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

Table des matières

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.

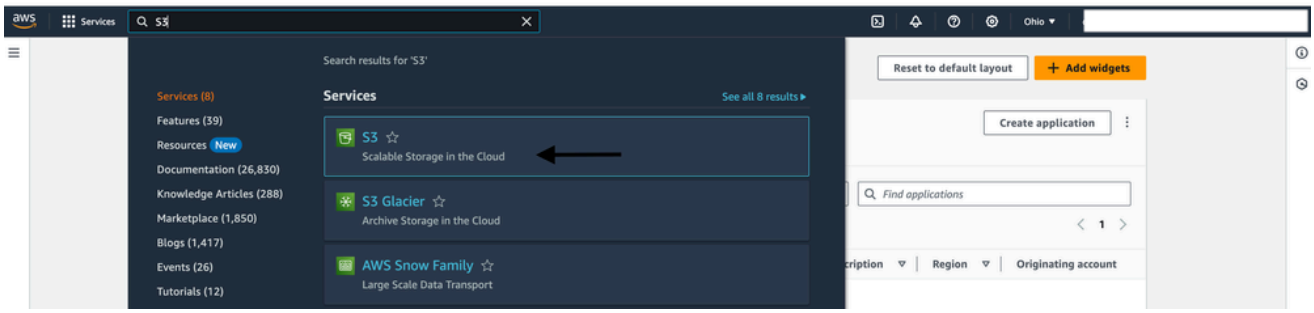
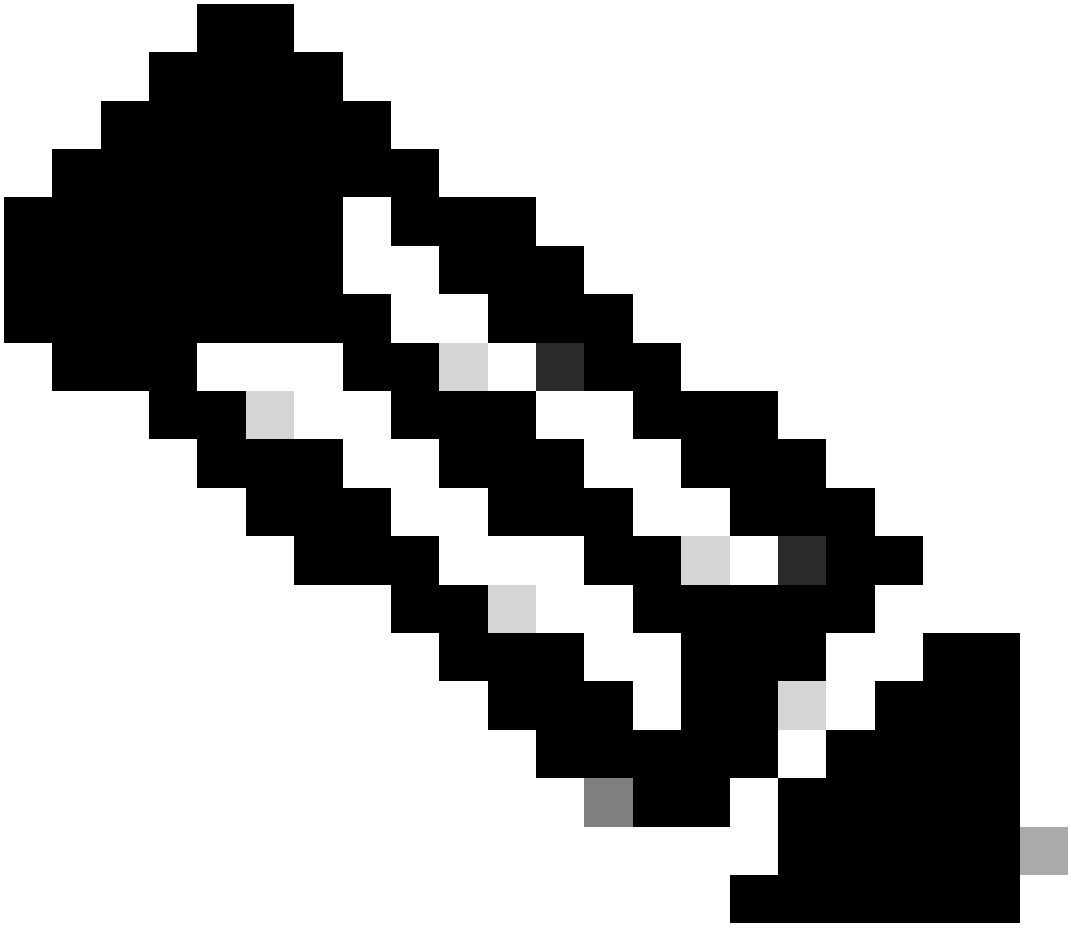
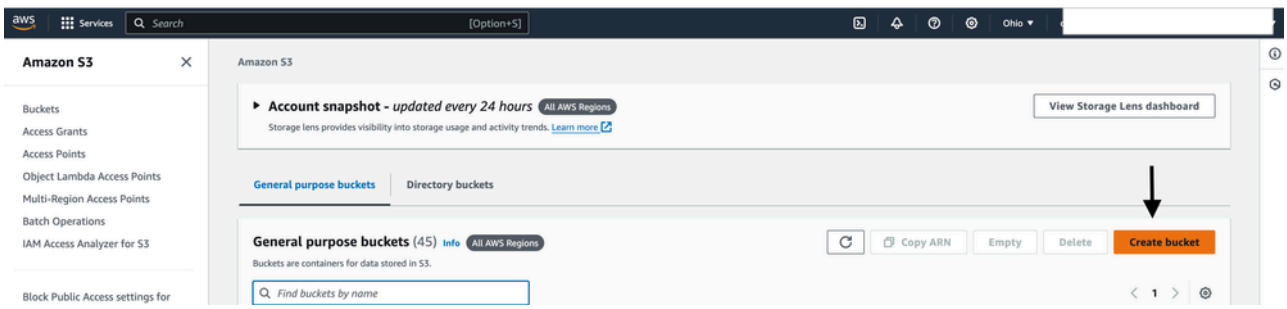


tableau de bord AWS



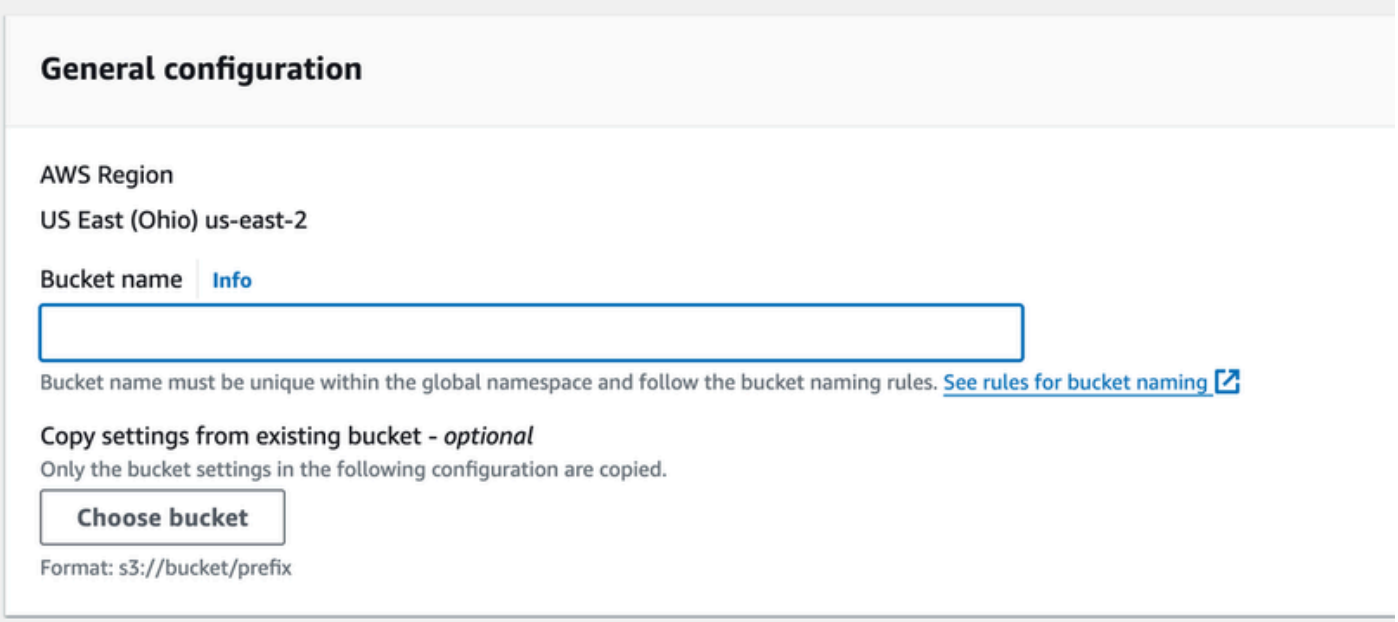
Remarque : Dans la démonstration, vous avez sélectionné la région de l'Ohio avec la zone de disponibilité us-east-2, elle est visible juste à côté de l'icône d'engrenage.

4: Cliquez sur Créer un compartiment.

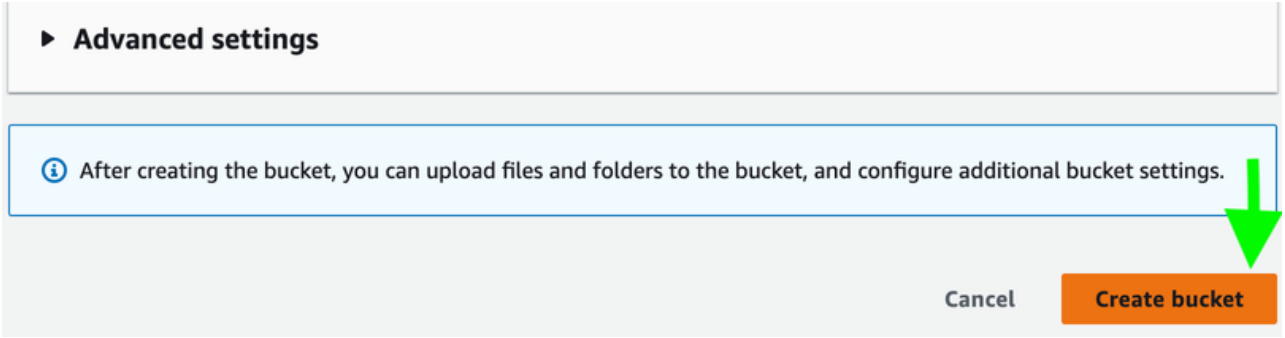


AWS-S3

5: Donnez un nom à bucket et laissez chaque option telle quelle, puis cliquez sur Create.

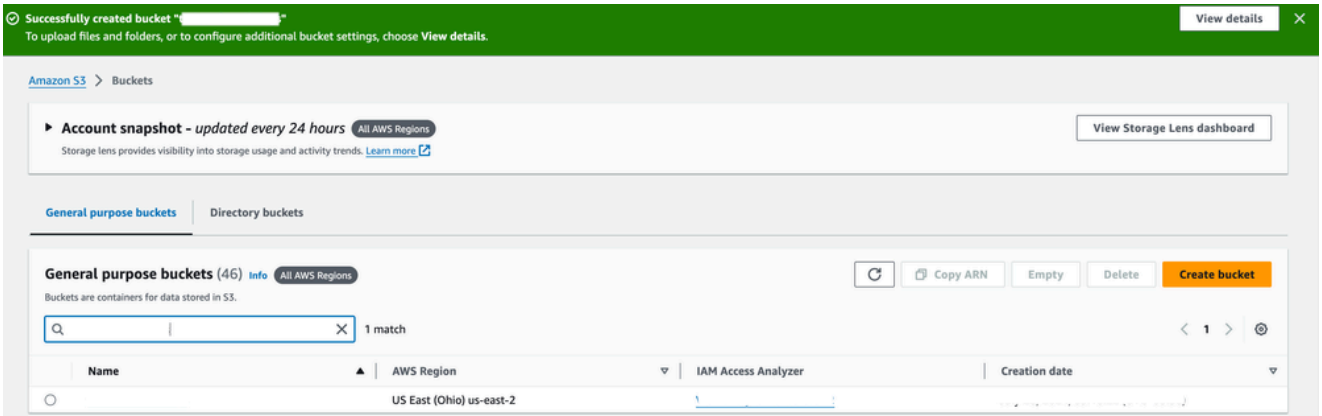


AWS-S3

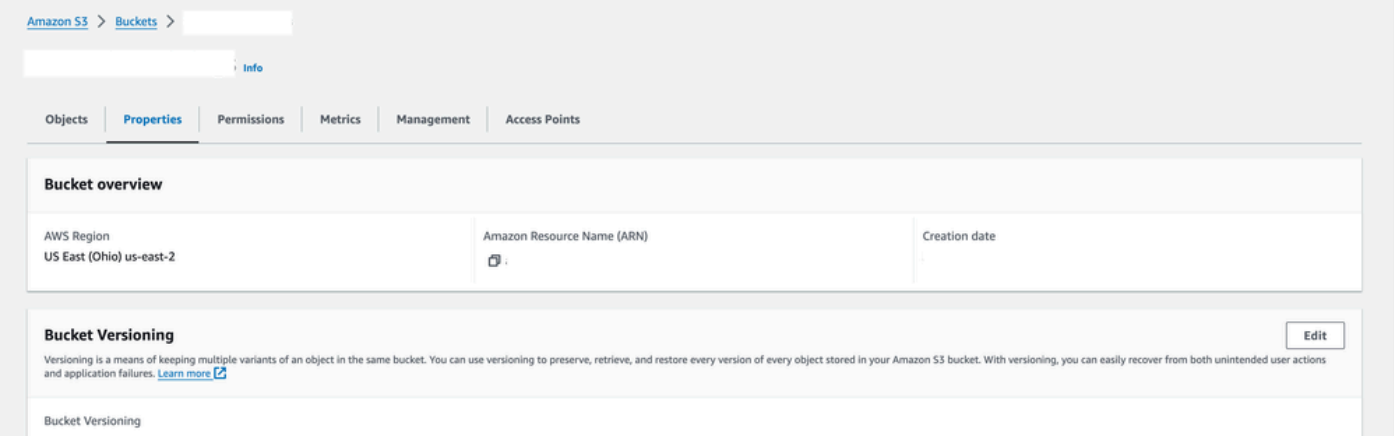


AWS-S3

6: Une fois que le bucket est créé avec succès, enregistrez le bucket ARN qui doit être utilisé plus tard pendant la configuration.



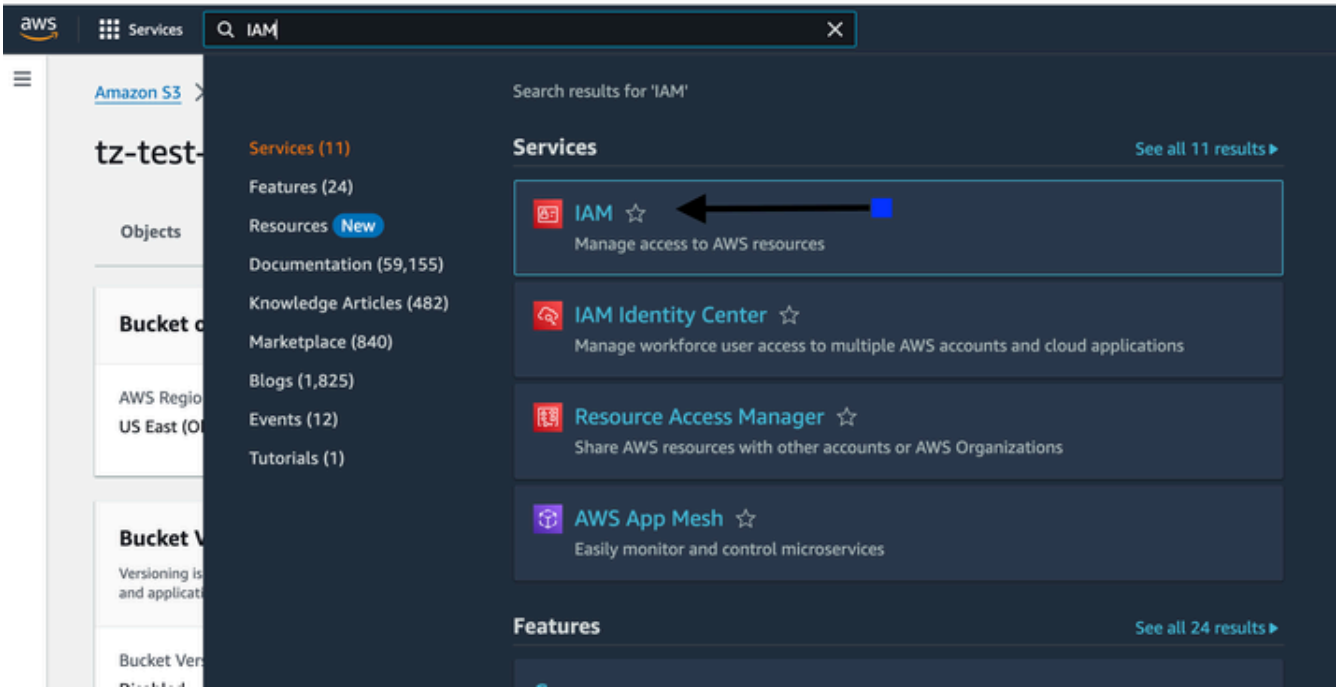
AWS-S3



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.



AWS-IAM

2: Accédez aux utilisateurs.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

Users

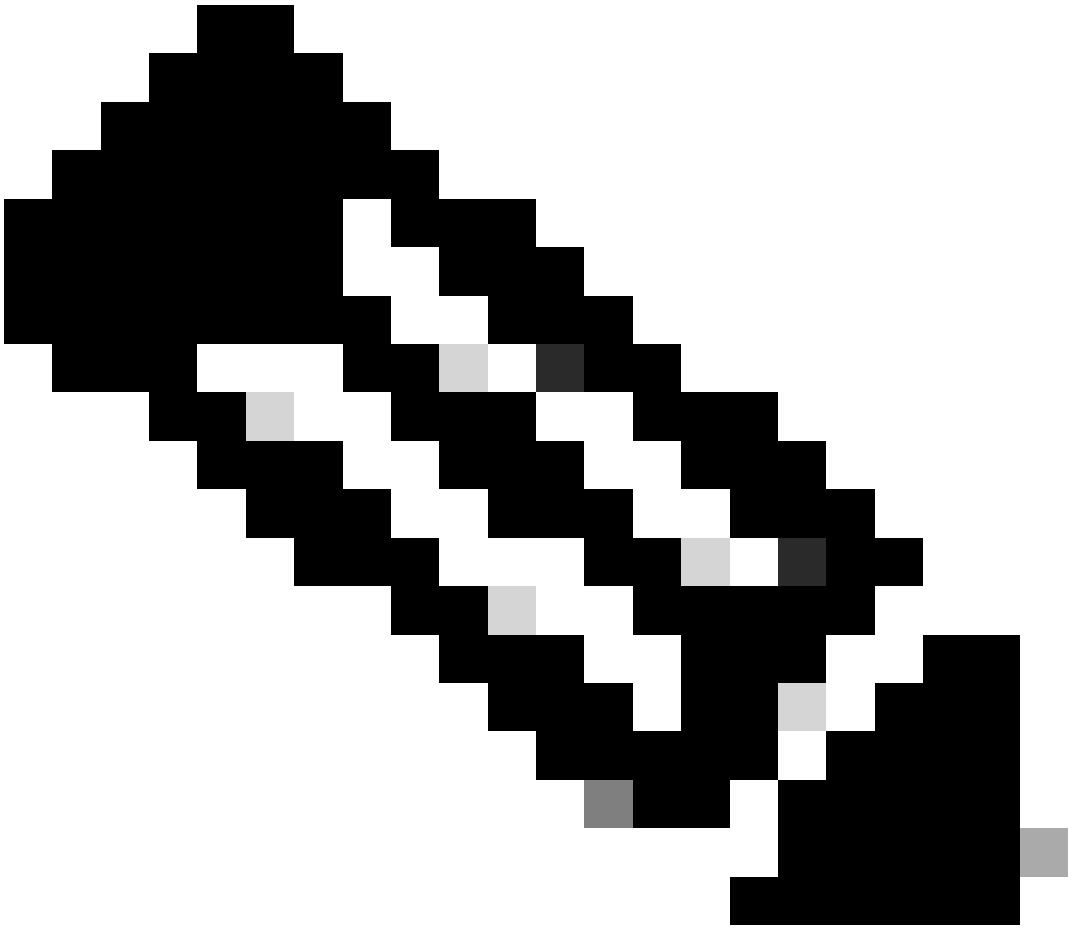
Roles

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.

---

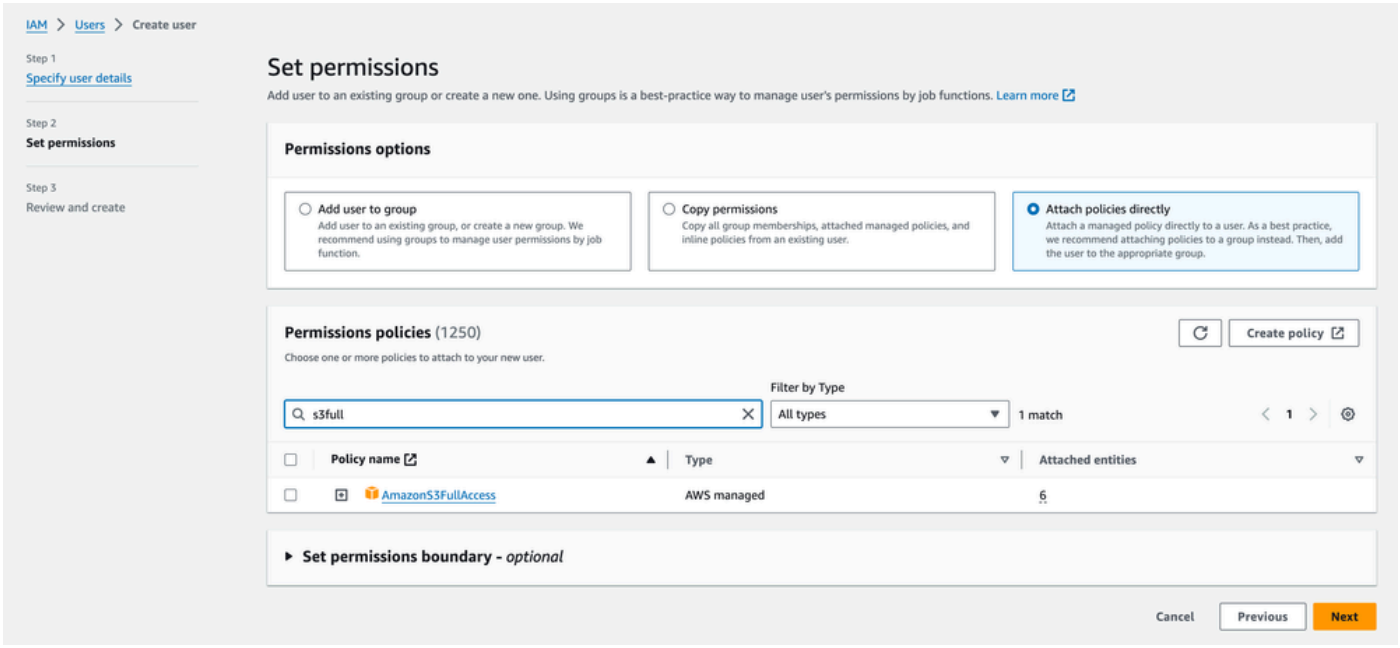
6 : Attribuez une stratégie en l'attribuant à l'utilisateur, en l'attachant directement à un groupe ou en la configurant en ligne.



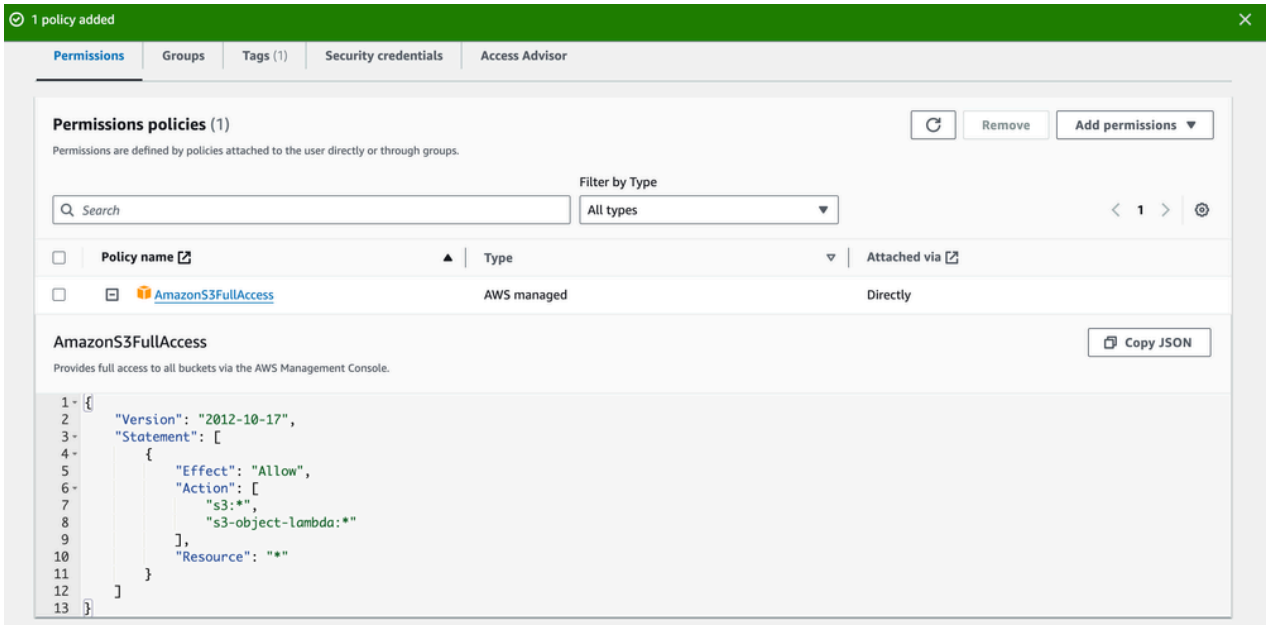
Remarque : Pour la démonstration, vous affectez directement la stratégie à l'utilisateur. Pour plus d'informations - Gestion des stratégies AWS

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.

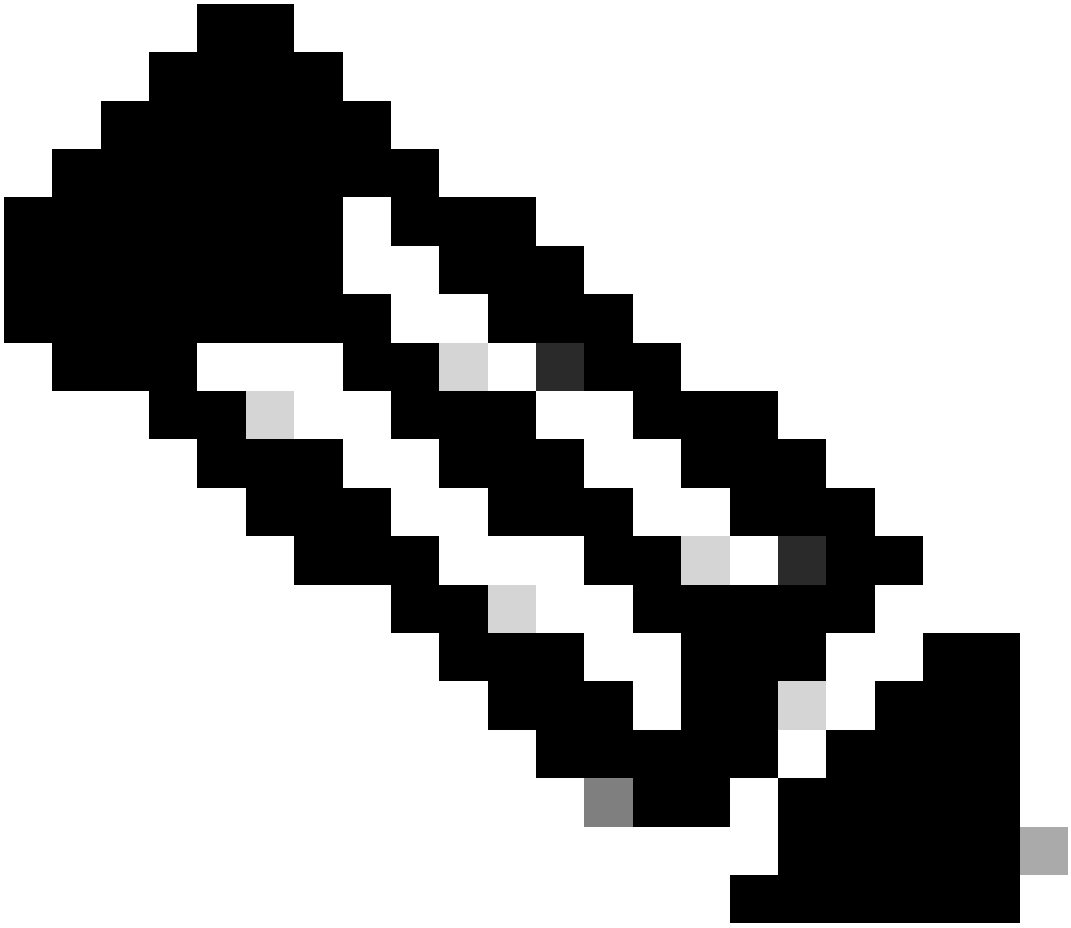
8: Cochez la case avec le nom de stratégie AmazonS3FullAccess et cliquez sur next.



AWS-IAM

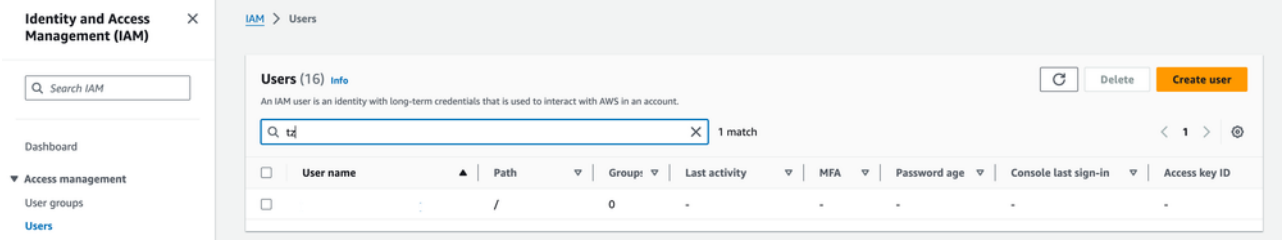


AWS-IAM

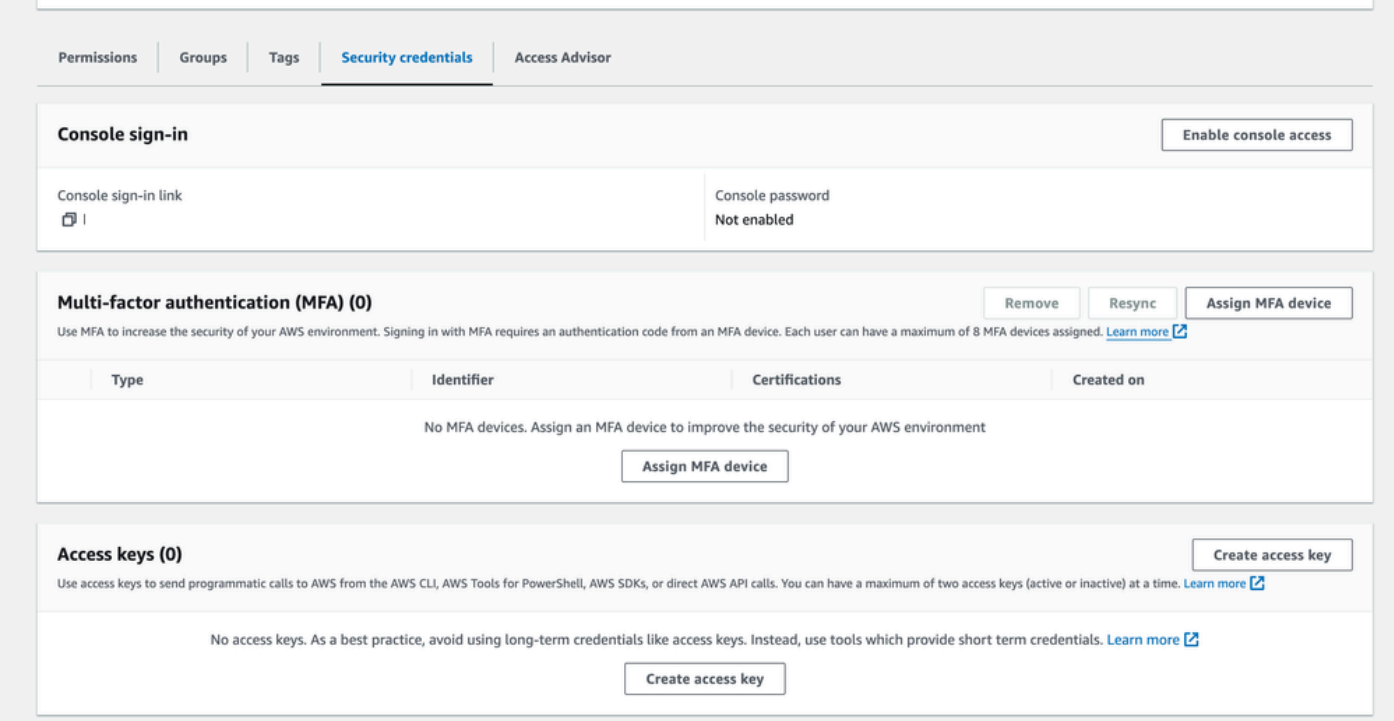


Remarque : Vous pouvez créer une stratégie plus granulaire en n'autorisant que des regroupements spécifiques. Accédez à [Création de stratégie] pour créer votre stratégie de regroupement S3 au format json.

9: Une fois l'utilisateur créé, répertoriez-le et accédez à l'onglet security credential et cliquez sur create access key.

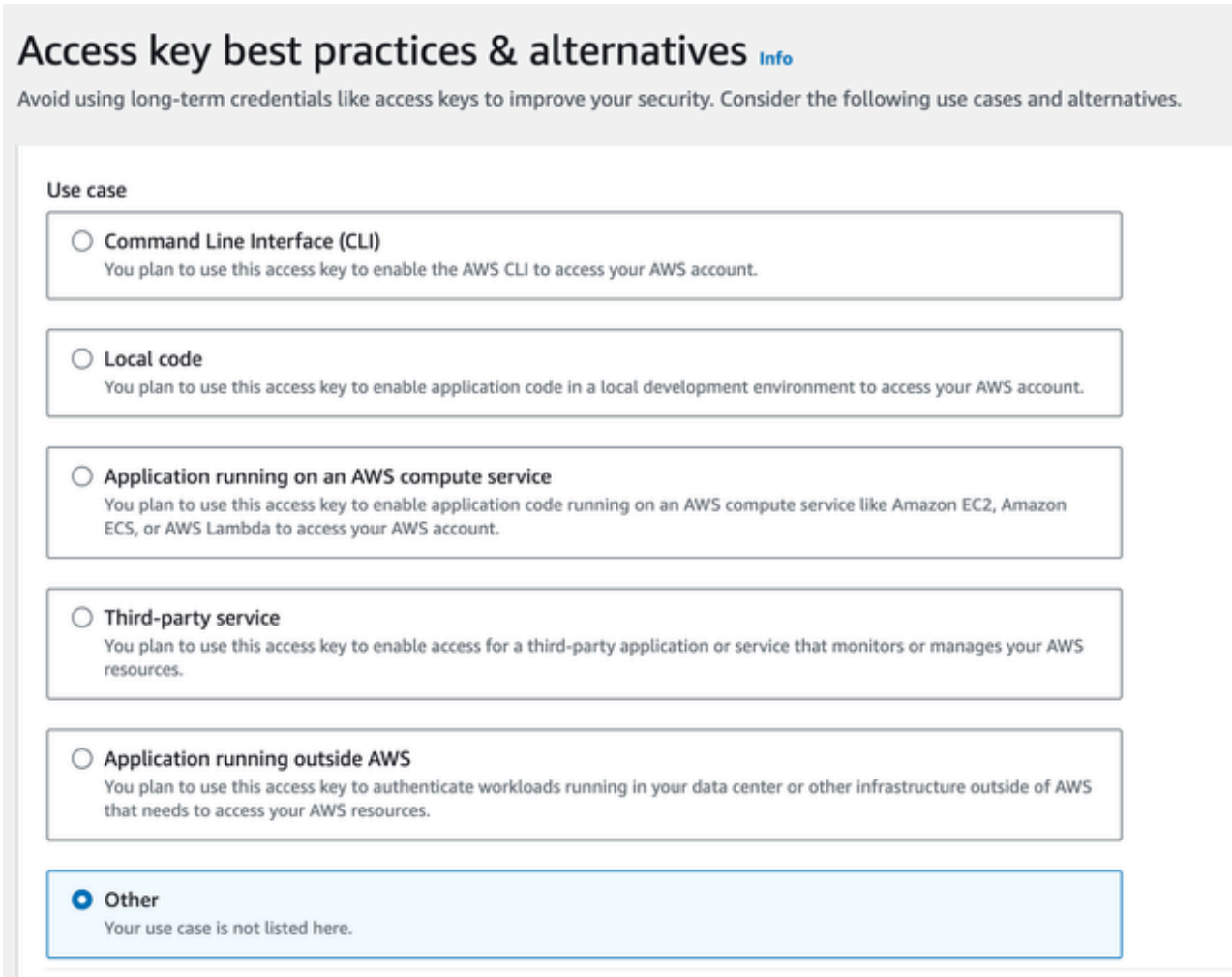


AWS-IAM

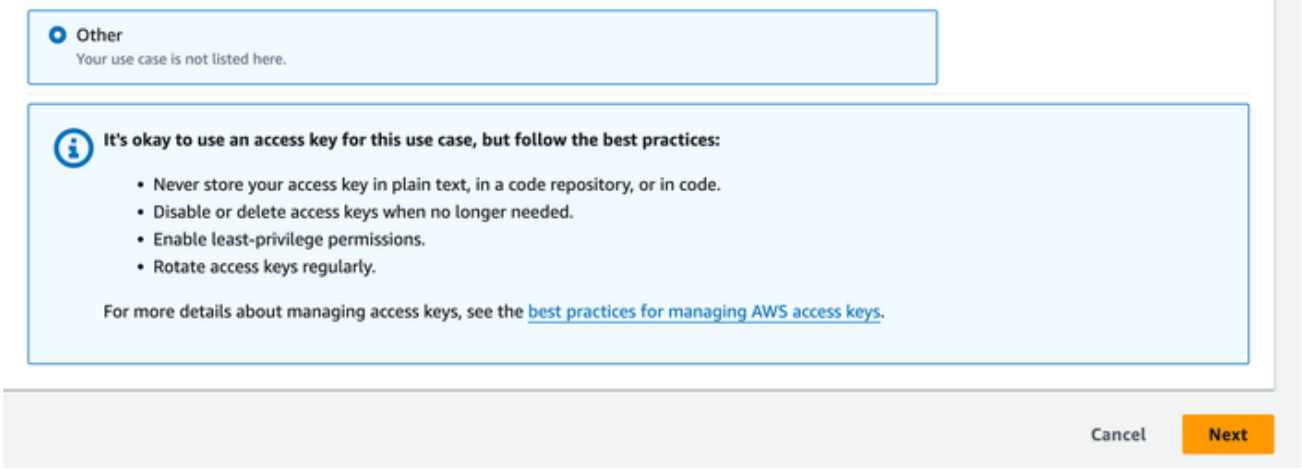


AWS-IAM

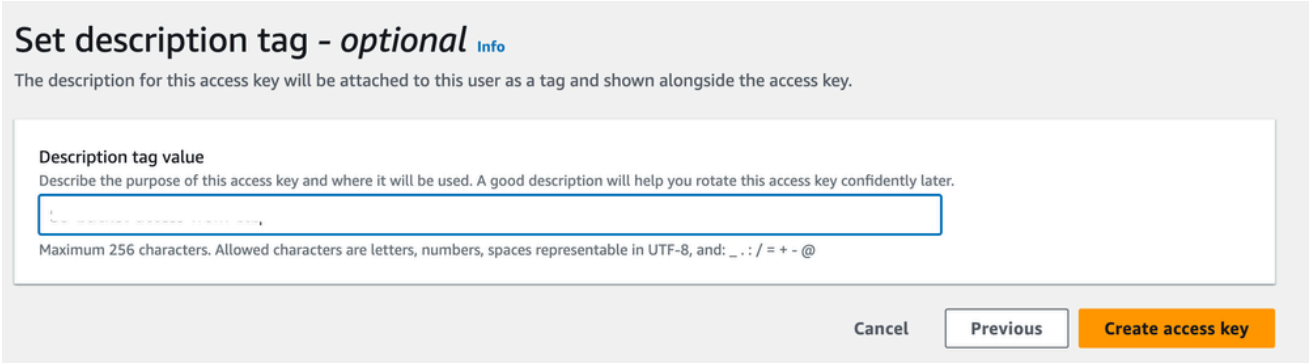
10: Sélectionnez l'autre case d'option et ajoutez éventuellement une balise.



AWS-IAM

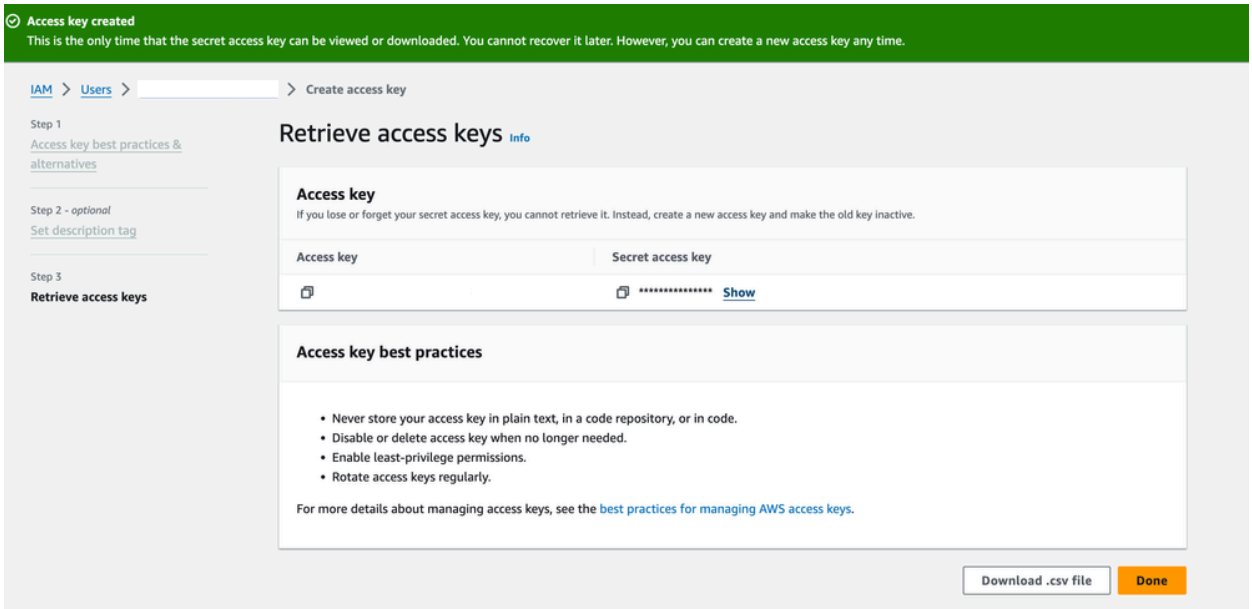


AWS-IAM



AWS-IAM

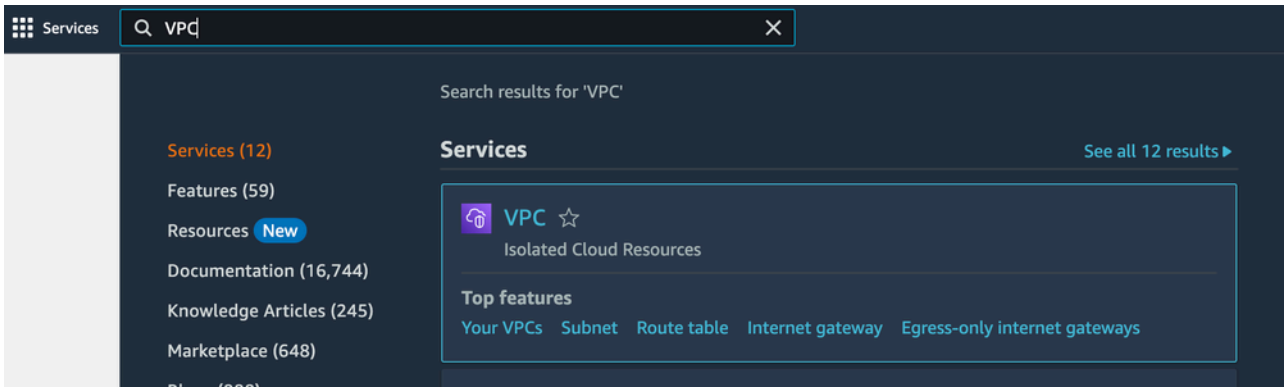
11 : Cliquez sur Télécharger le fichier .csv. Il s'agit de la clé d'accès d'un fichier csv qui n'est plus disponible pour le téléchargement ou l'affichage une fois que vous avez quitté cette page.



AWS-IAM

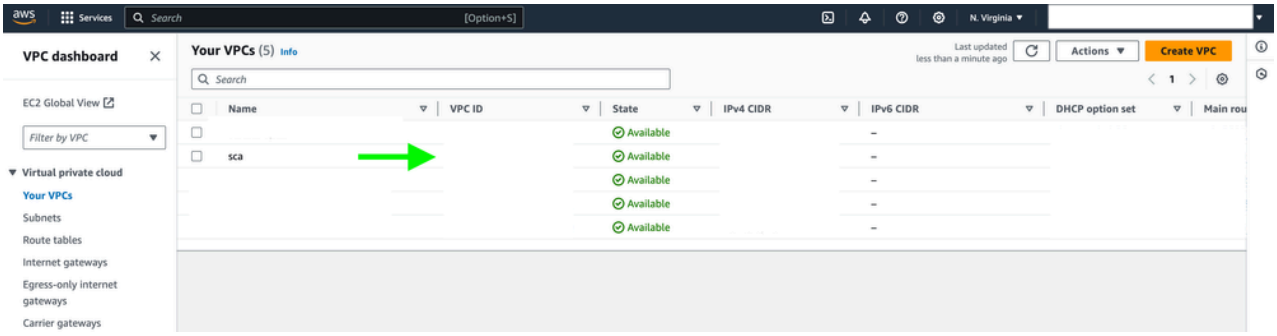
Étape 3 : configuration des journaux de flux VPC

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

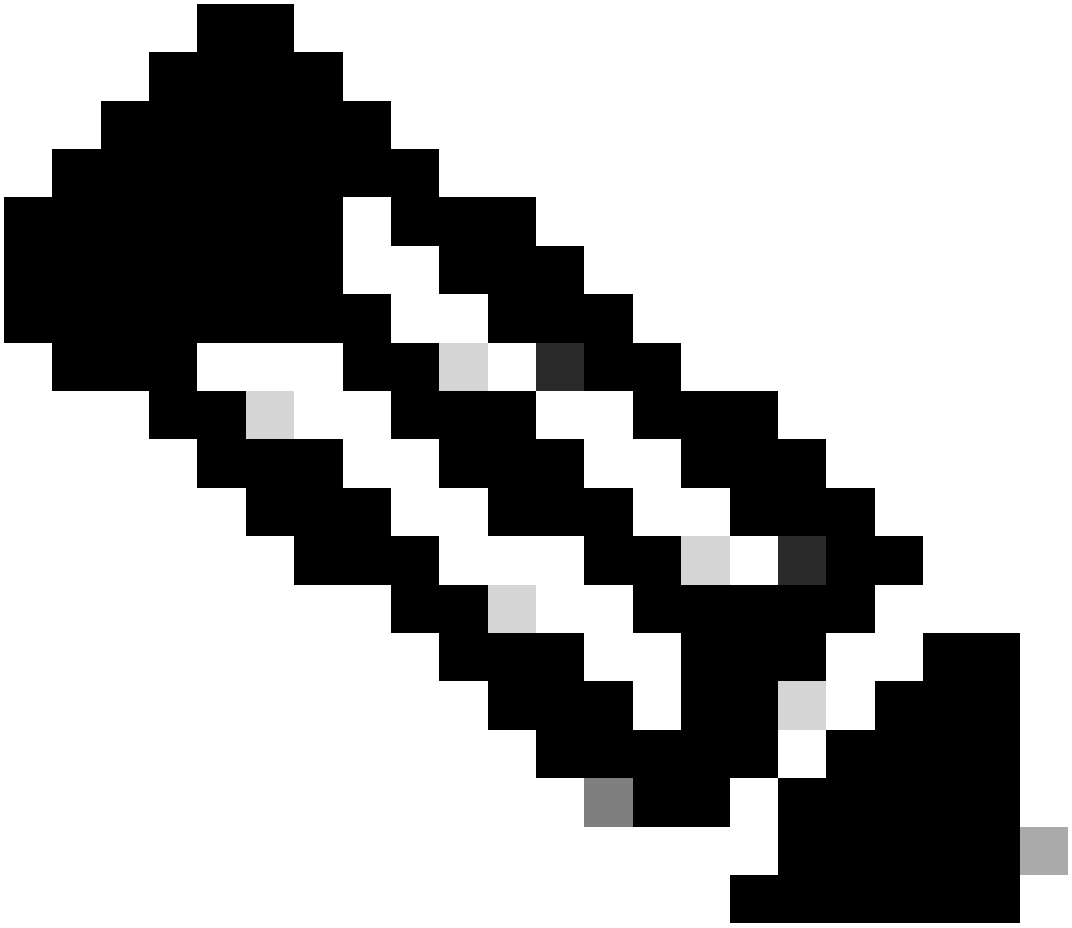


Journaux de flux AWS

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

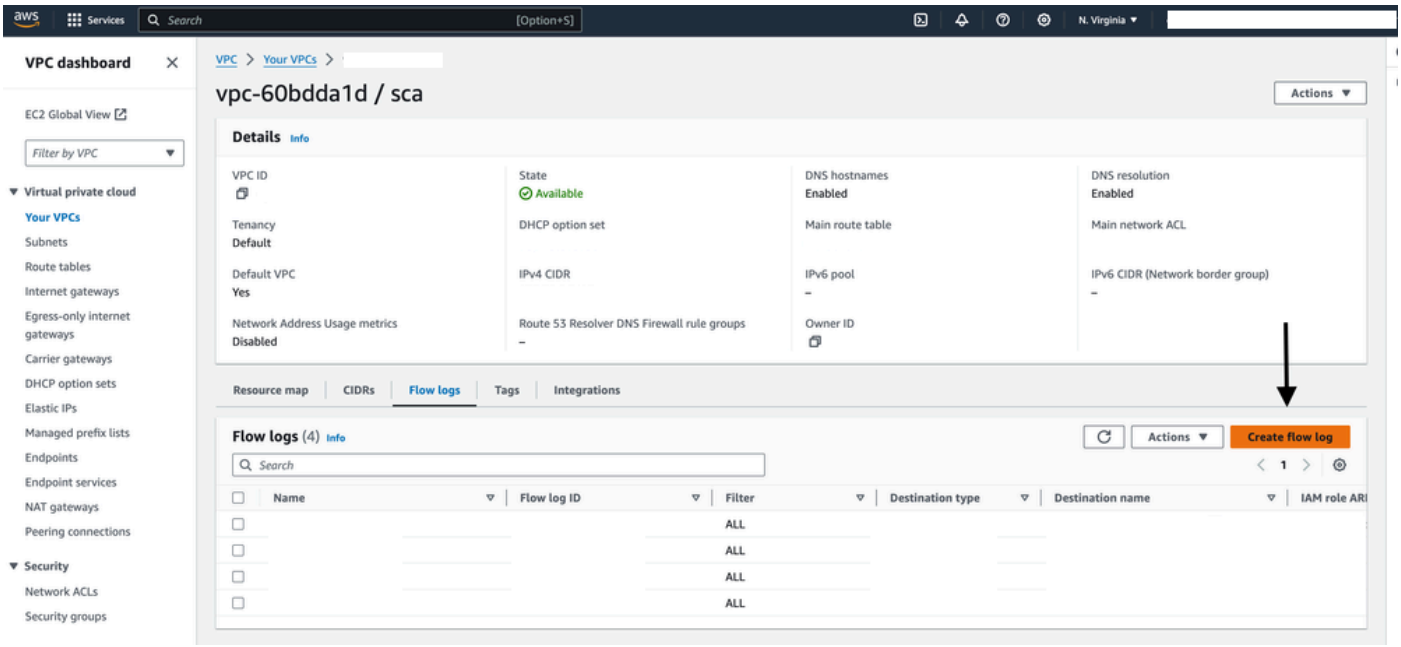


Journaux de flux AWS



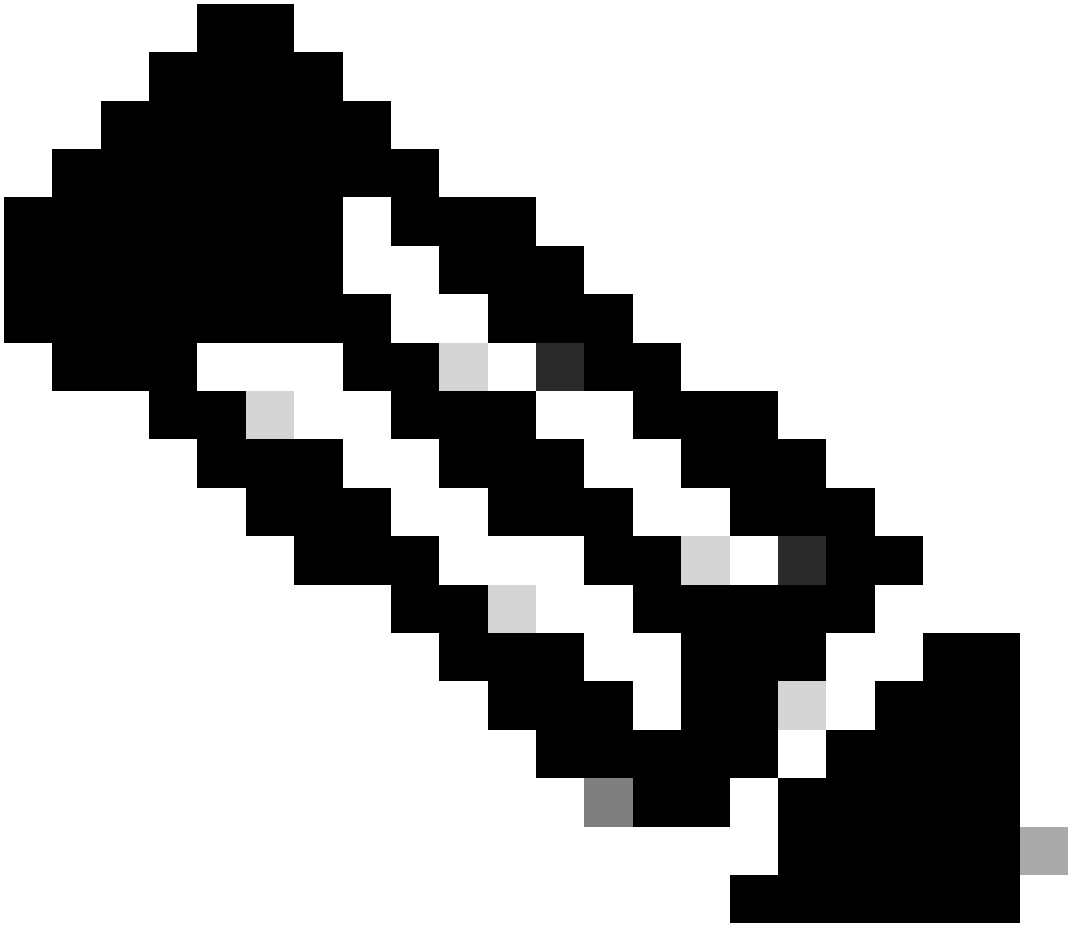
Remarque : Vous avez sélectionné le nom VPC SCA dans cette démonstration.

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



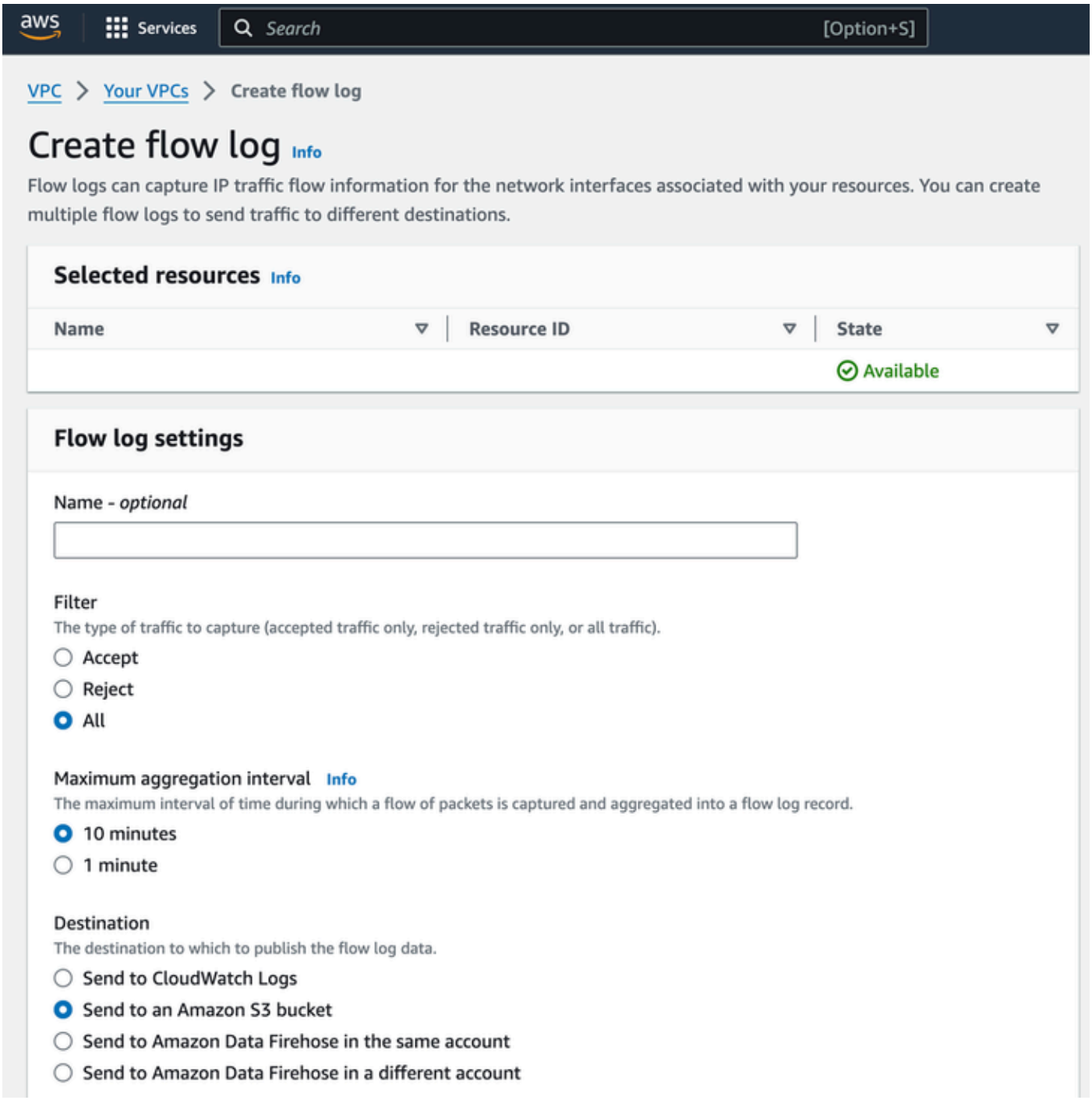
Journaux de flux AWS

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

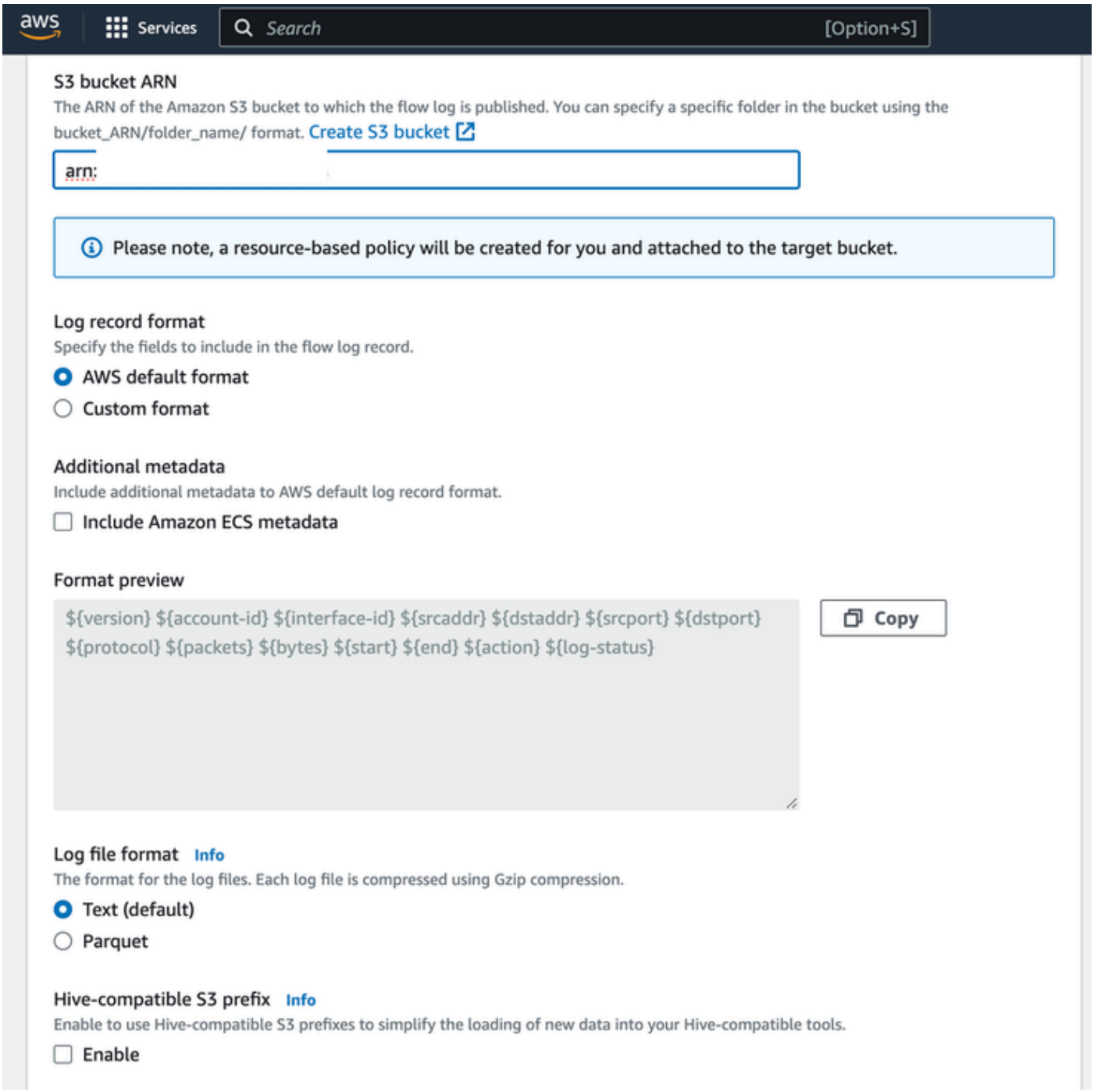


Remarque : Pour ARN, reportez-vous à Configuration du compartiment S3 - Étape 6

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.

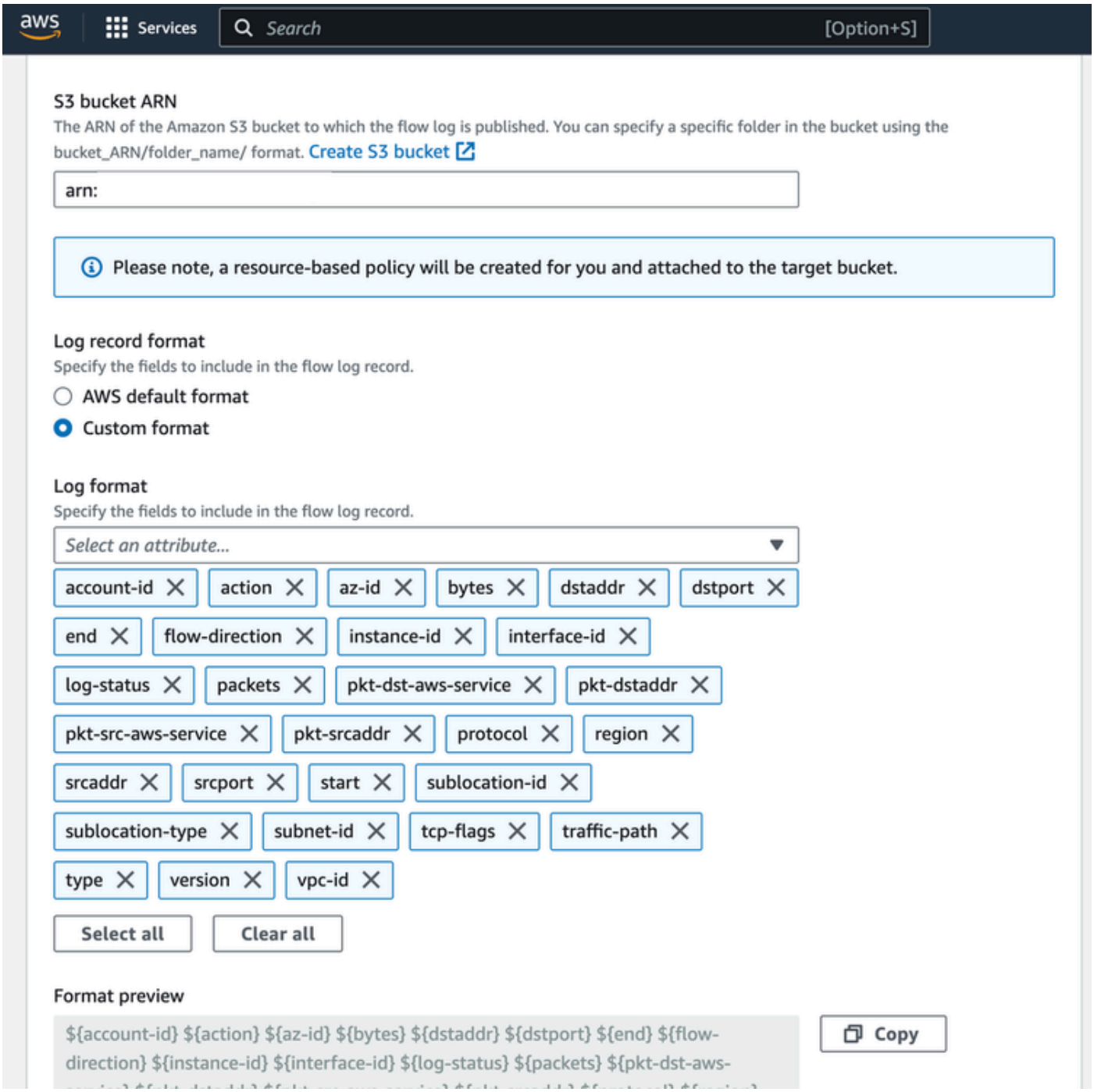


Journaux de flux AWS

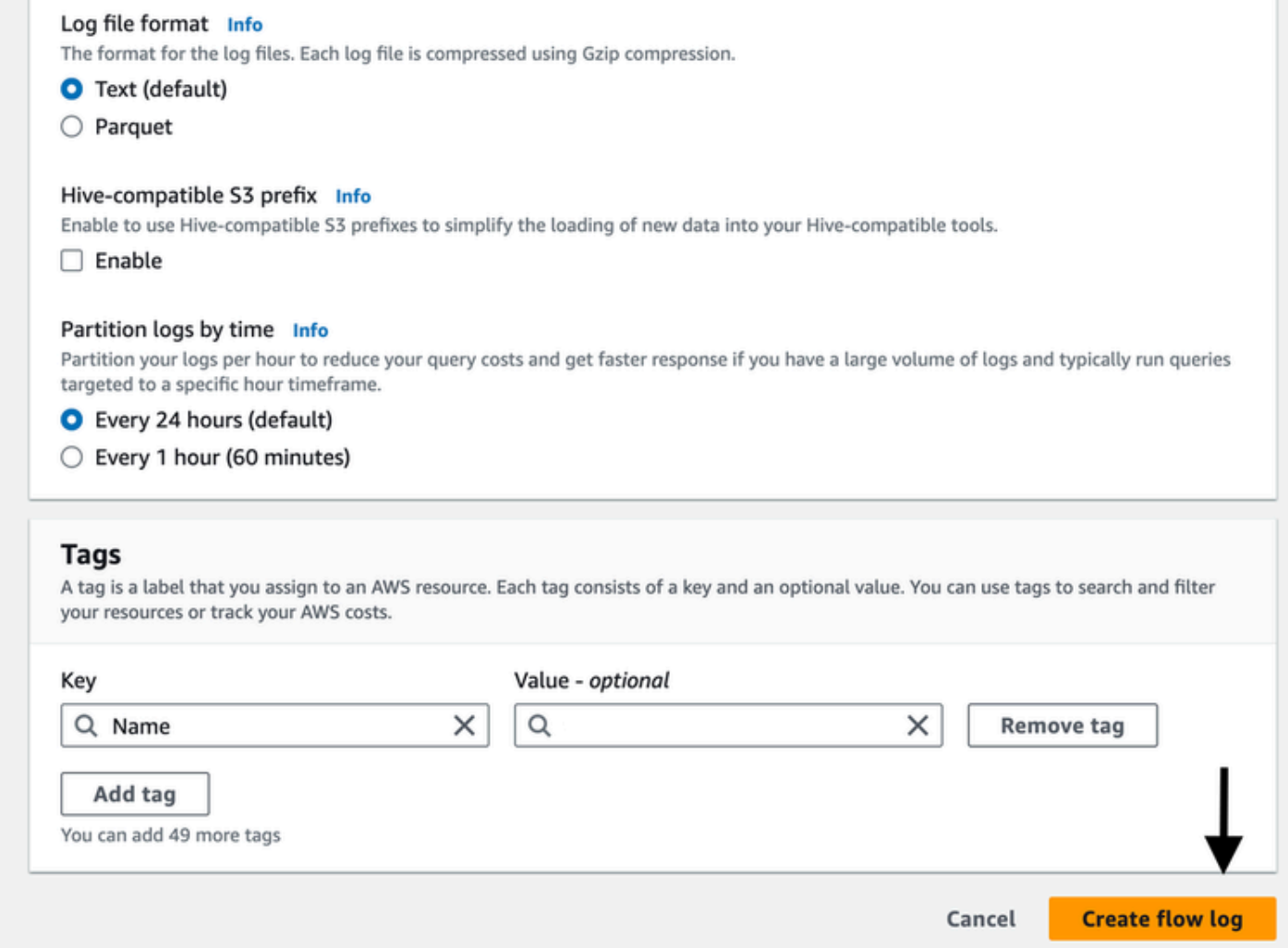


Journaux de flux AWS

7: Cliquez sur créer des journaux de flux.



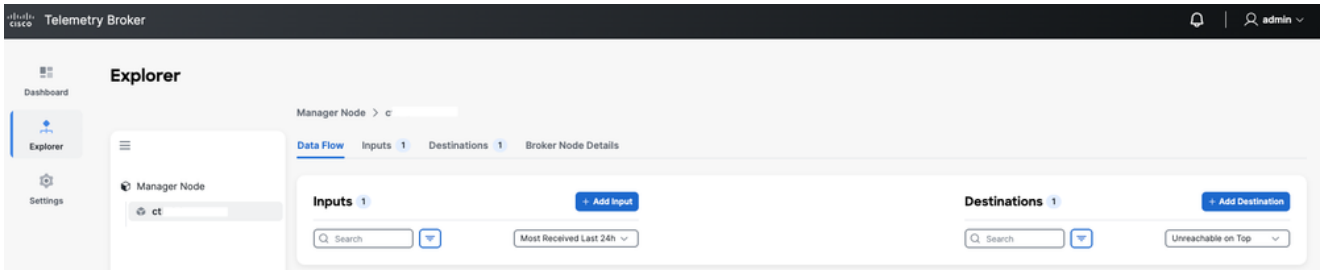
Journaux de flux AWS



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

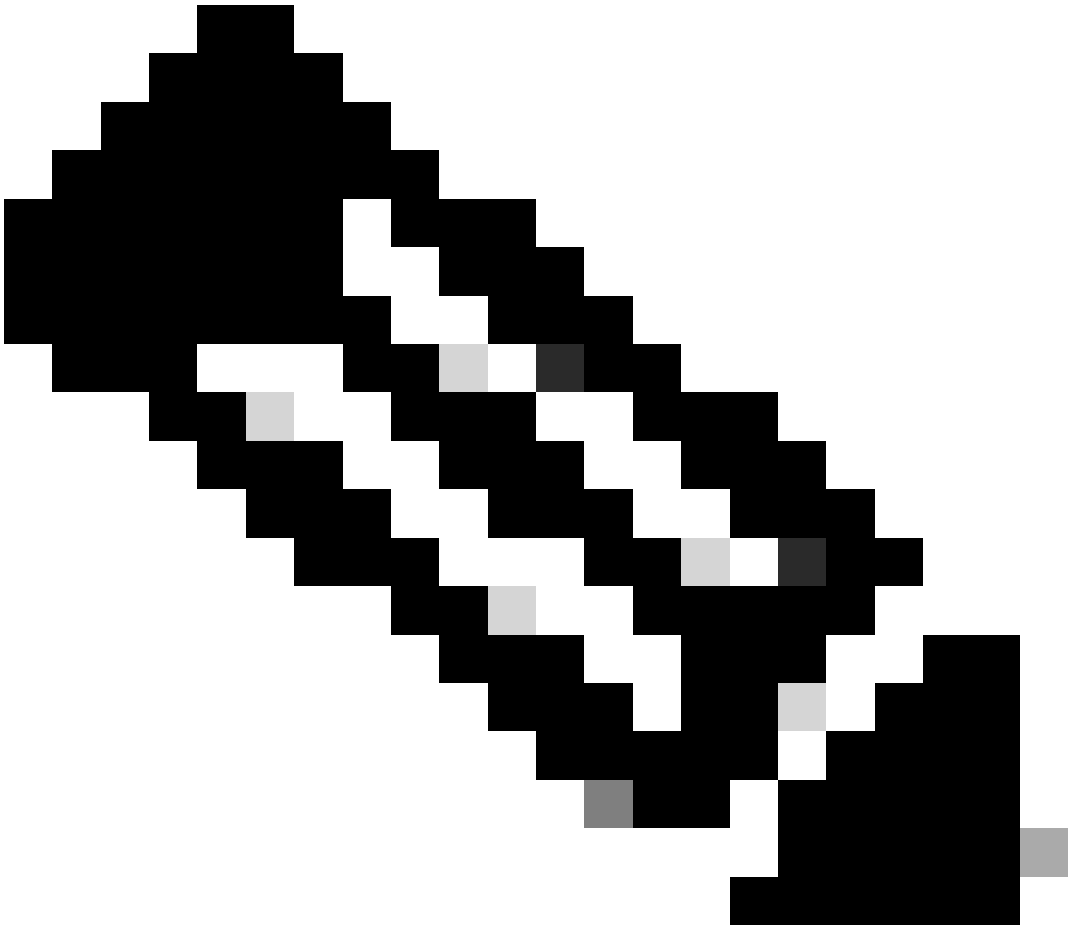
AWS VPC Flow log

AWS VPC Flow log

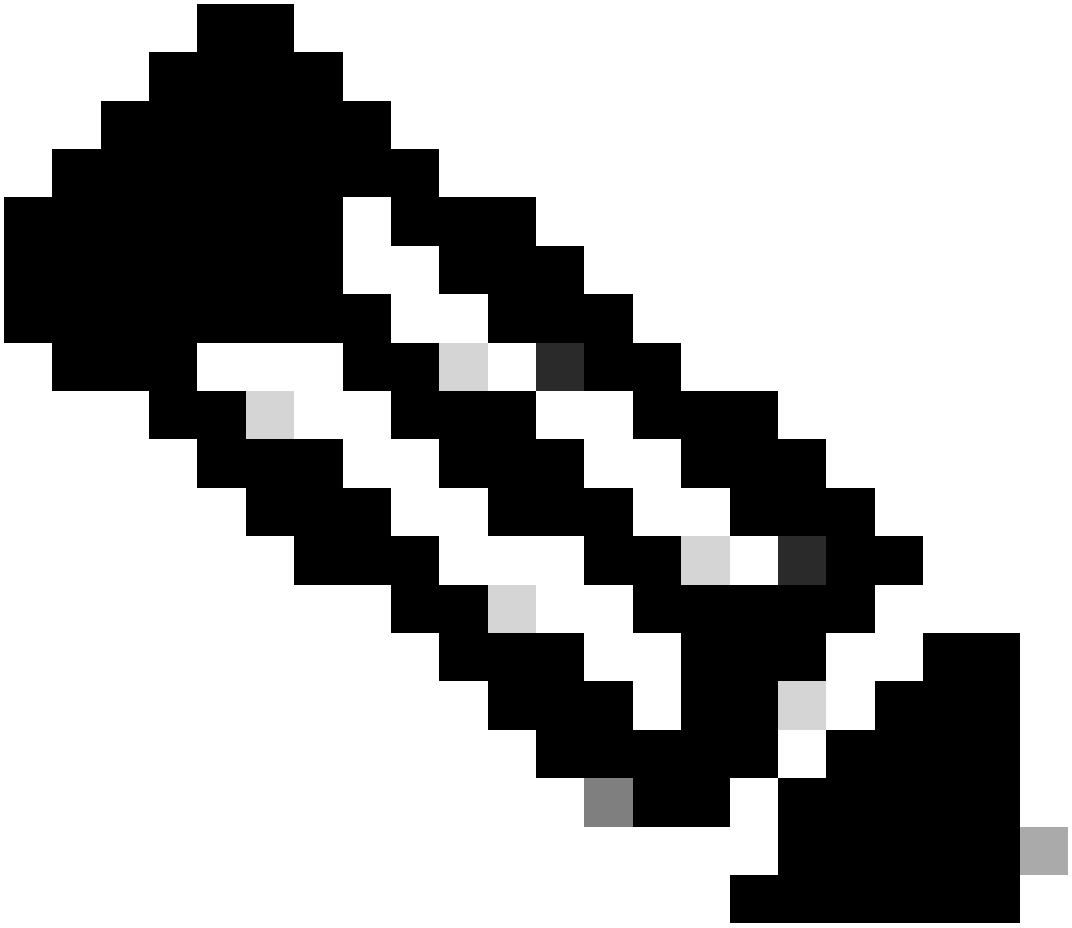
Azure NSG Flow log

Flow Generator Input

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

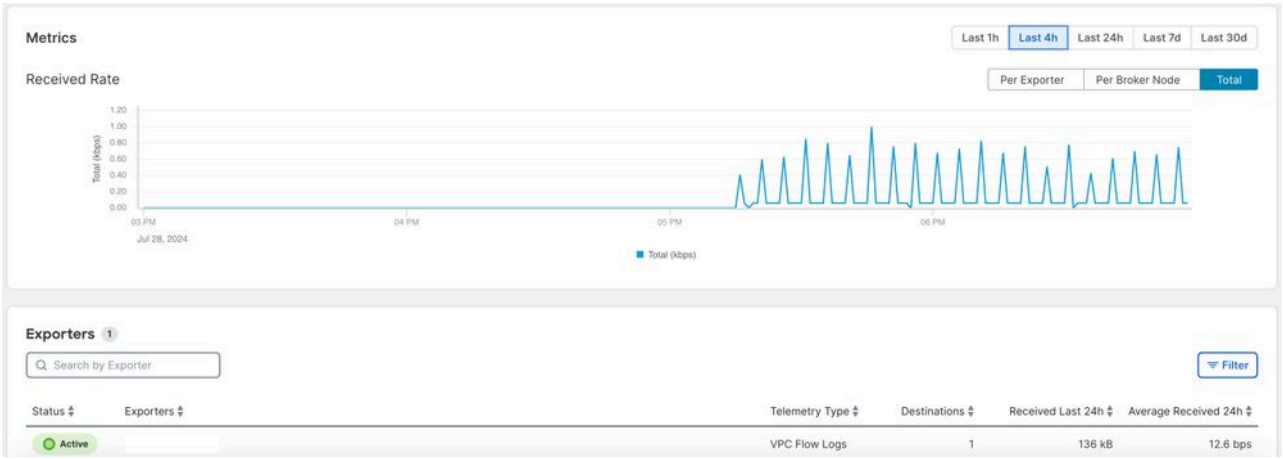
Vérifier

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 versExplorer> 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.


Metrics
Last 1h
Last 4h
Last 24h
Last 7d
Last 30d
Received Rate
Per Exporter
Per Broker Node
Total
1.20
1.00
0.80
0.60
0.40
0.20
0.00
Total (kbps)
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

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.