

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 administration.

Components Used

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

- CTB (v2.2.1+)
- AWS

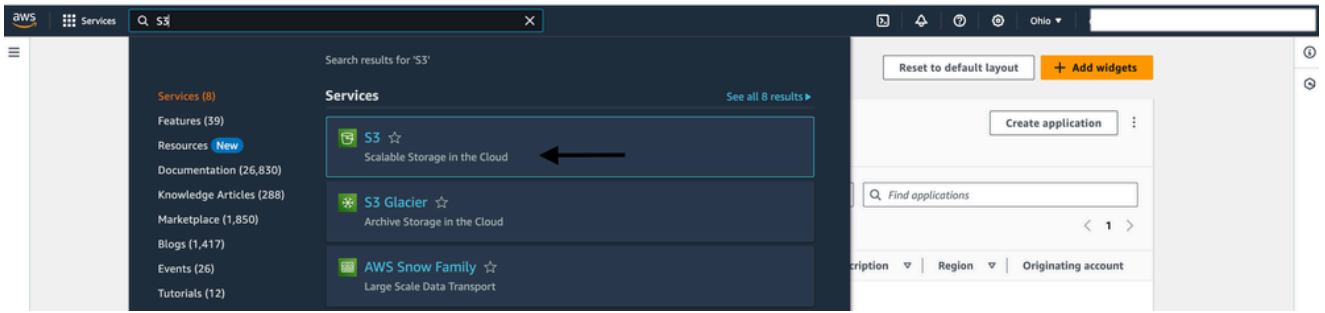
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configuration Steps

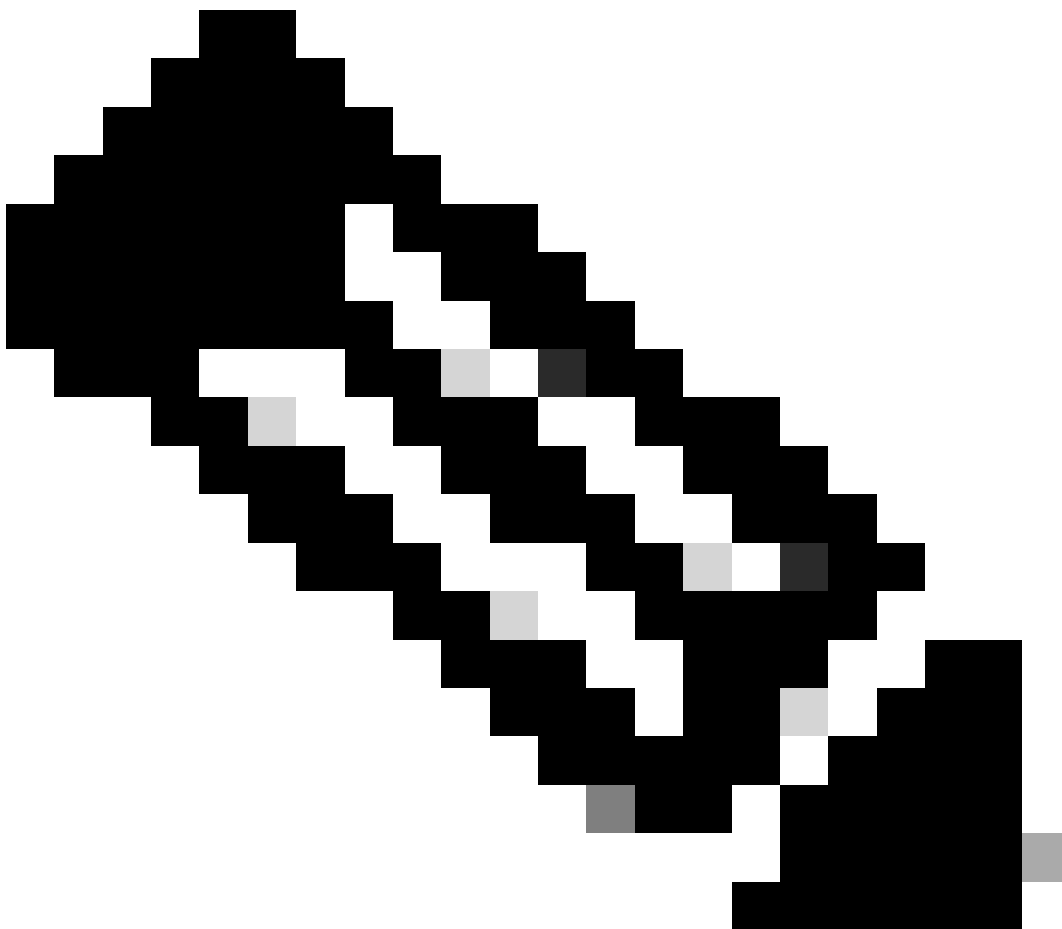
Step 1. Configure S3 Bucket in AWS

- 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**.

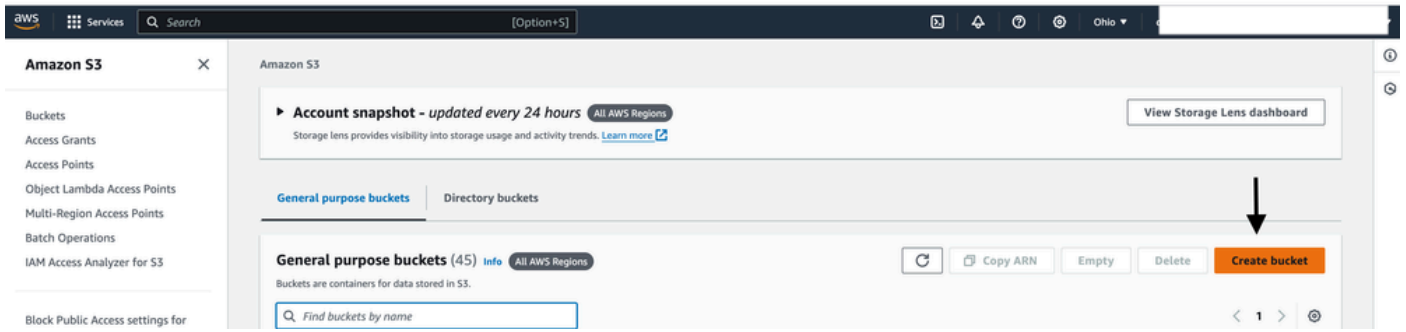


AWS-Dashboard



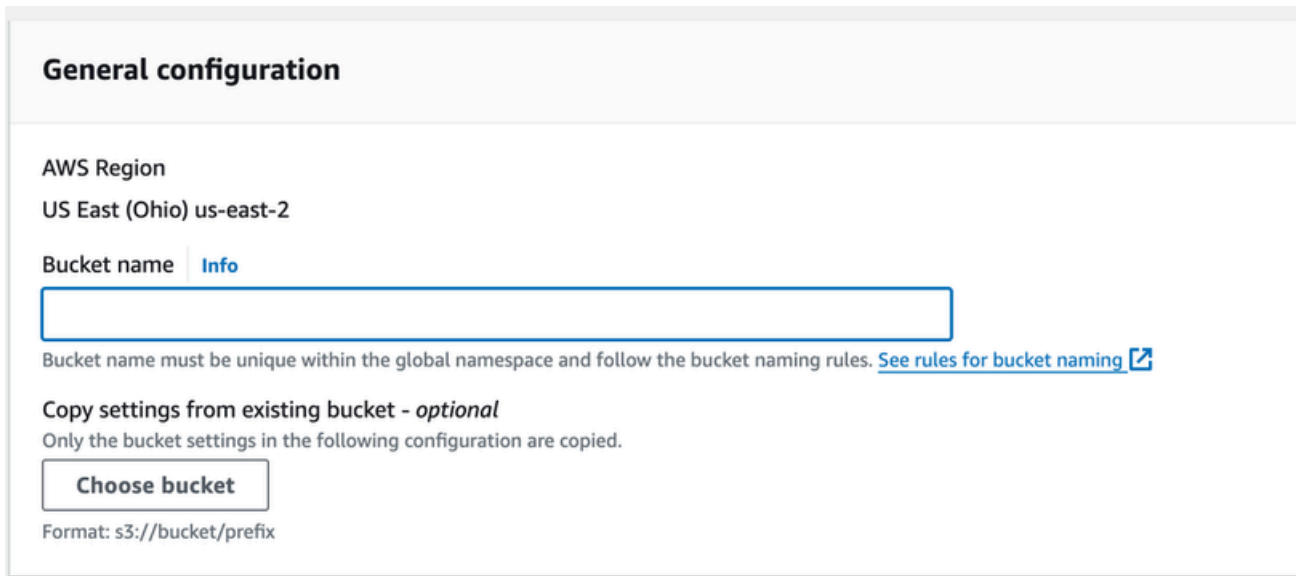
Note: In demo, you have selected Ohio region with us-east-2 availability zone, it is visible right next to the gear icon.

4: Click **create bucket**.

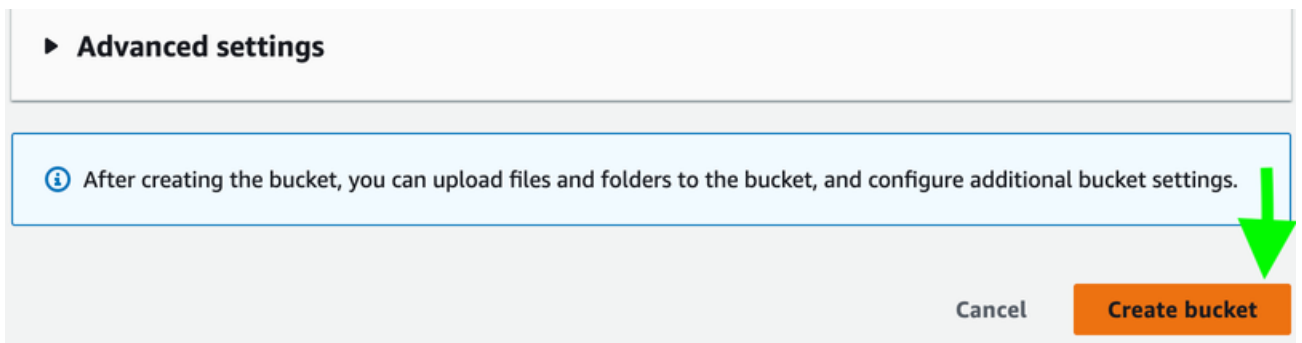


AWS-S3

5: Give **bucket** a name and leave every option as it is and click **create**.

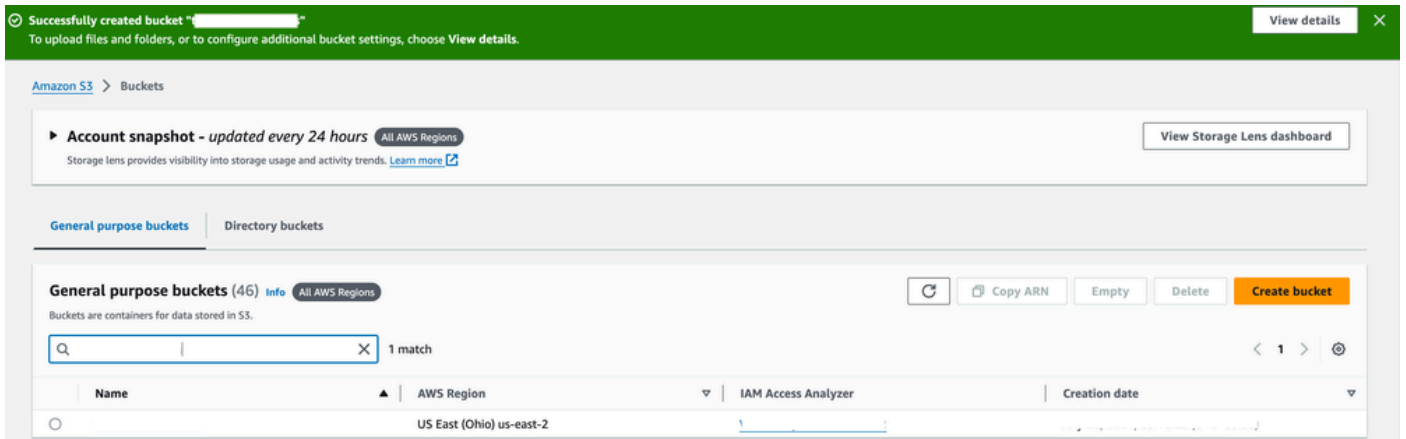


AWS-S3

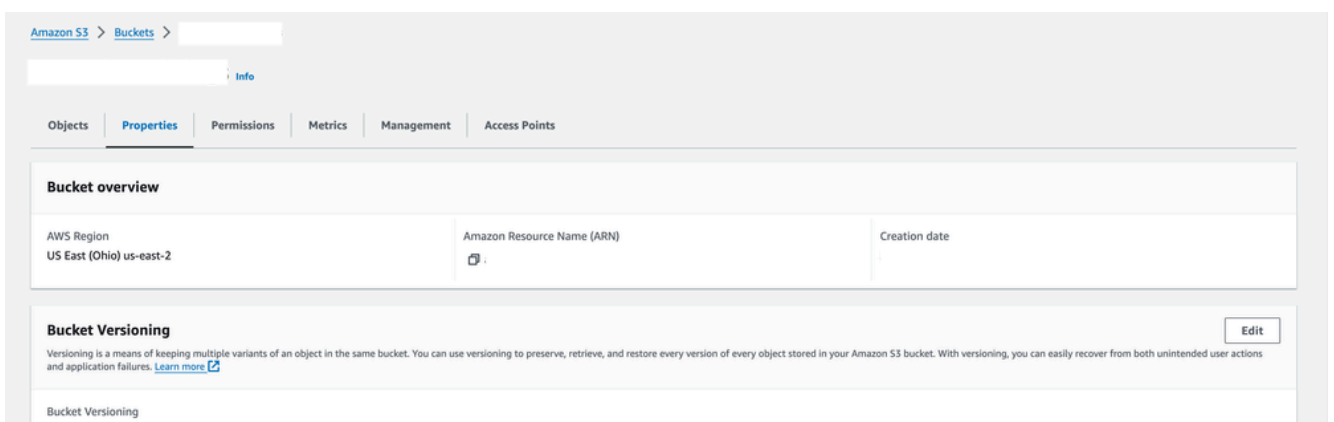


AWS-S3

6: Once bucket is successfully created, save the **bucket ARN** which is to be used later during the configuration.



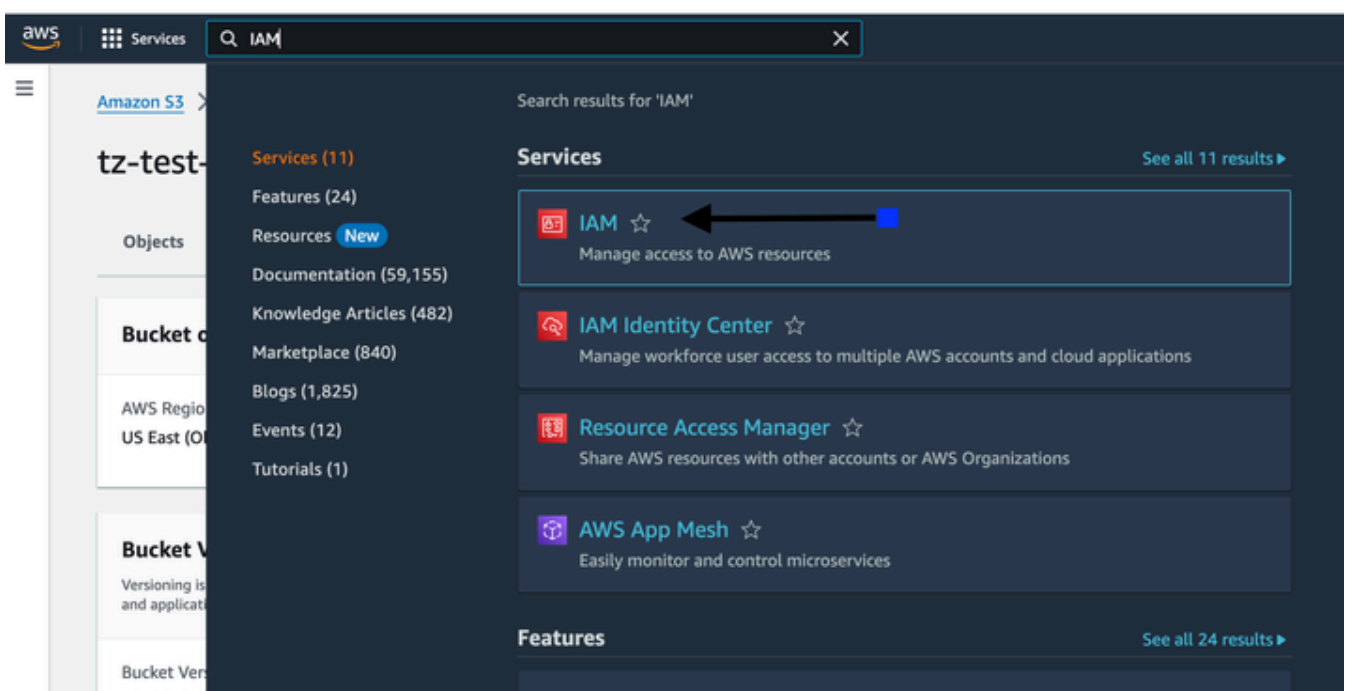
AWS-S3



AWS-S3

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

1: Launch the IAM from aws search bar.



2: Navigate to **users**.



Services



Search

Identity and Access Management (IAM)



Search IAM

Dashboard

▼ Access management

User groups

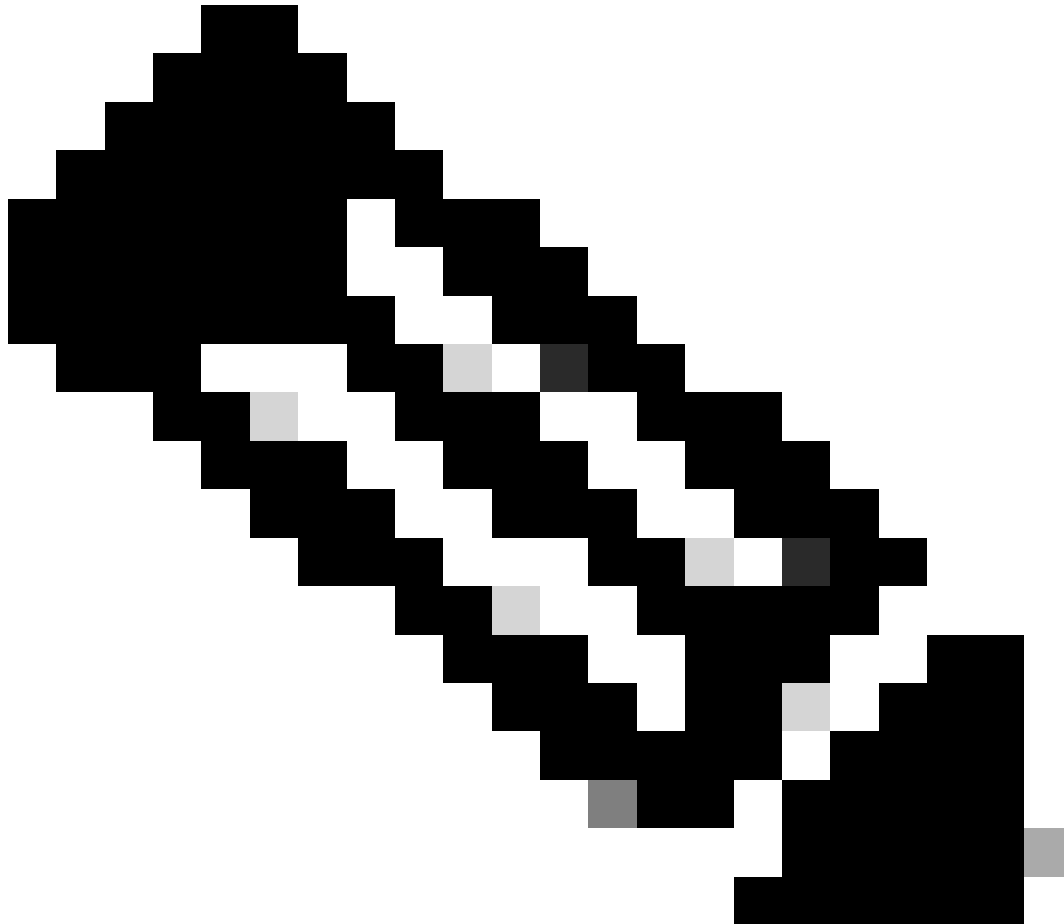
Users

Roles

Policies

: By unchecking the AWS management console access box, it prevents the user from logging in to AWS account using web UI.

6: Assign **policy** by assigning it to the user, directly attaching it to a group or configuring it inline.



Note: For demonstration, you directly assign policy to the user. For more information - [Managing AWS Policies](#)

7: Search for **S3 full access** and select **AmazonS3full** access, which allows the user to have full access for every S3 bucket created on its corresponding AWS account.

8: Check the box with policy name **AmazonS3FullAccess** and click **next**.

IAM > Users > Create user

Step 1
Specify user details

Step 2
Set permissions

Step 3
Review and create

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

- Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1250) Refresh Create policy

Choose one or more policies to attach to your new user.

Filter by Type

Search: s3full Clear | All types | 1 match

<input type="checkbox"/>	Policy name	Type	Attached entities
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	6

Set permissions boundary - optional

Cancel Previous Next

AWS-IAM

1 policy added

Permissions | Groups | Tags (1) | Security credentials | Access Advisor

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Search: | Filter by Type: All types | 1 match

<input type="checkbox"/>	Policy name	Type	Attached via
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	Directly

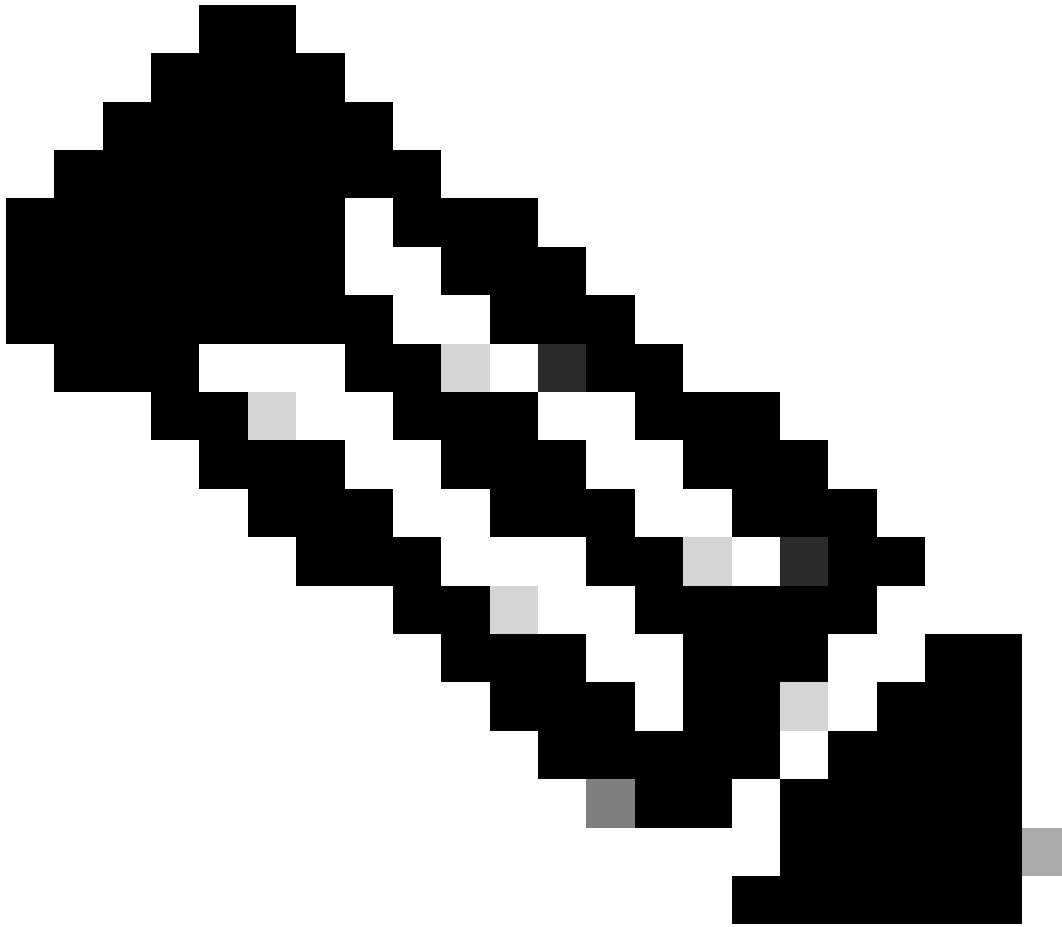
AmazonS3FullAccess Copy JSON

Provides full access to all buckets via the AWS Management Console.

```

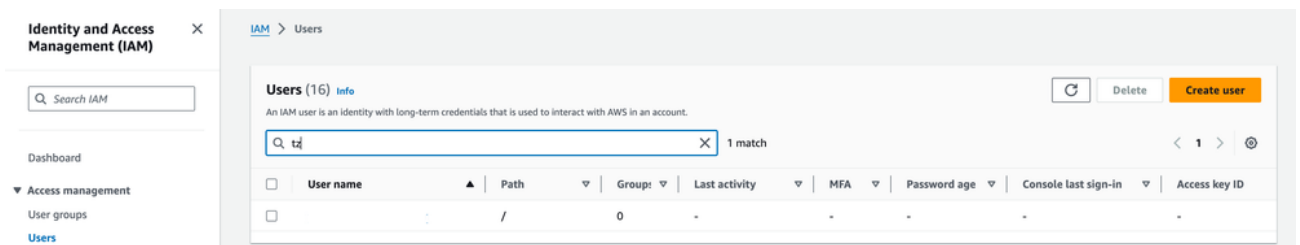
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": [
7-         "s3:*",
8-         "s3-object-lambda:*"
9-       ],
10-      "Resource": "*"
11-     }
12-   ]
13- }
```

AWS-IAM



Note: You can create more granular policy by allowing only specific bucket as well, please navigate to [Policy creation](#) to create your S3 bucket policy in json format.

9: Once user is created, list the **user** and navigate to **security credential** tab and click **create access key**.



Permissions | Groups | Tags | **Security credentials** | Access Advisor

Console sign-in Enable console access

Console sign-in link Console password
Not enabled

Multi-factor authentication (MFA) (0) Remove Resync Assign MFA device

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			
Assign MFA device			

Access keys (0) Create access key

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

No access keys. As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)

[Create access key](#)

AWS-IAM

10: Select the **other** radio button and optionally add a **tag**.

Access key best practices & alternatives Info

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

- Command Line Interface (CLI)**
You plan to use this access key to enable the AWS CLI to access your AWS account.
- Local code**
You plan to use this access key to enable application code in a local development environment to access your AWS account.
- Application running on an AWS compute service**
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.
- Third-party service**
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.
- Application running outside AWS**
You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.
- Other**
Your use case is not listed here.

AWS-IAM

Other
Your use case is not listed here.

It's okay to use an access key for this use case, but follow the best practices:

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access keys when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

Cancel **Next**

AWS-IAM

Set description tag - optional Info

The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value
Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ . : / = + - @

Cancel Previous **Create access key**

AWS-IAM

11: Click **Download .csv file**. This is the Access key in a csv file and it is no longer available to download or view once you navigate away from this page.

Access key created
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

IAM > Users > [User] > Create access key

Step 1
[Access key best practices & alternatives](#)

Step 2 - optional
[Set description tag](#)

Step 3
Retrieve access keys

Retrieve access keys Info

Access key
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
	***** Show

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

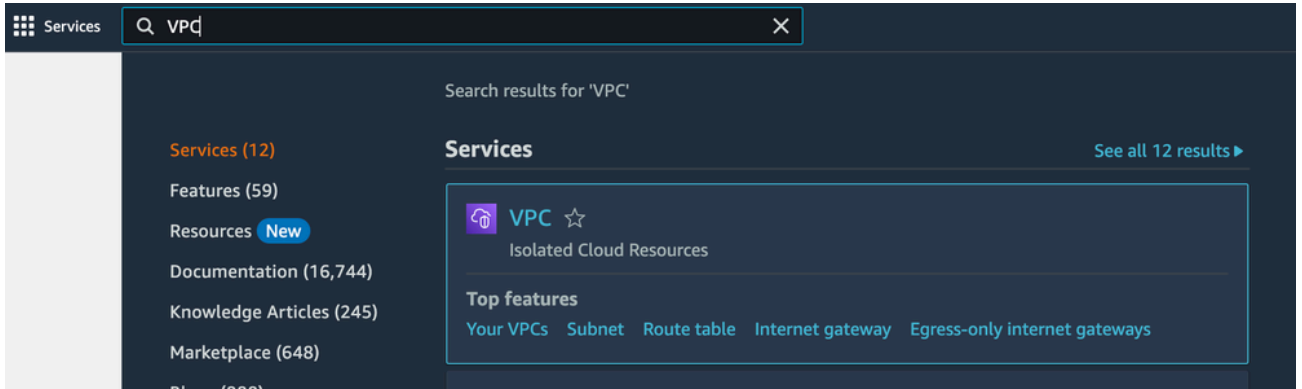
For more details about managing access keys, see the [best practices for managing AWS access keys](#).

[Download .csv file](#) **Done**

AWS-IAM

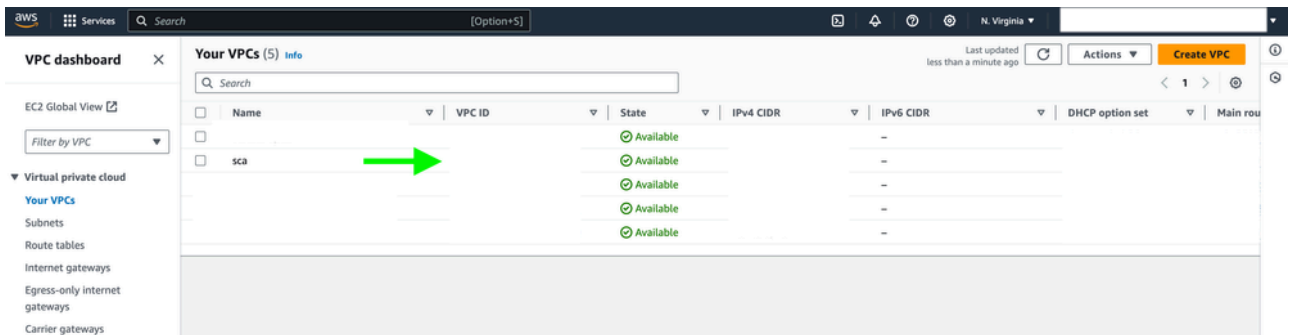
Step 3. Configure VPC Flow Logs

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



AWS-Flow-Logs

2: Select your **VPC** from the list showing on the screen.



AWS-Flow-Logs



Note: You have selected VPC name SCA in this demo.

3: Navigate to **Your VPCs** under **Virtual private cloud**, switch to the **Flow logs** tab and click **Create flow logs**.

The screenshot shows the AWS VPC console interface. The left sidebar contains navigation options for 'Virtual private cloud' and 'Security'. The main content area displays details for VPC 'vpc-60bdda1d / sca'. Below the details, the 'Flow logs' tab is active, showing a table with 4 flow logs. The 'Create flow log' button is highlighted in orange, and a black arrow points to it from the right side of the details section.

Name	Flow log ID	Filter	Destination type	Destination name	IAM role ARN
		ALL			
		ALL			
		ALL			
		ALL			

AWS-Flow-Logs

4: Give your flow logs a **name** and share the **S3 bucket ARN** created earlier.



Note: For ARN, see Configure S3 bucket - Step 6

5: You have an option to go with AWS default log format or create custom log format in case if more fields are required.

[VPC](#) > [Your VPCs](#) > Create flow log

Create flow log [Info](#)

Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple flow logs to send traffic to different destinations.

Selected resources [Info](#)

Name	Resource ID	State
		✔ Available

Flow log settings

Name - *optional*

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](#)

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

Additional metadata

Include additional metadata to AWS default log record format.

- Include Amazon ECS metadata

Format preview

```
 ${version} ${account-id} ${interface-id} ${srcaddr} ${dstaddr} ${srcport} ${dstport}
 ${protocol} ${packets} ${bytes} ${start} ${end} ${action} ${log-status}
```

 Copy

Log file format [Info](#)

The format for the log files. Each log file is compressed using Gzip compression.

- 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

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](#)

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

Log format

Specify the fields to include in the flow log record.

Format preview

```
{account-id} {action} {az-id} {bytes} {dstaddr} {dstport} {end} {flow-direction} {instance-id} {interface-id} {log-status} {packets} {pkt-dst-aws-
```

Log file format [Info](#)
 The format for the log files. Each log file is compressed using Gzip compression.

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:

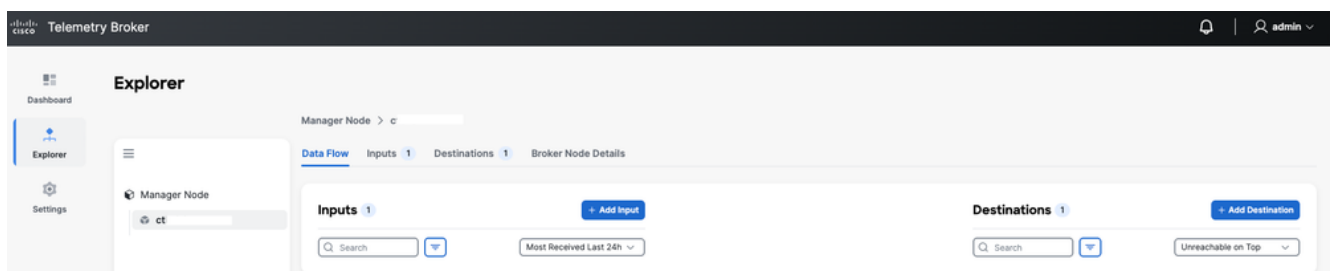
You can add 49 more tags



AWS-Flow-Logs

Step 4. Configure VPC Input to CTB

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



CTB-Input-UI

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

Add Input



Select Input type

Type or Select Input



UDP Input

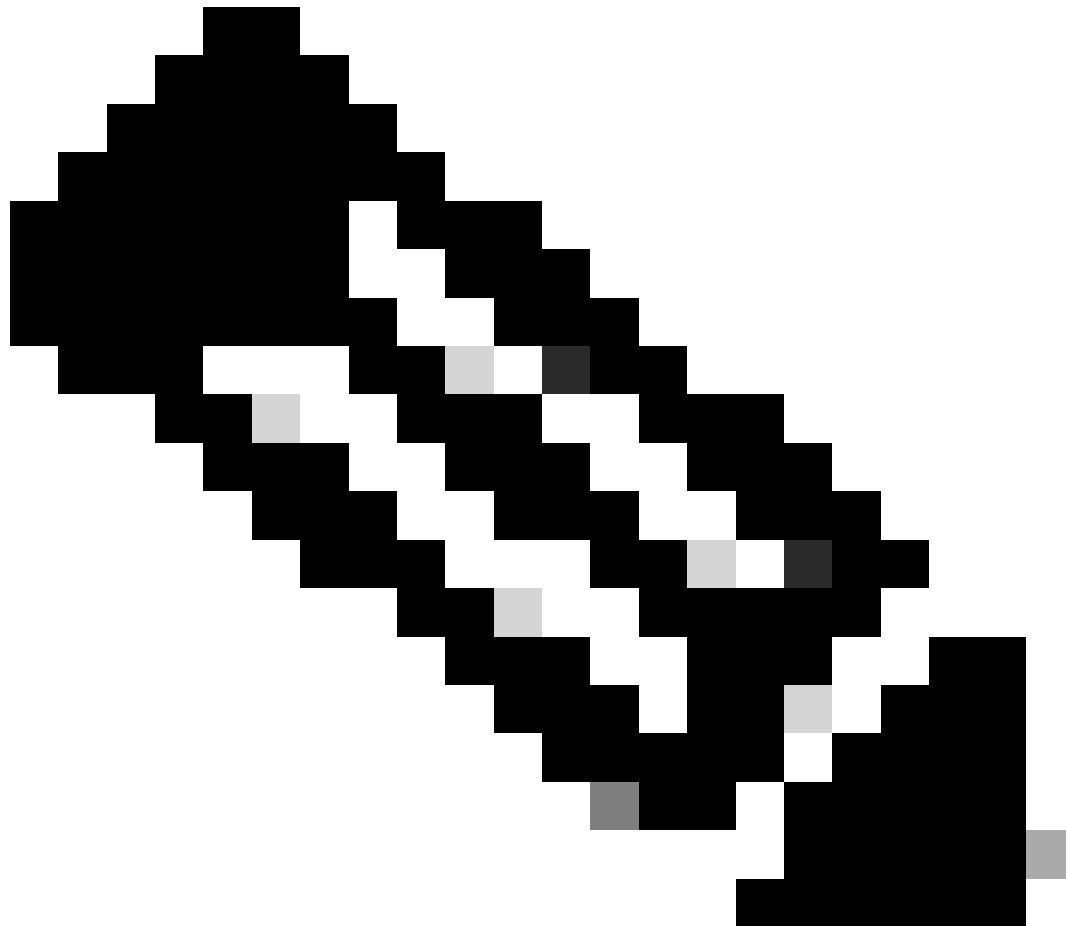
AWS VPC Flow log

AWS VPC Flow log

Azure NSG Flow log

Flow Generator Input

: 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 9

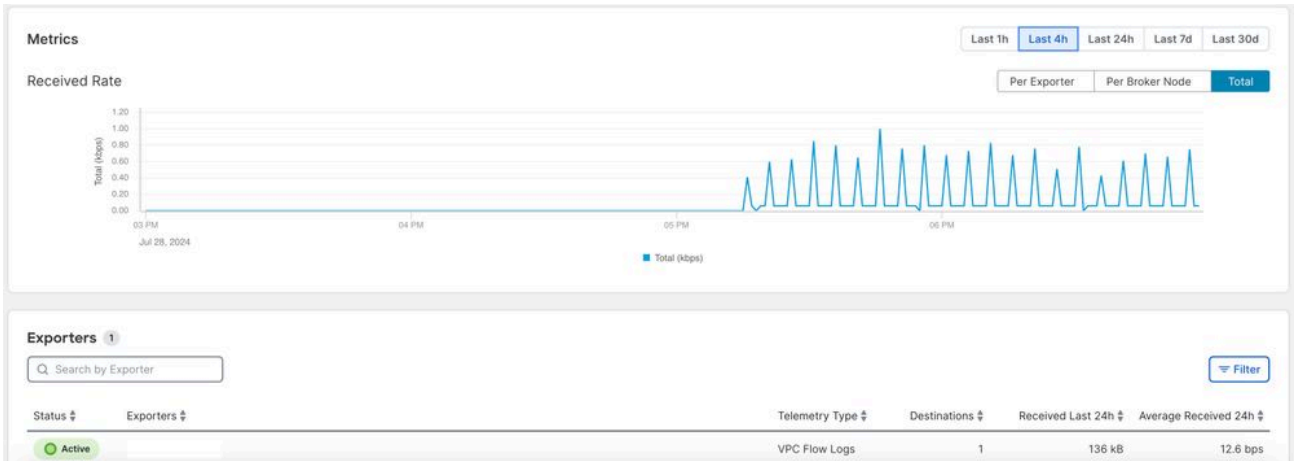
Verify

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 to Input > Click open AWS input.**

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



CTB-Input-UI