# Configurar os logs de fluxo do AWS VPC para entrada CTB

## Contents



## 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.

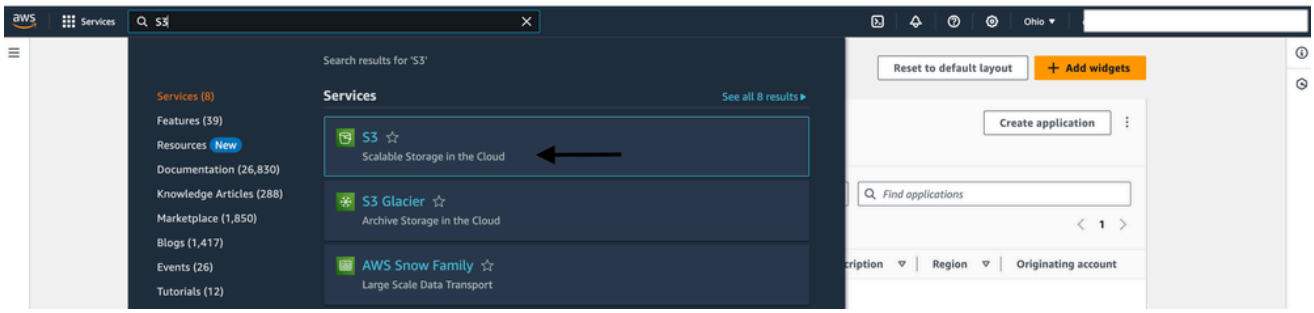
# Configuration Steps

## Etapa 1. Configurar o bucket do S3 no AWS

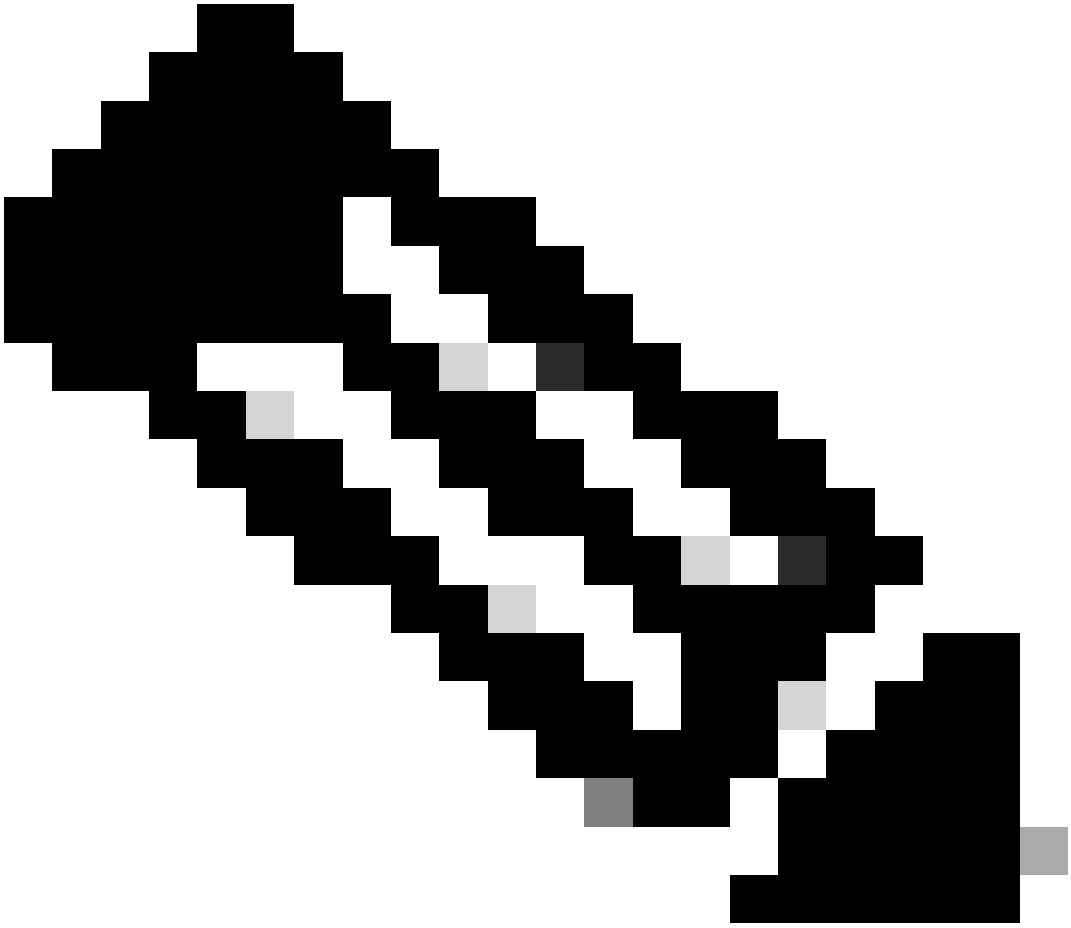
1: Faça login no console de gerenciamento AWS com nome de usuário e senha.

2: Certifique-se de fazer login na região apropriada.

3: Navegue até a barra de pesquisa e digite S3.



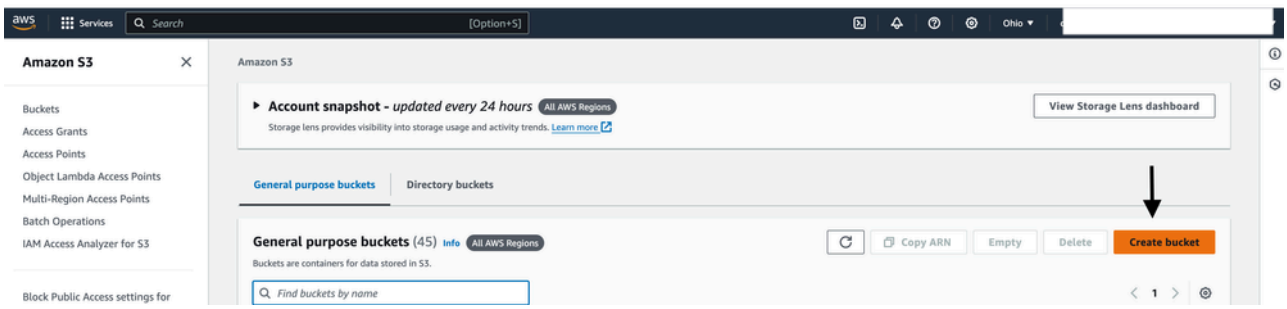

AWS-Dashboard



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.

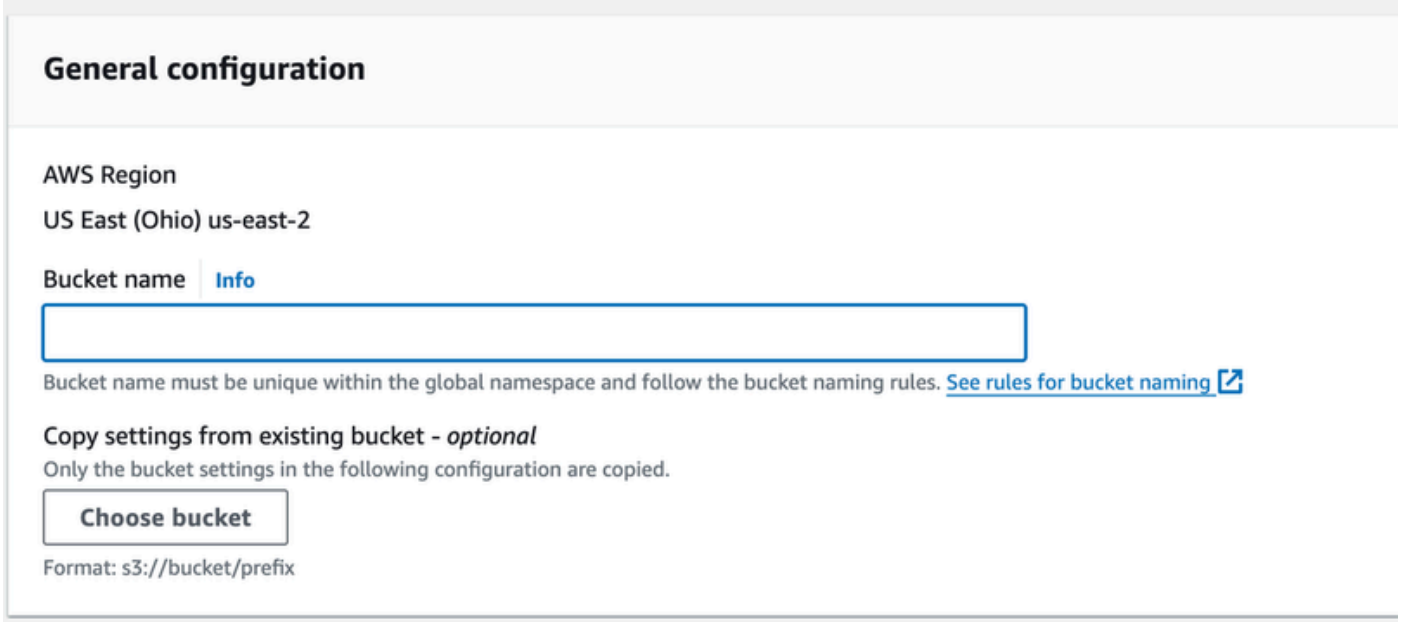
---

4: Clique em criar bucket.

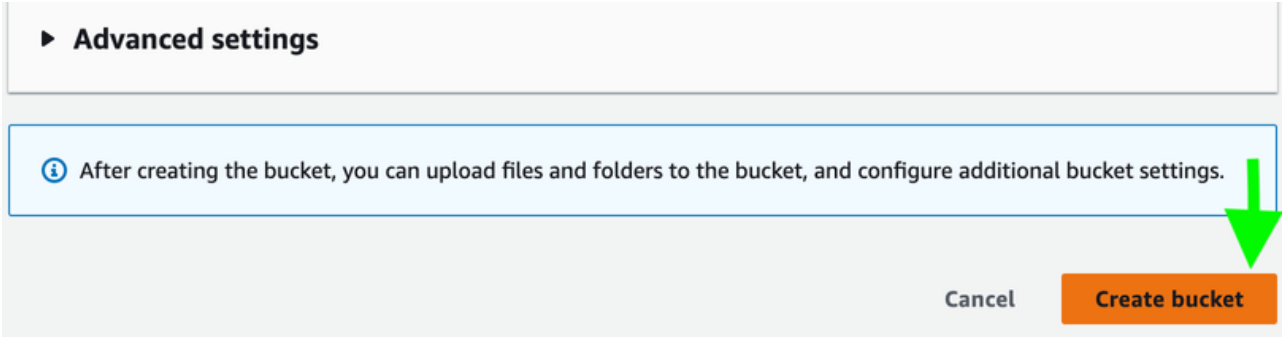



AWS-S3

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

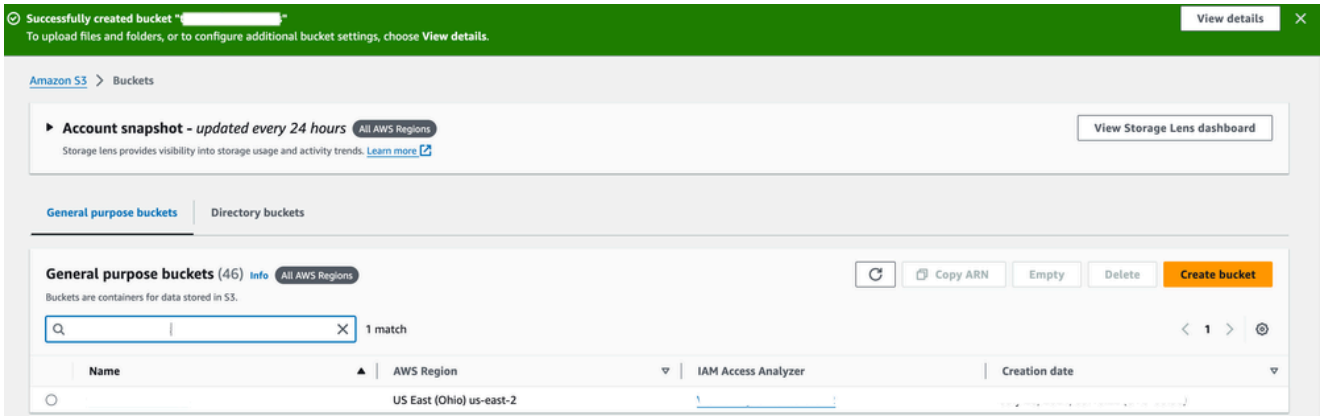



AWS-S3

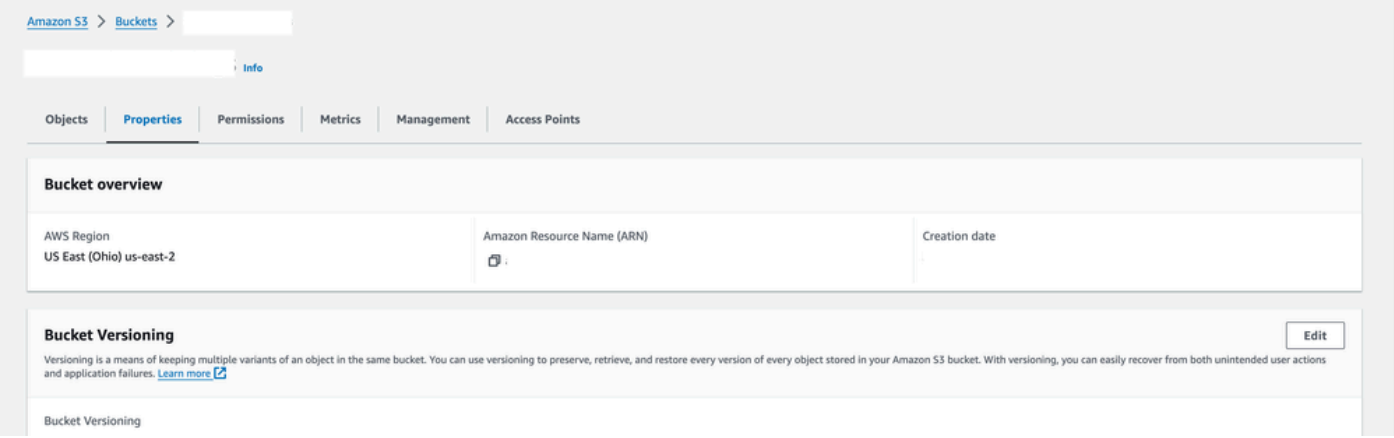



AWS-S3

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



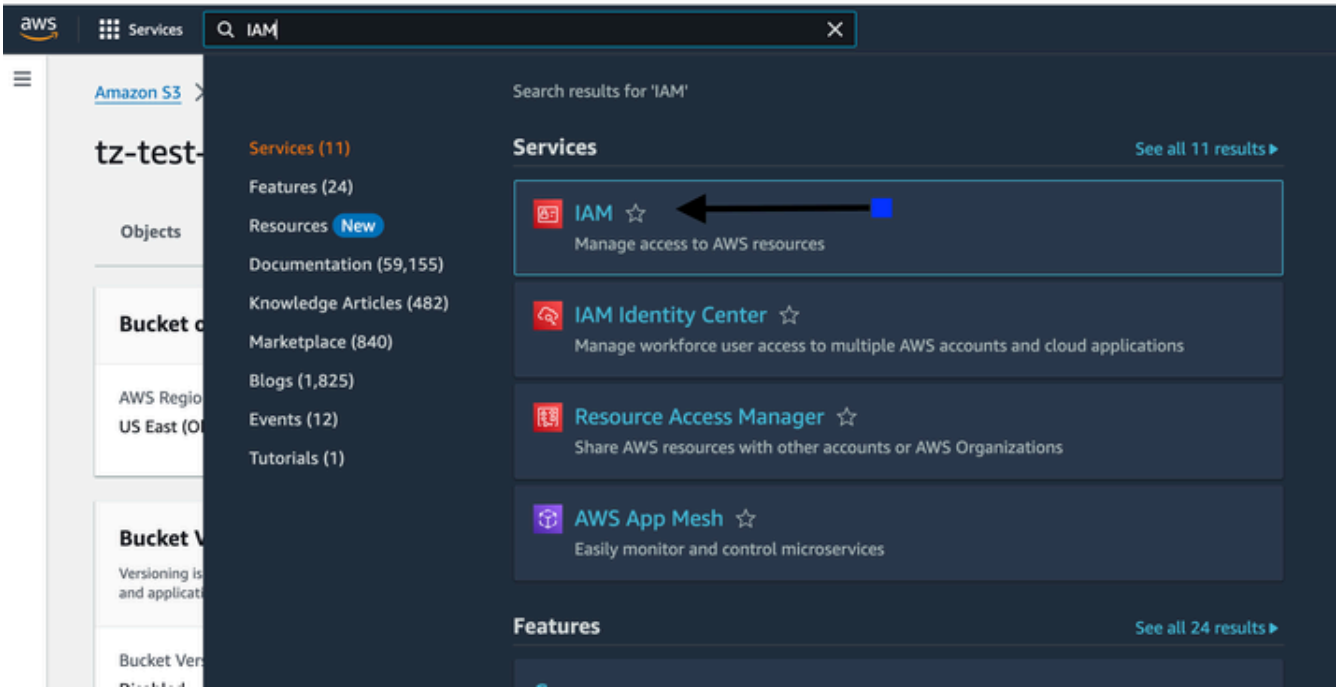

AWS-S3




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.


# Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

Roles

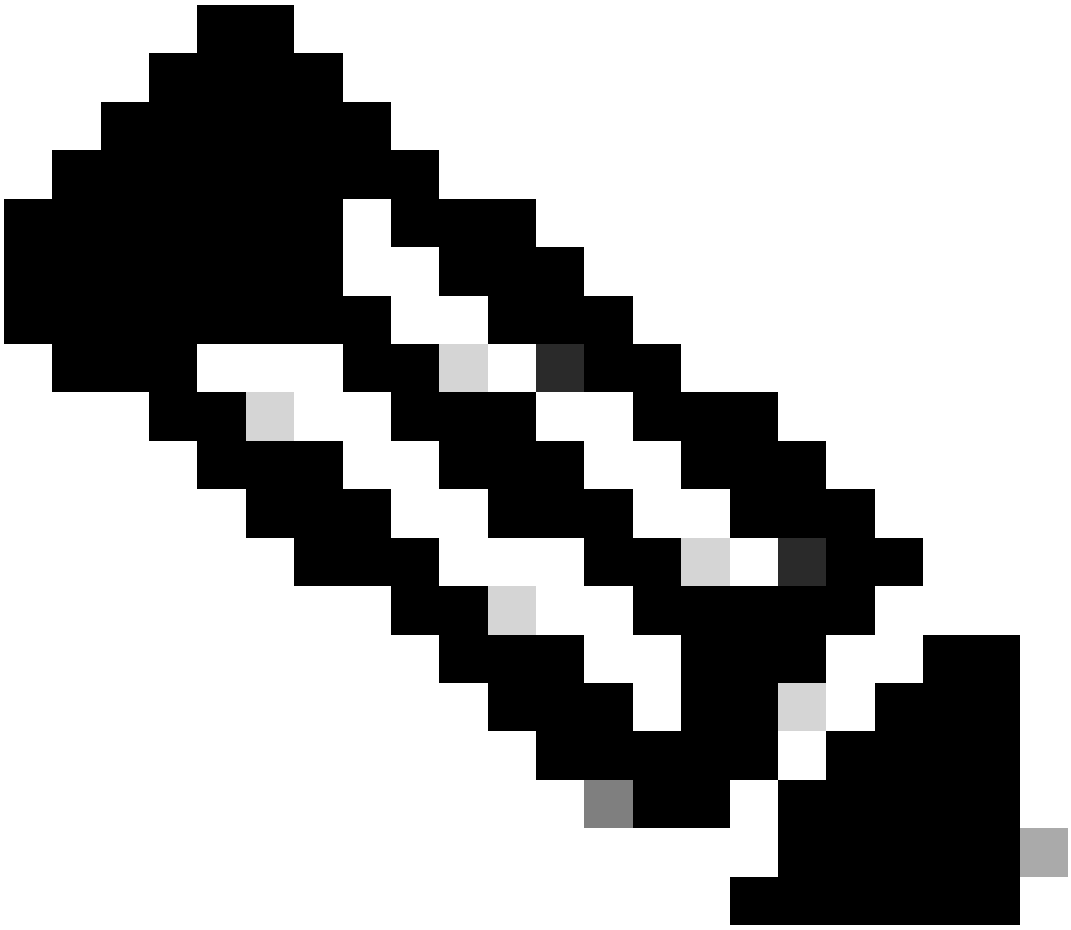
Policies

: 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.

---

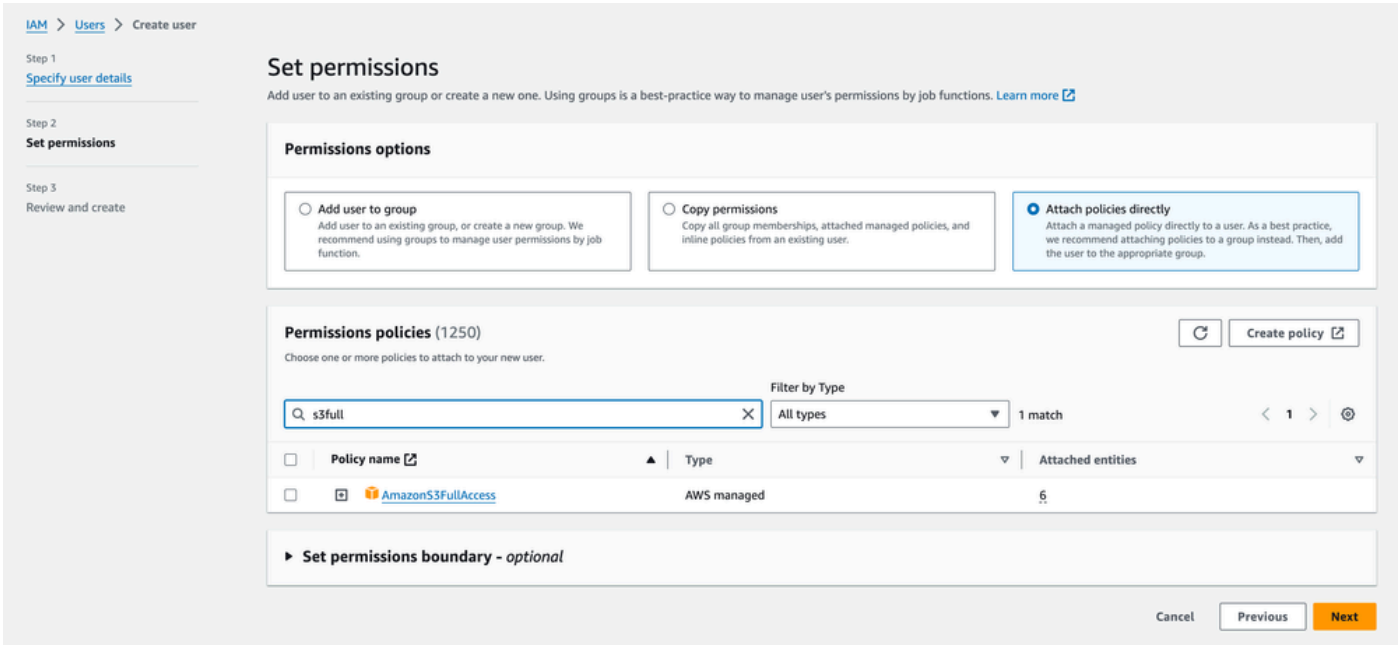


Note: Para demonstração, você atribui uma política diretamente ao usuário. Para obter mais informações - Gerenciamento de políticas AWS

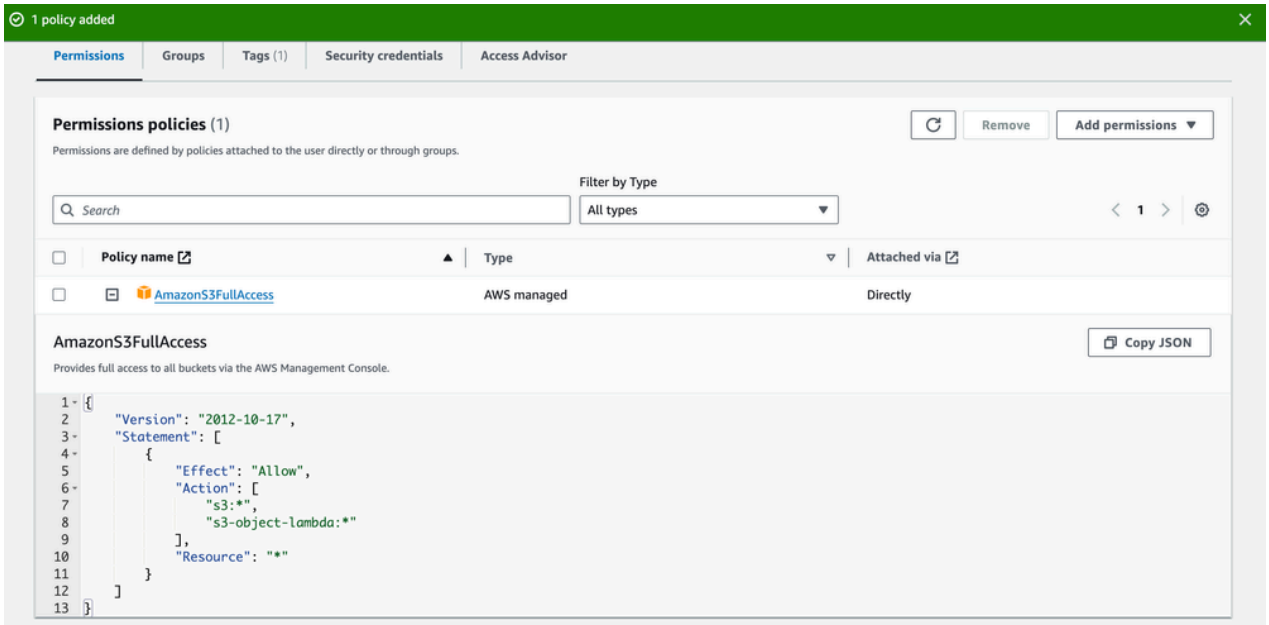
---

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.

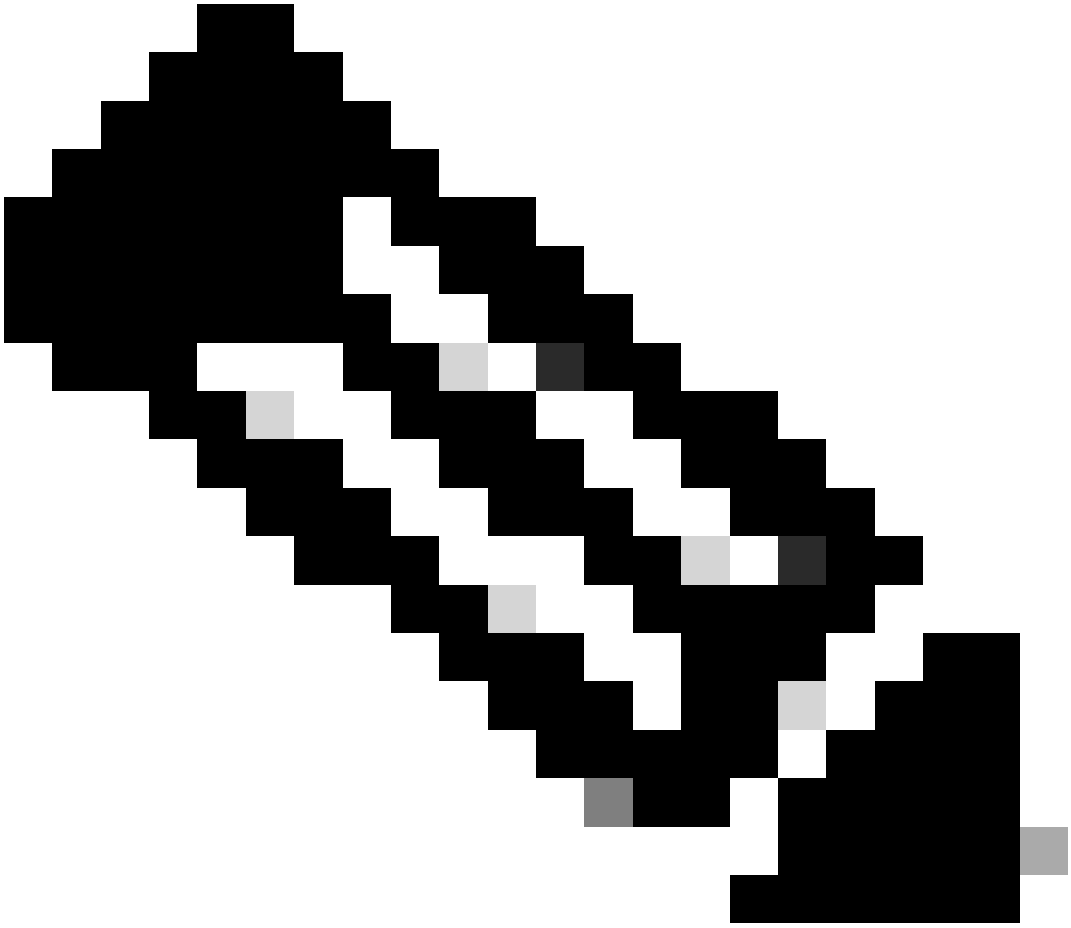
8 : Marque a caixa com o nome de política AmazonS3FullAccess e clique em Next.




AWS-IAM



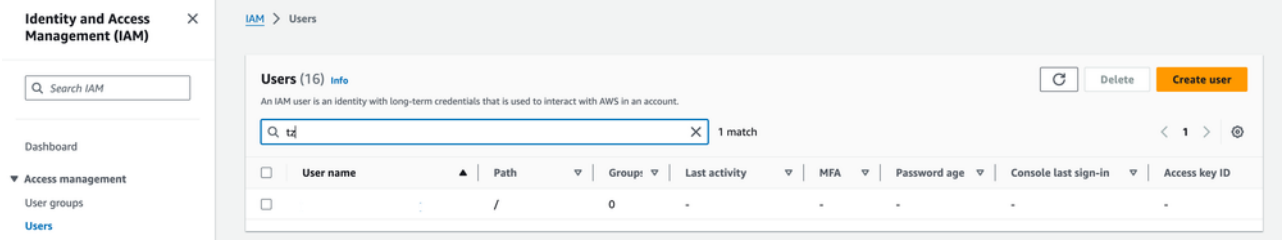

AWS-IAM



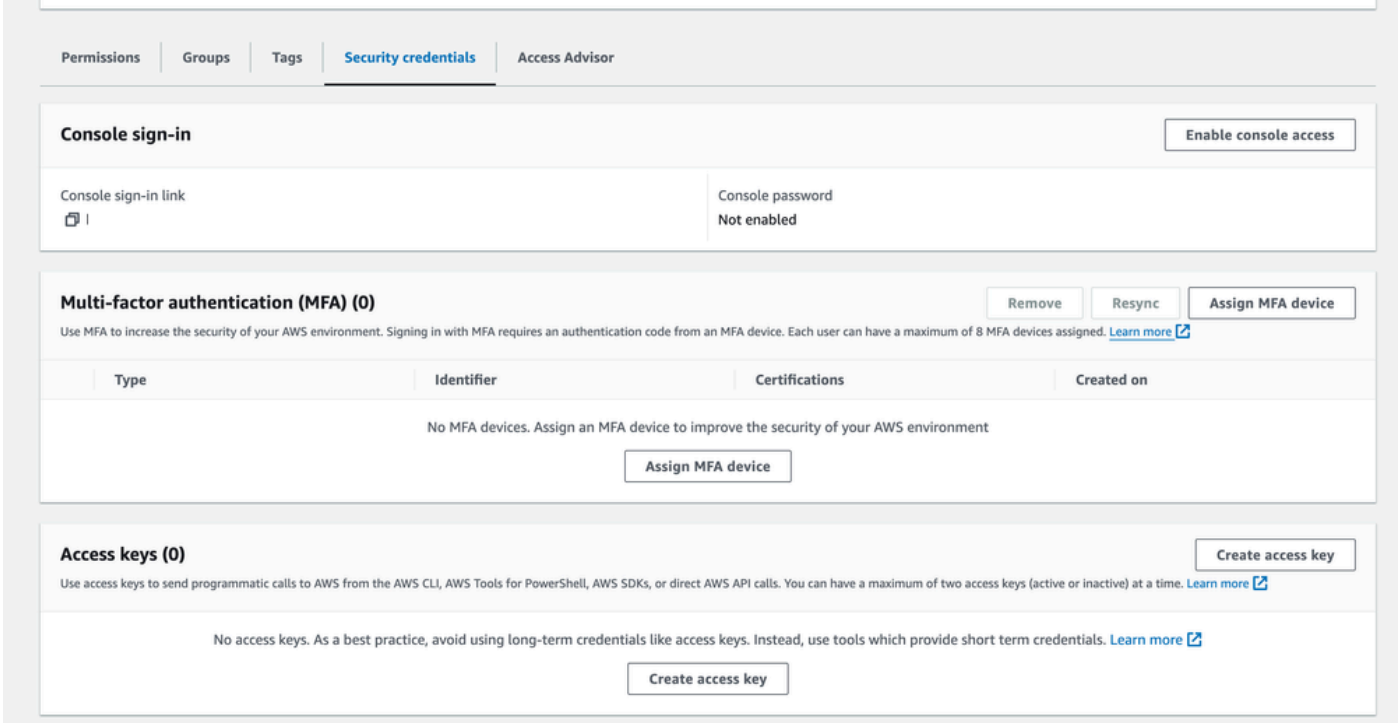
Note: Você pode criar uma política mais granular, permitindo apenas um bucket específico também. Navegue até Criação de política para criar sua política de bucket S3 no formato json.

---

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

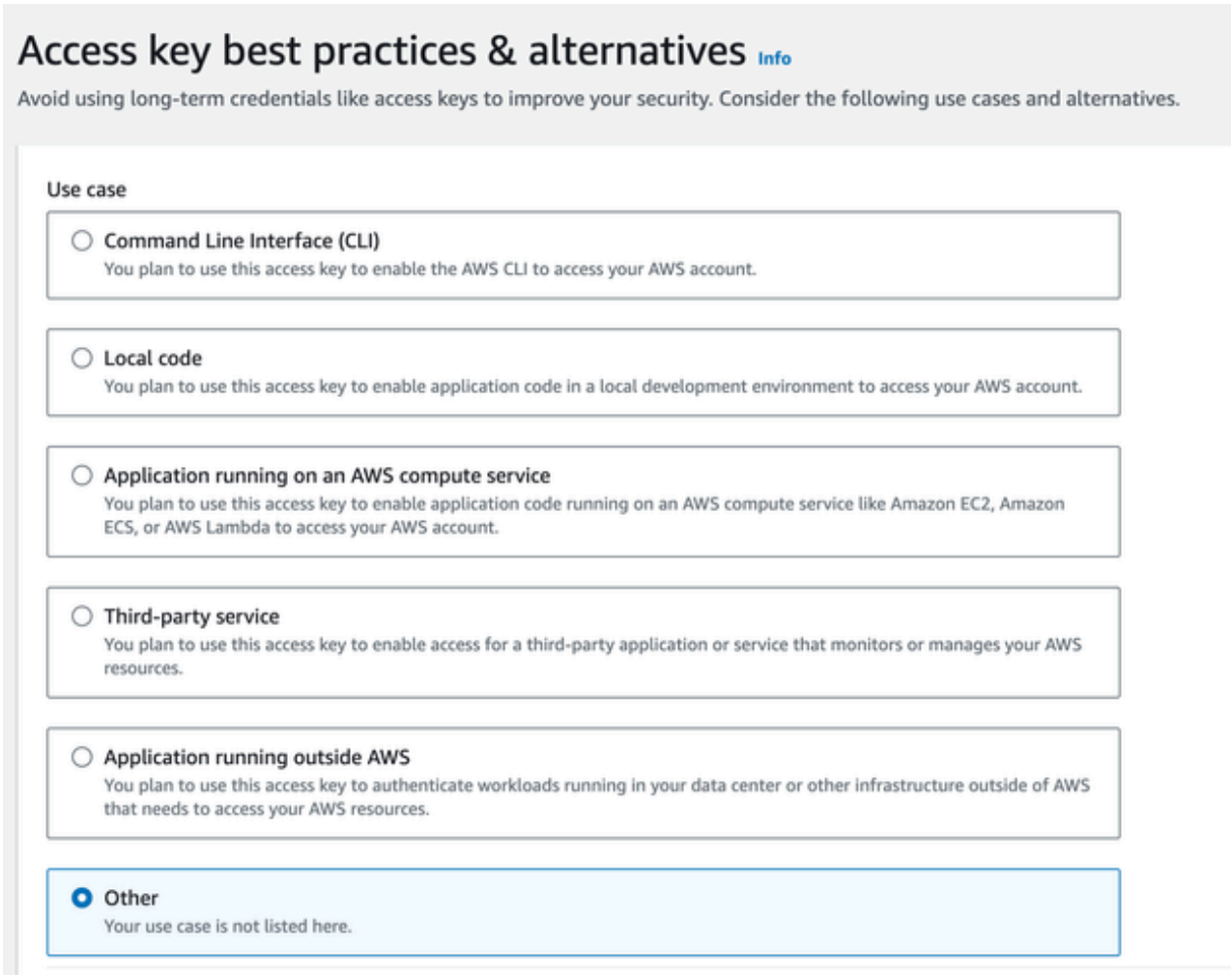



AWS-IAM

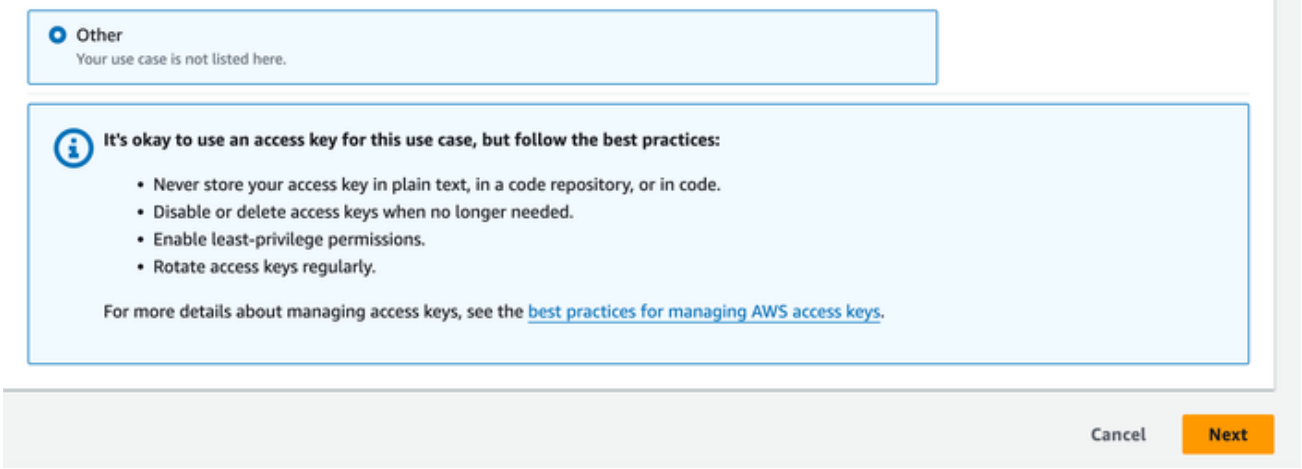



AWS-IAM

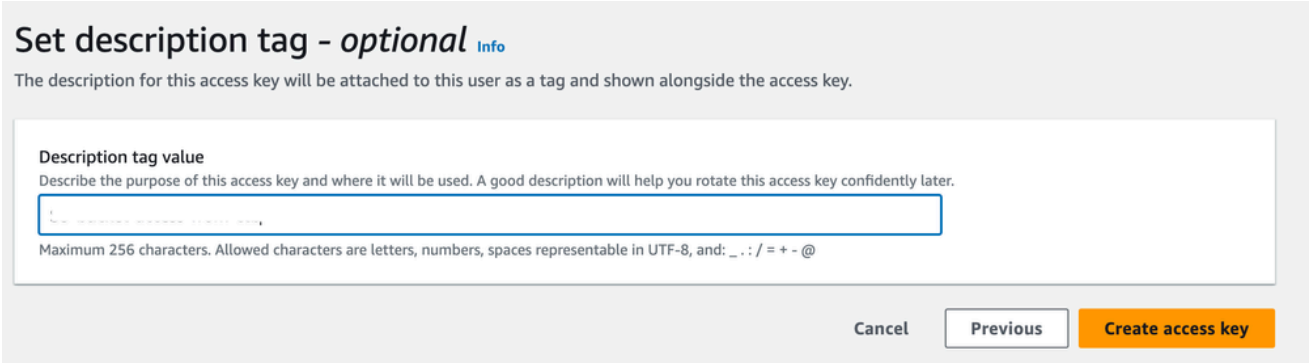
10 : Selecione o botão de opção other e, opcionalmente, adicione uma tag.




AWS-IAM

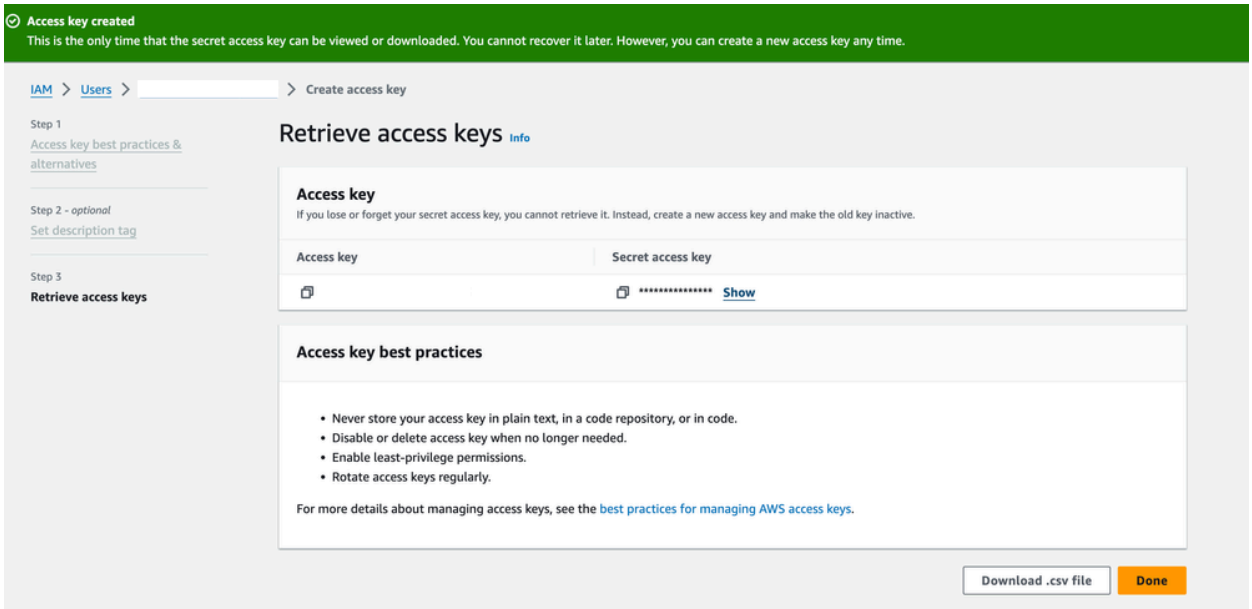



AWS-IAM




AWS-IAM

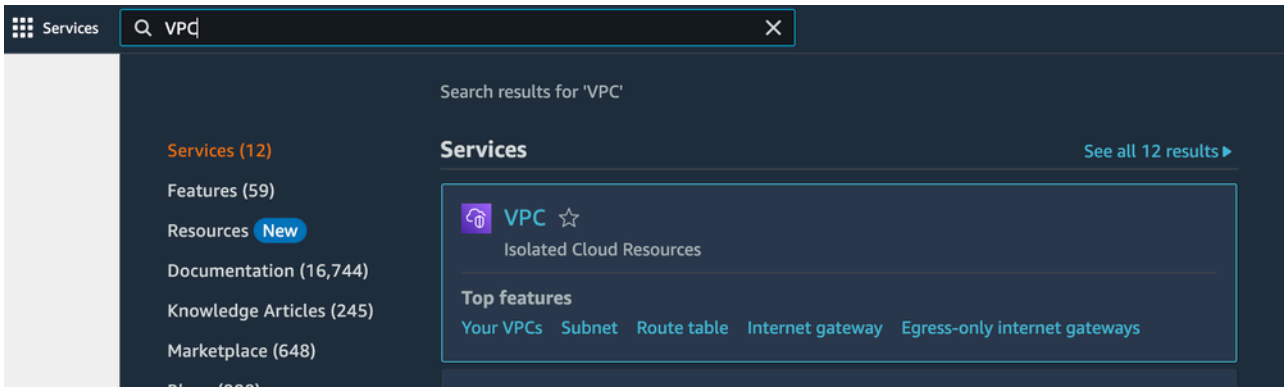
11: Clique em Baixar arquivo .csv. Esta é a chave de acesso em um arquivo csv e não está mais disponível para download ou exibição quando você sair desta página.




AWS-IAM

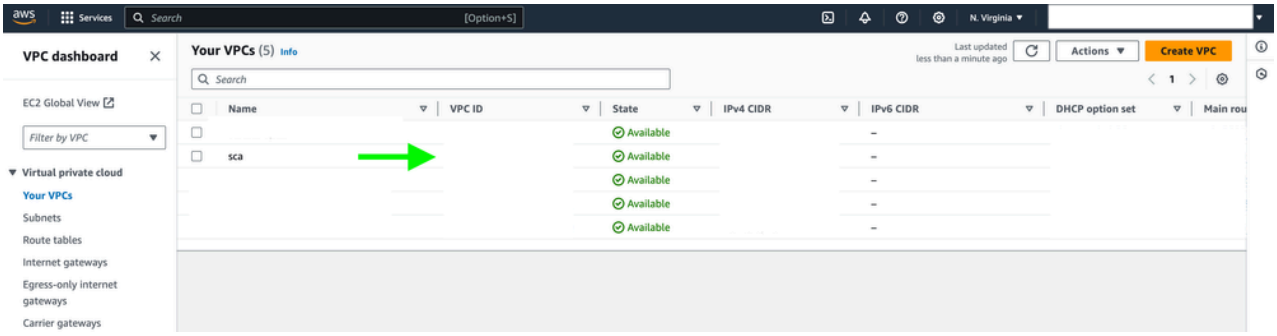
## Etapa 3. Configurar os logs de fluxo do VPC

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

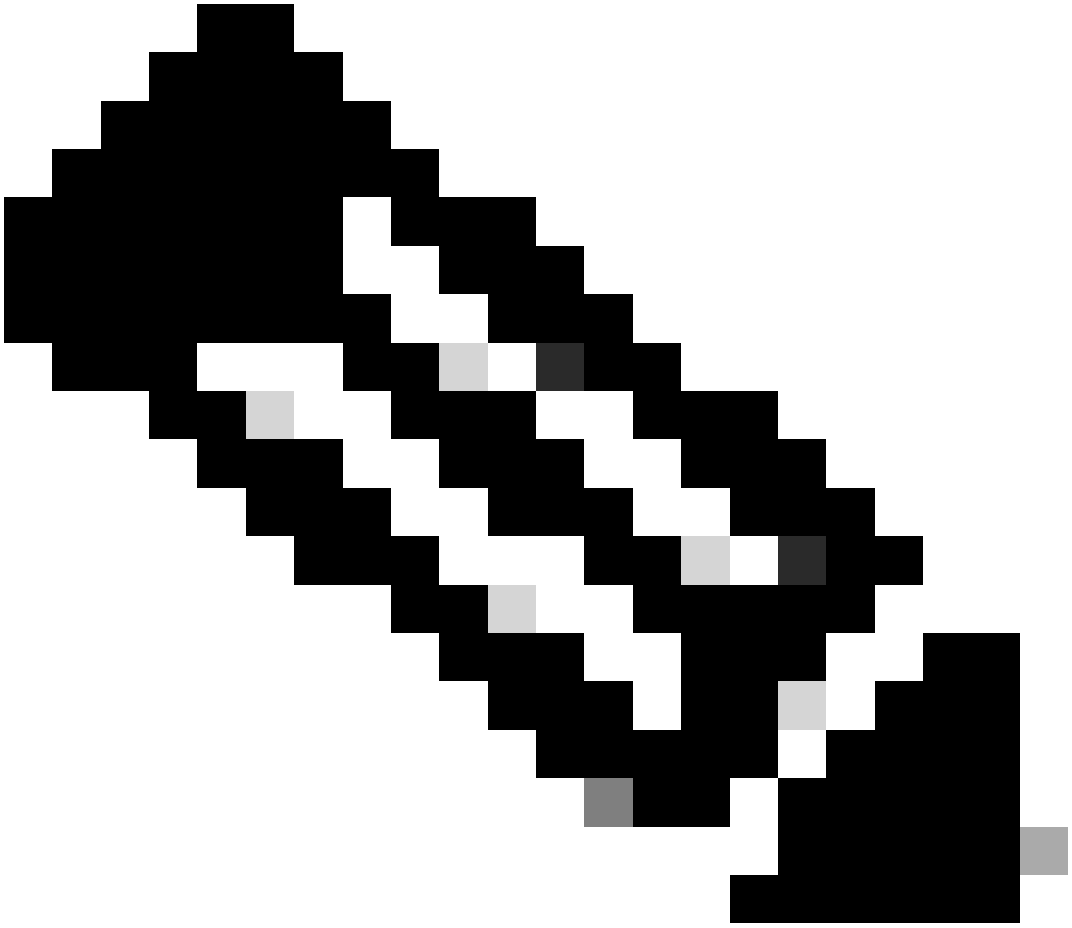



AWS-Flow-Logs

2: Selecione seu VPC na lista exibida na tela.

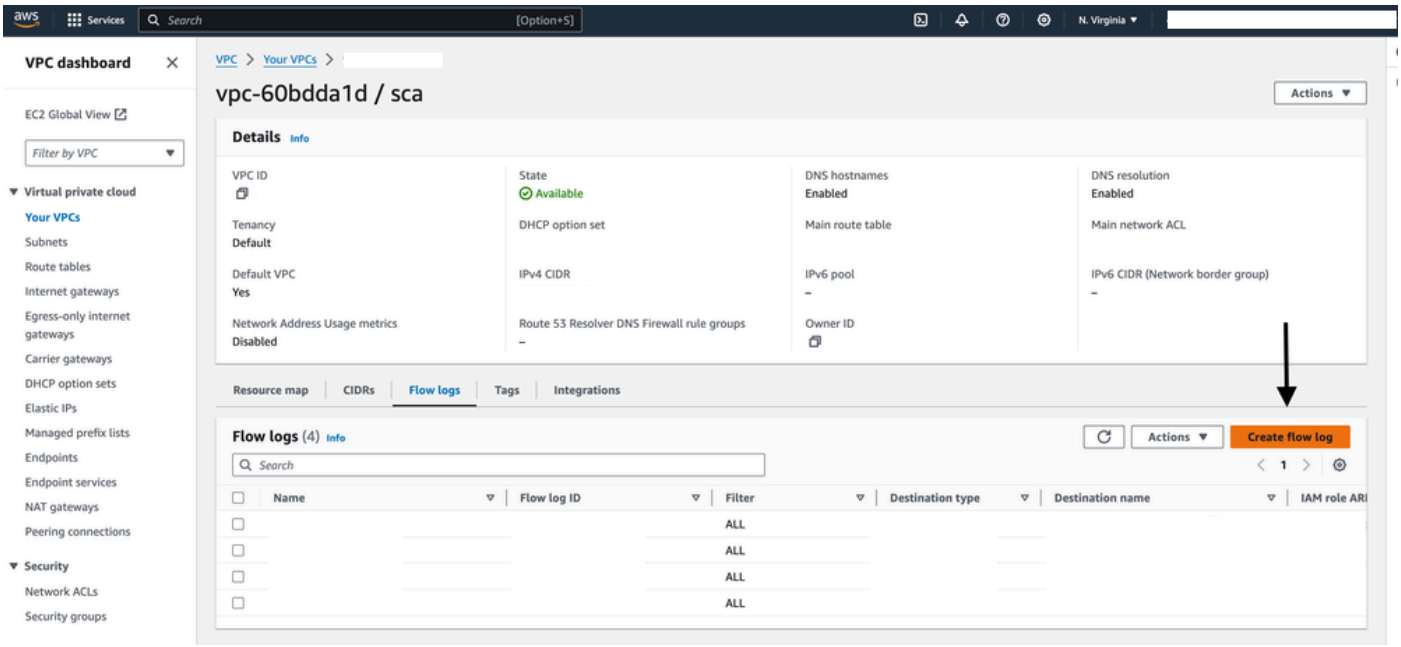



AWS-Flow-Logs



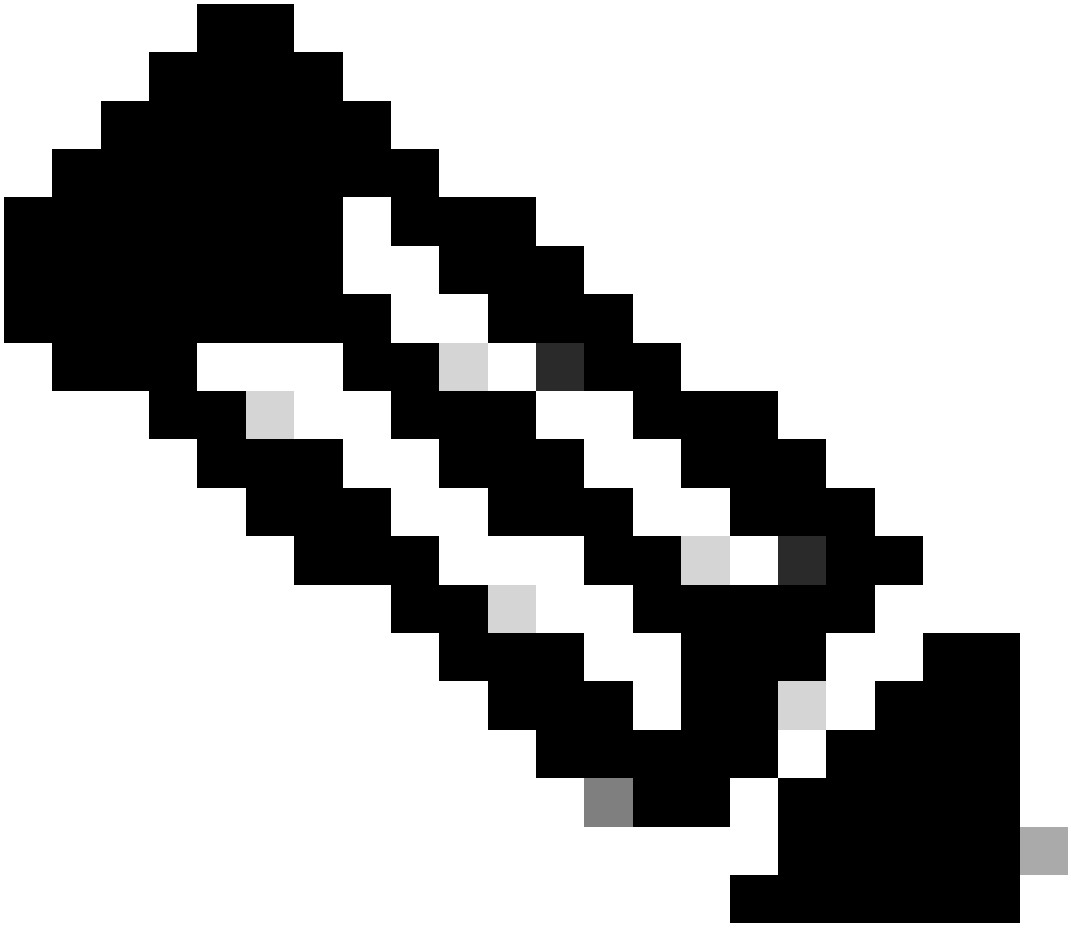
Note: Você selecionou o nome SCA do VPC nesta demonstração.

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



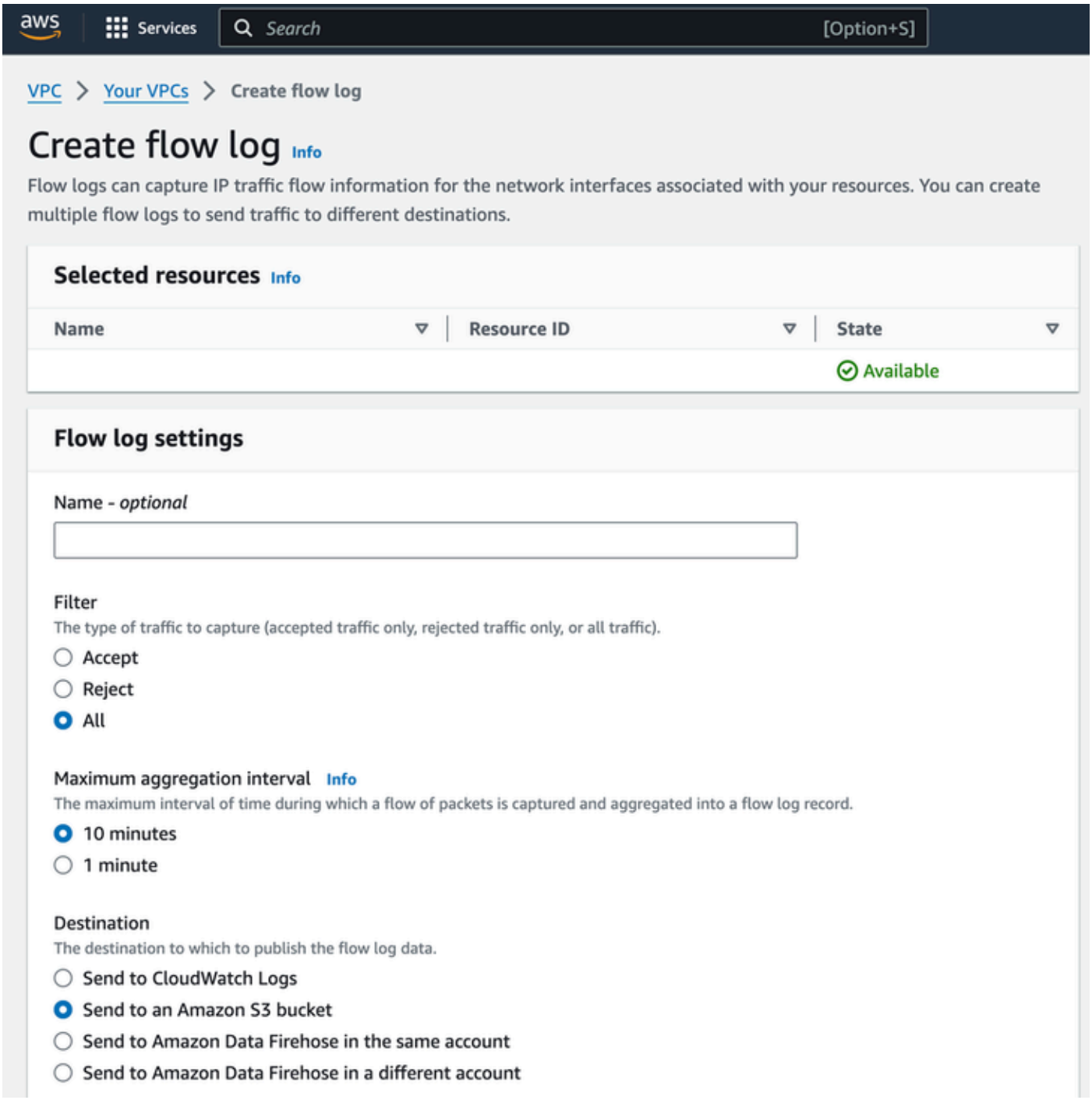

AWS-Flow-Logs

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

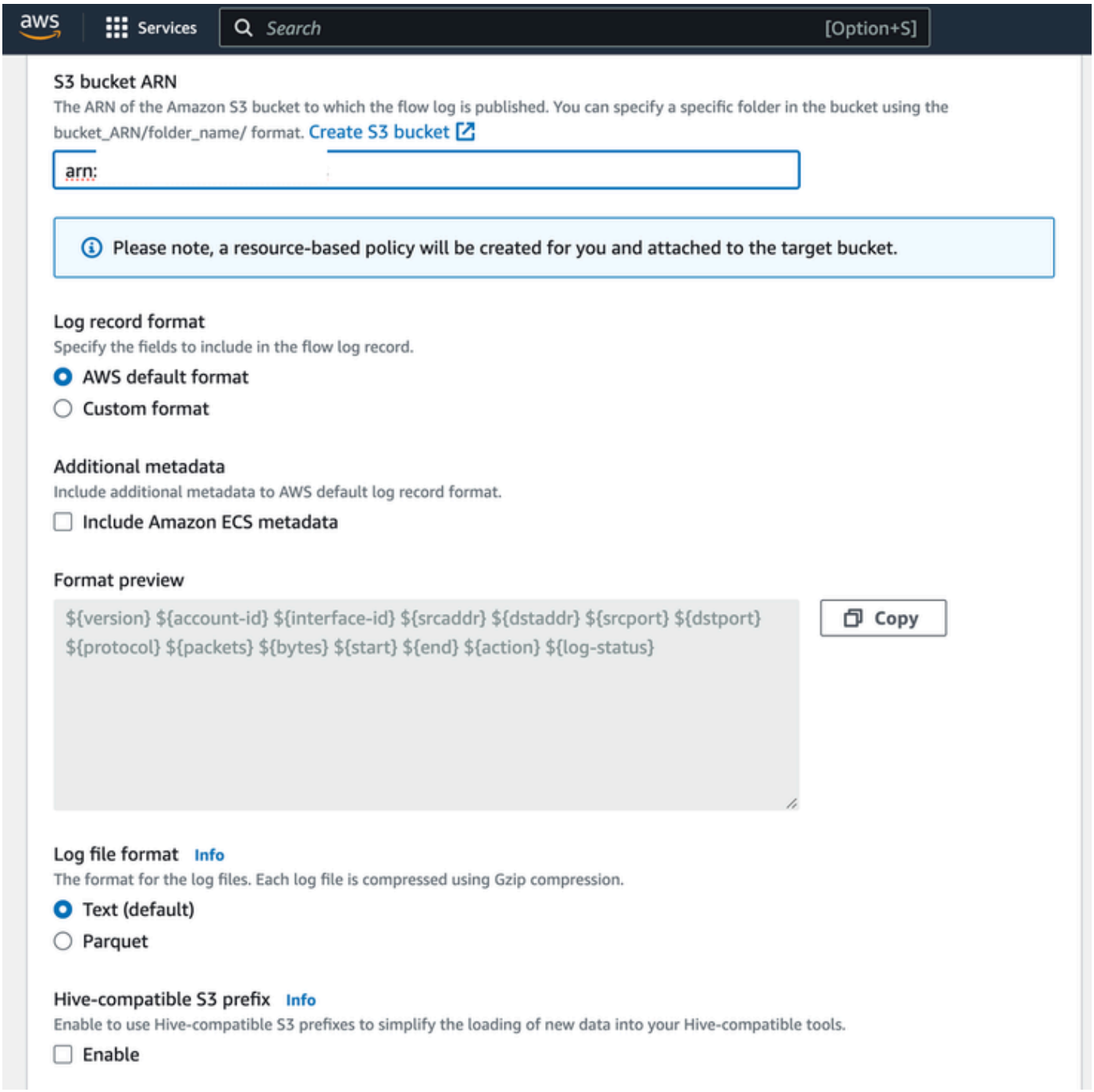


Note: Para ARN, consulte Configurar bucket de S3 - Etapa 6

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.

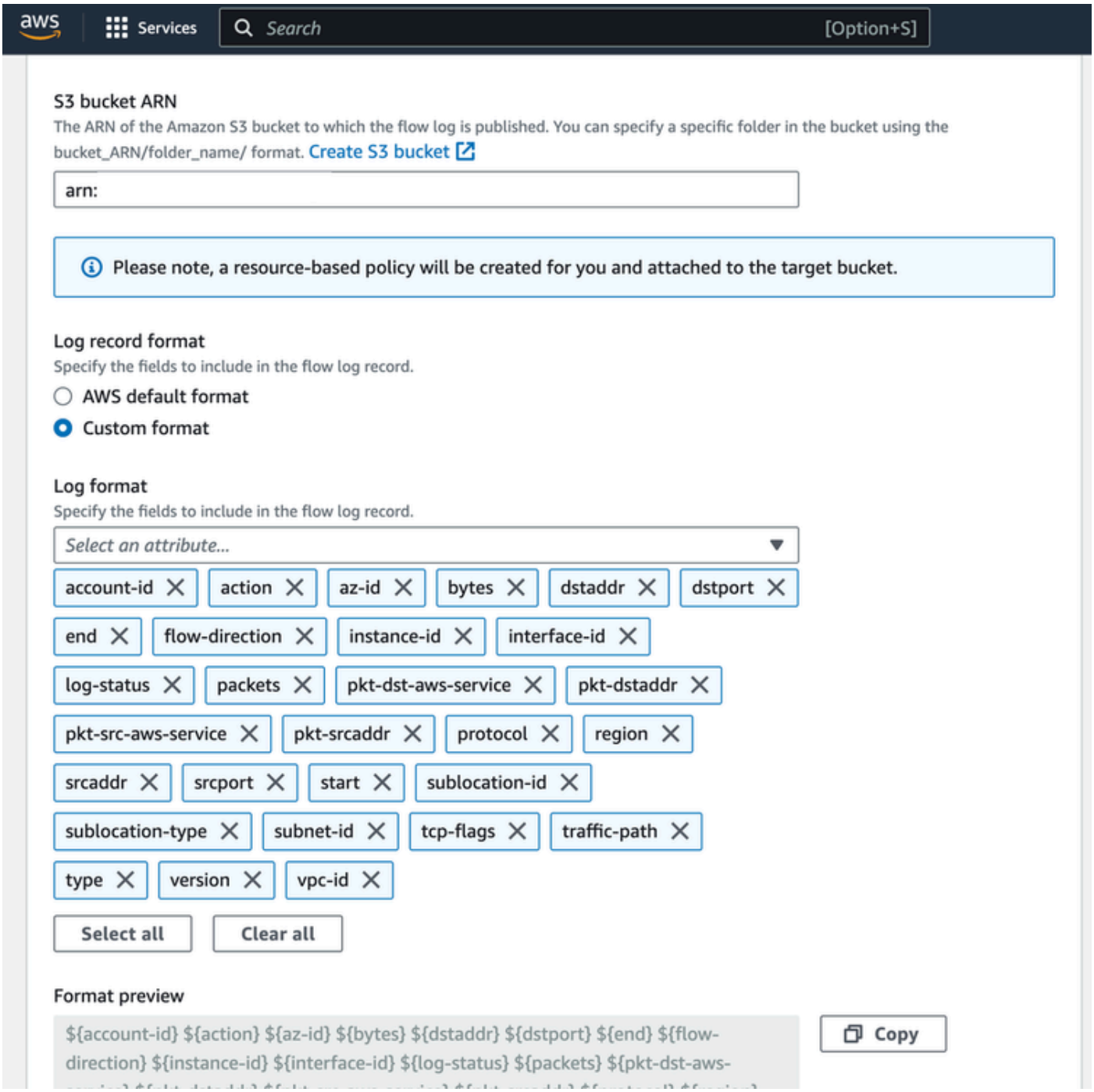



AWS-Flow-Logs

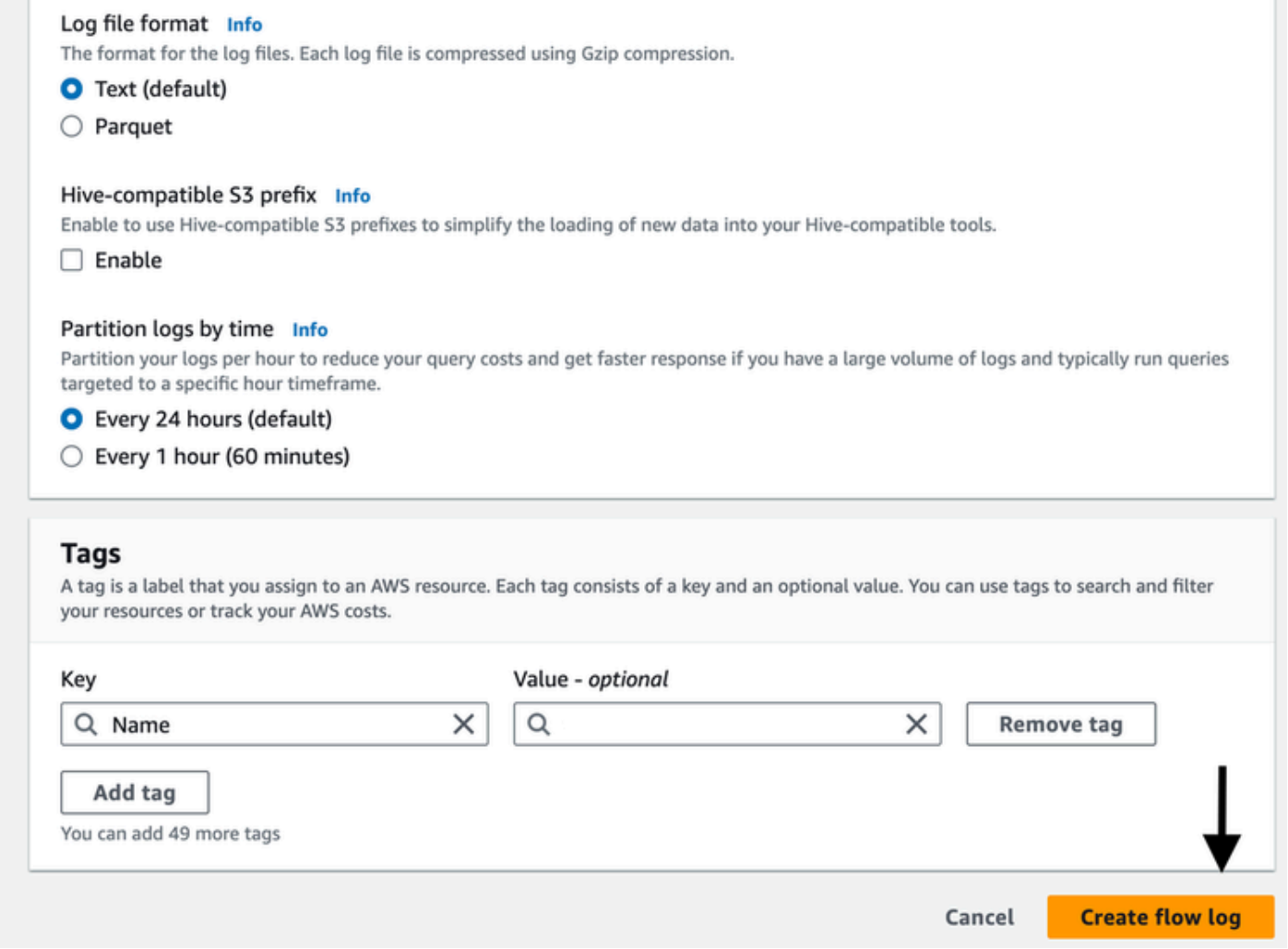



AWS-Flow-Logs

7 : Clique em criar logs de fluxo.



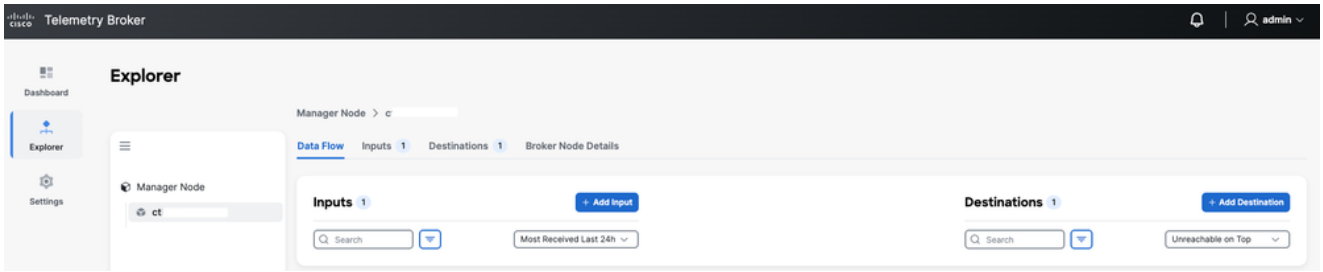

AWS-Flow-Logs




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

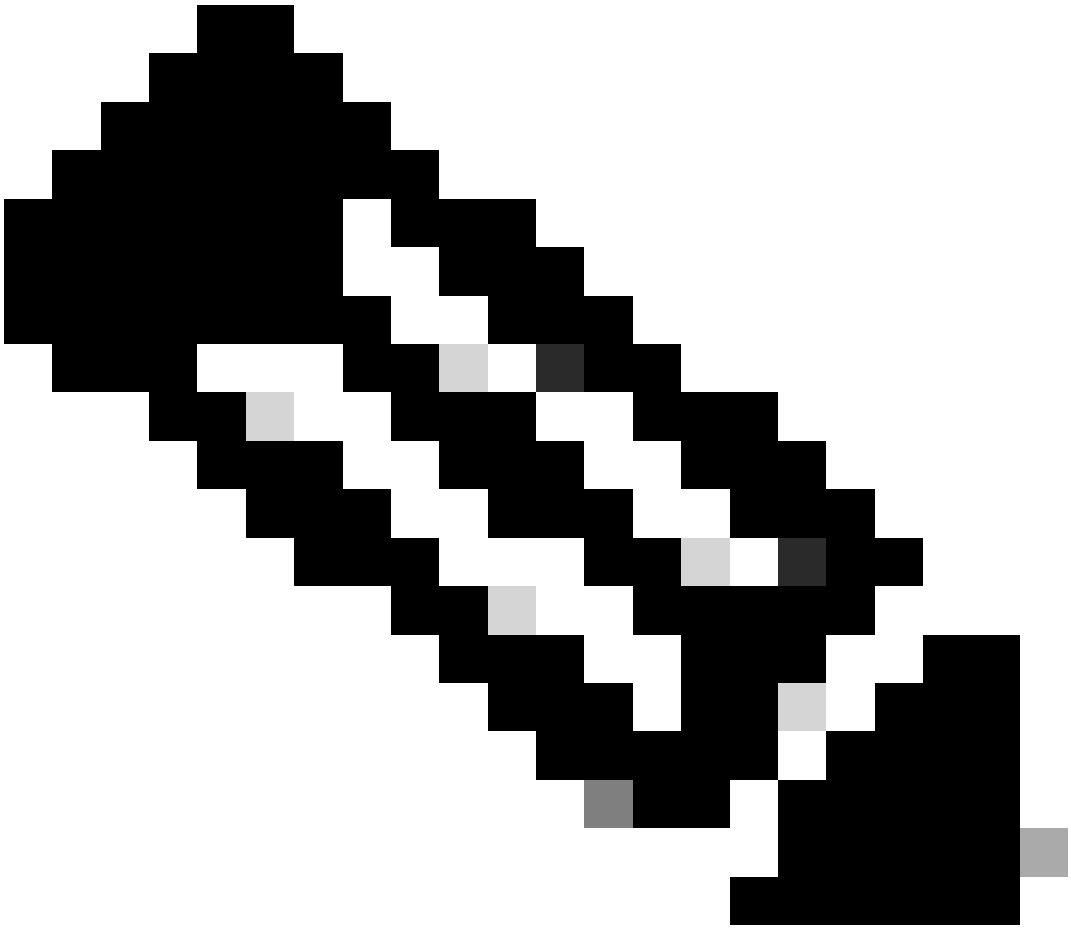
AWS VPC Flow log

AWS VPC Flow log

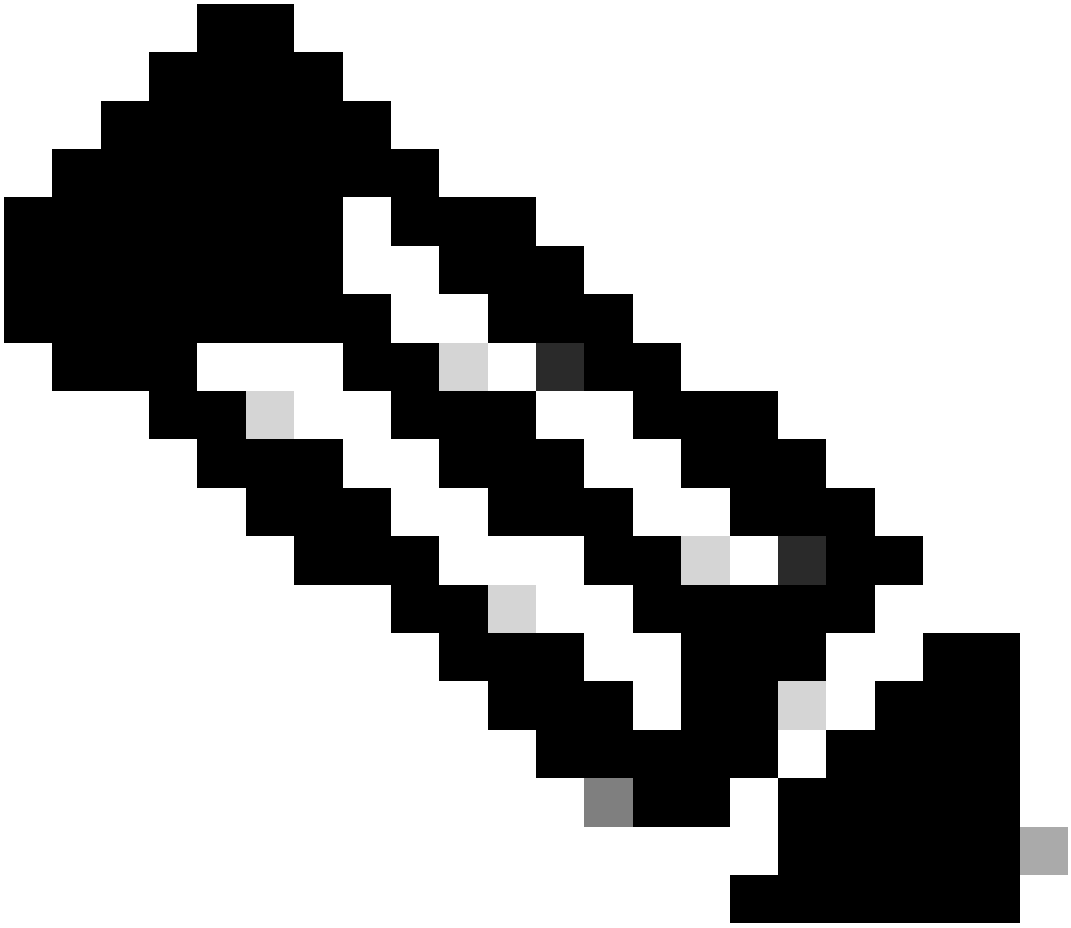
Azure NSG Flow log

Flow Generator Input

: 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

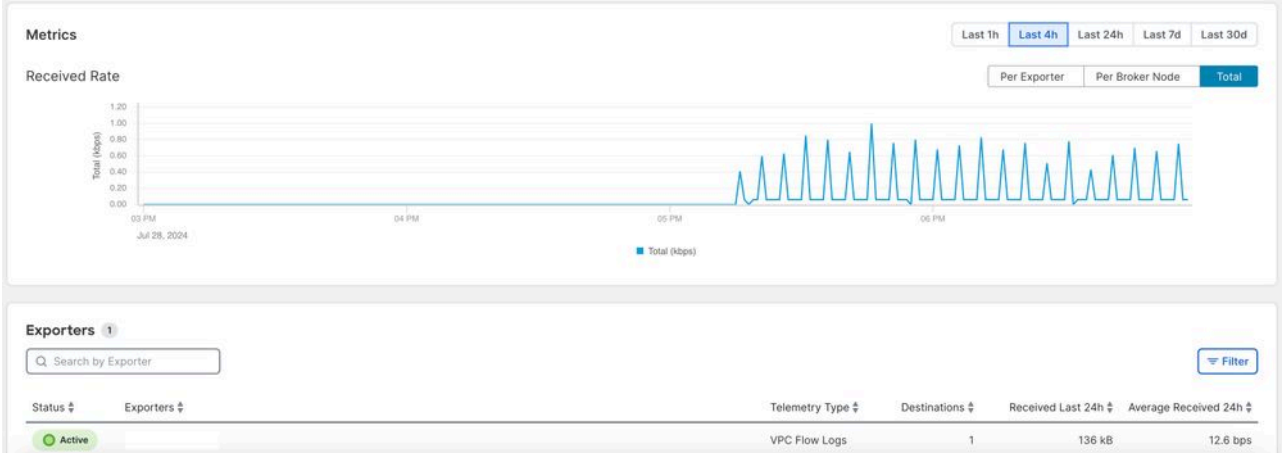
## Verificar

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**I**nput **>**Clique em abrir entrada AWS.

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


Metrics
Last 1h
Last 4h
Last 24h
Last 7d
Last 30d
Received Rate
Per Exporter
Per Broker Node
Total
Total (kbps)
1.20
1.00
0.80
0.60
0.40
0.20
0.00
03 PM
04 PM
05 PM
06 PM
Jul 28, 2024
Total (kbps)
Exporters 1
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

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.