

# AWS VPC-Flussprotokolle für CTB-Eingabe konfigurieren

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurationsschritte](#)

[Schritt 1: Konfigurieren von S3 Bucket in AWS](#)

[Schritt 2: IAM-Benutzer mit Zugriffsschlüssel erstellen und S3-Bucket-Richtlinie anhängen](#)

[Schritt 3: VPC-Ablaufprotokolle konfigurieren](#)

[Schritt 4: Konfigurieren der VPC-Eingabe in der CTB](#)

[Überprüfung](#)

---

## Einleitung

In diesem Dokument wird beschrieben, wie VPC Flow Logs als Eingabe für Cisco Telemetry Broker (CTB) konfiguriert werden.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Amazon Web Services (AWS)
- CTB-Verwaltung.

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

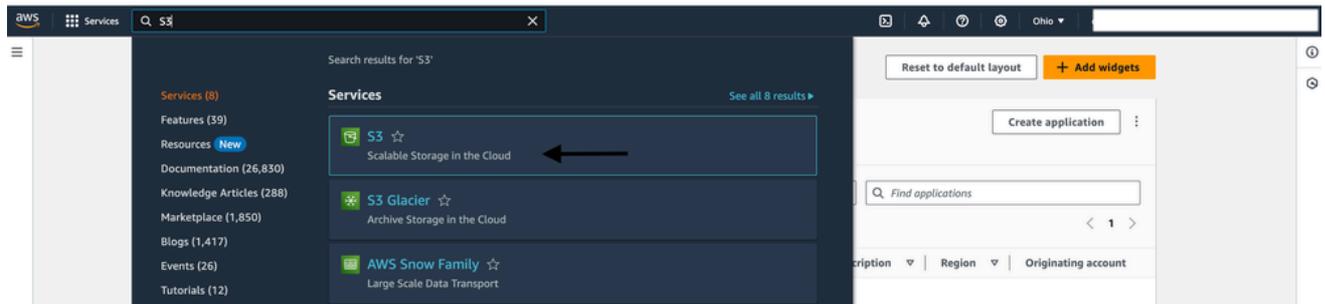
- CTB (v2.2.1+)
- AWS

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

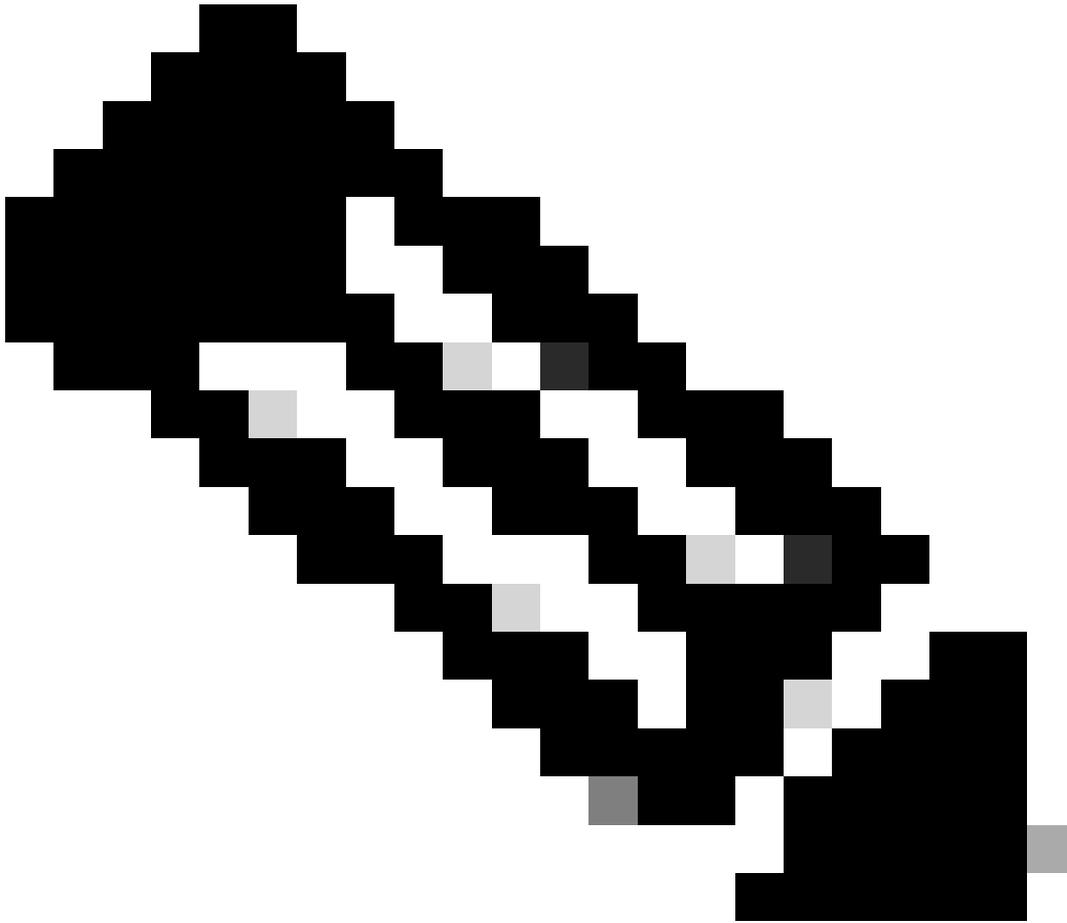
# Konfigurationsschritte

## Schritt 1: Konfigurieren von S3 Bucket in AWS

- 1: Melden Sie sich mit Benutzernamen und Kennwort bei der AWS-Verwaltungskonsole an.
- 2: Stellen Sie sicher, dass Sie sich bei der entsprechenden Region anmelden.
- 3: Navigieren Sie zur Suchleiste, und geben Sie S3 ein.

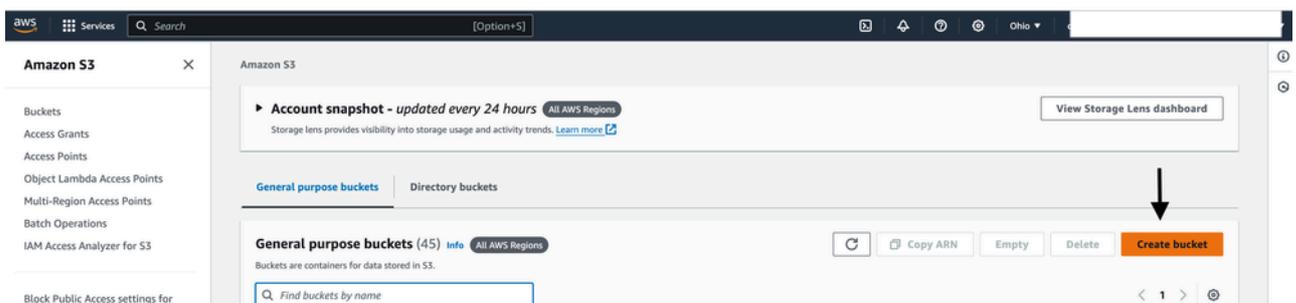


AWS-Dashboard



Anmerkung: In der Demo haben Sie Ohio Region mit us-east-2 Verfügbarkeitszone ausgewählt, sie ist direkt neben dem Zahnrad-Symbol zu sehen.

4: Klicken Sie auf Bucket erstellen.



AWS-S3

5: Geben Sie bucket einen Namen und lassen Sie alle Optionen unverändert, und klicken Sie auf Erstellen.

## 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

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

Cancel **Create bucket**

AWS-S3

6: Speichern Sie nach der erfolgreichen Erstellung des Buckets den Bucket-ARN, der später während der Konfiguration verwendet werden soll.

Successfully created bucket "..." [View details](#)

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 | Directory buckets

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

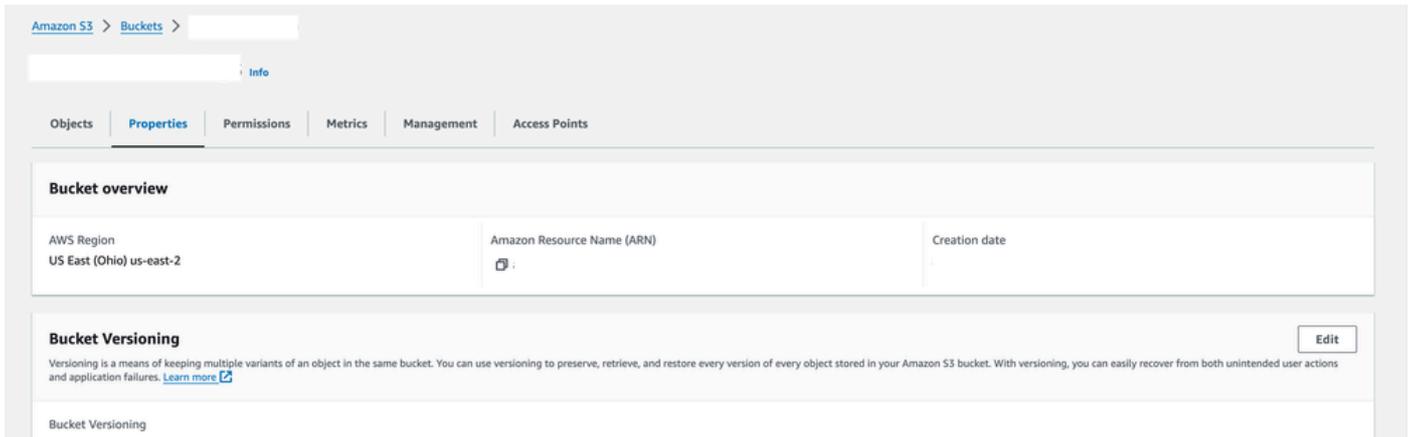
Buckets are containers for data stored in S3.

1 match

[Refresh](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

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

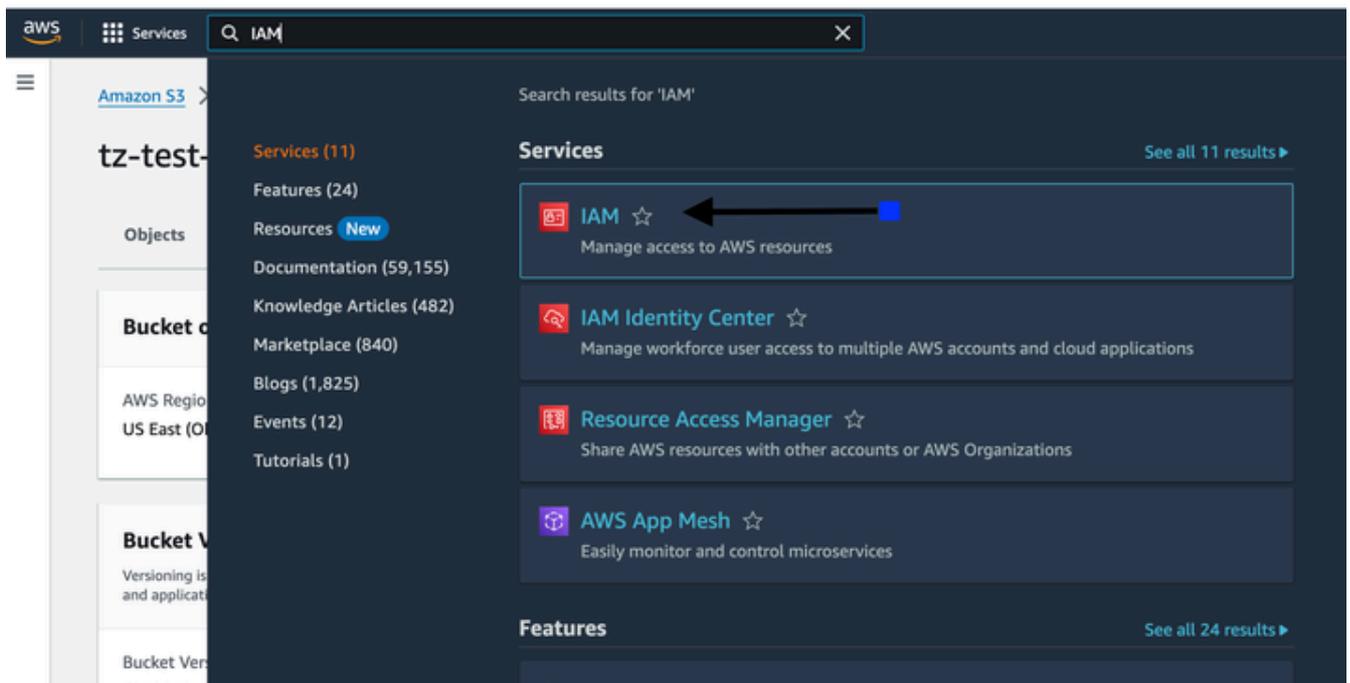
AWS-S3



AWS-S3

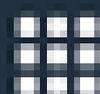
## Schritt 2: IAM-Benutzer mit Zugriffsschlüssel erstellen und S3-Bucket-Richtlinie anhängen

1: Starten Sie die IAM über die AWS-Suchleiste.



AWS-IAM

2: Navigieren Sie zu Benutzern.



Services



Search

# Identity and Access Management (IAM)



Search IAM

## Dashboard

### ▼ Access management

User groups

**Users**

Roles

Policies

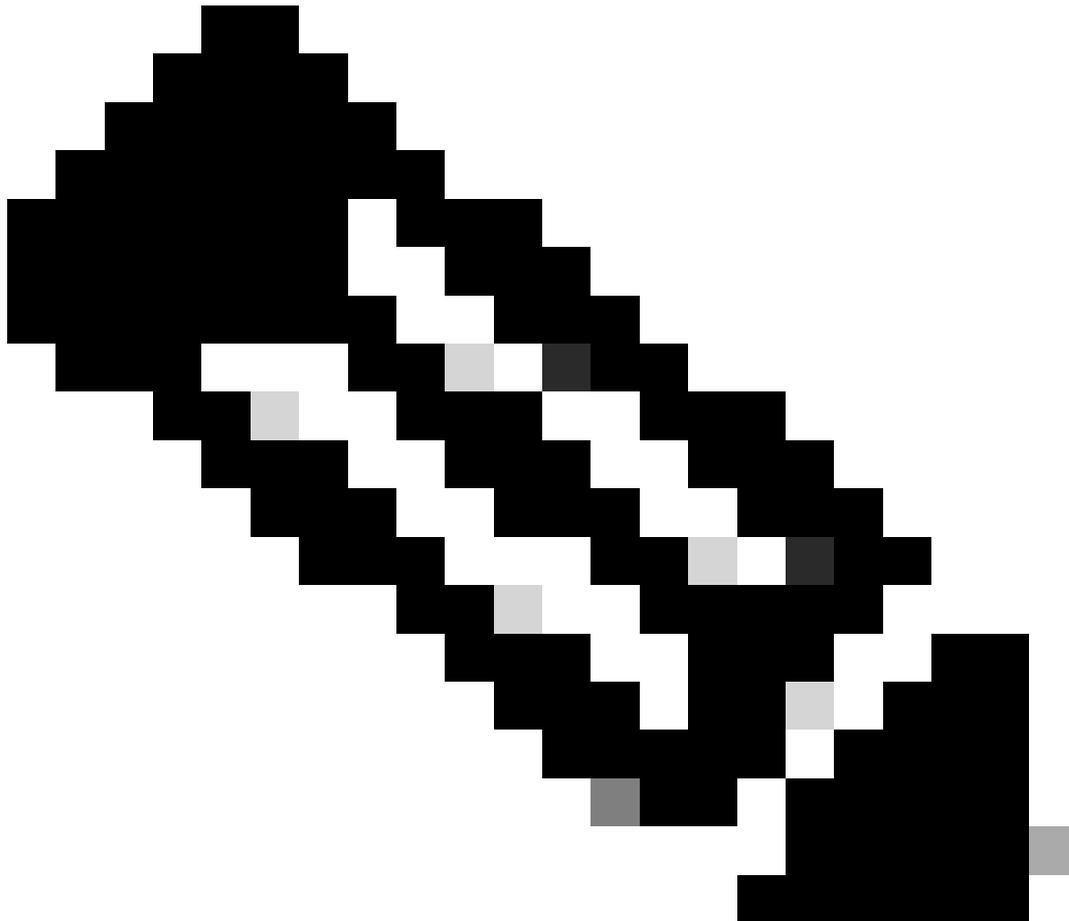
---

Durch die Deaktivierung des Zugriffsfelds für die AWS-Verwaltungskonsole wird verhindert, dass sich der Benutzer über die Webbenutzeroberfläche beim AWS-Konto anmeldet.

---

6: Weisen Sie eine Richtlinie zu, indem Sie sie dem Benutzer zuweisen, einer Gruppe direkt hinzufügen oder inline konfigurieren.

---



Anmerkung: Zu Demonstrationszwecken weisen Sie dem Benutzer direkt Richtlinien zu.  
Weitere Informationen - [Verwalten von AWS-Richtlinien](#)

---

7: Suchen Sie nach S3 Full Access und wählen Sie AmazonS3Full Access aus, wodurch der Benutzer vollen Zugriff für jeden S3-Bucket hat, der auf seinem entsprechenden AWS-Konto erstellt wurde.

8: Aktivieren Sie das Kontrollkästchen mit dem Richtliniennamen AmazonS3FullAccess, und klicken Sie auf Weiter.

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 Filter: 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. Refresh Remove Add permissions

Filter by Type

Search: Search Filter: All types 1 match

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

**AmazonS3FullAccess** Copy JSON

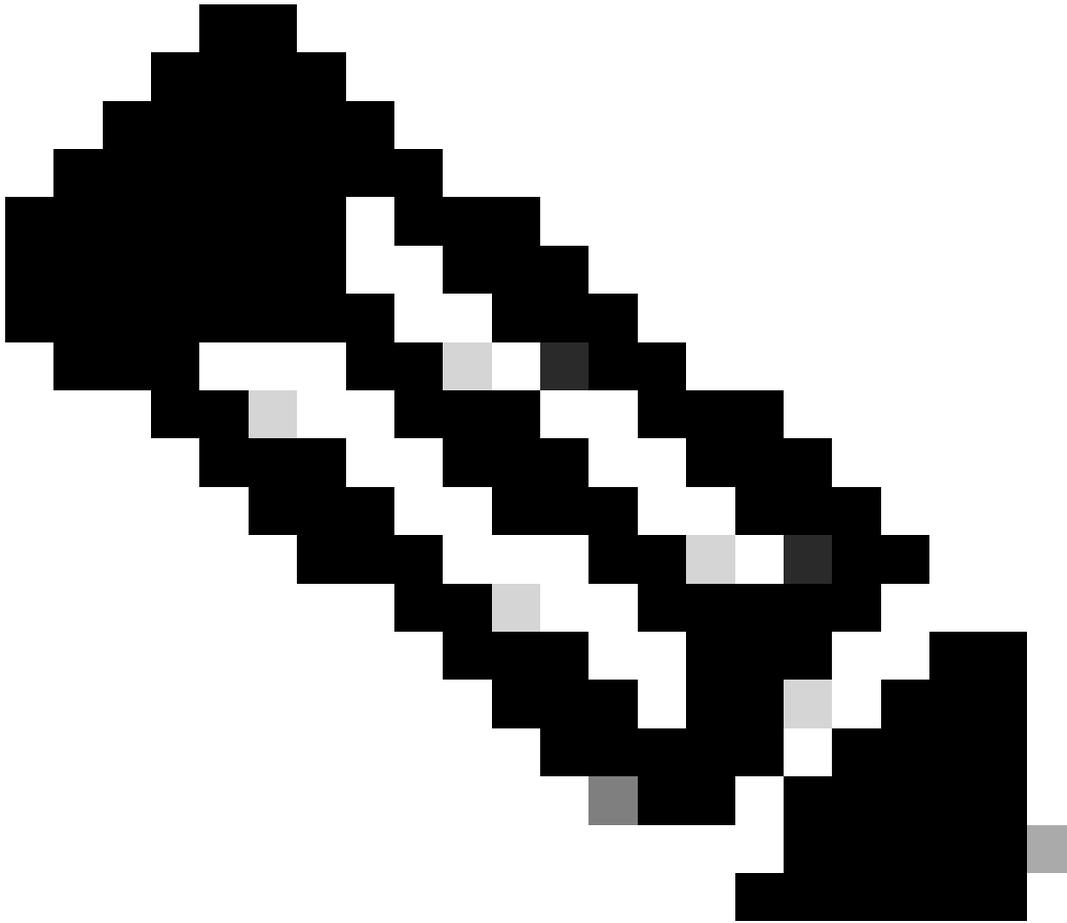
Provides full access to all buckets via the AWS Management Console.

```

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 }

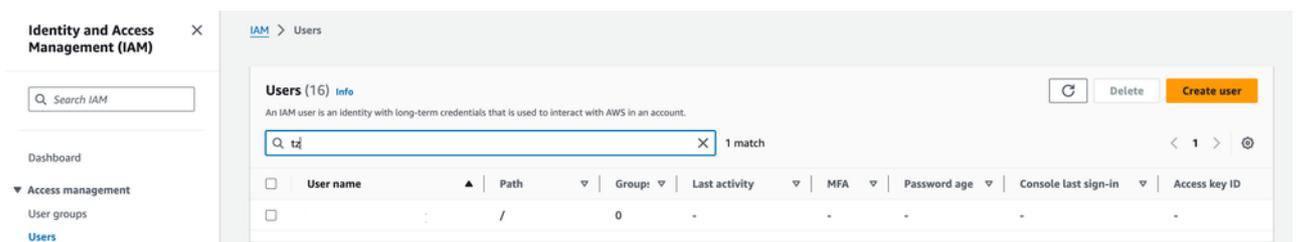
```

AWS-IAM



Anmerkung: Sie können detailliertere Richtlinien erstellen, indem Sie nur bestimmte Gruppen zulassen. Navigieren Sie zu [Richtlinienerstellung](#), um Ihre S3-Gruppen-Richtlinie im JSON-Format zu erstellen.

9: Sobald der Benutzer erstellt wurde, listen Sie den Benutzer auf und navigieren zur Registerkarte Sicherheitsanmeldeinformationen, und klicken Sie auf Zugriffsschlüssel erstellen.



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: Wählen Sie das andere Optionsfeld aus, und fügen Sie optional ein Tag hinzu.

## 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: Klicken Sie auf CSV-Datei herunterladen. Dies ist der Zugriffsschlüssel in einer CSV-Datei, der nicht mehr heruntergeladen oder angezeigt werden kann, wenn Sie diese Seite verlassen.

**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.

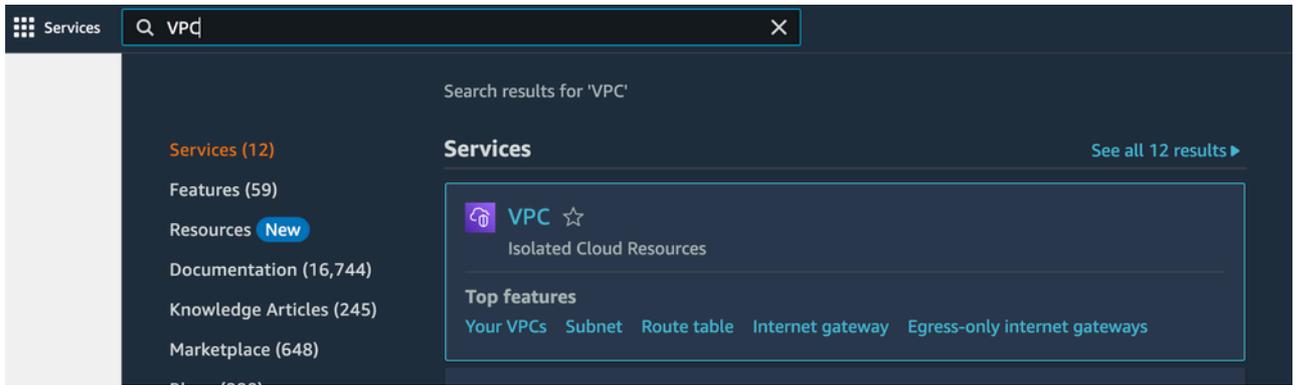
For more details about managing access keys, see the [best practices for managing AWS access keys](#).

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

AWS-IAM

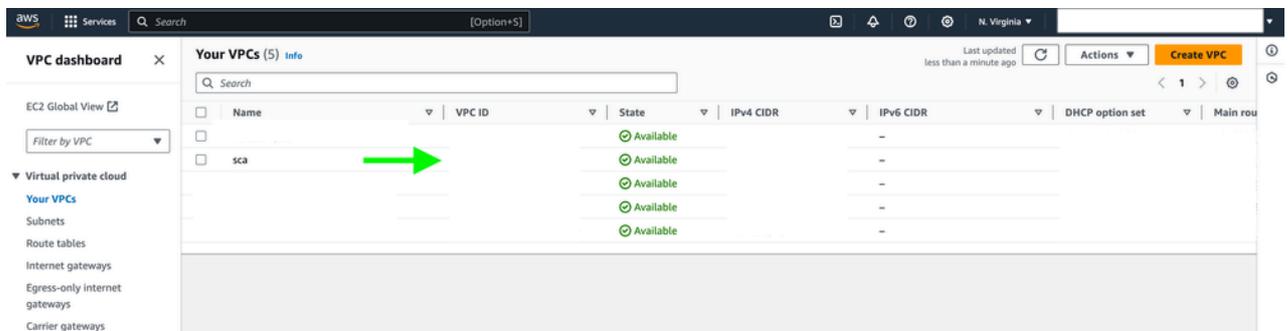
## Schritt 3: VPC-Ablaufprotokolle konfigurieren

1: Starten Sie VPC in der gewünschten Region, und navigieren Sie zu Ihrer VPC-Option.

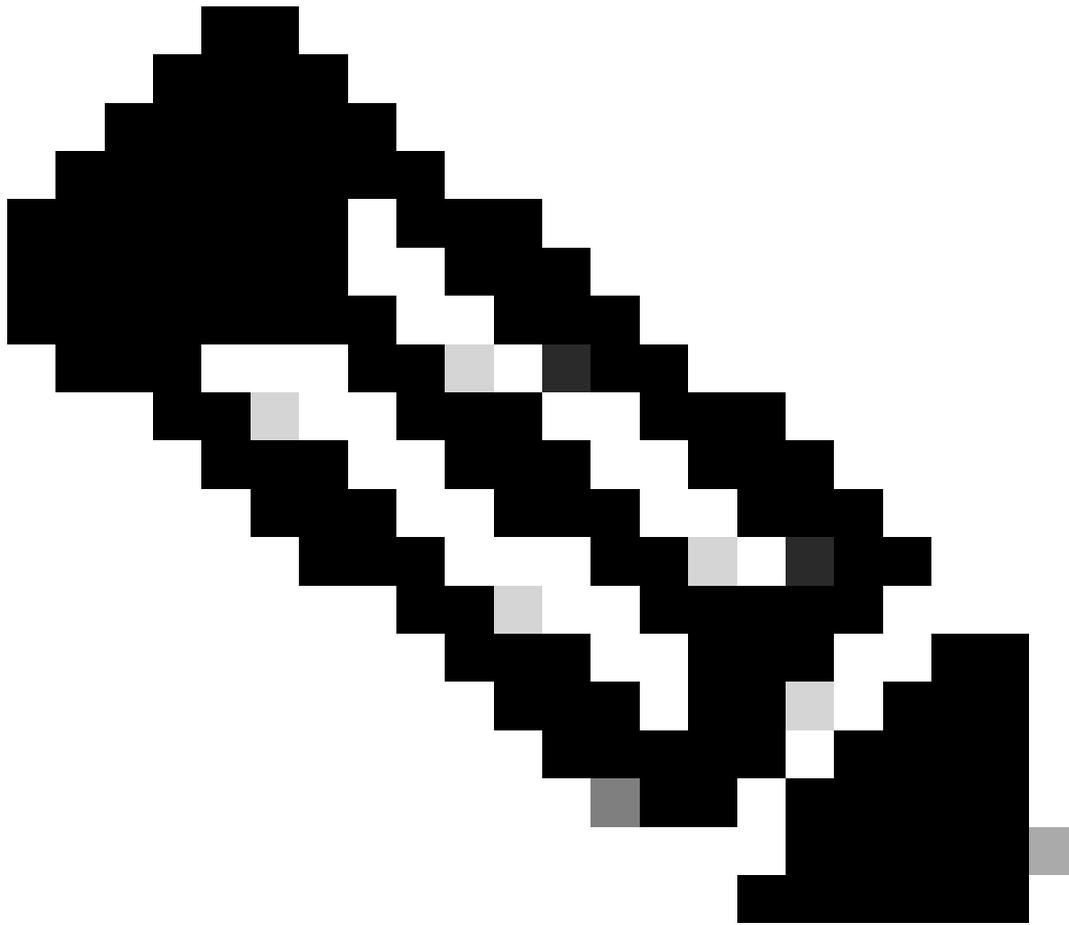


AWS-Flow-Protokolle

2: Wählen Sie Ihre vPC aus der Liste auf dem Bildschirm aus.



AWS-Flow-Protokolle



Anmerkung: Sie haben in dieser Demo den VPC-Namen SCA ausgewählt.

---

3: Navigieren Sie zu Ihren vPCs unter Virtual Private Cloud, wechseln Sie zur Registerkarte Flow-Protokolle, und klicken Sie auf Flow-Protokolle erstellen.

The screenshot shows the AWS Management Console interface for a VPC. The breadcrumb navigation is 'VPC > Your VPCs > vpc-60bdda1d / sca'. The 'Details' section shows various VPC settings, including 'State: Available', 'DNS hostnames: Enabled', and 'DNS resolution: Enabled'. The 'Flow logs' tab is active, displaying a table with 4 flow logs. A 'Create flow log' button is visible in the top right of the flow logs section, with a black arrow pointing to it.

**Details**

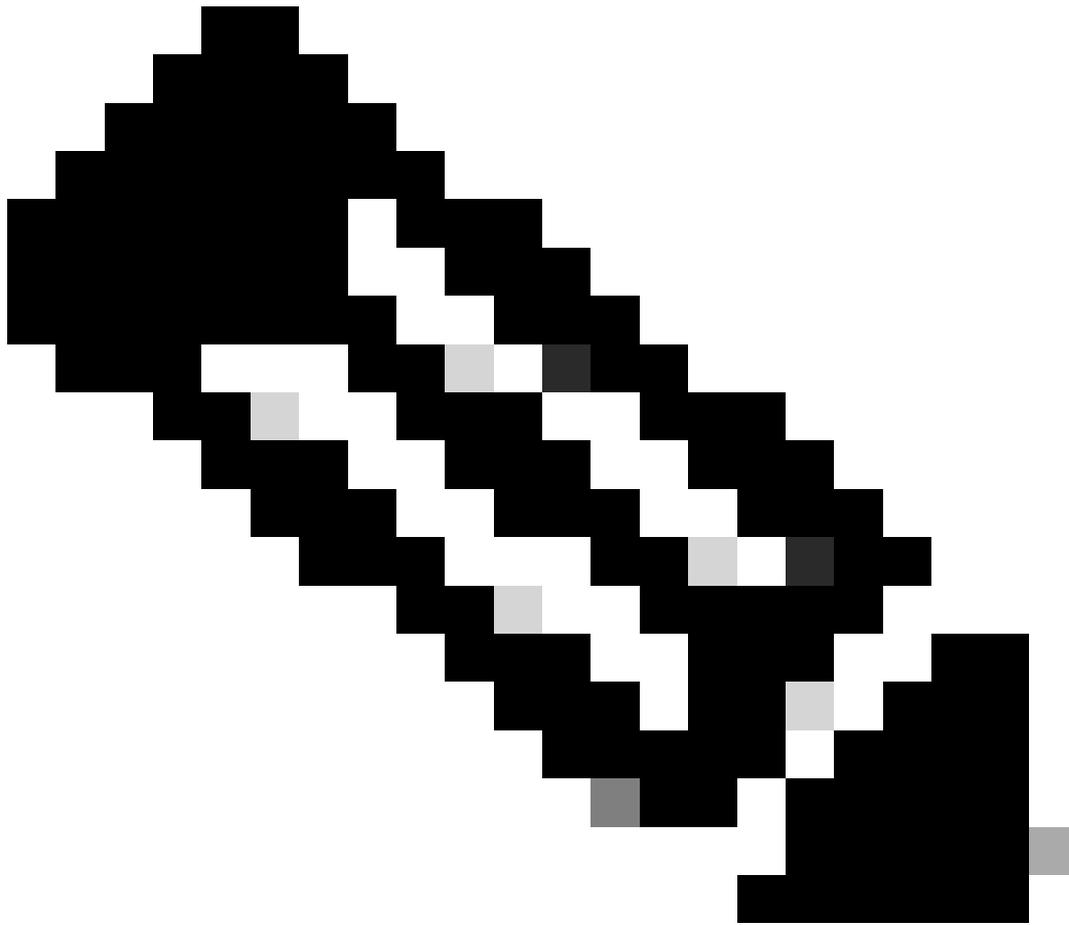
VPC ID	State	DNS hostnames	DNS resolution
📄	🟢 Available	Enabled	Enabled
Tenancy	DHCP option set	Main route table	Main network ACL
Default			
Default VPC	IPv4 CIDR	IPv6 pool	IPv6 CIDR (Network border group)
Yes		-	-
Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups	Owner ID	
Disabled	-	📄	

**Flow logs (4)**

<input type="checkbox"/>	Name	Flow log ID	Filter	Destination type	Destination name	IAM role ARN
<input type="checkbox"/>			ALL			
<input type="checkbox"/>			ALL			
<input type="checkbox"/>			ALL			
<input type="checkbox"/>			ALL			

AWS-Flow-Protokolle

4: Geben Sie Ihren Flow-Protokollen einen Namen, und geben Sie die zuvor erstellte S3-Bucket-ARN frei.



Anmerkung: Informationen zu ARN finden Sie unter Konfigurieren von S3 bucket - Schritt 6

---

5: Sie haben die Möglichkeit, das AWS-Standardprotokollformat zu verwenden oder ein benutzerdefiniertes Protokollformat zu erstellen, falls weitere Felder erforderlich sind.

[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

AWS-Flow-Protokolle

7: Klicken Sie auf Flussprotokolle erstellen.

### 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:

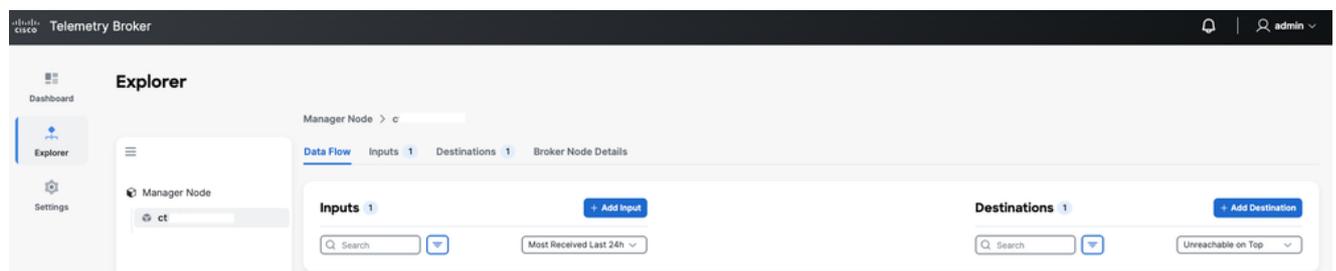
You can add 49 more tags



AWS-Flow-Protokolle

## Schritt 4: Konfigurieren der VPC-Eingabe in der CTB

1: Zugriff auf CTB Web UI, navigieren Sie zu Explorer > Broker-Knoten Registerkarte > klicken Sie auf Öffnen Broker-Knoten > Datenfluss-Registerkarte > Klicken Sie auf Eingabe hinzufügen.



CTB-Eingabe-Benutzeroberfläche

2: Wählen Sie als Eingabetyp AWS VPC Flow log aus, und klicken Sie auf Weiter.

# Add Input



## Select Input type

Type or Select Input



UDP Input

AWS VPC Flow log

AWS VPC Flow log

Azure NSG Flow log

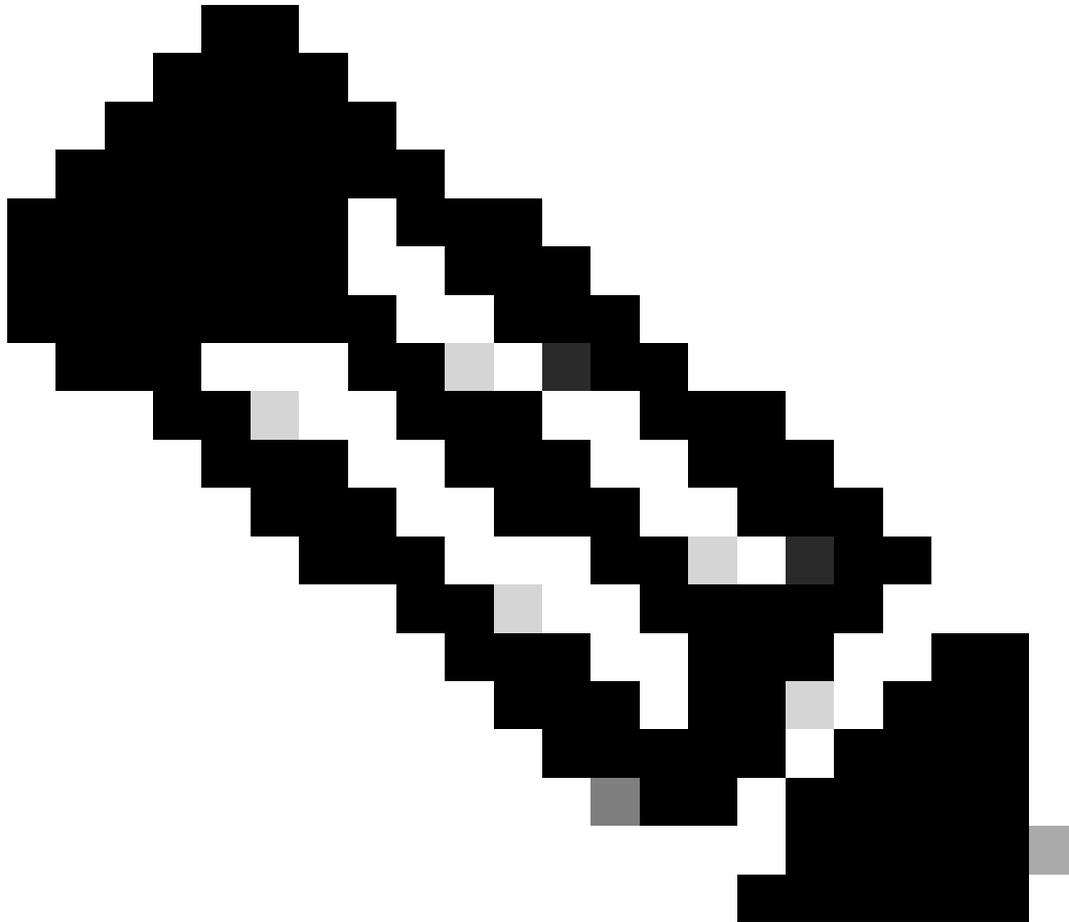
Flow Generator Input

---

Informationen zu S3 Bucket Path finden Sie unter Konfigurieren von VPC-Flow-Protokollen - Schritt 7.

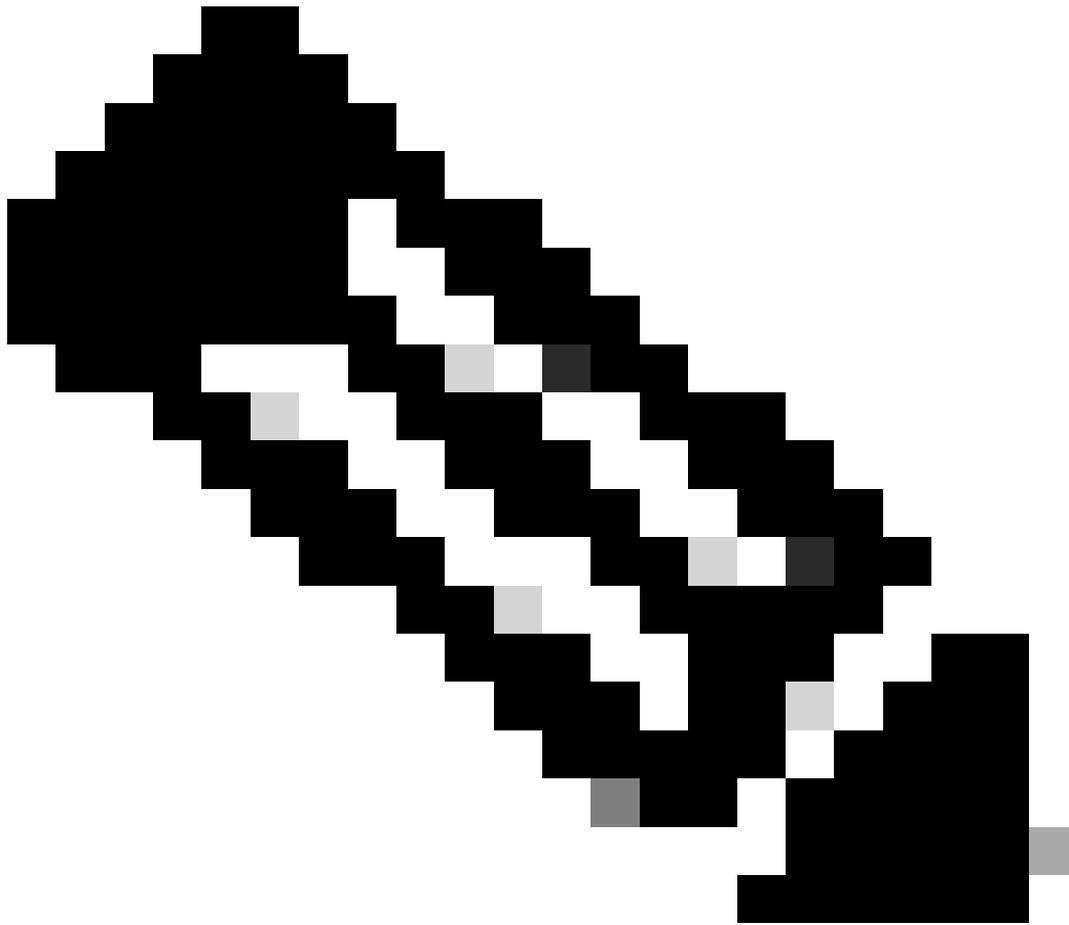
---

---



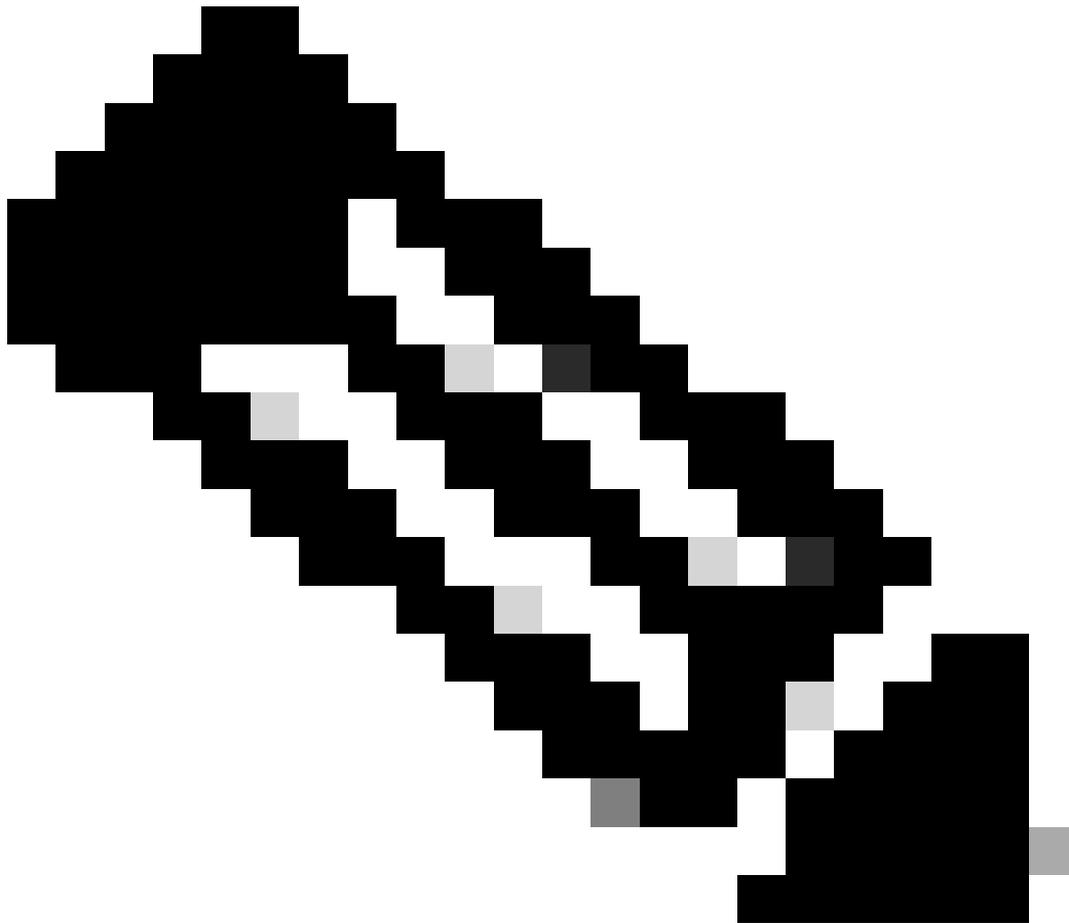
Anmerkung: Die Regionskennzahl finden Sie auf der AWS-Startseite neben dem Zahnradsymbol.

---



Hinweis: Jede IP-Adresse, die als Eingabe-IP-Adresse konfiguriert ist (eindeutige, von keinem anderen Exporteur gemeinsam genutzte IP-Adresse), wird als Exporteur für die umgewandelten NetFlow-Daten gemeldet.

---



Anmerkung: Informationen zur AWS-Zugriffsschlüssel-ID finden Sie unter Konfigurieren des IAM-Benutzers für den Zugriffsschlüssel mit der S3-Zugriffsrichtlinie, Schritt 9

---

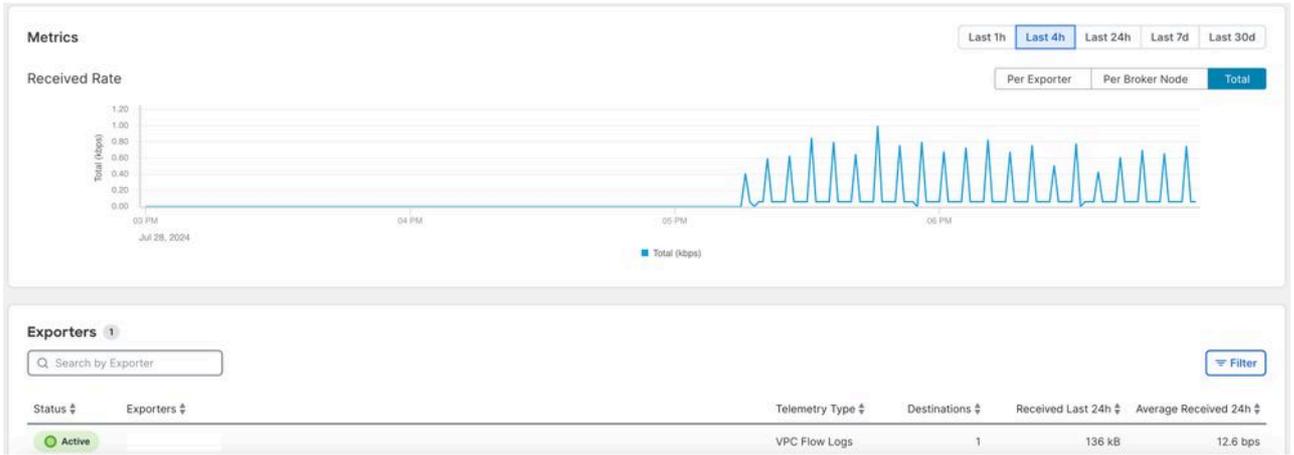
## Überprüfung

Nach einigen Minuten der Konfiguration der AWS VPC-Eingabe wird die Statusspalte aktiviert, wenn der AWS S3-Bucket Daten enthält.

Überprüfen Sie mithilfe dieser Schritte den Status der AWS VPC-Eingabe.

1: Melden Sie sich bei der CTB-Benutzeroberfläche an, und navigieren Sie zu Explorer > Broker node tab > click open broker node > switch tab to Input > Click open AWS input.

2: Überprüfen Sie, ob die konfigurierten WS-Flow-Protokolle den Status "Aktiv" aufweisen und die empfangene Metrik einen steigenden Graphen aufweist.



CTB-Eingabe-Benutzeroberfläche

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.