

Configurar os logs de fluxo do AWS VPC para entrada CTB

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configuration Steps](#)

[Etapa 1. Configurar o bucket do S3 no AWS](#)

[Etapa 2. Criar Usuário do IAM com Chave de Acesso e Anexar Política de Compartimento S3](#)

[Etapa 3. Configurar os logs de fluxo do VPC](#)

[Etapa 4. Configurar a entrada VPC para CTB](#)

[Verificar](#)

Introdução

Este documento descreve como configurar os Logs de fluxo do VPC como uma entrada para o Cisco Telemetry Broker (CTB).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Amazon Web Services (AWS)
- Administração CTB.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

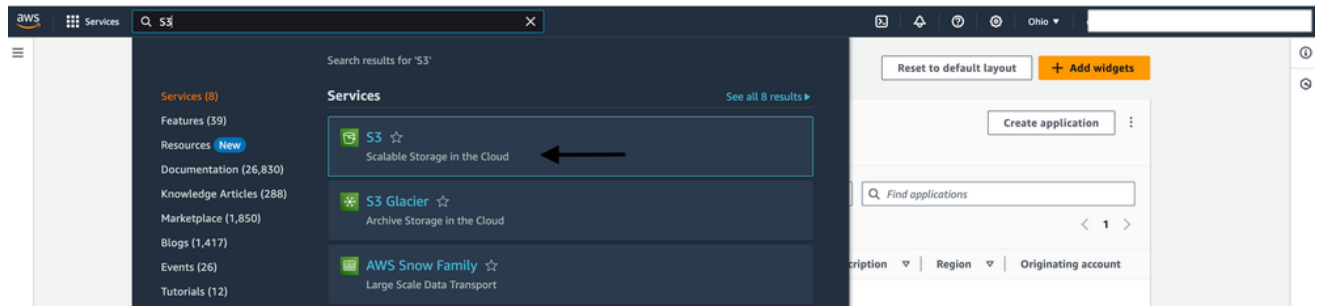
- CTB (v2.2.1+)
- AWS

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configuration Steps

Etapa 1. Configurar o bucket do S3 no AWS

- 1: Faça login no console de gerenciamento AWS com nome de usuário e senha.
- 2: Certifique-se de fazer login na região apropriada.
- 3: Navegue até a barra de pesquisa e digite S3.

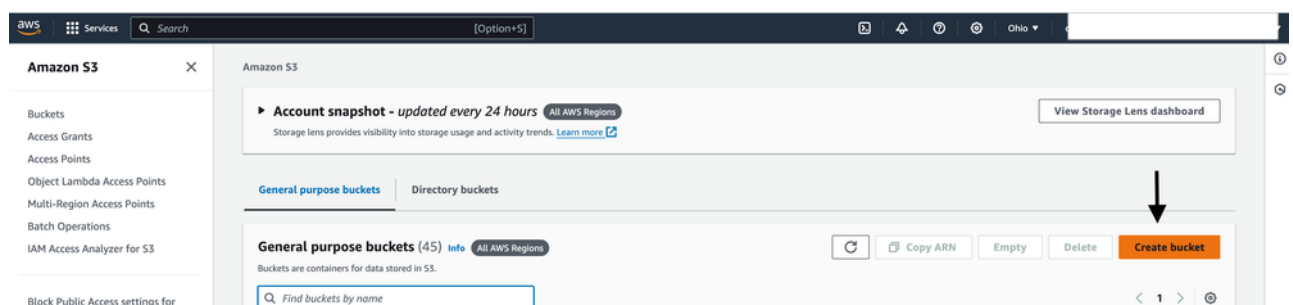


AWS-Dashboard



Note: Na demonstração, você selecionou a região de Ohio com a zona de disponibilidade us-east-2, que fica visível ao lado do ícone de engrenagem.

4: Clique em criar bucket.



AWS-S3

5: Dê um nome ao bucket e deixe todas as opções como estão e clique em criar.

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 : Depois que o bucket for criado com êxito, salve o bucket ARN que será usado posteriormente durante a configuração.

 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](#)

Storage lens provides visibility into storage usage and activity trends. [Learn more](#)

[View Storage Lens dashboard](#)

[General purpose buckets](#) | [Directory buckets](#)

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

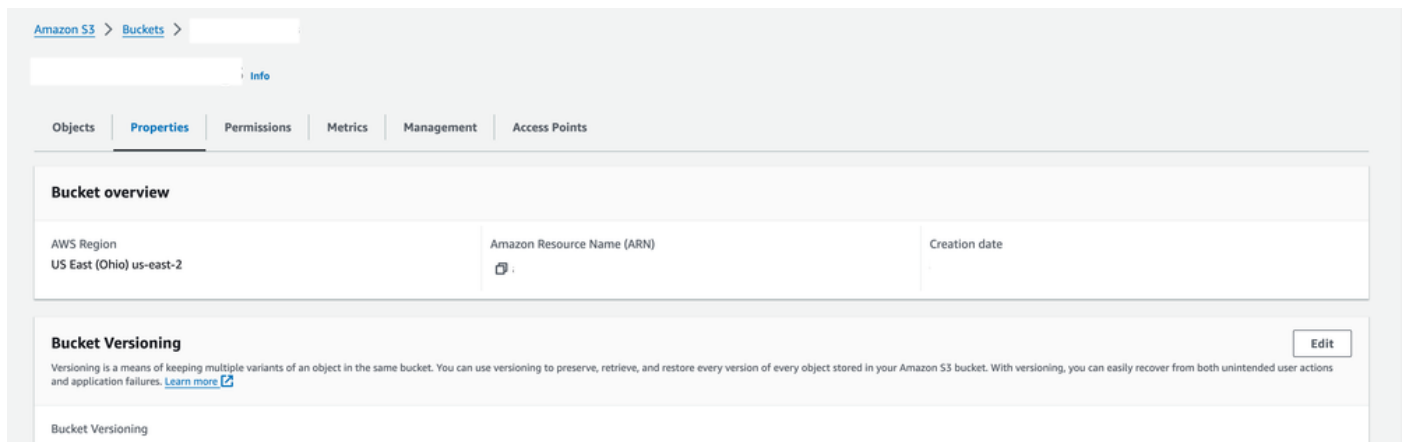
Buckets are containers for data stored in S3.

 1 match

  Copy ARN  Empty  Delete  Create bucket

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

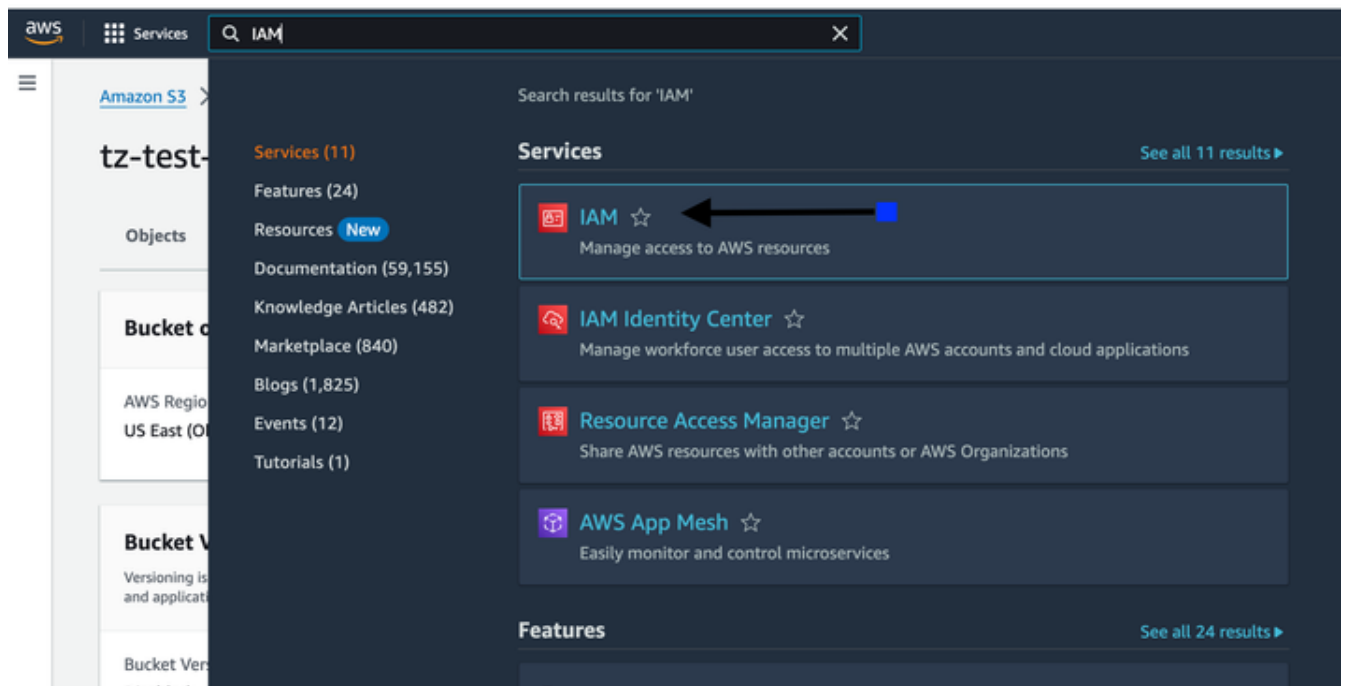
AWS-S3



AWS-S3

Etapa 2. Criar Usuário do IAM com Chave de Acesso e Anexar Política de Compartimento S3

1: Inicie o IAM na barra de pesquisa do aws.



AWS-IAM

2: Navegue até usuários.



Services



Search

Identity and Access Management (IAM)



Search IAM

Dashboard

▼ Access management

User groups

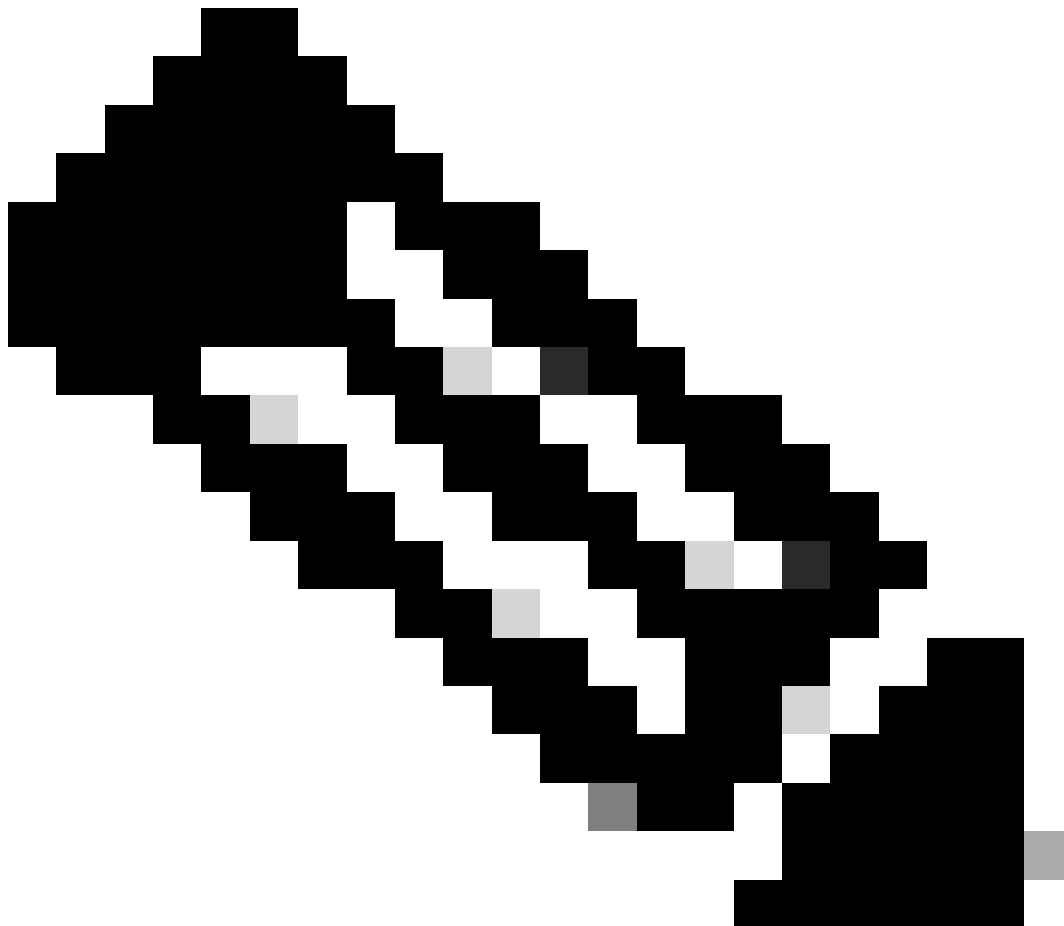
Users

Roles

Policies

: Ao desmarcar a caixa de acesso do console de gerenciamento do AWS, ele impede que o usuário faça login na conta do AWS usando a interface do usuário da Web.

6: Atribua a política atribuindo-a ao usuário, conectando-a diretamente a um grupo ou configurando-a em linha.



Note: Para demonstração, você atribui uma política diretamente ao usuário. Para obter mais informações - [Gerenciamento de políticas AWS](#)

7 : Procure o acesso completo S3 e selecione o acesso AmazonS3full, que permite que o usuário tenha acesso total para cada compartimento de memória S3 criado em sua conta AWS correspondente.

8 : Marque a caixa com o nome de política AmazonS3FullAccess e clique em 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-
3-
4-
5-
6-
7-
8-
9-
10-
11-
12-
13-
}

```
"Version": "2012-10-17",
"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "s3:*",
      "s3-object-lambda:*"
    ],
    "Resource": "*"
  }
]
```

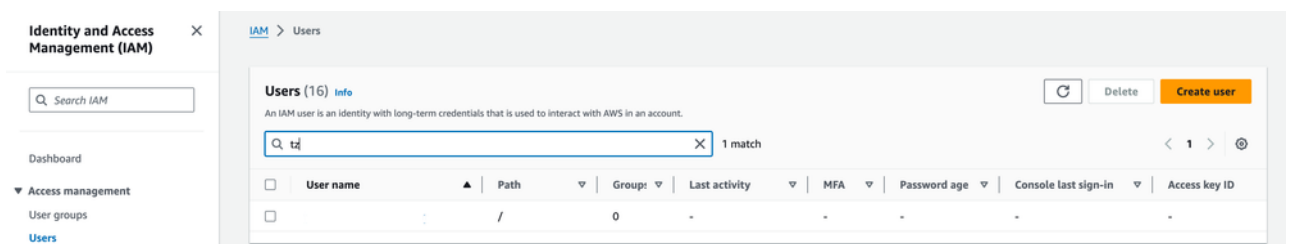
Copy JSON

AWS-IAM



Note: Você pode criar uma política mais granular, permitindo apenas um bucket específico também. Navegue até [Criação de política](#) para criar sua política de bucket S3 no formato json.

9 : Depois que o usuário for criado, liste o usuário, navegue até a guia credencial de segurança e clique em criar chave de acesso.



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 : Selecione o botão de opção other e, opcionalmente, adicione uma 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: Clique em Baixar arquivo .csv. Esta é a chave de acesso em um arquivo csv e não está mais disponível para download ou exibição quando você sair desta 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 > > 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.

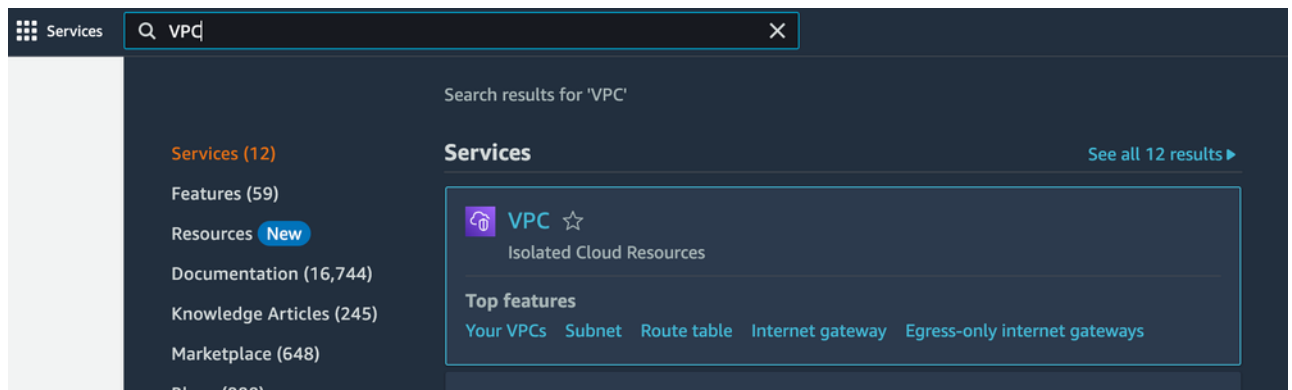
For more details about managing access keys, see the [best practices for managing AWS access keys](#).

Download .csv file
Done

AWS-IAM

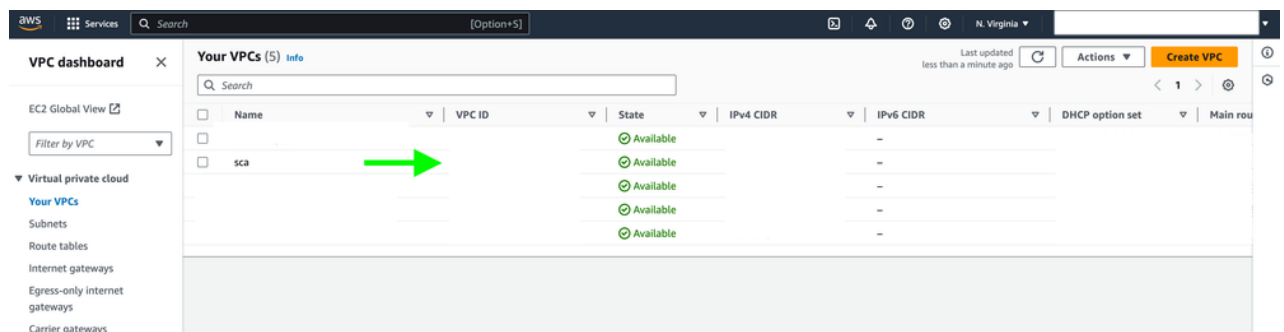
Etapa 3. Configurar os logs de fluxo do VPC

1: Inicie o VPC na região desejada e navegue até a opção Seu VPC.



AWS-Flow-Logs

2: Seleccione seu VPC na lista exibida na tela.



AWS-Flow-Logs



Note: Você selecionou o nome SCA do VPC nesta demonstração.

3: Navegue até Seus VPCs em Nuvem privada virtual, alterne para a guia Logs de fluxo e clique em Criar Logs de fluxo.

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 	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 < 1 >

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

AWS-Flow-Logs

4: Dê um nome aos registros de fluxo e compartilhe o ARN de bucket S3 criado anteriormente.



Note: Para ARN, consulte Configurar bucket de S3 - Etapa 6

5: Você tem a opção de usar o formato de log padrão do AWS ou criar um formato de log personalizado caso mais campos sejam necessários.

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 : Clique em criar logs de fluxo.

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

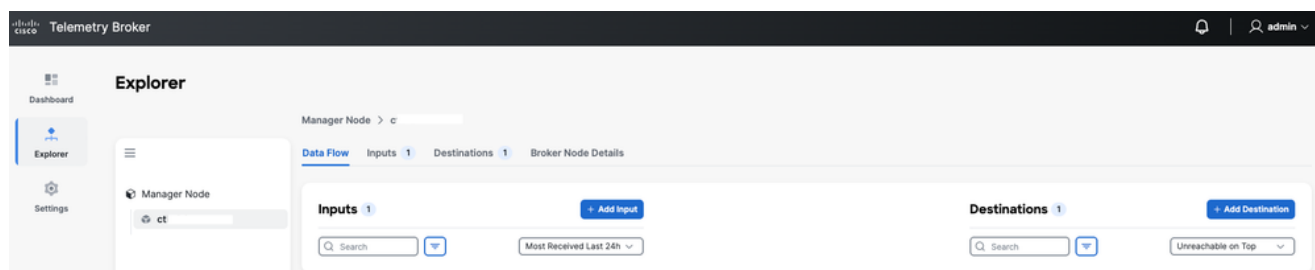
You can add 49 more tags

↓

AWS-Flow-Logs

Etapa 4. Configurar a entrada VPC para CTB

1: Acessar a interface de usuário da Web do CTB, navegue para o Explorer> guia do nó do agente > clique em abrir nó do agente >guia Fluxo de dados > Clique em Adicionar entrada.



CTB-Input-UI

2: Selecione o tipo de entrada como AWS VPC Flow log e clique em next.

Add Input



Select Input type

Type or Select Input ^

UDP Input

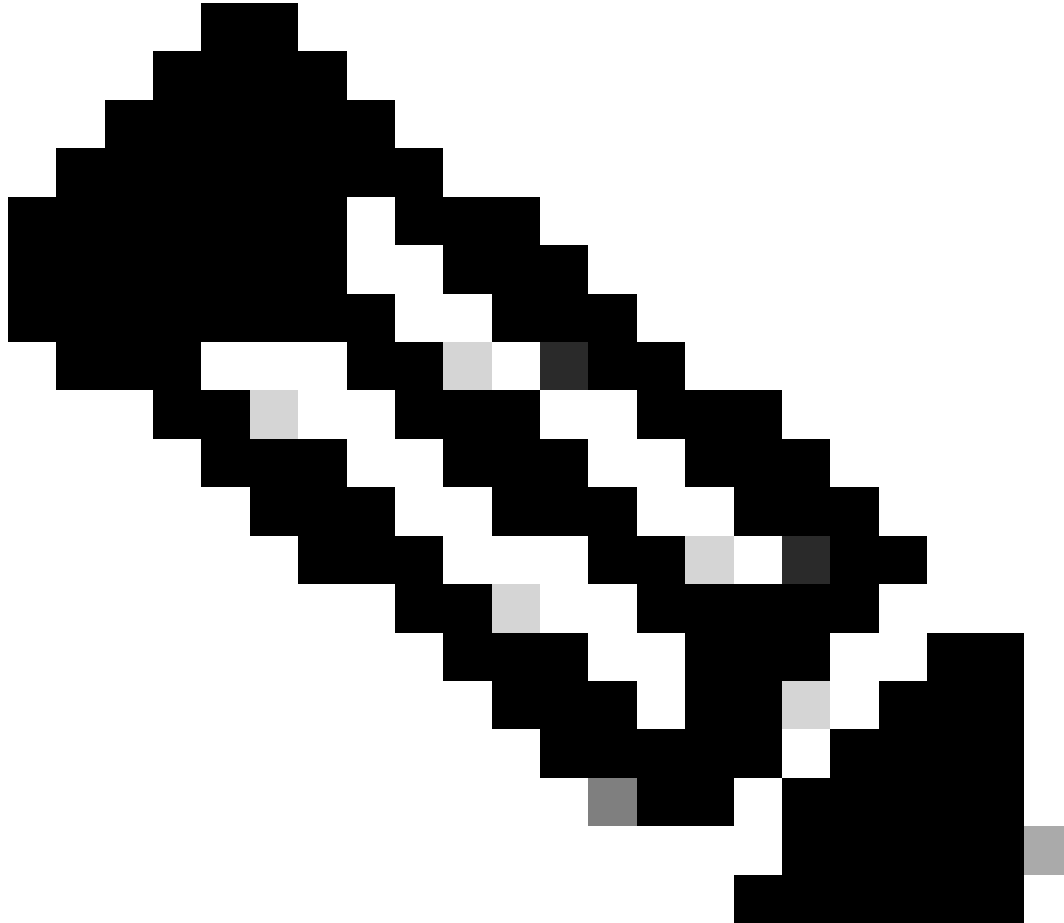
AWS VPC Flow log

Azure NSG Flow log

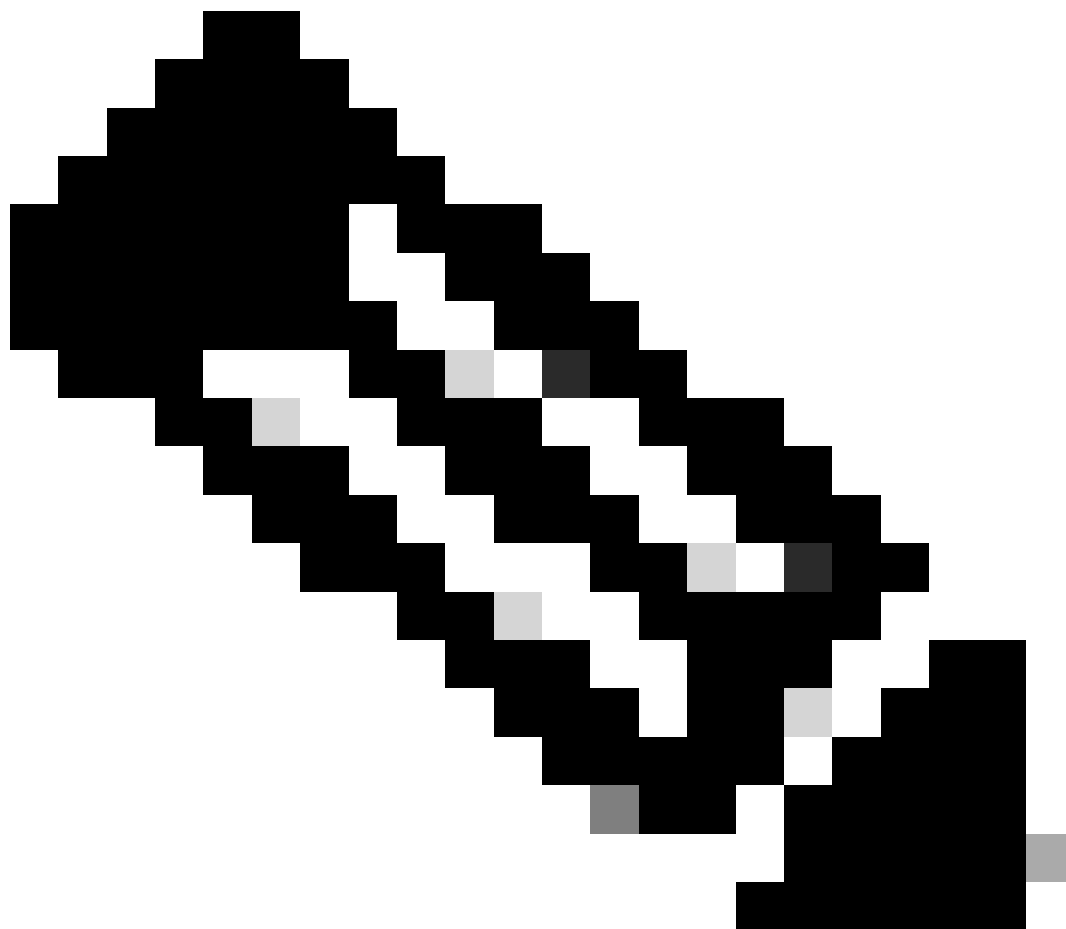
Flow Generator Input

AWS VPC Flow log

: Para obter o código da região, consulte a página inicial do AWS ao lado do ícone de engrenagem.



Observação: qualquer endereço IP configurado como o endereço IP de entrada (IP exclusivo não compartilhado por nenhum outro exportador) é informado como o exportador para os dados de netflow transformados.



Note: Para o ID da Chave de Acesso do AWS, consulte Configurar o usuário do IAM para a chave de acesso com a política de acesso S3, etapa 9

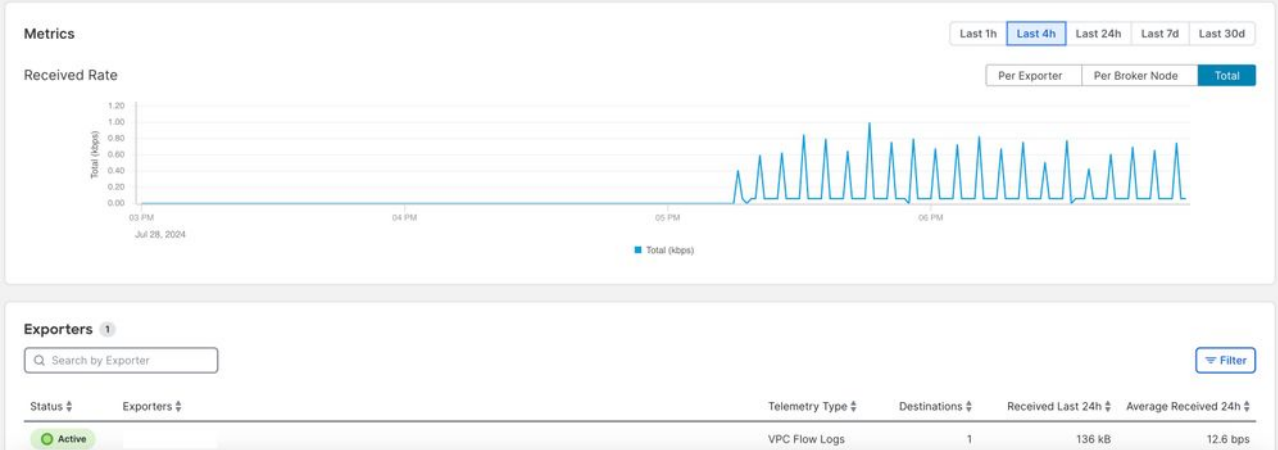
Verificar

Após alguns minutos de configuração da entrada do AWS VPC, a coluna de status se tornará ativa se o bucket do AWS S3 tiver dados nele.

Verifique o status da entrada AWS VPC usando estas etapas.

1: Faça login na interface do usuário do CTB e navegue para Explorer > guia do nó Broker > clique no nó openbroker > guia Switch para Input > Clique em abrir entrada AWS.

2: Verifique se os logs aws-flow configurados têm status ativo e se a métrica recebida tem gráfico crescente.



CTB-Input-UI

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.