

AWS VPC Flow Logs configureren voor CTB-invoer

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratiestappen](#)

[Stap 1. S3-emmer in AWS configureren](#)

[Stap 2. Maak een IAM-gebruiker met toegangssleutel en voeg S3-pakketbeleid toe](#)

[Stap 3. VPC Flow Logs configureren](#)

[Stap 4. Configureer VPC Invoer naar CTB](#)

[Verifiëren](#)

Inleiding

Dit document beschrijft hoe u VPC Flow Logs kunt configureren als een ingang voor Cisco Telemetry Broker (CTB).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

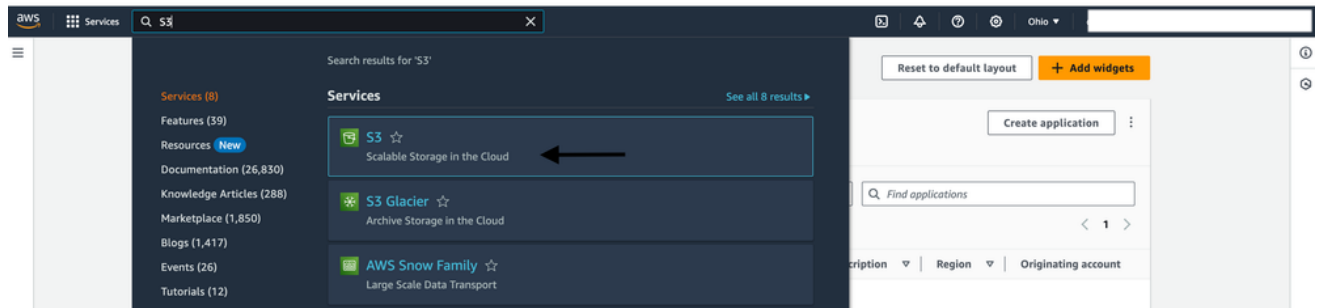
- CTB (v2.2.1+)
- AWS

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratiestappen

Stap 1. S3-emmer in AWS configureren

- 1: Meld u aan bij de AWS-beheerconsole met gebruikersnaam en wachtwoord.
- 2: Zorg ervoor dat u inlogt bij de juiste regio.
- 3: Navigeer naar de zoekbalk en typ S3.

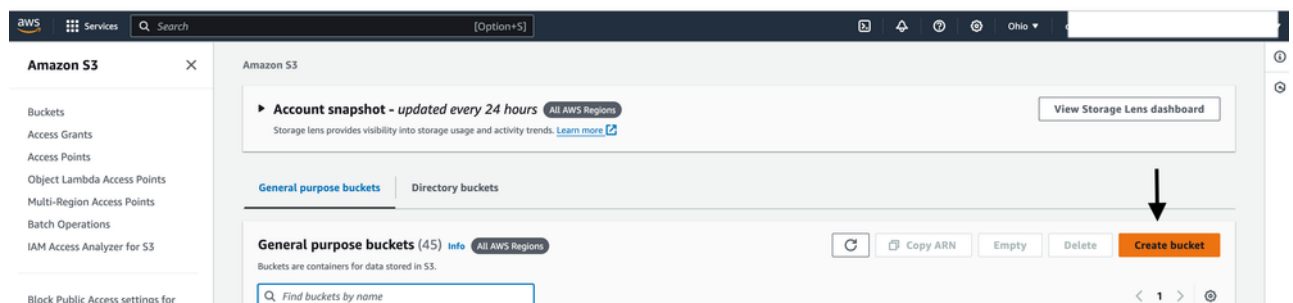


AWS-Dashboard



Opmerking: In demo, hebt u geselecteerd Ohio regio met ons-oost-2 beschikbaarheidszone, het is zichtbaar vlak naast het tandwielpictogram.

4: Klik op emmer maken.



AWS-S3,

5: Geef emmer een naam en laat elke optie ongewijzigd en klik op aanmaken.

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: Zodra de emmer met succes is gemaakt, slaat u de emmer ARN op die later tijdens de configuratie moet worden gebruikt.

 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

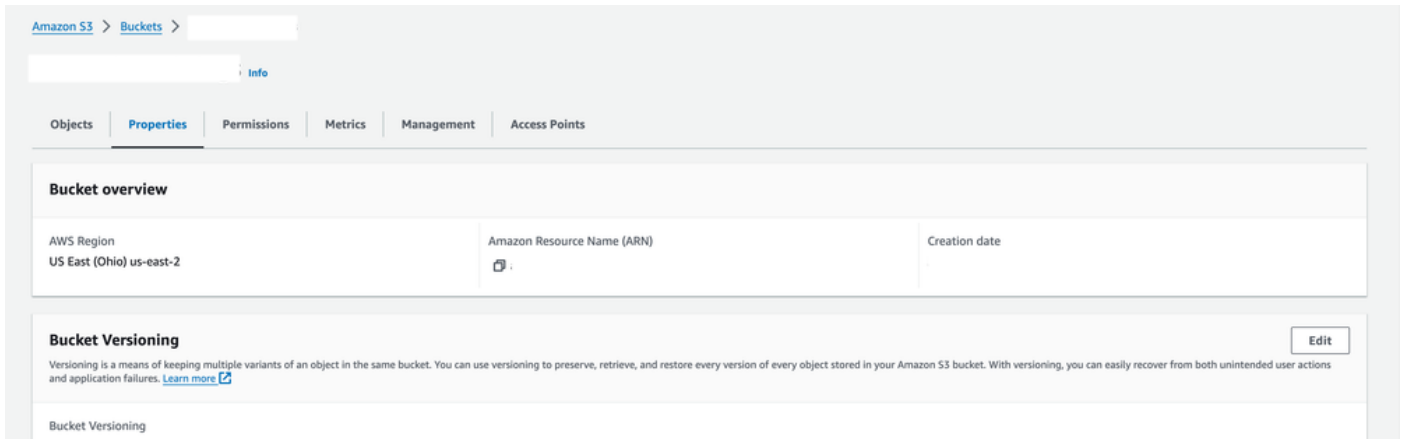
Buckets are containers for data stored in S3.

1 match

< 1 > 

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

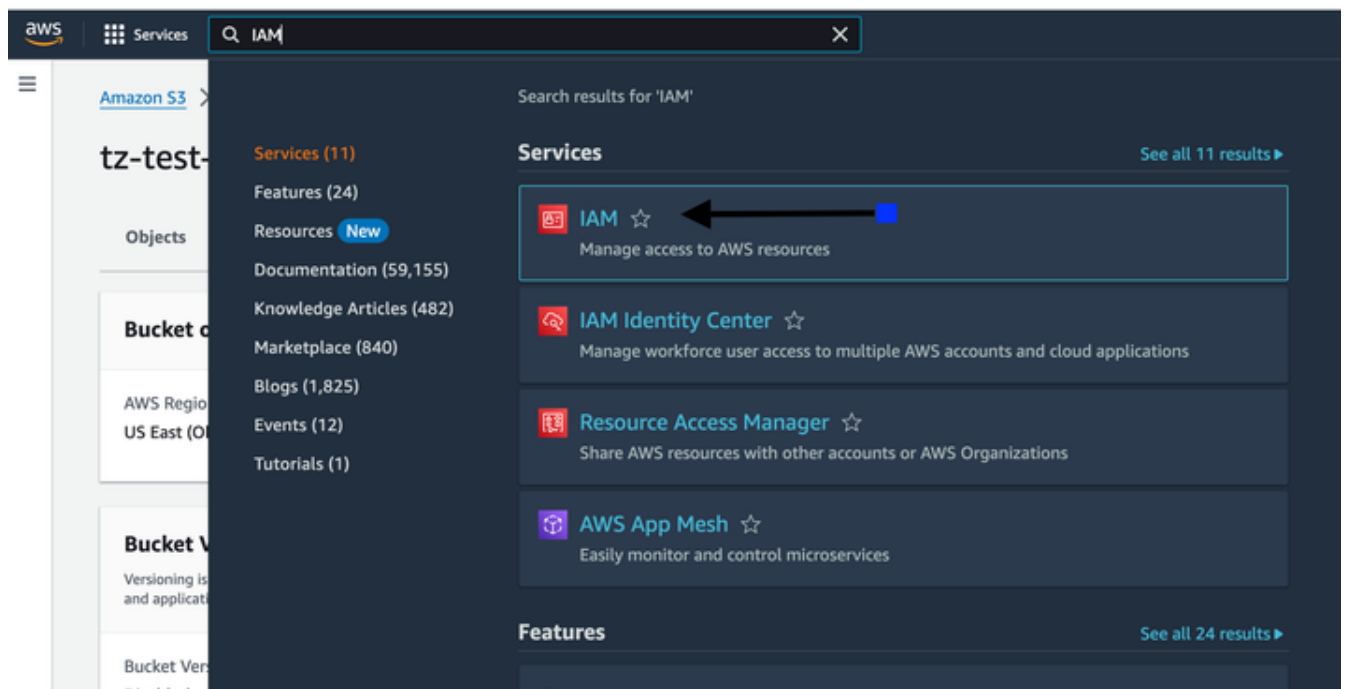
AWS-S3,



AWS-S3,

Stap 2. Maak een IAM-gebruiker met toegangssleutel en voeg S3-pakketbeleid toe

1: Start de IAM vanuit de zoekbalk.



AWS-IAM

2: Navigeer naar gebruikers.



Services



Search

Identity and Access Management (IAM)



Search IAM

Dashboard

▼ Access management

User groups

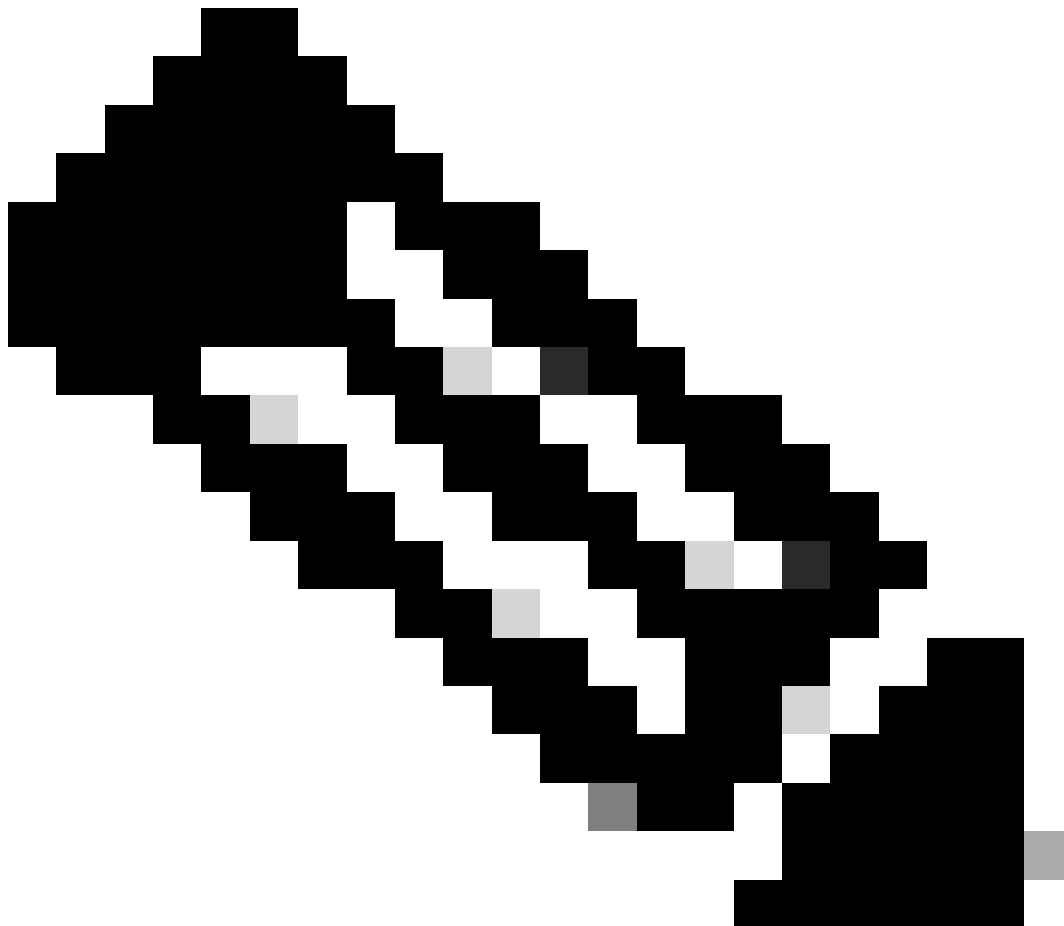
Users

Roles

Policies

Door het toegangsvak voor de AWS-beheerconsole uit te schakelen, voorkomt u dat de gebruiker zich bij de AWS-account aanmeldt via de web-UI.

6: Wijs beleid toe door het toe te wijzen aan de gebruiker, het rechtstreeks aan een groep vast te maken of het inline te configureren.



Opmerking: Voor demonstratie, wijst u direct beleid aan de gebruiker toe. Voor meer informatie - [AWS-beleid beheren](#)

7: Zoek naar S3 volledige toegang en selecteer AmazonS3full toegang, die de gebruiker volledige toegang voor elke S3 emmer die op zijn corresponderende AWS-account wordt gemaakt verleent.

8: Controleer het vakje met de beleidsnaam AmazonS3FullAccess en klik op volgende.

[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.

Q

s3full

X

Filter by Type

All types

1 match

<

1

>

⌕

☐	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)

Refresh

Remove

Add permissions

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

Q

Search

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.

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



Opmerking: U kunt meer granulair beleid maken door alleen specifieke emmer toe te staan, navigeer naar [Policy creatie](#) om uw S3 emmer beleid in json-formaat te maken.

9: Zodra de gebruiker is gemaakt, selecteert u de gebruiker en gaat u naar het tabblad Beveiligingsreferenties en klikt u op Toegangssleutel maken.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

IAM > Users

Users (16) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Search tz 1 match

☐	User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access key ID
☐		/	0	-	-	-	-	-

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: Selecteer het andere keuzerondje en voeg eventueel een tag toe.

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: Klik op Download .csv-bestand. Dit is de Access-toets in een csv-bestand en het is niet meer beschikbaar om te downloaden of te bekijken zodra u weg van deze pagina navigeert.

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.

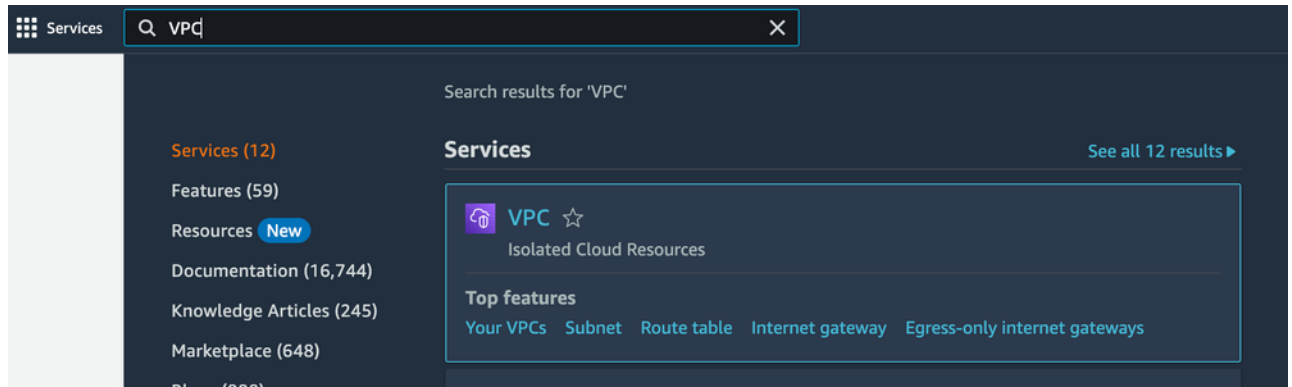
For more details about managing access keys, see the [best practices for managing AWS access keys](#).

Download .csv file
Done

AWS-IAM

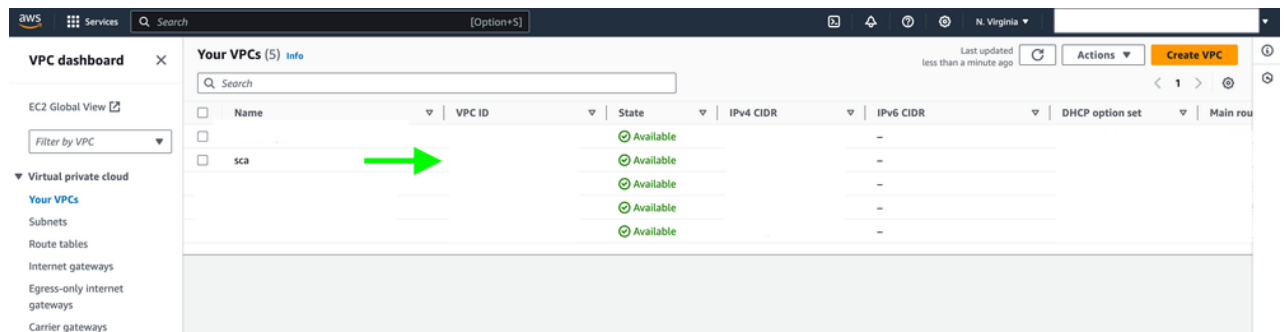
Stap 3. VPC Flow Logs configureren

1: Start uw VPC op uw gewenste regio en navigeer naar uw VPC-optie.



AWS-Flow-logs

2: Selecteer uw VPC in de lijst op het scherm.



AWS-Flow-logs



Opmerking: U hebt in deze demo de naam SCA van VPC geselecteerd.

3: Navigeer naar uw VPCs onder Virtual Private Cloud, switch naar het tabblad Flow logs en klik op Create flow logs.

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 > Your VPCs > vpc-60bdda1d / sca Actions ▾

Details Info

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

Resource map | CIDRs | **Flow logs** | Tags | Integrations

Flow logs (4) Info Actions ▾ **Create flow log**

Q Search

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

AWS-Flow-logs

4: Geef uw flow logboeken een naam en deel de S3 emmer ARN eerder gemaakt.



Opmerking: Zie S3-emmer configureren voor ARN - Stap 6

5: U hebt een optie om te gaan met AWS standaard logindeling of aangepaste logindeling te maken voor het geval er meer velden nodig zijn.

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

AWS-Flow-logs

7: Klik op Stroomlogboeken maken.

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

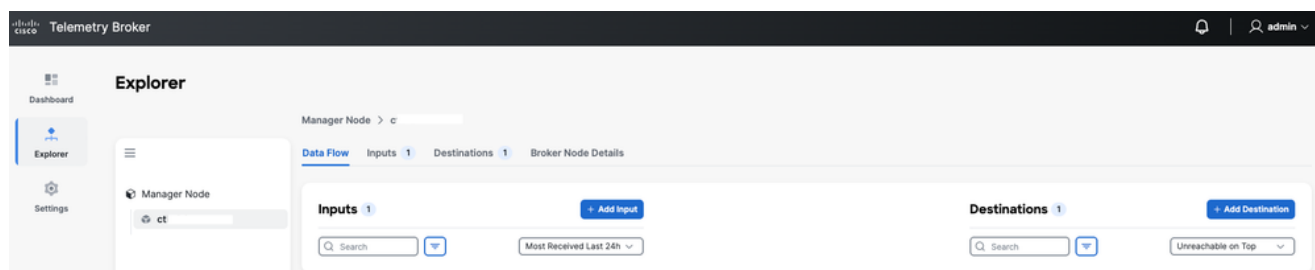
You can add 49 more tags

↓

AWS-Flow-logs

Step 4. Configureer VPC Invoer naar CTB

1: Toegang tot CTB Web UI, navigeer naar Explorer> Broker knooppunt tabblad > klik op open broker node >Data Flowtab > Klik op Add Input.



CTB-Input-UI

2: Selecteer het type ingangssignaal als AWS VPC Flow-logbestand en klik op volgende.

Add Input



Select Input type

Type or Select Input ^

UDP Input

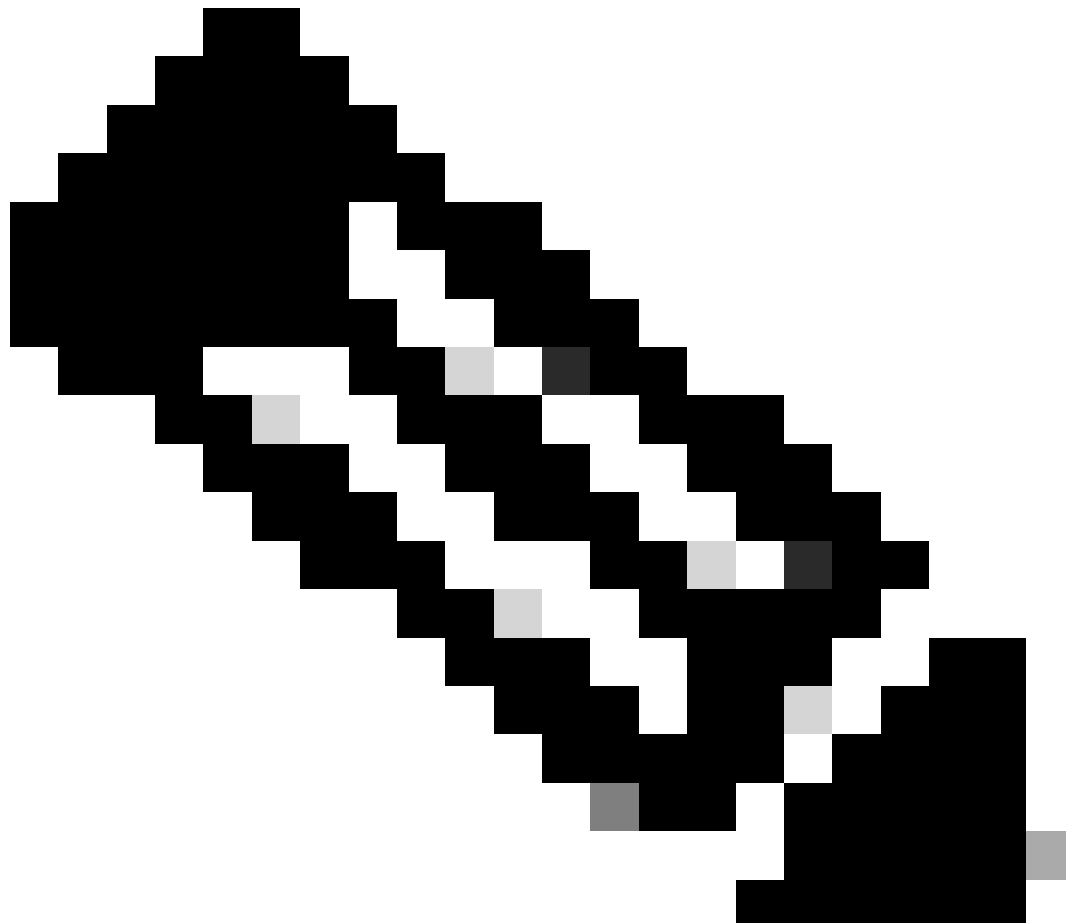
AWS VPC Flow log

Azure NSG Flow log

Flow Generator Input

AWS VPC Flow log

: elk IP-adres dat is ingesteld als het Input IP-adres (uniek IP dat niet door een andere exporteur wordt gedeeld) wordt gerapporteerd als de exporteur voor de getransformeerde netflow-gegevens.



Opmerking: Zie IAM-gebruiker configureren voor toegangssleutel met S3-toegangsbeleid, stap 9 voor AWS Access Key ID

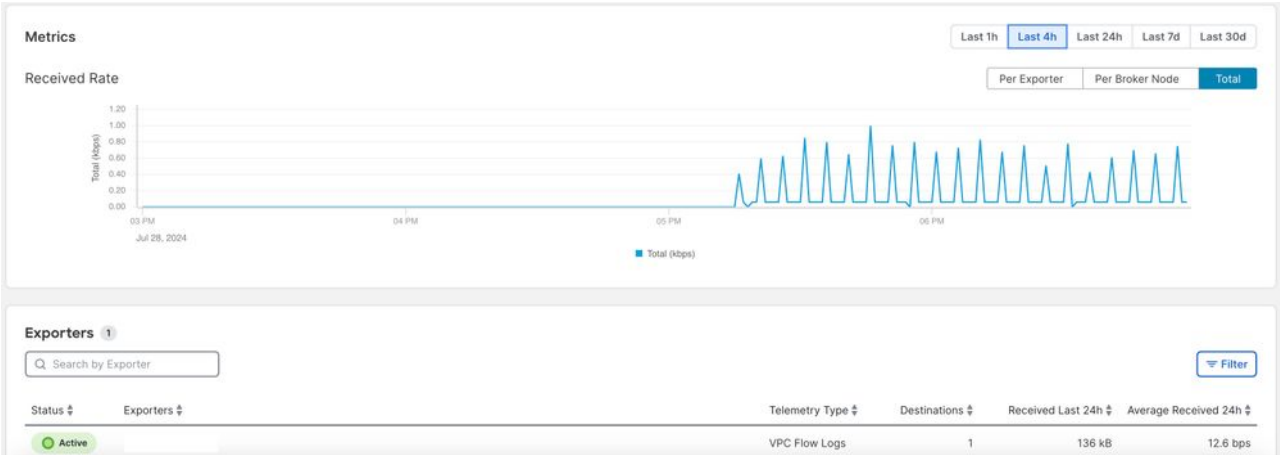
Verifiëren

Na enkele minuten van de configuratie van de AWS VPC-ingang wordt de statuskolom actief als de AWS S3-emmer gegevens bevat.

Controleer de status van de AWS VPC-input met deze stappen.

1: Log in op CTB UI en navigeer naar **Verkenner > tabblad Broker > klik op openbroker node > tabblad switch toInput > Klik op AWS-ingang openen.**

2: Controleer dat de geconfigureerde ws-flow logs actieve status hebben en ontvangen metriek hebben stijgende grafiek.



CTB-Input-UI

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.