

# Configura log di flusso VPC AWS per input CTB

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Procedura di configurazione](#)

[Passaggio 1. Configurare il bucket S3 in AWS](#)

[Passaggio 2. Creare l'utente IAM con la chiave di accesso e allegare il criterio bucket S3](#)

[Passaggio 3. Configurare i log di flusso VPC](#)

[Passaggio 4. Configurare l'input VPC su CTB](#)

[Verifica](#)

---

## Introduzione

Questo documento descrive come configurare i log di flusso VPC come input per Cisco Telemetry Broker (CTB).

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Servizi Web Amazon (AWS)
- Amministrazione CTB.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

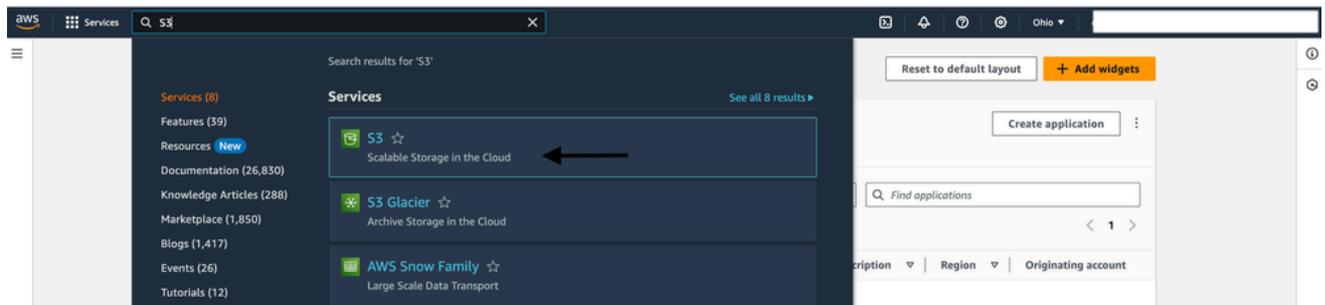
- CTB (v2.2.1+)
- AWS

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

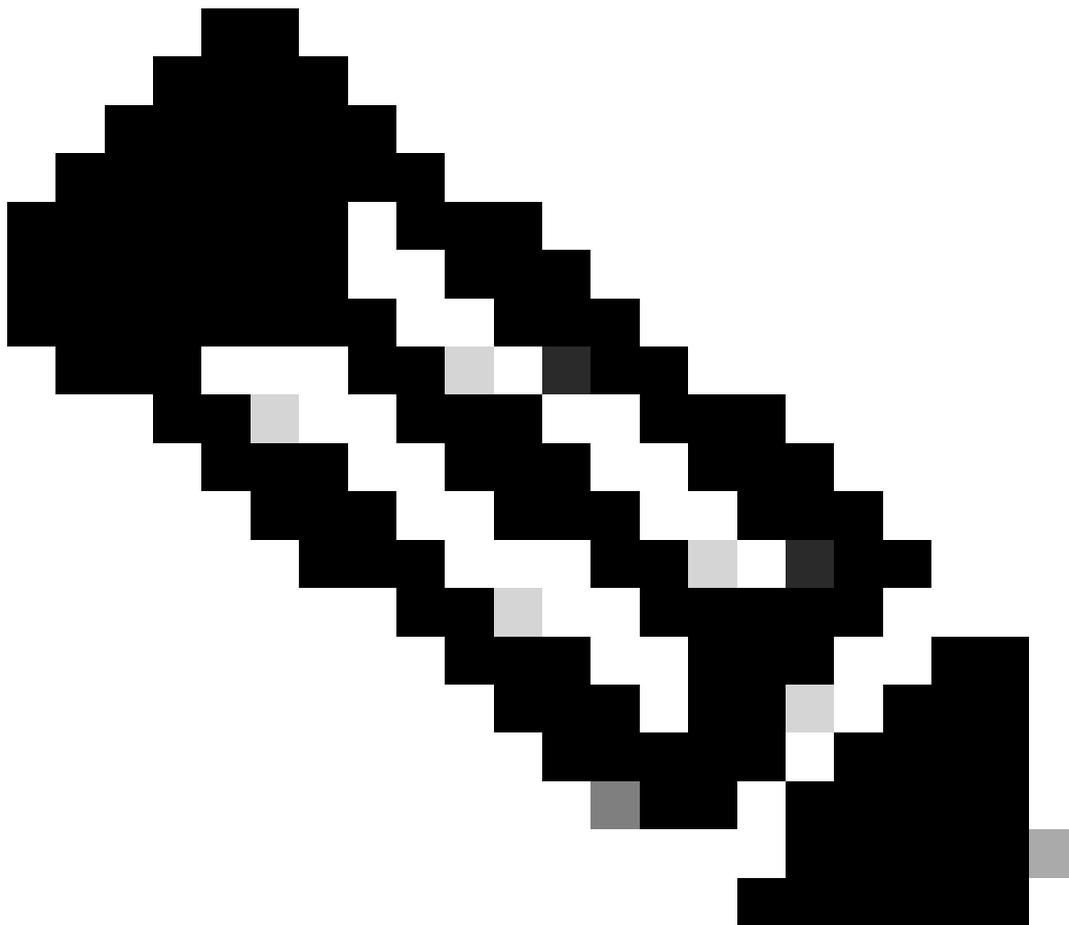
## Procedura di configurazione

## Passaggio 1. Configurare il bucket S3 in AWS

- 1: Accedere alla console di gestione AWS con nome utente e password.
- 2: Accertarsi di accedere all'area appropriata.
- 3: Passare alla barra di ricerca e digitare S3.

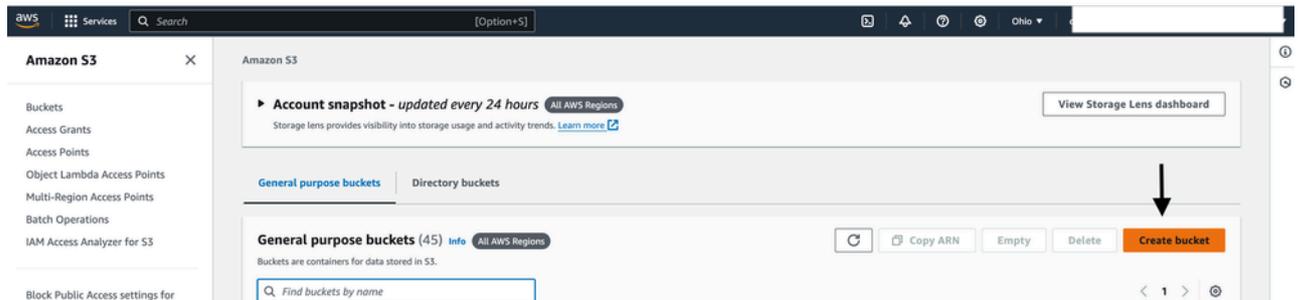


AWS-Dashboard



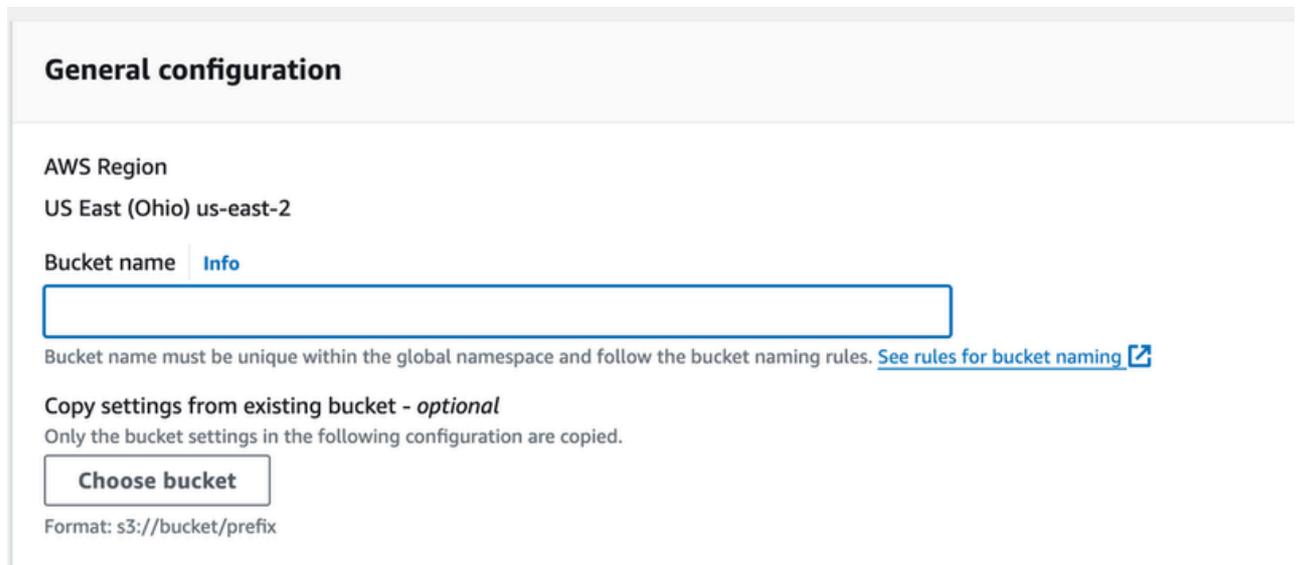
Nota: In demo, avete selezionato Ohio regione con us-east-2 zona di disponibilità, è visibile proprio accanto all'icona ingranaggio.

4: Fare clic su Crea bucket.

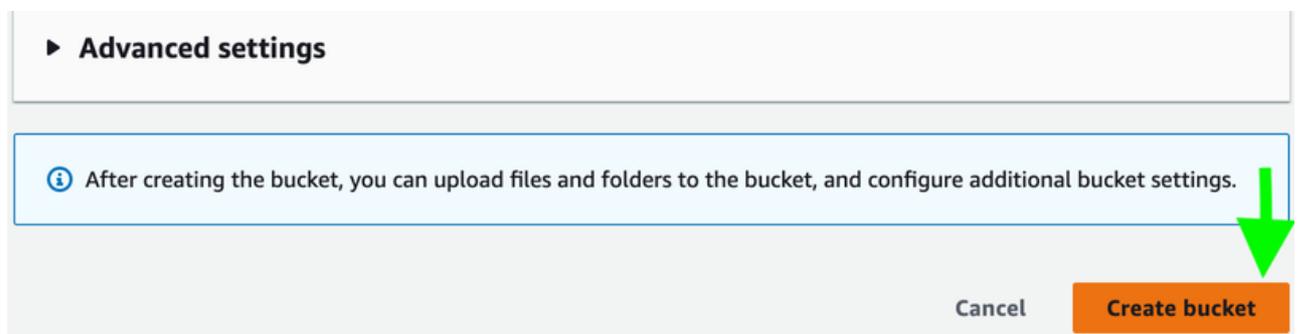


AWS-S3

5: Assegnare un nome al bucket e lasciare invariate tutte le opzioni, quindi fare clic su Crea.

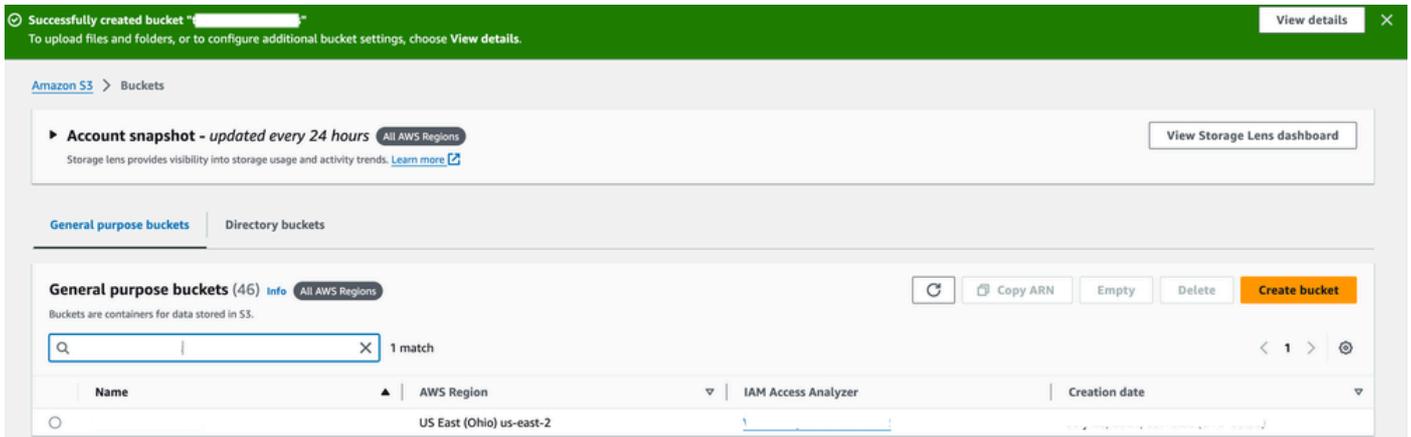


AWS-S3

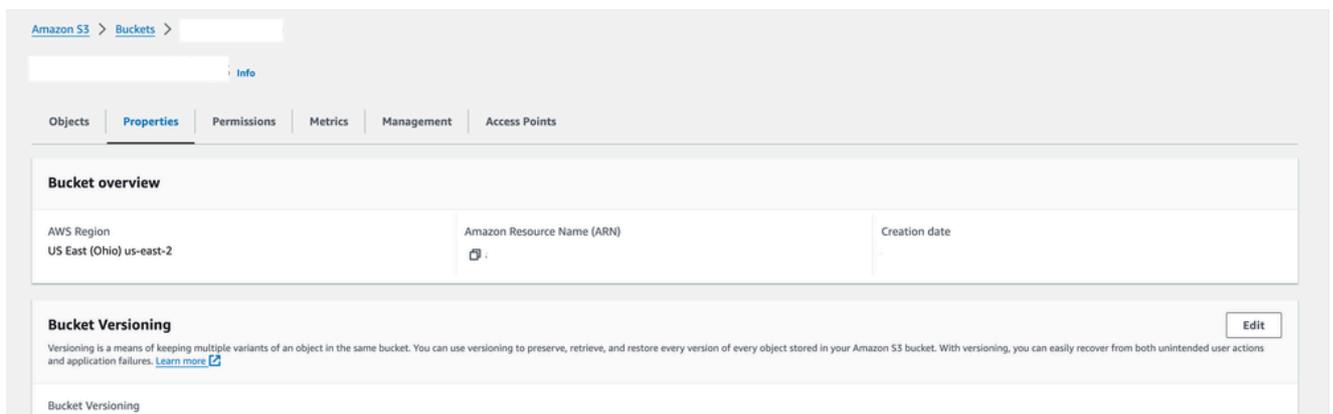


AWS-S3

6: Una volta creato il bucket, salvare il bucket ARN che verrà utilizzato successivamente durante la configurazione.



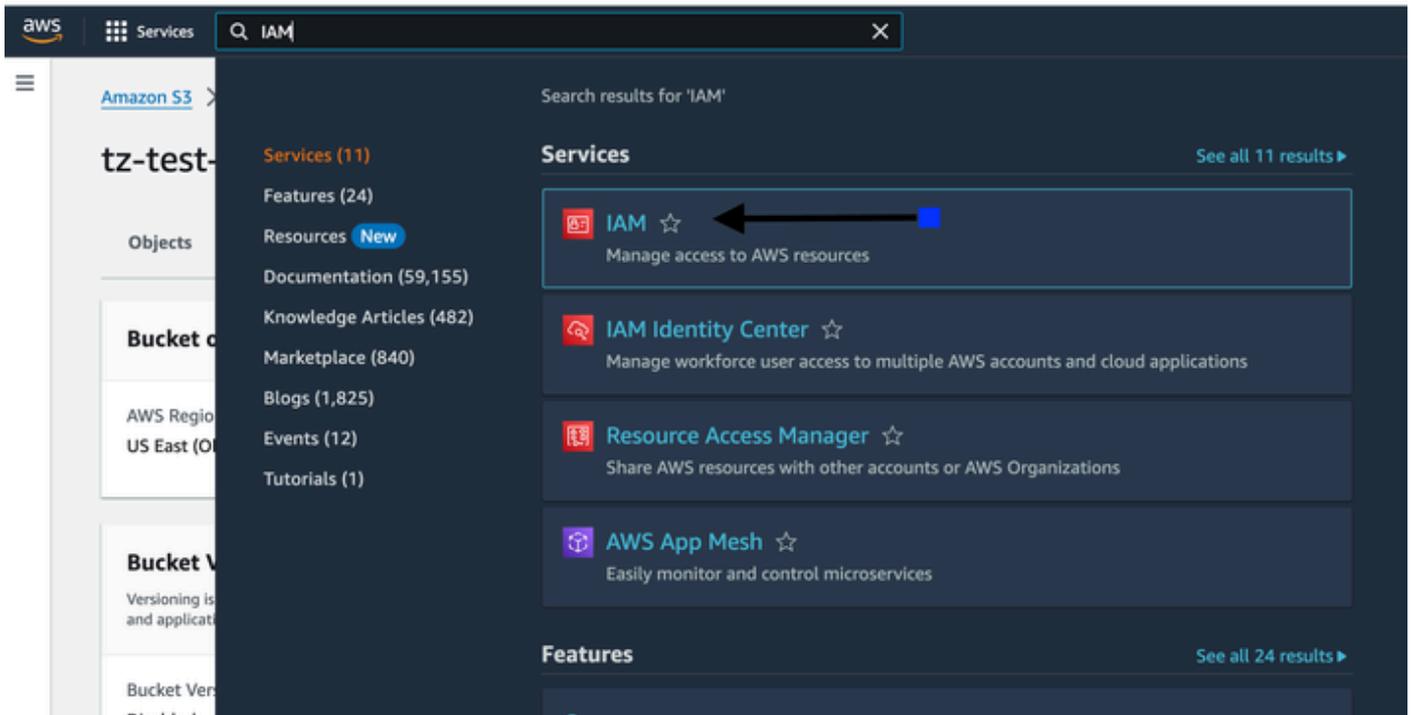
AWS-S3



AWS-S3

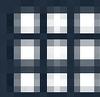
## Passaggio 2. Creare l'utente IAM con la chiave di accesso e allegare il criterio bucket S3

1: Avviare IAM dalla barra di ricerca aws.



AWS-IAM

2: Passare agli utenti.



Services



Search

# Identity and Access Management (IAM)



Search IAM

## Dashboard

### ▼ Access management

User groups

**Users**

Roles

Policies

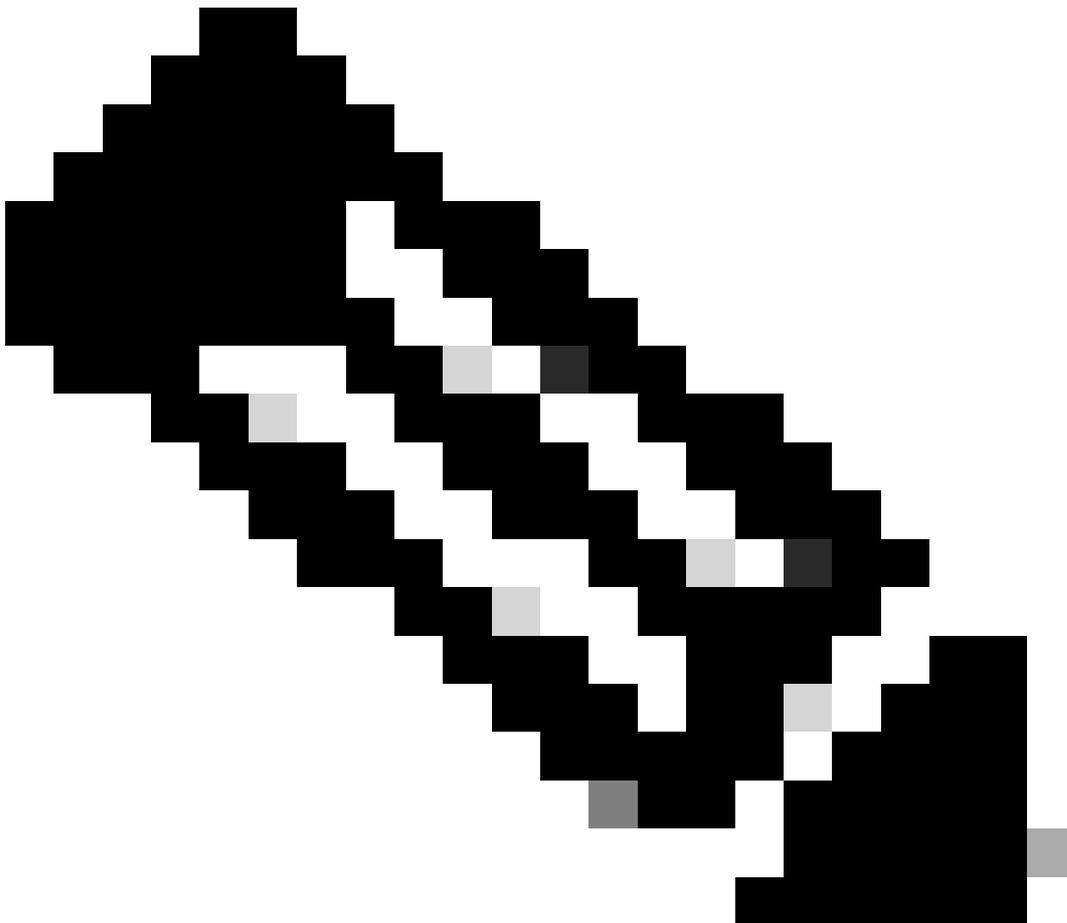
---

Deselezionando la casella di accesso alla console di gestione AWS, si impedisce all'utente di accedere all'account AWS tramite l'interfaccia utente Web.

---

6: assegnare i criteri assegnandoli all'utente, collegandoli direttamente a un gruppo o configurandoli in linea.

---



Nota: Per la dimostrazione, assegnare direttamente i criteri all'utente. Per ulteriori informazioni - [Gestione dei criteri AWS](#)

---

7: Cercare accesso completo S3 e selezionare AmazonS3full access, che consente all'utente di avere accesso completo per ogni bucket S3 creato sul suo account AWS corrispondente.

8: Selezionare la casella con il nome del criterio AmazonS3FullAccess e fare clic su avanti.

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

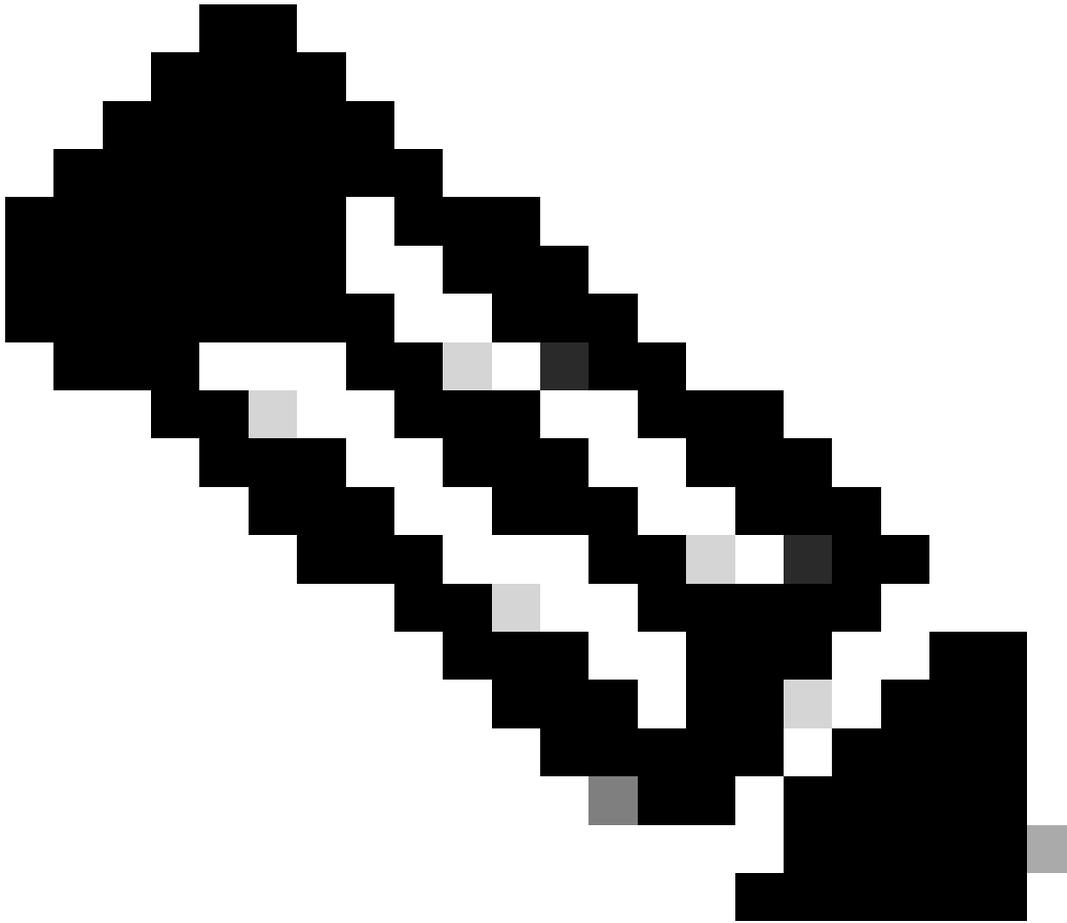
Provides full access to all buckets via the AWS Management Console. [Copy JSON](#)

```

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- }

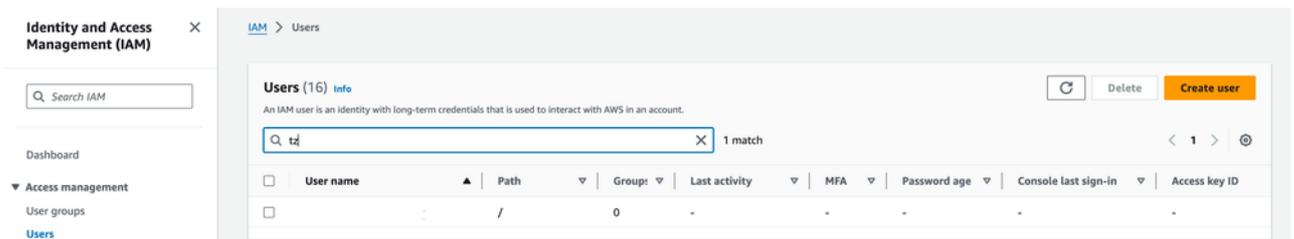
```

AWS-IAM



Nota: È possibile creare criteri più granulari consentendo solo un bucket specifico. Passare a [Creazione criteri](#) per creare il criterio bucket S3 in formato json.

9: Una volta creato l'utente, elencarlo e passare alla scheda Credenziali di sicurezza e fare clic su Crea chiave di accesso.



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: Selezionare l'altro pulsante di scelta e aggiungere facoltativamente un 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: Fare clic su Scarica file CSV. Questa è la chiave di accesso in un file CSV e non è più disponibile per il download o la visualizzazione dopo essere usciti da questa pagina.

**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.

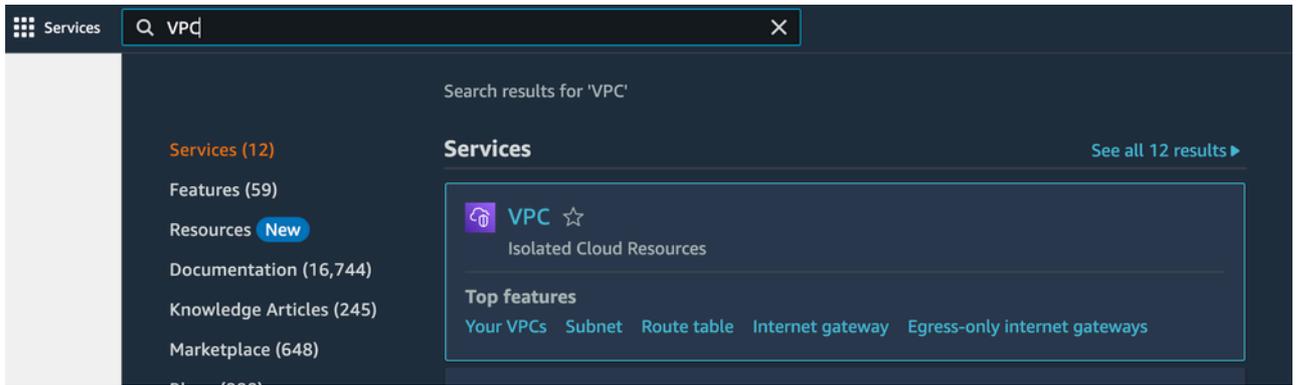
For more details about managing access keys, see the [best practices for managing AWS access keys](#).

Download .csv file **Done**

AWS-IAM

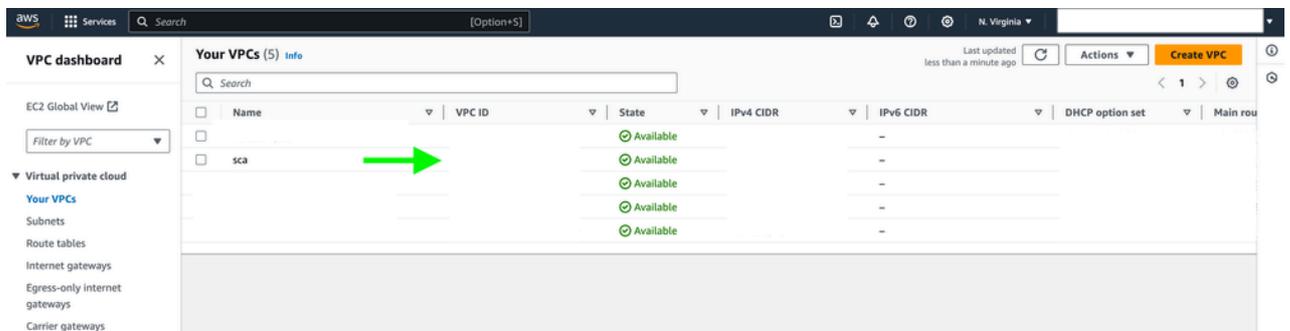
## Passaggio 3. Configurare i log di flusso VPC

1: Avviare il VPC nell'area desiderata e selezionare l'opzione VPC.



AWS-Flow-Logs

2: Selezionare il VPC dall'elenco visualizzato sullo schermo.



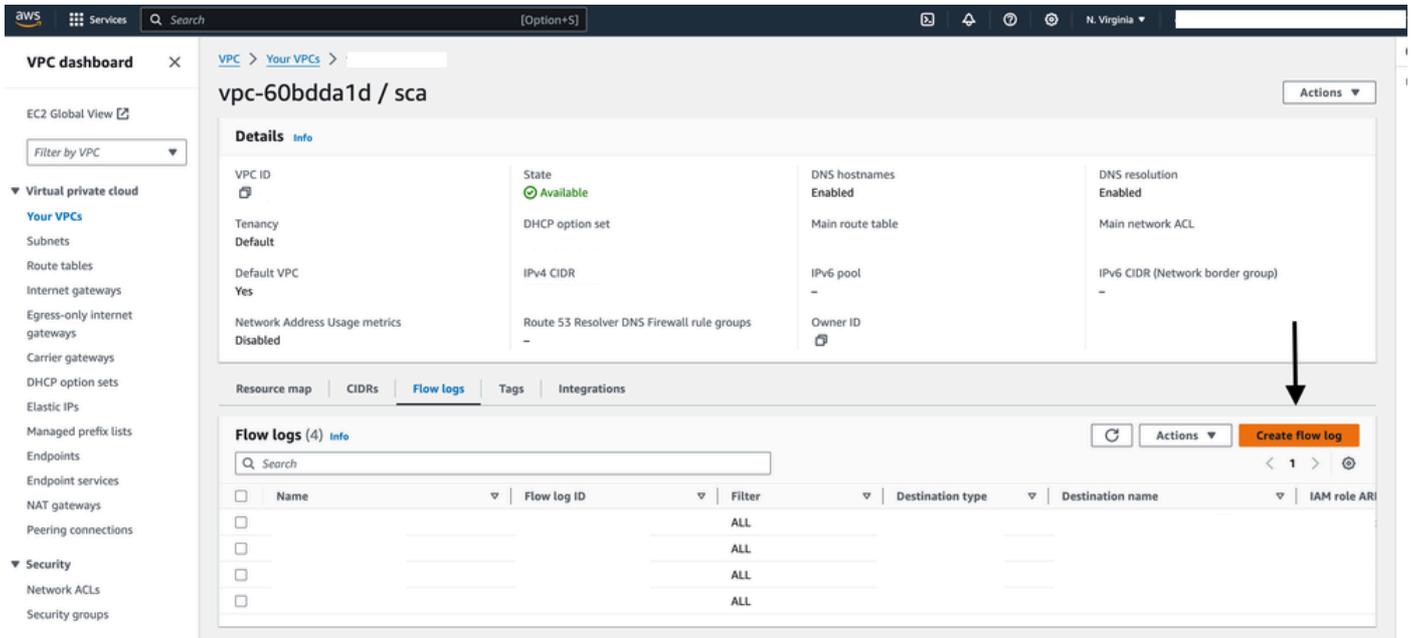
AWS-Flow-Logs



Nota: In questa demo è stato selezionato il nome VPC SCA.

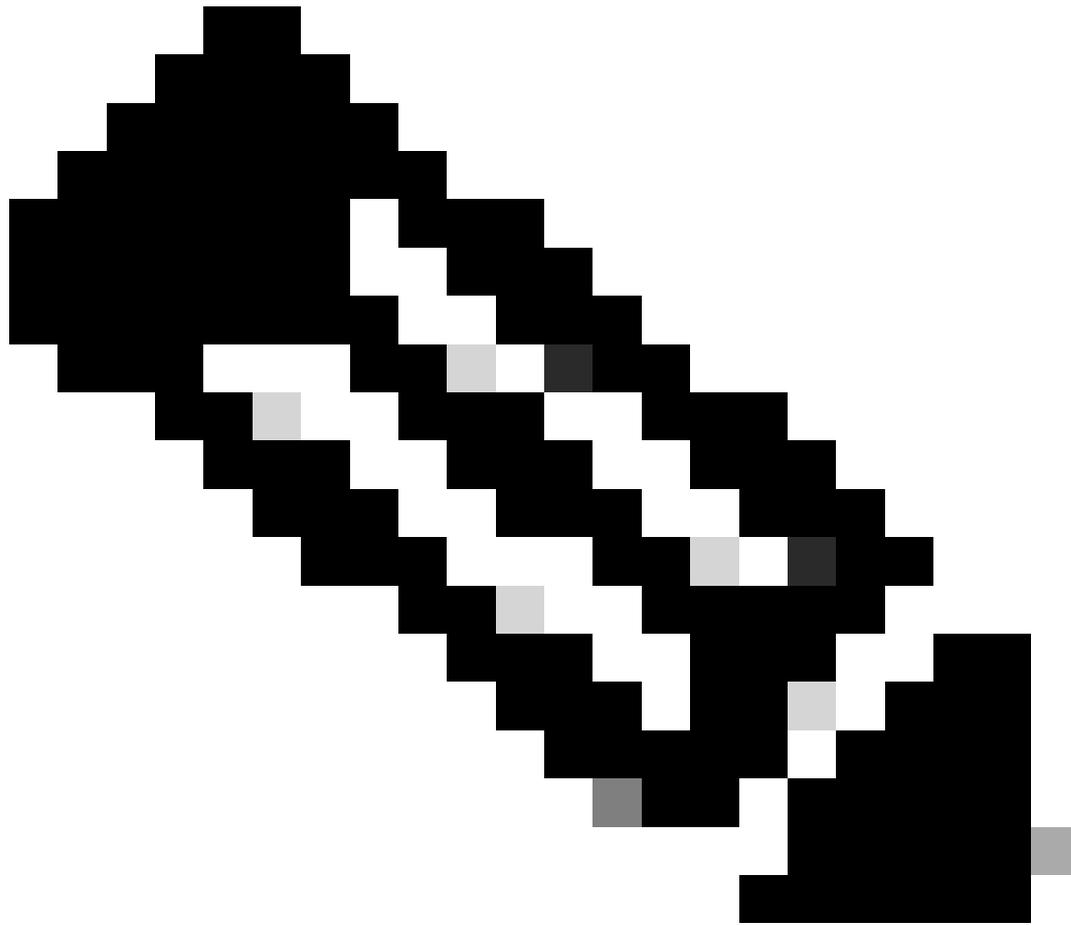
---

3: Passare alle VPC in Virtual private cloud, passare alla scheda Log di flusso e fare clic su Crea log di flusso.



## AWS-Flow-Logs

4: Assegnare un nome ai log di flusso e condividere il bucket S3 ARN creato in precedenza.



Nota: Per ARN, vedere Configurare il bucket S3 - Passaggio 6

---

5: È possibile scegliere di utilizzare il formato di registro predefinito di AWS o di creare un formato di registro personalizzato nel caso in cui siano necessari più campi.

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:

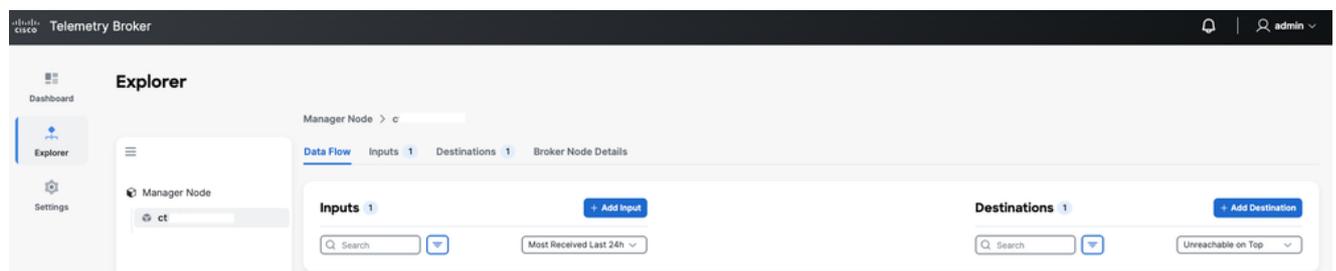
You can add 49 more tags



AWS-Flow-Logs

## Passaggio 4. Configurare l'input VPC su CTB

1: Accedi all'interfaccia utente Web CTB, passare a Esplora risorse > scheda nodo Broker > fare clic su apri nodo Broker > Flusso di dati scheda > Fare clic su Aggiungi input.



CTB-Input-UI

2: Selezionare il tipo di input AWS VPC Flow log e fare clic su avanti.

# Add Input



## Select Input type

Type or Select Input



UDP Input

AWS VPC Flow log

AWS VPC Flow log

Azure NSG Flow log

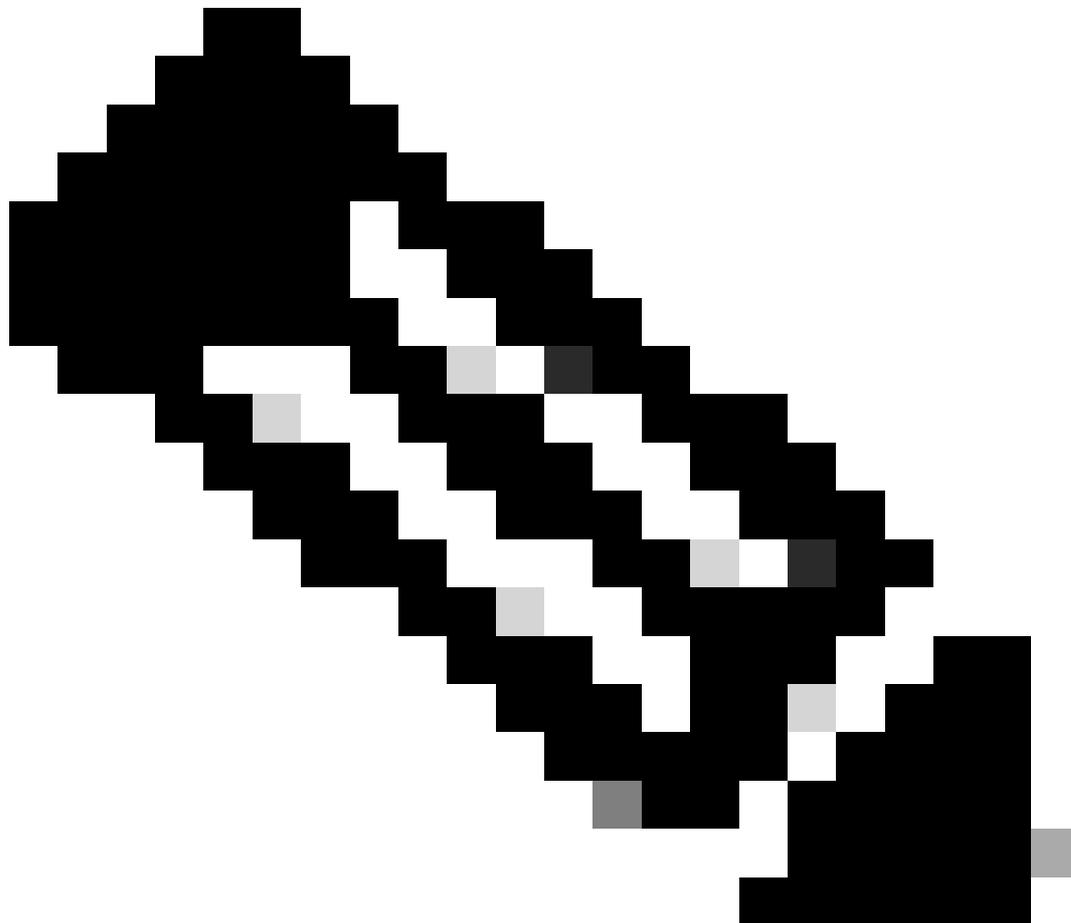
Flow Generator Input

---

: qualsiasi indirizzo IP configurato come indirizzo IP di input (indirizzo IP univoco non condiviso da nessun altro esportatore) viene segnalato come esportatore per i dati netflow trasformati.

---

---



Nota: Per l'ID della chiave di accesso AWS, vedere Configurare l'utente IAM per la chiave di accesso con i criteri di accesso S3, passo 9

---

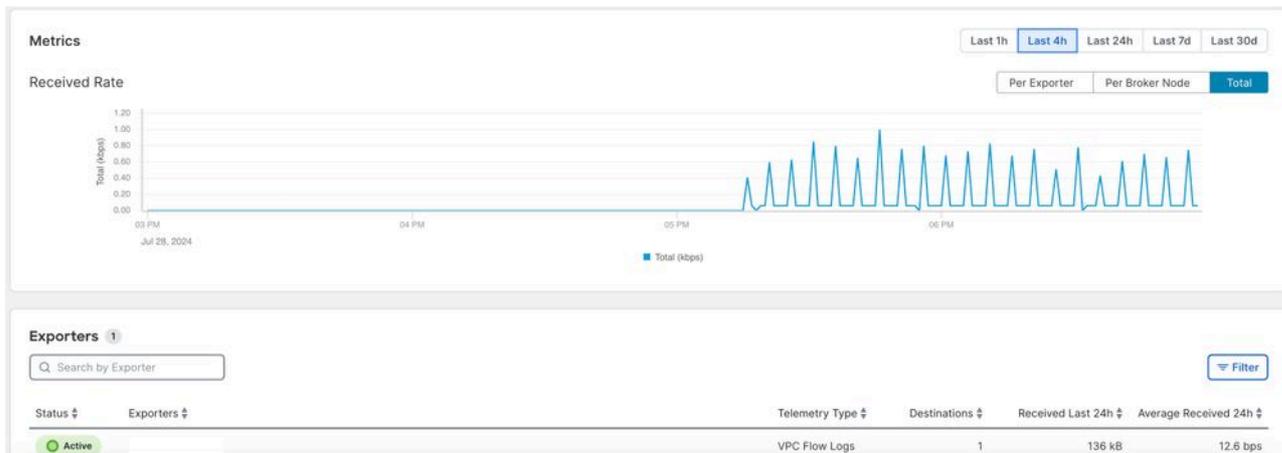
## Verifica

Dopo alcuni minuti di configurazione dell'input VPC AWS, la colonna di stato diventa attiva se il bucket S3 AWS contiene dati.

Verificare lo stato dell'input VPC AWS attenendosi alla seguente procedura.

1: Accedere all'interfaccia utente CTB e selezionare Explorer > Broker node tab > click openbroker node > switch tab toInput > Click open AWS input.

2: Verificare che i log di flusso AWS configurati abbiano lo stato attivo e che la metrica ricevuta presenti un grafico in aumento.



CTB-Input-UI

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).