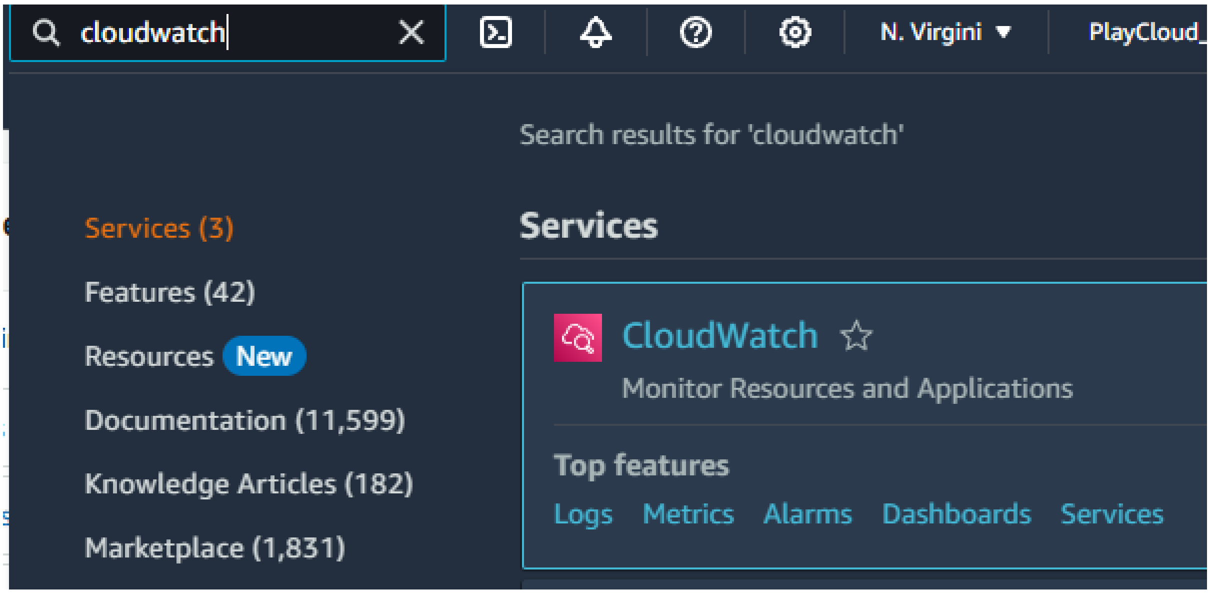
☑ Stop

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 the **Stop checkbox** is unchecked.
- **Disabled**: The instance can forward traffic, useful for NAT, routing, or firewall roles. This is when the **Stop checkbox** is checked.

Create a CloudWatch Log Group

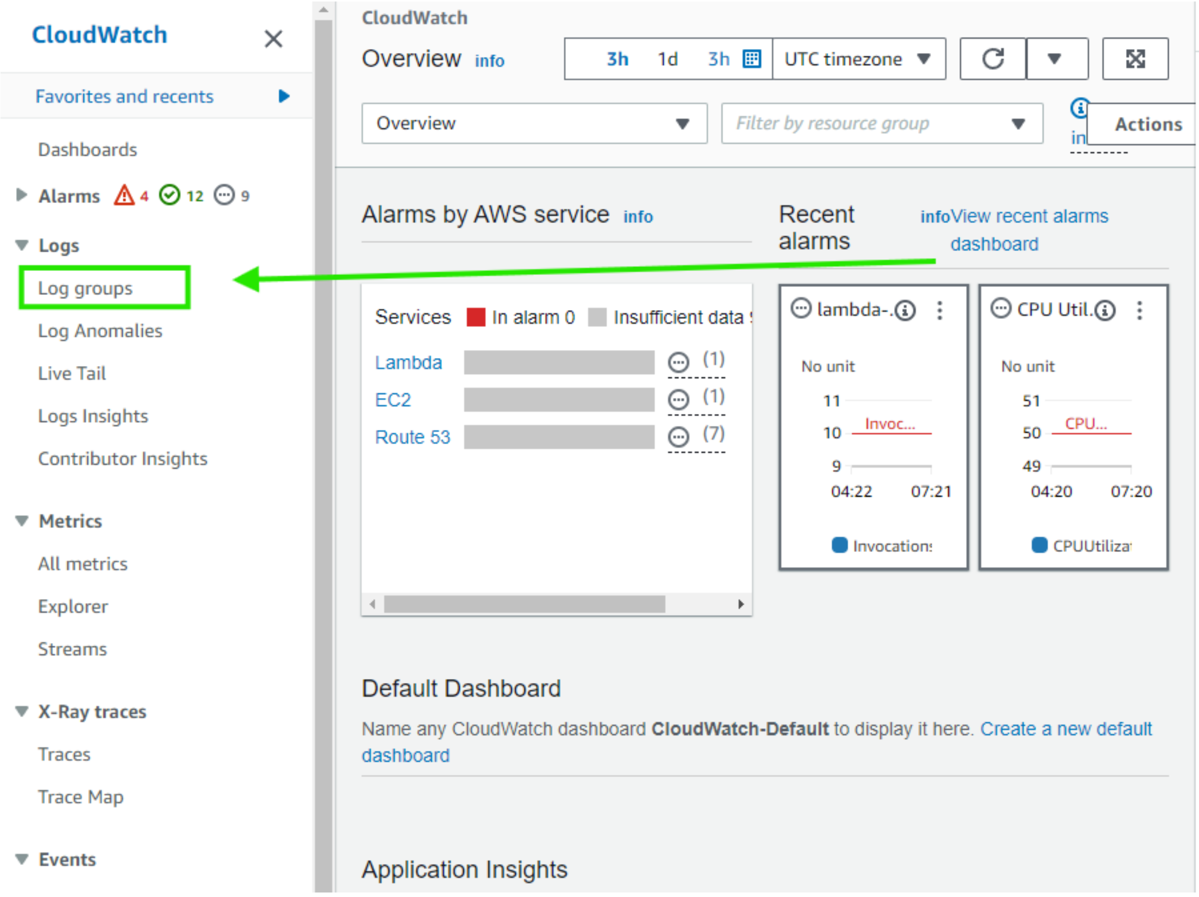
1. Navigate to the Cloudwatch.



cloudwatch

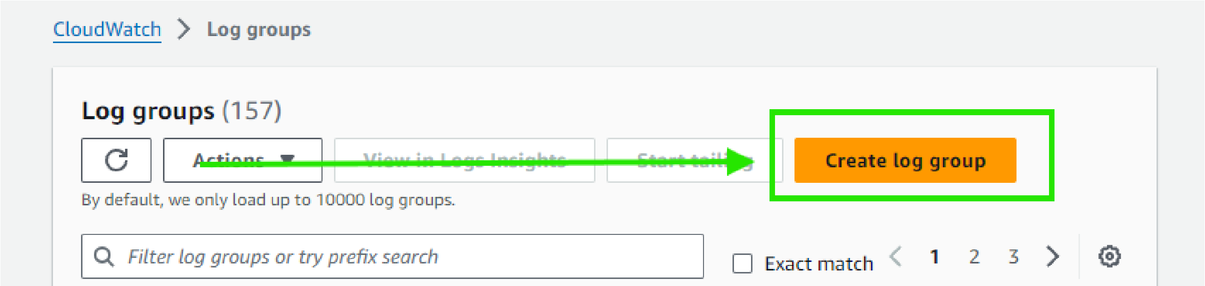
Search results for 'cloudwatch'

2. Locate the **Logs** section in the left-side navigation and click on **Log groups** to view the existing log groups.

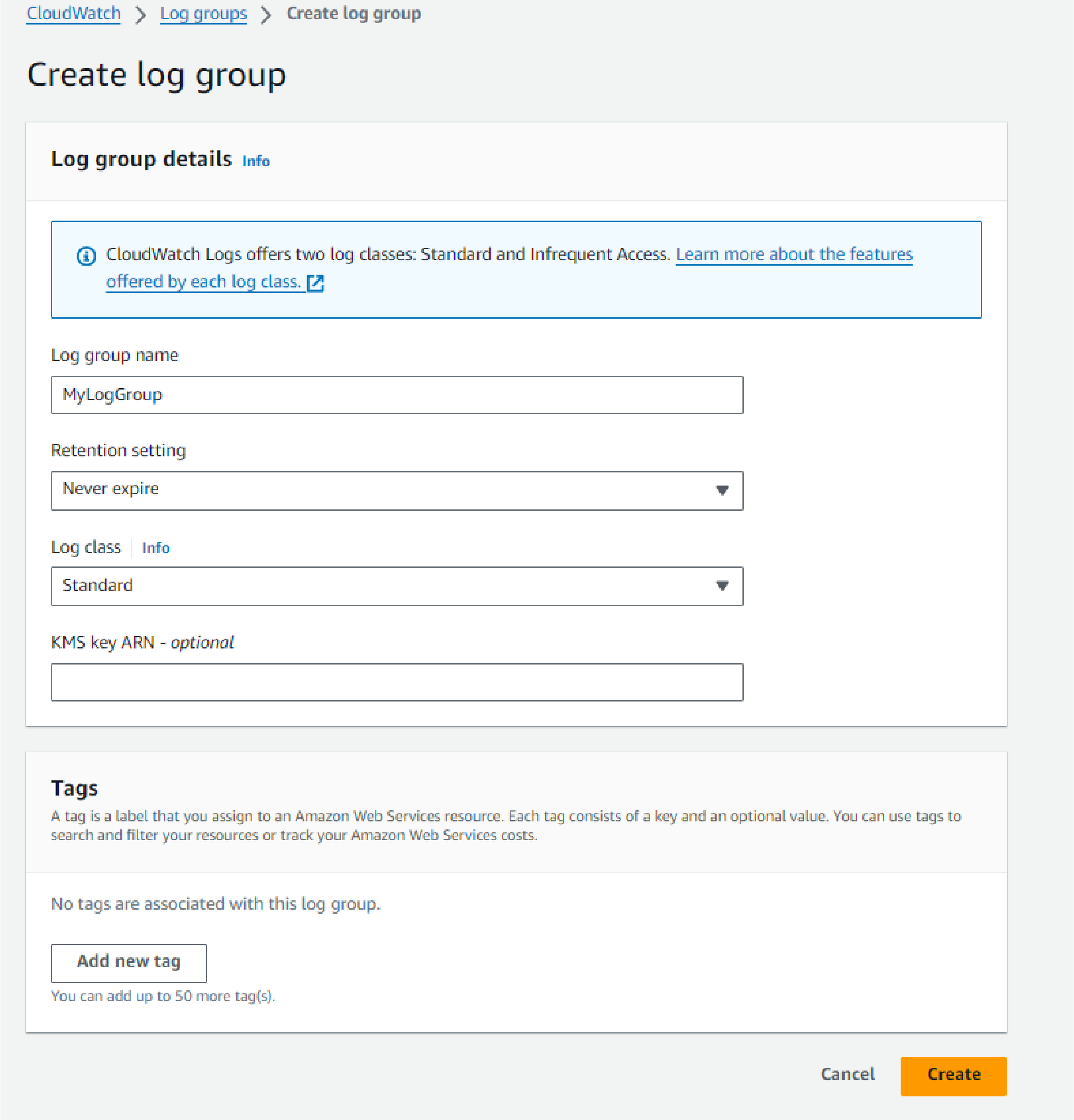


Name any CloudWatch dashboard **CloudWatch-Default** to display it here. Create a new default dashboard

3. Click the **Create log group** button at the top.



4. Enter a name for your new log group in the **Log group name** field. Ensure the name is descriptive and relevant to the logs it will contain.



CloudWatch Logs offers two log classes: Standard and Infrequent Access. Learn more about the features offered by each log class.

Log group name: MyLogGroup

Retention setting: Never expire

Log class: Standard

KMS key ARN - *optional*

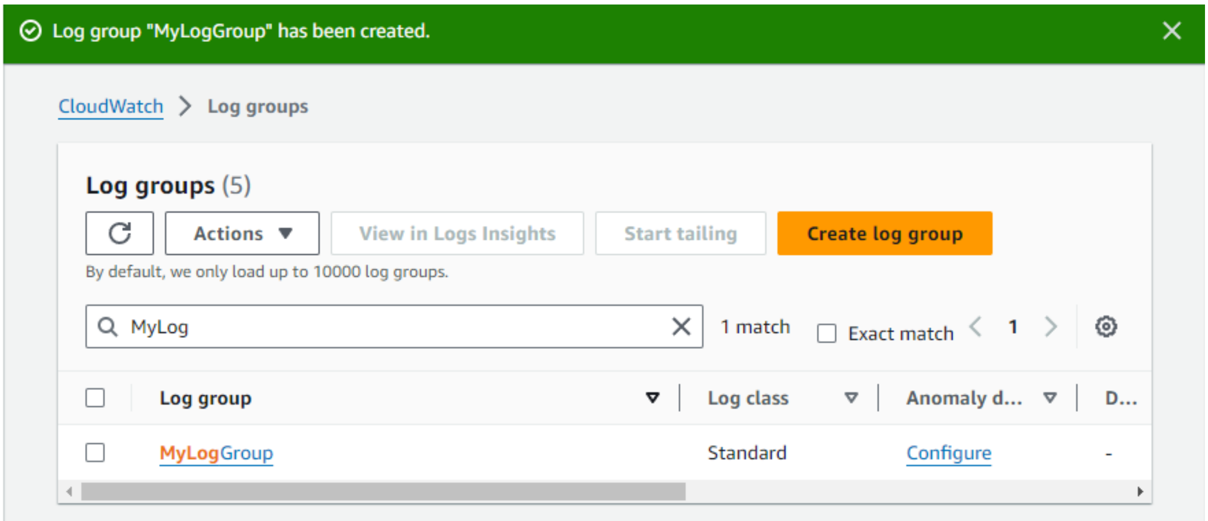
Tags

A tag is a label that you assign to an Amazon Web Services resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your Amazon Web Services costs.

No tags are associated with this log group.

You can add up to 50 more tag(s).

5. Click **Create log group** to finalize the process.



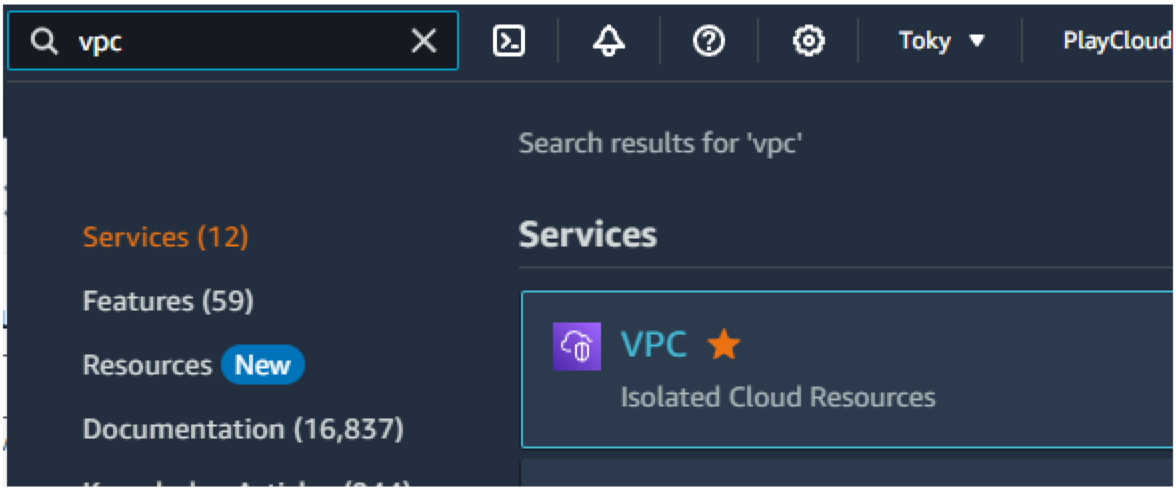
Log group "MyLogGroup" has been created.

Search: MyLog

□	Log group	Log class	Anomaly d...	D...
□	MyLogGroup	Standard	Configure	-

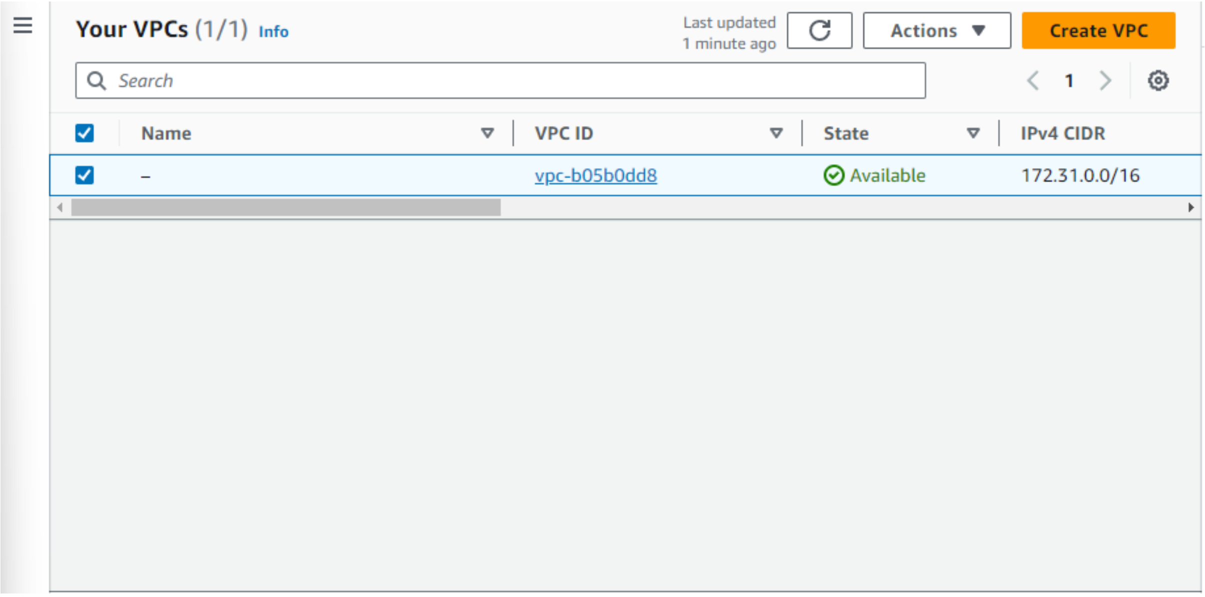
Create a VPC Flow Log

1. Navigate to the VPC Dashboard.



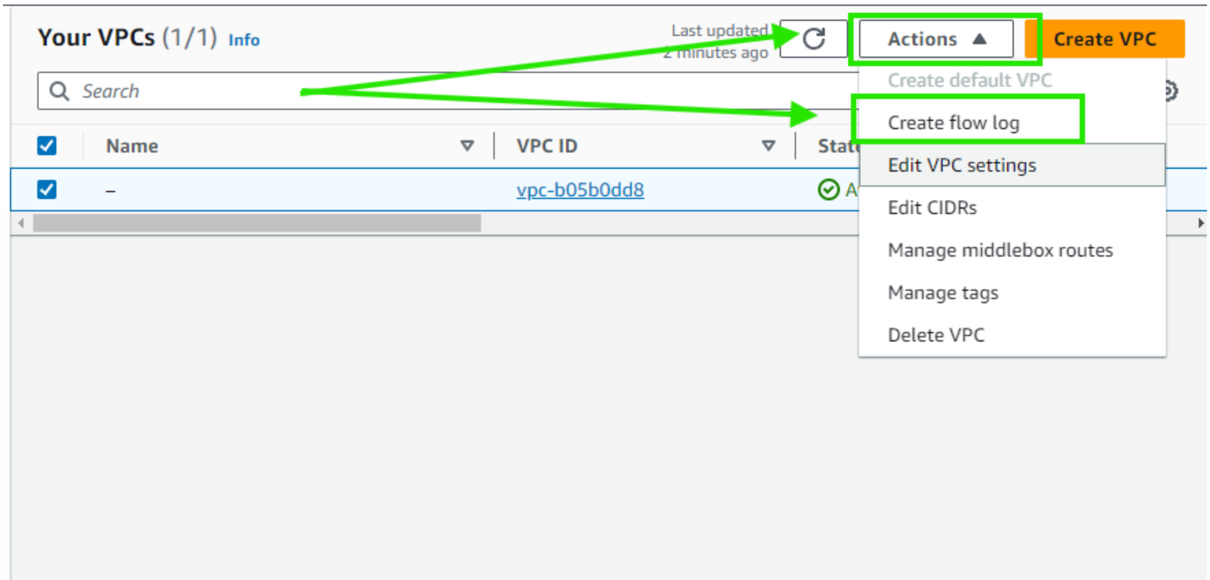
Search: vpc

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.



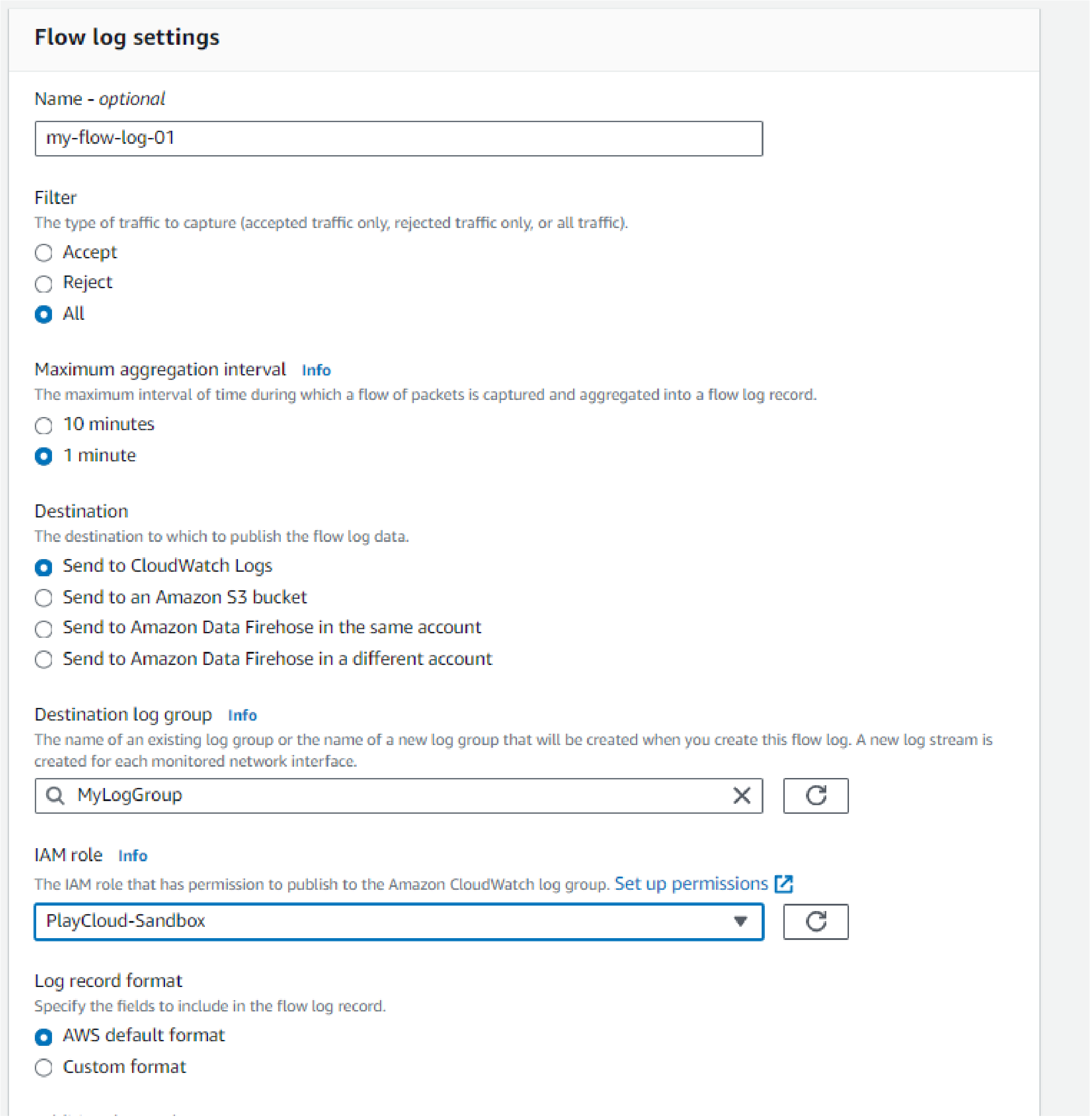
☑	Name	VPC ID	State	IPv4 CIDR
☑	–	vpc-b05b0dd8	Available	172.31.0.0/16

3. Click **Actions** and select **Create flow log**.



4. Configure the flow log:

- Name: **my-flow-log-01**
- Filter: **All**
- Maximum aggregation interval: **1 minute**
- Destination: **Send to CloudWatch Logs**
- Log group name: Choose the Log group created previously **MyLogGroup**
- IAM role: Select **PlayCloud-Sandbox**
- Log record format: Select **AWS default format**



Flow log settings

Name - *optional*

my-flow-log-01

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

Destination log group Info

The name of an existing log group or the name of a new log group that will be created when you create this flow log. A new log stream is created for each monitored network interface.

MyLogGroup

IAM role Info

The IAM role that has permission to publish to the Amazon CloudWatch log group. Set up permissions

PlayCloud-Sandbox

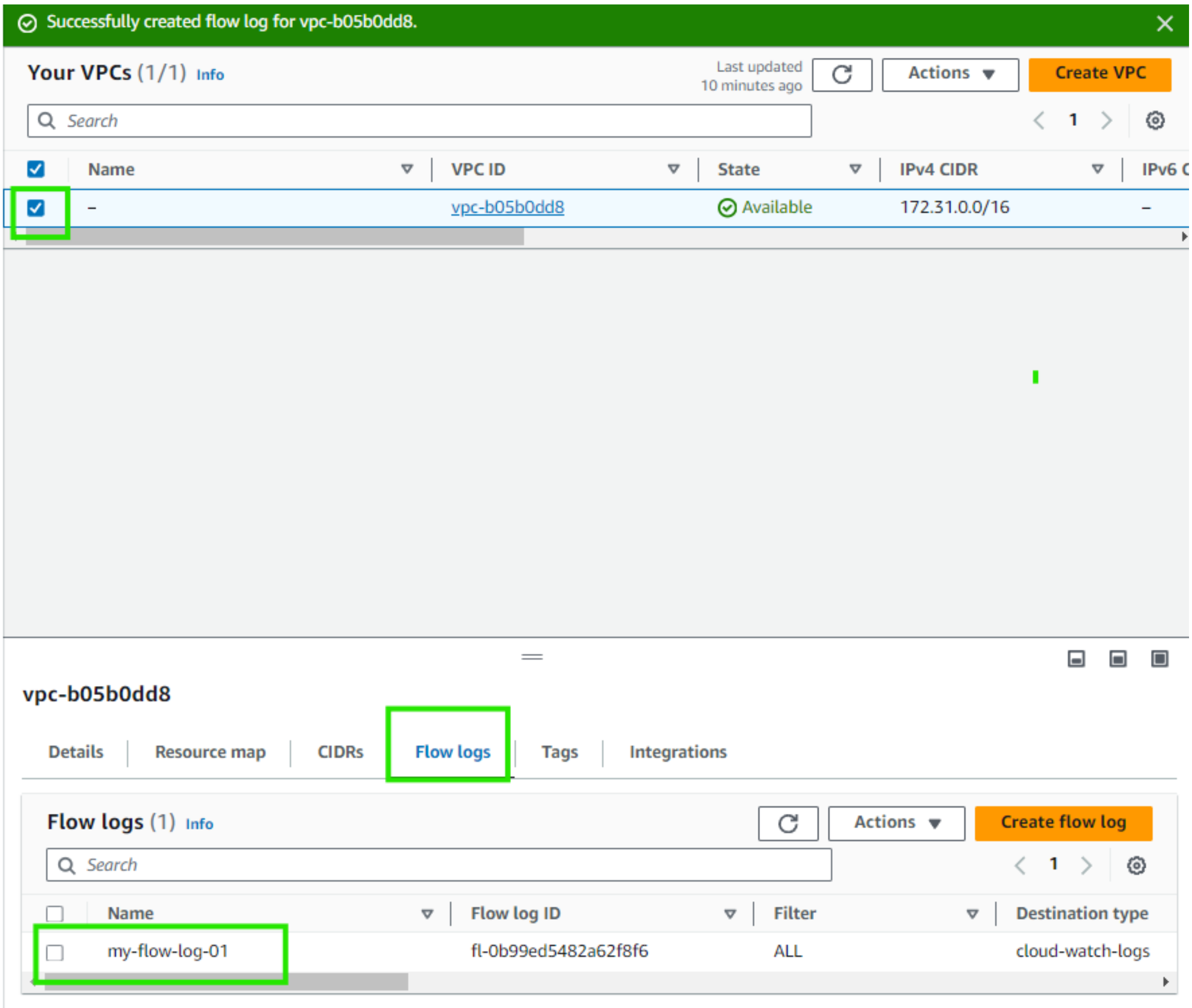
Log record format

Specify the fields to include in the flow log record.

● AWS default format
○ Custom format

5. Click **Create Flow Log.**

6. To check the flow log, navigate to the **Flow logs** tab in the VPC Dashboard. Ensure that the VPC is selected.



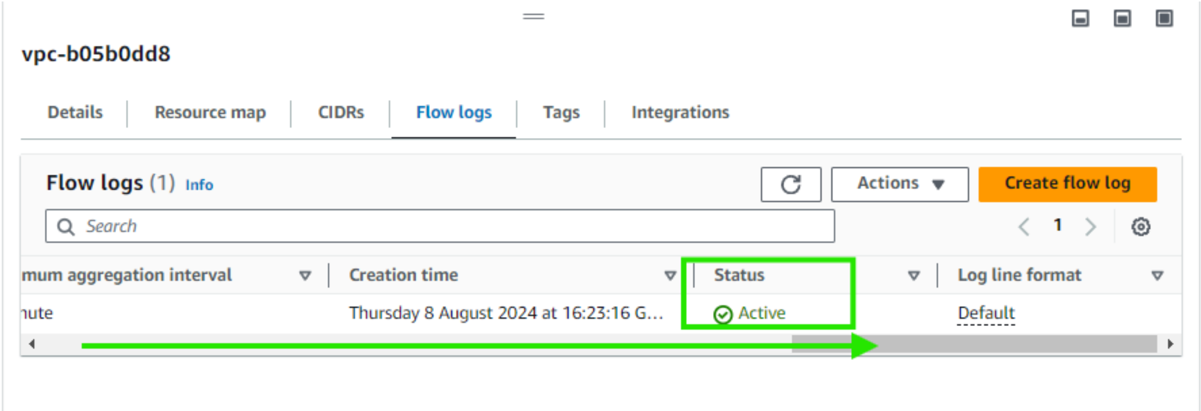
Successfully created flow log for vpc-b05b0dd8.

☑	Name	VPC ID	State	IPv4 CIDR	IPv6 C
☑	–	vpc-b05b0dd8	✓ Available	172.31.0.0/16	–

vpc-b05b0dd8

□	Name	Flow log ID	Filter	Destination type
□	my-flow-log-01	fl-0b99ed5482a62f8f6	ALL	cloud-watch-logs

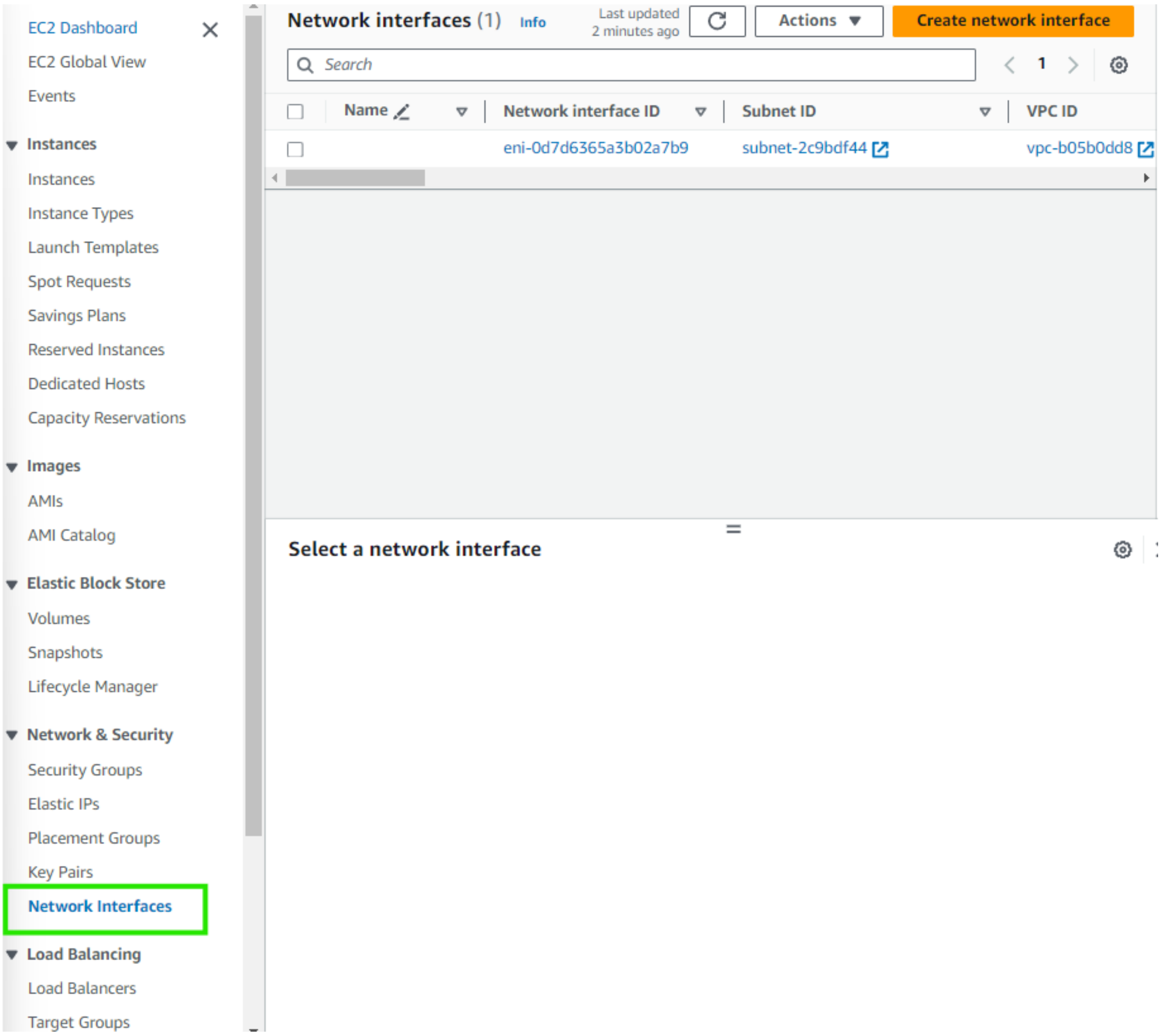
7. Scroll to the right to check the status of this flow log.



vpc-b05b0dd8

mum aggregation interval	Creation time	Status	Log line format
ıute	Thursday 8 August 2024 at 16:23:16 G…	✓ Active	Default

8. Navigate back to the **EC2 Dashboard > Network & Security > Network Interfaces.**

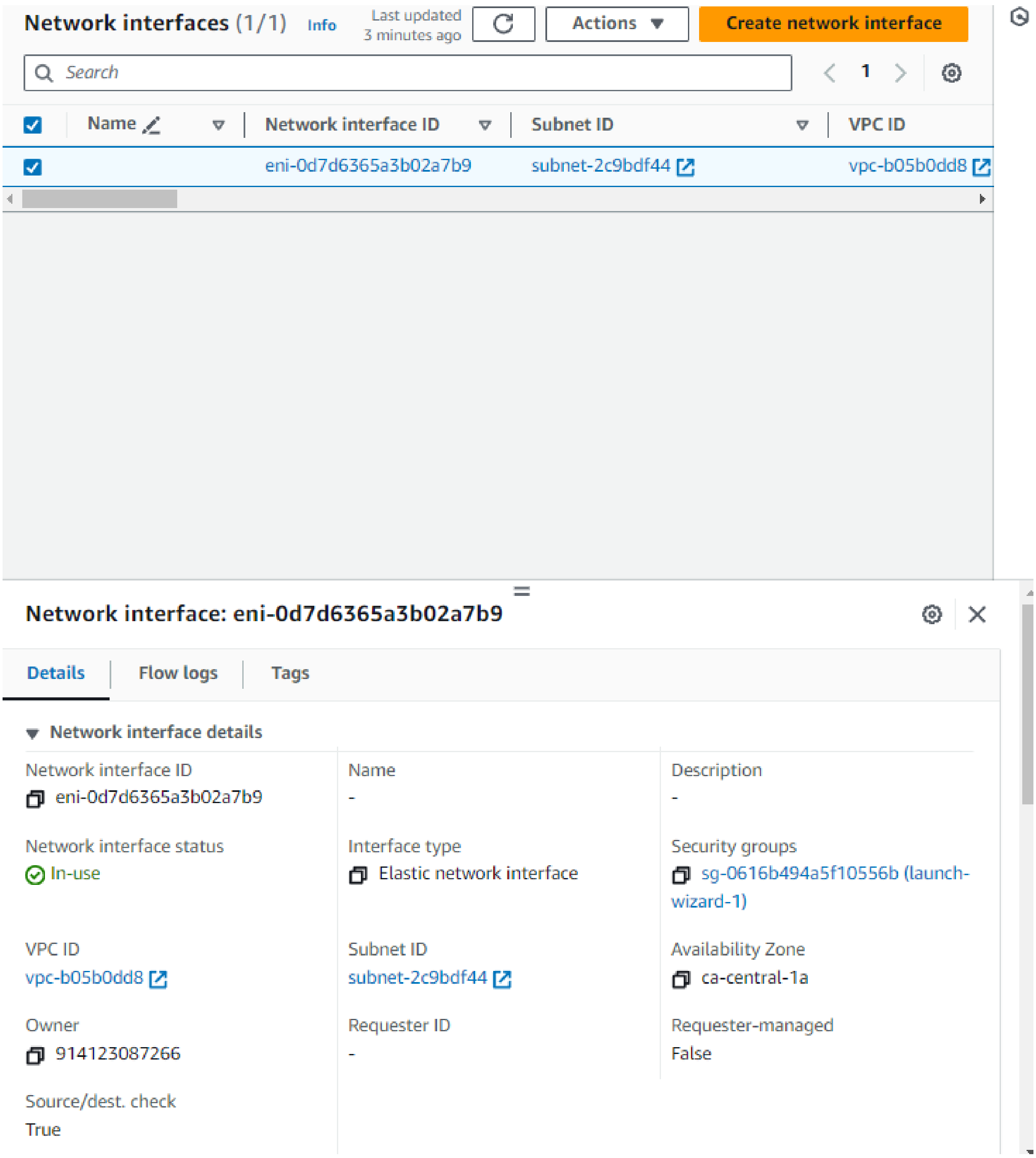


Network interfaces (1)

□	Name	Network interface ID	Subnet ID	VPC ID
□		eni-0d7d6365a3b02a7b9	subnet-2c9bdf44	vpc-b05b0dd8

Select a network interface

9. Find and select the network interface associated with your EC2 instance.



☑	Name	Network interface ID	Subnet ID	VPC ID
☑		eni-0d7d6365a3b02a7b9	subnet-2c9bdf44	vpc-b05b0dd8

Network interface: eni-0d7d6365a3b02a7b9

Network interface details

Network interface ID: eni-0d7d6365a3b02a7b9

Name: -

Description: -

Network interface status: In-use

Interface type: Elastic network interface

Security groups: sg-0616b494a5f10556b (launch-wizard-1)

VPC ID: vpc-b05b0dd8

Subnet ID: subnet-2c9bdf44

Availability Zone: ca-central-1a

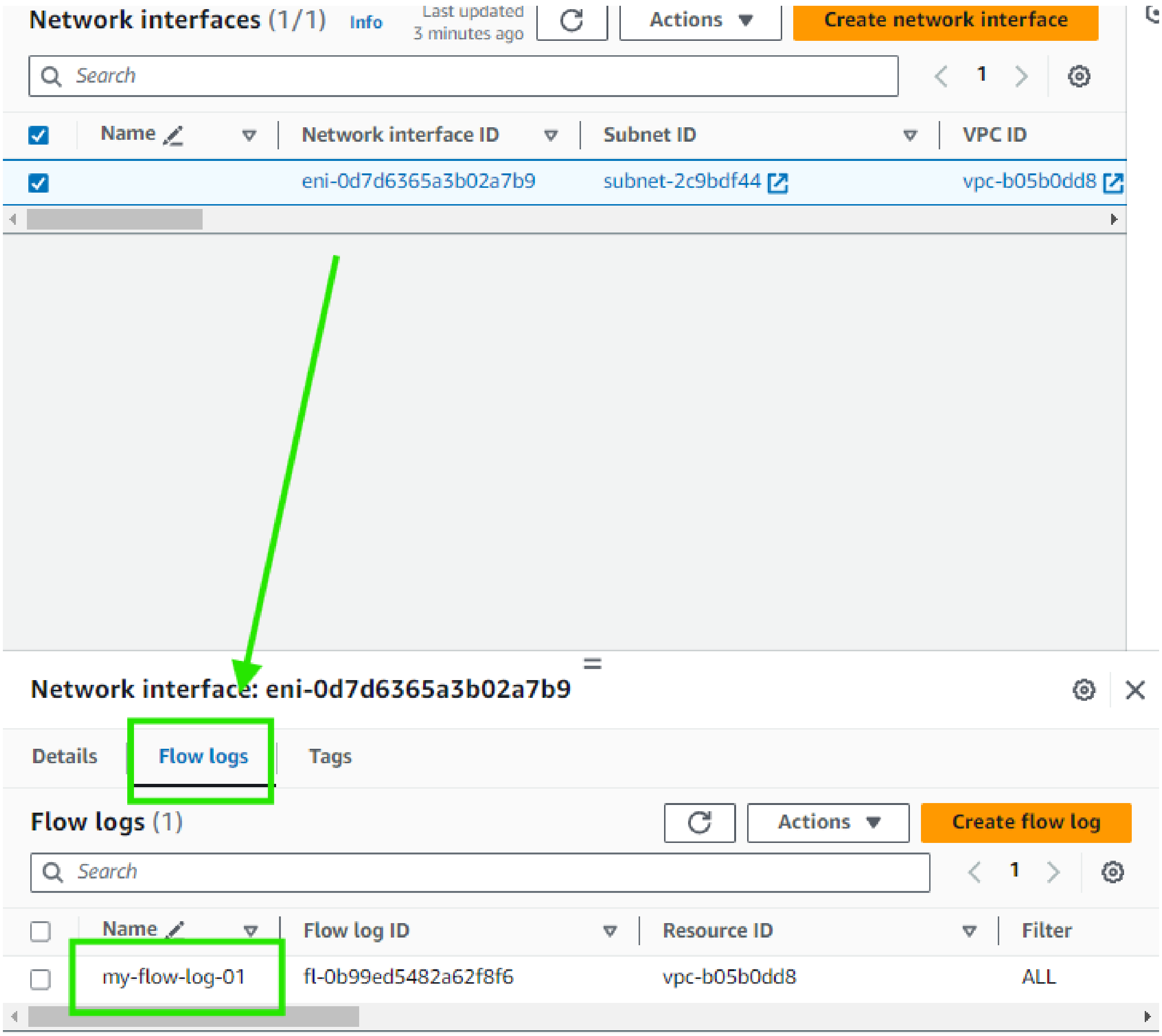
Owner: 914123087266

Requester ID: -

Requester-managed: False

Source/dest. check: True

10. Go to the Flow logs tab to see the same flow log group created previously.



☑	Name	Network interface ID	Subnet ID	VPC ID
☑		eni-0d7d6365a3b02a7b9	subnet-2c9bdf44	vpc-b05b0dd8

Network interface: eni-0d7d6365a3b02a7b9

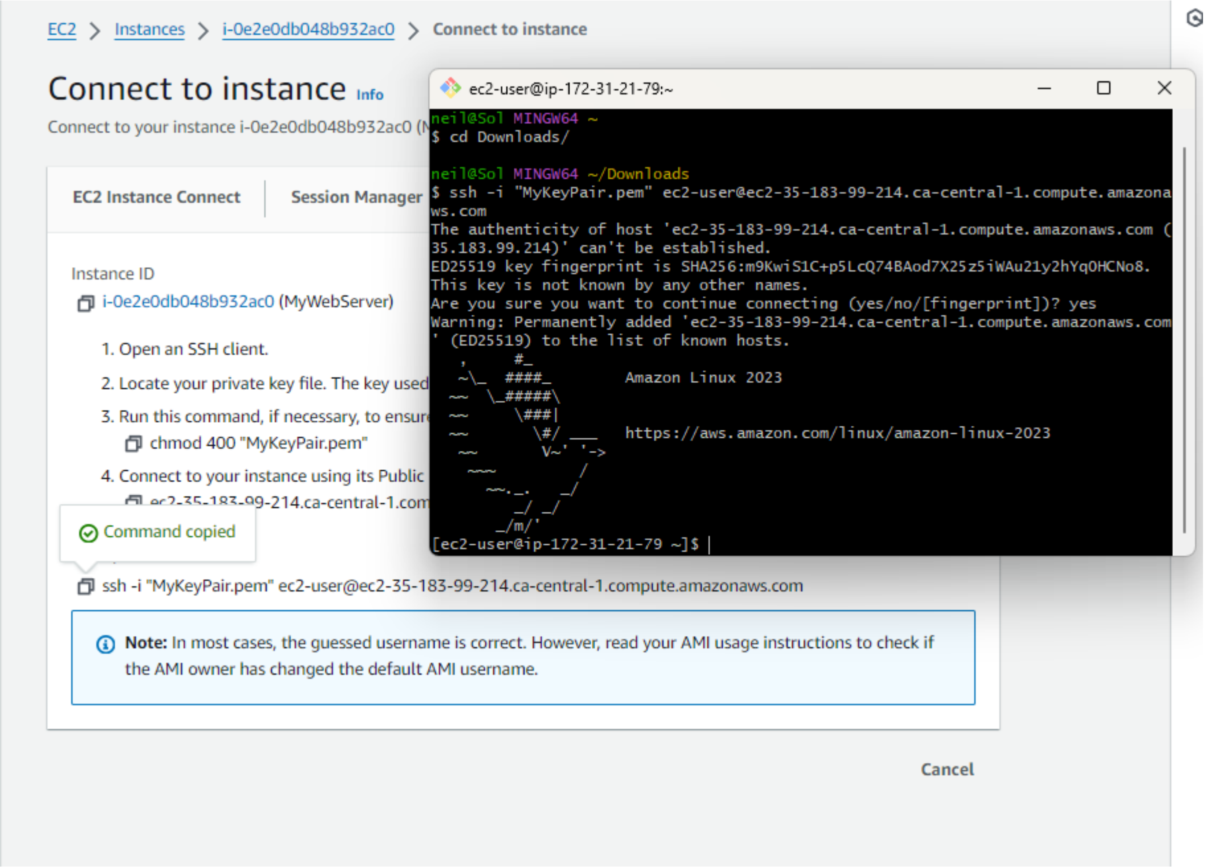
□	Name	Flow log ID	Resource ID	Filter
□	my-flow-log-01	fl-0b99ed5482a62f8f6	vpc-b05b0dd8	ALL

11. Take your time to review the flow logs.

Test the Flow Logs

1. Connect to your EC2 instance using SSH.

- Open your terminal
- Navigate to the directory of your .pem key.
- Copy the command in the **EC2 > Instances > <Instance_ID> > Connect to instance**
- Paste it to your Terminal.



EC2 > Instances > i-0e2e0db048b932ac0 > Connect to instance

Connect to instance Info

Connect to your instance i-0e2e0db048b932ac0 (M

Instance ID

i-0e2e0db048b932ac0 (MyWebServer)

1. Open an SSH client.
2. Locate your private key file. The key used
3. Run this command, if necessary, to ensur
   chmod 400 "MyKeyPair.pem"
4. Connect to your instance using its Public
   ec2-35-183-99-214.ca-central-1.com

Command copied

ssh -i "MyKeyPair.pem" ec2-user@ec2-35-183-99-214.ca-central-1.compute.amazonaws.com

Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

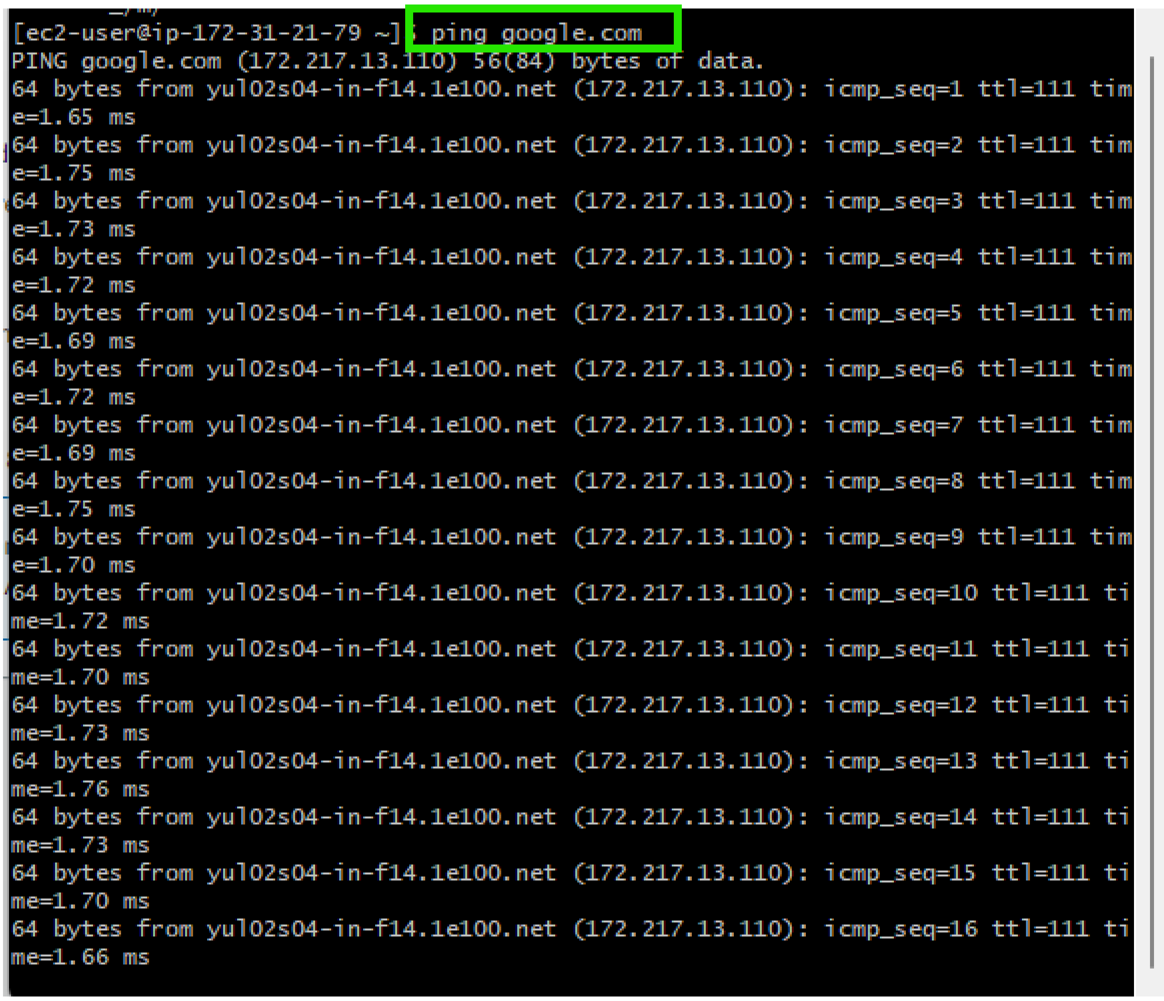
ec2-user@ip-172-31-21-79:~

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

neil@Sol MINGW64 ~/Downloads
$ ssh -i "MyKeyPair.pem" ec2-user@ec2-35-183-99-214.ca-central-1.compute.amazona
ws.com
The authenticity of host 'ec2-35-183-99-214.ca-central-1.compute.amazonaws.com (
35.183.99.214)' can't be established.
ED25519 key fingerprint is SHA256:m9KwiS1C+p5LcQ74BAod7X25z5iWAu21y2hYq0HCNo8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-35-183-99-214.ca-central-1.compute.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-172-31-21-79 ~]$ |
```

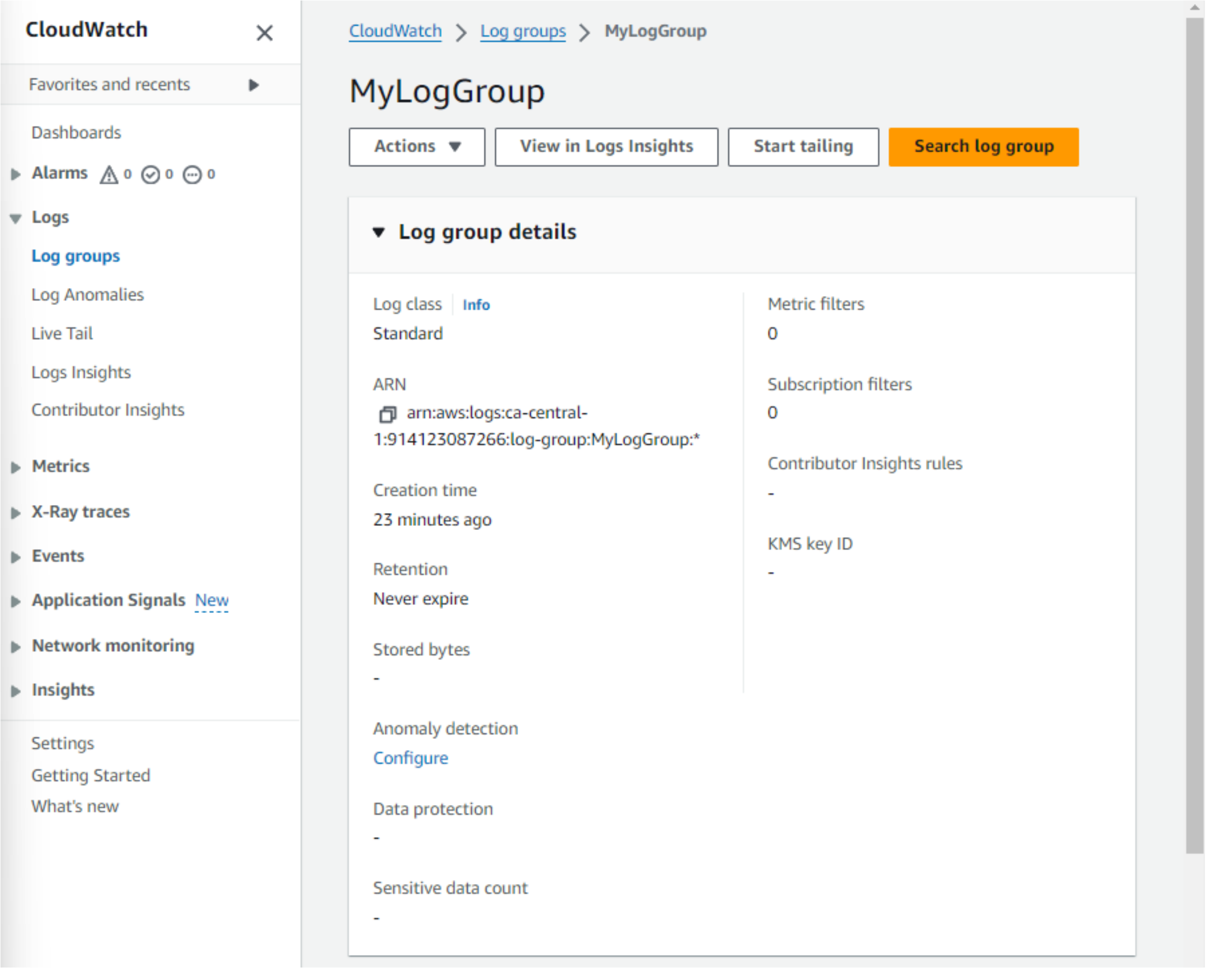
2. Generate network traffic by running commands such as ping or accessing websites using curl.

- Example: ping google.com



```
[ec2-user@ip-172-31-21-79 ~]$ ping google.com
PING google.com (172.217.13.110) 56(84) bytes of data.
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=1 ttl=111 tim
e=1.65 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=2 ttl=111 tim
e=1.75 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=3 ttl=111 tim
e=1.73 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=4 ttl=111 tim
e=1.72 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=5 ttl=111 tim
e=1.69 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=6 ttl=111 tim
e=1.72 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=7 ttl=111 tim
e=1.69 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=8 ttl=111 tim
e=1.75 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=9 ttl=111 tim
e=1.70 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=10 ttl=111 ti
me=1.72 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=11 ttl=111 ti
me=1.70 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=12 ttl=111 ti
me=1.73 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=13 ttl=111 ti
me=1.76 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=14 ttl=111 ti
me=1.73 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=15 ttl=111 ti
me=1.70 ms
64 bytes from yul02s04-in-f14.1e100.net (172.217.13.110): icmp_seq=16 ttl=111 ti
me=1.66 ms
```

3. Navigate to the **CloudWatch Dashboard > Log groups**



MyLogGroup

Log group details

Log class Info
Standard

ARN
arn:aws:logs:ca-central-1:914123087266:log-group:MyLogGroup:*

Creation time
23 minutes ago

Retention
Never expire

Stored bytes
-

Anomaly detection
Configure

Data protection
-

Sensitive data count
-

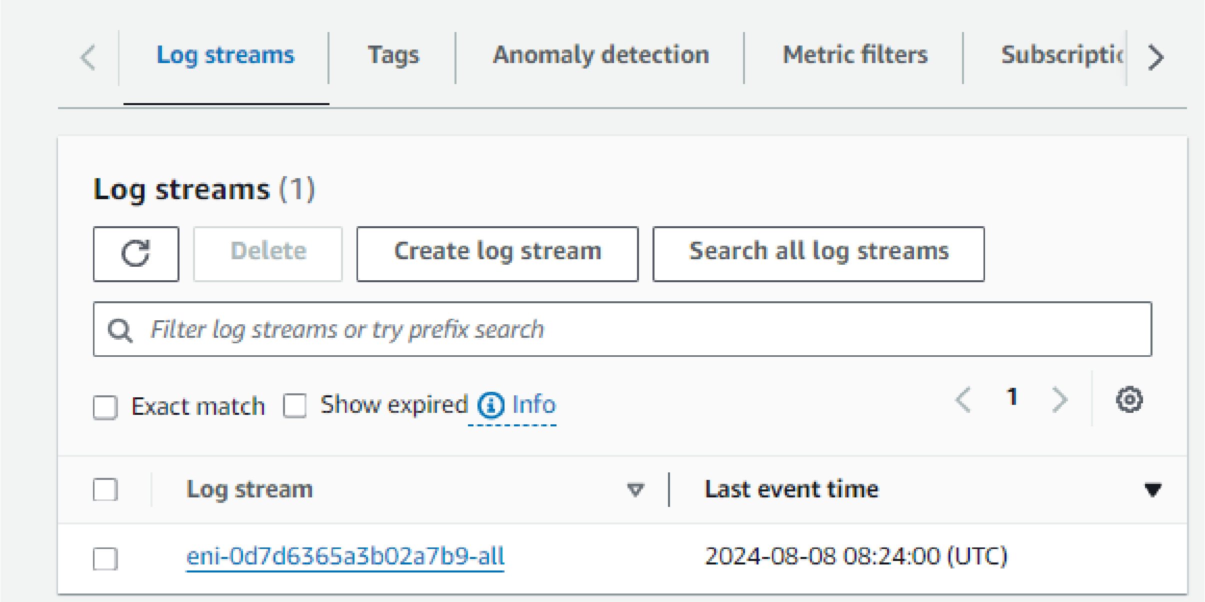
Metric filters
0

Subscription filters
0

Contributor Insights rules
-

KMS key ID
-

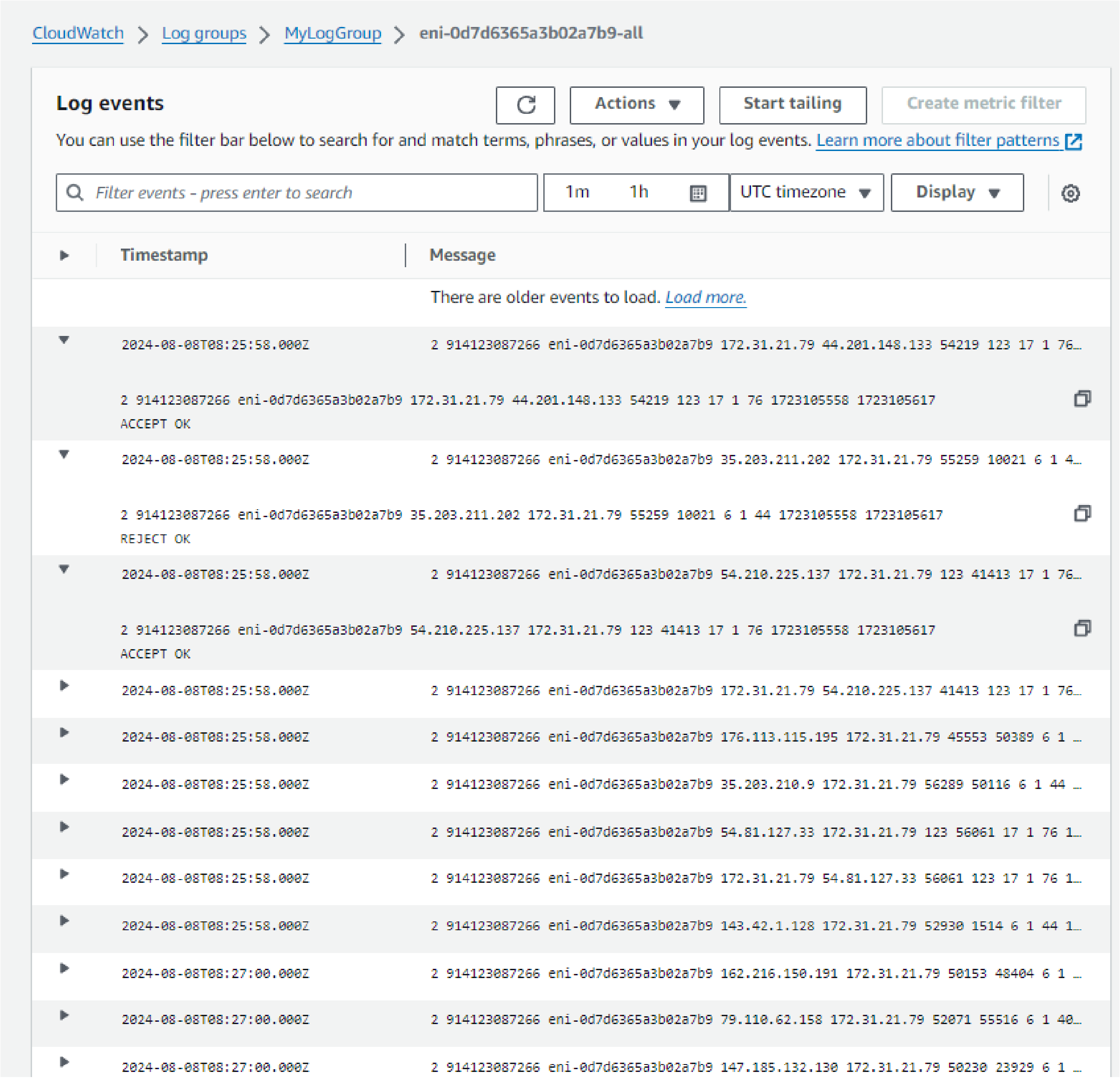
4. You should see log entries detailing the network traffic to and from your EC2 instance.



Log streams (1)

Log stream	Last event time
eni-0d7d6365a3b02a7b9-all	2024-08-08 08:24:00 (UTC)

5. Click on the log stream. You should see Log events similar to the image below.


CloudWatch > Log groups > MyLogGroup > eni-0d7d6365a3b02a7b9-all
Log events
Actions
Start tailing
Create metric filter
Filter events - press enter to search
1m
1h
UTC timezone
Display

You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

There are older events to load. Load more.

```
Timestamp                  Message
2024-08-08T08:25:58.000Z   2 914123087266 eni-0d7d6365a3b02a7b9 172.31.21.79 44.201.148.133 54219 123 17 1 76…

2 914123087266 eni-0d7d6365a3b02a7b9 172.31.21.79 44.201.148.133 54219 123 17 1 76 1723105558 1723105617
ACCEPT OK
2024-08-08T08:25:58.000Z   2 914123087266 eni-0d7d6365a3b02a7b9 35.203.211.202 172.31.21.79 55259 10021 6 1 4…

2 914123087266 eni-0d7d6365a3b02a7b9 35.203.211.202 172.31.21.79 55259 10021 6 1 44 1723105558 1723105617
REJECT OK
2024-08-08T08:25:58.000Z   2 914123087266 eni-0d7d6365a3b02a7b9 54.210.225.137 172.31.21.79 123 41413 17 1 76…

2 914123087266 eni-0d7d6365a3b02a7b9 54.210.225.137 172.31.21.79 123 41413 17 1 76 1723105558 1723105617
ACCEPT OK
2024-08-08T08:25:58.000Z   2 914123087266 eni-0d7d6365a3b02a7b9 172.31.21.79 54.210.225.137 41413 123 17 1 76…
2024-08-08T08:25:58.000Z   2 914123087266 eni-0d7d6365a3b02a7b9 176.113.115.195 172.31.21.79 45553 50389 6 1 …
2024-08-08T08:25:58.000Z   2 914123087266 eni-0d7d6365a3b02a7b9 35.203.210.9 172.31.21.79 56289 50116 6 1 44 …
2024-08-08T08:25:58.000Z   2 914123087266 eni-0d7d6365a3b02a7b9 54.81.127.33 172.31.21.79 123 56061 17 1 76 1…
2024-08-08T08:25:58.000Z   2 914123087266 eni-0d7d6365a3b02a7b9 172.31.21.79 54.81.127.33 56061 123 17 1 76 1…
2024-08-08T08:25:58.000Z   2 914123087266 eni-0d7d6365a3b02a7b9 143.42.1.128 172.31.21.79 52930 1514 6 1 44 1…
2024-08-08T08:27:00.000Z   2 914123087266 eni-0d7d6365a3b02a7b9 162.216.150.191 172.31.21.79 50153 48404 6 1 …
2024-08-08T08:27:00.000Z   2 914123087266 eni-0d7d6365a3b02a7b9 79.110.62.158 172.31.21.79 52071 55516 6 1 40…
2024-08-08T08:27:00.000Z   2 914123087266 eni-0d7d6365a3b02a7b9 147.185.132.130 172.31.21.79 50230 23929 6 1 …
```

6. Take your time to review and familiarize yourself with the log format:
${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr} ${srcport} ${dstport} ${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-status}

That's it! Congratulations, you successfully created VPC Flow Logs for the network interface of an EC2 instance using the AWS Management Console. By setting up VPC Flow Logs, you enabled detailed logging of IP traffic for monitoring and troubleshooting purposes. Additionally, you tested the flow logs by generating network traffic and verifying the logs in CloudWatch, ensuring that the setup works correctly. This setup provides valuable insights into network traffic, helping to enhance security, troubleshoot network issues, and optimize performance in your AWS environment.