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.

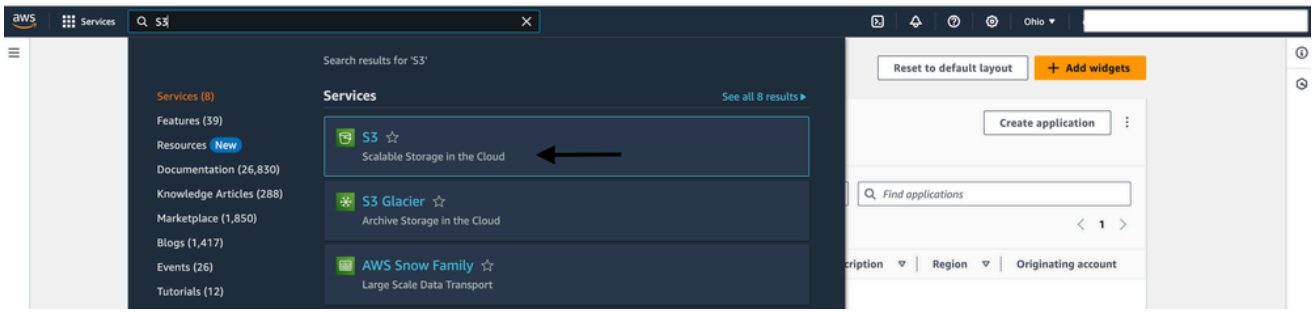
Configuratiestappen

Stap 1. S3-emmer in AWS configureren

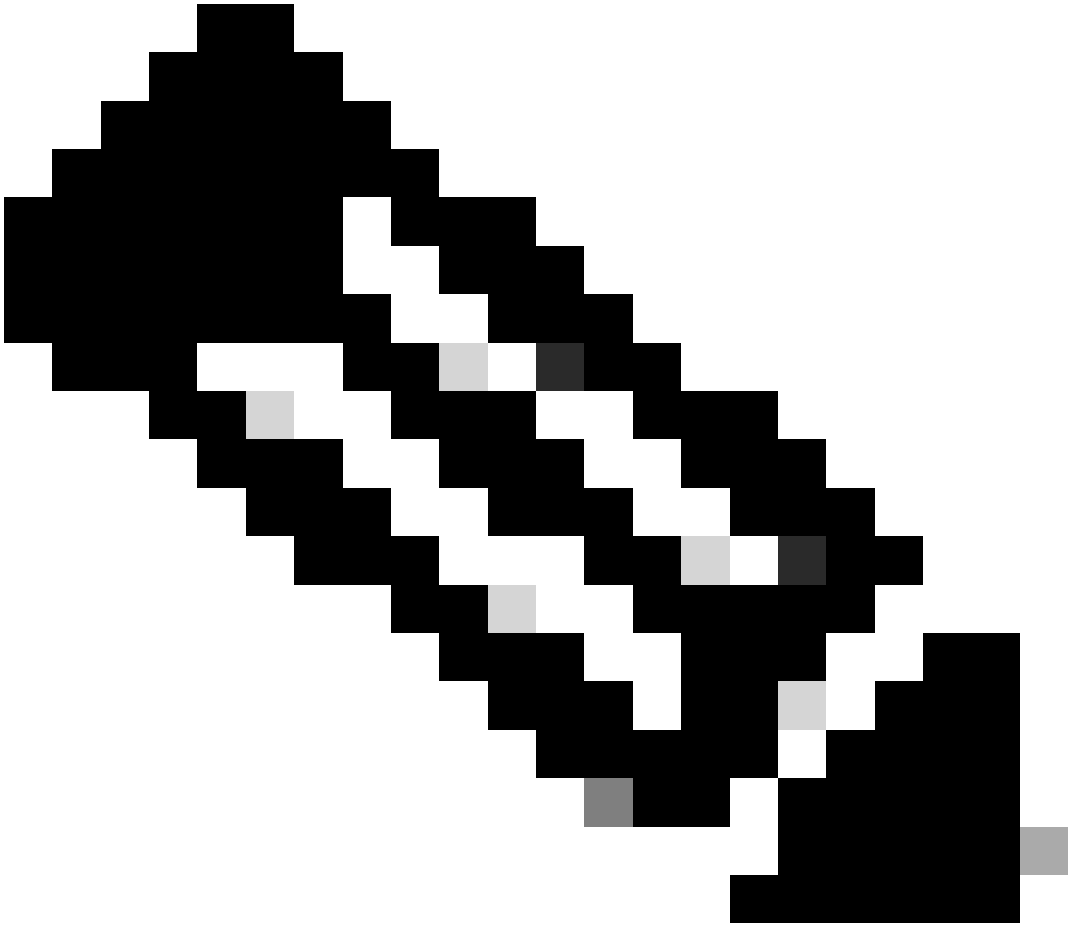
1: Meld u aan bij de AWS-beheerconsole met gebruikersnaam en wachtwoord.

2: Zorg ervoor dat u inlogt bij de juiste regio.

3: Navigeer naar de zoekbalk en typ S3.

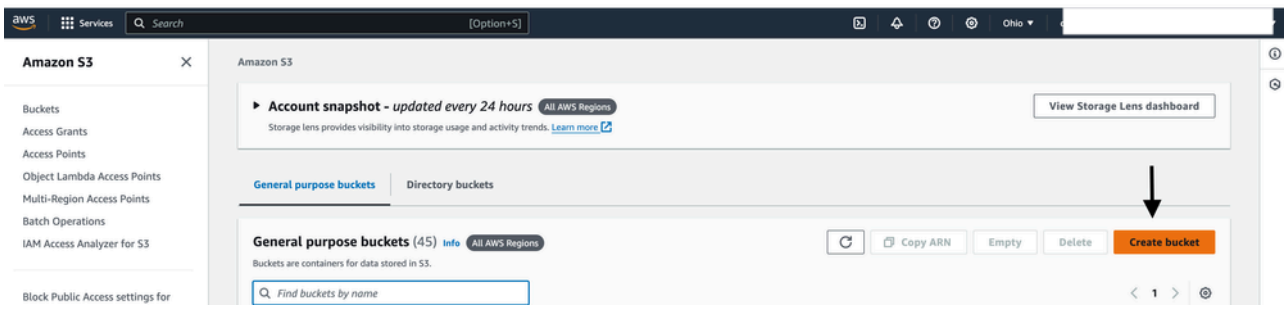


AWS-Dashboard



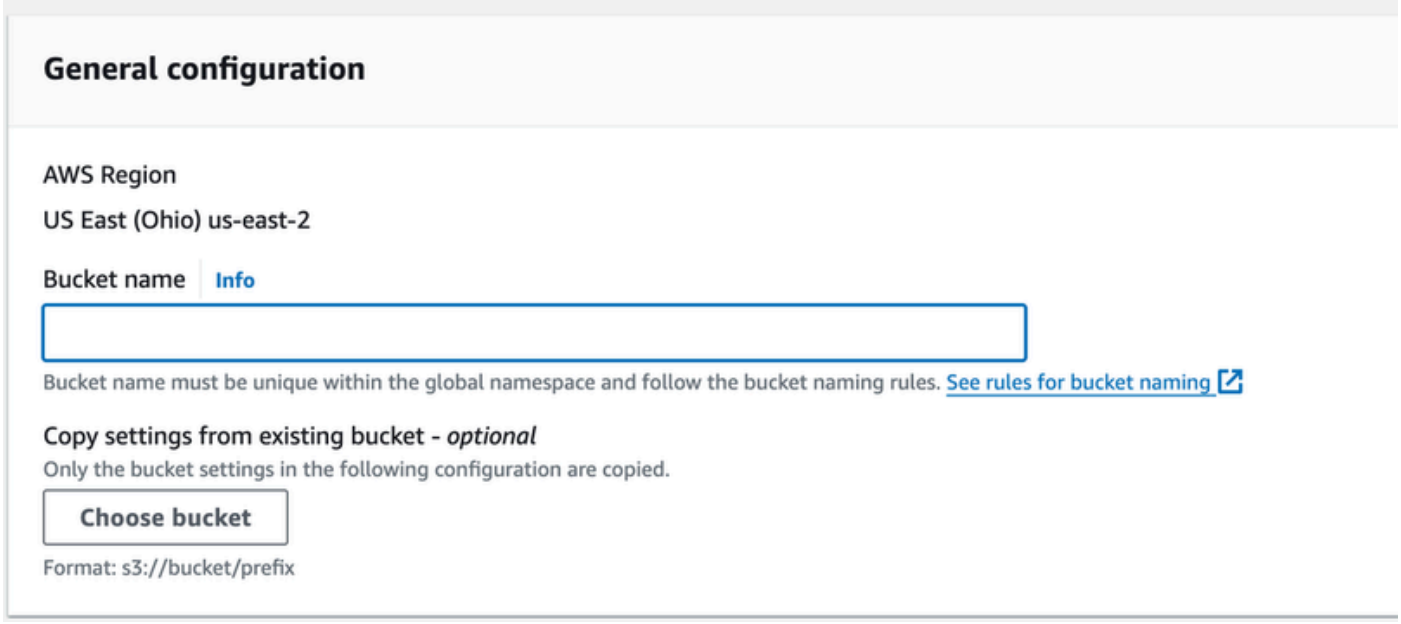
Opmerking: In demo, hebt u geselecteerd Ohio regio met ons-oost-2 beschikbaarheidszone, het is zichtbaar vlak naast het tandwielpictogram.

4: Klik op emmer maken.

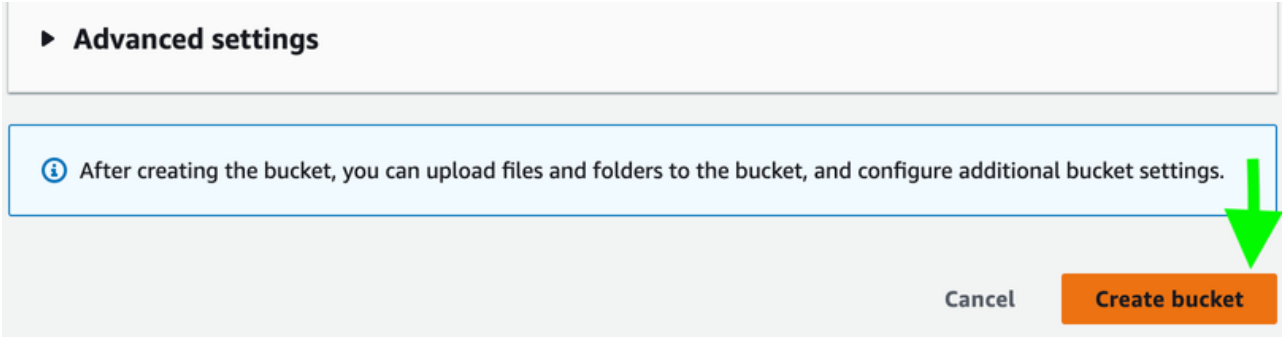


AWS-S3,

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

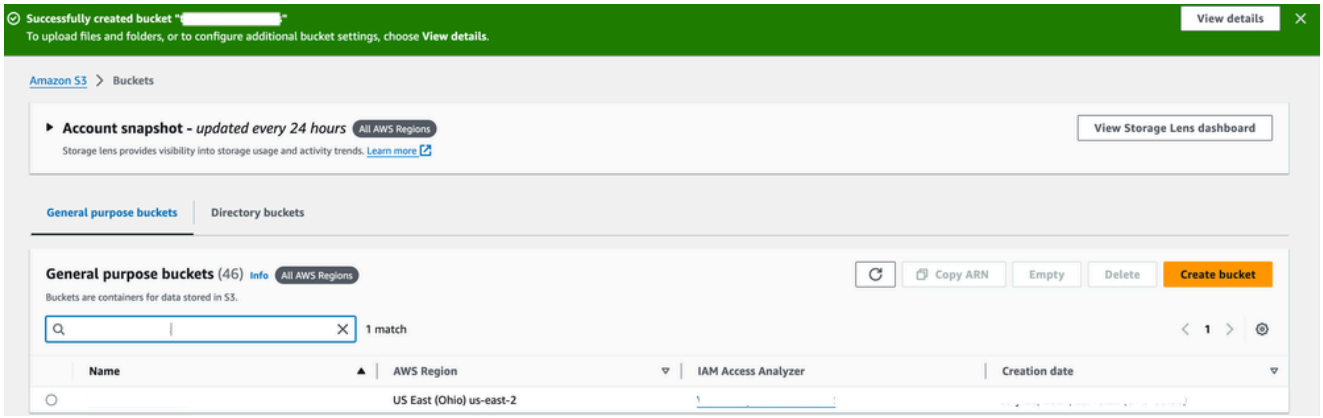


AWS-S3,

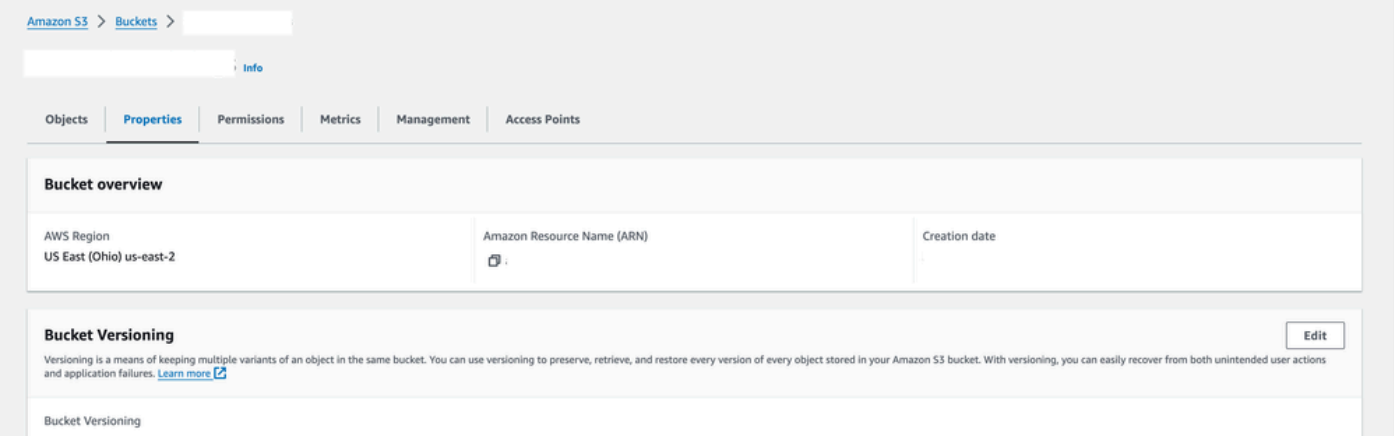


AWS-S3,

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



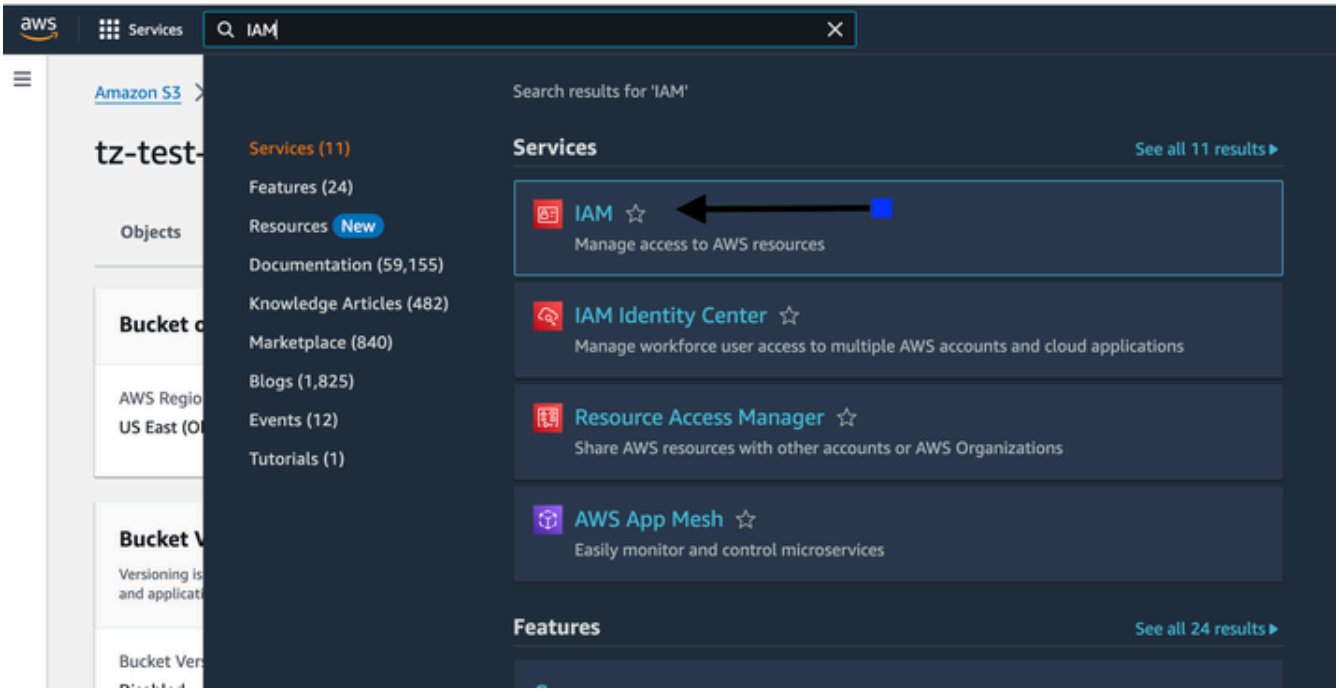
AWS-S3,



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.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

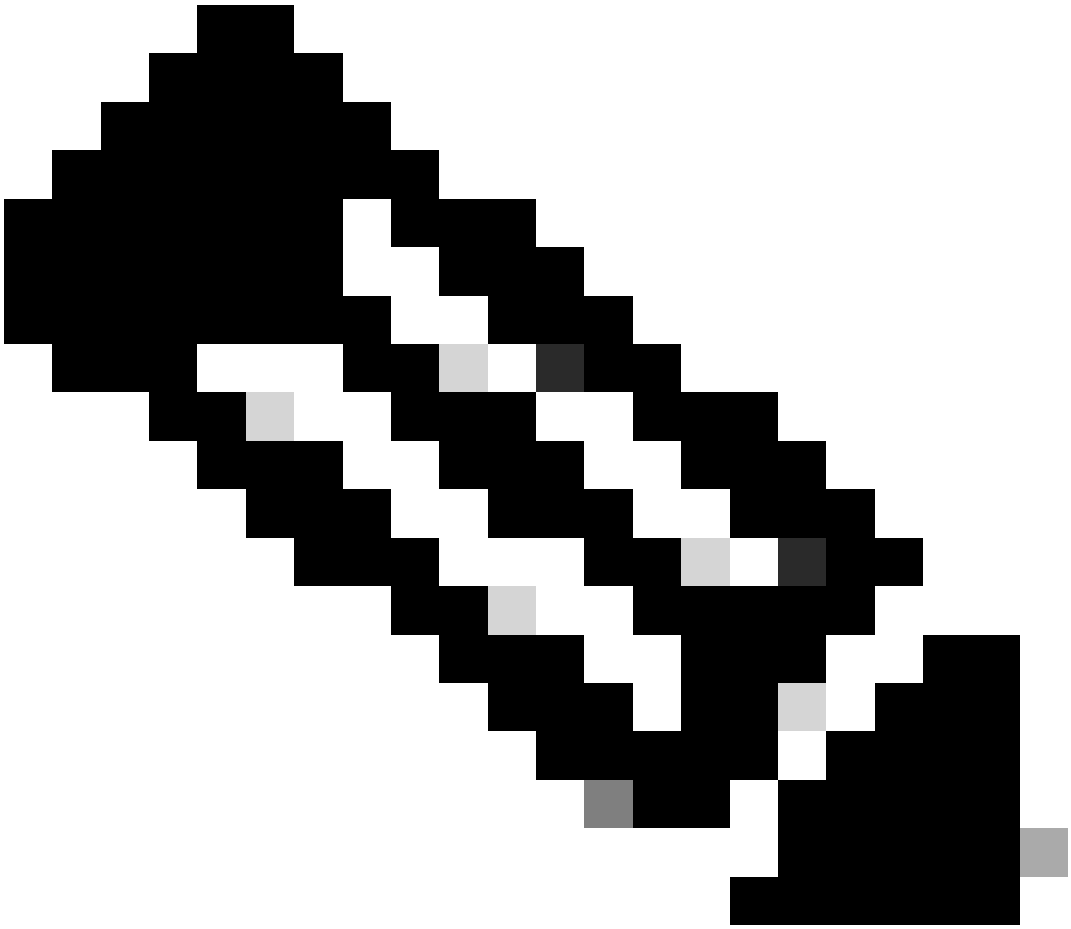
Users

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.

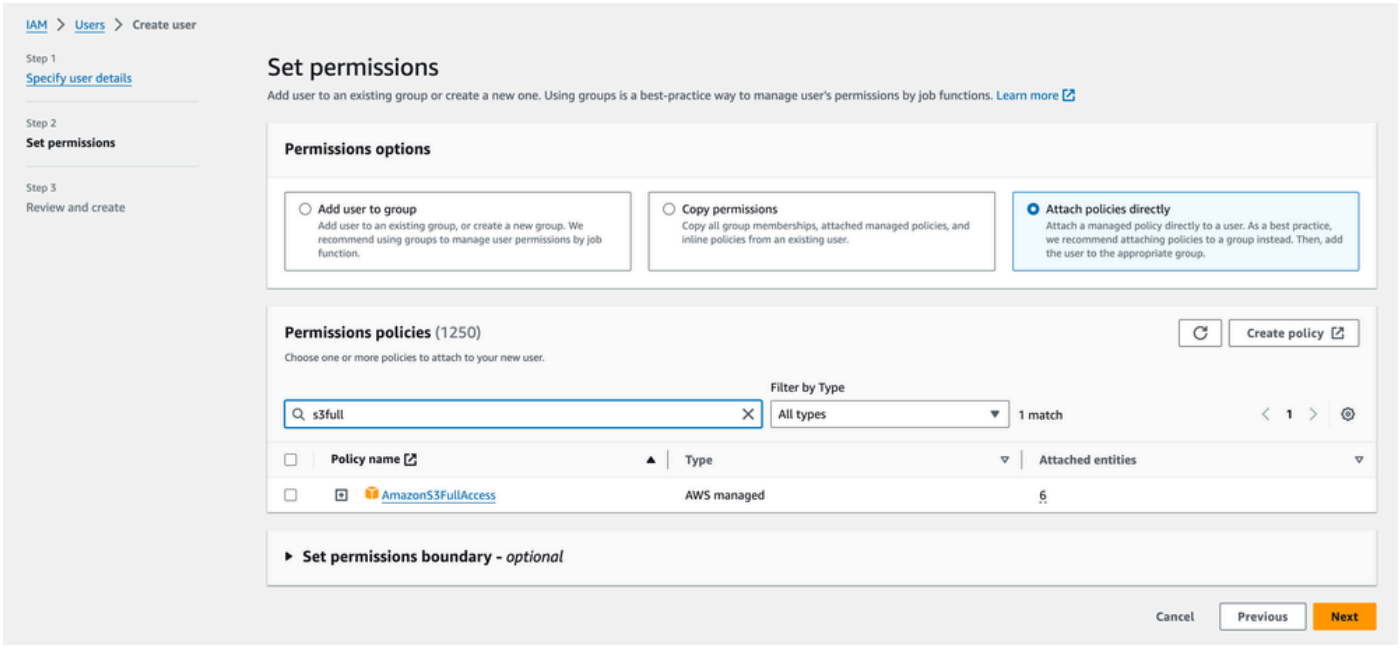


Opmerking: Voor demonstratie, wijst u direct beleid aan de gebruiker toe. Voor meer informatie - AWS-beleid beheren

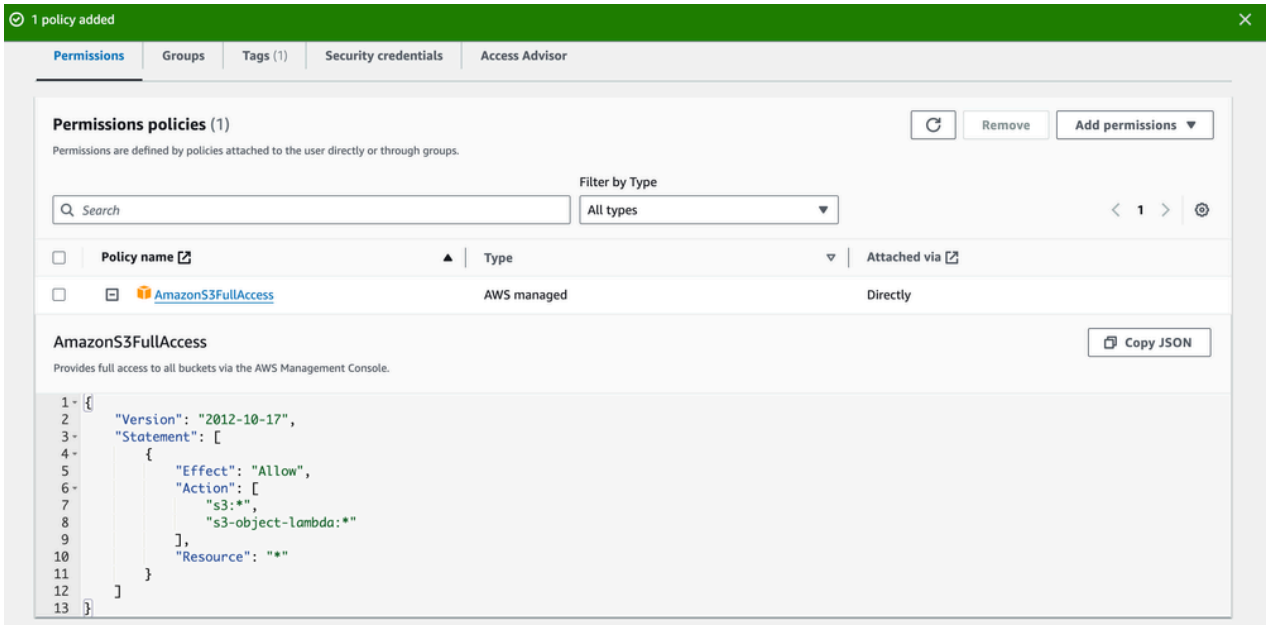
---

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.

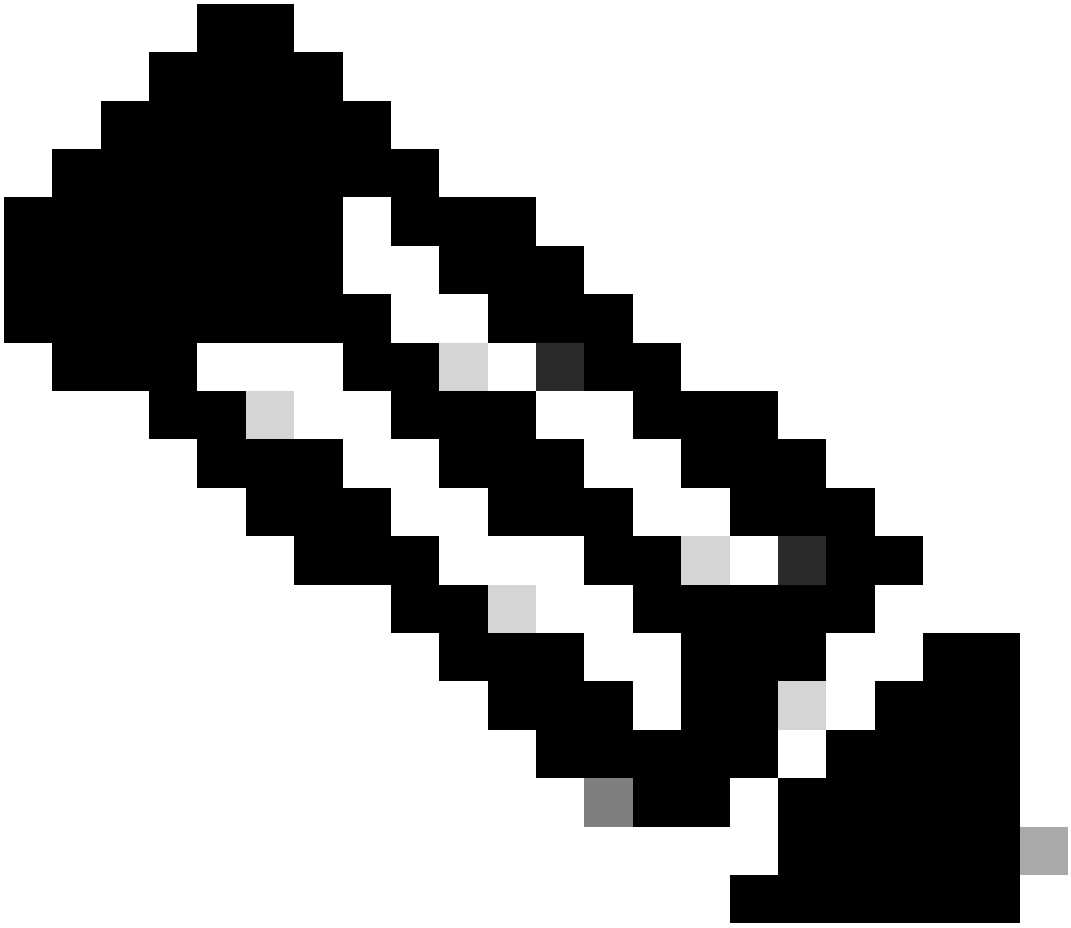
8: Controleer het vakje met de beleidsnaam AmazonS3FullAccess en klik op volgende.



AWS-IAM

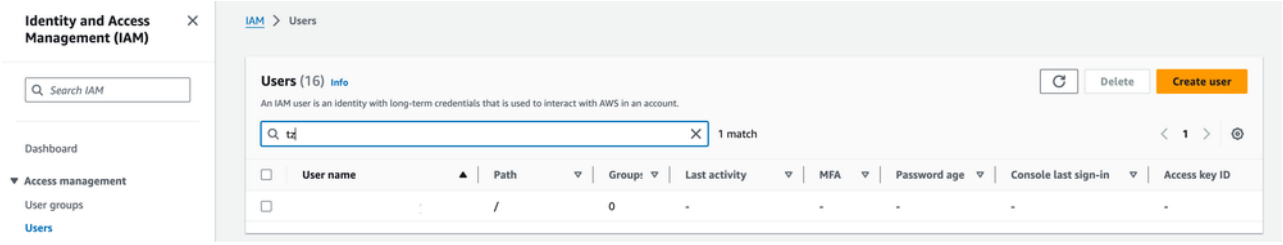


AWS-IAM

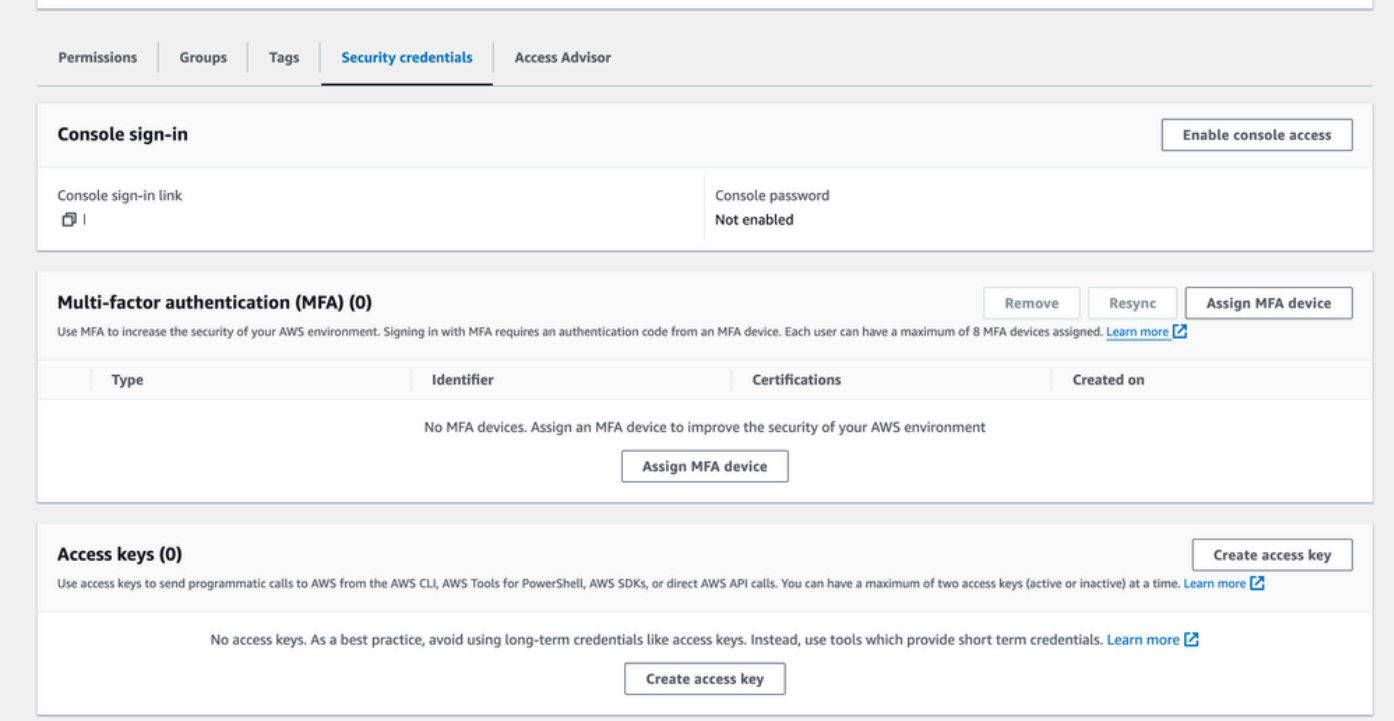


Opmerking: U kunt meer granulair beleid maken door alleen specifieke emmer toe te staan, navigeer naar [Policy creatie] om uw S3 emmer beleid in json-formaat te maken.

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

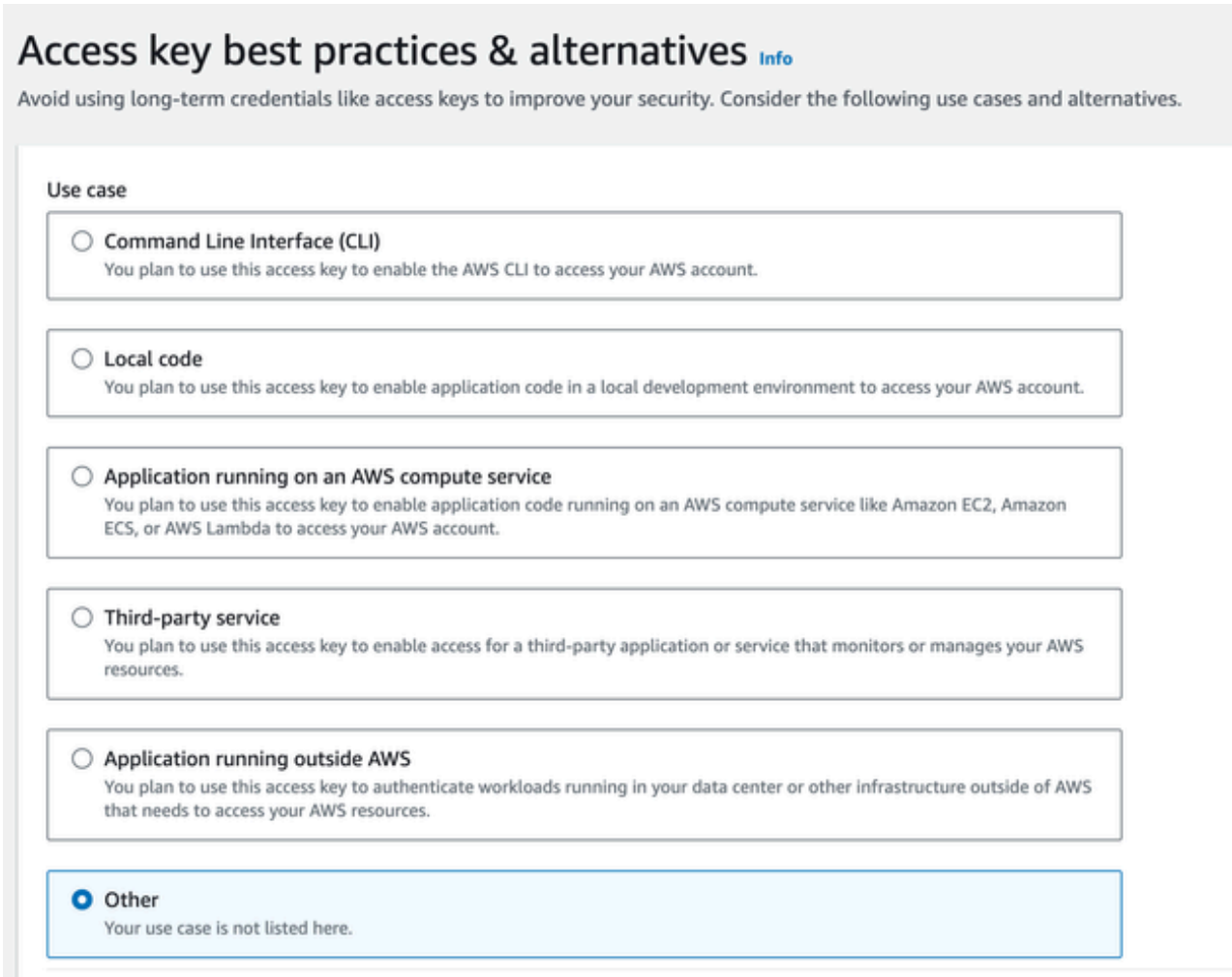


AWS-IAM

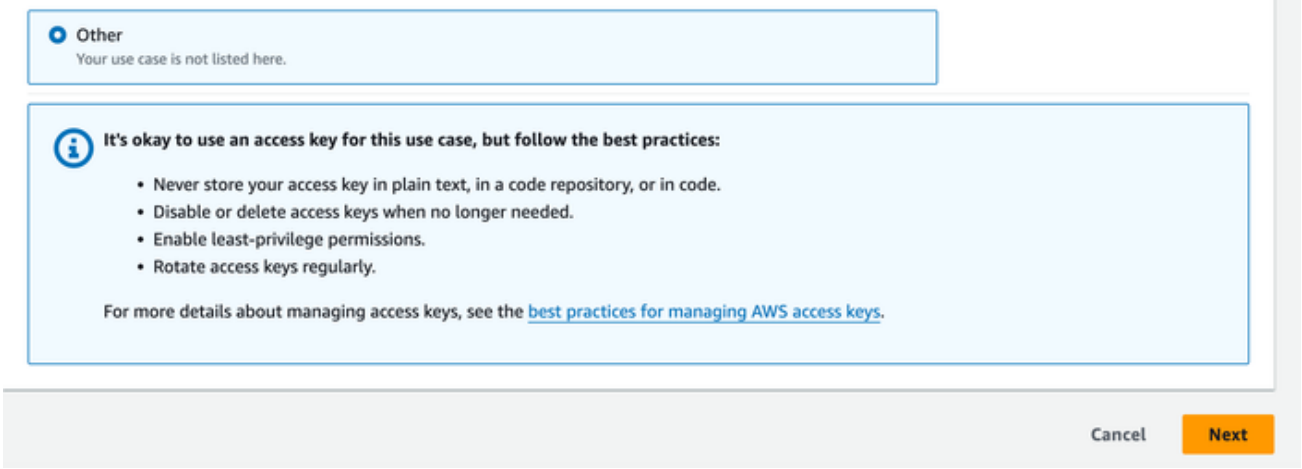


AWS-IAM

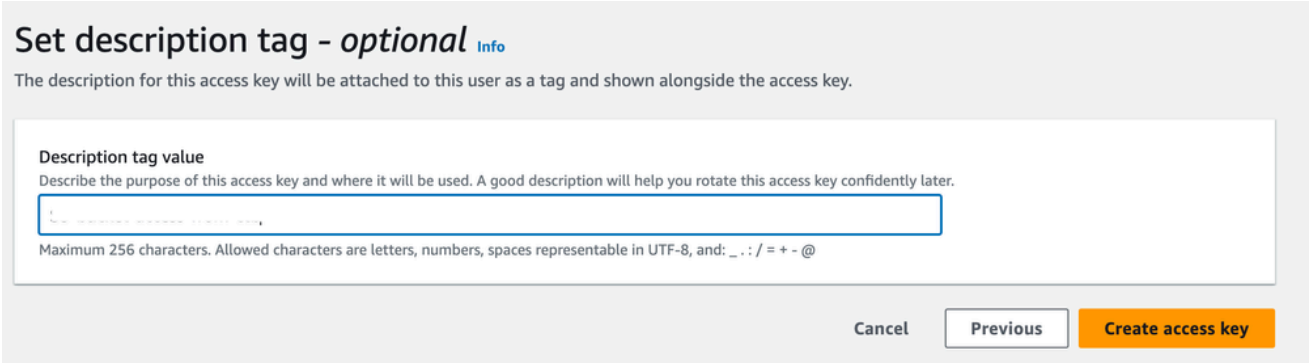
10: Selecteer het andere keuzerondje en voeg eventueel een tag toe.



AWS-IAM

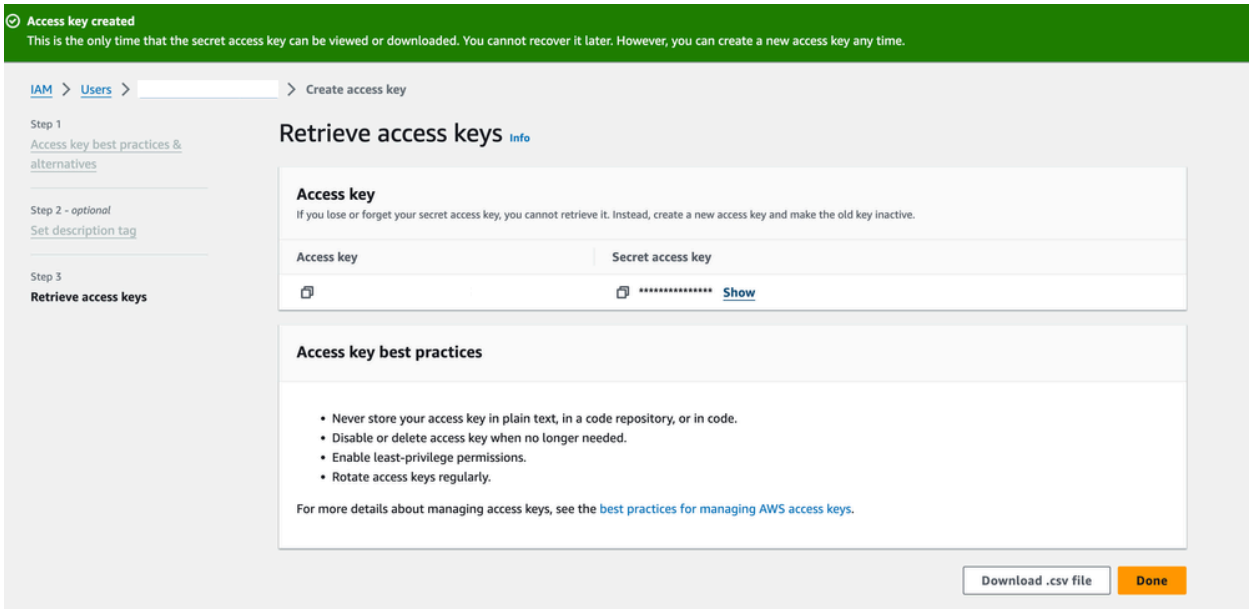


AWS-IAM



AWS-IAM

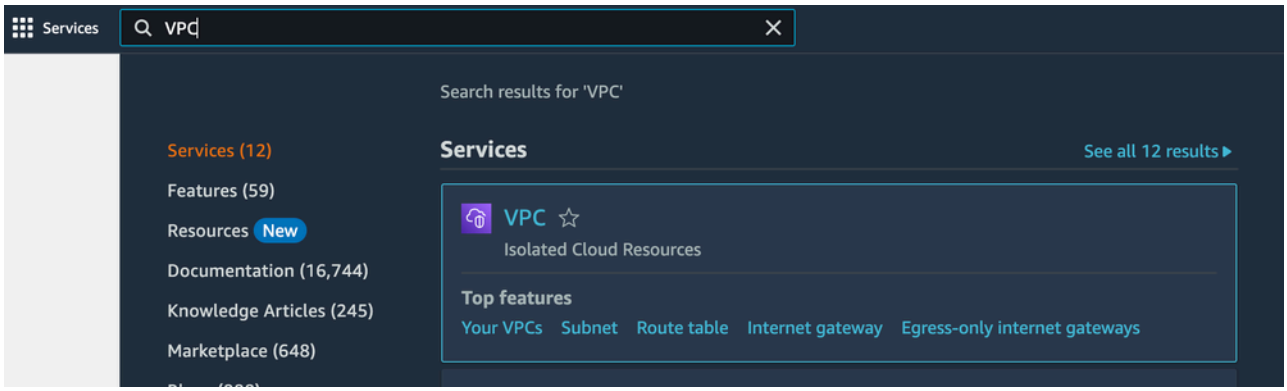
11: Klik op Download .csv-bestand. Dit is de Access-toets in een csv-bestand en het is niet meer beschikbaar om te downloaden of te bekijken zodra u weg van deze pagina navigeert.



AWS-IAM

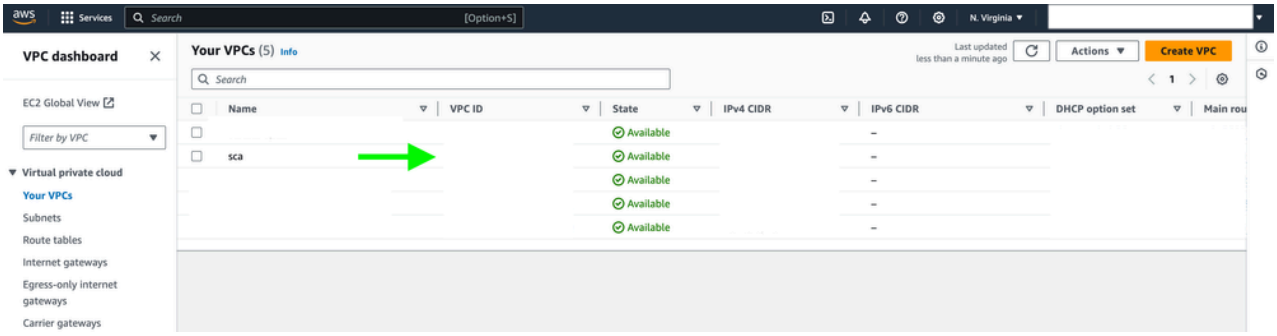
Stap 3. VPC Flow Logs configureren

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

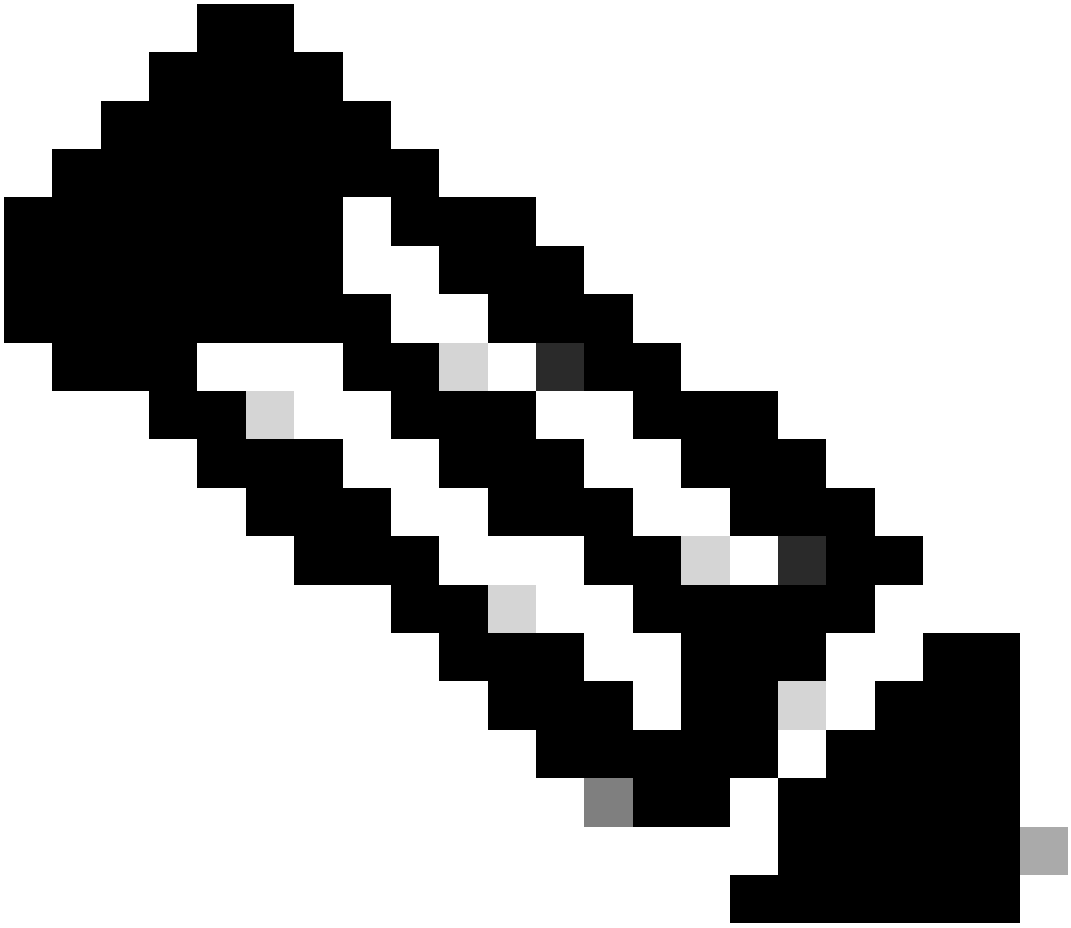


AWS-Flow-logs

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

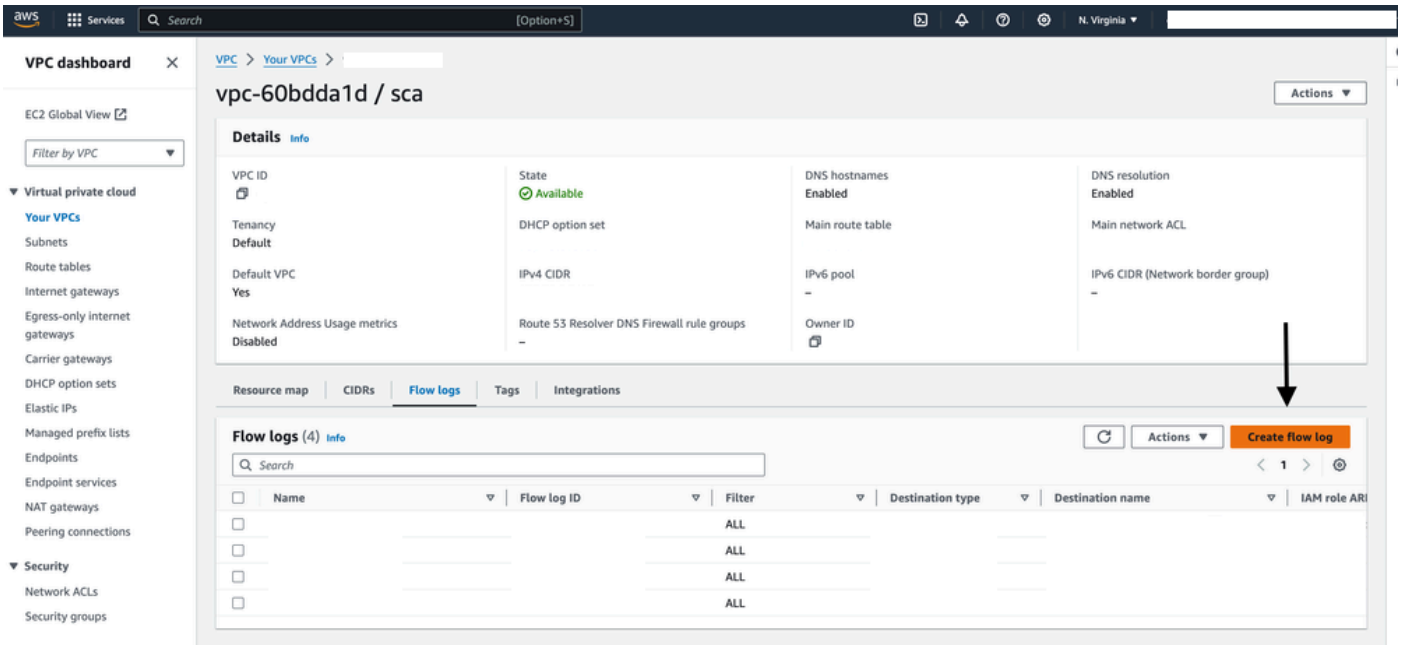


AWS-Flow-logs



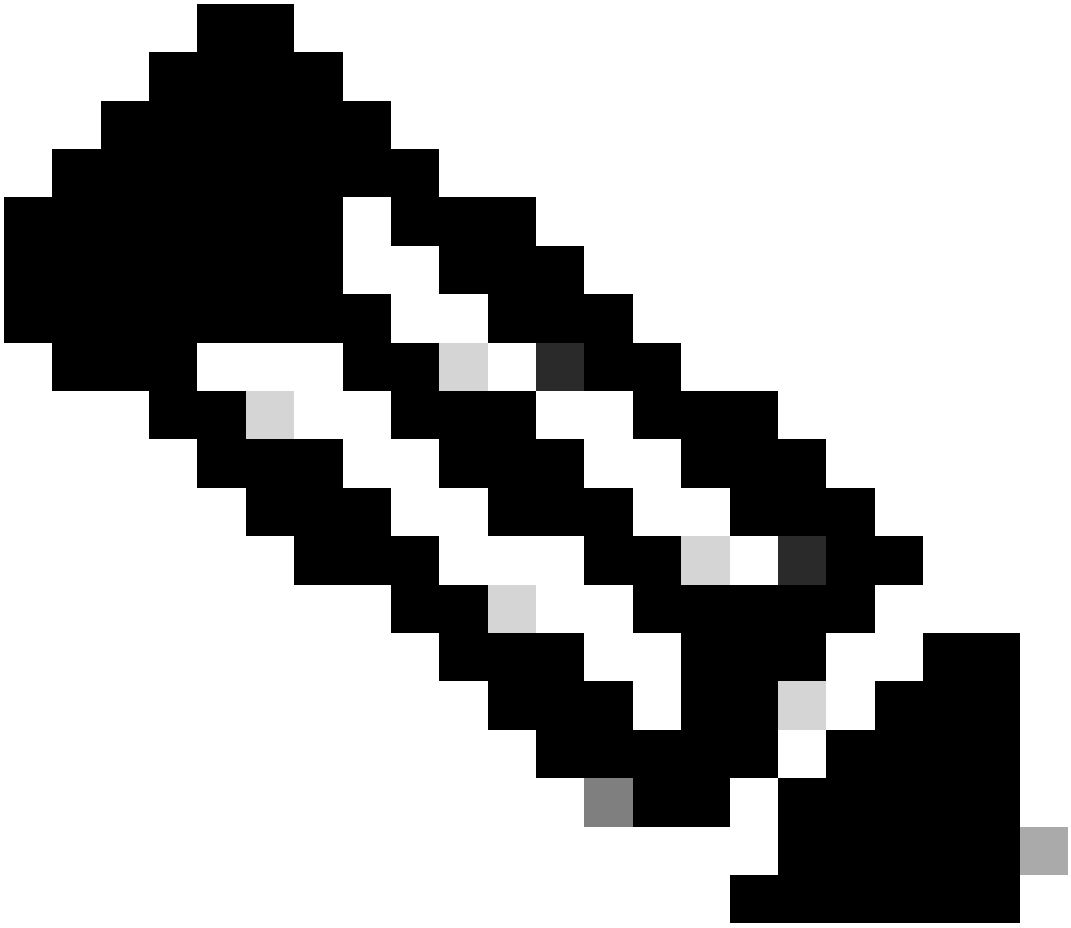
Opmerking: U hebt in deze demo de naam SCA van VPC geselecteerd.

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



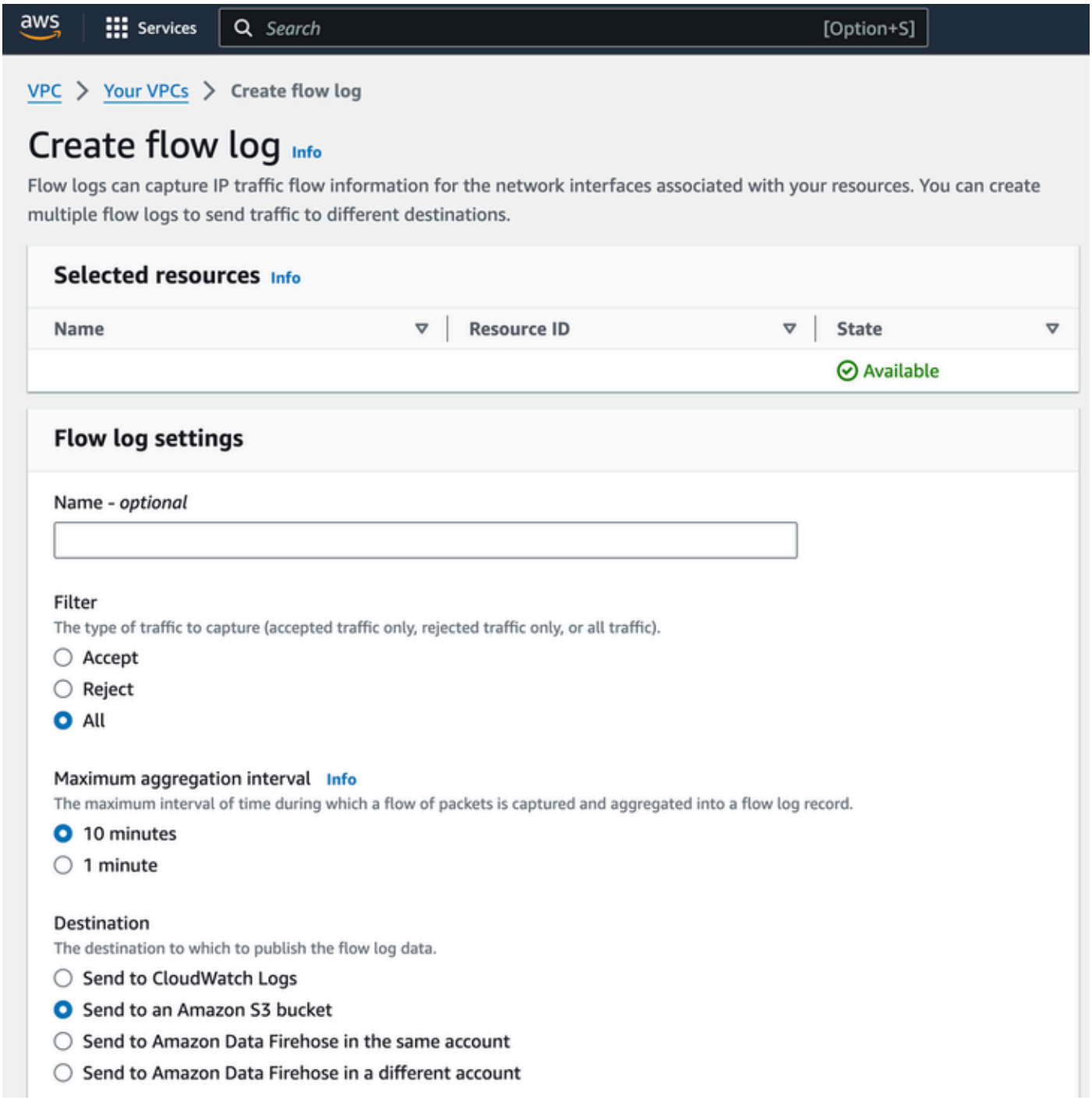
AWS-Flow-logs

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

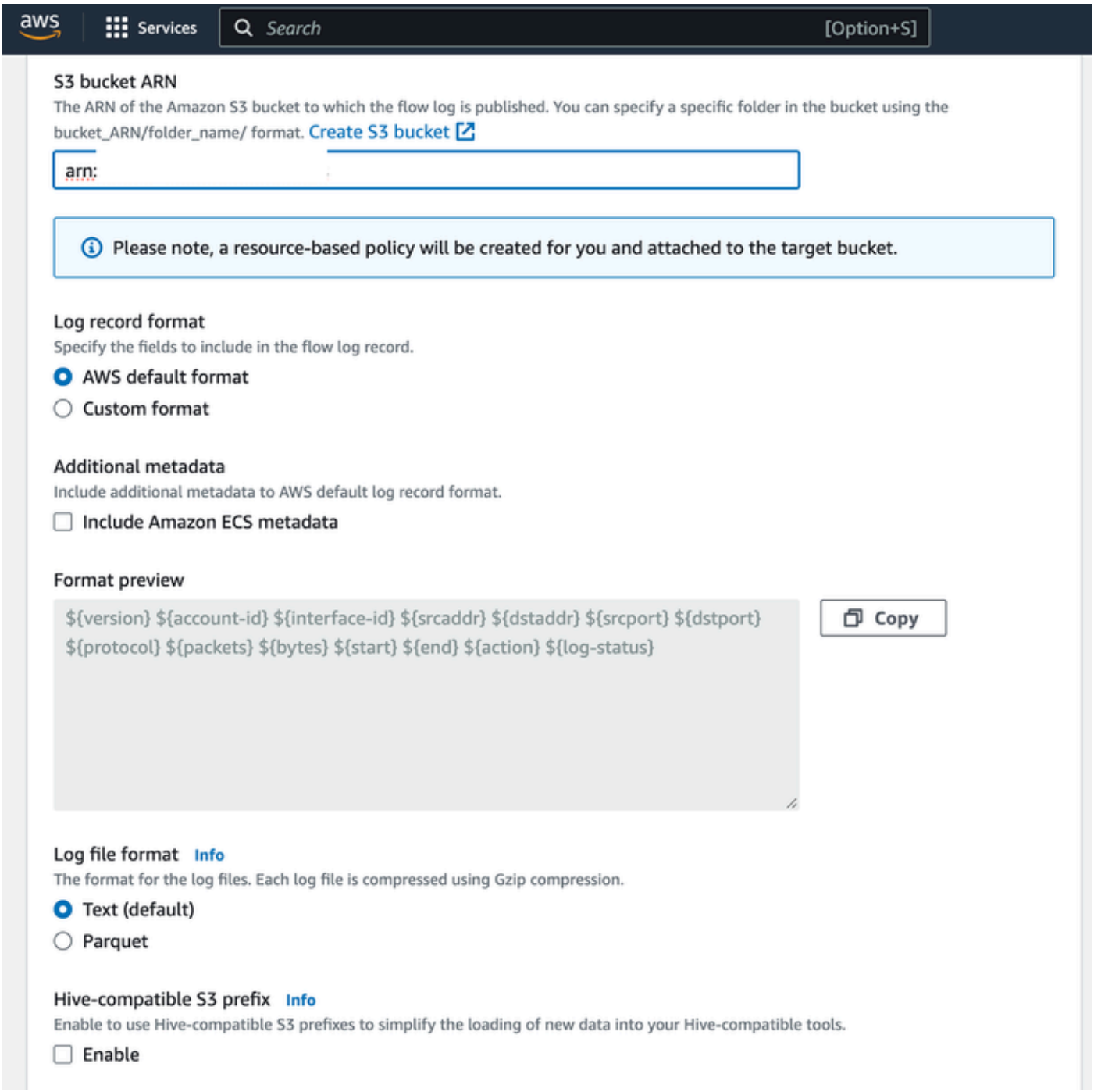


Opmerking: Zie S3-emmer configureren voor ARN - Stap 6

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.

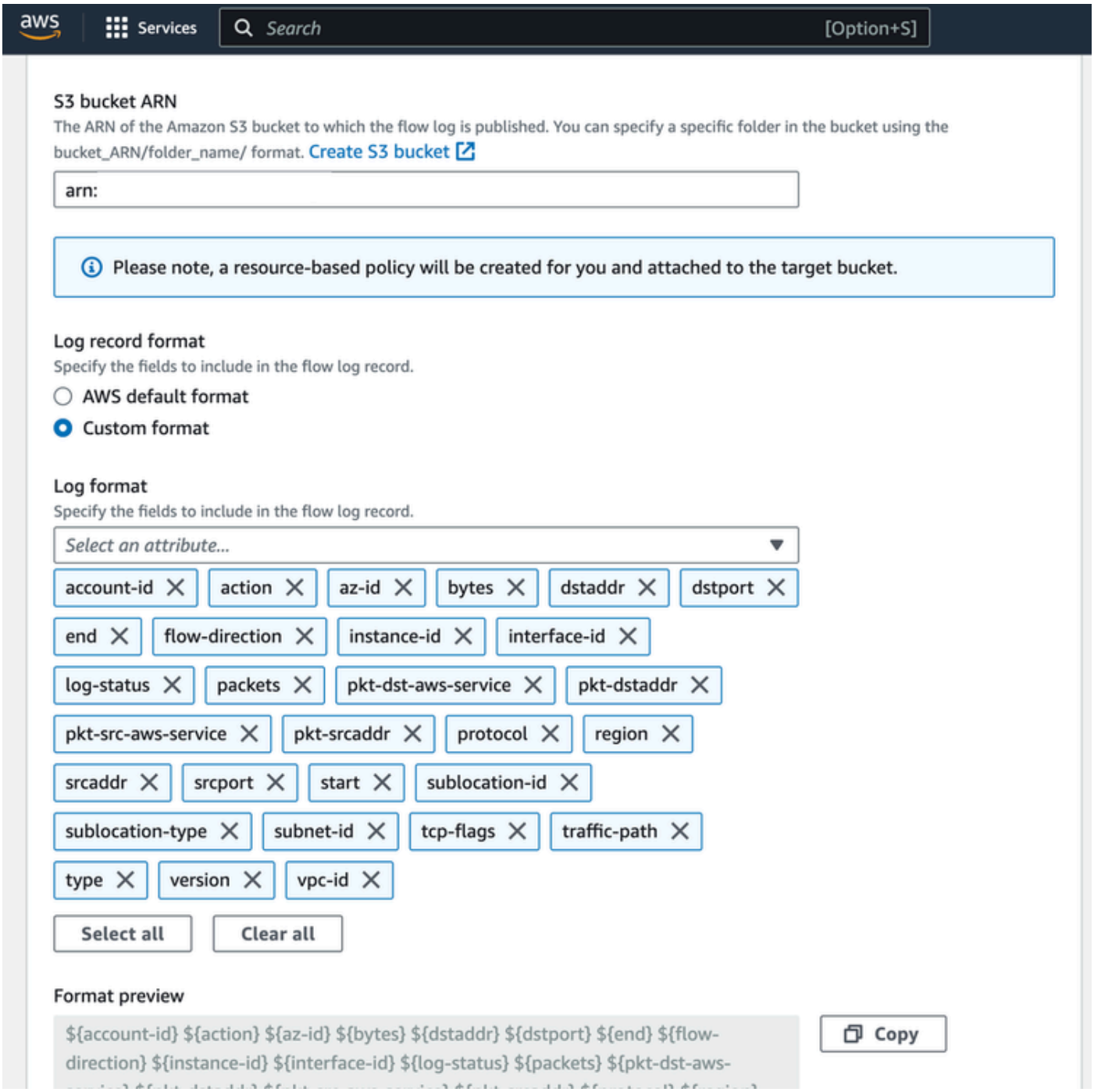


AWS-Flow-logs

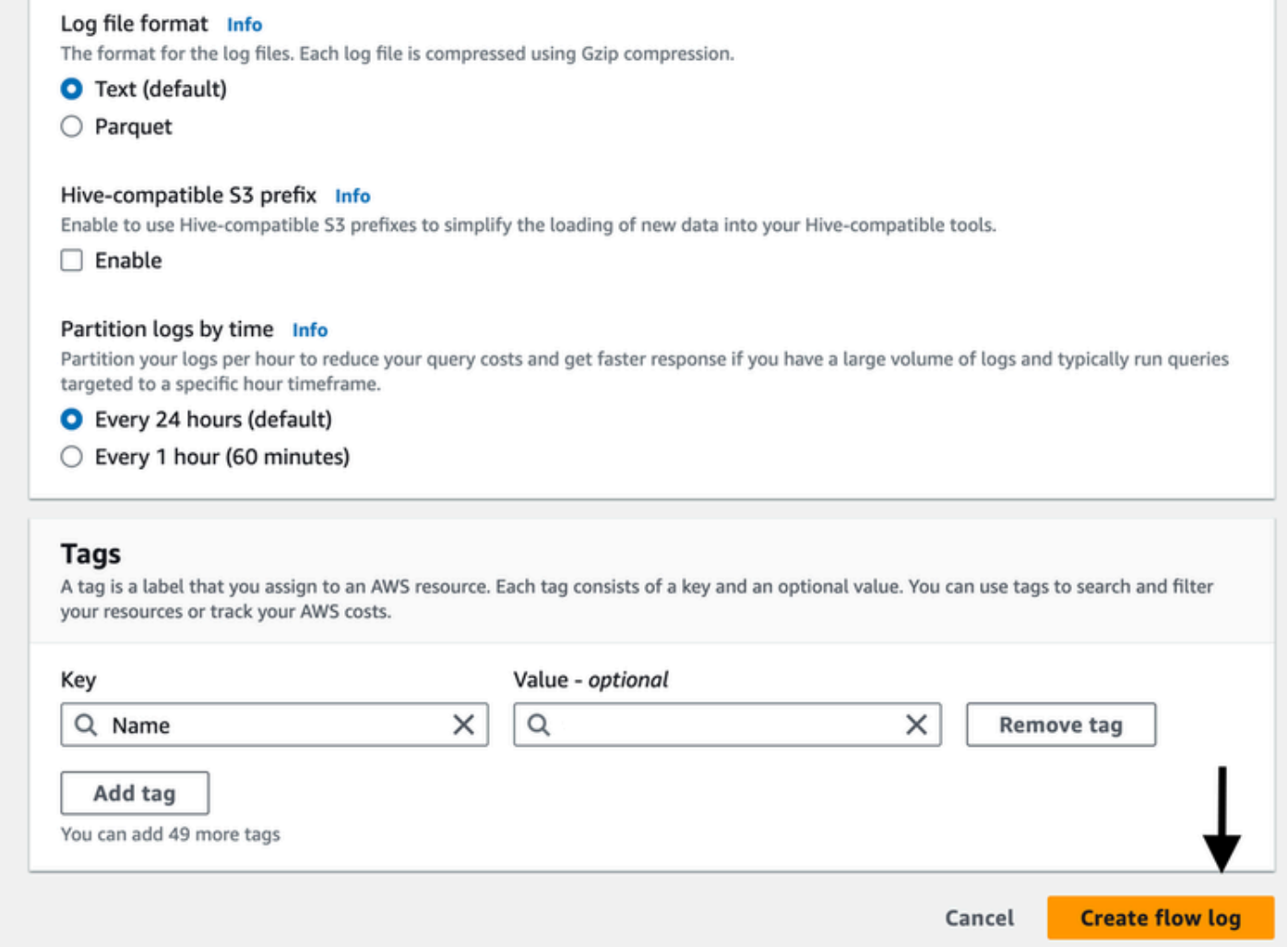


AWS-Flow-logs

7: Klik op Stroomlogboeken maken.



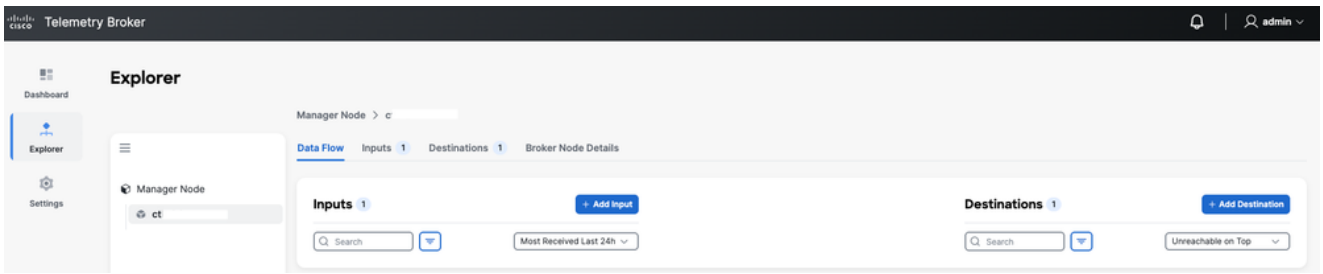
AWS-Flow-logs



AWS-Flow-logs

Stap 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

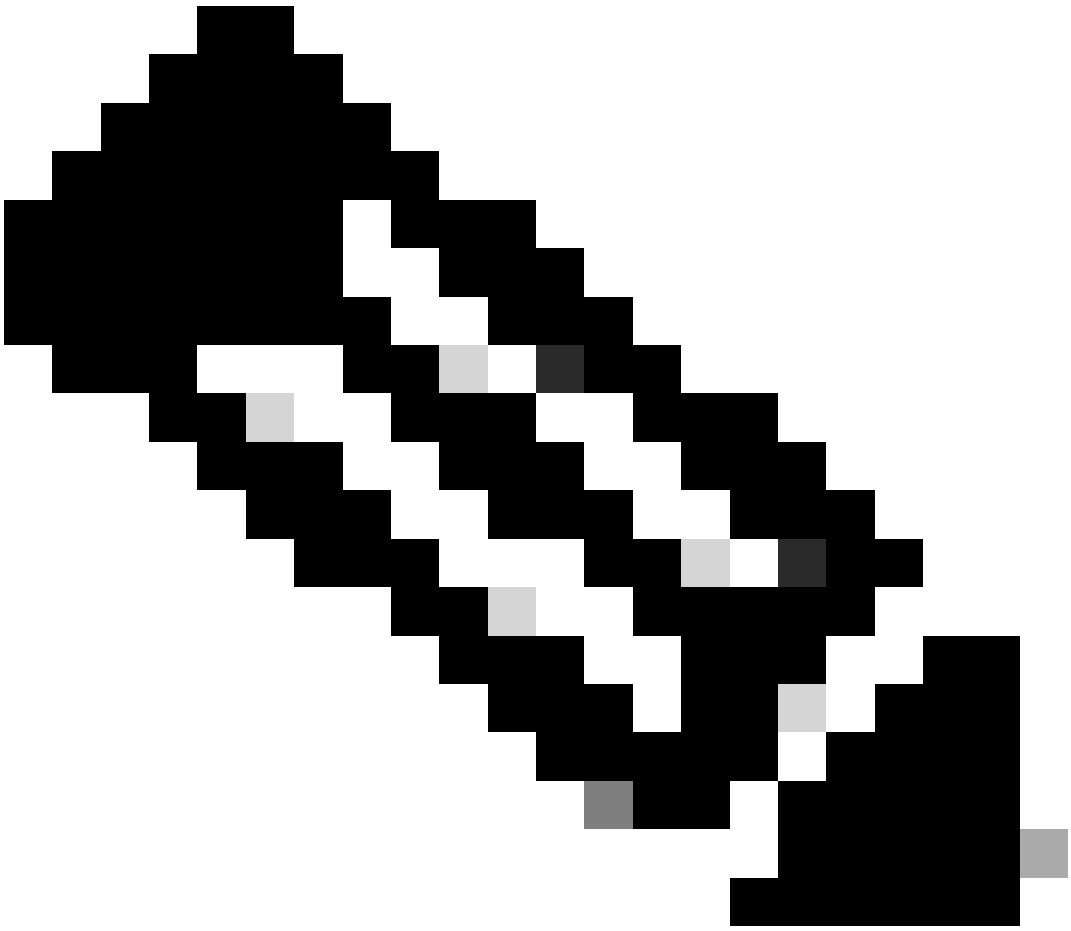
AWS VPC Flow log

AWS VPC Flow log

Azure NSG Flow log

Flow Generator Input

: 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

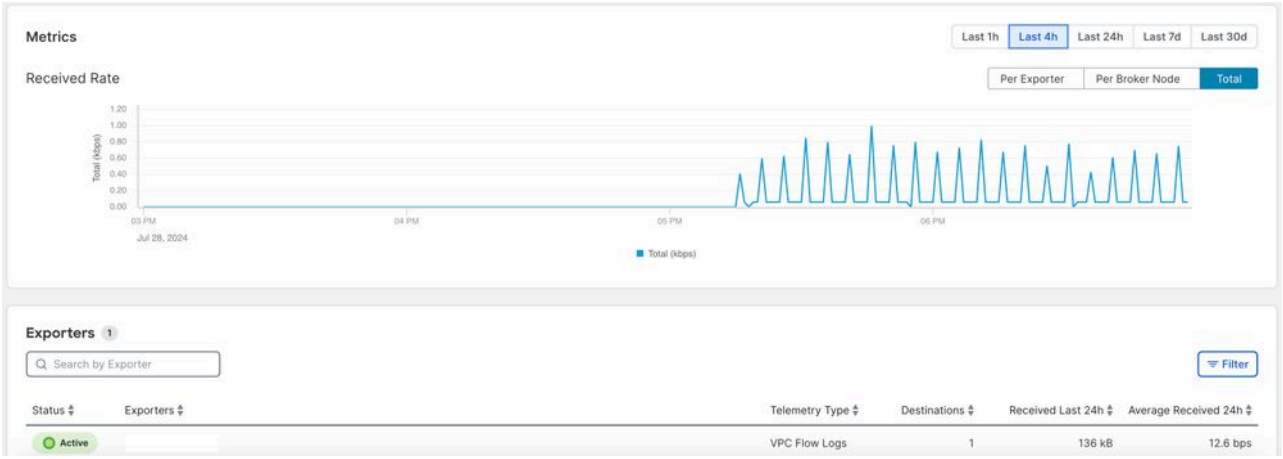
Verifiëren

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 naarVerkenner> 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.