

Configuration des journaux de flux VPC AWS pour l'entrée CTB

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configuration Steps](#)

[Étape 1 : configuration du compartiment S3 dans AWS](#)

[Étape 2. Créer un utilisateur IAM avec une clé d'accès et joindre une stratégie de groupement S3](#)

[Étape 3 : configuration des journaux de flux VPC](#)

[Étape 4. Configuration de l'entrée VPC dans CTB](#)

[Vérifier](#)

Introduction

Ce document décrit comment configurer les journaux de flux VPC en tant qu'entrée du service Cisco Telemetry Broker (CTB).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Services Web Amazon (AWS)
- Administration de CTB.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration Steps

Étape 1 : configuration du compartiment S3 dans AWS

- 1: Connectez-vous à la console de gestion AWS avec un nom d'utilisateur et un mot de passe.
- 2: Assurez-vous de vous connecter à la région appropriée.
- 3: Accédez à la barre de recherche et tapez S3.

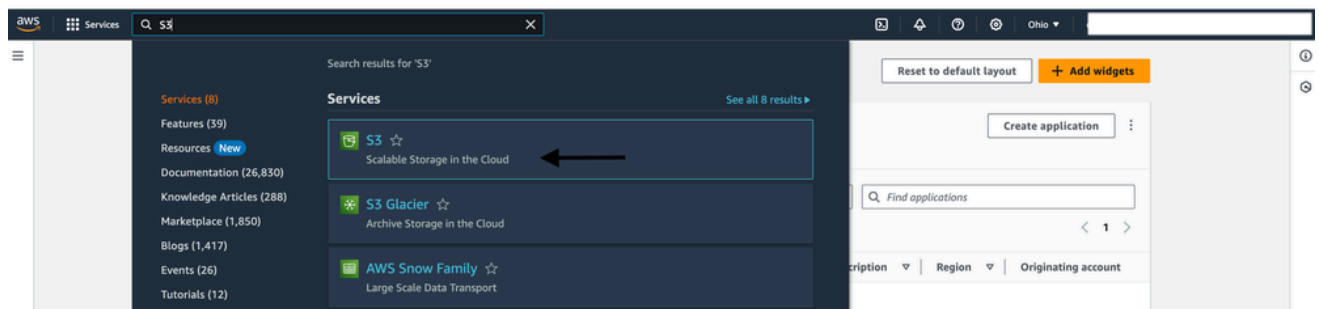
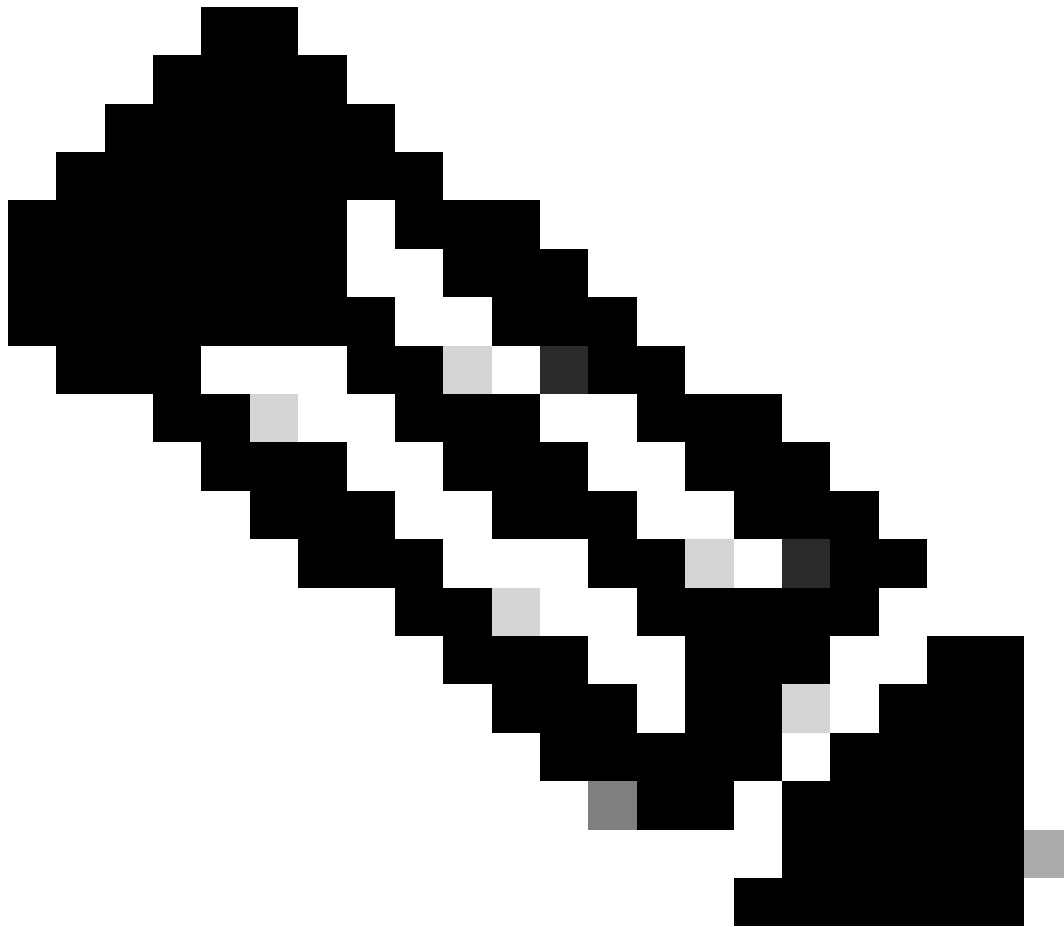
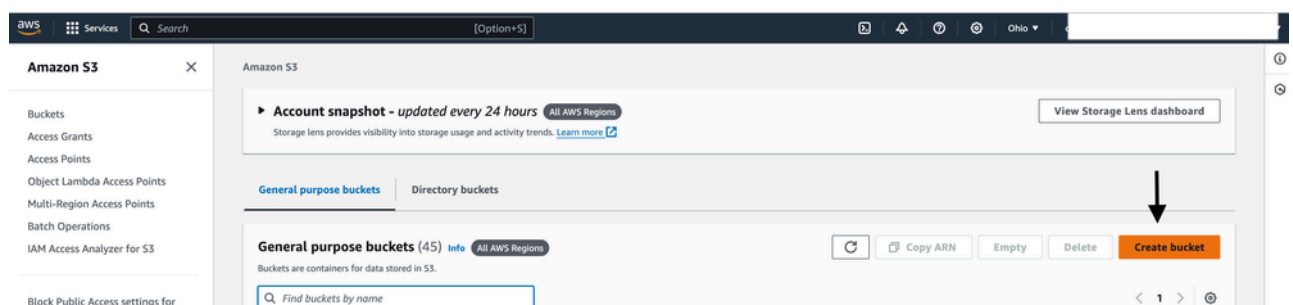


tableau de bord AWS



Remarque : Dans la démonstration, vous avez sélectionné la région de l'Ohio avec la zone de disponibilité us-east-2, elle est visible juste à côté de l'icône d'engrenage.

4: Cliquez sur Créer un compartiment.



AWS-S3

5: Donnez un nom à bucket et laissez chaque option telle quelle, puis cliquez sur 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: Une fois que le bucket est créé avec succès, enregistrez le bucket ARN qui doit être utilisé plus tard pendant la configuration.

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

[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](#)

  Copy ARN  Empty  Delete  Create bucket

Buckets are containers for data stored in S3.

1 match

Name ▲

AWS Region ▼

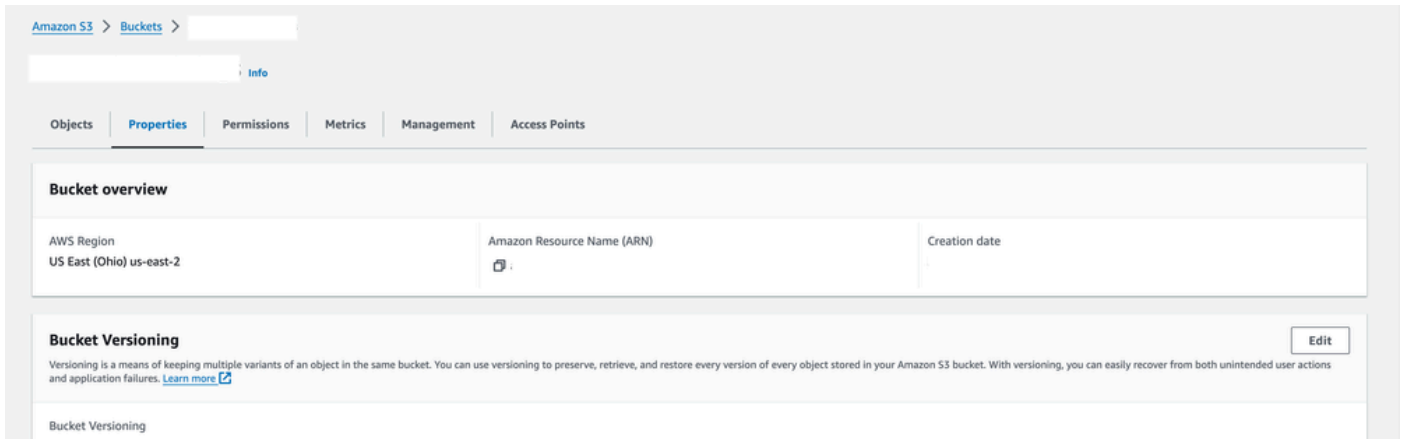
IAM Access Analyzer

Creation date ▼

○

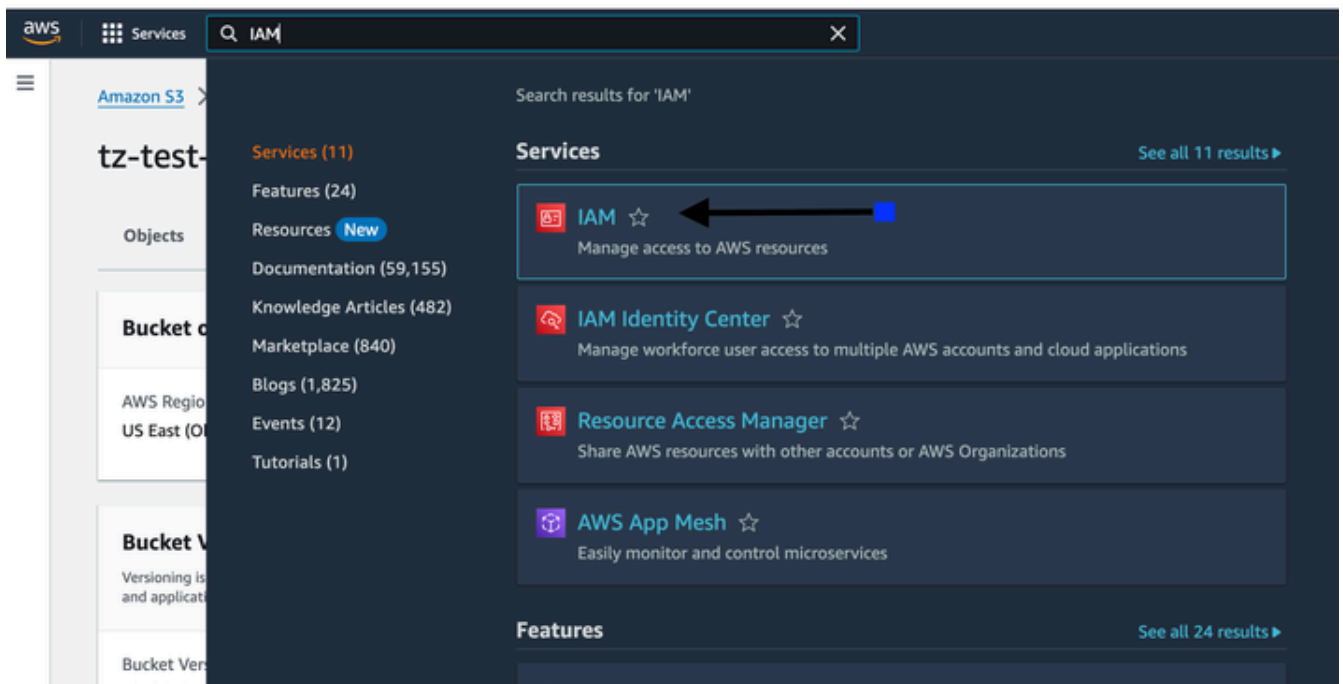
US East (Ohio) us-east-2

AWS-S3



Étape 2. Créer un utilisateur IAM avec une clé d'accès et joindre une stratégie de groupement S3

1: Lancez l'IAM à partir de la barre de recherche AWS.



2: Accédez aux utilisateurs.



Services



Search

Identity and Access Management (IAM)



Search IAM

Dashboard

▼ Access management

User groups

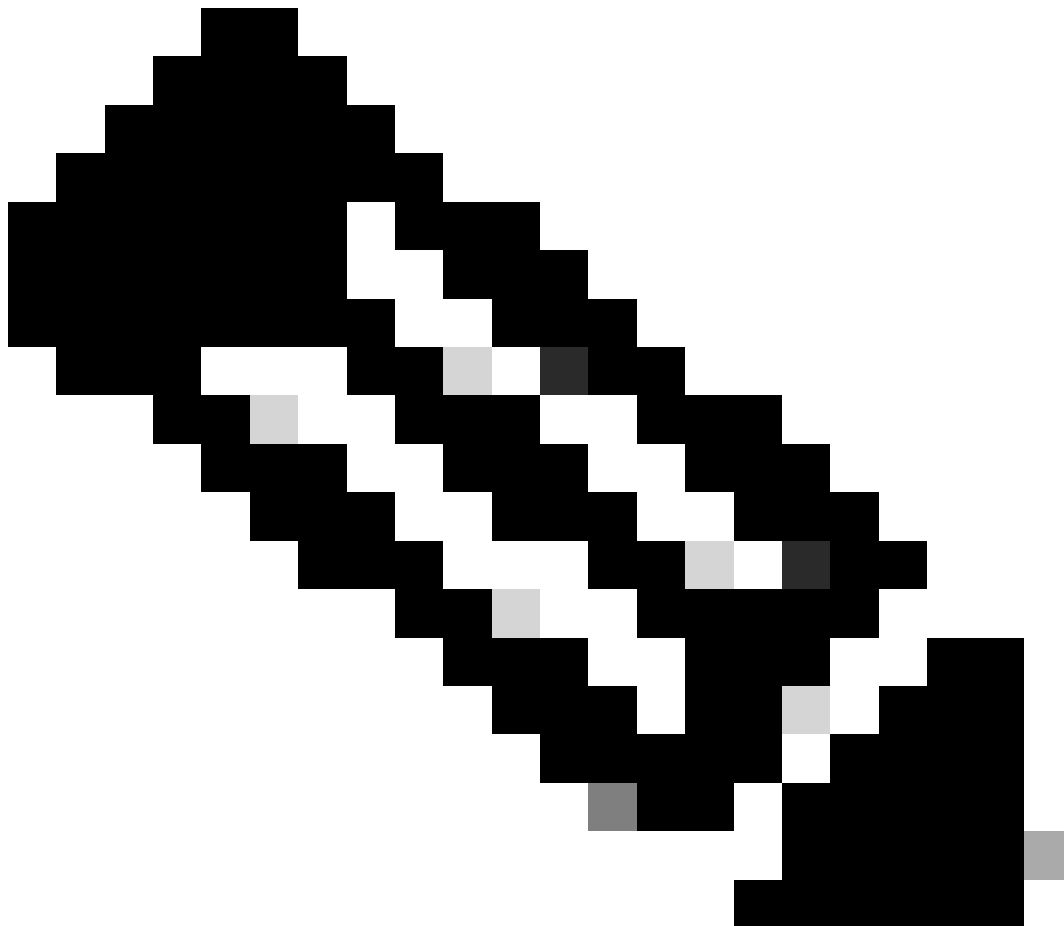
Users

Roles

Policies

En décochant la case d'accès à la console de gestion AWS, l'utilisateur ne peut pas se connecter au compte AWS à l'aide de l'interface utilisateur Web.

6 : Attribuez une stratégie en l'attribuant à l'utilisateur, en l'attachant directement à un groupe ou en la configurant en ligne.



Remarque : Pour la démonstration, vous affectez directement la stratégie à l'utilisateur.
Pour plus d'informations - [Gestion des stratégies AWS](#)

7: Recherchez S3 full access et sélectionnez AmazonS3full access, qui permet à l'utilisateur d'avoir un accès complet pour chaque compartiment S3 créé sur son compte AWS correspondant.

8: Cochez la case avec le nom de stratégie AmazonS3FullAccess et cliquez sur 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

All types

1 match

☐	Policy name	Type	Attached entities
☐	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

All types

< 1 >

☐	Policy name	Type	Attached via
☐	AmazonS3FullAccess	AWS managed	Directly

AmazonS3FullAccess

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

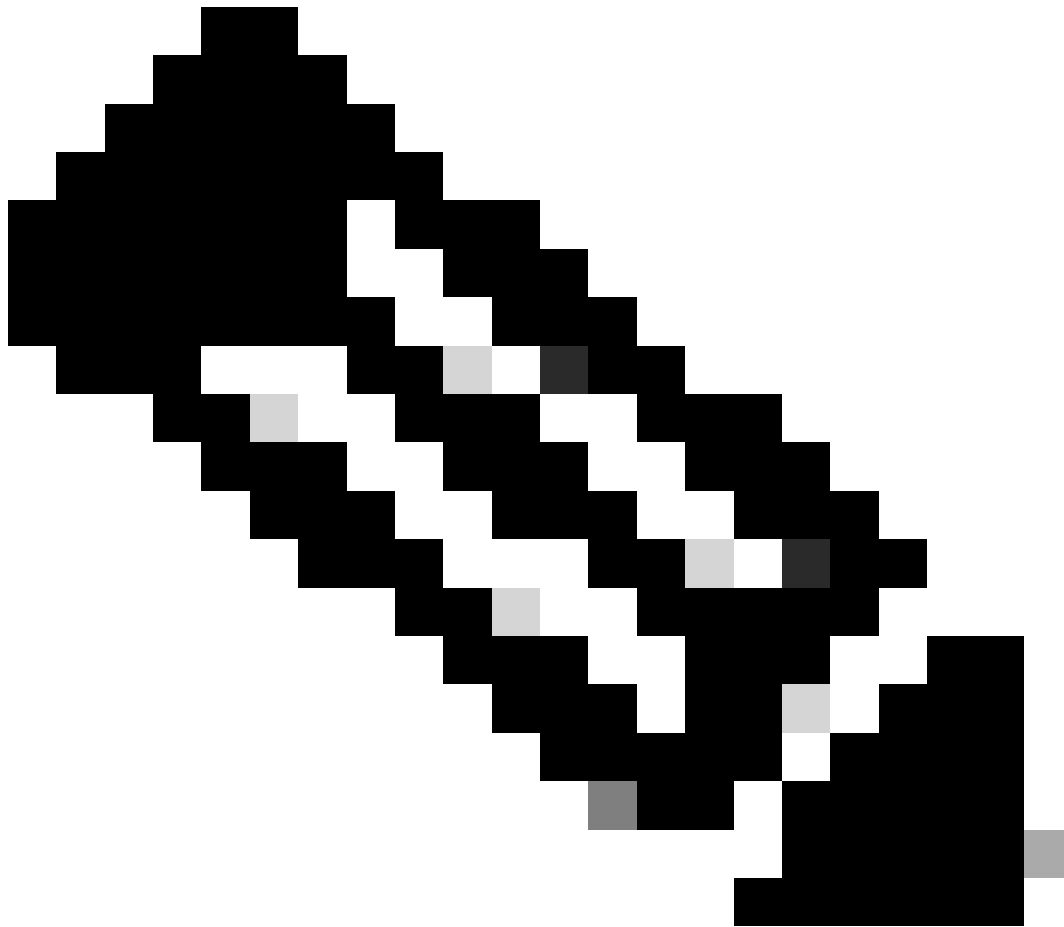
]

13

}

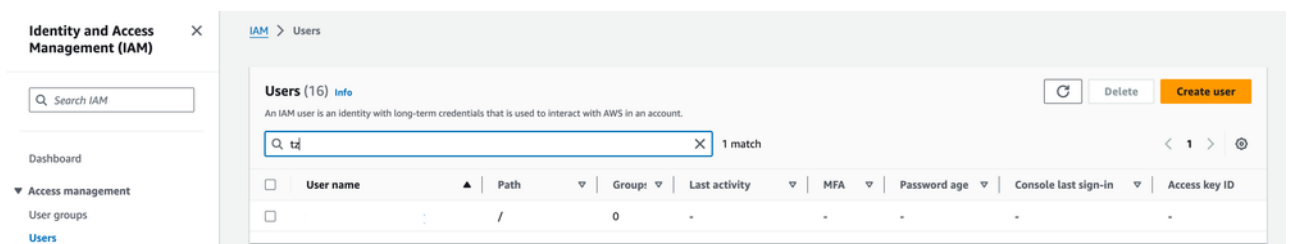
Copy JSON

AWS-IAM



Remarque : Vous pouvez créer une stratégie plus granulaire en n'autorisant que des regroupements spécifiques. Accédez à [Création de stratégie](#) pour créer votre stratégie de regroupement S3 au format json.

9: Une fois l'utilisateur créé, répertoriez-le et accédez à l'onglet security credential et cliquez sur 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: Sélectionnez l'autre case d'option et ajoutez éventuellement une balise.

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 : Cliquez sur Télécharger le fichier .csv. Il s'agit de la clé d'accès d'un fichier csv qui n'est plus disponible pour le téléchargement ou l'affichage une fois que vous avez quitté cette 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 > > 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.

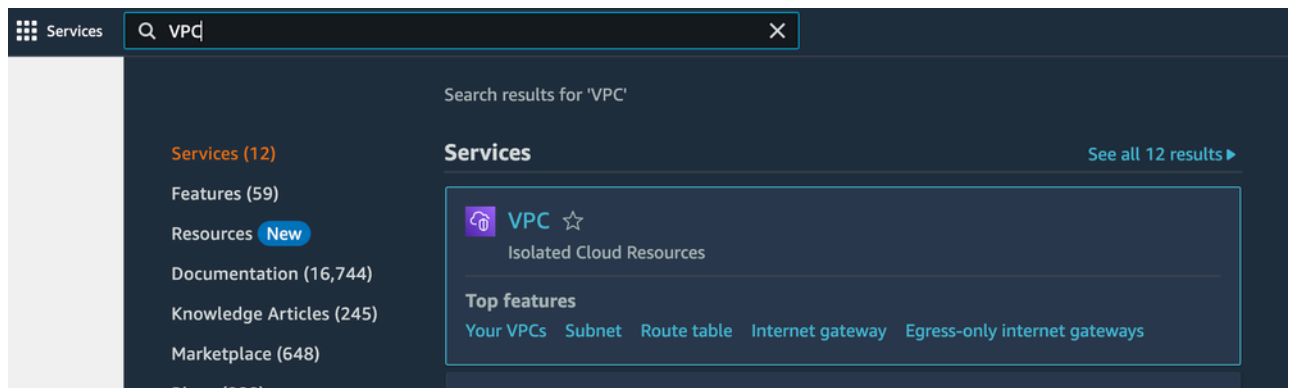
For more details about managing access keys, see the [best practices for managing AWS access keys](#).

Download .csv file
Done

AWS-IAM

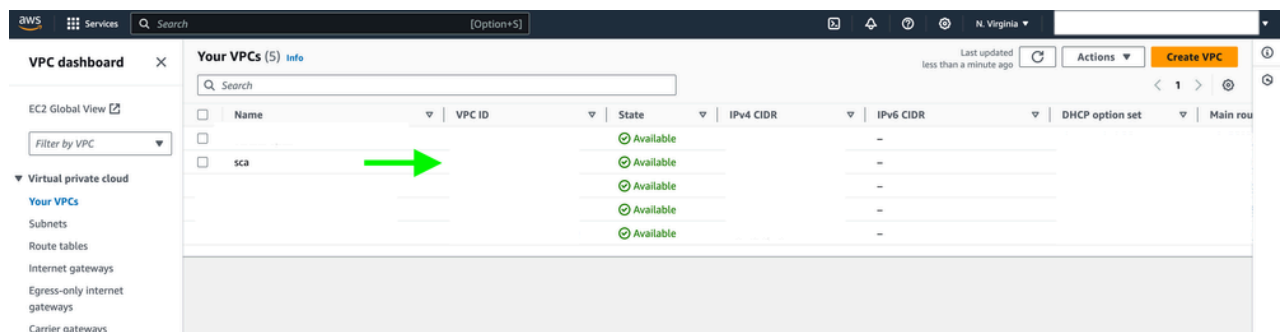
Étape 3 : configuration des journaux de flux VPC

1: Lancez votre VPC dans la région de votre choix et accédez à votre option VPC.

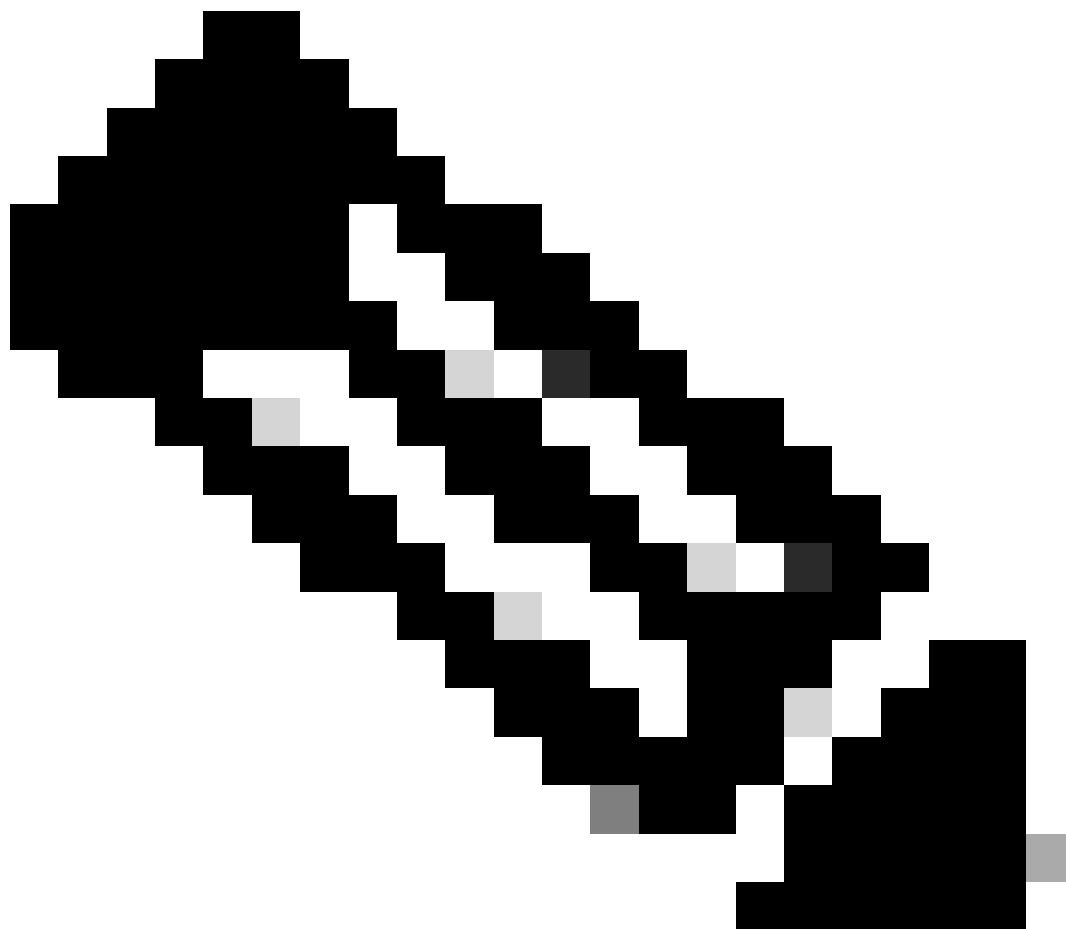


Journaux de flux AWS

2: Sélectionnez votre VPC dans la liste qui s'affiche à l'écran.



Journaux de flux AWS



Remarque : Vous avez sélectionné le nom VPC SCA dans cette démonstration.

3: Accédez à Vos VPC sous Cloud privé virtuel, passez à l'onglet Journaux de flux et cliquez sur Créer des journaux de flux.

aws Services Search [Option+S] N. Virginia

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Network ACLs

Security groups

vpc-60bdda1d / sca

Details

VPC ID: vpc-60bdda1d

Tenancy: Default

Default VPC: Yes

Network Address Usage metrics: Disabled

State: Available

DHCP option set: -

IPv4 CIDR: -

Route 53 Resolver DNS Firewall rule groups: -

DNS hostnames: Enabled

Main route table: -

IPv6 pool: -

Owner ID: -

DNS resolution: Enabled

Main network ACL: -

IPv6 CIDR (Network border group): -

Resource map | CIDRs | Flow logs | Tags | Integrations

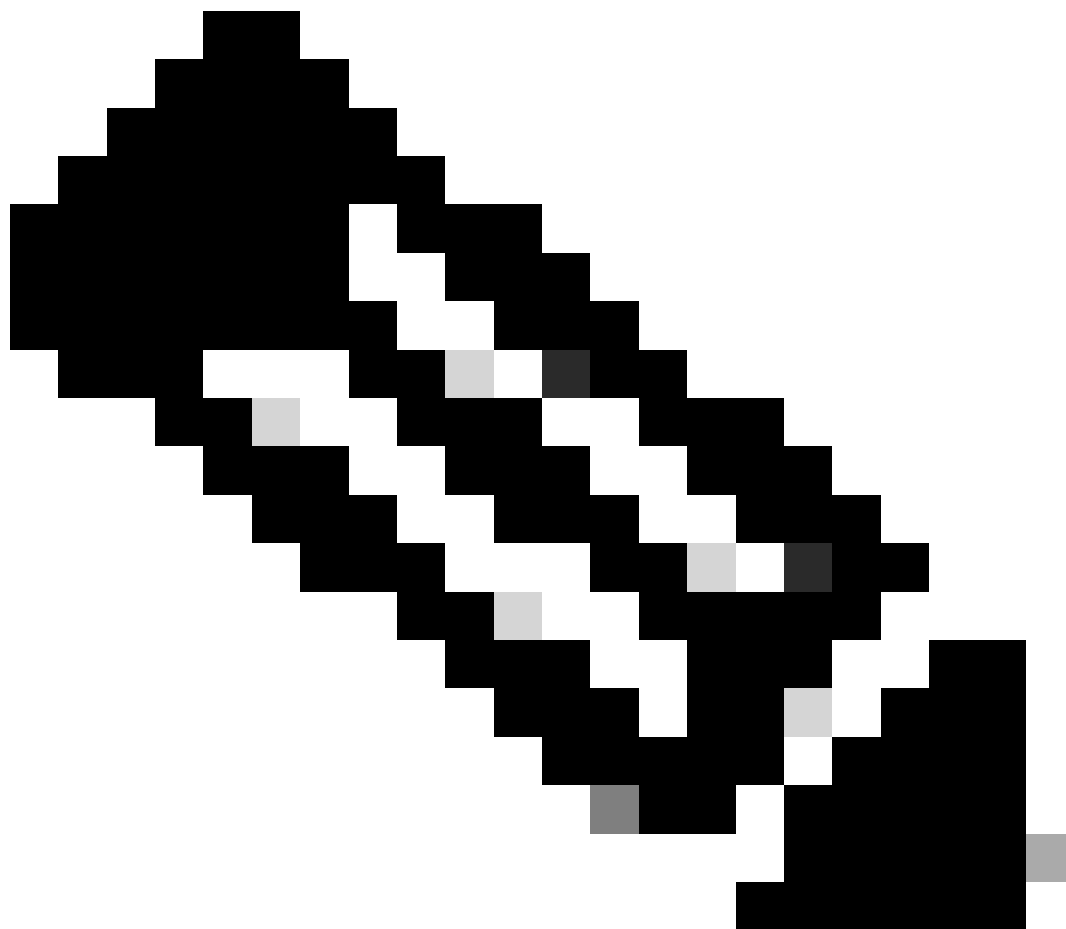
Flow logs (4)

Create flow log

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

Journaux de flux AWS

4: Donnez un nom à vos journaux de flux et partagez le compartiment S3 ARN créé précédemment.



Remarque : Pour ARN, reportez-vous à Configuration du compartiment S3 - Étape 6

5: Vous avez la possibilité d'utiliser le format de journal par défaut AWS ou de créer un format de journal personnalisé au cas où d'autres champs seraient nécessaires.

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

aws

Services

Search

[Option+S]

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](#)

arn:

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

Journaux de flux AWS

7: Cliquez sur créer des journaux de flux.

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](#)

arn:

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.

Select an attribute...

account-id

action

az-id

bytes

dstaddr

dstport

end

flow-direction

instance-id

interface-id

log-status

packets

pkt-dst-aws-service

pkt-dstaddr

pkt-src-aws-service

pkt-srcaddr

protocol

region

srcaddr

srcport

start

sublocation-id

sublocation-type

subnet-id

tcp-flags

traffic-path

type

version

vpc-id

Select all

Clear all

Format preview

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

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

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	
Name		Remove tag

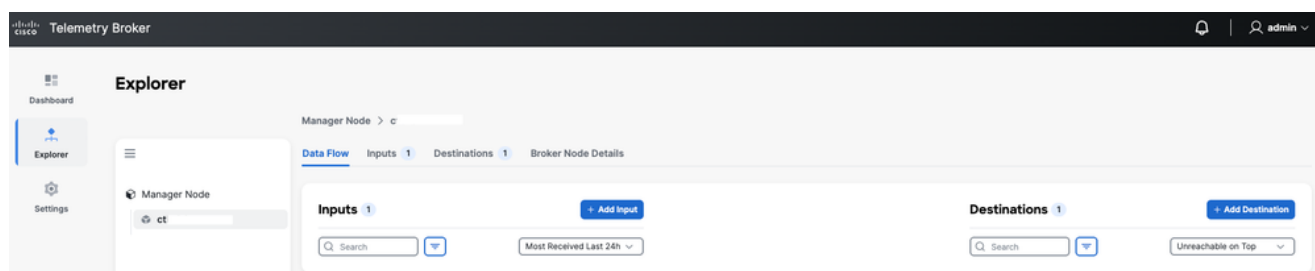
You can add 49 more tags



Journaux de flux AWS

Étape 4. Configuration de l'entrée VPC dans CTB

1 : Accédez à l'interface utilisateur Web de CTB, naviguez jusqu'à Explorer> Onglet de noeud Broker > cliquez sur ouvrir le noeud Broker > onglet Flux de données > cliquez sur Ajouter une entrée.



CTB-Input-UI

2: Sélectionnez Input type as AWS VPC Flow log et cliquez sur next.

Add Input



Select Input type

Type or Select Input ^

UDP Input

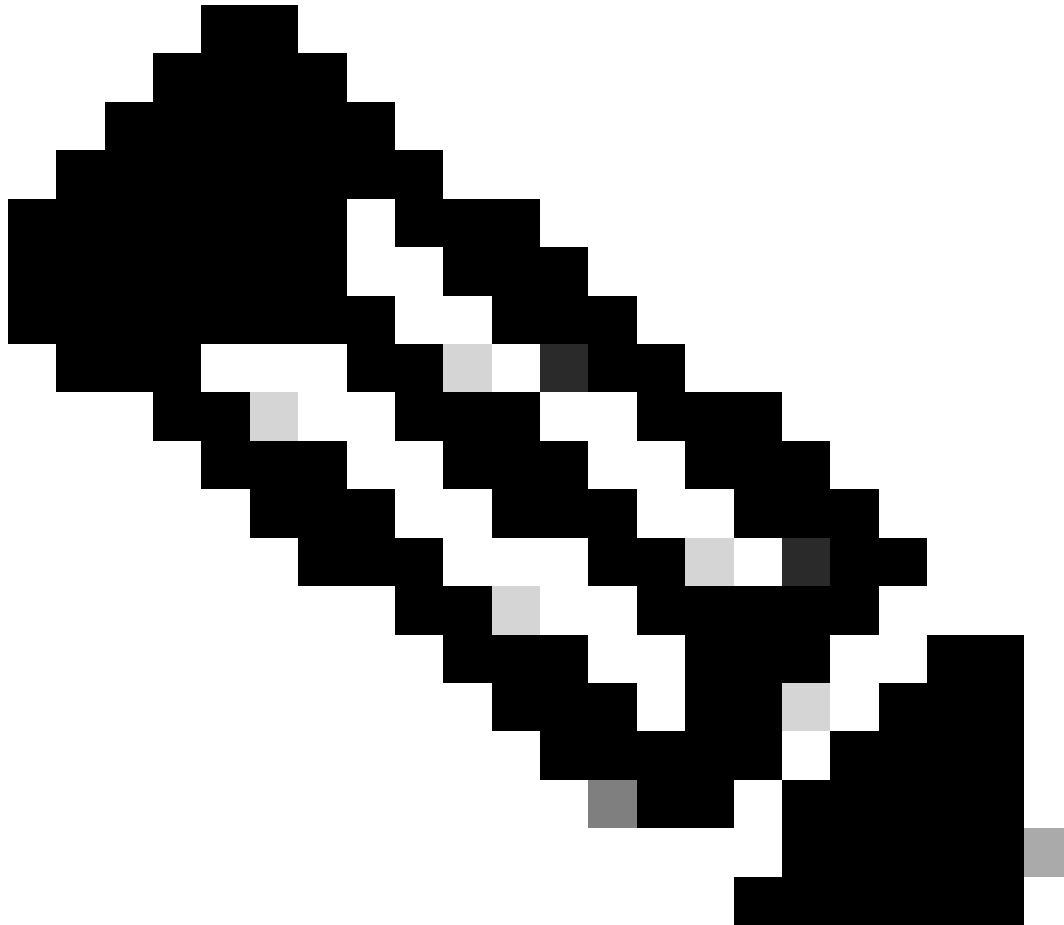
AWS VPC Flow log

Azure NSG Flow log

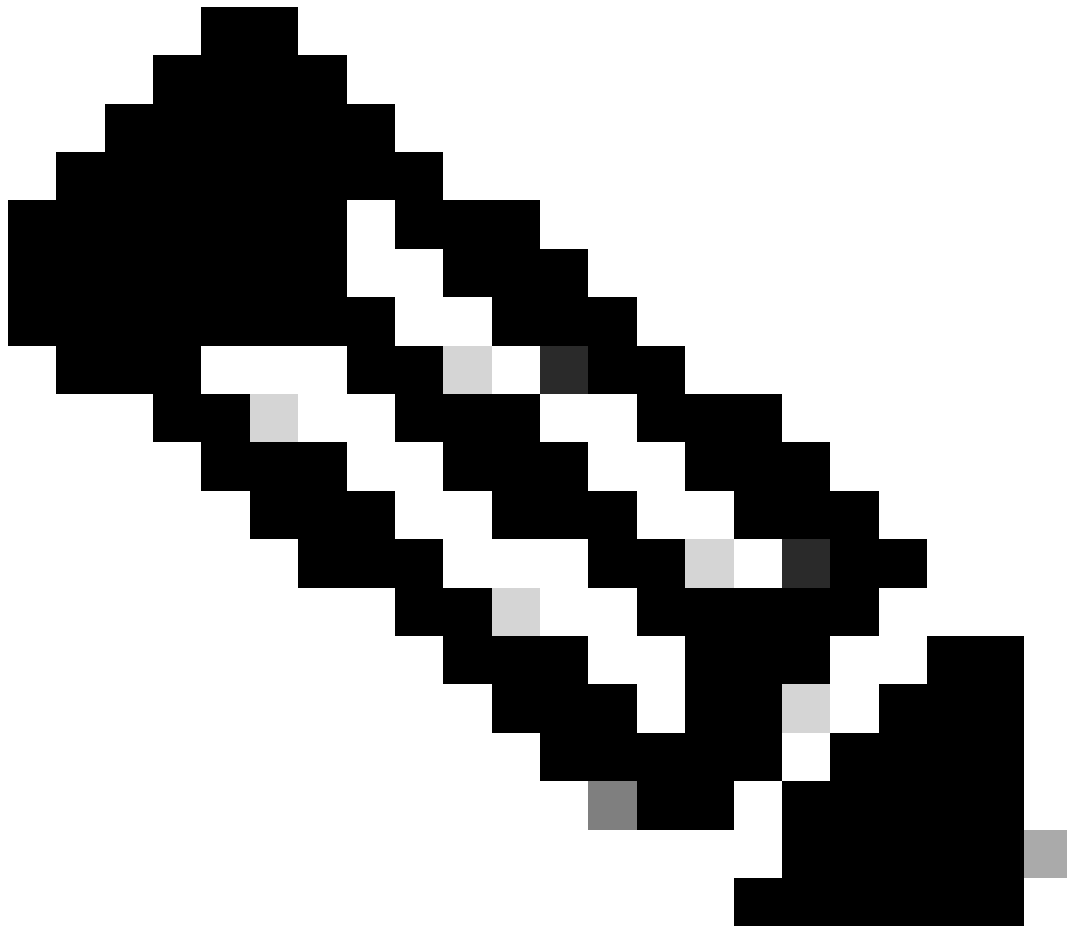
Flow Generator Input

AWS VPC Flow log

Pour connaître le code de la région, consultez la page d'accueil AWS en regard de l'icône du matériel.



Remarque : toute adresse IP configurée comme adresse IP d'entrée (adresse IP unique non partagée par un autre exportateur) est déclarée comme exportateur pour les données de flux réseau transformées.



Remarque : Pour l'ID de clé d'accès AWS, voir Configurer l'utilisateur IAM pour la clé d'accès avec la stratégie d'accès S3, étape 9

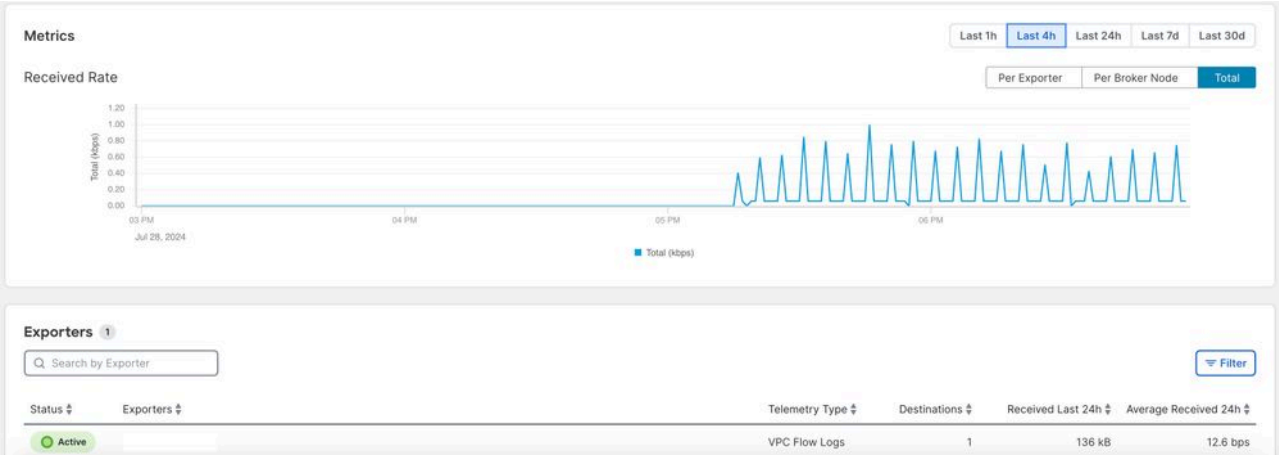
Vérifier

Après quelques minutes de configuration de l'entrée VPC AWS, la colonne d'état devient active si le compartiment AWS S3 contient des données.

Vérifiez l'état de l'entrée VPC AWS en procédant comme suit.

1: Connectez-vous à l'interface utilisateur de CTB et naviguez vers Explorer > onglet de noeud Broker > cliquez sur openbroker node > onglet de commutateur à Input > cliquez sur open AWS input.

2: Vérifiez que les journaux de flux aws configurés ont l'état actif et que les métriques reçues ont un graphique ascendant.



Exporters 1

Q 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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.