

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, setting filter criteria, and specifying an Amazon S3 bucket

Tools required: AWS workspace

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 console navigation pane, search and select **VPC**



1.2 Click on VPCs under the Resources by Region section

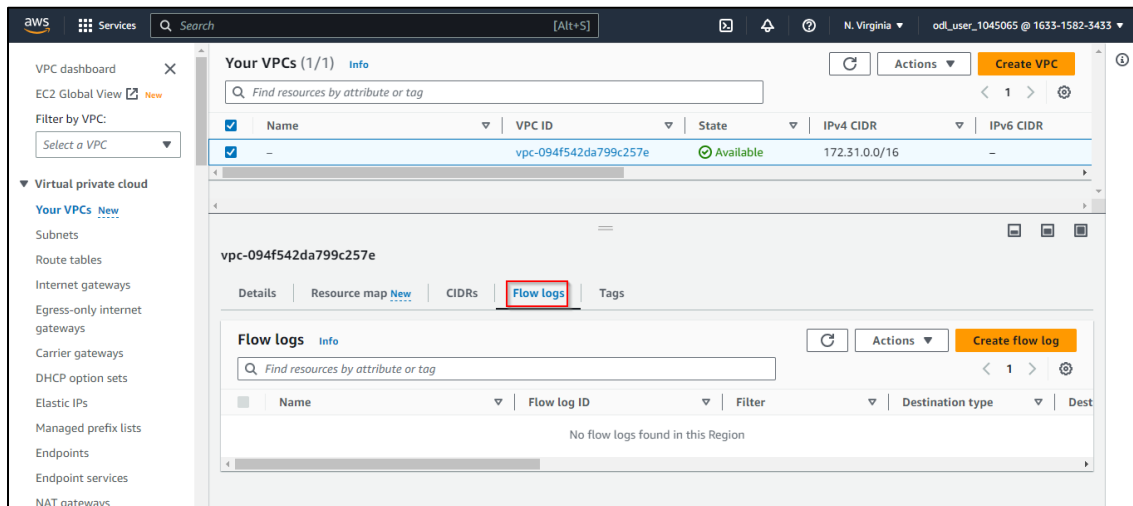
The screenshot shows the AWS VPC dashboard. On the left is a navigation sidebar with 'VPC dashboard' at the top and a list of VPC resources. The main area is titled 'Resources by Region' and displays a grid of resource counts for the US East region. The 'VPCs' resource is highlighted with a red rectangular box. Other resources shown include Subnets, NAT Gateways, Route Tables, VPC Peering Connections, Network ACLs, Internet Gateways, Security Groups, Egress-only Internet Gateways, and Customer Gateways.

1.3 Choose the default VPC

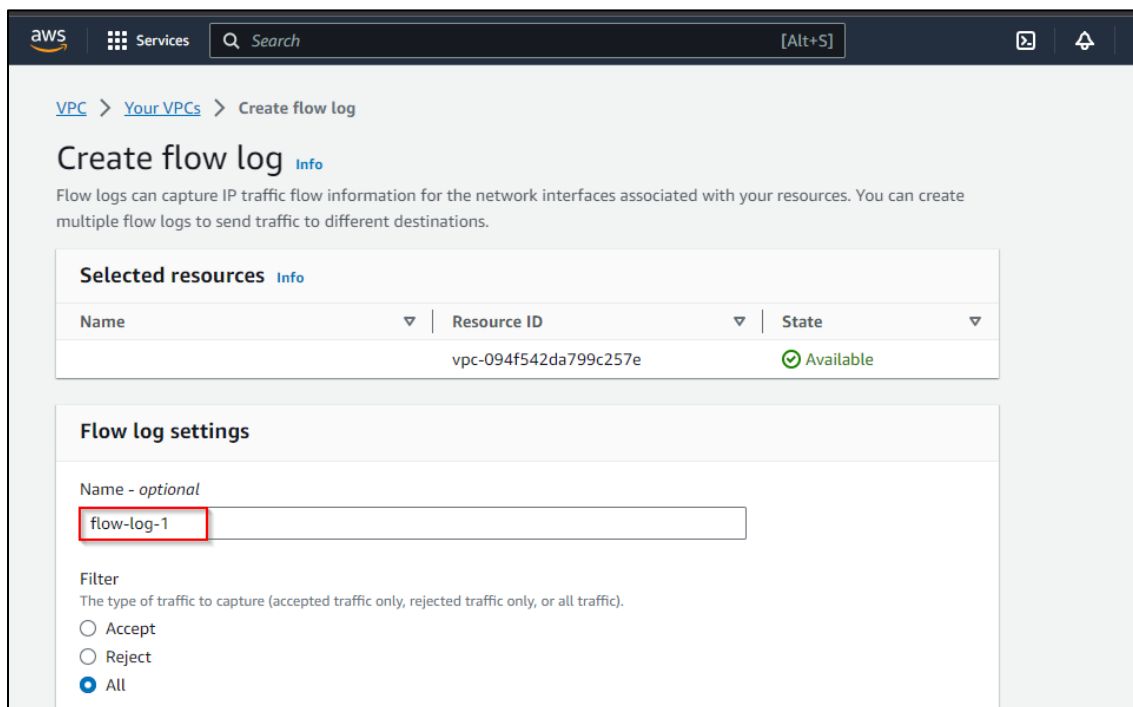
This screenshot shows the 'Your VPCs' page in the AWS console. A table lists the available VPCs. The first VPC is selected, indicated by a checked checkbox in the first column. Below the table, the details for the selected VPC are shown, including tabs for 'Details', 'Resource map', 'CIDRs', 'Flow logs', and 'Tags'.

<input checked="" type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
<input checked="" type="checkbox"/>	-	vpc-094f542da799c257e	Available	172.31.0.0/16	-

1.4 Click on **Flow logs**, then select **Create flow log**



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



1.6 Configure the log settings by setting the filter to **All**, maximum aggregation interval to **1 minute**, and 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

1.7 Obtain the **S3 bucket ARN**: Create a new S3 bucket, navigate to the **properties** tab, and copy the ARN. Paste the ARN in the **S3 bucket ARN** field.

☐ 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::testing--2023

[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

Format preview
\${version} \${account-id} \${interface-id} \${srcaddr} \${dstaddr} \${srcport} \${dstport} [Copy](#)

Note: Refer to the previous demos to know how to create S3 bucket

1.8 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 Value - optional

Q Name X Q flow-log-1 X Remove tag

Add tag

You can add 49 more tags

Cancel Create flow log

Successfully created flow log for vpc-094f542da799c257e. [Explore integration options](#)

Your VPCs (1/1) [Info](#)

[Find resources by attribute or tag](#)

<input checked="" type="checkbox"/>	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR
<input checked="" type="checkbox"/>	-	vpc-094f542da799c257e	Available	172.31.0.0/16	-

vpc-094f542da799c257e

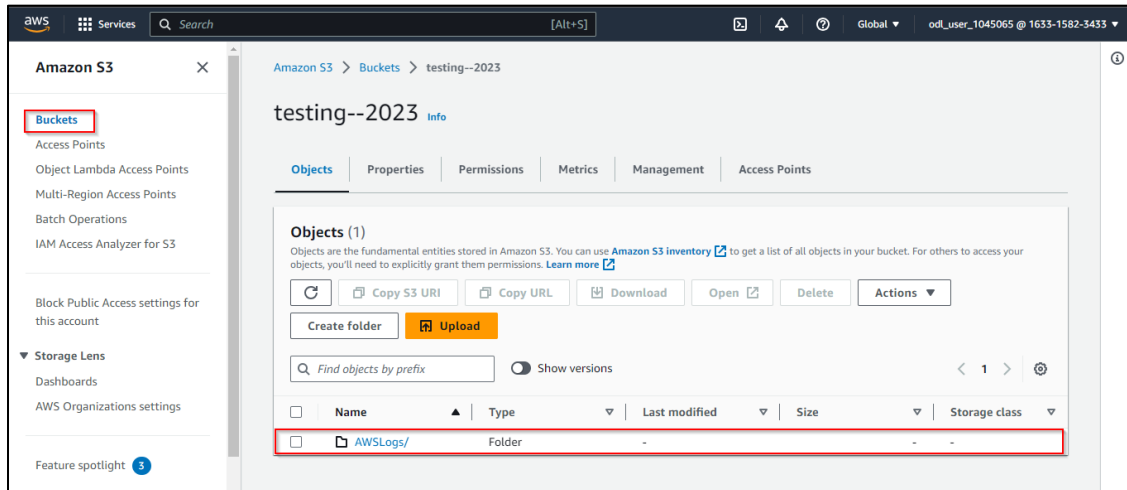
[Details](#) [Resource map](#) [CIDRs](#) [Flow logs](#) [Tags](#)

Details

VPC ID	State	DNS hostnames	DNS resolution
vpc-094f542da799c257e	Available	Enabled	Enabled
Tenancy	DHCP option set	Main route table	Main network ACL
Default	default	rtb-037dfc6f6c77d8f1e	acl-00460004b1f5b37c8

The flow log has been successfully created.

1.9 To view the flow log in S3, click on the **S3 bucket**, and you can see the flow log folder created in your bucket



By following these steps, we have successfully executed the creation of a VPC Flow Log in the AWS environment. This process involved accessing the VPC console, selecting the default VPC, and setting up the flow log.