Configure AWS VPC Flow Logs for CTB Input

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configuration Steps

- Step 1. Configure S3 Bucket in AWS
- Step 2. Create IAM User with Access key and Attach S3 Bucket Policy
- Step 3. Configure VPC Flow Logs
- Step 4. Configure VPC Input to CTB

Verify

Introduction

This document describes how to configure VPC Flow Logs as an input to Cisco Telemetry Broker (CTB).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Amazon Web Services (AWS)
- CTB admininstration.

Components Used

The information in this document is based on these software and hardware versions:

- CTB (v2.2.1+)
- AWS

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

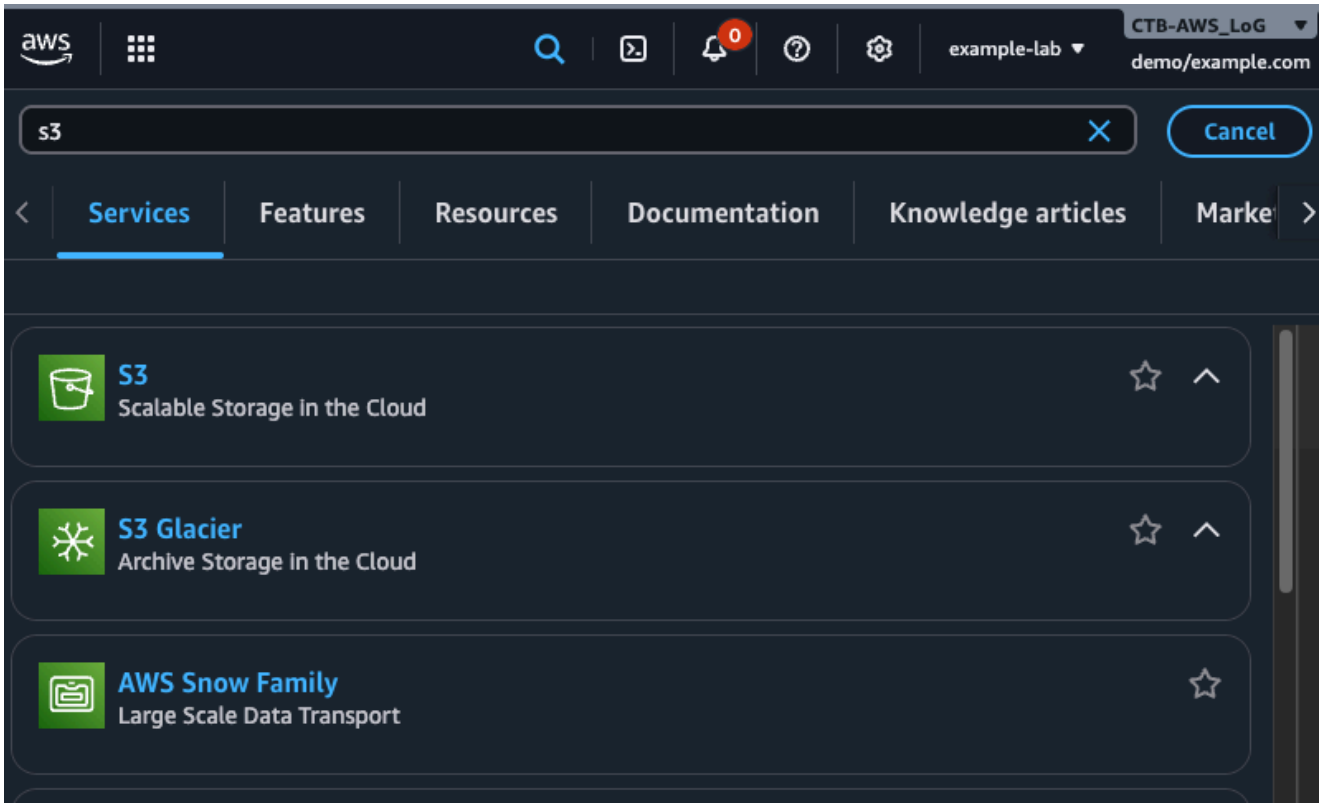
Configuration Steps

Step 1. Configure S3 Bucket in AWS

1: Log in to **AWS management console** with username and password.

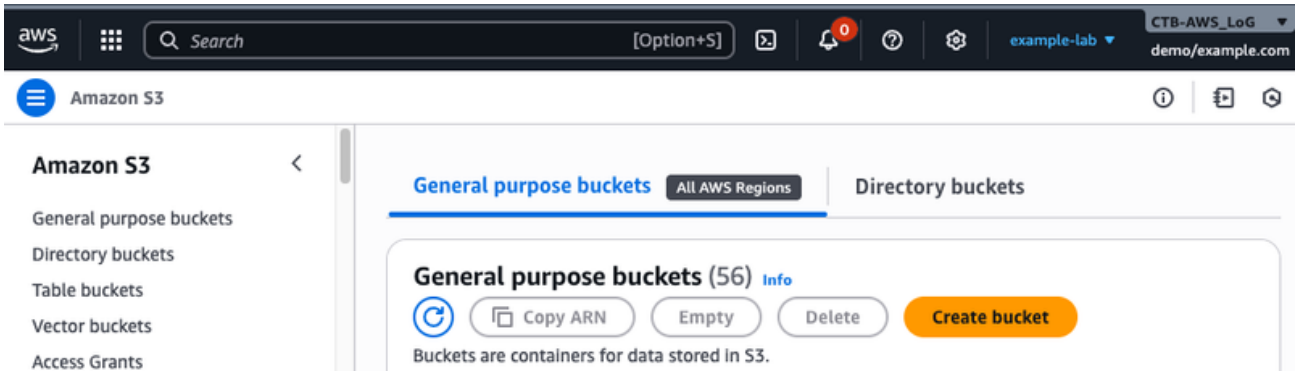
2: Ensure you log in to appropriate region.

3: Navigate to **search bar** and type **S3**.



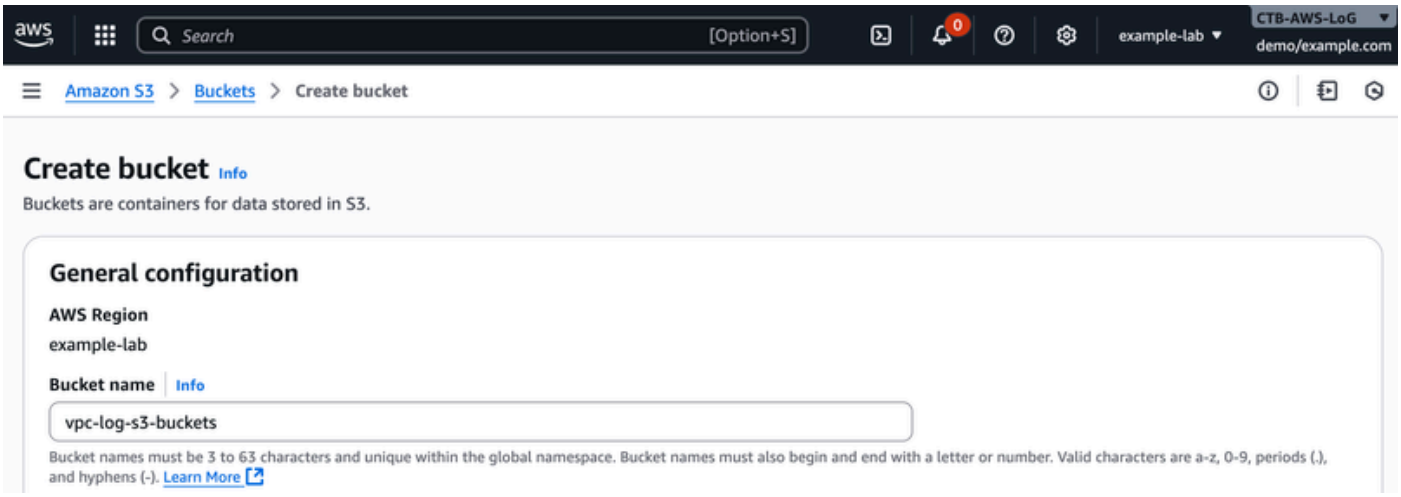
Navigating-To-S3-Bucket

4: Click **create bucket**.

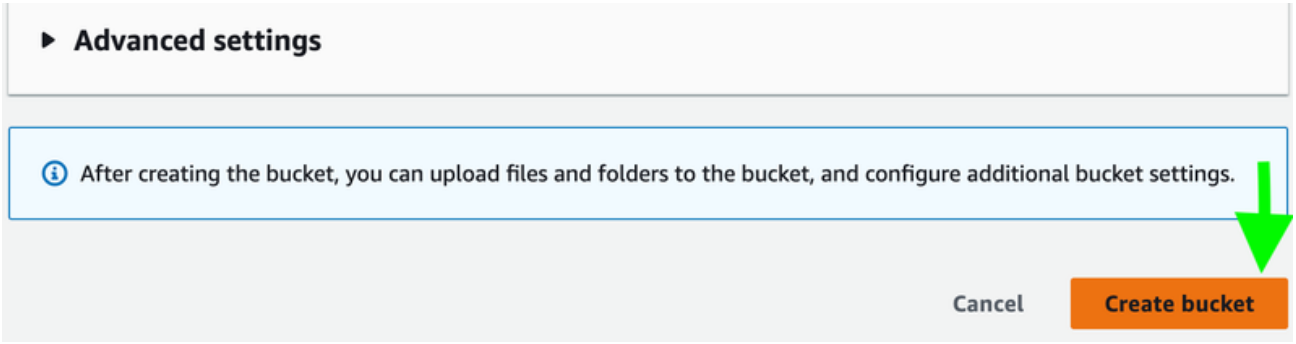


Click-Create-S3-Bucket

5: Define **bucket** name and leave every option as it is and click **create bucket** on the bottom of the page.

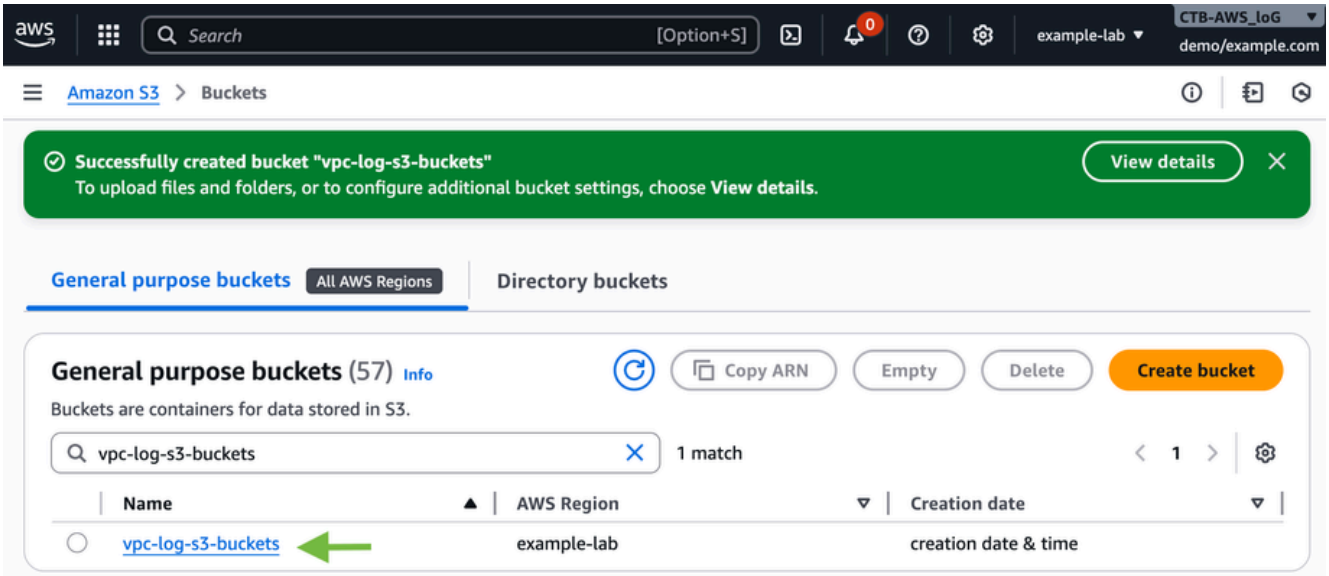


Name-S3-Bucket



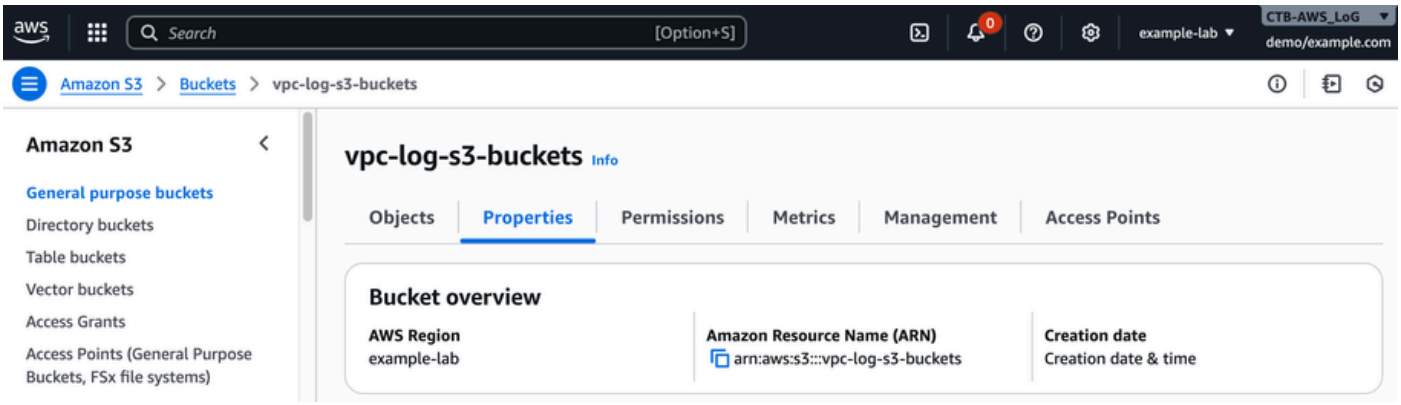
AWS-S3

6: Once bucket is successfully created, place the created bucket name on serach bar and click open to see details.



Review-Created-Bucket

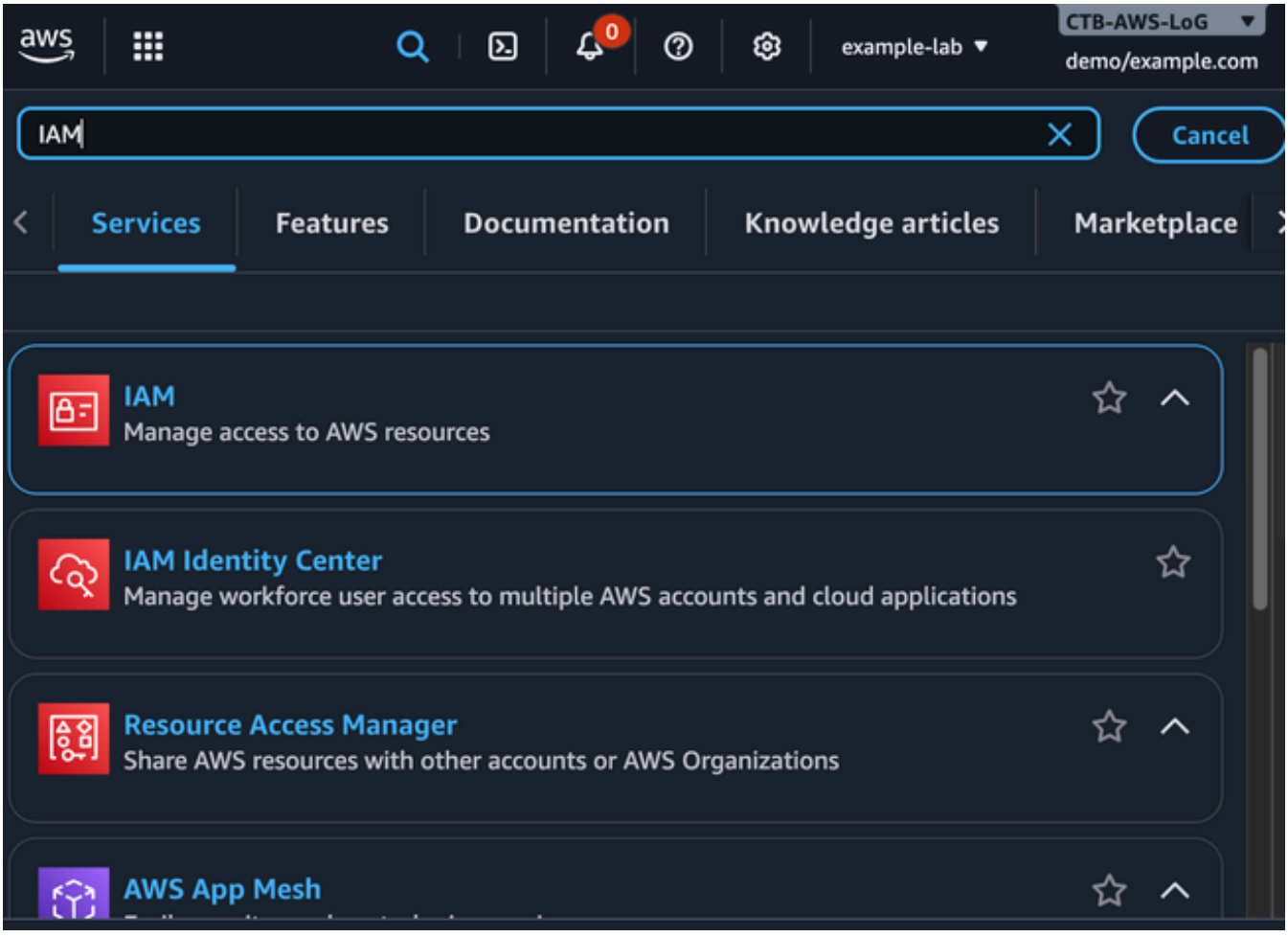
7: Switch the tab to **Properties** and save the **bucket ARN**.



Get-Bucket-ARN-Details

Step 2. Create IAM User with Access key and Attach S3 Bucket Policy

1: Launch the **IAM** from **aws search bar**.



Launch-IAM

2: Navigate to **users**.



Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

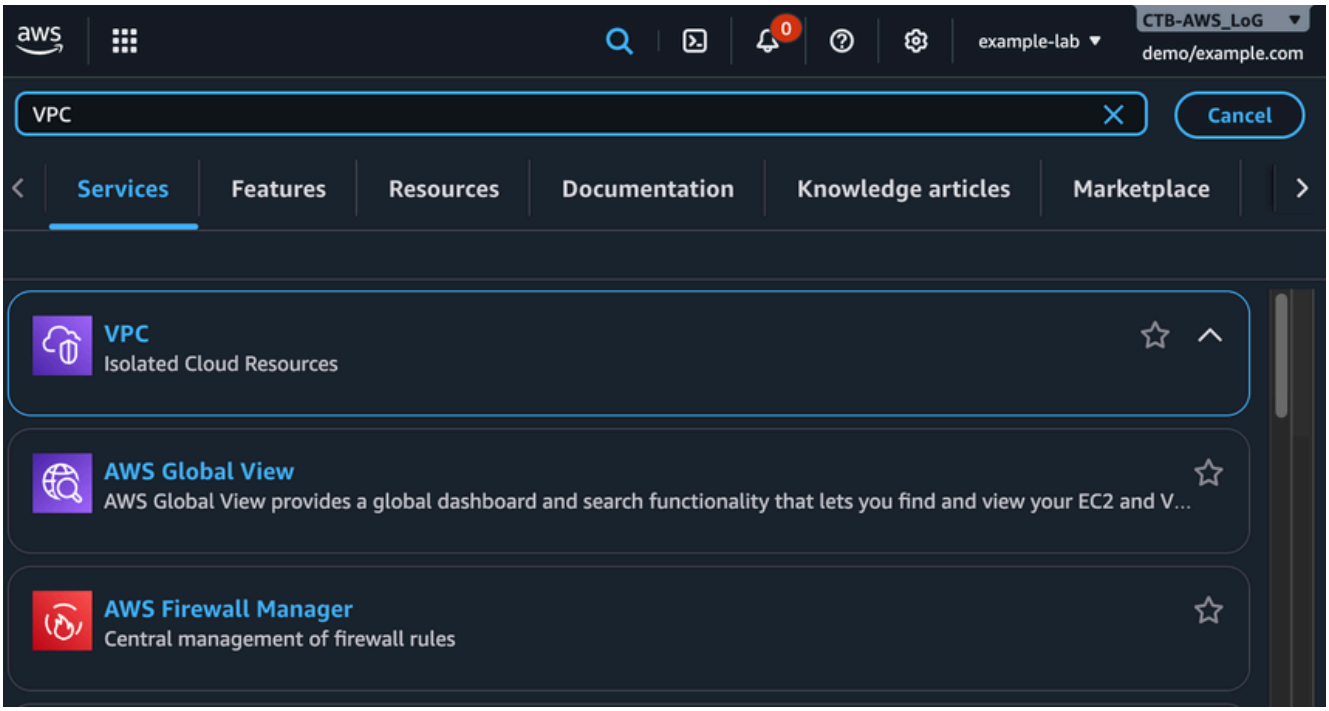
Roles

Policies

: The Access key in a csv file and it is no longer available to download or view once you navigate away from this page

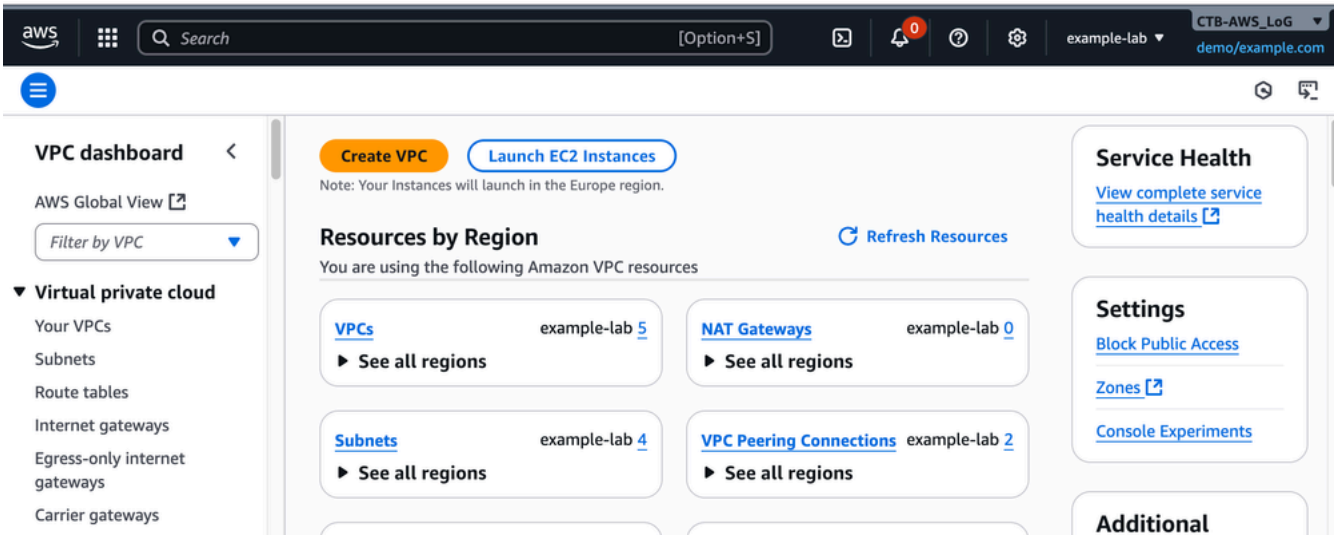
Step 3. Configure VPC Flow Logs

1: Launch your **VPC** on your desired region and navigate to **Your VPC** option.



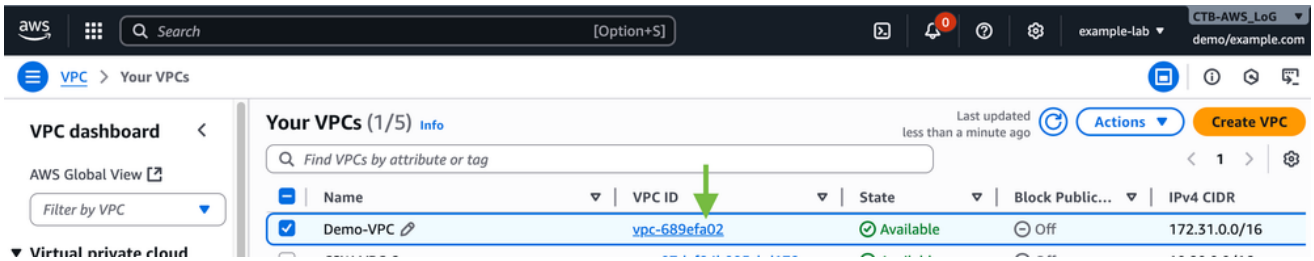
Launch-VPC

2: Click on **VPCs**.



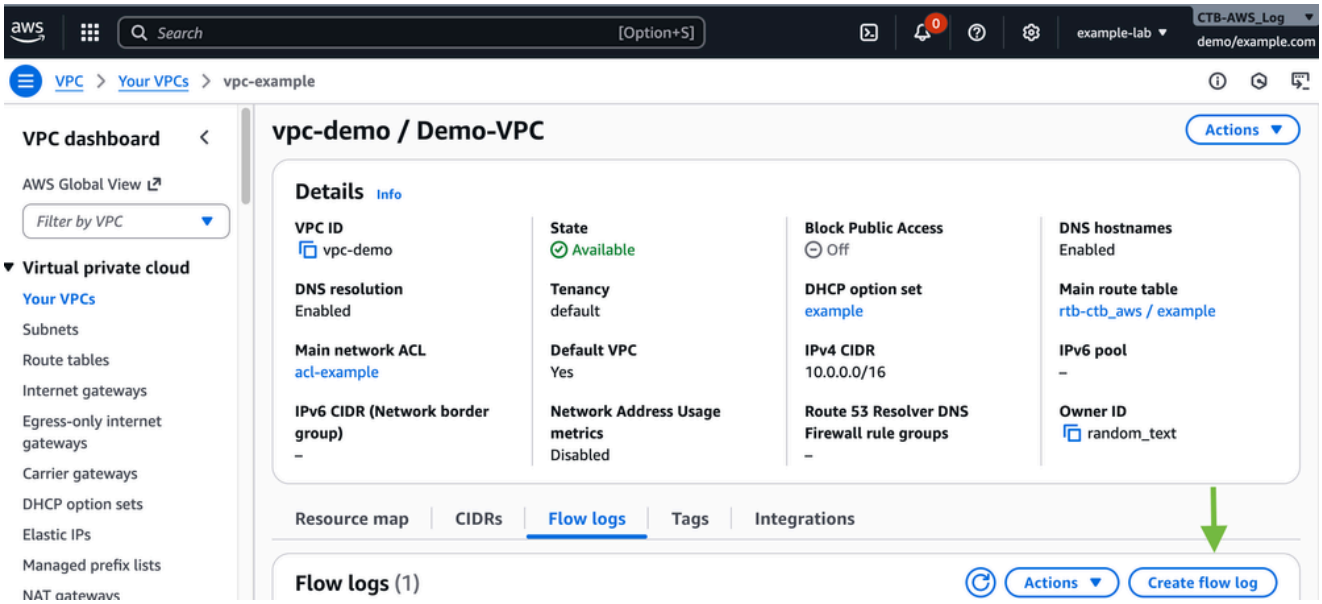
Click-VPC

3: Click on your **VPC ID** .



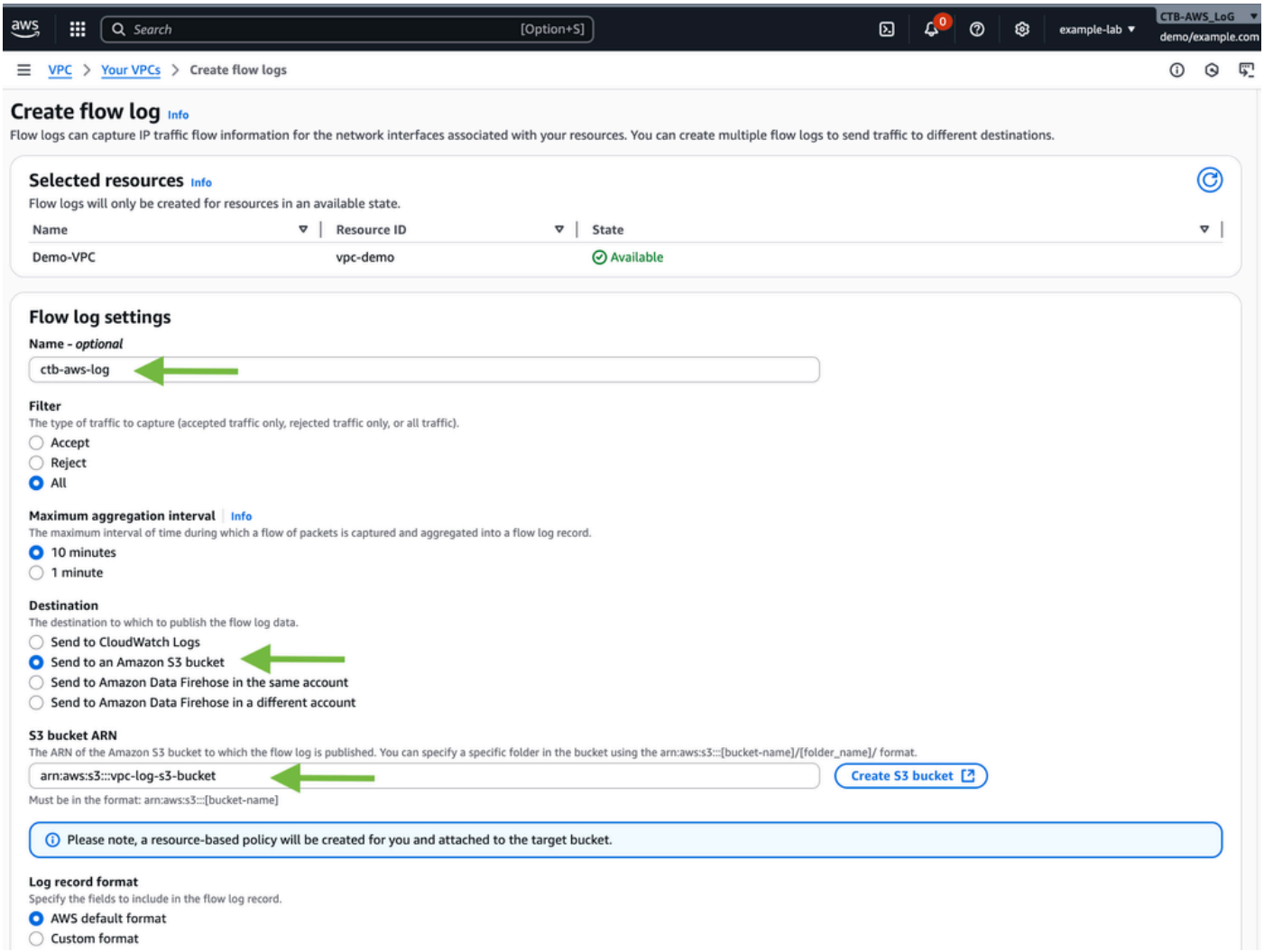
Open-VPC

4: Switch to **Flow Logs** tab and click **Create flow log**.



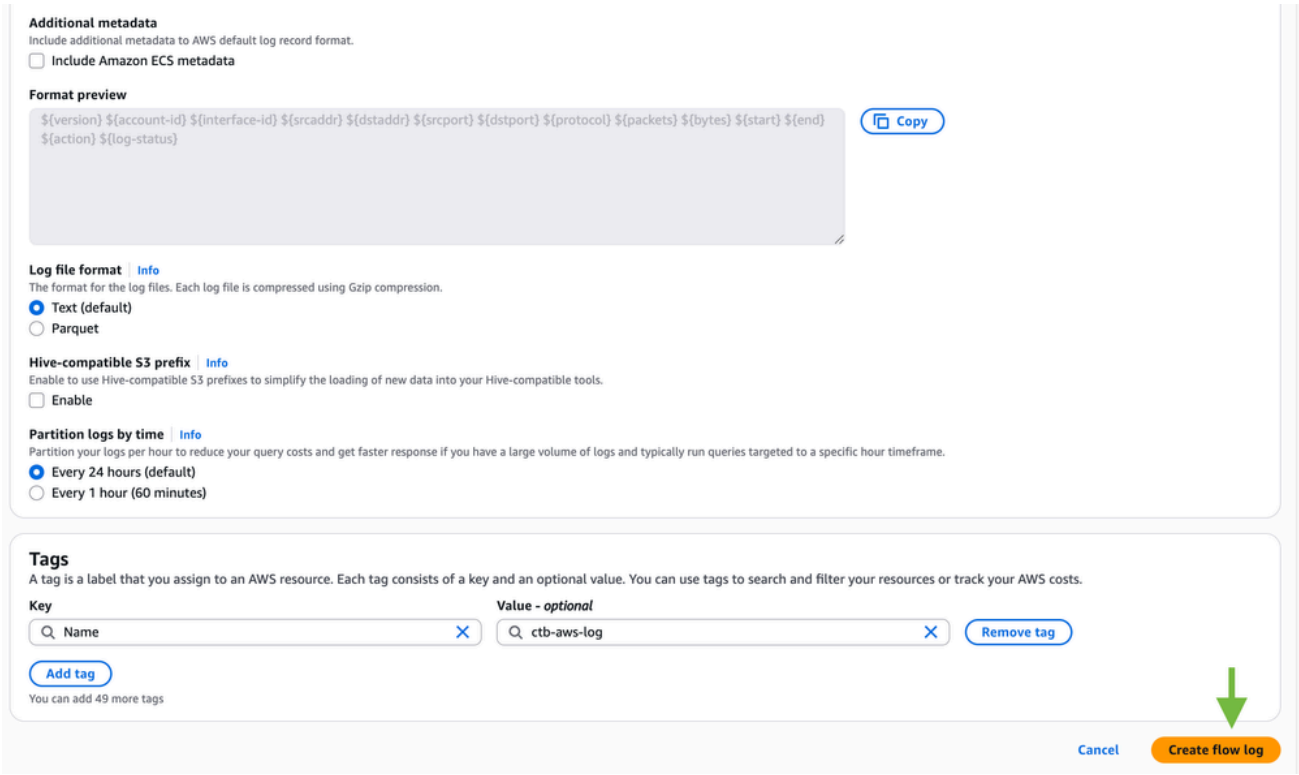
Click-Create-FlowLog

5:Under Flow log settings Select destination **send to an Amazon S3 bucket** , enter **S3 Bucket ARN,** leave everything as default and **click create flow log**.



Flow-log-Details

.

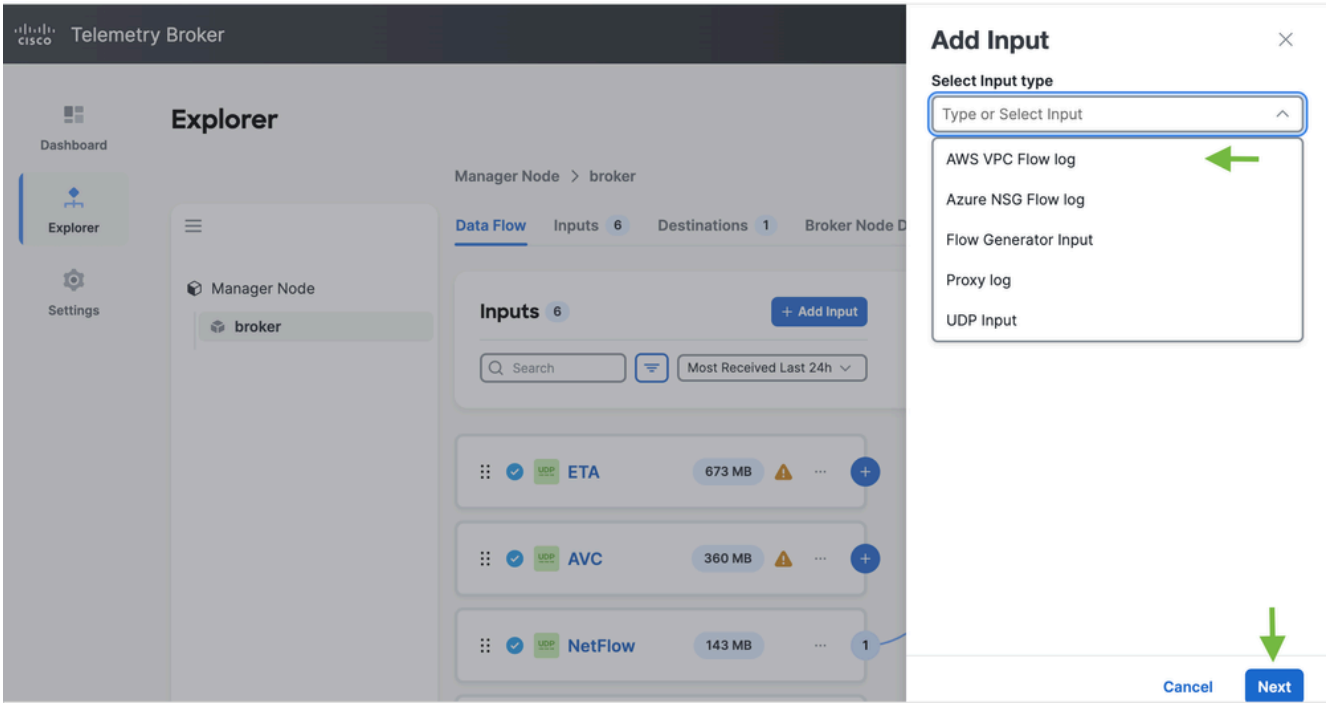


Click-Create

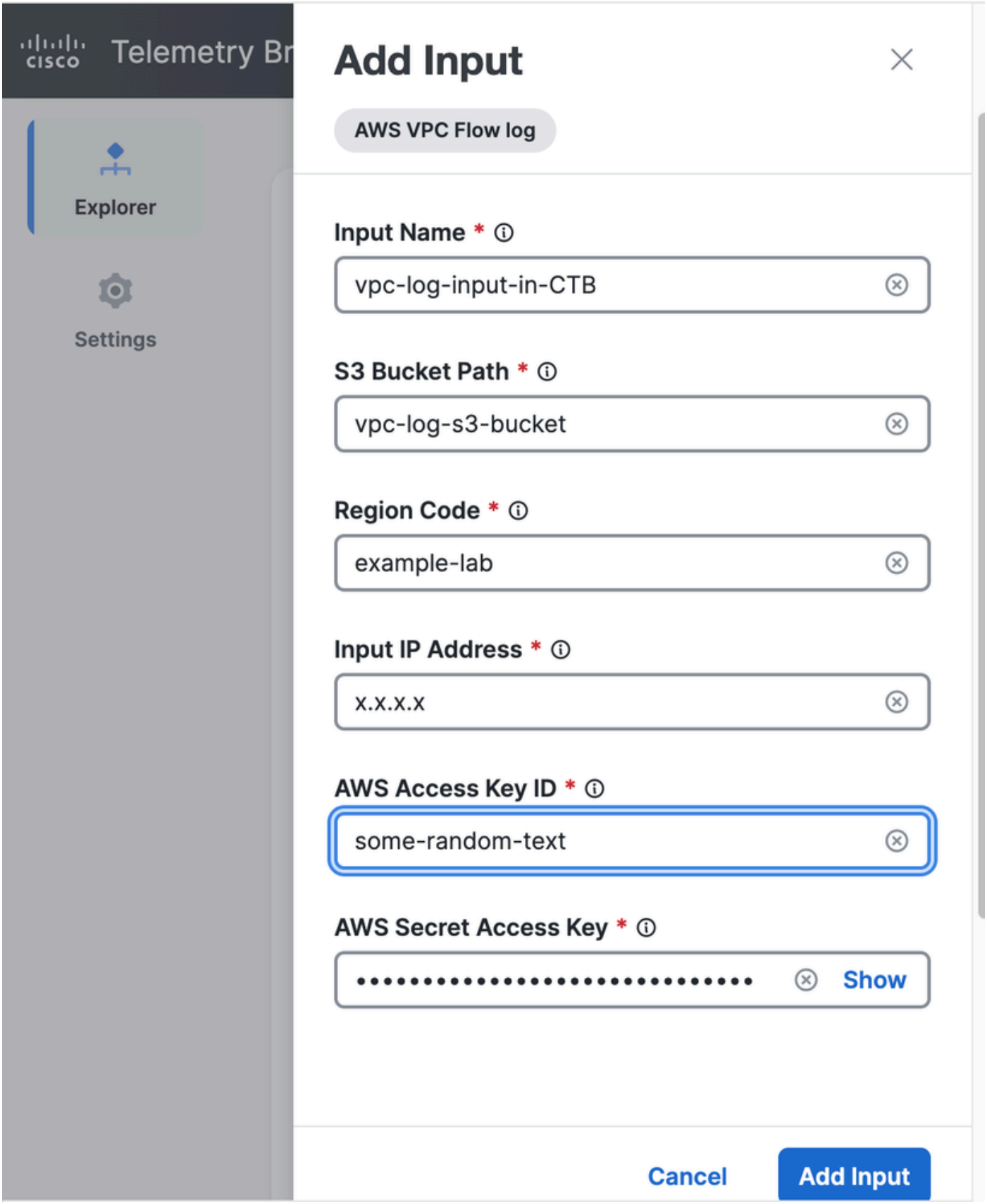
Step 4. Configure VPC Input to CTB

1: Access **CTB Web UI**, navigate to **Explorer> Broker node tab > click open broker node >Data Flow tab > Click Add Input.**

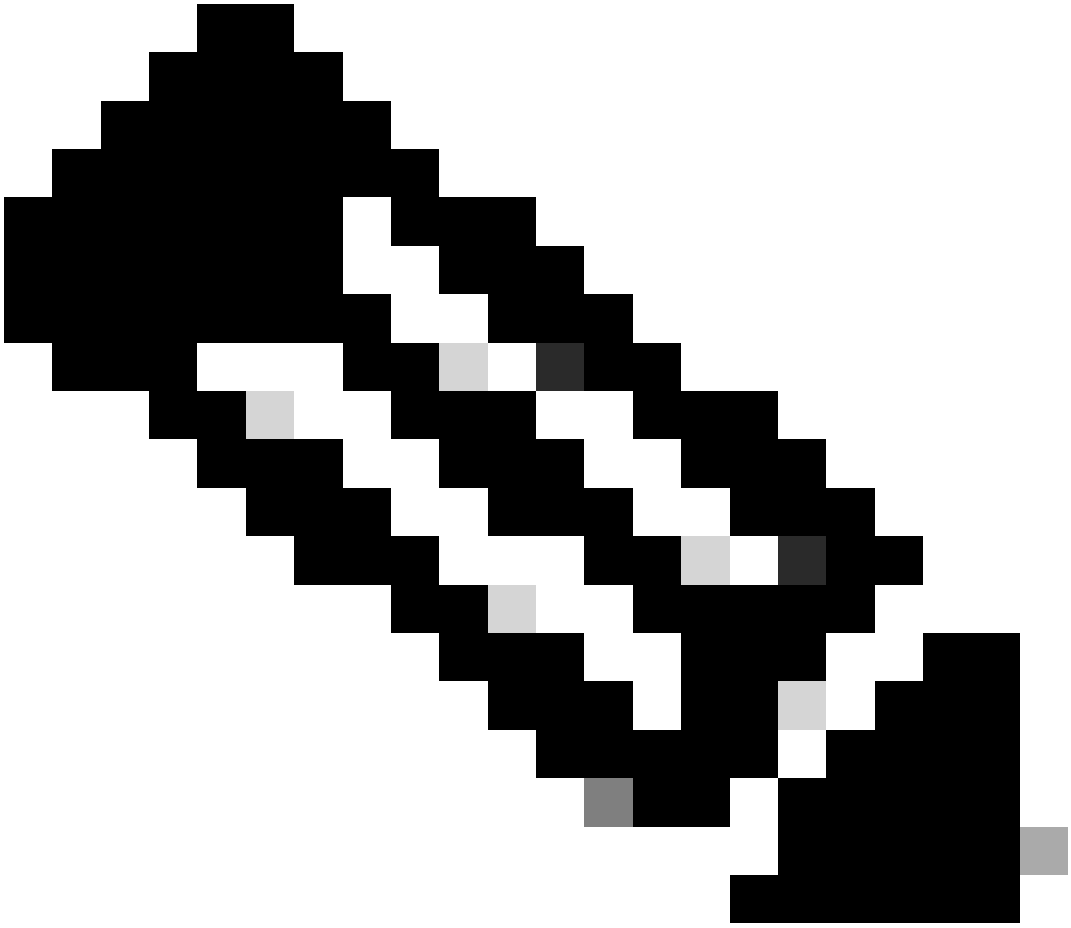
2: Select Input type **AWS VPC Flow log and** click **next.**



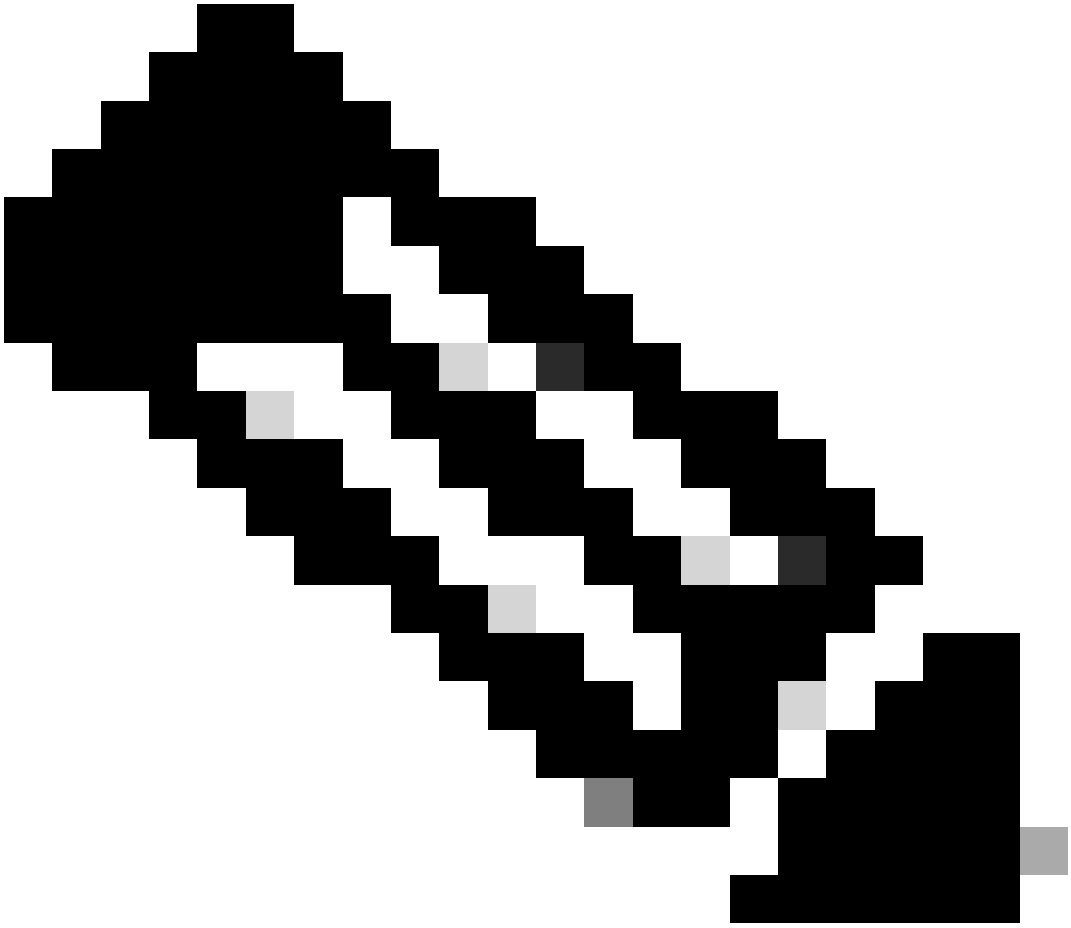
2: Fill the details **Input name**, **S3 Bucket Path**, **Region Code**, **Input IP Address**, **AWS Access Key ID**, **AWS Secret Access Key** and click **Add input**.



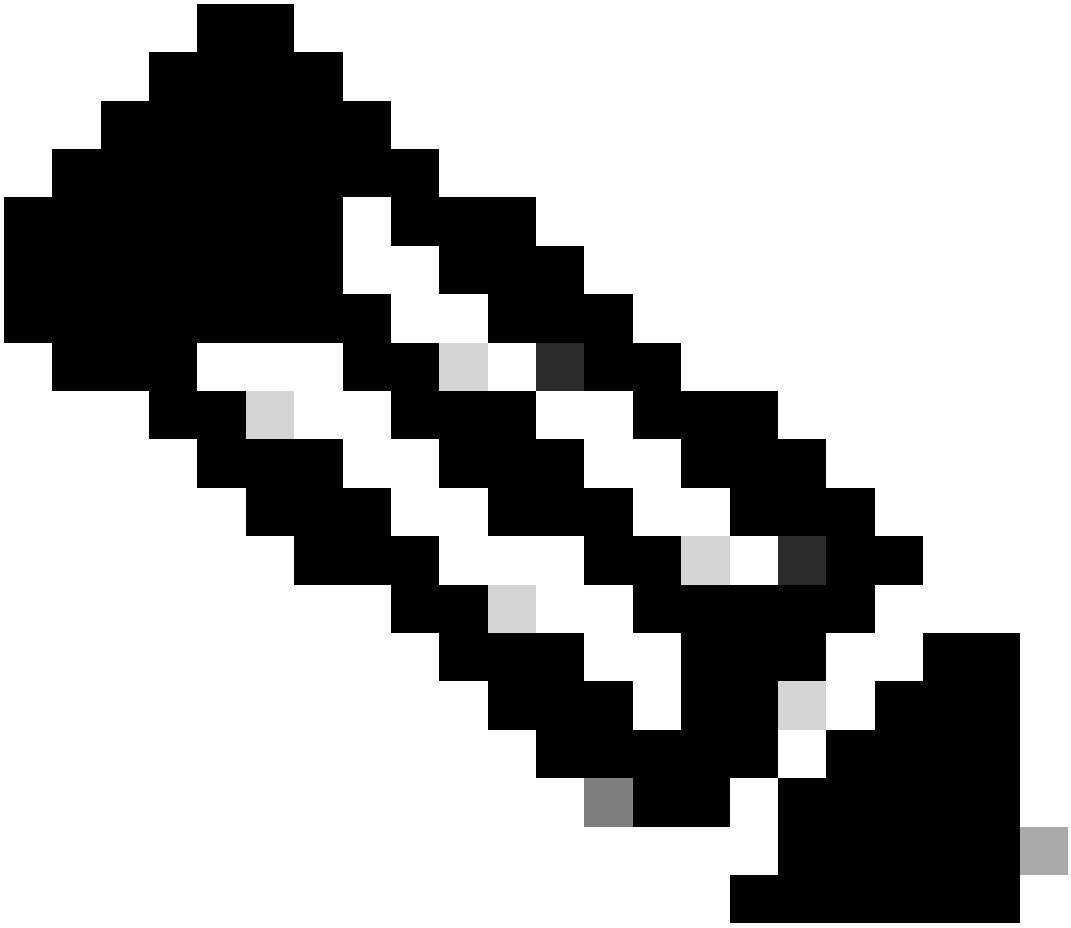
Input-parameter-in CTB



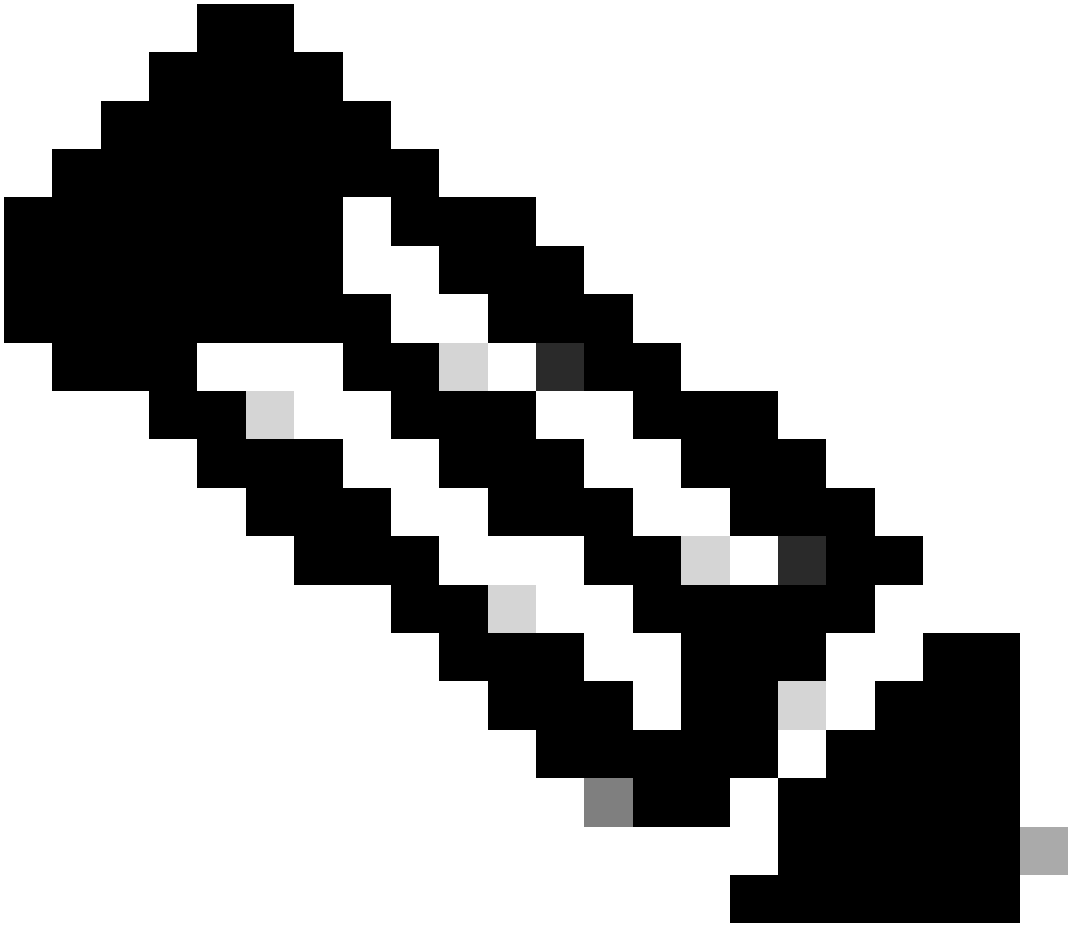
Note: S3 Bucket Path is bucket-name/Optional suffix.



Note: For Region code, see AWS home page next to gear icon.



Note: Any IP Address configured as the Input IP Address (unique IP not shared by any other exporter) is reported as the exporter for the transformed netflow data.



Note: For AWS Access Key ID, see Configure IAM user for access key with S3 access policy, step 10

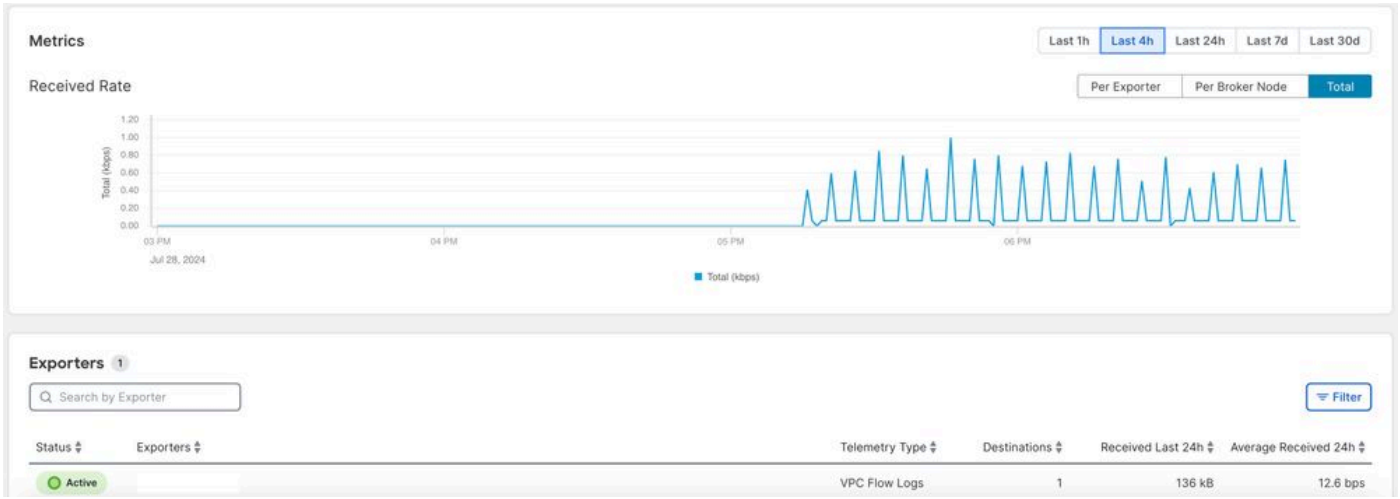
Verify

After a few minutes of configuring AWS VPC input, the status column becomes active if the AWS S3 bucket has data in it.

Verify the status of AWS VPC input using these steps.

1: Log in to CTB UI and navigate to**Explorer> Broker node tab > click openbroker node >switch tab toInput >Click open AWS input**.

2: Verify that configured aws-flow logs have active status and received metric have rising graph.


Metrics
Last 1h
Last 4h
Last 24h
Last 7d
Last 30d
Received Rate
Per Exporter
Per Broker Node
Total
Total (kbps)
1.20
1.00
0.80
0.60
0.40
0.20
0.00
03 PM
04 PM
05 PM
06 PM
Jul 28, 2024
Total (kbps)
Exporters 1
Search by Exporter
Filter
Status
Exporters
Telemetry Type
Destinations
Received Last 24h
Average Received 24h
Active
VPC Flow Logs
1
136 kB
12.6 bps

CTB-Input-UI