

Lesson 05 Demo 04

Creating a Flow Log in the VPC

Objective: To create a VPC flow log within the AWS framework and configure the logging settings, set filter criteria, and specify an Amazon S3 bucket

Tools required: AWS Web Console

Prerequisites: AWS account

Steps to be followed:

1. Create a flow log in the default VPC

Step 1: Create a flow log in the default VPC

- 1.1 In the AWS web console, search for and select the **VPC** service



1.2 Click on VPCs under the Resources by Region section

The screenshot shows the AWS VPC dashboard. On the left, there's a sidebar with 'Virtual private cloud' expanded. The main area is titled 'Resources by Region' and shows a grid of resource counts for the US East region. The 'VPCs' link is highlighted with a red box. Other resources shown include Subnets (6), NAT Gateways (0), VPC Peering Connections (0), Route Tables (1), Network ACLs (2), Internet Gateways (1), Security Groups (1), Egress-only Internet Gateways (0), and Customer Gateways (0).

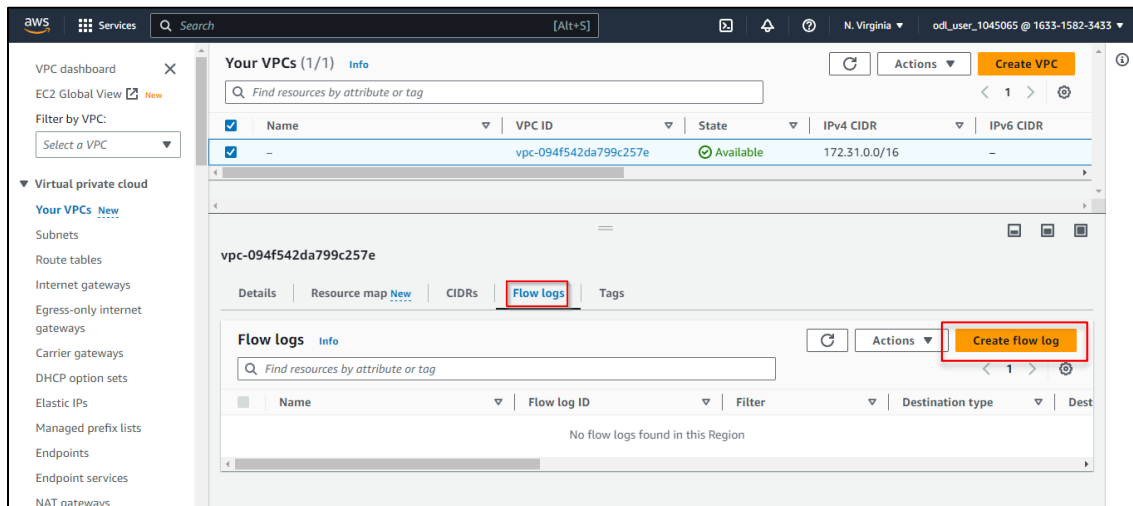
1.3 Select the default VPC

The screenshot shows the 'Your VPCs' page in the AWS console. A table lists the available VPCs. The first VPC is selected with a checkbox. Below the table, the details for the selected VPC are shown.

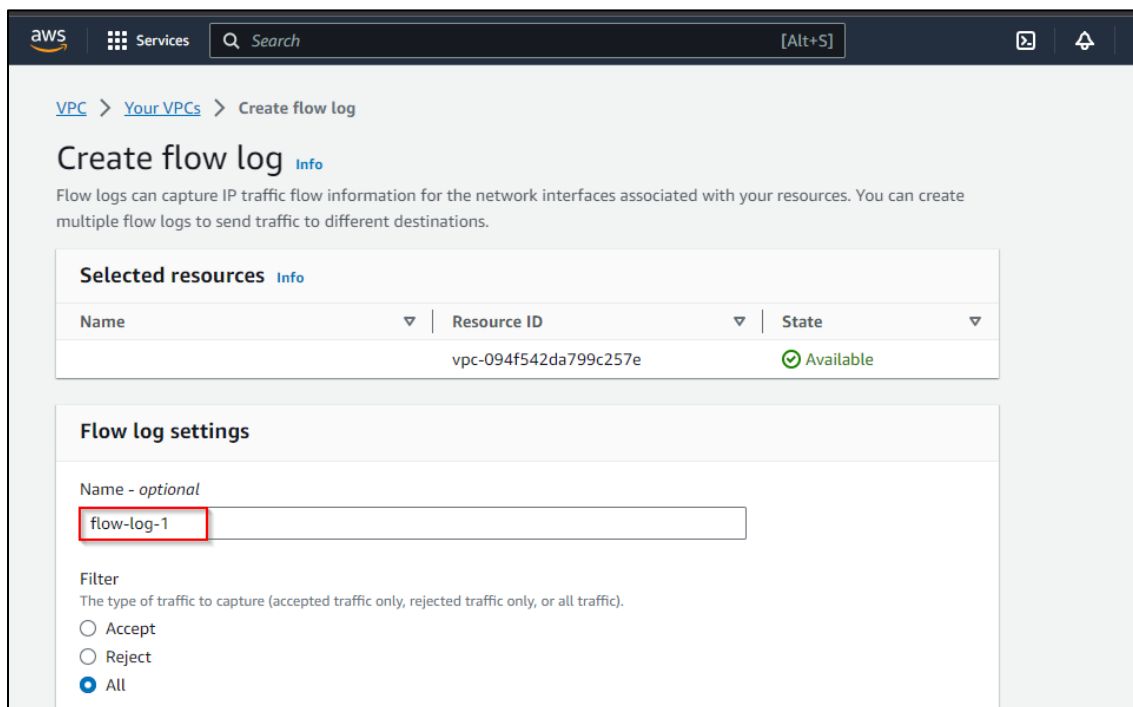
Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
-	vpc-094f542da799c257e	Available	172.31.0.0/16	-

Below the table, the VPC ID **vpc-094f542da799c257e** is displayed, along with tabs for Details, Resource map, CIDRs, Flow logs, and Tags.

1.4 Go to the **Flow logs** tab and click **Create flow log**



1.5 Enter the name as **flow-log-1**



1.6 Configure the log settings by setting the filter to **All**, the maximum aggregation interval to **1 minute**, and the destination to **Send to an Amazon S3 bucket**

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 Kinesis Firehose in the same account
☐ Send to Kinesis 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::my-bucket

Note: To obtain the S3 bucket ARN, click **Create S3 bucket** and copy the ARN. Paste the ARN in the **S3 bucket ARN** field. Refer to Lesson 3 Demo 1 to see how to create an S3 bucket.

1.7 Click on **Create flow log**

☒ Text (default)
☐ Parquet

Hive-compatible S3 prefix [Info](#)
Enable to use Hive-compatible S3 prefixes to simplify the loading of new data into your Hive-compatible tools.

☐ Enable

Partition logs by time [Info](#)
Partition your logs per hour to reduce your query costs and get faster response if you have a large volume of logs and typically run queries targeted to a specific hour timeframe.

☒ Every 24 hours (default)
☐ Every 1 hour (60 minutes)

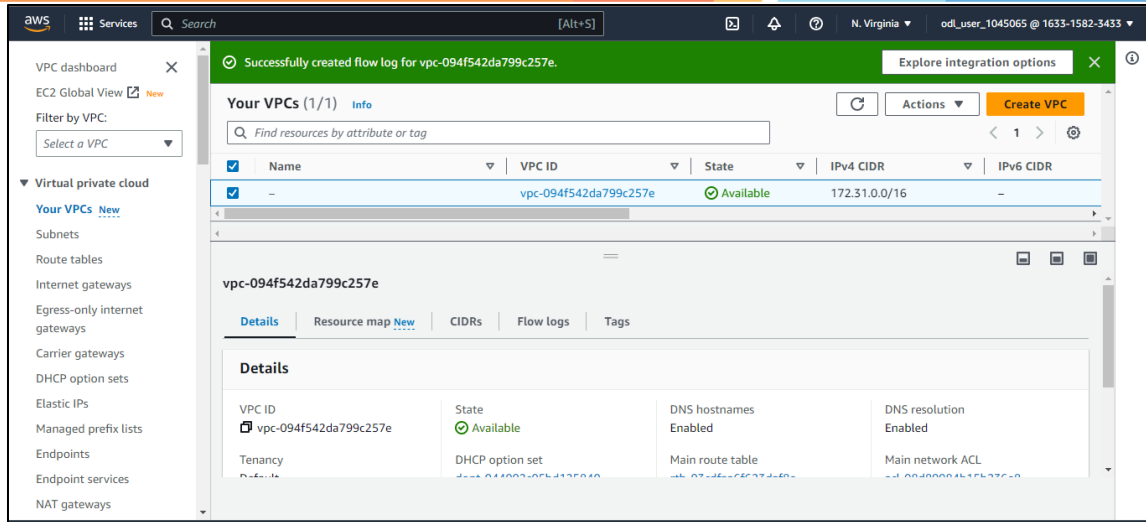
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Name Value - optional: flow-log-1

[Add tag](#) [Remove tag](#)

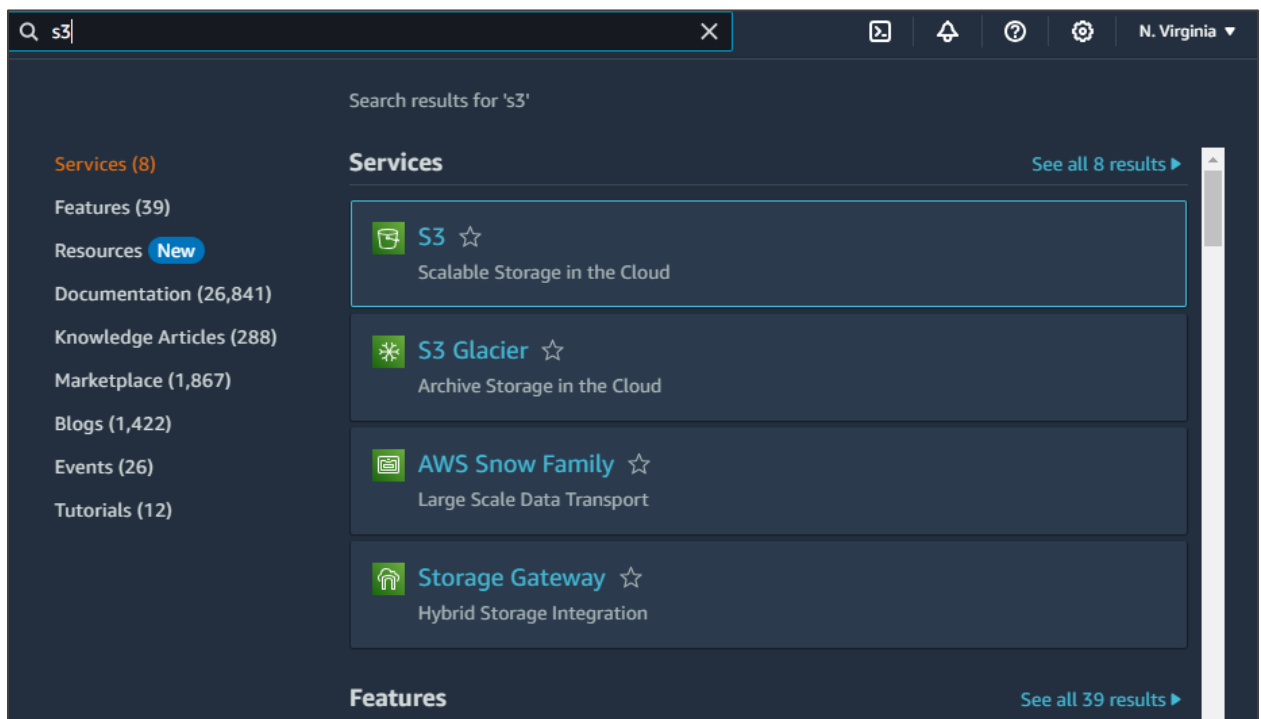
You can add 49 more tags

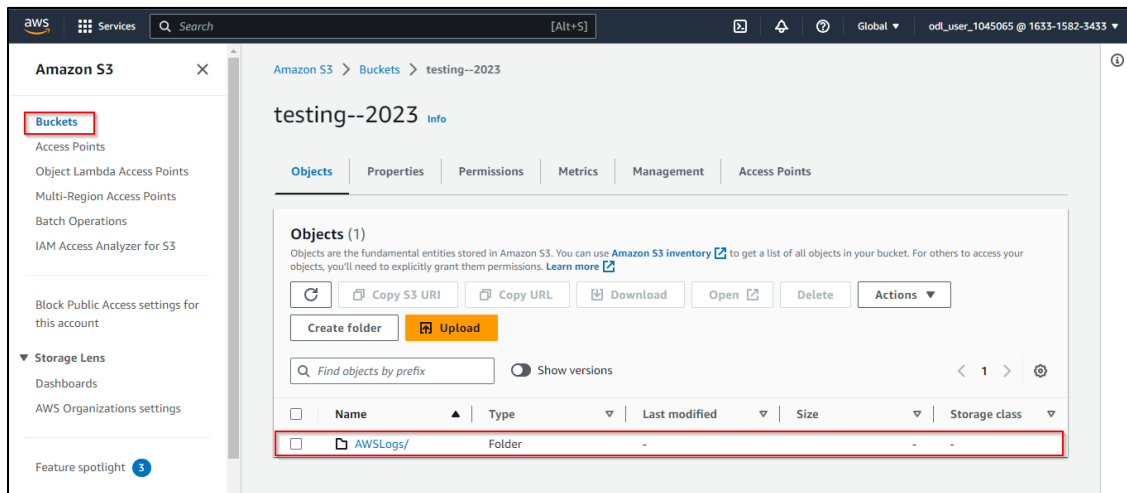
[Cancel](#) [Create flow log](#)



The flow log has been successfully created.

1.8 To view the flow log in S3, search for **S3** service and click on it





You can see the flow log folder created in your bucket.

By following these steps, you have successfully created a VPC Flow Log in the AWS environment. This process involves accessing the VPC console, selecting the default VPC, and setting up the flow log.