AWS VPC-Flussprotokolle für CTB-Eingabe konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie VPC Flow Logs als Eingabe für Cisco Telemetry Broker (CTB) konfiguriert werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- CTB (v2.2.1+)
- AWS

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

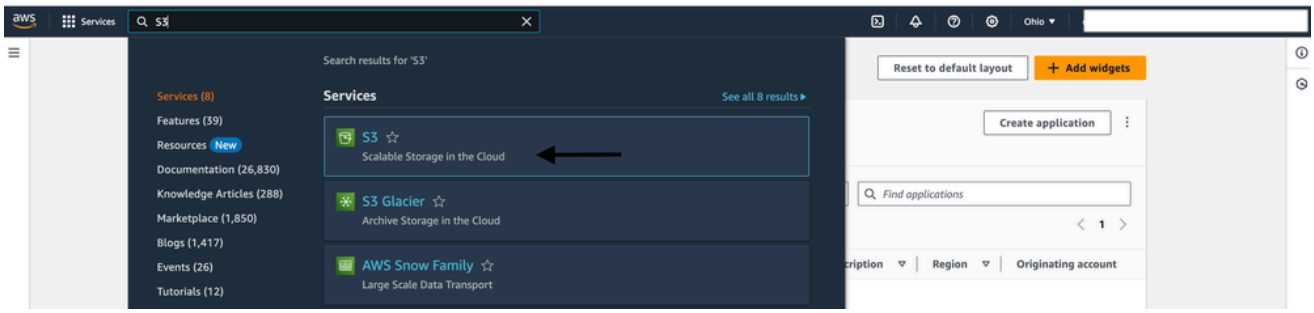
Konfigurationsschritte

Schritt 1: Konfigurieren von S3 Bucket in AWS

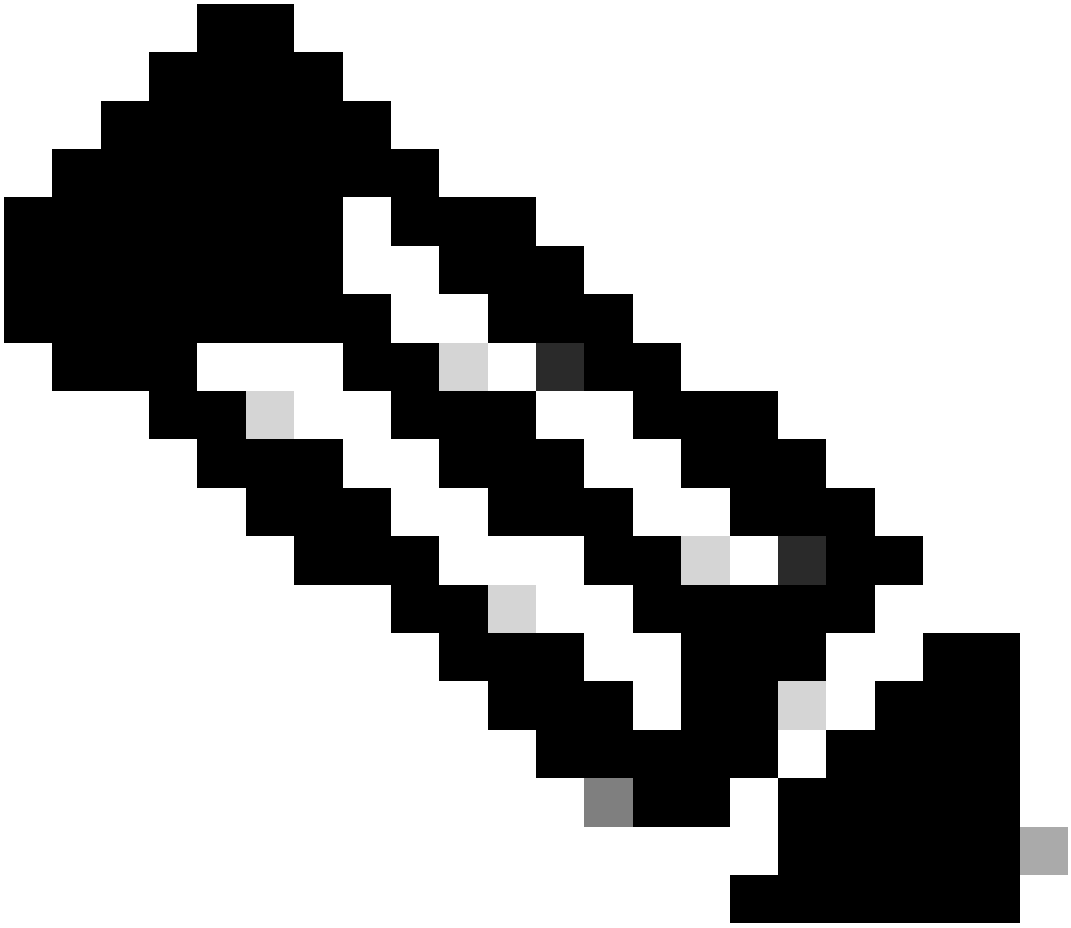
1: Melden Sie sich mit Benutzername und Kennwort bei der AWS-Verwaltungskonsole an.

2: Stellen Sie sicher, dass Sie sich bei der entsprechenden Region anmelden.

3: Navigieren Sie zur Suchleiste, und geben Sie S3 ein.

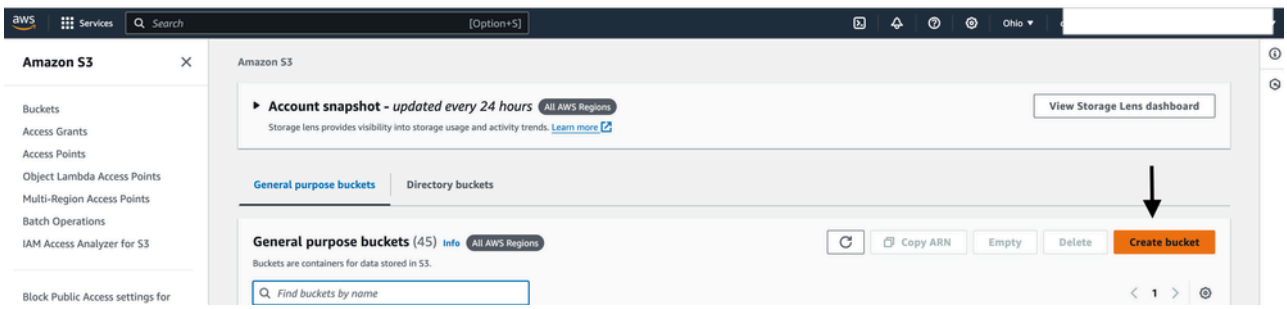


AWS-Dashboard



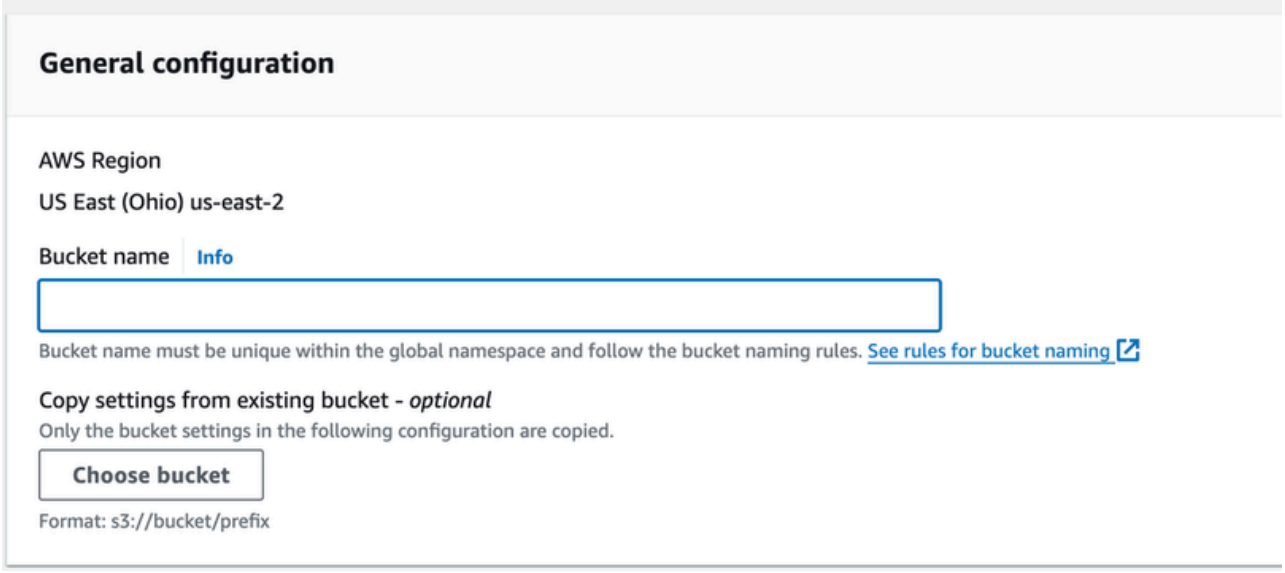
Anmerkung: In der Demo haben Sie Ohio Region mit us-east-2 Verfügbarkeitszone ausgewählt, sie ist direkt neben dem Zahnrad-Symbol zu sehen.

4: Klicken Sie auf Bucket erstellen.

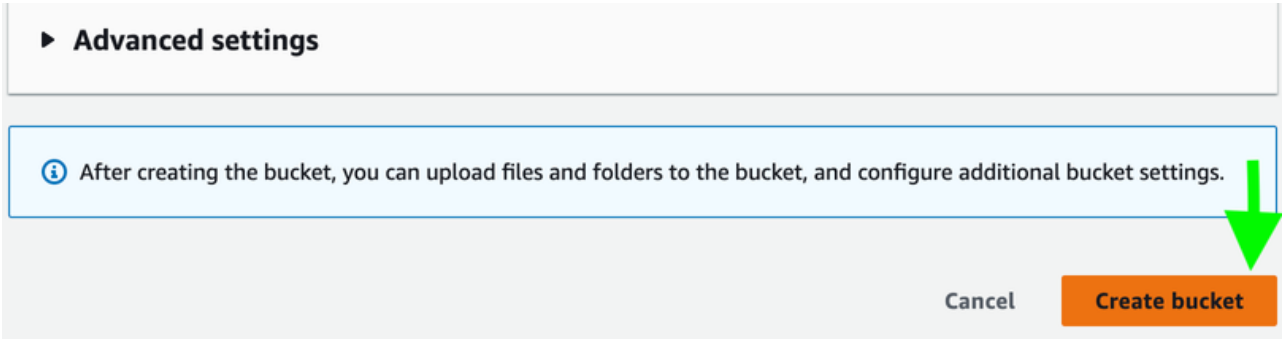


AWS-S3

5: Geben Sie bucket einen Namen und lassen Sie alle Optionen unverändert, und klicken Sie auf Erstellen.

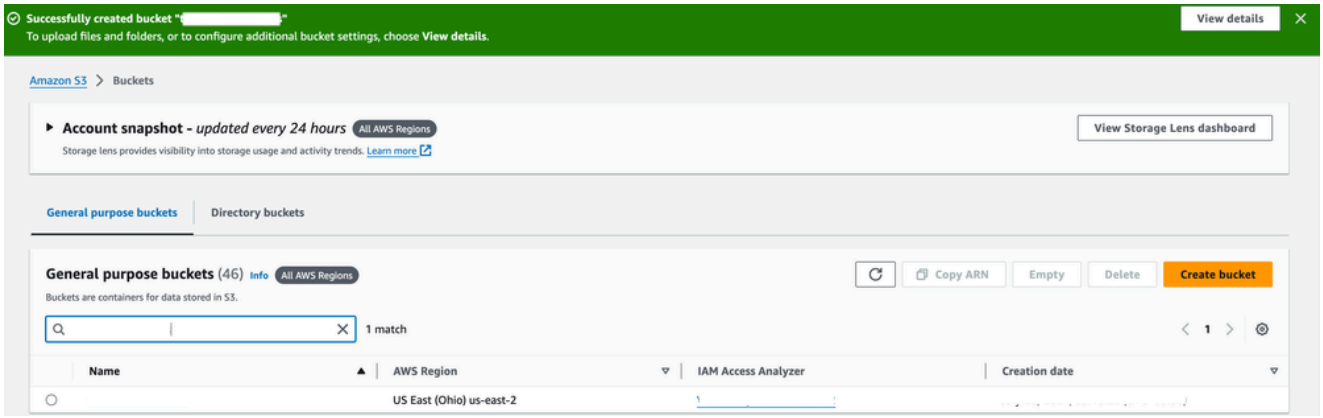


AWS-S3

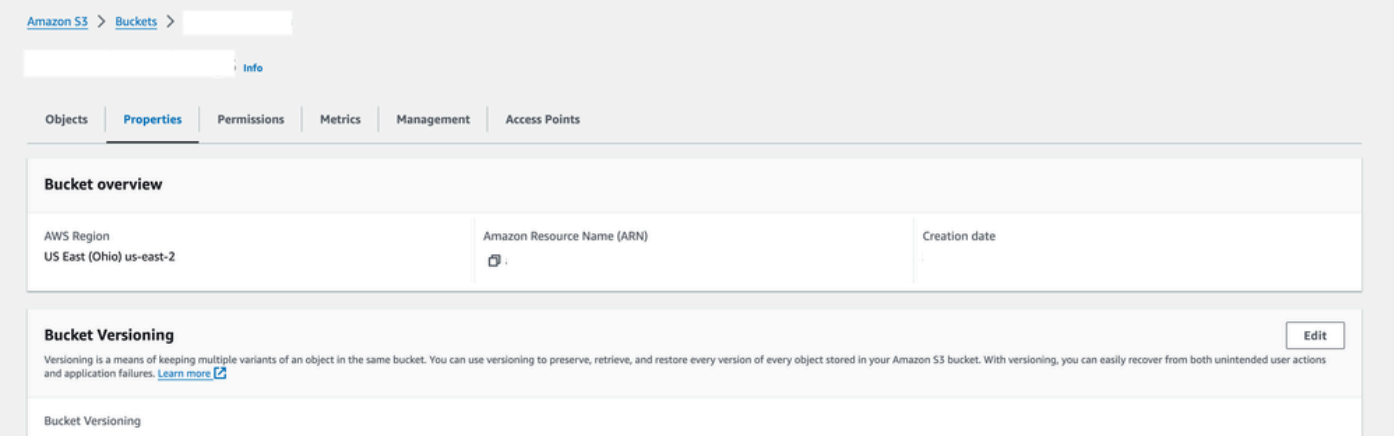


AWS-S3

6: Speichern Sie nach der erfolgreichen Erstellung des Buckets den Bucket-ARN, der später während der Konfiguration verwendet werden soll.



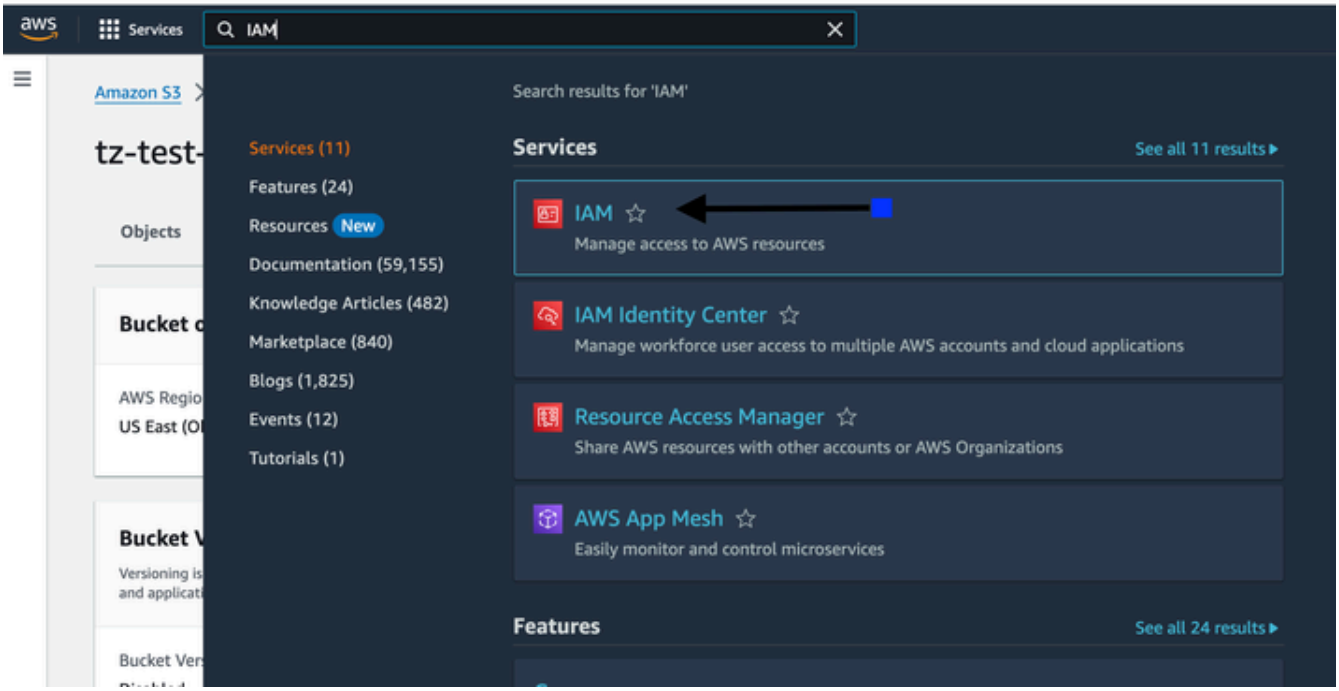
AWS-S3



AWS-S3

Schritt 2: IAM-Benutzer mit Zugriffsschlüssel erstellen und S3-Bucket-Richtlinie anhängen

1: Starten Sie die IAM über die AWS-Suchleiste.



AWS-IAM

2: Navigieren Sie zu Benutzern.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

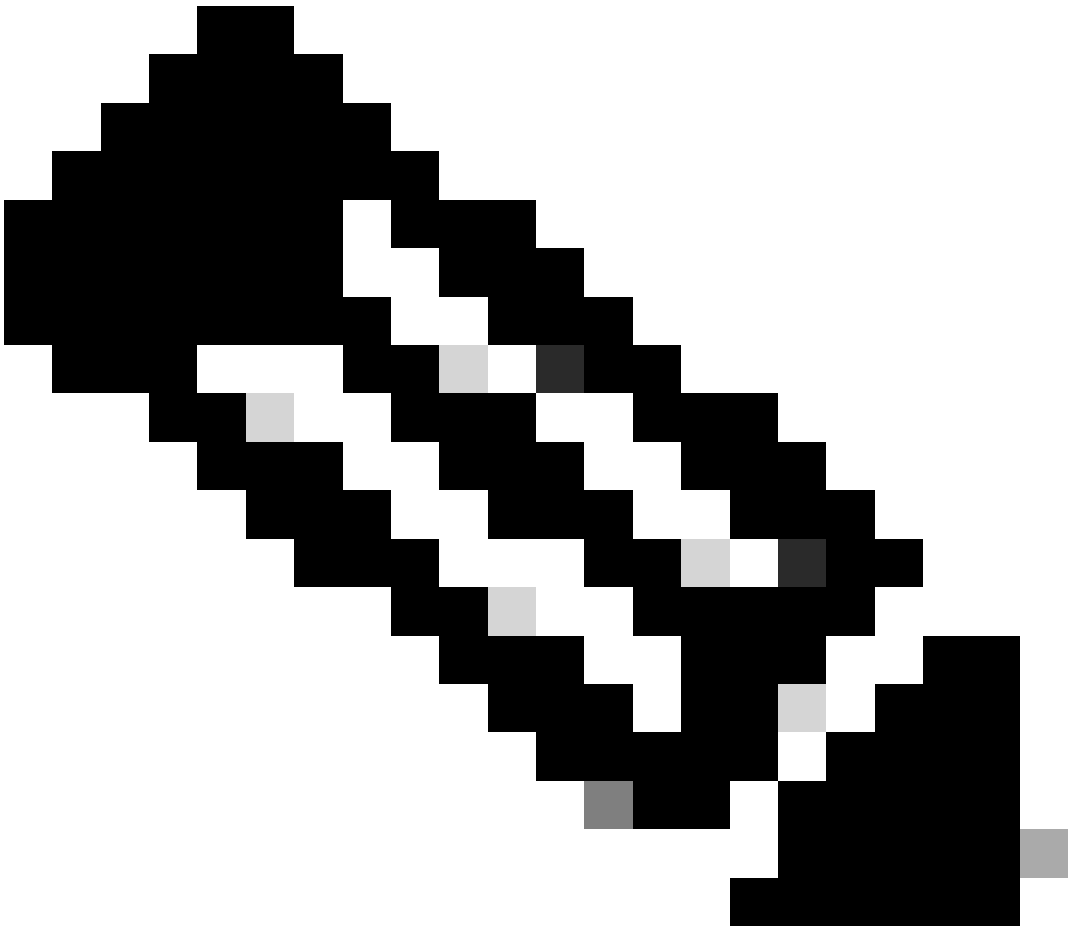
Users

Roles

Policies

Durch die Deaktivierung des Zugriffsfelds für die AWS-Verwaltungskonsole wird verhindert, dass sich der Benutzer über die Webbenutzeroberfläche beim AWS-Konto anmeldet.

6: Weisen Sie eine Richtlinie zu, indem Sie sie dem Benutzer zuweisen, einer Gruppe direkt hinzufügen oder inline konfigurieren.

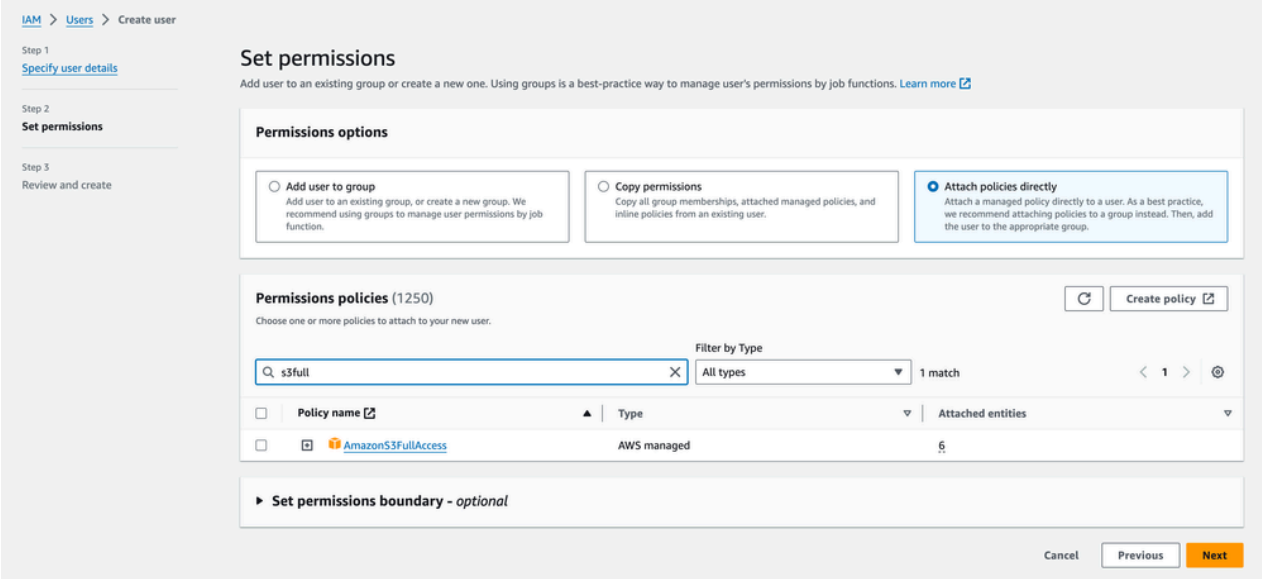


Anmerkung: Zu Demonstrationszwecken weisen Sie dem Benutzer direkt Richtlinien zu. Weitere Informationen - Verwalten von AWS-Richtlinien

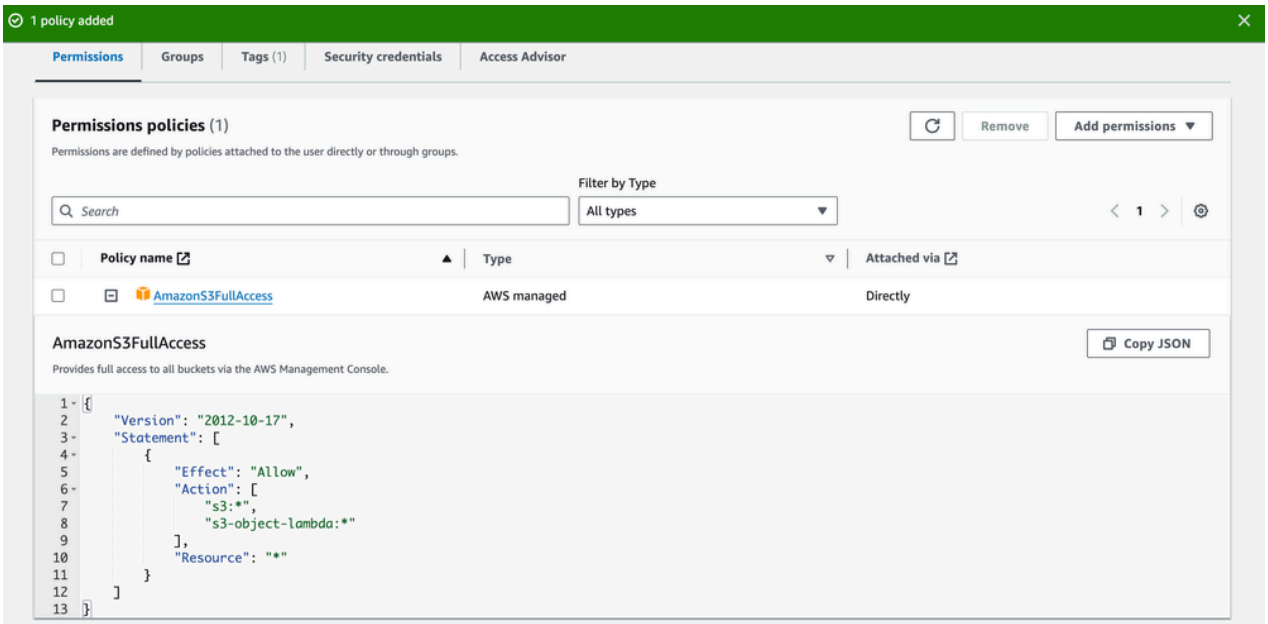
---

7: Suchen Sie nach S3 Full Access und wählen Sie AmazonS3Full Access aus, wodurch der Benutzer vollen Zugriff für jeden S3-Bucket hat, der auf seinem entsprechenden AWS-Konto erstellt wurde.

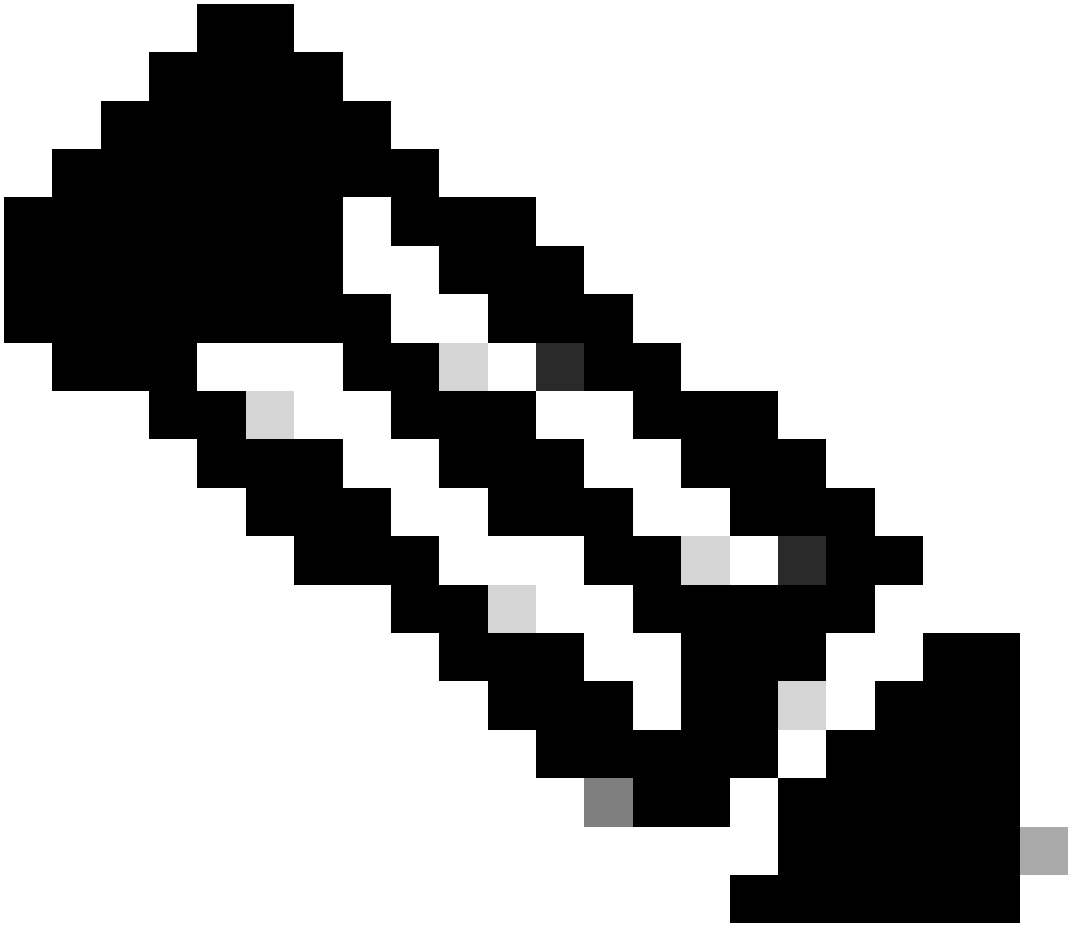
8: Aktivieren Sie das Kontrollkästchen mit dem Richtliniennamen AmazonS3FullAccess, und klicken Sie auf Weiter.



AWS-IAM

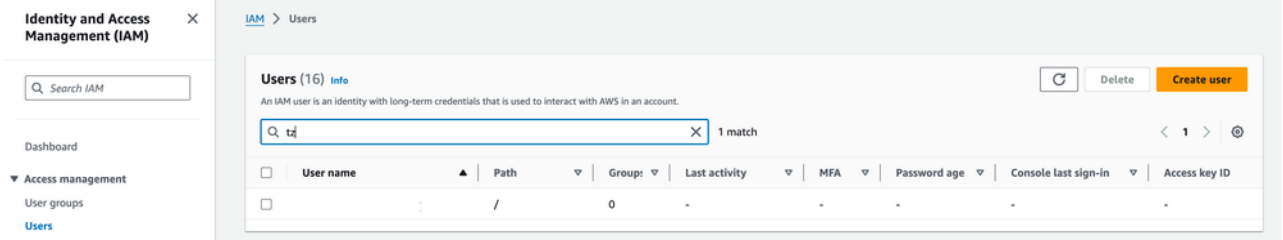


AWS-IAM

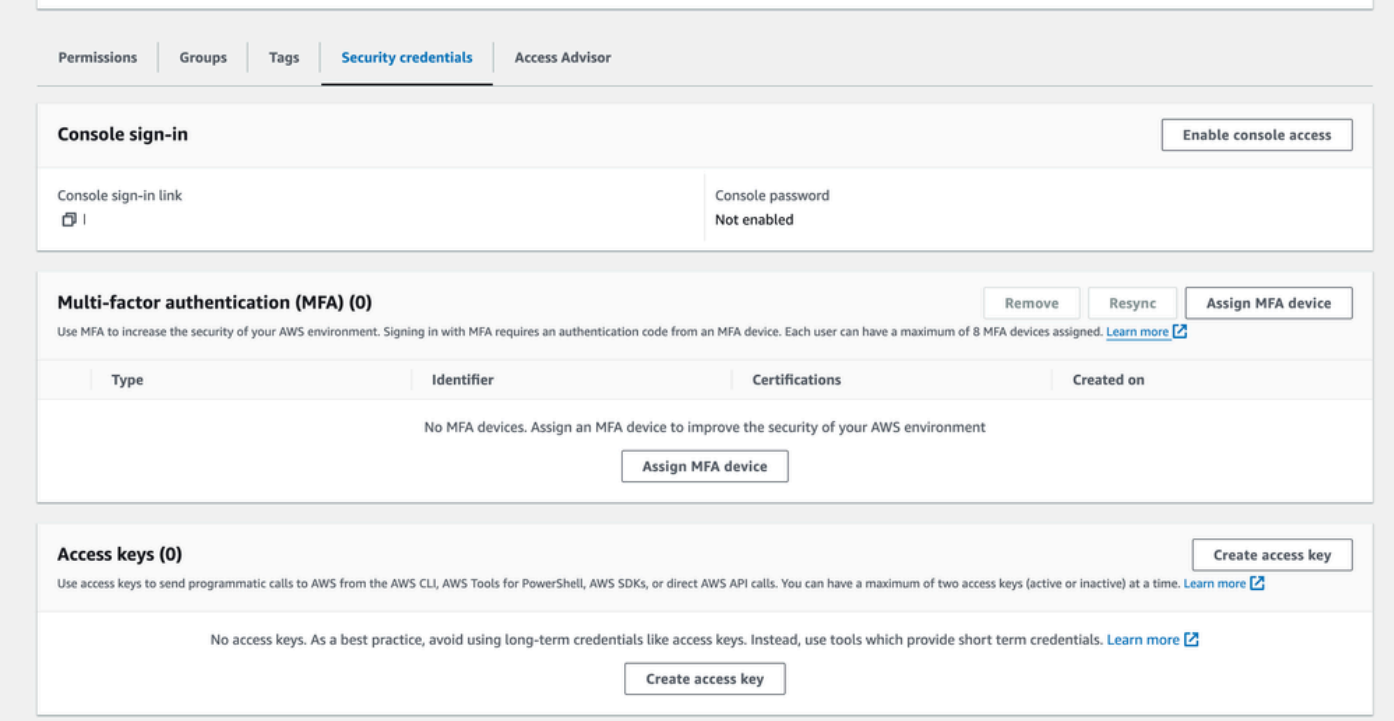


Anmerkung: Sie können detailliertere Richtlinien erstellen, indem Sie nur bestimmte Gruppen zulassen. Navigieren Sie zu [Richtlinienerstellung,](#) um Ihre S3-Gruppen-Richtlinie im JSON-Format zu erstellen.

9: Sobald der Benutzer erstellt wurde, listen Sie den Benutzer auf und navigieren zur Registerkarte Sicherheitsanmeldeinformationen, und klicken Sie auf Zugriffsschlüssel erstellen.

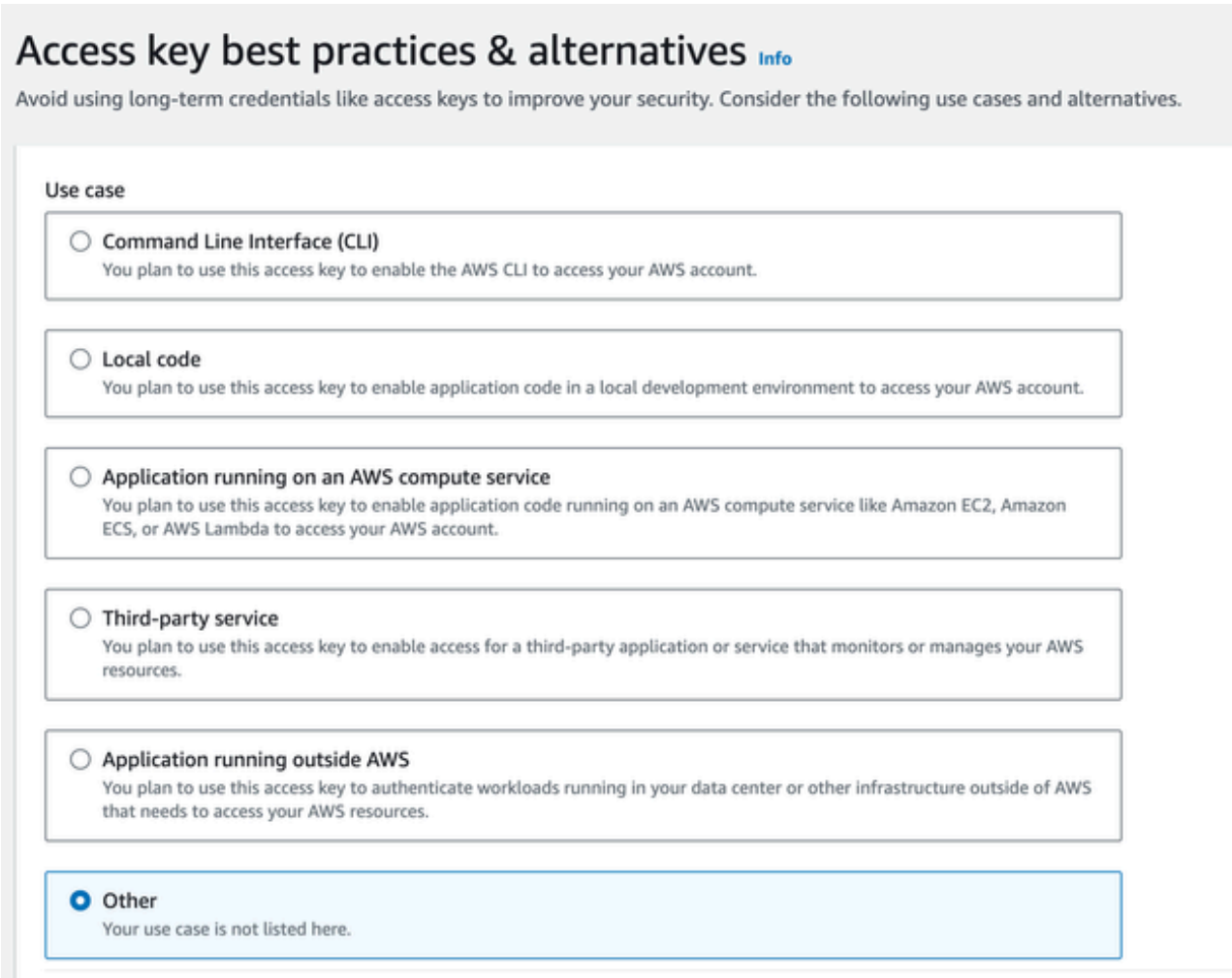


AWS-IAM

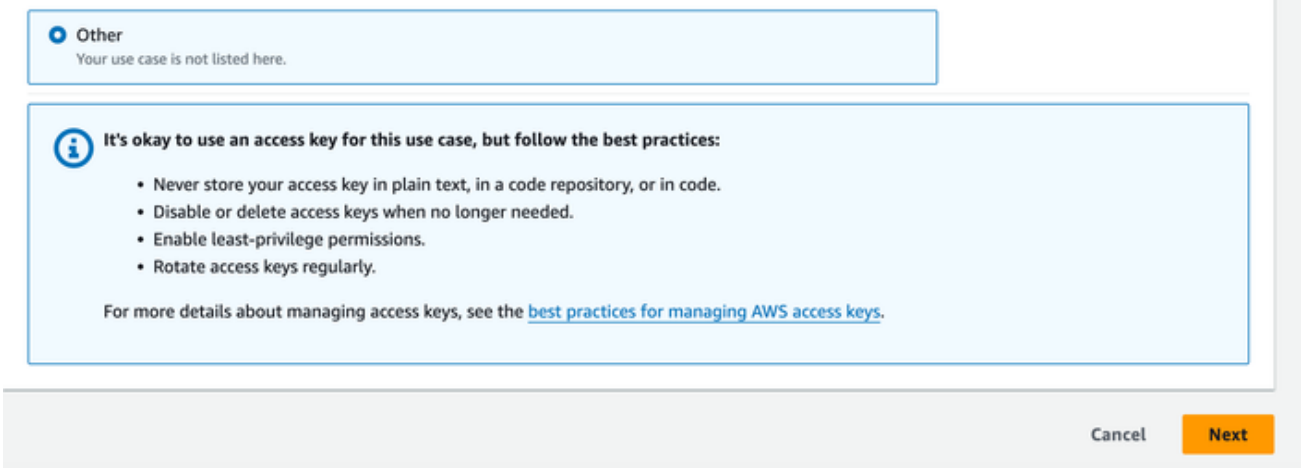


AWS-IAM

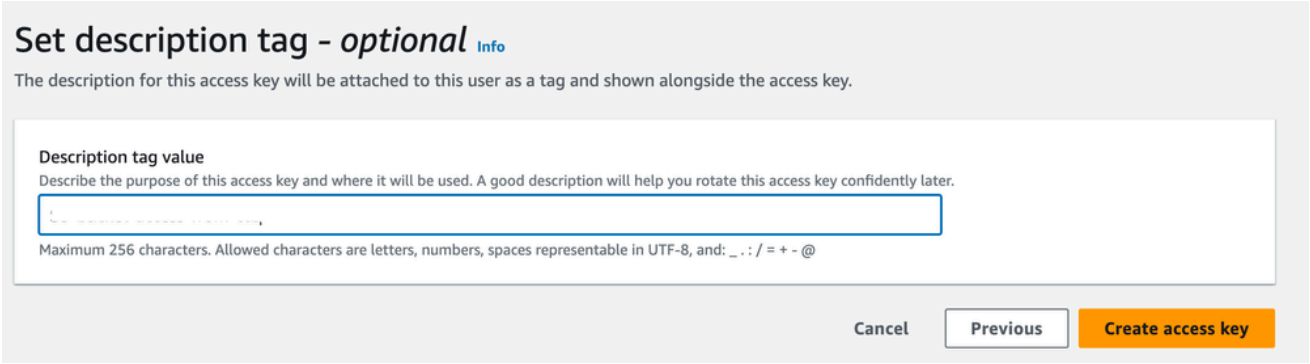
10: Wählen Sie das andere Optionsfeld aus, und fügen Sie optional ein Tag hinzu.



AWS-IAM

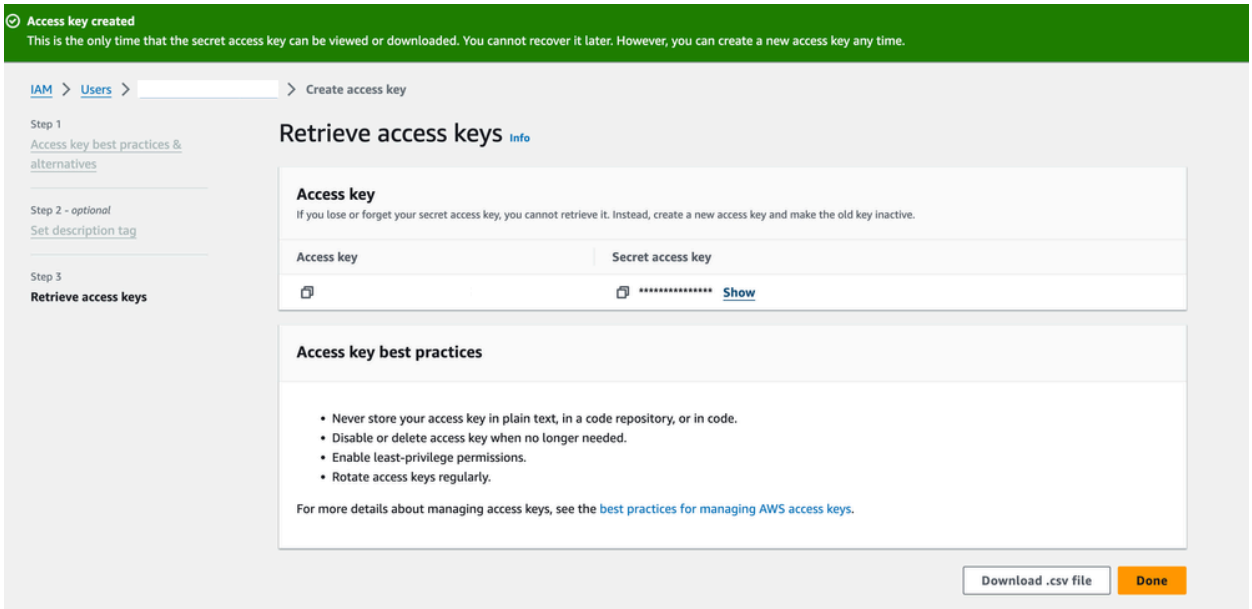


AWS-IAM



AWS-IAM

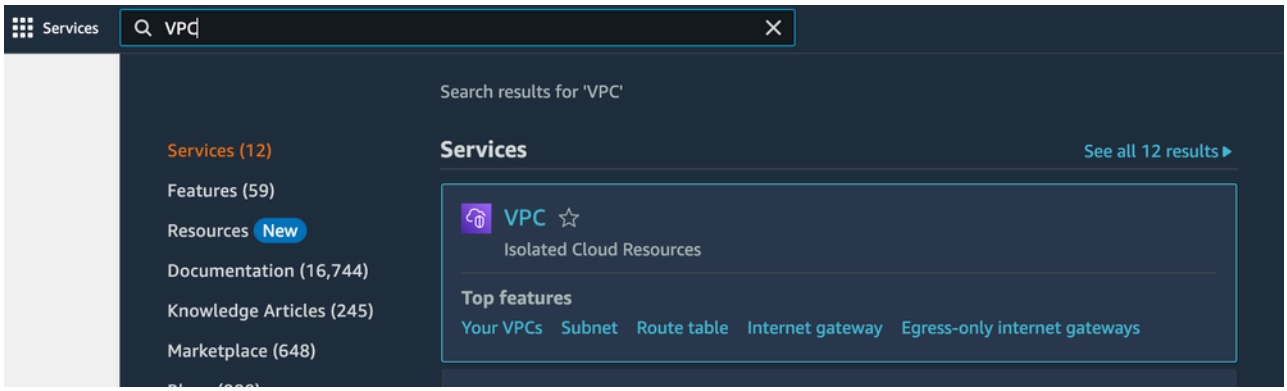
11: Klicken Sie auf CSV-Datei herunterladen. Dies ist der Zugriffsschlüssel in einer CSV-Datei, der nicht mehr heruntergeladen oder angezeigt werden kann, wenn Sie diese Seite verlassen.



AWS-IAM

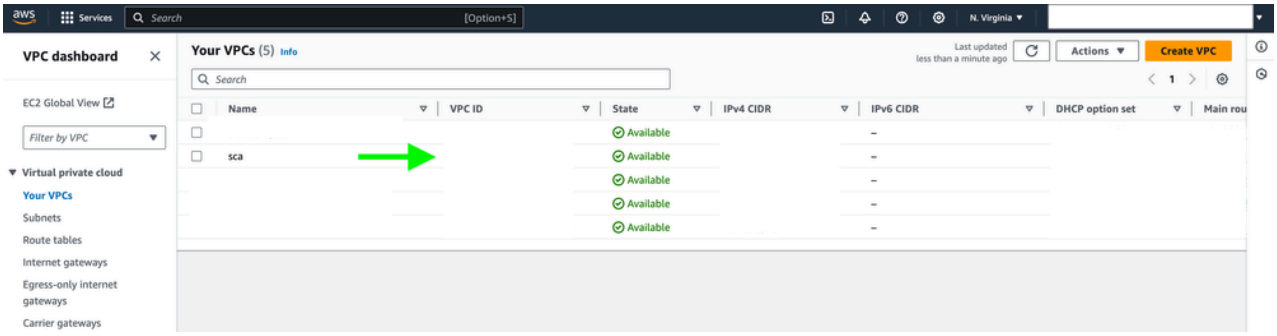
Schritt 3: VPC-Ablaufprotokolle konfigurieren

1: Starten Sie VPC in der gewünschten Region, und navigieren Sie zu Ihrer VPC-Option.

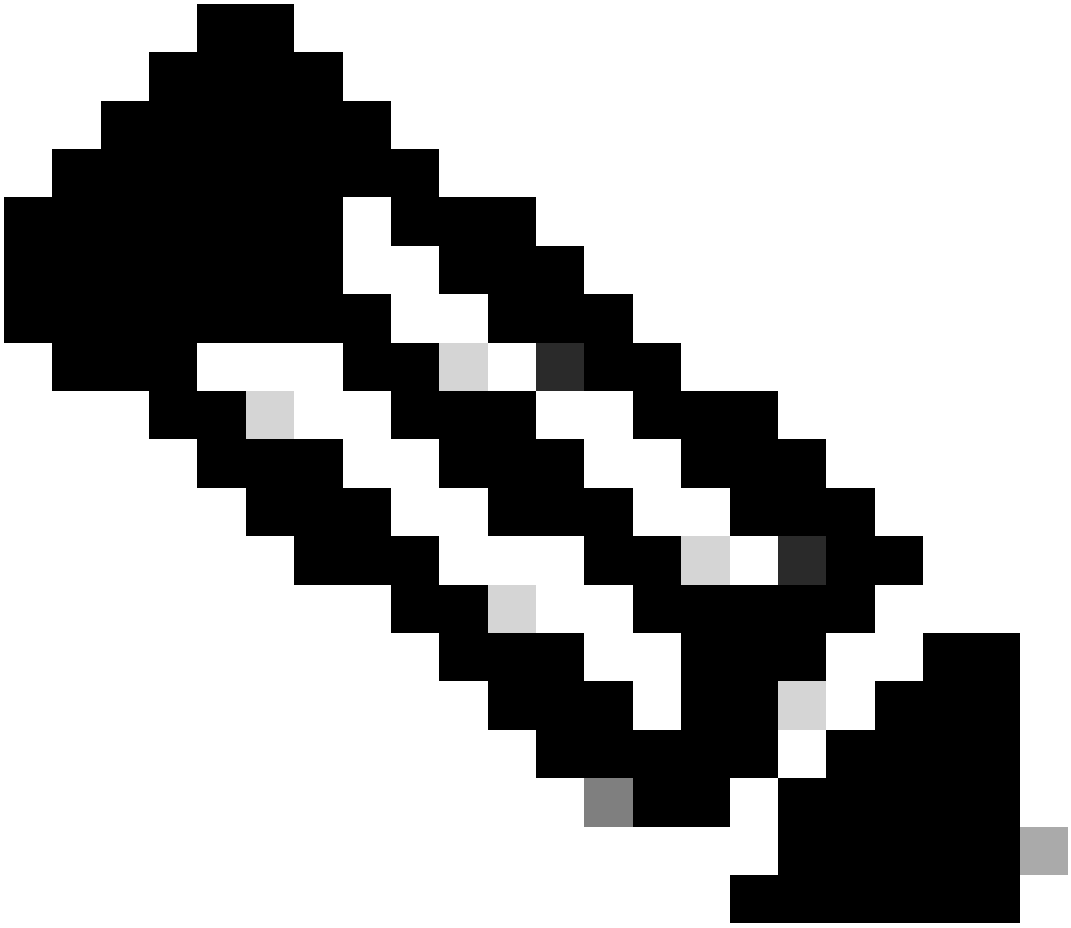


AWS-Flow-Protokolle

2: Wählen Sie Ihre vPC aus der Liste auf dem Bildschirm aus.

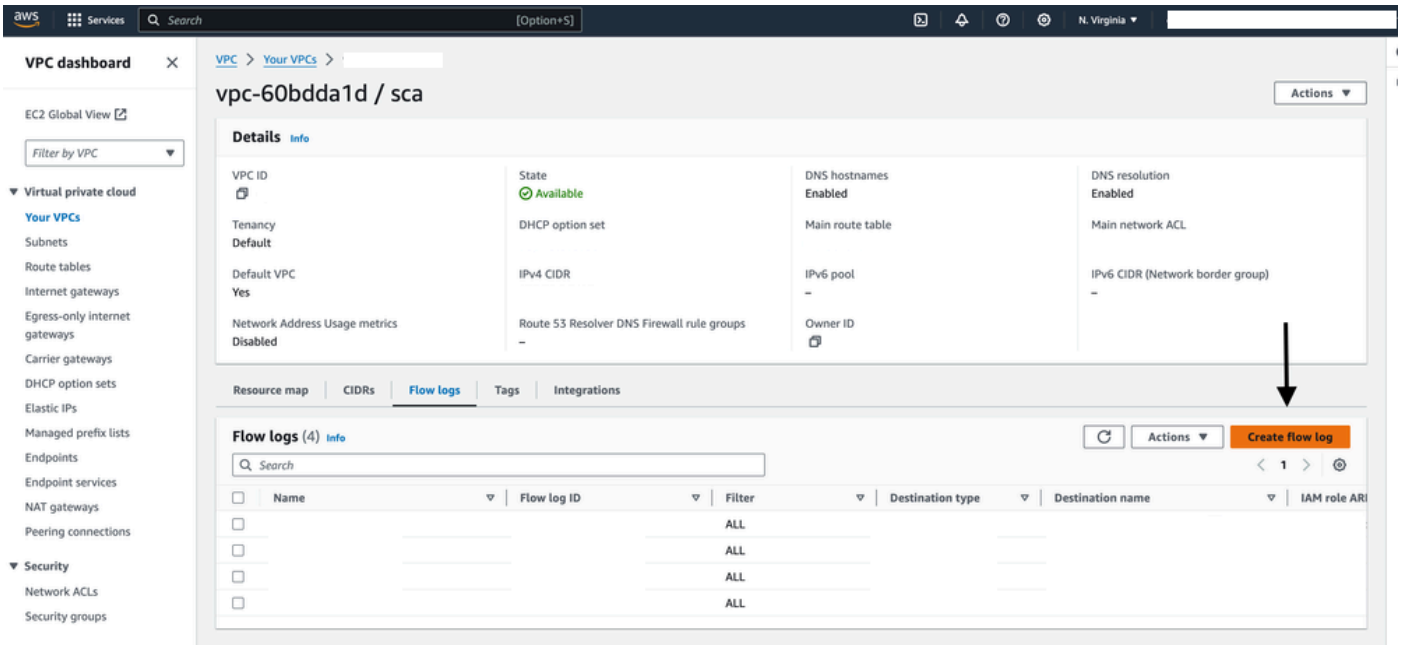


AWS-Flow-Protokolle



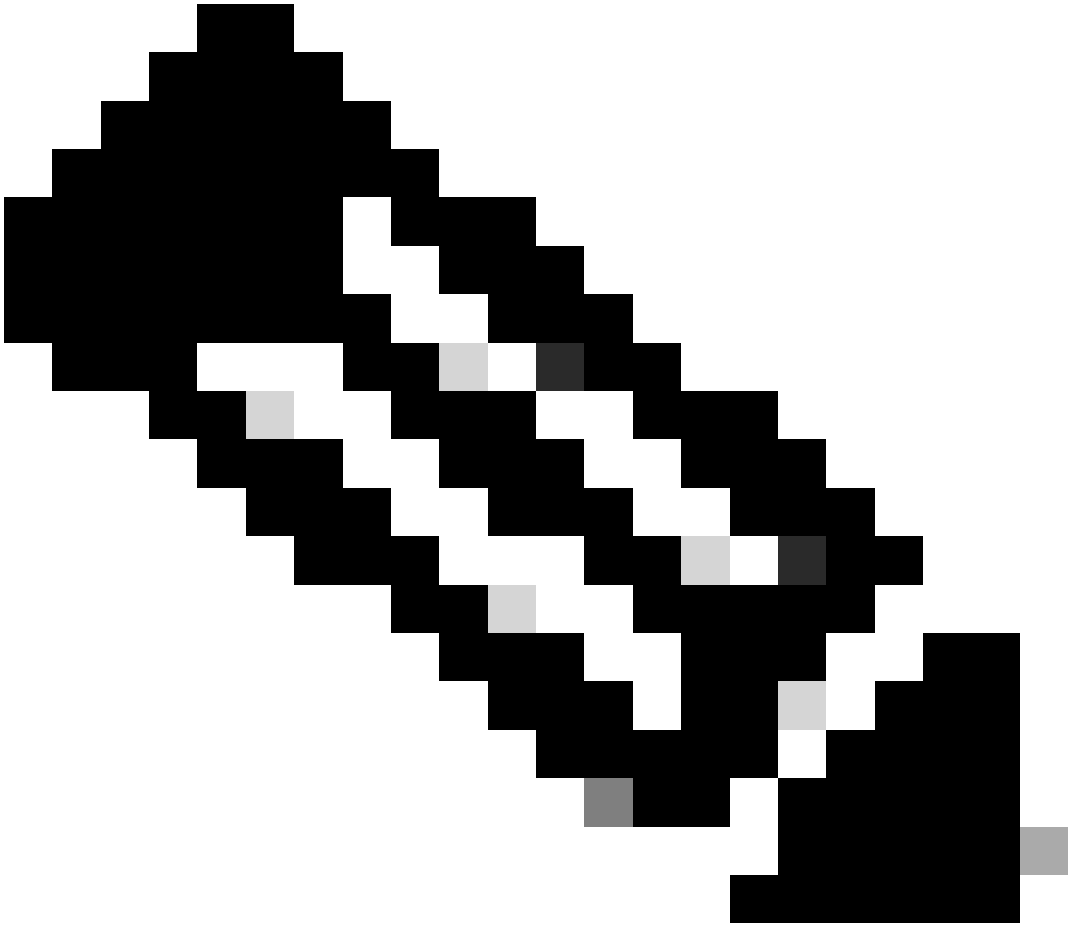
Anmerkung: Sie haben in dieser Demo den VPC-Namen SCA ausgewählt.

3: Navigieren Sie zu Ihren vPCs unter Virtual Private Cloud, wechseln Sie zur Registerkarte Flow-Protokolle, und klicken Sie auf Flow-Protokolle erstellen.



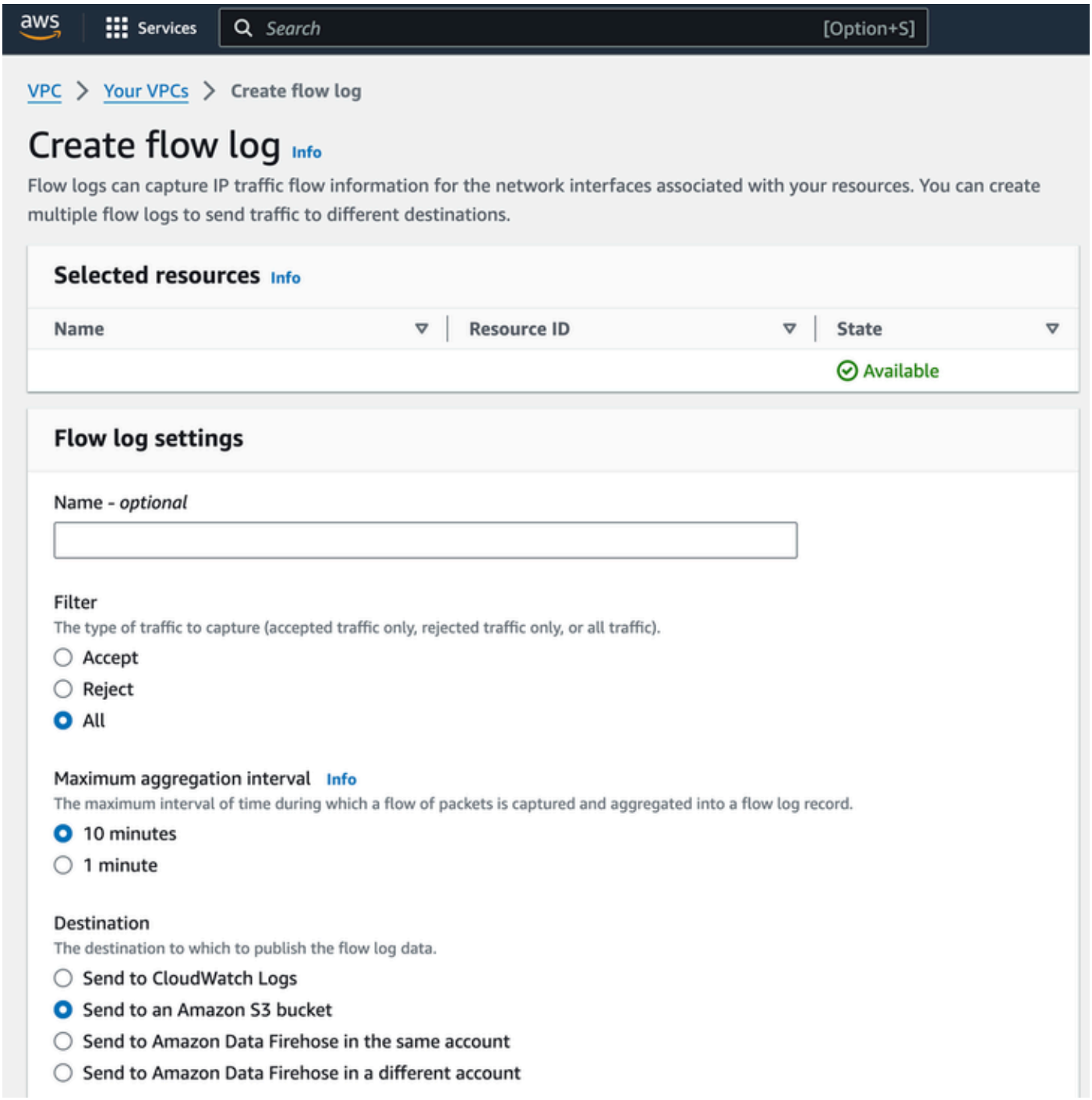
AWS-Flow-Protokolle

4: Geben Sie Ihren Flow-Protokollen einen Namen, und geben Sie die zuvor erstellte S3-Bucket-ARN frei.

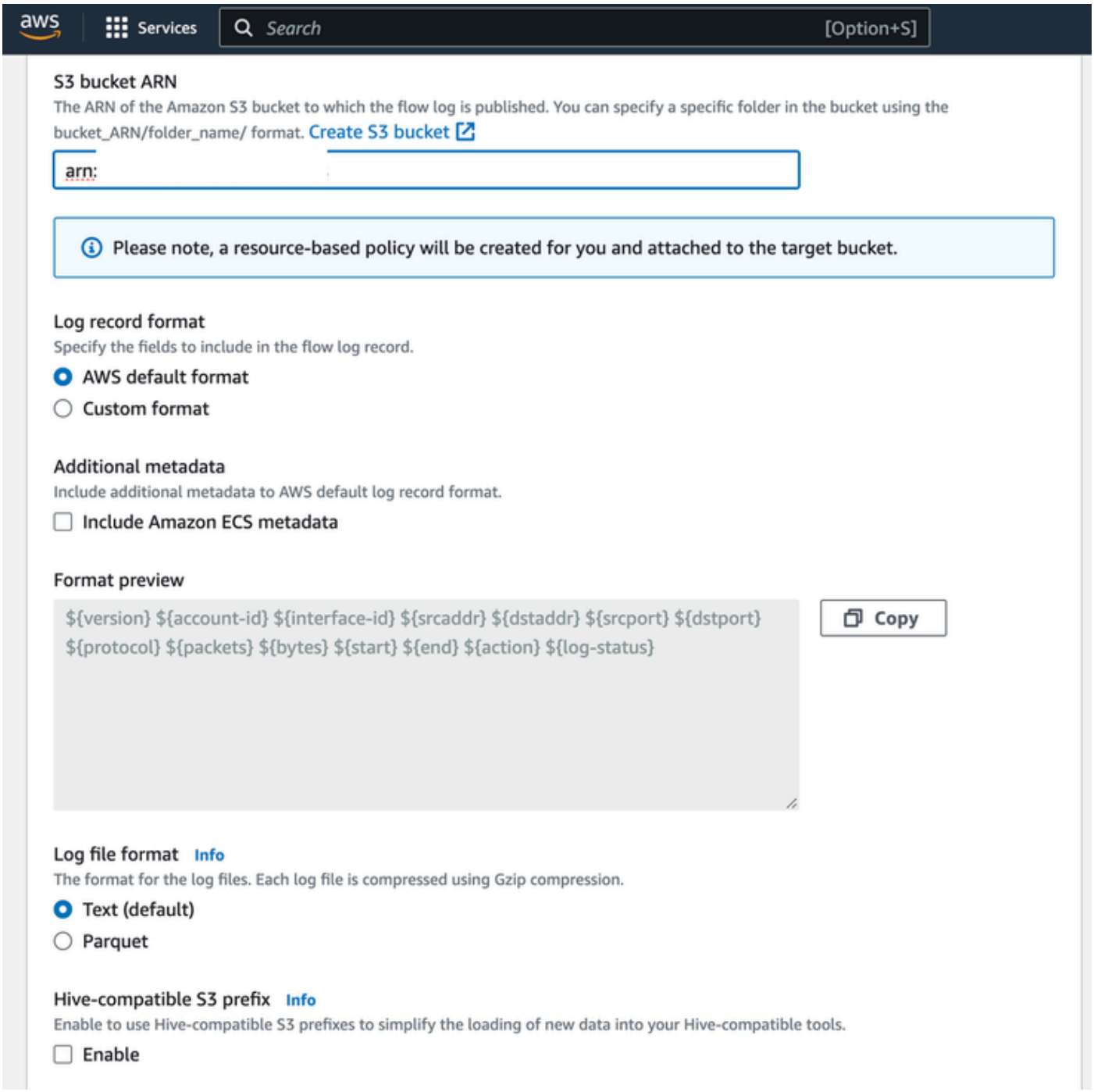


Anmerkung: Informationen zu ARN finden Sie unter Konfigurieren von S3 bucket - Schritt 6

5: Sie haben die Möglichkeit, das AWS-Standardprotokollformat zu verwenden oder ein benutzerdefiniertes Protokollformat zu erstellen, falls weitere Felder erforderlich sind.

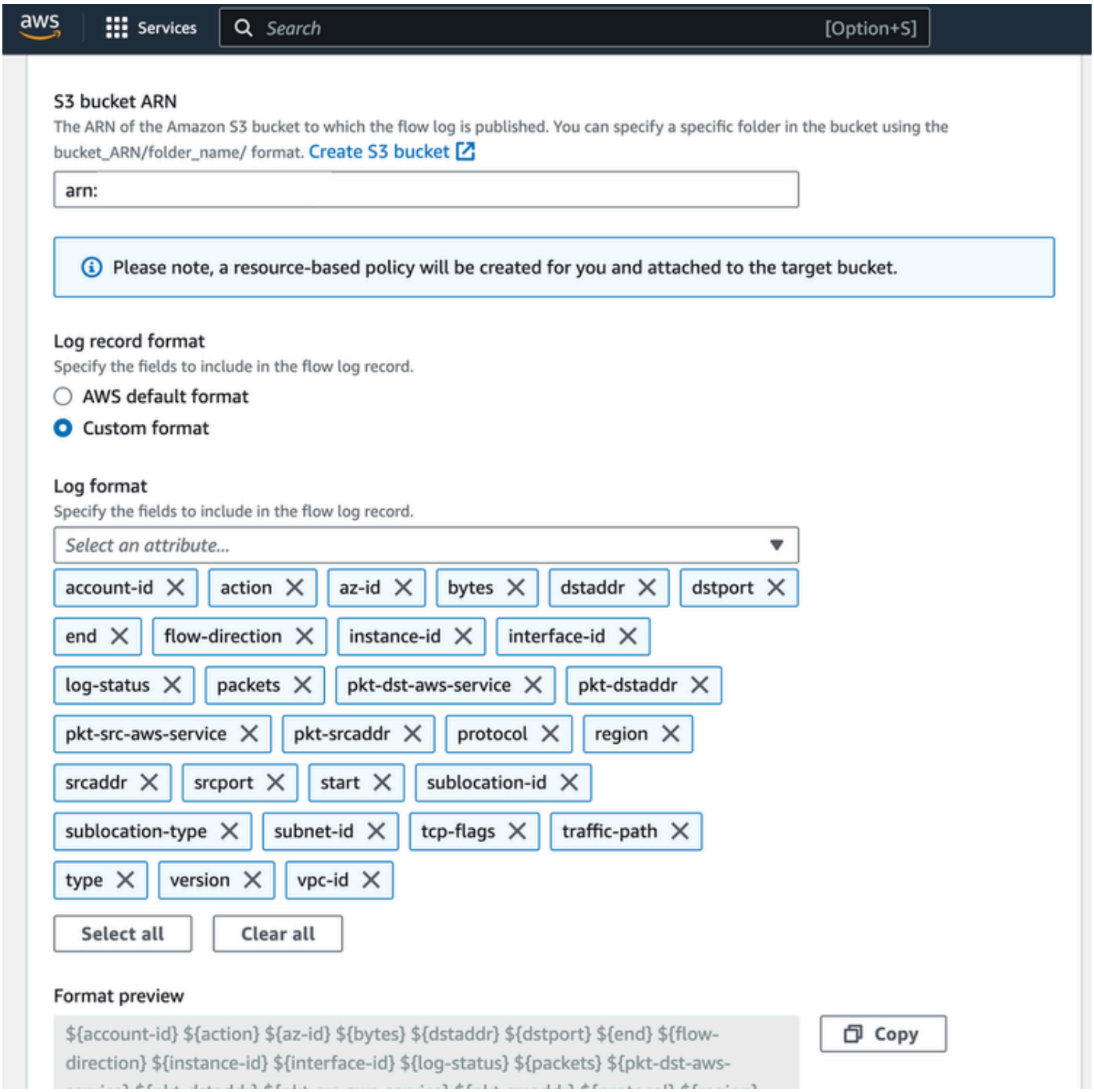


AWS-Flow-Protokolle

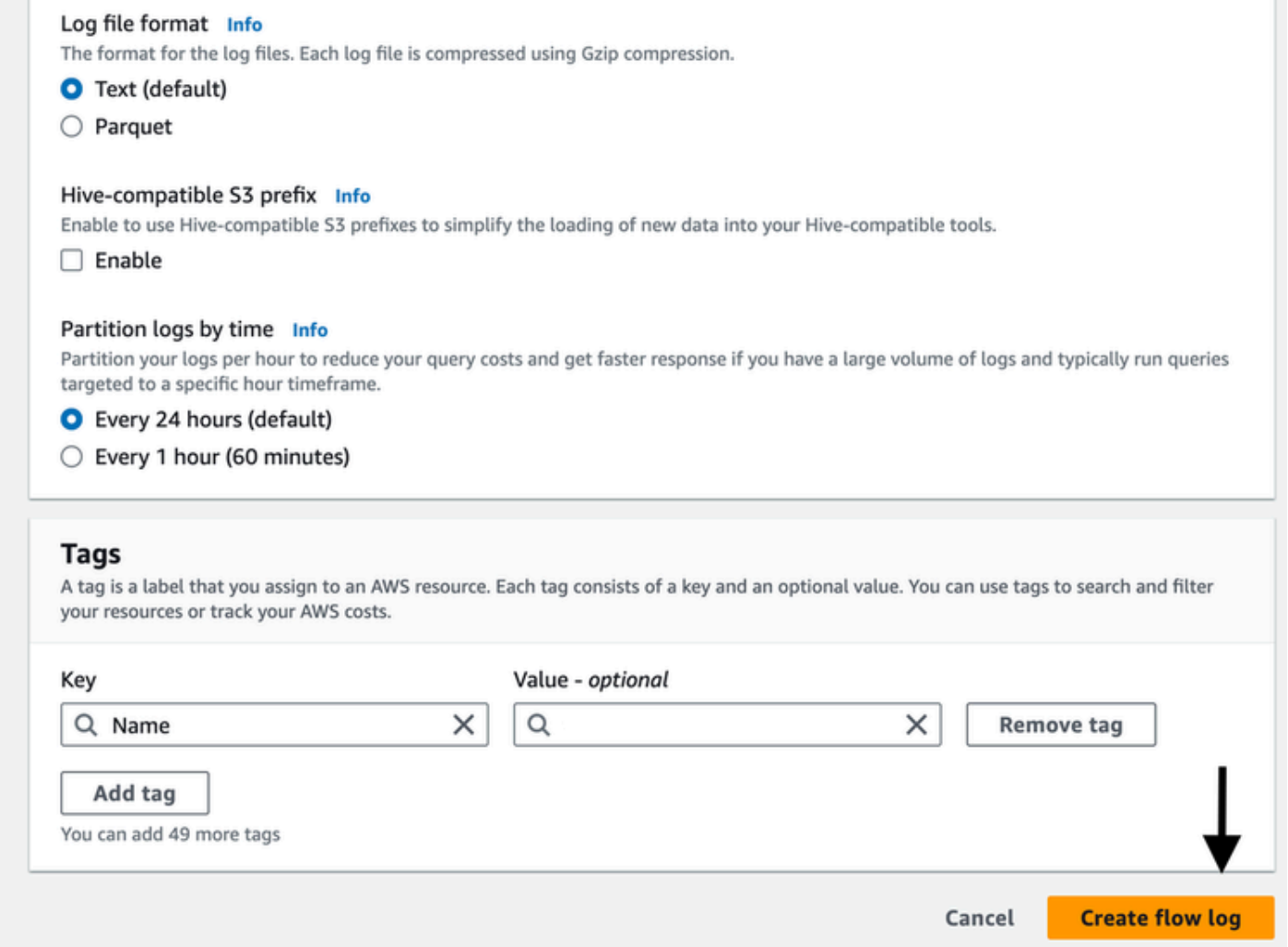


AWS-Flow-Protokolle

7: Klicken Sie auf Flussprotokolle erstellen.



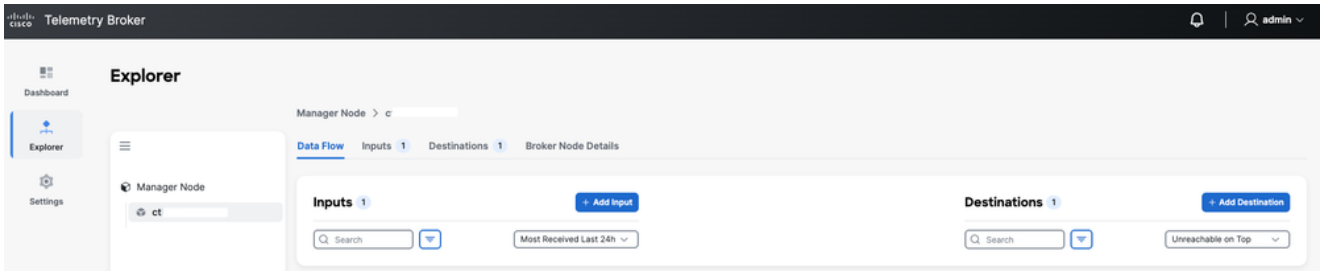
AWS-Flow-Protokolle



AWS-Flow-Protokolle

Schritt 4: Konfigurieren der VPC-Eingabe in der CTB

1: Zugriff auf CTB Web UI, navigieren Sie zu Explorer> Broker-Knoten Registerkarte > klicken Sie auf Öffnen Broker-Knoten > Datenfluss-Registerkarte > Klicken Sie auf Eingabe hinzufügen.



CTB-Eingabe-Benutzeroberfläche

2: Wählen Sie als Eingabetyp AWS VPC Flow log aus, und klicken Sie auf Weiter.

Add Input

Select Input type

Type or Select Input

UDP Input

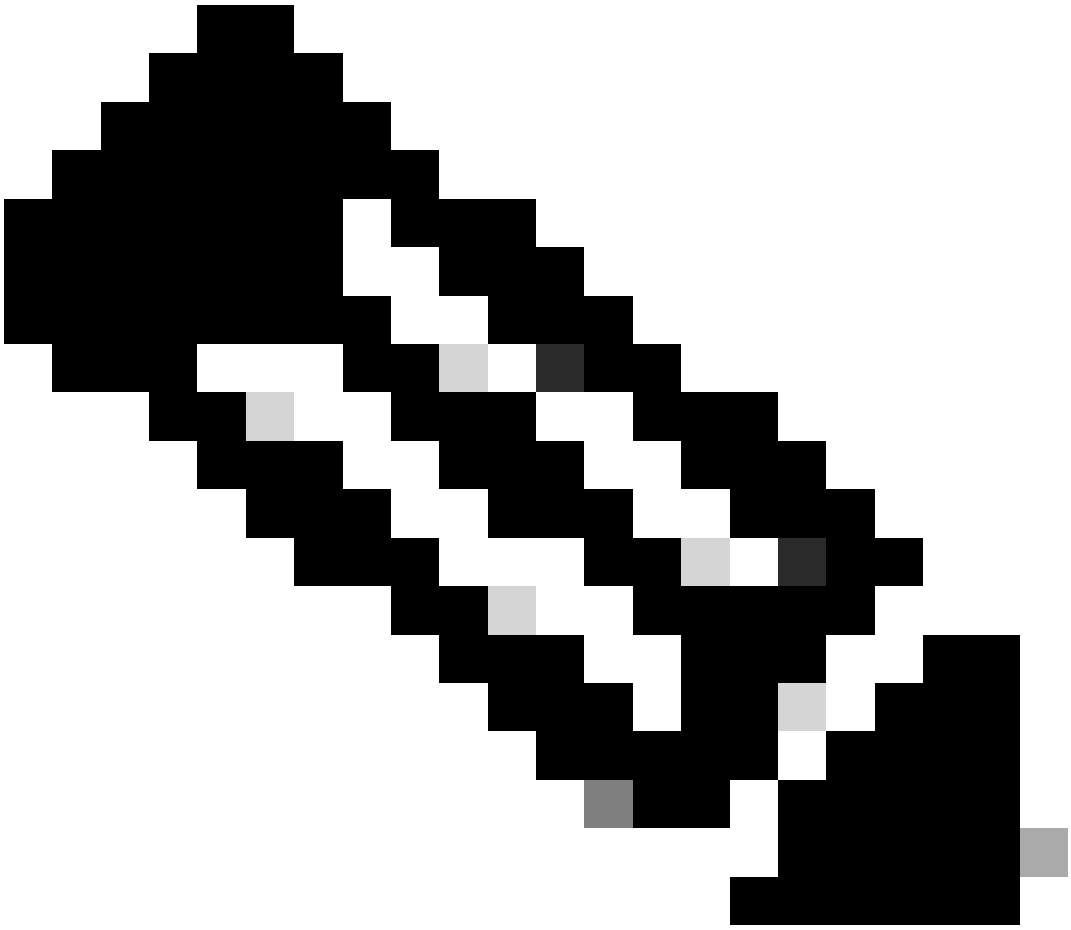
AWS VPC Flow log

AWS VPC Flow log

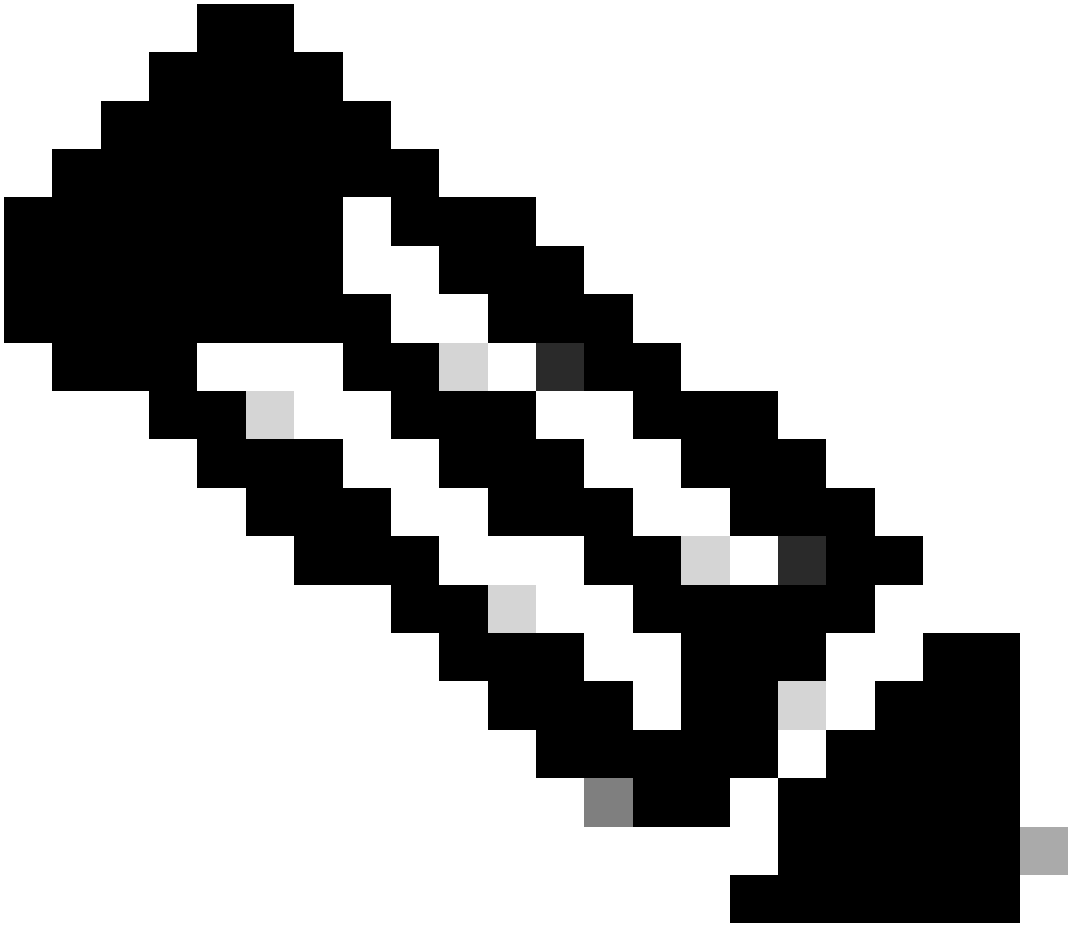
Azure NSG Flow log

Flow Generator Input

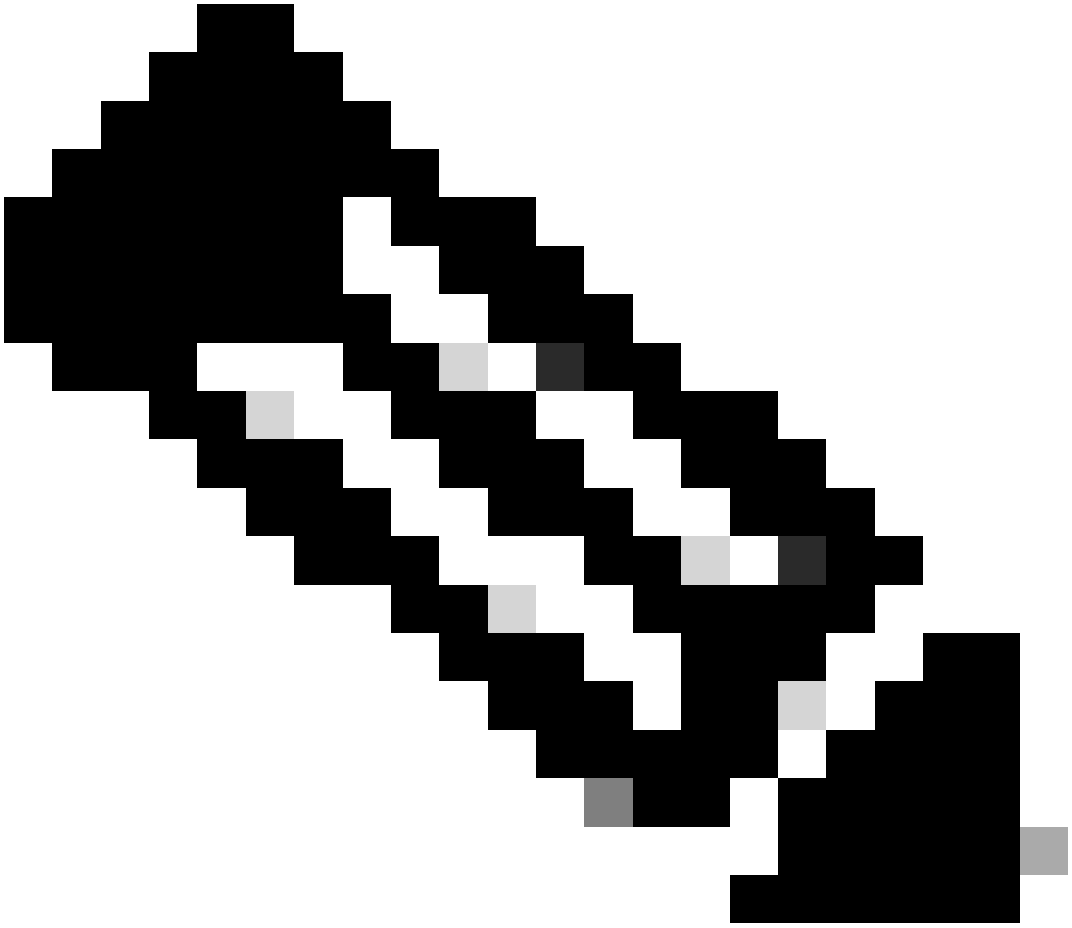
Informationen zu S3 Bucket Path finden Sie unter Konfigurieren von VPC-Flow-Protokollen - Schritt 7.



Anmerkung: Die Regionskennzahl finden Sie auf der AWS-Startseite neben dem Zahnradsymbol.



Hinweis: Jede IP-Adresse, die als Eingabe-IP-Adresse konfiguriert ist (eindeutige, von keinem anderen Exporteur gemeinsam genutzte IP-Adresse), wird als Exporteur für die umgewandelten NetFlow-Daten gemeldet.



Anmerkung: Informationen zur AWS-Zugriffsschlüssel-ID finden Sie unter Konfigurieren des IAM-Benutzers für den Zugriffsschlüssel mit der S3-Zugriffsrichtlinie, Schritt 9

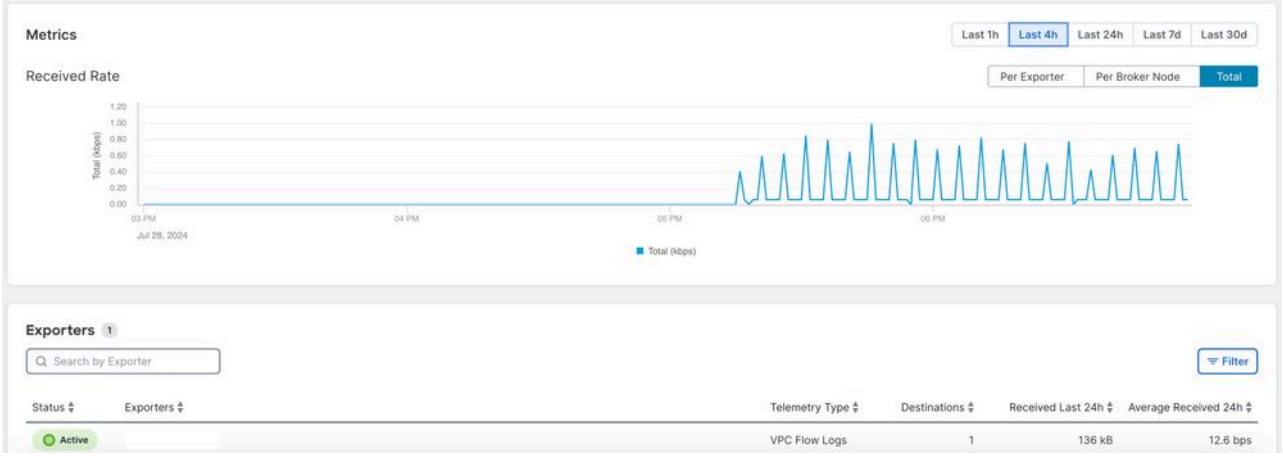
Überprüfung

Nach einigen Minuten der Konfiguration der AWS VPC-Eingabe wird die Statusspalte aktiviert, wenn der AWS S3-Bucket Daten enthält.

Überprüfen Sie mithilfe dieser Schritte den Status der AWS VPC-Eingabe.

1: Melden Sie sich bei der CTB-Benutzeroberfläche an, und navigieren Sie zuExplorer> Broker node tab > click openbroker node > switch tab toInput > Click open AWS input.

2: Überprüfen Sie, ob die konfigurierten WS-Flow-Protokolle den Status "Aktiv" aufweisen und die empfangene Metrik einen steigenden Graphen aufweist.



CTB-Eingabe-Benutzeroberfläche

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.