Configura log di flusso VPC AWS per input CTB

Sommario

Introduzione

Prerequisiti

- Requisiti
- Componenti usati

Procedura di configurazione

- Passaggio 1. Configurare il bucket S3 in AWS
- Passaggio 2. Creare l'utente IAM con la chiave di accesso e allegare il criterio bucket S3
- Passaggio 3. Configurare i log di flusso VPC
- Passaggio 4. Configurare l'input VPC su CTB

Verifica

Introduzione

Questo documento descrive come configurare i log di flusso VPC come input per Cisco Telemetry Broker (CTB).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Servizi Web Amazon (AWS)
- Amministrazione CTB.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CTB (v2.2.1+)
- AWS

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

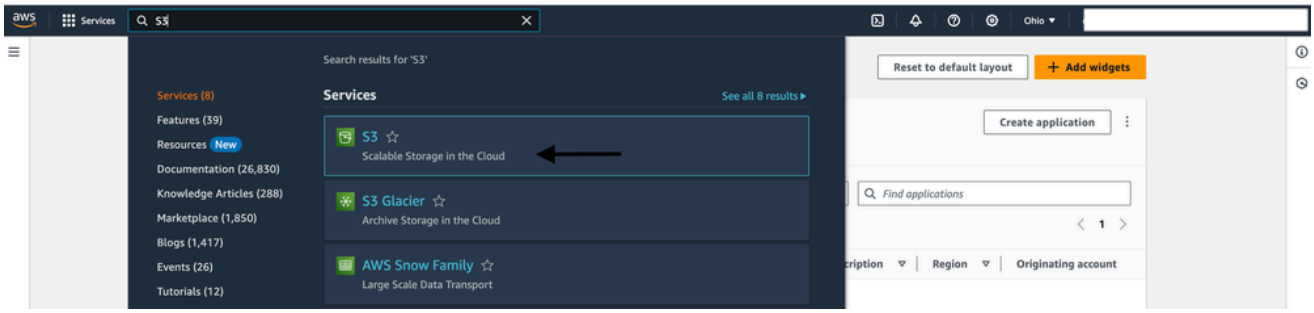
Procedura di configurazione

Passaggio 1. Configurare il bucket S3 in AWS

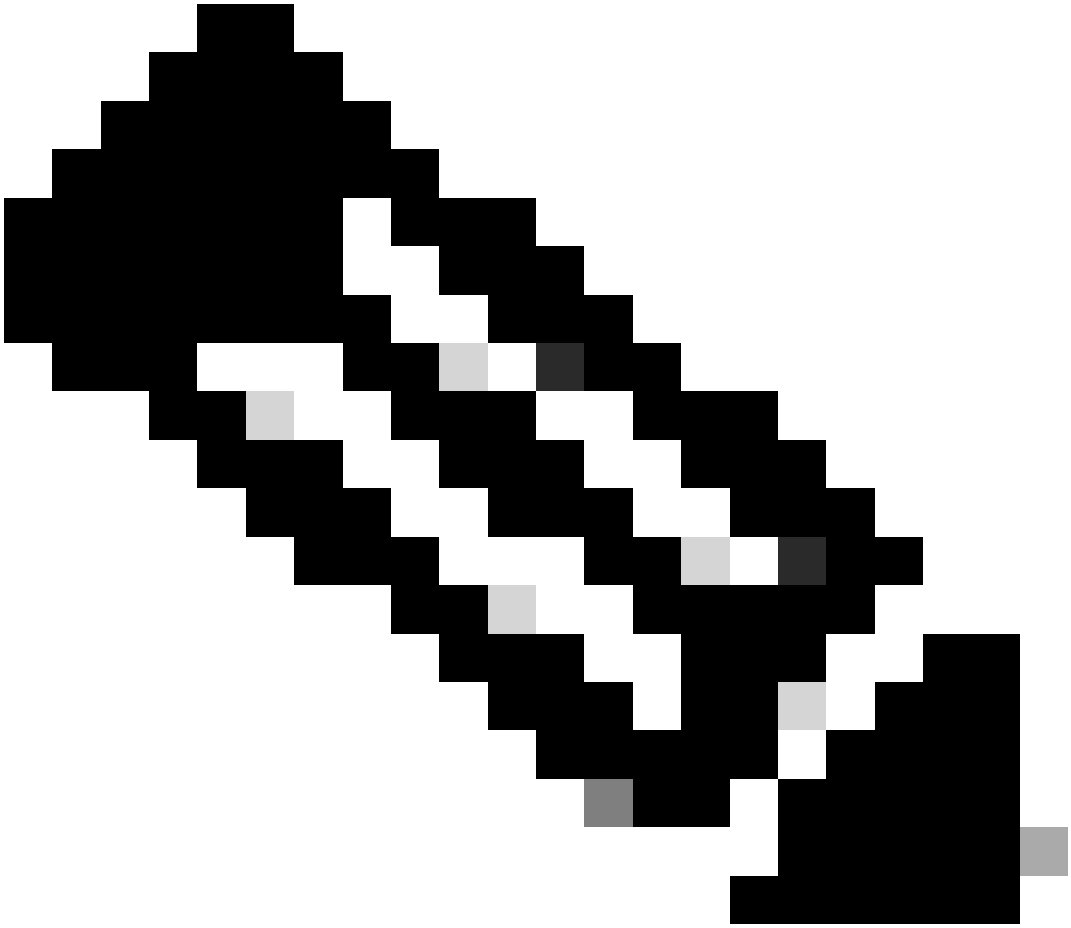
1: Accedere alla console di gestione AWS con nome utente e password.

2: Accertarsi di accedere all'area appropriata.

3: Passare alla barra di ricerca e digitare S3.

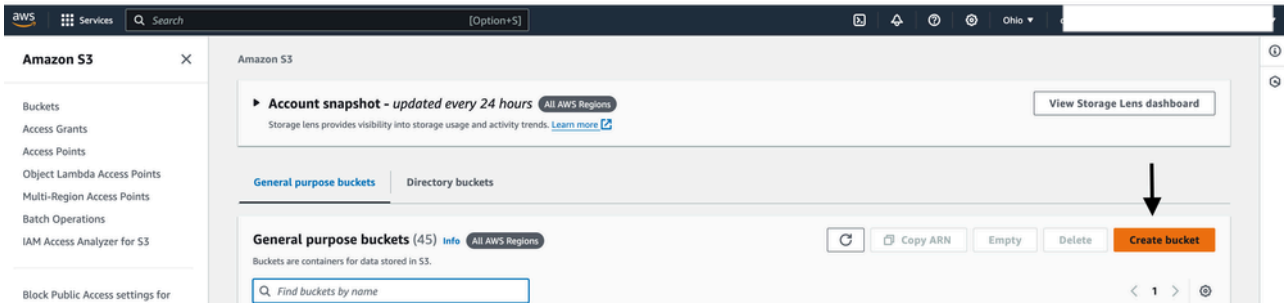


AWS-Dashboard



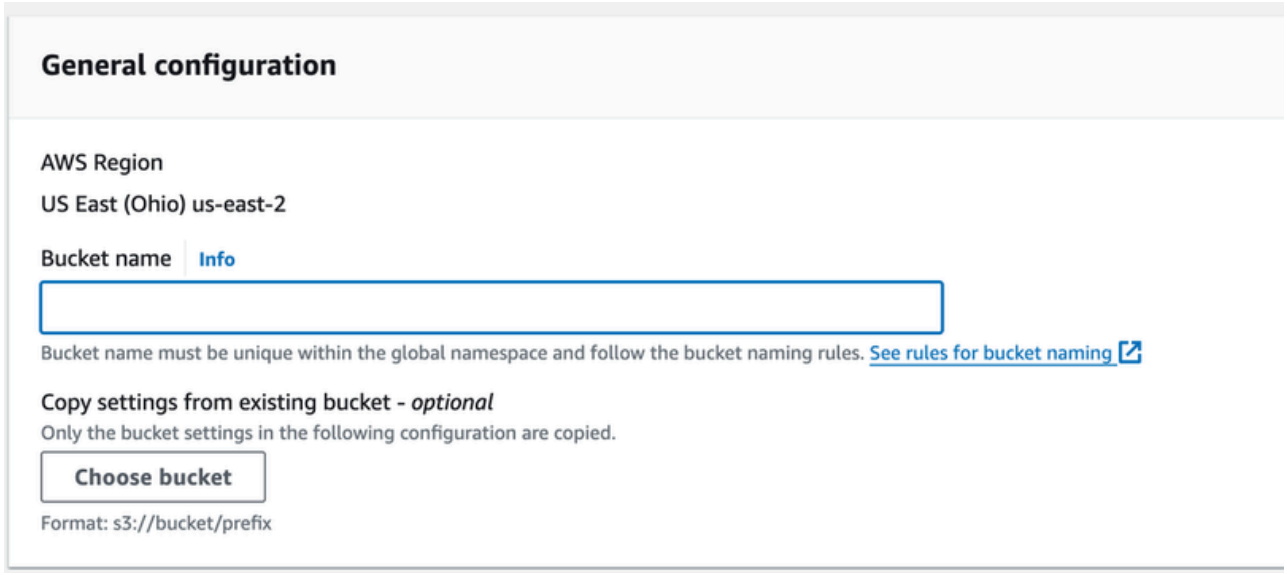
Nota: In demo, avete selezionato Ohio regione con us-east-2 zona di disponibilità, è visibile proprio accanto all'icona ingranaggio.

4: Fare clic su Crea bucket.

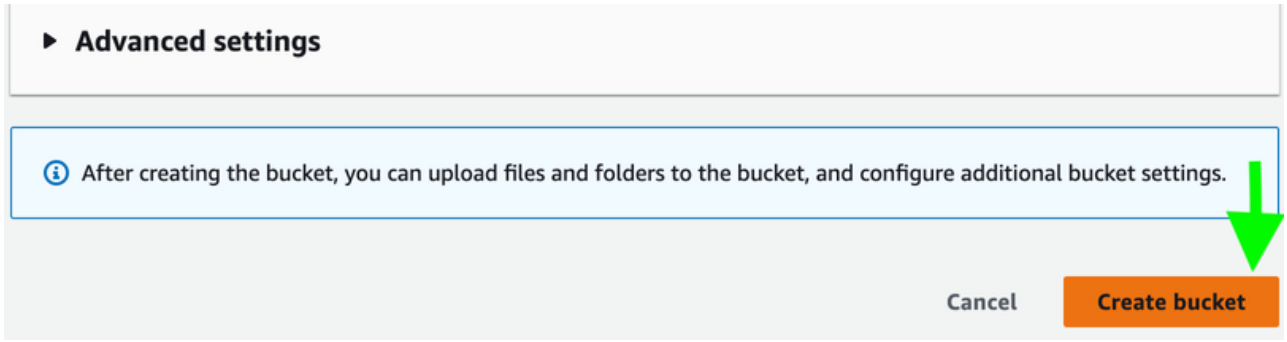


AWS-S3

5: Assegnare un nome al bucket e lasciare invariate tutte le opzioni, quindi fare clic su Crea.

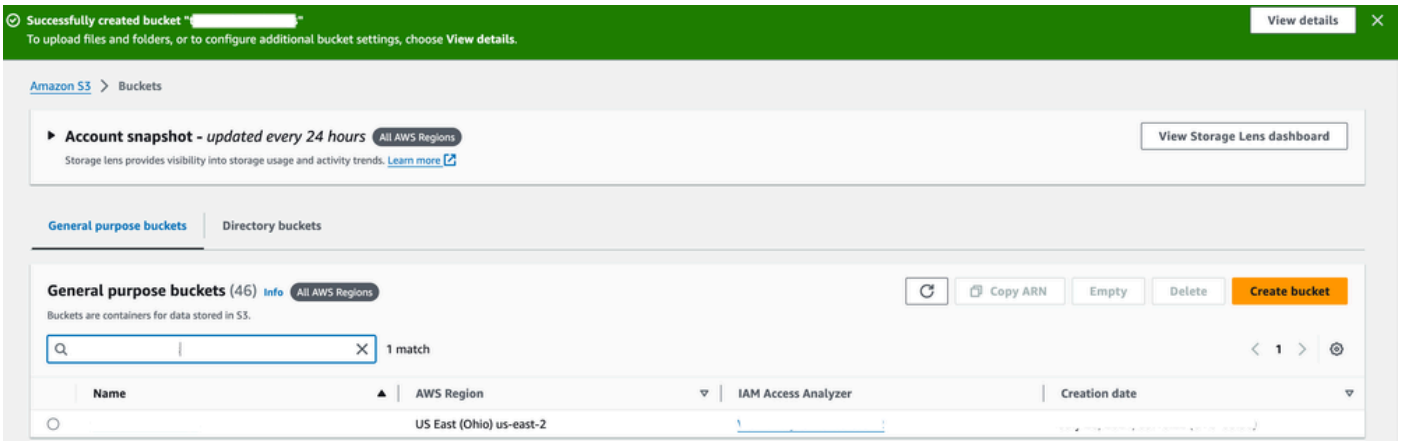


AWS-S3

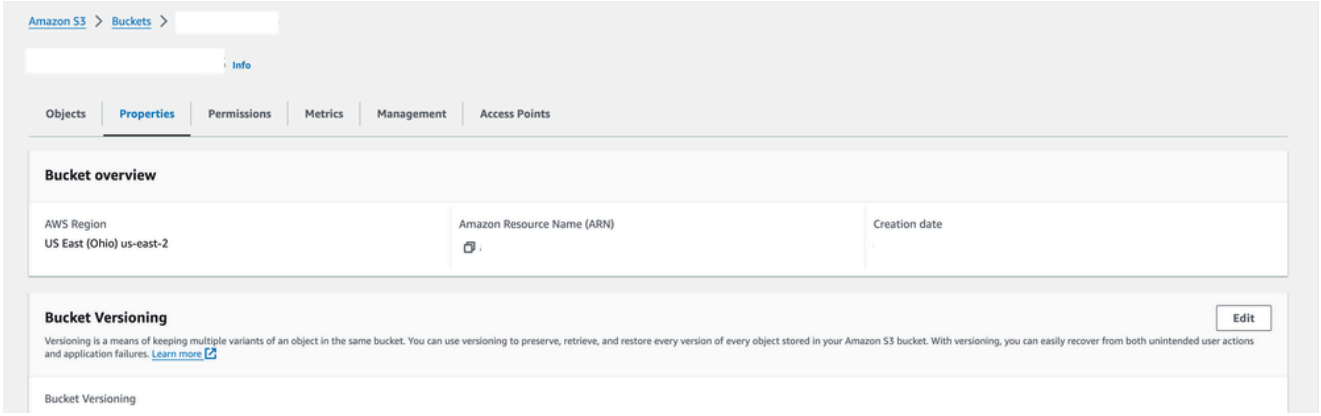


AWS-S3

6: Una volta creato il bucket, salvare il bucket ARN che verrà utilizzato successivamente durante la configurazione.



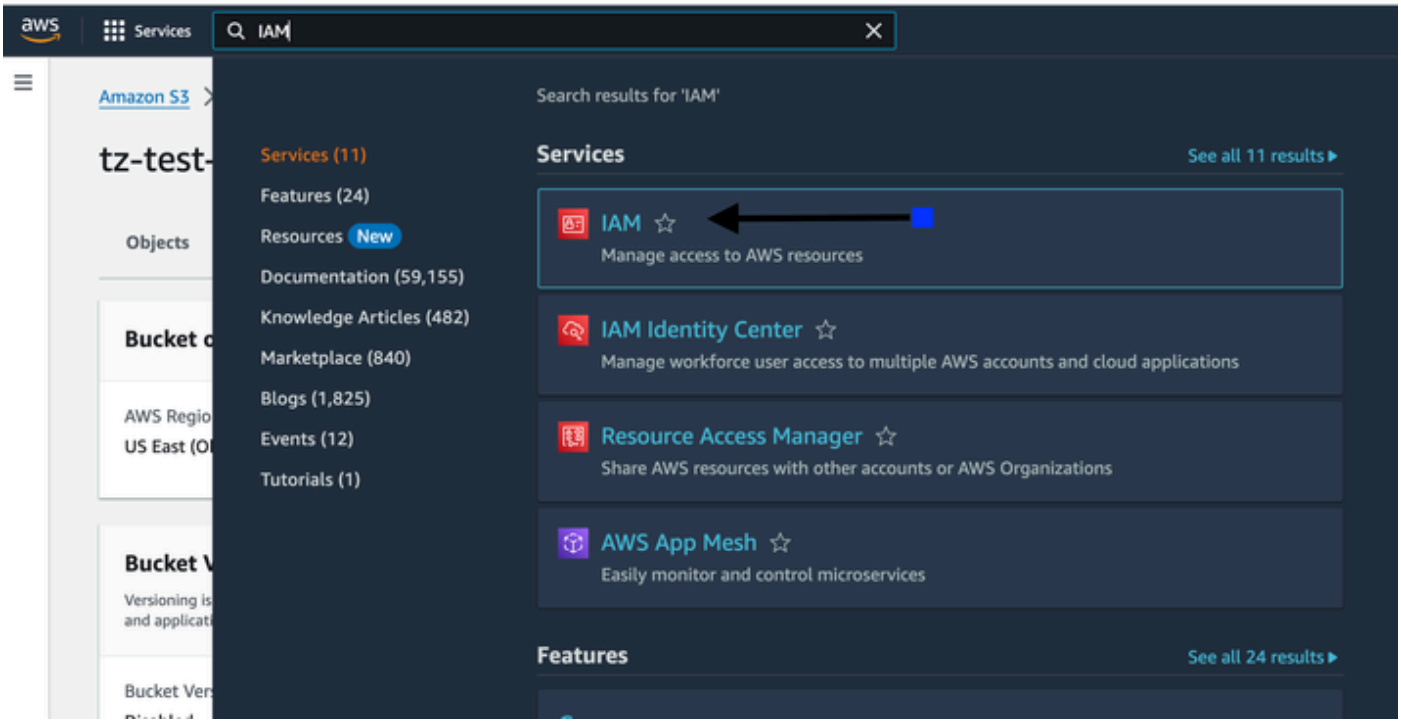
AWS-S3



AWS-S3

Passaggio 2. Creare l'utente IAM con la chiave di accesso e allegare il criterio bucket S3

1: Avviare IAM dalla barra di ricerca aws.



AWS-IAM

2: Passare agli utenti.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

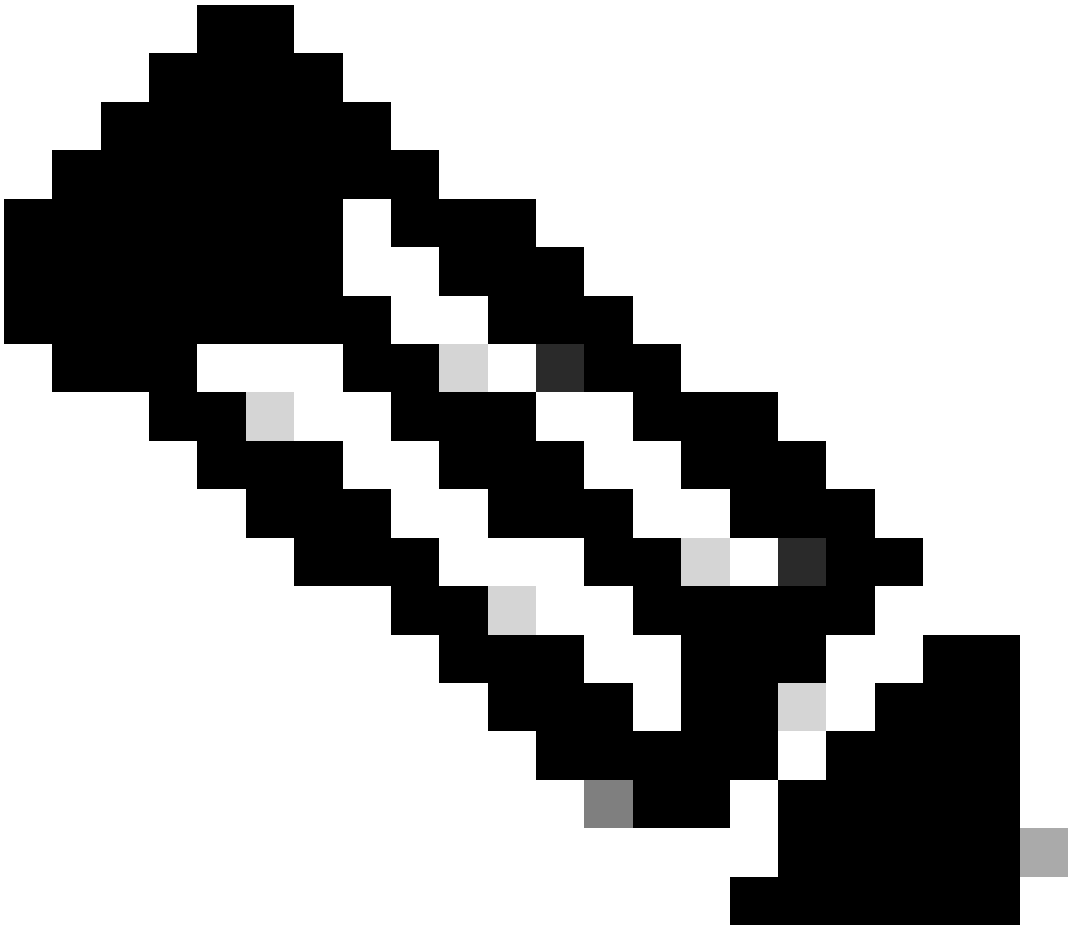
Users

Roles

Policies

Deselezionando la casella di accesso alla console di gestione AWS, si impedisce all'utente di accedere all'account AWS tramite l'interfaccia utente Web.

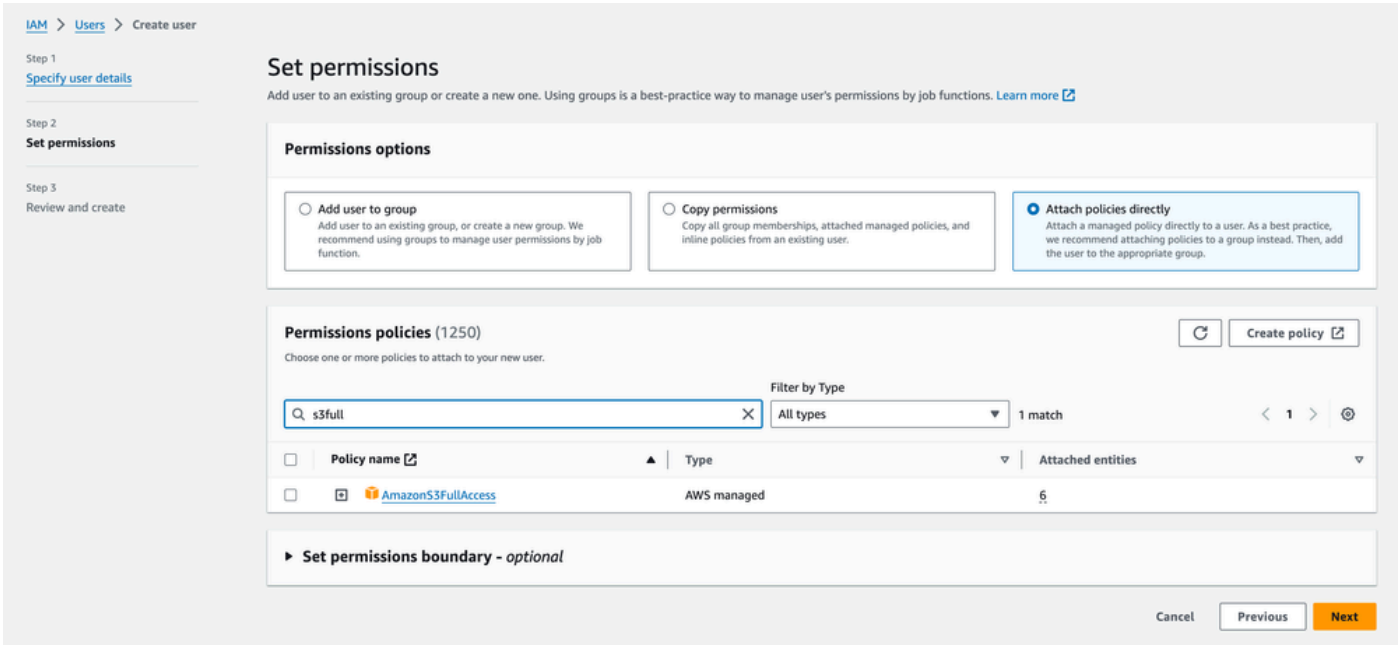
6: assegnare i criteri assegnandoli all'utente, collegandoli direttamente a un gruppo o configurandoli in linea.



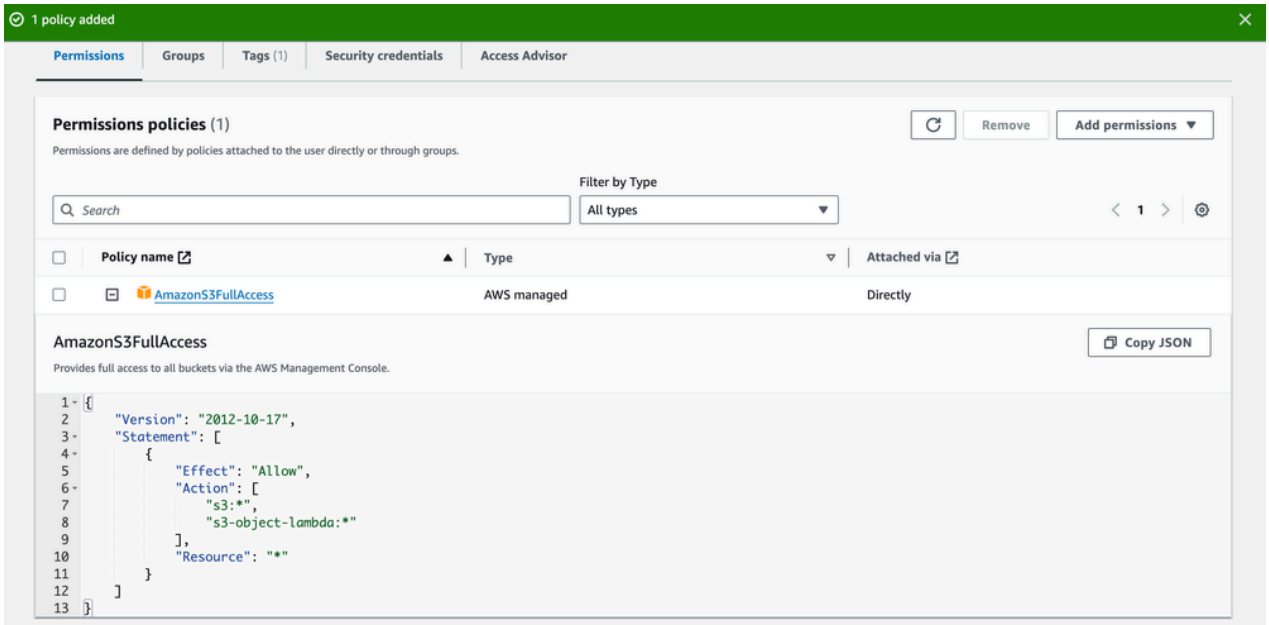
Nota: Per la dimostrazione, assegnare direttamente i criteri all'utente. Per ulteriori informazioni - Gestione dei criteri AWS

7: Cercare accesso completo S3 e selezionare AmazonS3full access, che consente all'utente di avere accesso completo per ogni bucket S3 creato sul suo account AWS corrispondente.

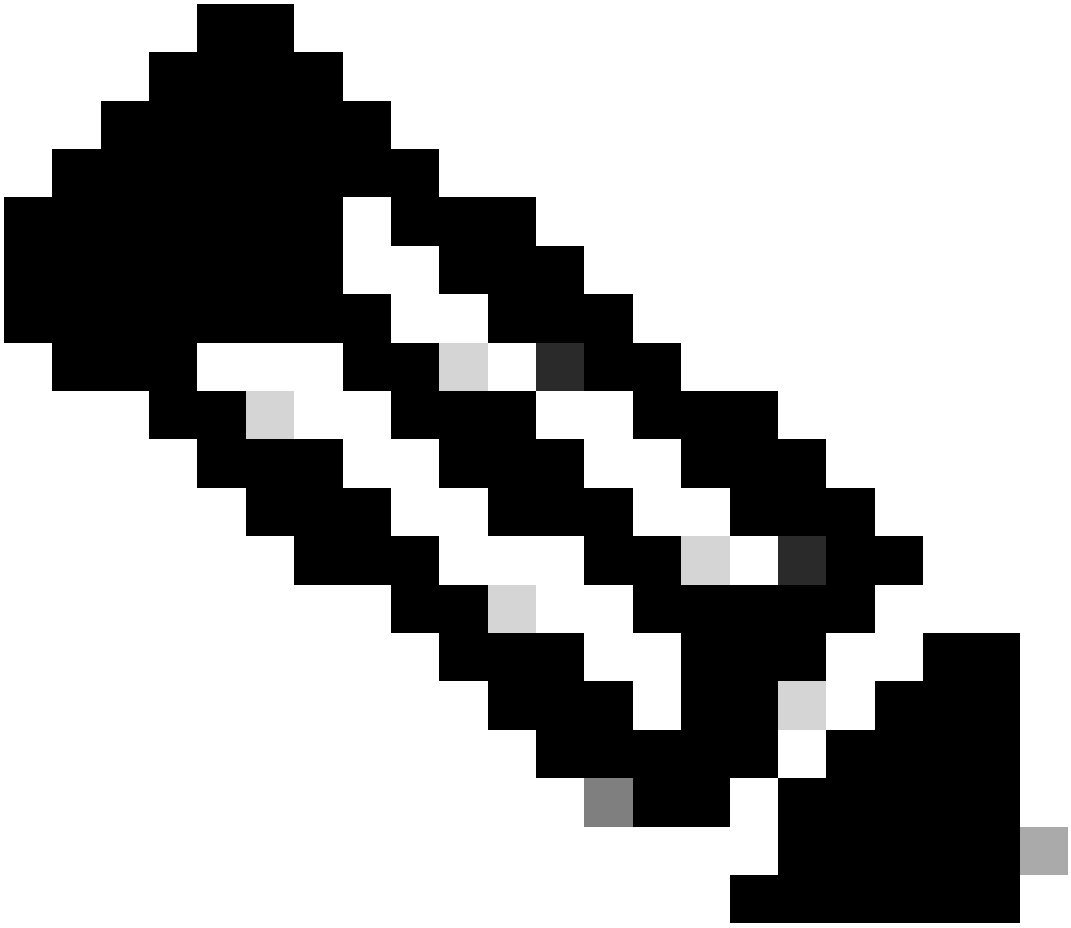
8: Selezionare la casella con il nome del criterio AmazonS3FullAccess e fare clic su avanti.



AWS-IAM

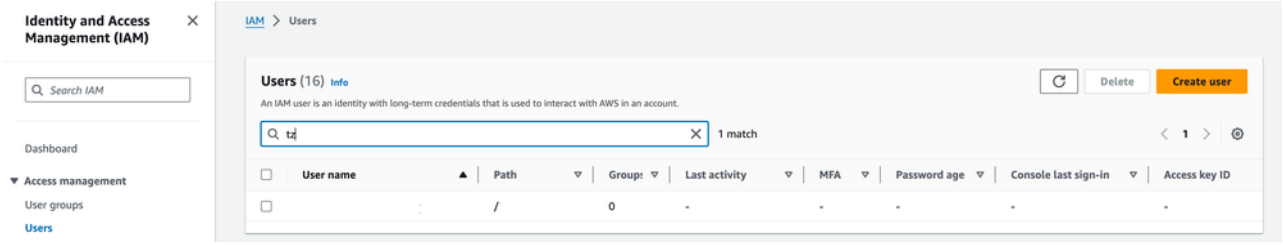


AWS-IAM

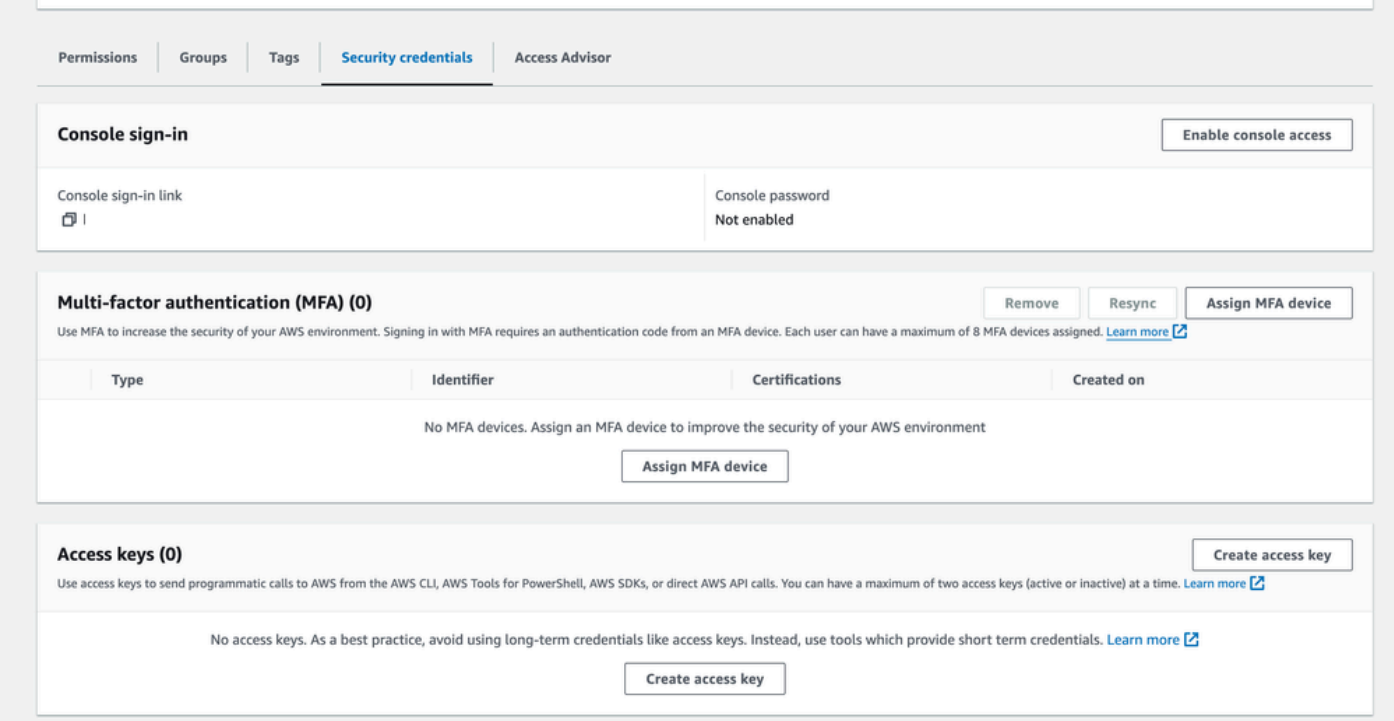


Nota: È possibile creare criteri più granulari consentendo solo un bucket specifico. Passare a Creazione criteri per creare il criterio bucket S3 in formato json.

9: Una volta creato l'utente, elencarlo e passare alla scheda Credenziali di sicurezza e fare clic su Crea chiave di accesso.

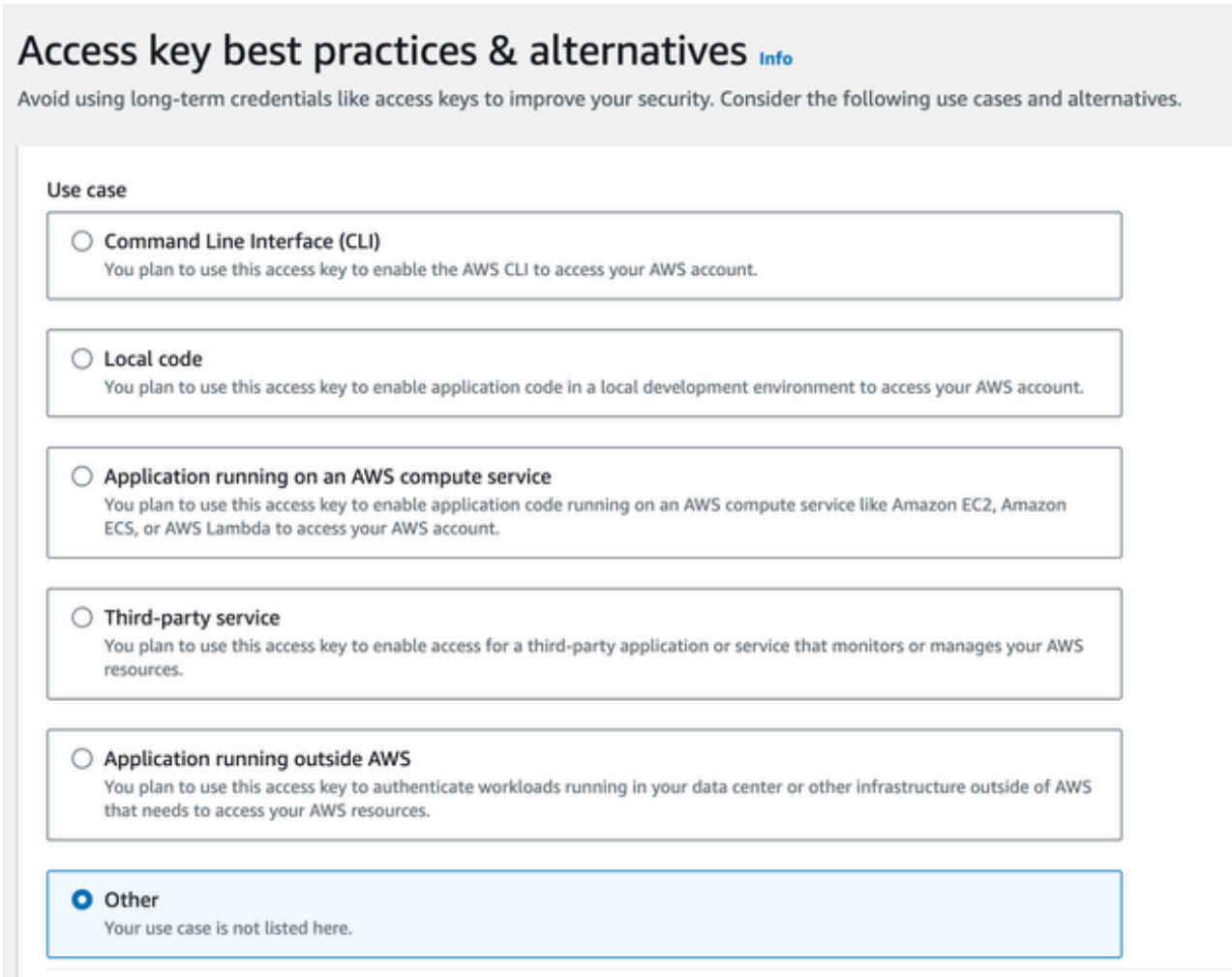


AWS-IAM

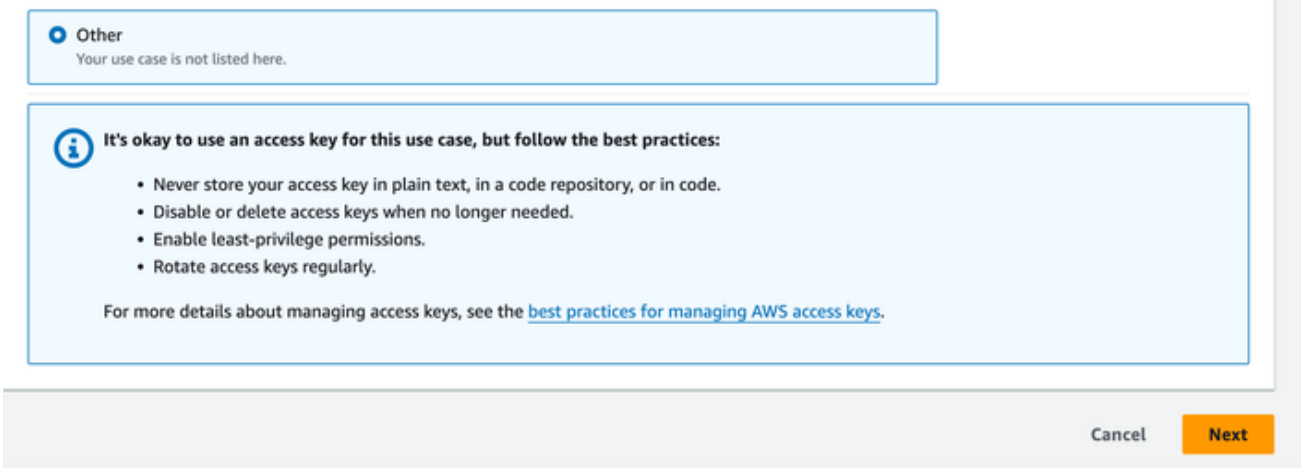


AWS-IAM

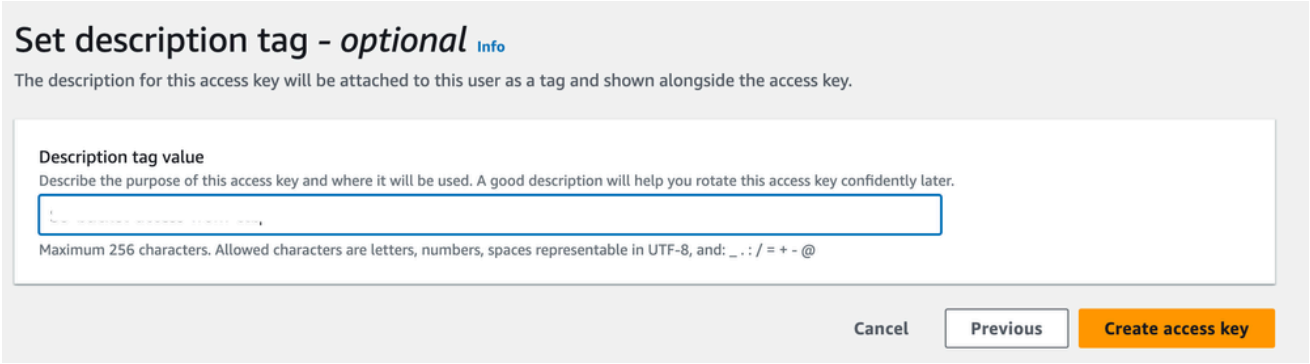
10: Selezionare l'altro pulsante di scelta e aggiungere facoltativamente un tag.



AWS-IAM

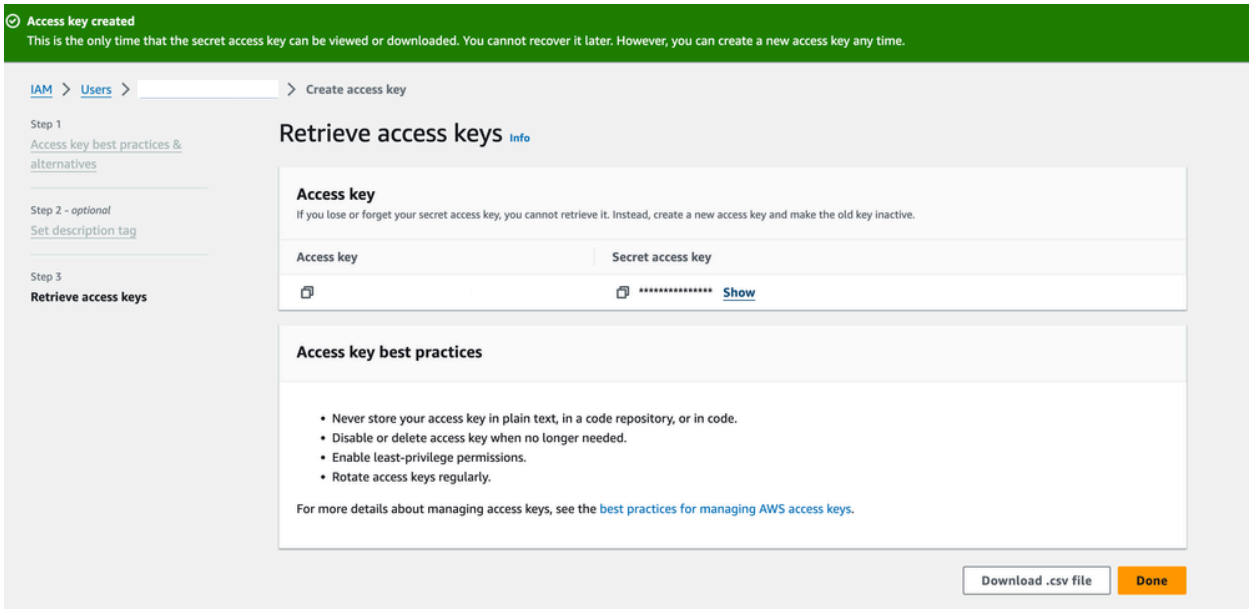


AWS-IAM



AWS-IAM

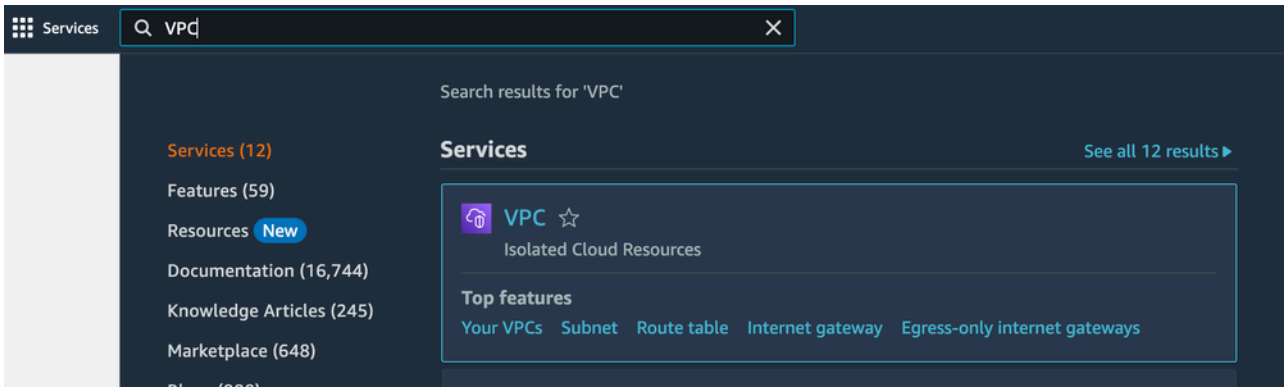
11: Fare clic su Scarica file CSV. Questa è la chiave di accesso in un file CSV e non è più disponibile per il download o la visualizzazione dopo essere usciti da questa pagina.



AWS-IAM

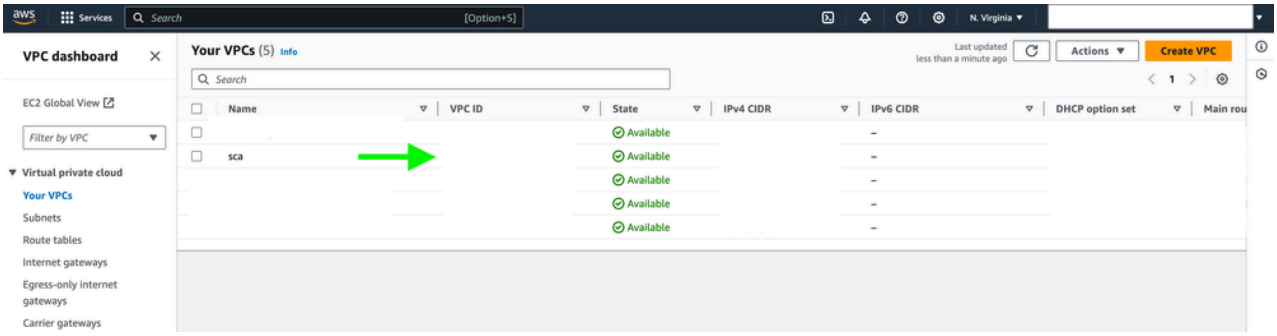
Passaggio 3. Configurare i log di flusso VPC

1: Avviare il VPC nell'area desiderata e selezionare l'opzione VPC.

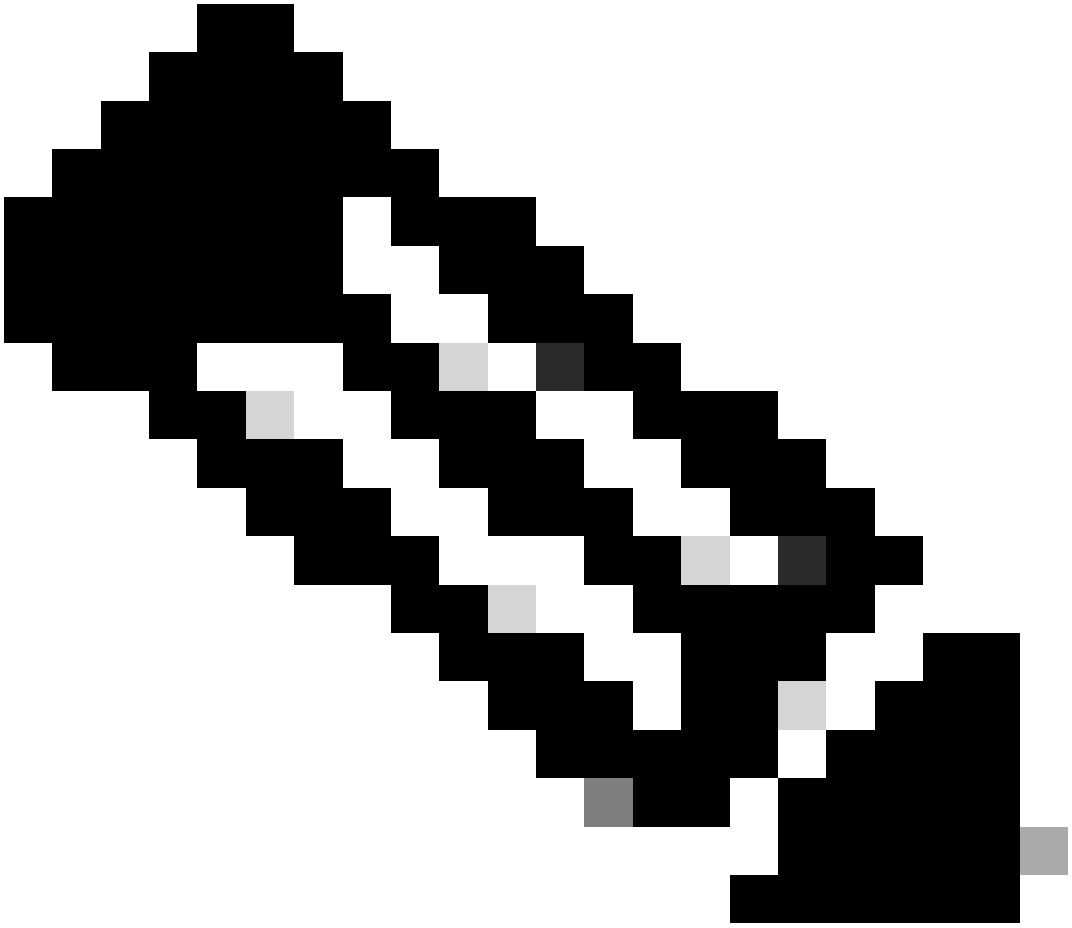


AWS-Flow-Logs

2: Selezionare il VPC dall'elenco visualizzato sullo schermo.

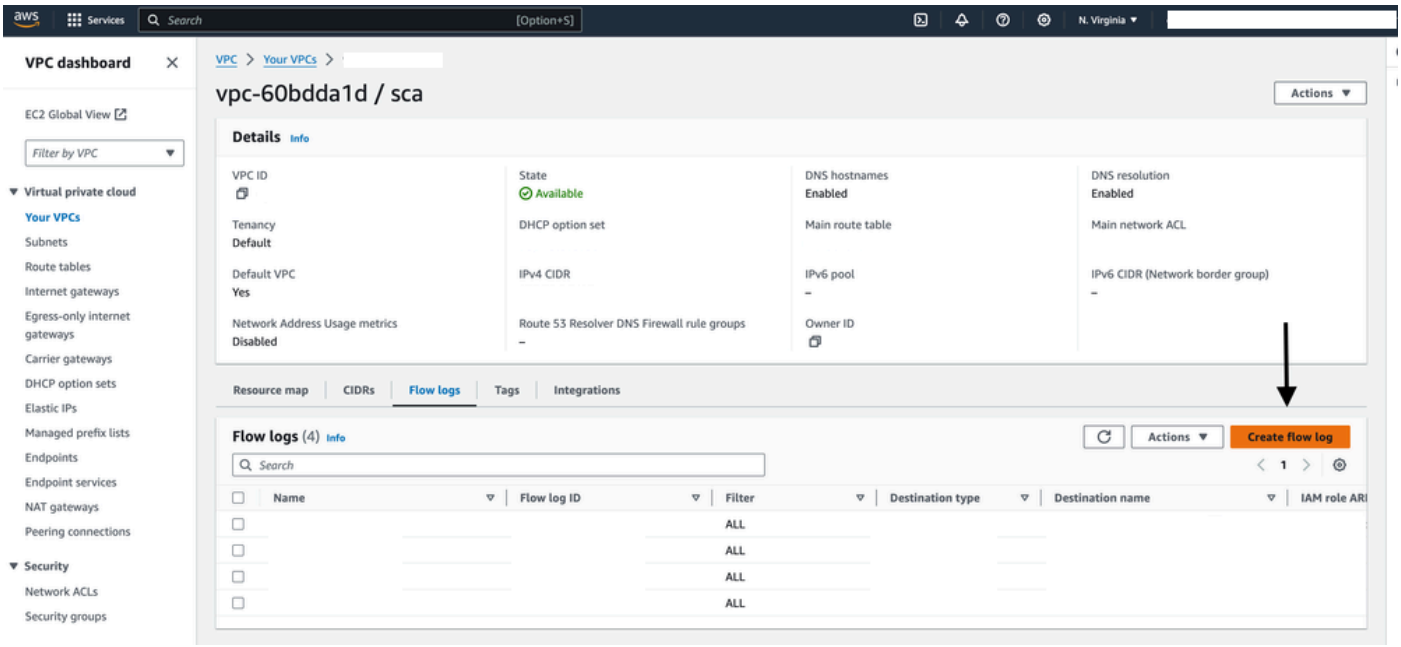


AWS-Flow-Logs



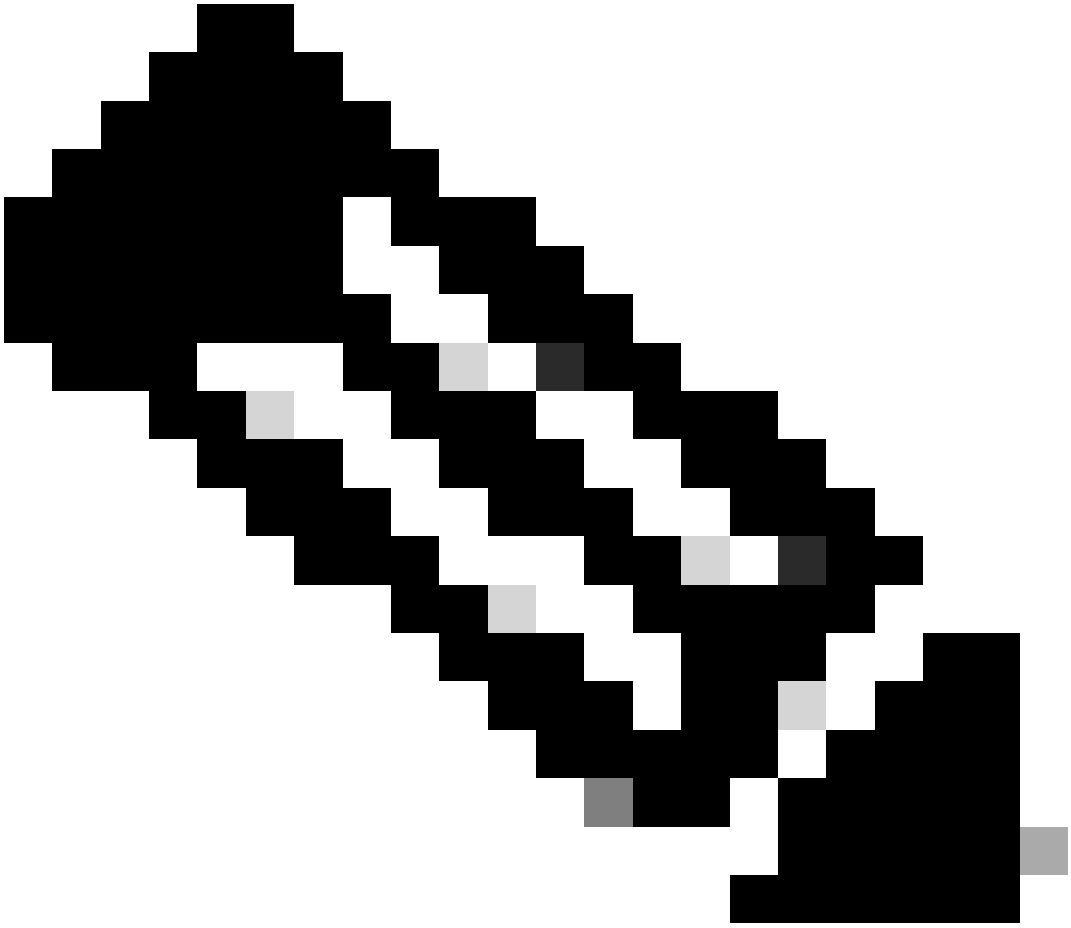
Nota: In questa demo è stato selezionato il nome VPC SCA.

3: Passare alle VPC in Virtual private cloud, passare alla scheda Log di flusso e fare clic su Crea log di flusso.



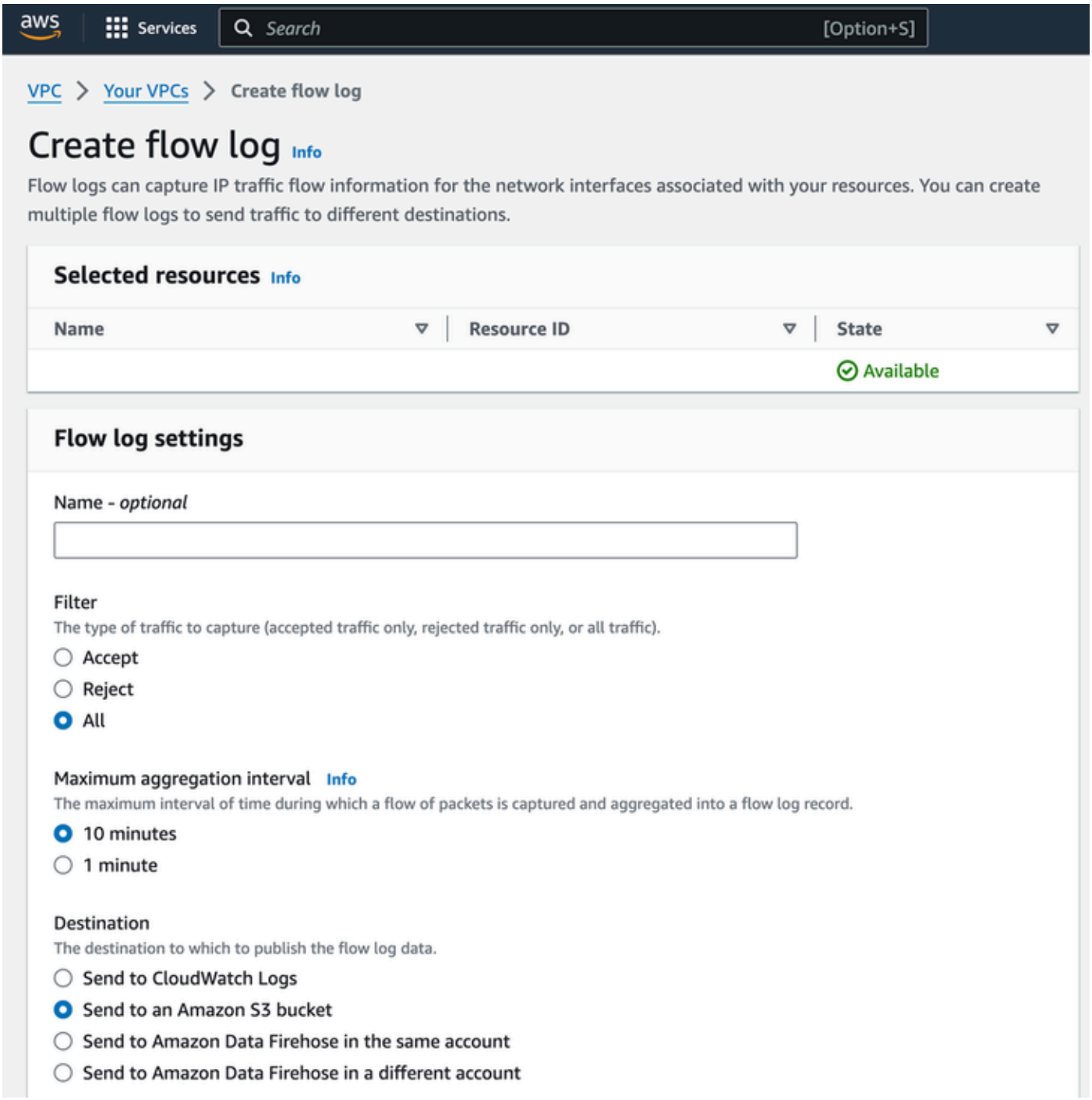
AWS-Flow-Logs

4: Assegnare un nome ai log di flusso e condividere il bucket S3 ARN creato in precedenza.

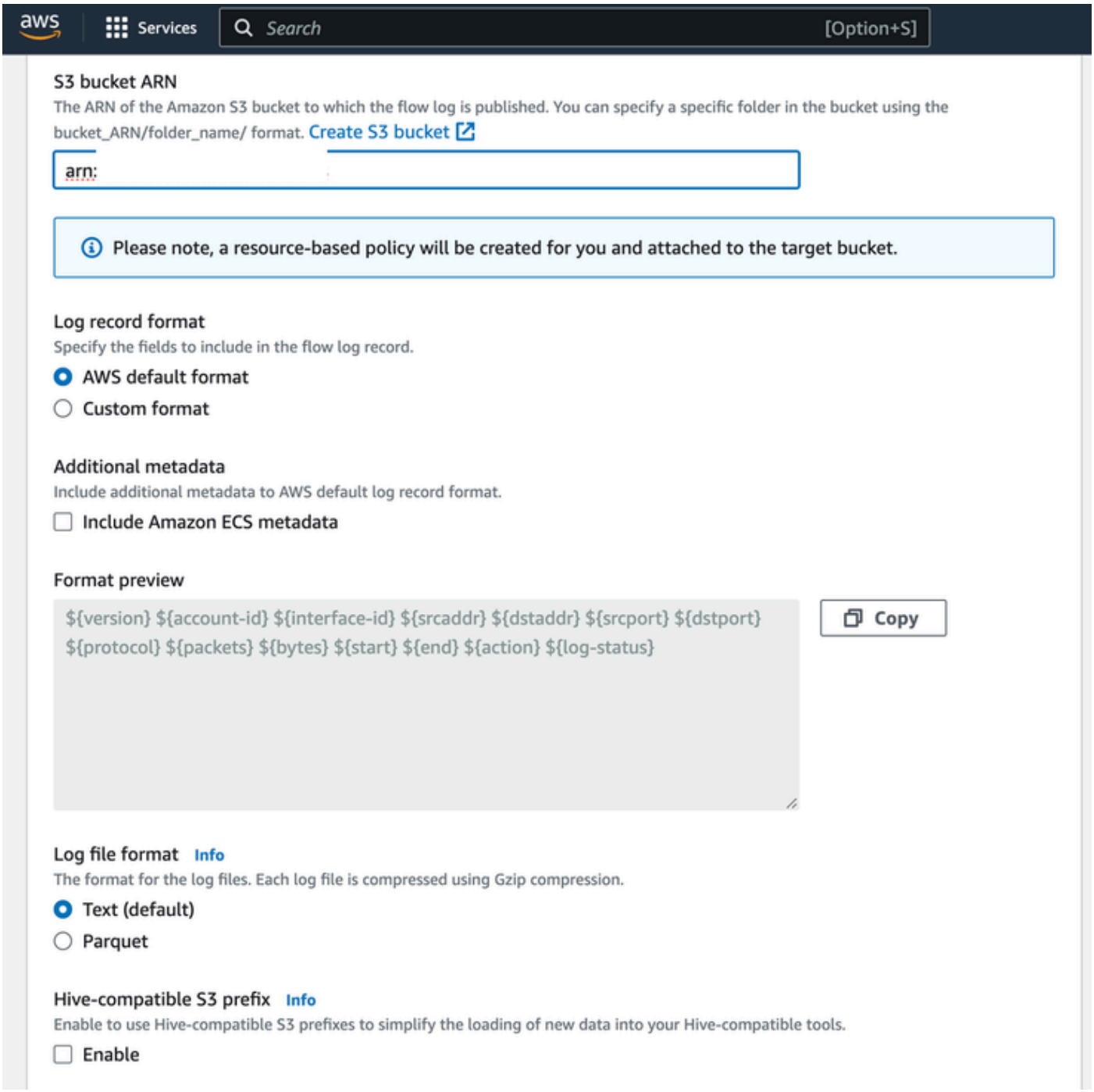


Nota: Per ARN, vedere Configurare il bucket S3 - Passaggio 6

5: È possibile scegliere di utilizzare il formato di registro predefinito di AWS o di creare un formato di registro personalizzato nel caso in cui siano necessari più campi.

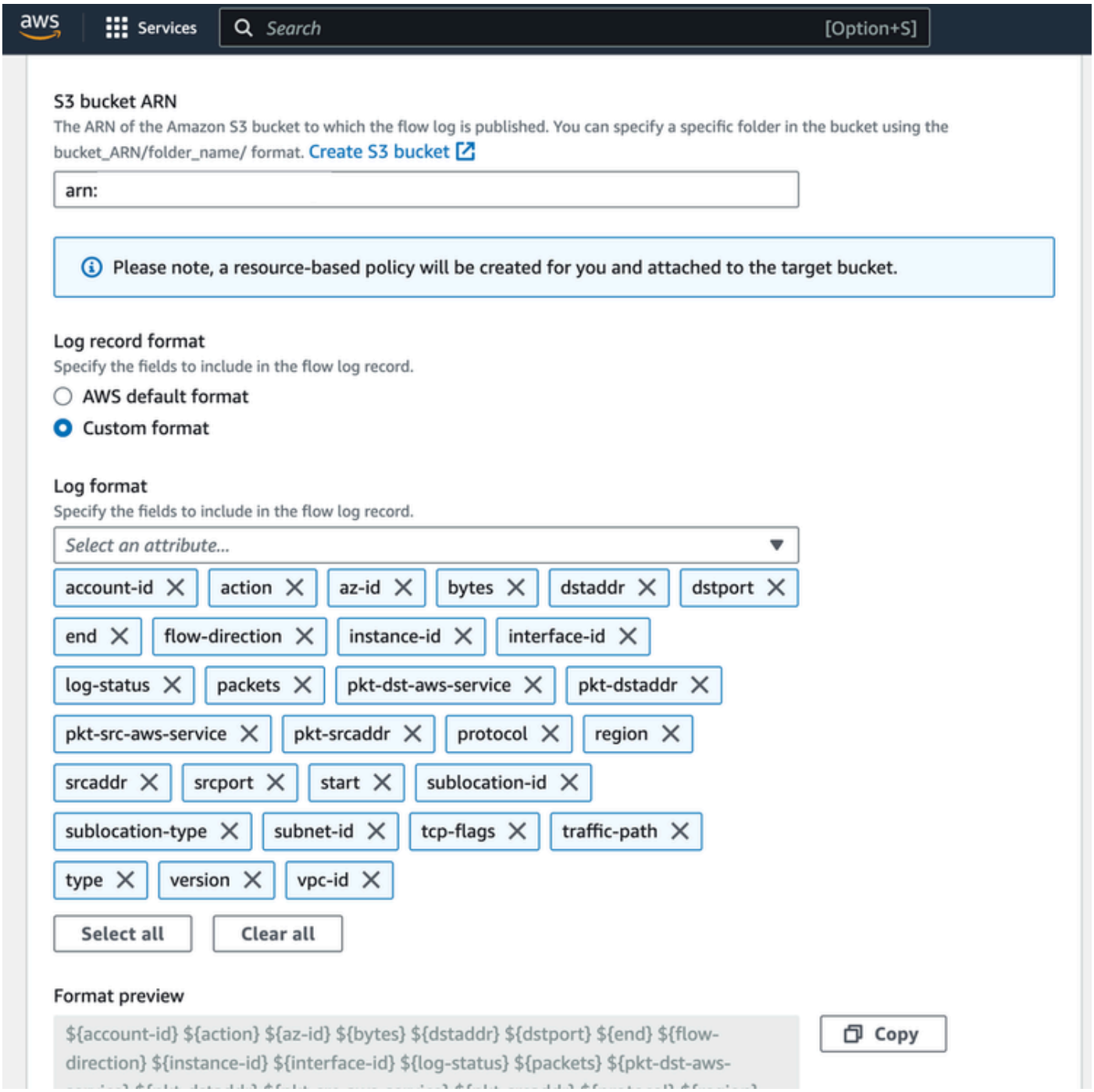


AWS-Flow-Logs

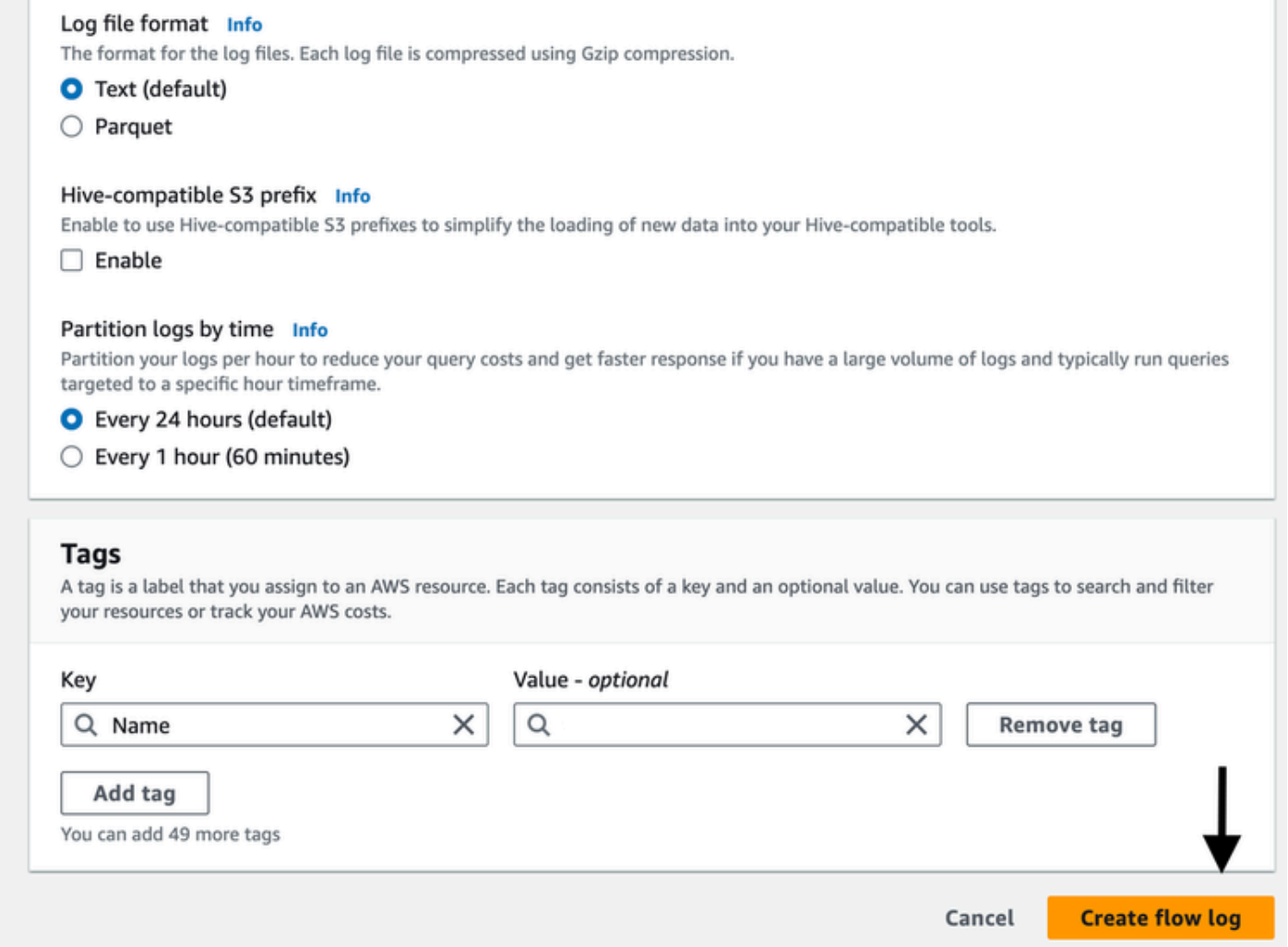


AWS-Flow-Logs

7: Fare clic su Crea log di flusso.



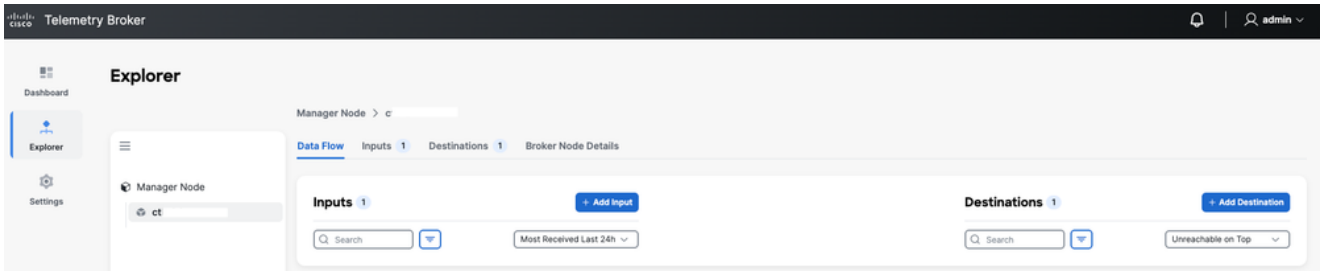
AWS-Flow-Logs



AWS-Flow-Logs

Passaggio 4. Configurare l'input VPC su CTB

1: Accedi all'interfaccia utente Web CTB, passare a Esplora risorse> scheda nodo Broker > fare clic su apri nodo Broker >Flusso di dati scheda > Fare clic su Aggiungi input.



CTB-Input-UI

2: Selezionare il tipo di input AWS VPC Flow log e fare clic su avanti.

Add Input

Select Input type

Type or Select Input

UDP Input

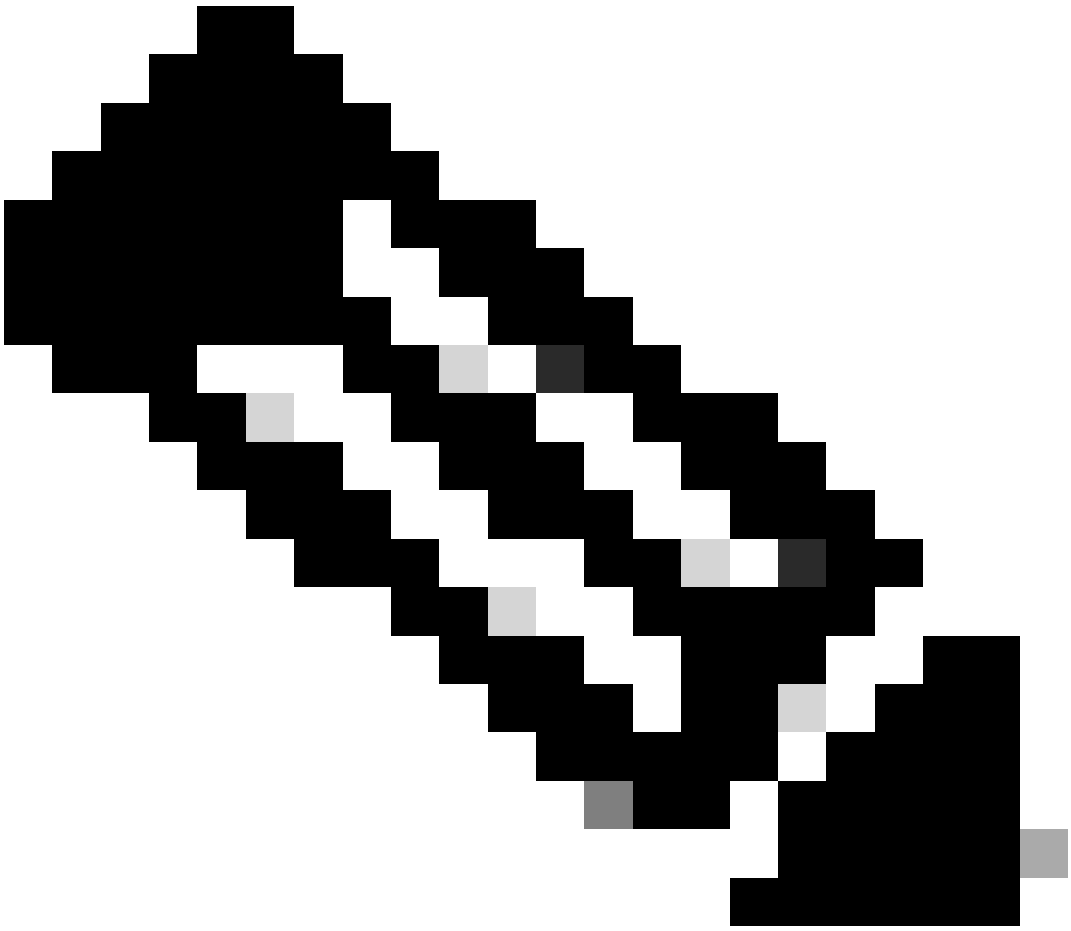
AWS VPC Flow log

AWS VPC Flow log

Azure NSG Flow log

Flow Generator Input

: qualsiasi indirizzo IP configurato come indirizzo IP di input (indirizzo IP univoco non condiviso da nessun altro esportatore) viene segnalato come esportatore per i dati netflow trasformati.



Nota: Per l'ID della chiave di accesso AWS, vedere Configurare l'utente IAM per la chiave di accesso con i criteri di accesso S3, passo 9

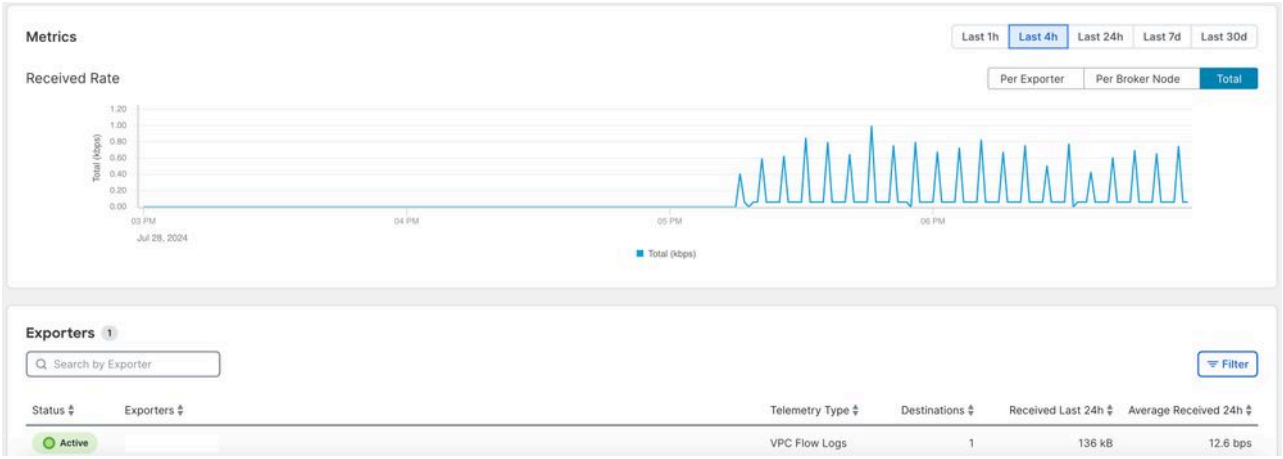
Verifica

Dopo alcuni minuti di configurazione dell'input VPC AWS, la colonna di stato diventa attiva se il bucket S3 AWS contiene dati.

Verificare lo stato dell'input VPC AWS attenendosi alla seguente procedura.

1: Accedere all'interfaccia utente CTB e selezionare Explorer> Broker node tab > click openbroker node > switch tab toInput > Click open AWS input.

2: Verificare che i log di flusso AWS configurati abbiano lo stato attivo e che la metrica ricevuta presenti un grafico in aumento.



CTB-Input-UI

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).