

# Configuración de registros de flujo de AWS VPC para entrada CTB

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuration Steps](#)

[Paso 1. Configure el Bucket S3 en AWS](#)

[Paso 2. Crear usuario IAM con clave de acceso y Adjuntar política de depósito S3](#)

[Paso 3. Configuración de los registros de flujo de VPC](#)

[Paso 4. Configuración de la entrada VPC en CTB](#)

[Verificación](#)

---

## Introducción

Este documento describe cómo configurar los registros de flujo de VPC como entrada para Cisco Telemetry Broker (CTB).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servicios web de Amazon (AWS)
- Administración de CTB.

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

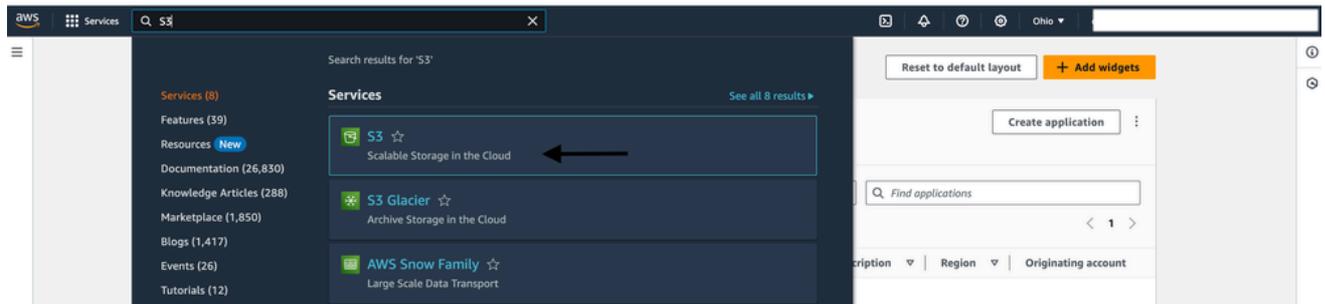
- CTB (v2.2.1+)
- AWS

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

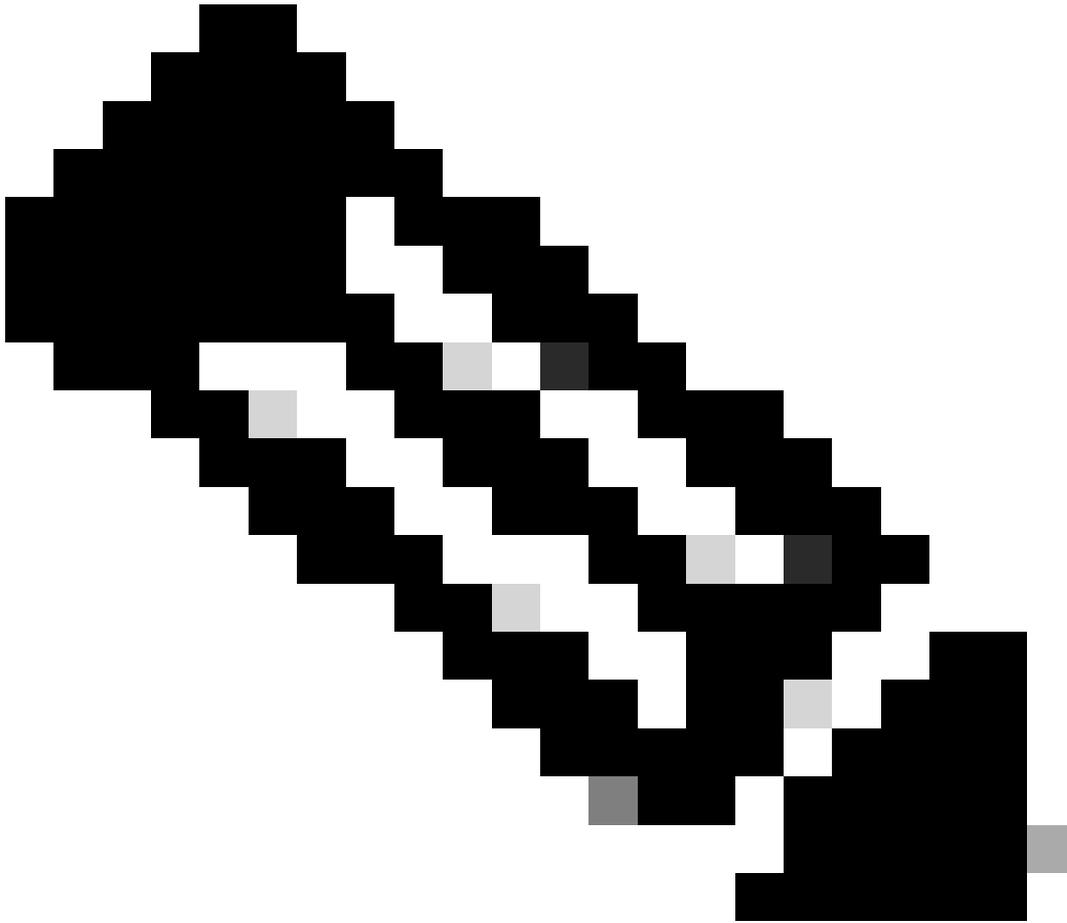
# Configuration Steps

## Paso 1. Configure el Bucket S3 en AWS

- 1: Inicie sesión en la consola de administración de AWS con nombre de usuario y contraseña.
- 2: Asegúrese de iniciar sesión en la región adecuada.
- 3: Vaya a la barra de búsqueda y escriba S3.

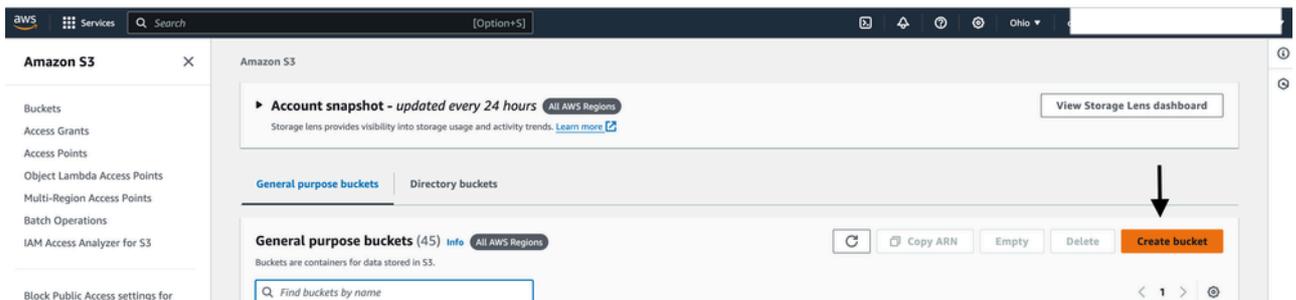


AWS-Dashboard



Nota: En la demostración, ha seleccionado la región de Ohio con la zona de disponibilidad us-east-2, que es visible justo al lado del icono del engranaje.

4: Haga clic en crear depósito.



AWS-S3

5: Dé un nombre a bucket y deje cada opción tal cual y haga clic en create.

## General configuration

AWS Region

US East (Ohio) us-east-2

Bucket name [Info](#)

Bucket name must be unique within the global namespace and follow the bucket naming rules. [See rules for bucket naming](#)

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

[Choose bucket](#)

Format: s3://bucket/prefix

AWS-S3

### ▶ Advanced settings

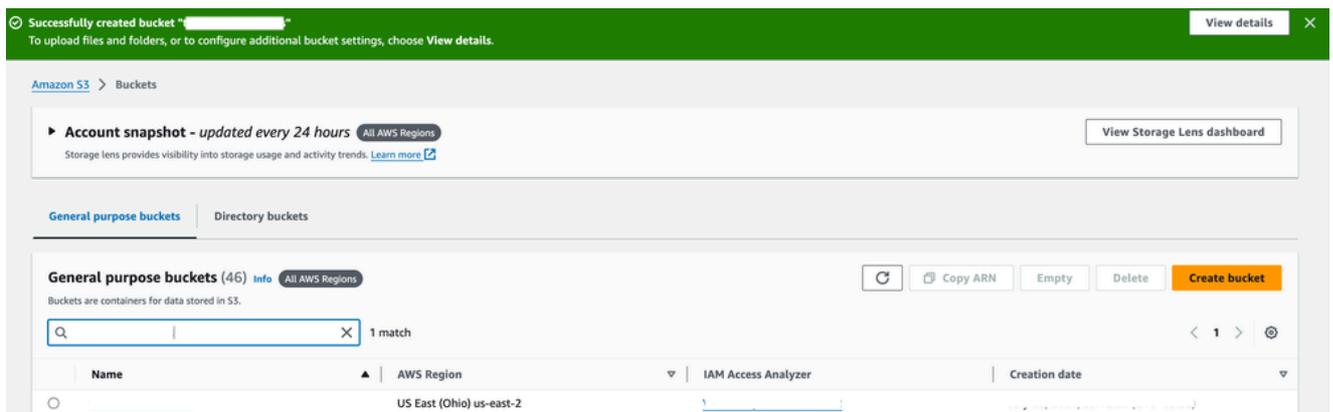
 After creating the bucket, you can upload files and folders to the bucket, and configure additional bucket settings.

Cancel

Create bucket

AWS-S3

6: Una vez que la cubeta se haya creado correctamente, guarde el ARN de la cubeta que se utilizará más adelante durante la configuración.



Successfully created bucket "..."  
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

Amazon S3 > Buckets

▶ **Account snapshot - updated every 24 hours** All AWS Regions [View Storage Lens dashboard](#)  
Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

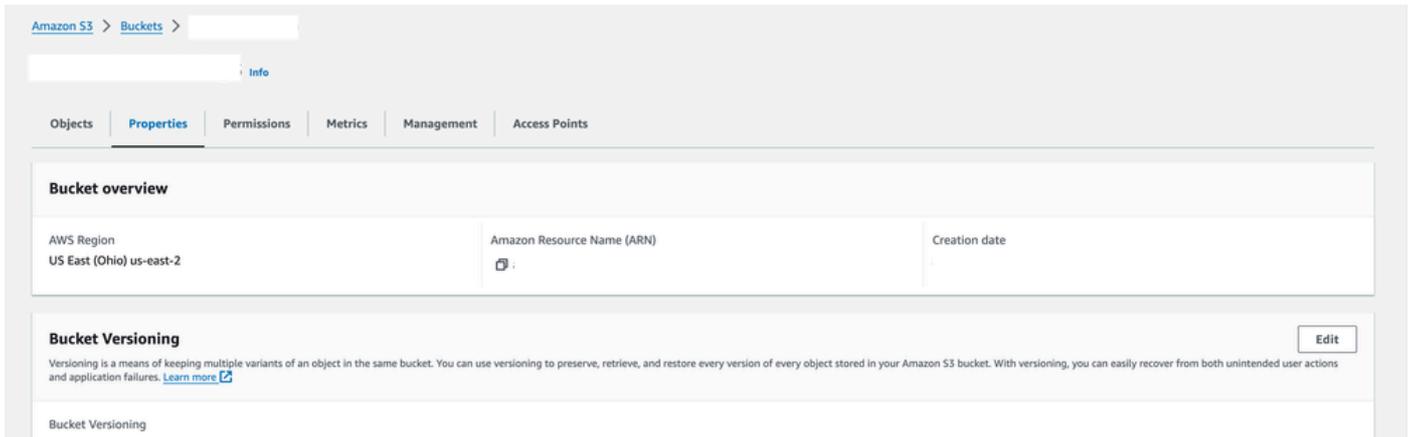
**General purpose buckets** (46) All AWS Regions [Info](#)

Buckets are containers for data stored in S3.

1 match

Name	AWS Region	IAM Access Analyzer	Creation date
	US East (Ohio) us-east-2		

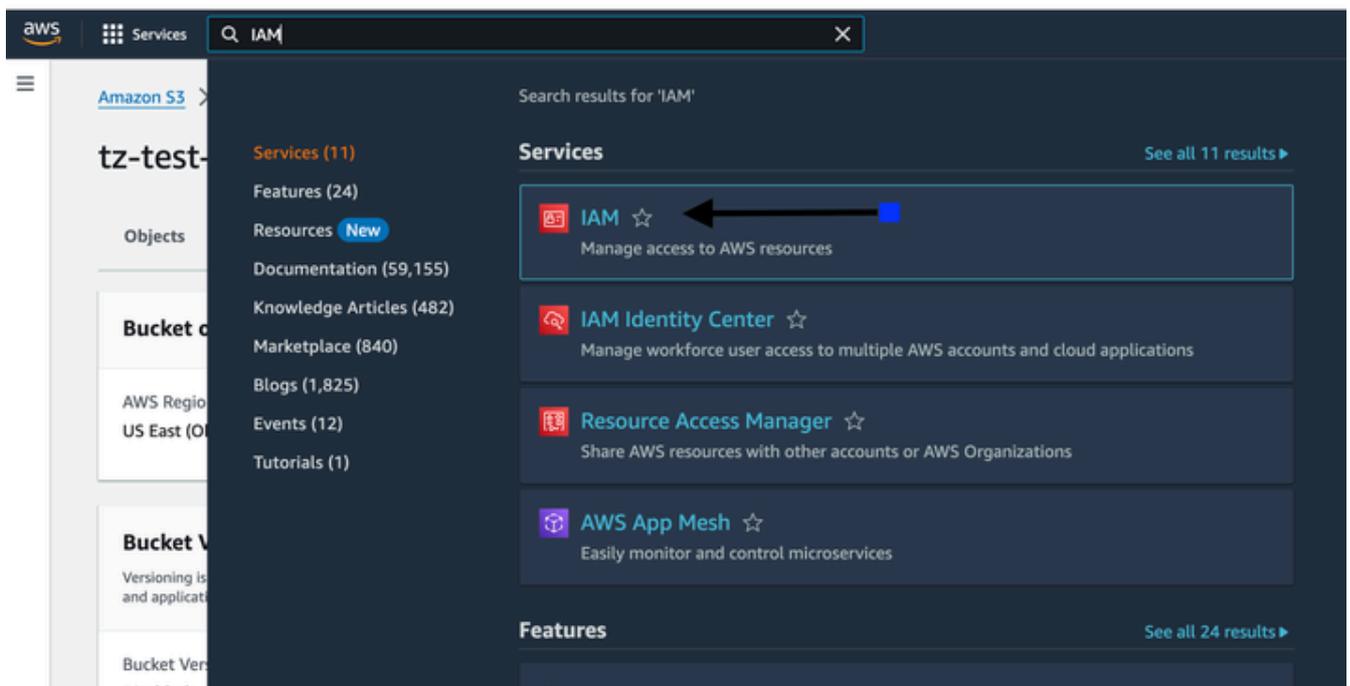
AWS-S3



AWS-S3

## Paso 2. Crear usuario IAM con clave de acceso y Adjuntar política de depósito S3

1: Inicie el IAM desde la barra de búsqueda de AWS.



AWS-IAM

2: Desplácese hasta usuarios.



Services



Search

# Identity and Access Management (IAM)



Search IAM

## Dashboard

### ▼ Access management

User groups

**Users**

Roles

Policies

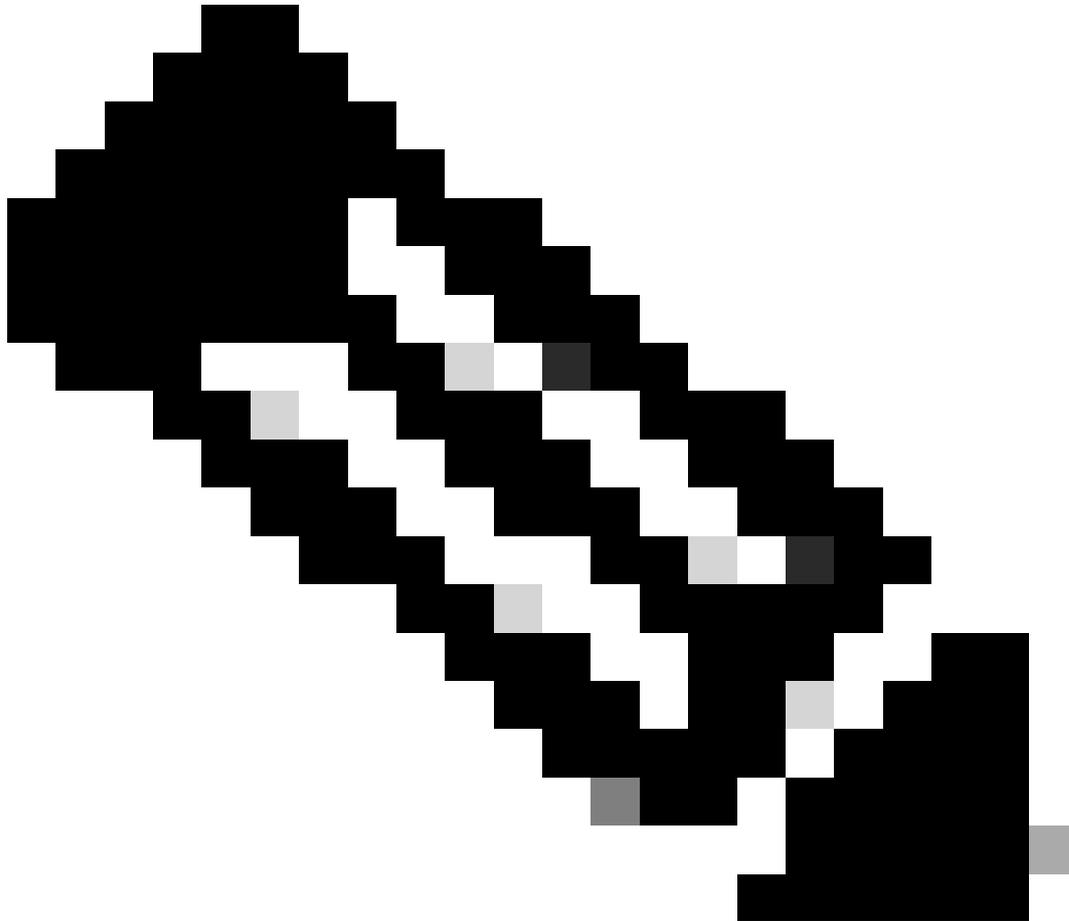
---

Al desactivar la casilla de acceso de la consola de administración de AWS, evita que el usuario inicie sesión en la cuenta de AWS mediante la interfaz de usuario web.

---

6: Asigne la política al usuario, asociándola directamente a un grupo o configurándola en línea.

---



Nota: Para ver una demostración, puede asignar directamente una directiva al usuario.  
Para obtener más información: [administración de políticas de AWS](#)

---

7: Busque S3 full access y seleccione AmazonS3full access, que permite al usuario tener acceso completo para cada cubeta S3 creada en su cuenta AWS correspondiente.

8: Marque la casilla con el nombre de la política AmazonS3FullAccess y haga clic en 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)

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

Filter by Type

Search: s3full | 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.

Filter by Type

Search: Search | All types | 1 match

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

#### AmazonS3FullAccess

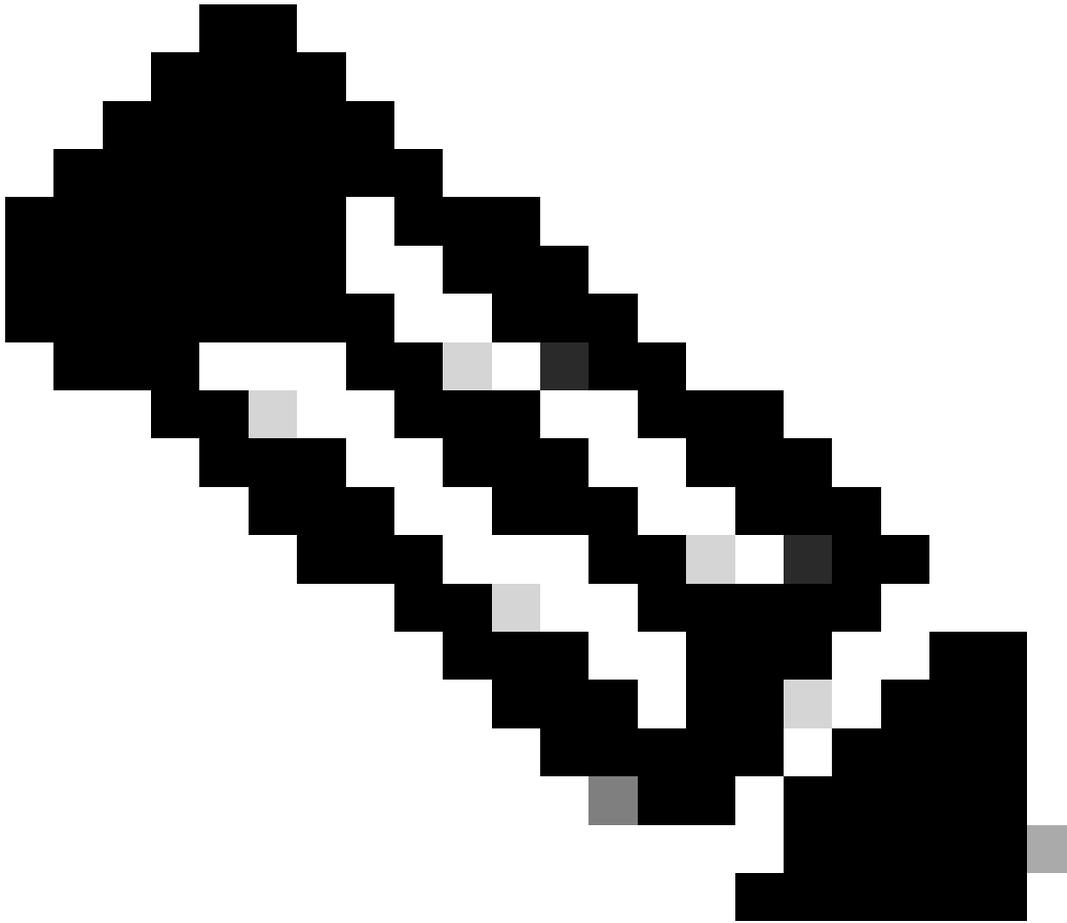
Provides full access to all buckets via the AWS Management Console. [Copy JSON](#)

```

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- }

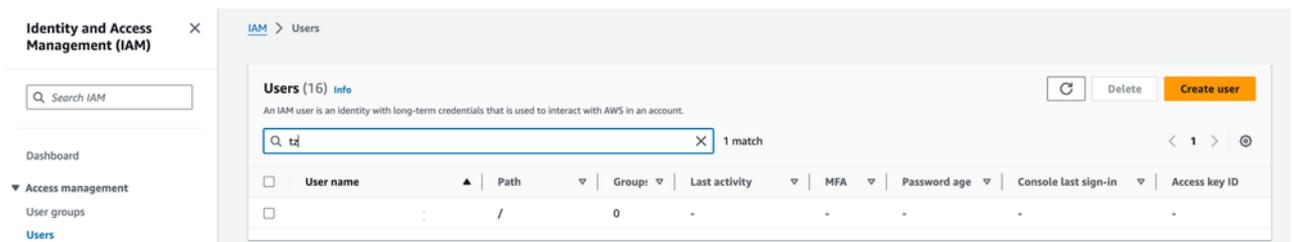
```

AWS-IAM



Nota: Puede crear una política más granular permitiendo solo un depósito específico también. Navegue hasta [Creación de política](#) para crear su política de depósito S3 en formato json.

9: Una vez creado el usuario, enumere el usuario y navegue hasta la ficha credencial de seguridad y haga clic en crear clave de acceso.



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			
<a href="#">Assign MFA device</a>			

---

**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: Seleccione el otro botón de opción y, opcionalmente, agregue una etiqueta.

## 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: Haga clic en Descargar archivo .csv. Esta es la clave de acceso de un archivo csv y ya no está disponible para descargar o ver una vez que se desplace fuera de esta página.

**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
	***** <a href="#">Show</a>

**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.

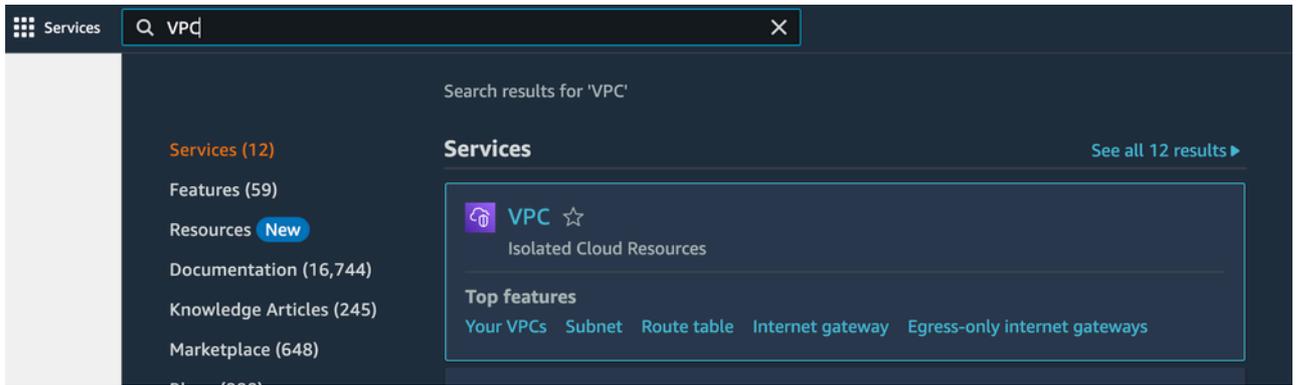
For more details about managing access keys, see the [best practices for managing AWS access keys](#).

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

AWS-IAM

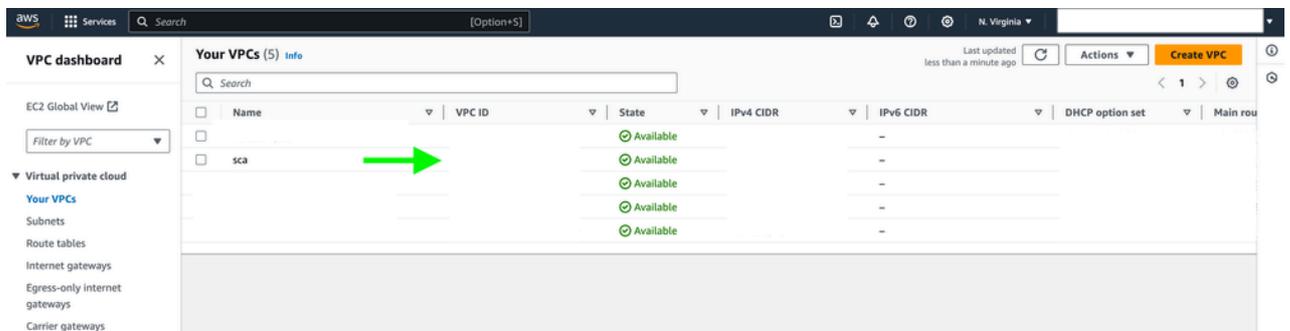
## Paso 3. Configuración de los registros de flujo de VPC

1: Inicie el VPC en la región deseada y navegue hasta la opción Your VPC.



AWS-Flow-Logs

2: Seleccione el VPC en la lista que aparece en la pantalla.



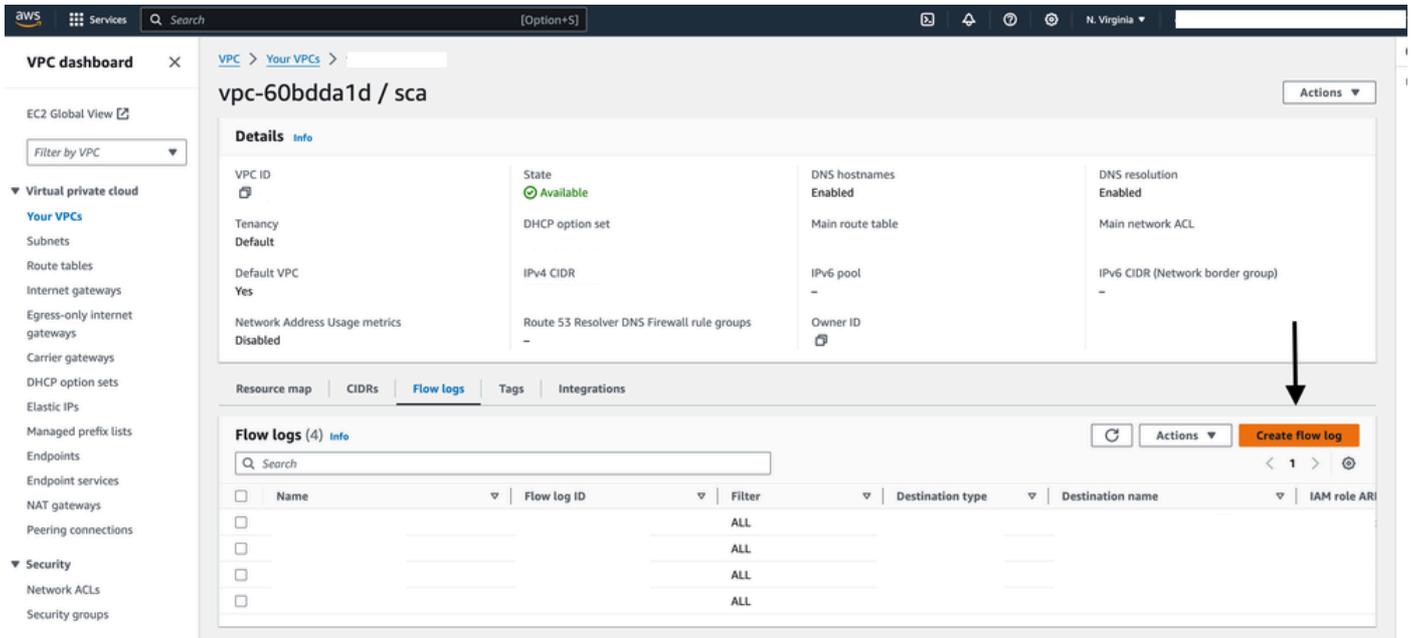
AWS-Flow-Logs



Nota: Ha seleccionado el nombre VPC SCA en esta demostración.

---

3: Navegue hasta Sus VPC en Nube privada virtual, cambie a la pestaña Registros de flujo y haga clic en Crear registros de flujo.



## AWS-Flow-Logs

4: Dé un nombre a sus registros de flujo y comparte el ARN de cubeta S3 creado anteriormente.



Nota: Para ARN, consulte [Configure S3 bucket - Step 6](#)

---

5: Tiene la opción de utilizar el formato de registro predeterminado de AWS o crear un formato de registro personalizado en caso de que se necesiten más campos.

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:

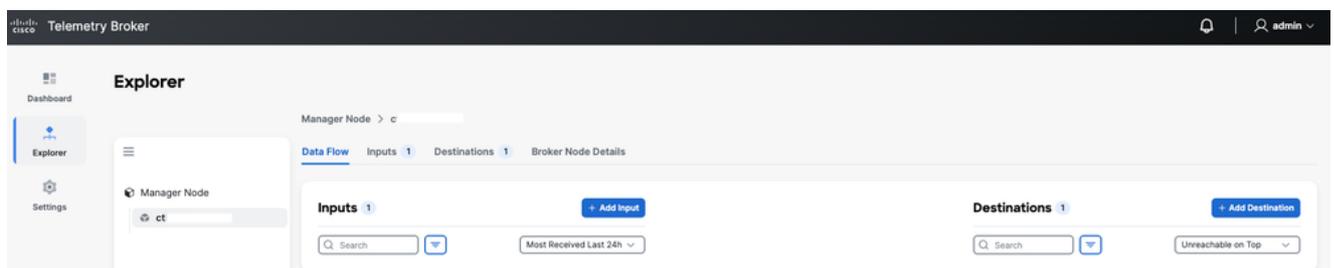
You can add 49 more tags



AWS-Flow-Logs

## Paso 4. Configuración de la entrada VPC en CTB

1: Acceda a la interfaz de usuario web de CTB, navegue hasta Explorador > ficha Nodo de Broker > haga clic en Abrir nodo de broker > ficha Flujo de datos > Haga clic en Agregar entrada.



CTB-Input-UI

2: Seleccione Input type as AWS VPC Flow log y haga clic en next.

# Add Input



## Select Input type

Type or Select Input



UDP Input

AWS VPC Flow log

AWS VPC Flow log

Azure NSG Flow log

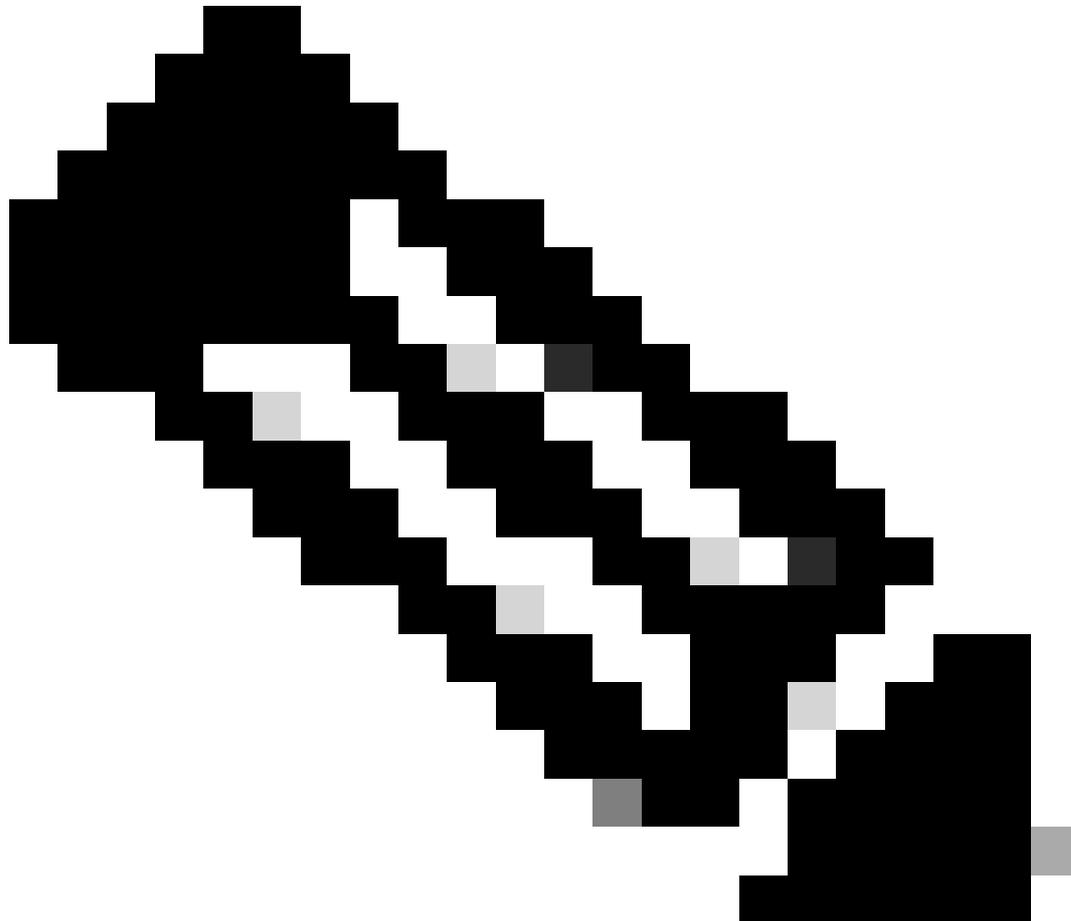
Flow Generator Input

---

: Cualquier dirección IP configurada como dirección IP de entrada (IP única no compartida por ningún otro exportador) se notifica como el exportador para los datos de NetFlow transformados.

---

---



Nota: Para el ID de clave de acceso de AWS, consulte Configuración del usuario IAM para la clave de acceso con la política de acceso S3, paso 9

---

## Verificación

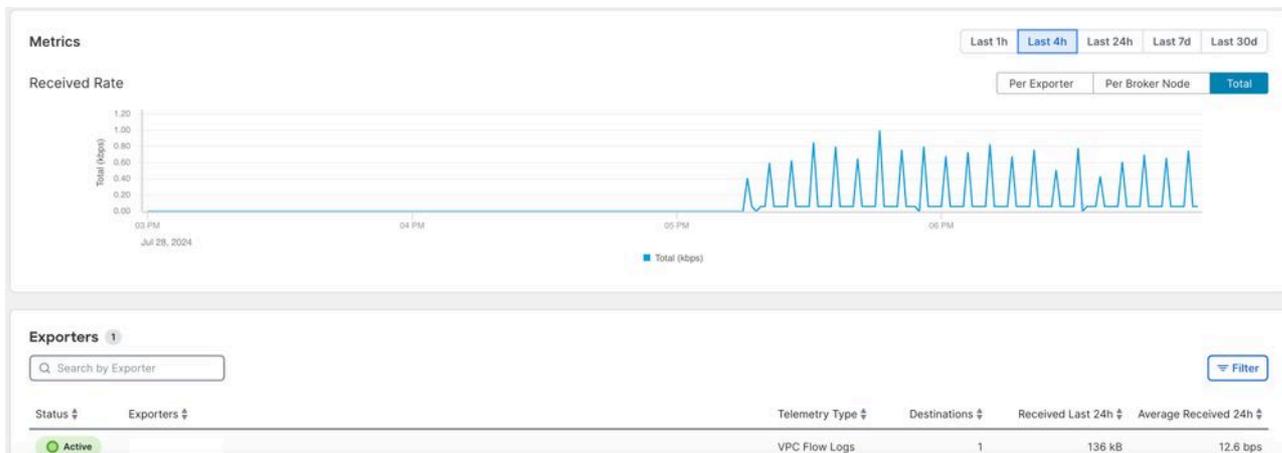
Después de unos minutos de configurar la entrada AWS VPC, la columna de estado se activa si la cubeta AWS S3 tiene datos.

Verifique el estado de la entrada AWS VPC mediante estos pasos.

1: Inicie sesión en la interfaz de usuario de CTB y navegue hasta Explorador > ficha Nodo de Broker > haga clic en nodo de OpenBroker > cambie a Entrada > Haga clic en Abrir entrada de

AWS.

2: Verifique que los logs de aws-flow configurados tengan el estado activo y que la métrica recibida tenga un gráfico ascendente.



CTB-Input-UI

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).