# تكوين سجلات تدفق AWS VPC لإدخال CTB

## المحتويات



## المقدمة

يصف هذا المستند كيفية تكوين سجلات تدفق VPC كإدخال إلى وسيط بيانات تتبع الاستخدام (CTB) من Cisco.

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Amazon Web Services (AWS)
- إدارة CTB.

### المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- CTB (الإصدار 2.2.1+)
- AWS

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

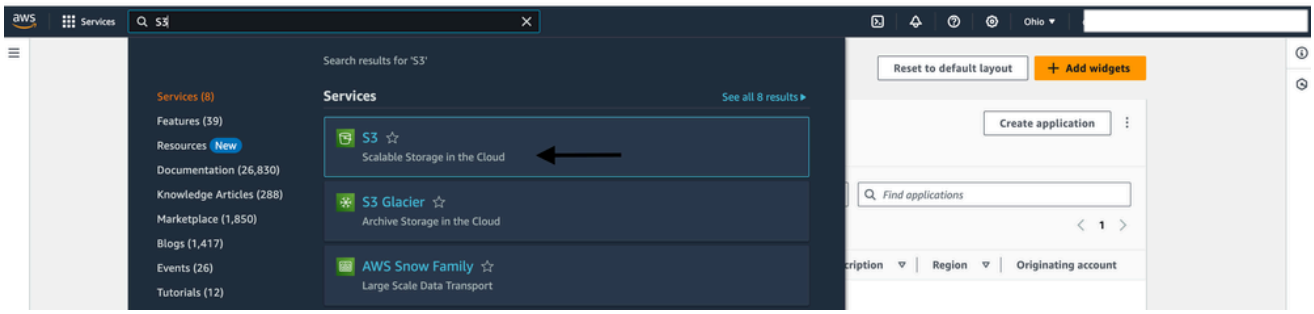
## خطوات التكوين

### الخطوة 1. تكوين دلو S3 في AWS

1: سجل الدخول إلى وحدة تحكم إدارة AWS باسم المستخدم وكلمة المرور.

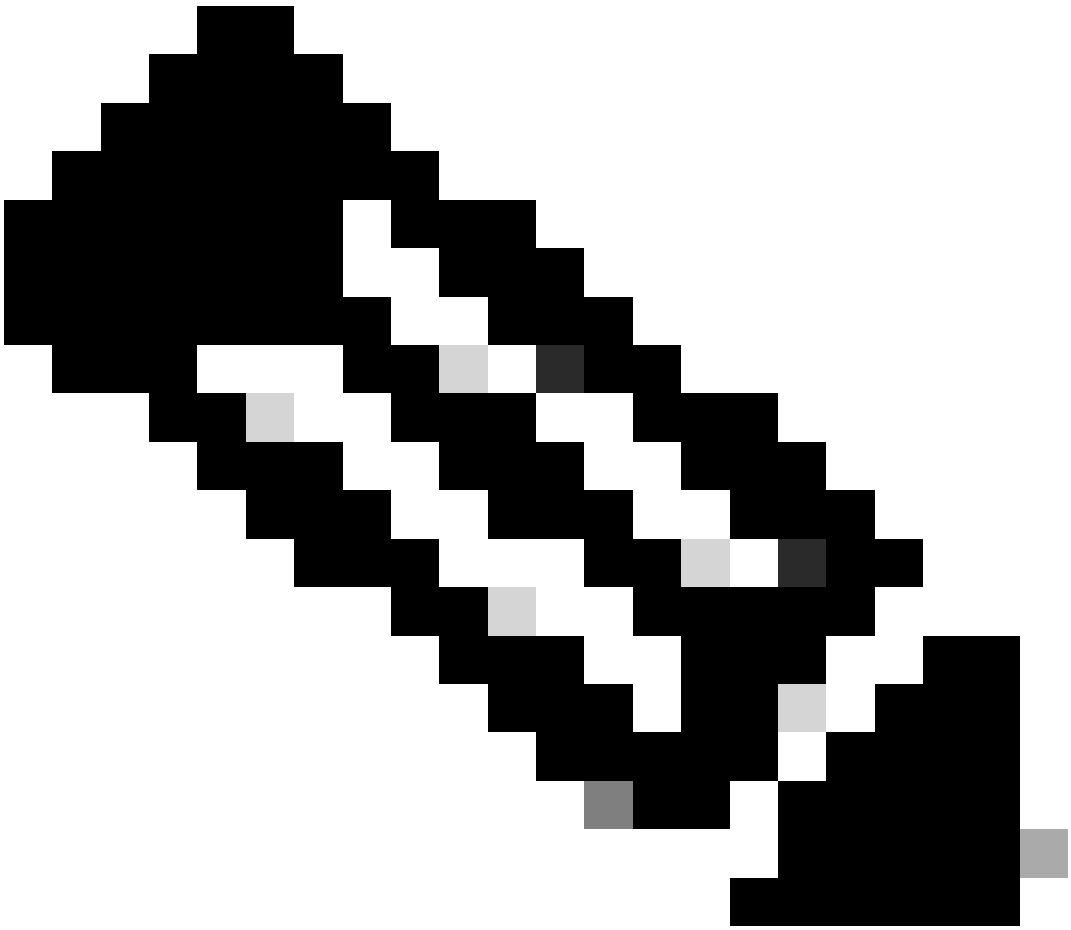
2: تأكد من تسجيل الدخول إلى المنطقة المناسبة.

3: انتقل إلى شريط البحث والنوع S3.




لوحة معلومات AWS

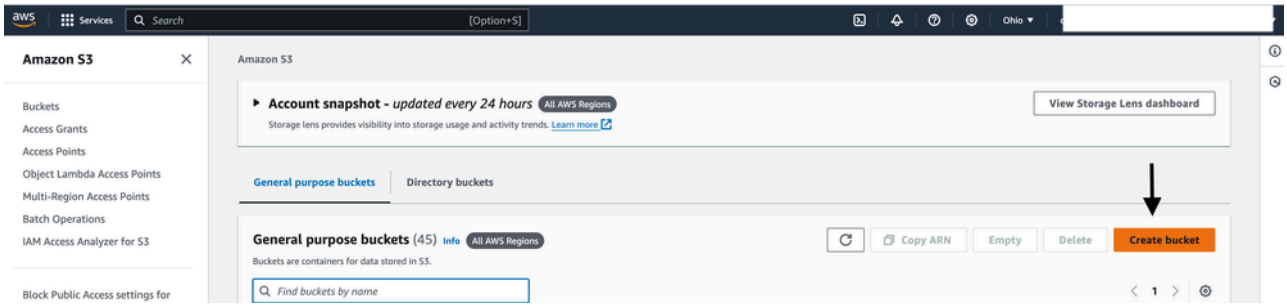
---



ملاحظة: في العرض التوضيحي، لقد قمت بتحديد منطقة أوهايو التي تضم منطقة الإتاحة Us-East-2، والتي تظهر بجوار أيقونة العداد مباشرة.

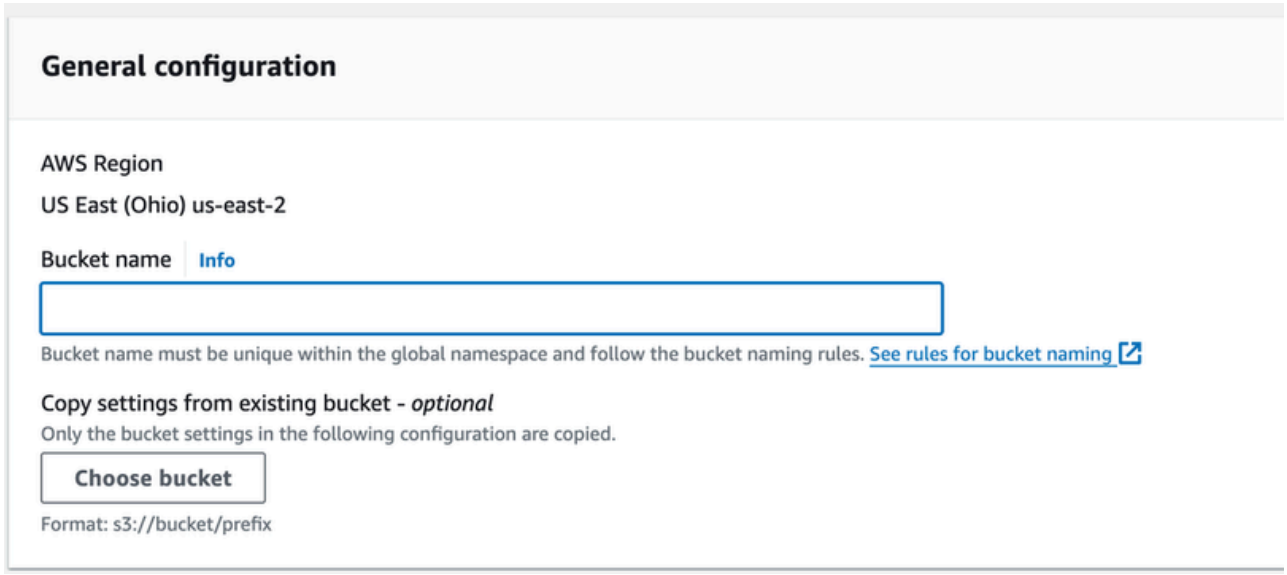
---

4: انقر فوق إنشاء مستودع.

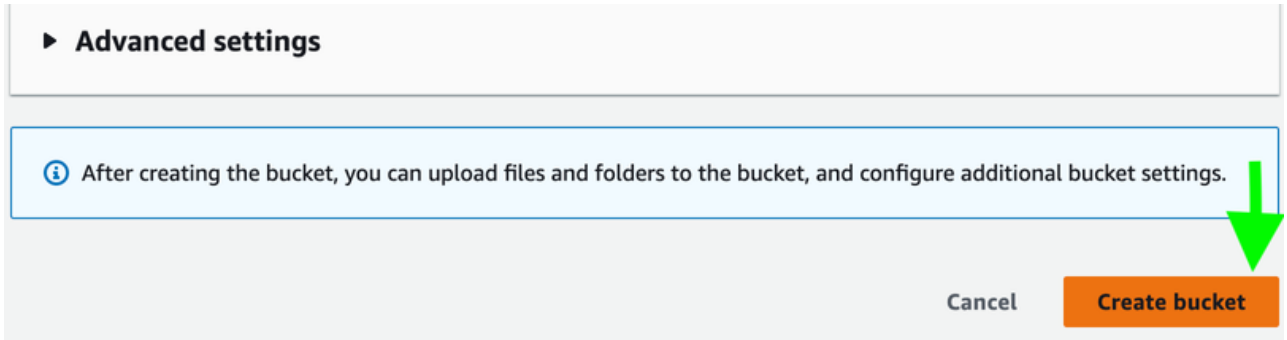



AWS-S3

5: قم بتسديد اسم وترك كل خيار كما هو وانقر إنشاء.

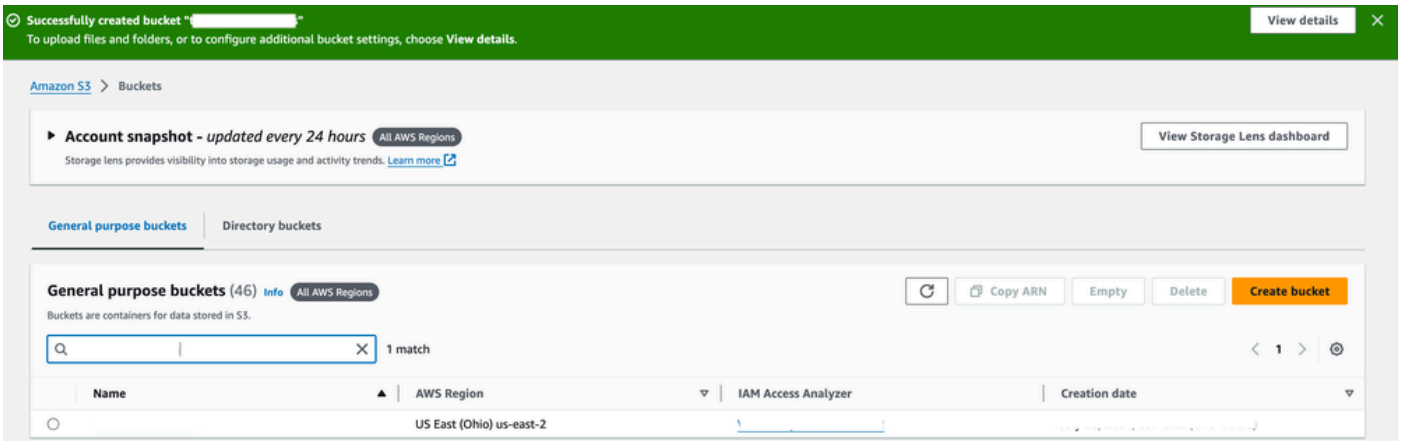



AWS-S3

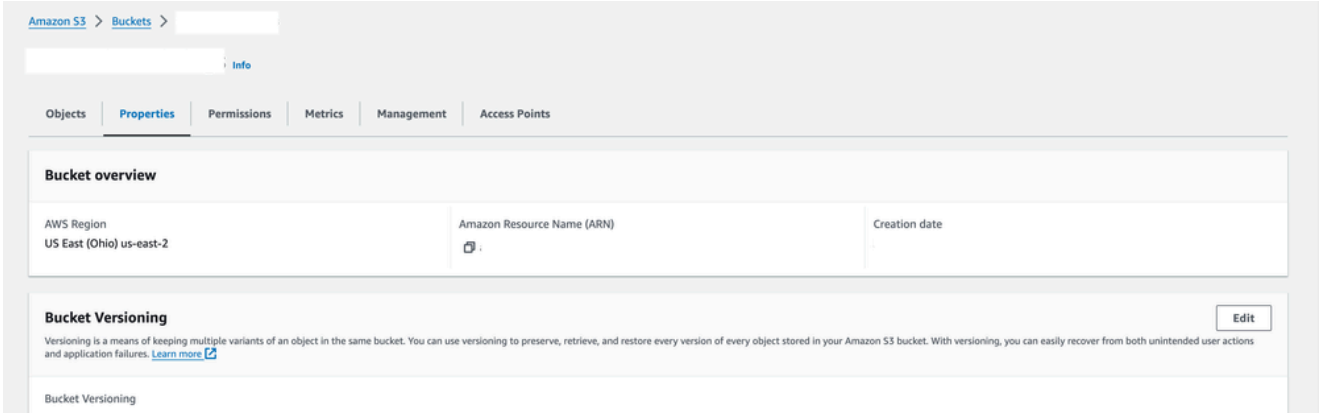



AWS-S3

6: وبمجرد إنشاء المستودع بنجاح، احفظ ARN الخاص بالدلو والذي سيتم إستخدامه لاحقا أثناء التكوين.



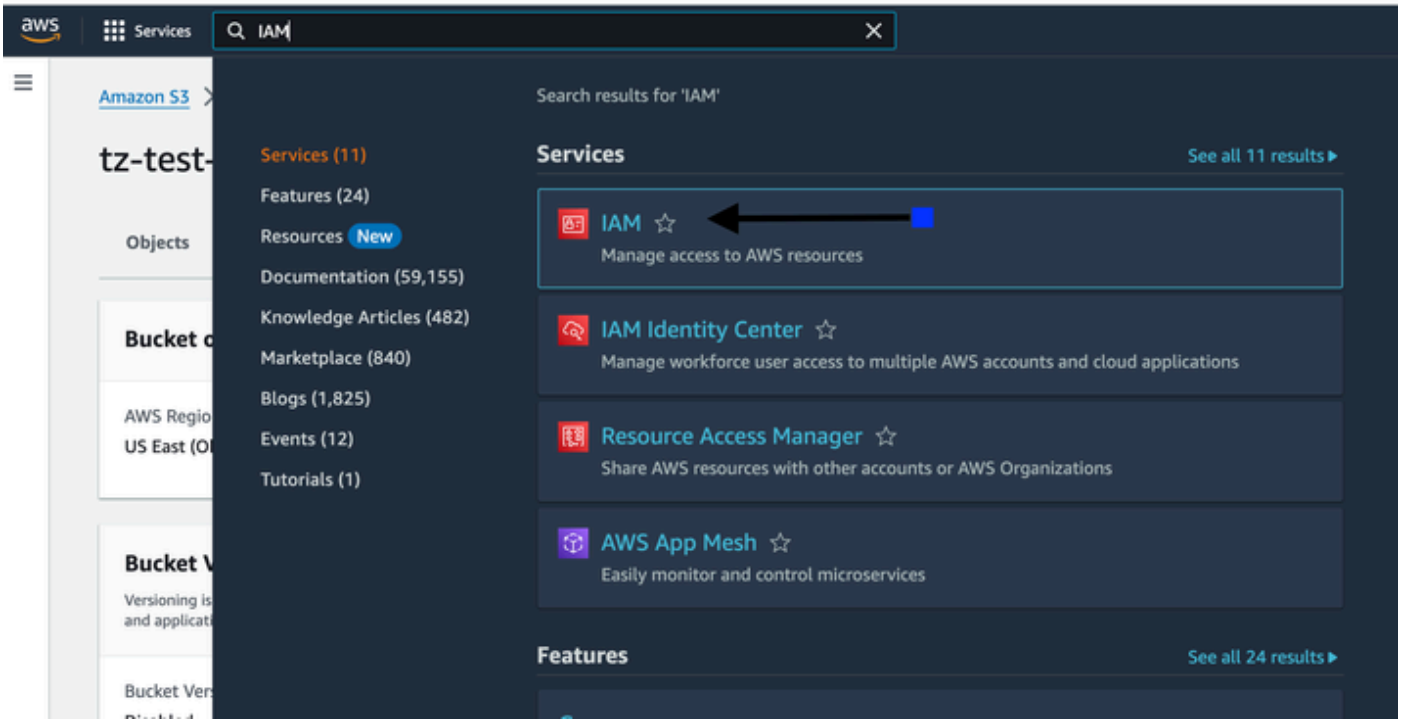

AWS-S3




AWS-S3

## الخطوة 2. قم بإنشاء مستخدم IAM باستخدام مفتاح الوصول ونهج مستودع S3 المرفق

1: قم بتشغيل IAM من شريط البحث AWS.




أوس-إيام

2: انتقل إلى المستخدمين.


# Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

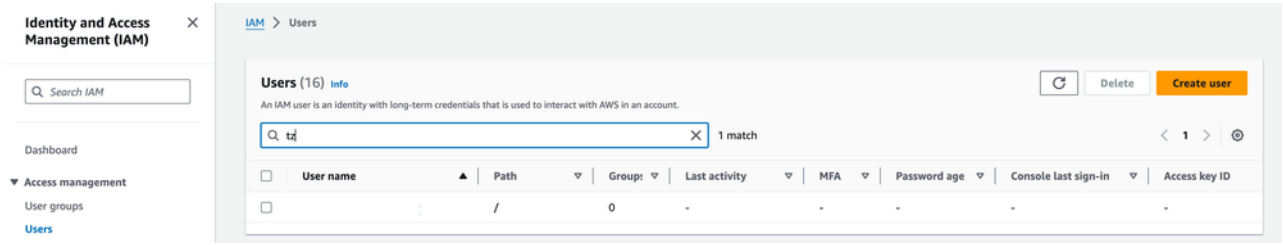
Users

Roles

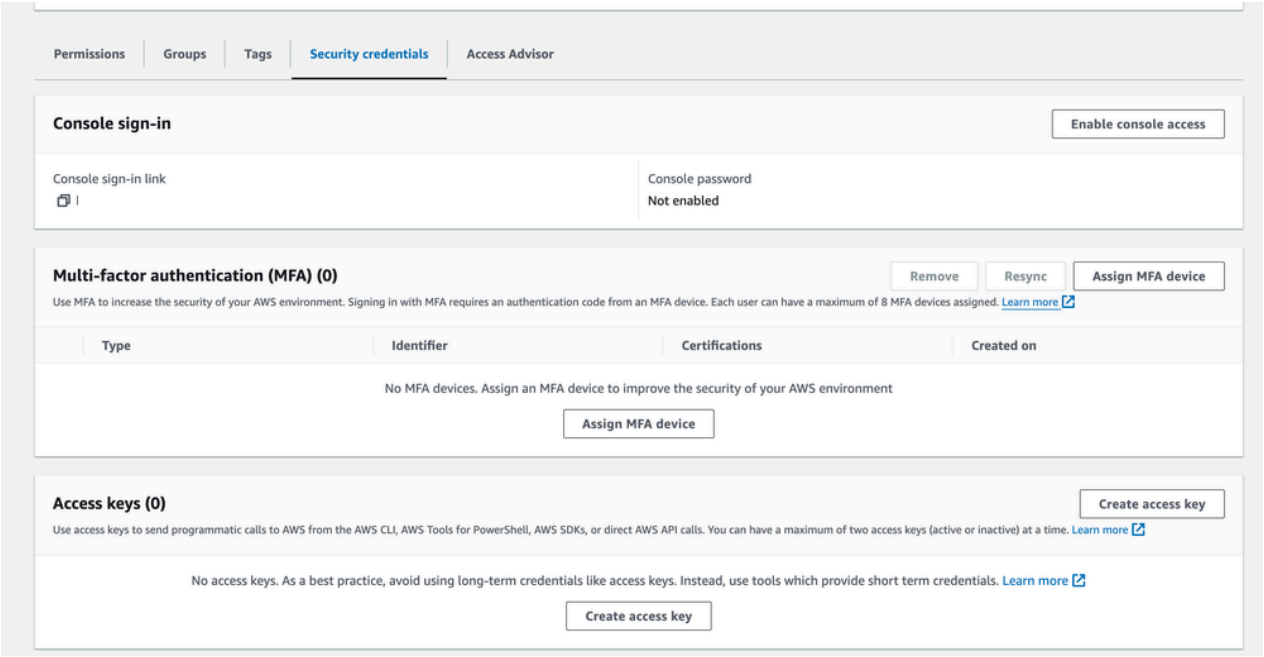
Policies

يمكنك إنشاء نهج أكثر دقة عن طريق السماح بسطل معين فقط أيضا، الرجاء الانتقال إلى إنشاء النهج لإنشاء نهج S3 Bucket بتنسيق json.

9: بمجرد إنشاء المستخدم، قم بسرد المستخدم وانتقل إلى علامة التبويب بيانات اعتماد الأمان وانقر فوق إنشاء مفتاح الوصول.

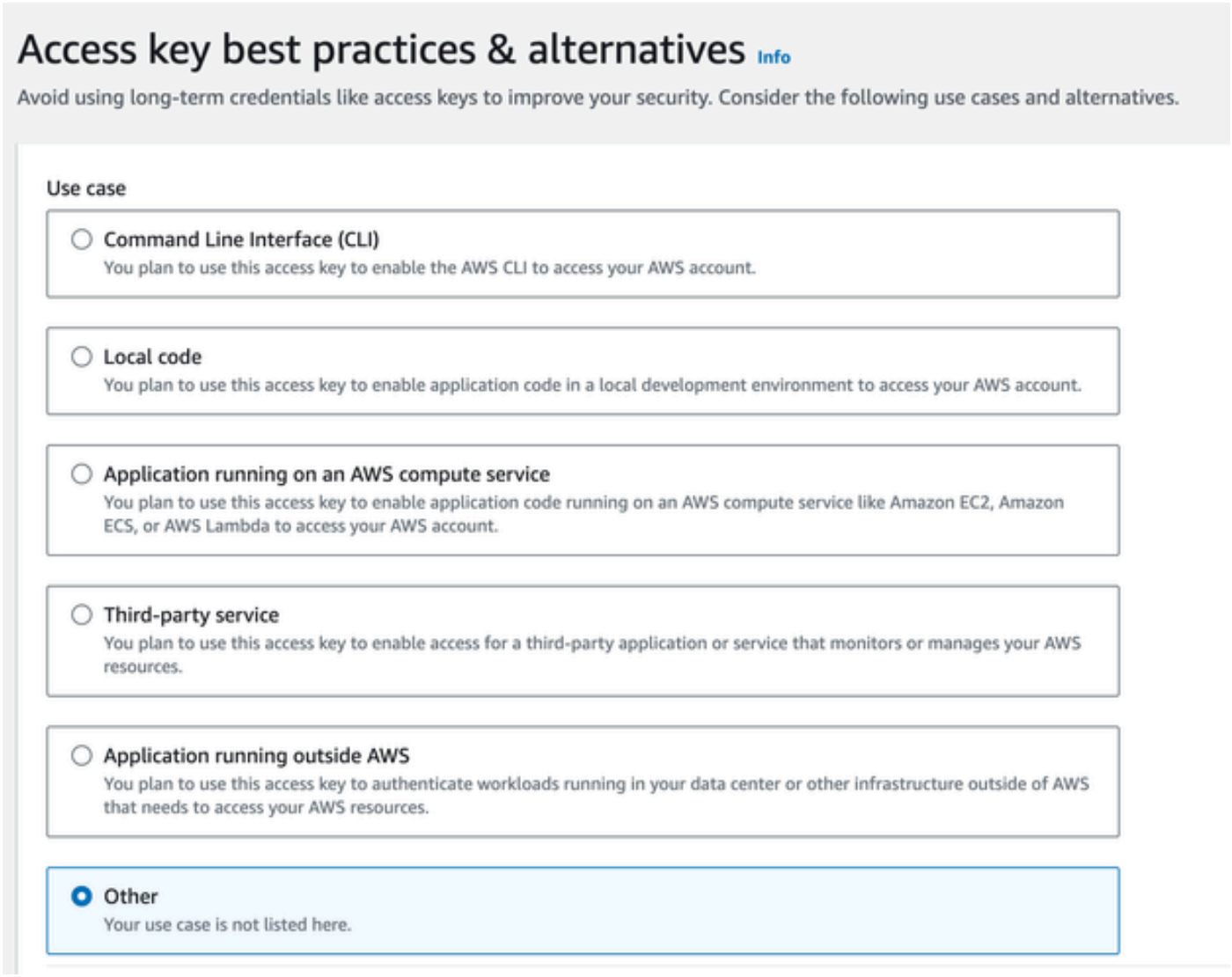



أوس-يام

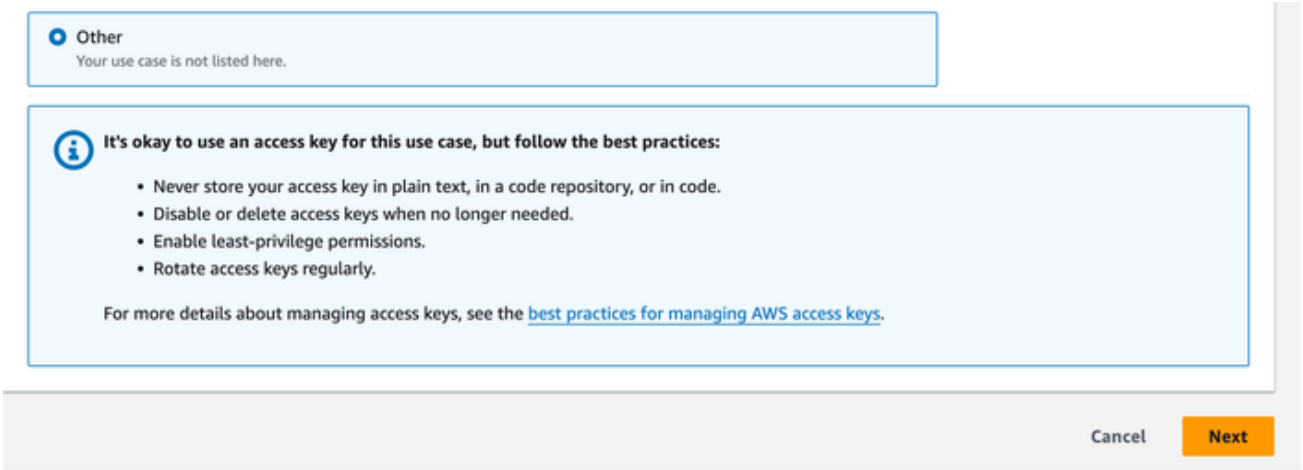



أوس-يام

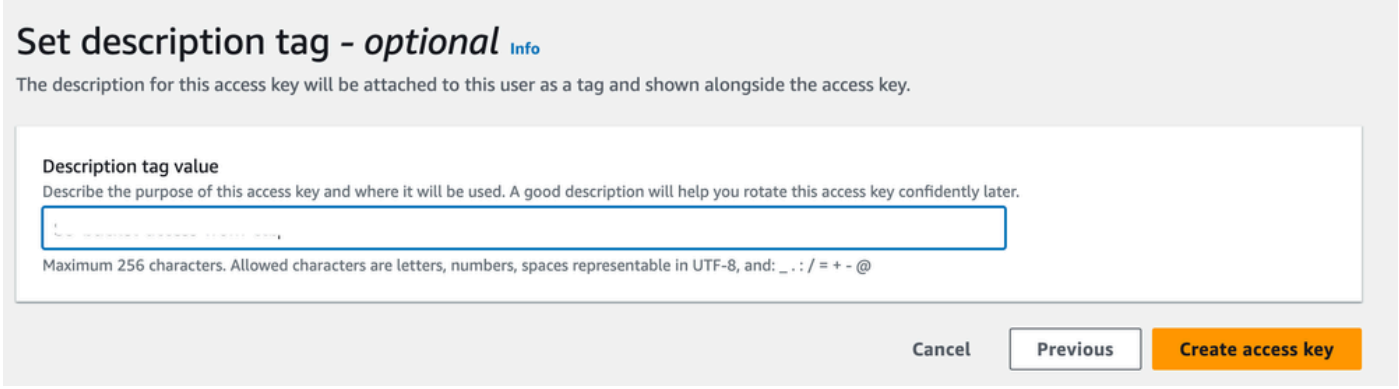
10: حدد زر الخيار الآخر وقم بإضافة علامة تمييز إختياري.




م اي-س وأ

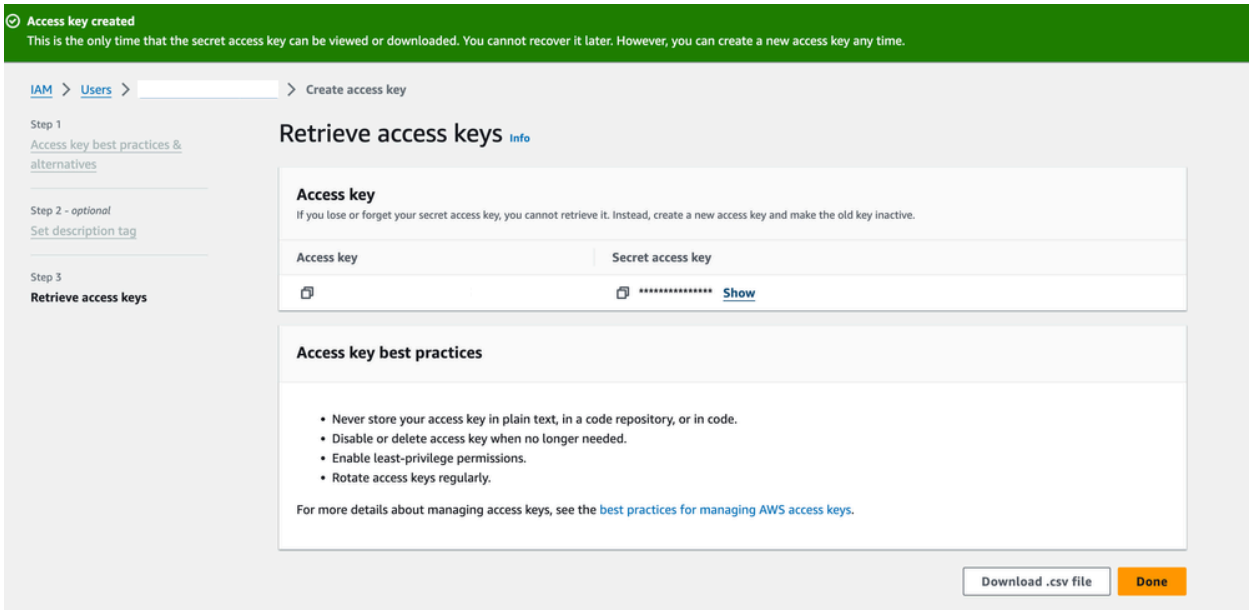



م اي-س وأ




أوس-إيه

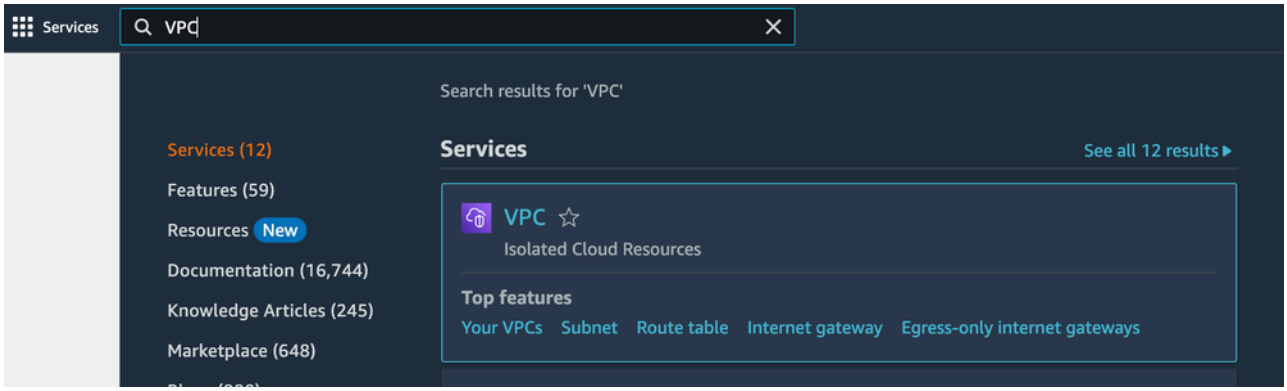
انقر فوق تنزيل ملف csv. هذا هو مفتاح Access في ملف csv ولم يعد متوفرا للتنزيل أو العرض بمجرد الانتقال من هذه الصفحة.




أوس-إيه

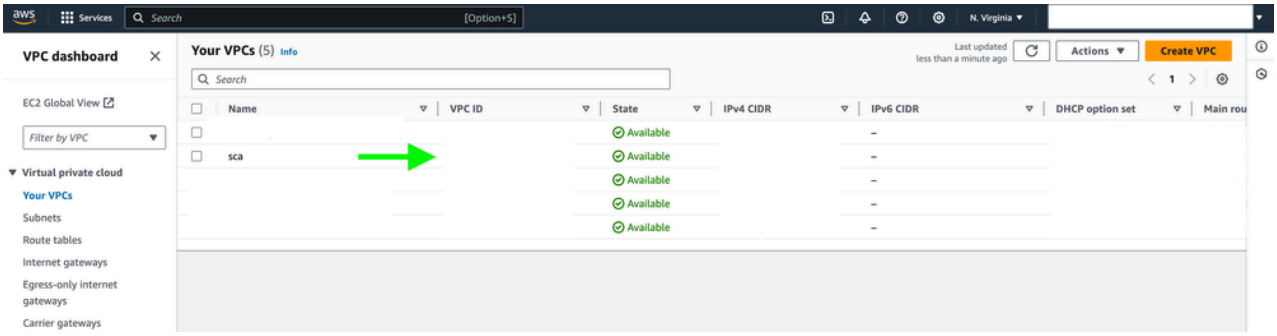
## الخطوة 3. تكوين سجلات تدفق VPC

1: قم بتشغيل جهاز VPC لديك على المنطقة التي تريدها وانتقل إلى خيار جهاز VPC الخاص بك.



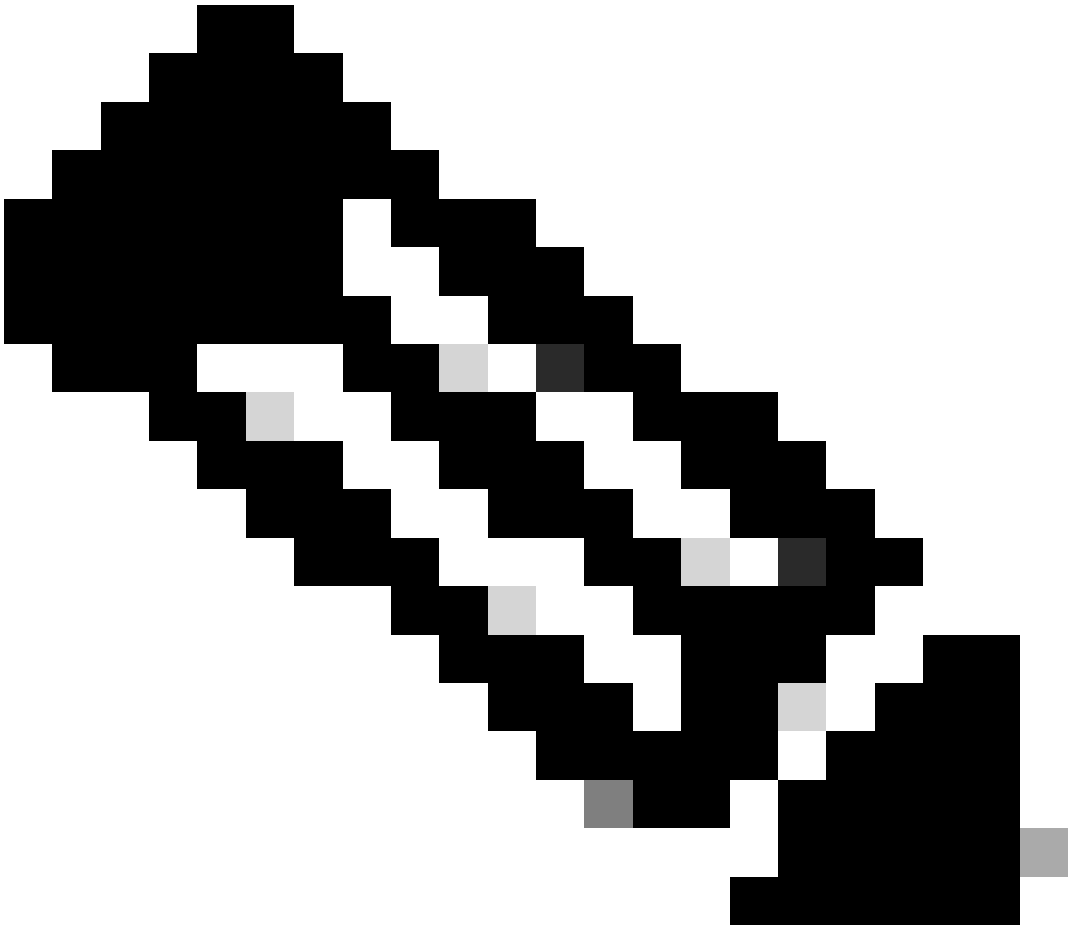

AWS-Flow-LOG

2: حدد VPC الخاص بك من القائمة المعروضة على الشاشة.




AWS-Flow-LOG

---

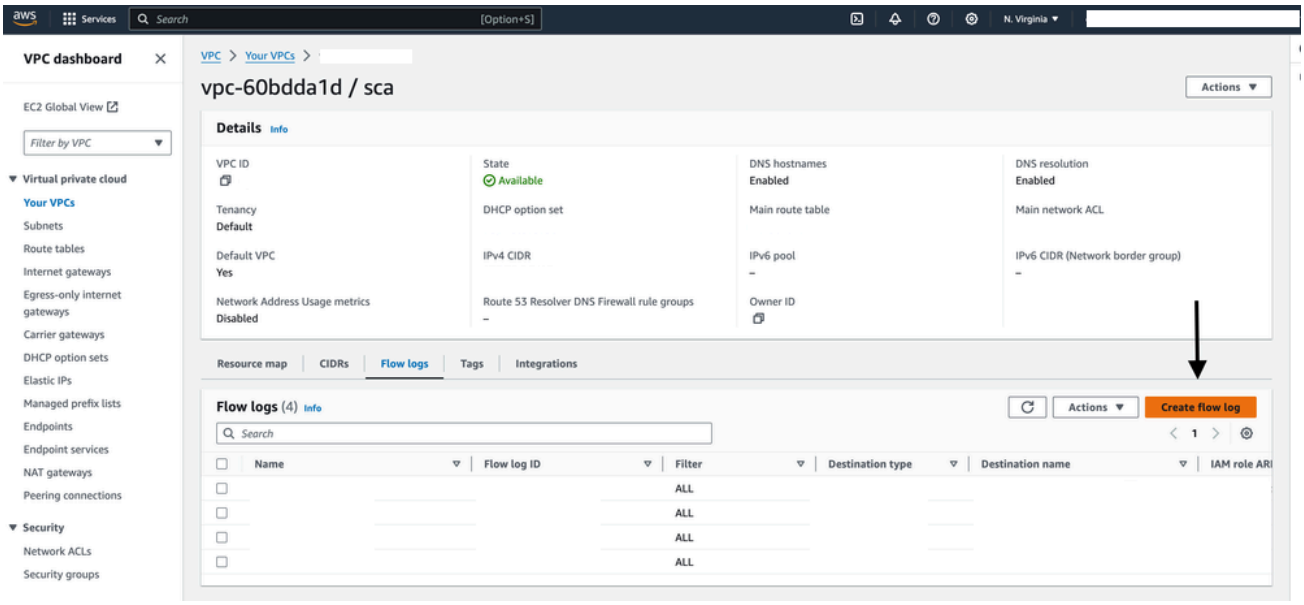


ملاحظة: لقد حددت SCA لاسم VPC في هذا العرض التوضيحي.

---

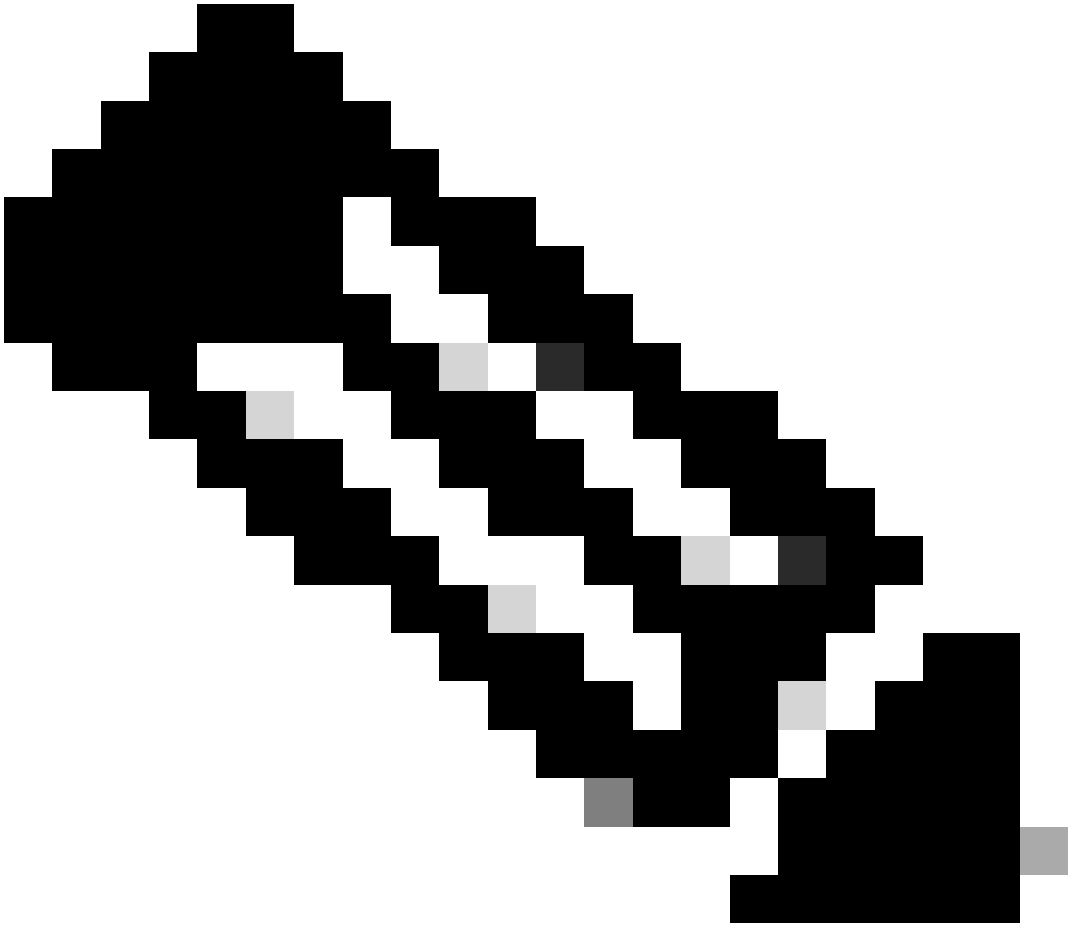
3: انتقل إلى شبكات VPC الخاصة بك ضمن السحابة الخاصة الظاهرية، وقم بالتبديل إلى

علامة التبويب سجلات التدفق وانقر فوق إنشاء سجلات التدفق.



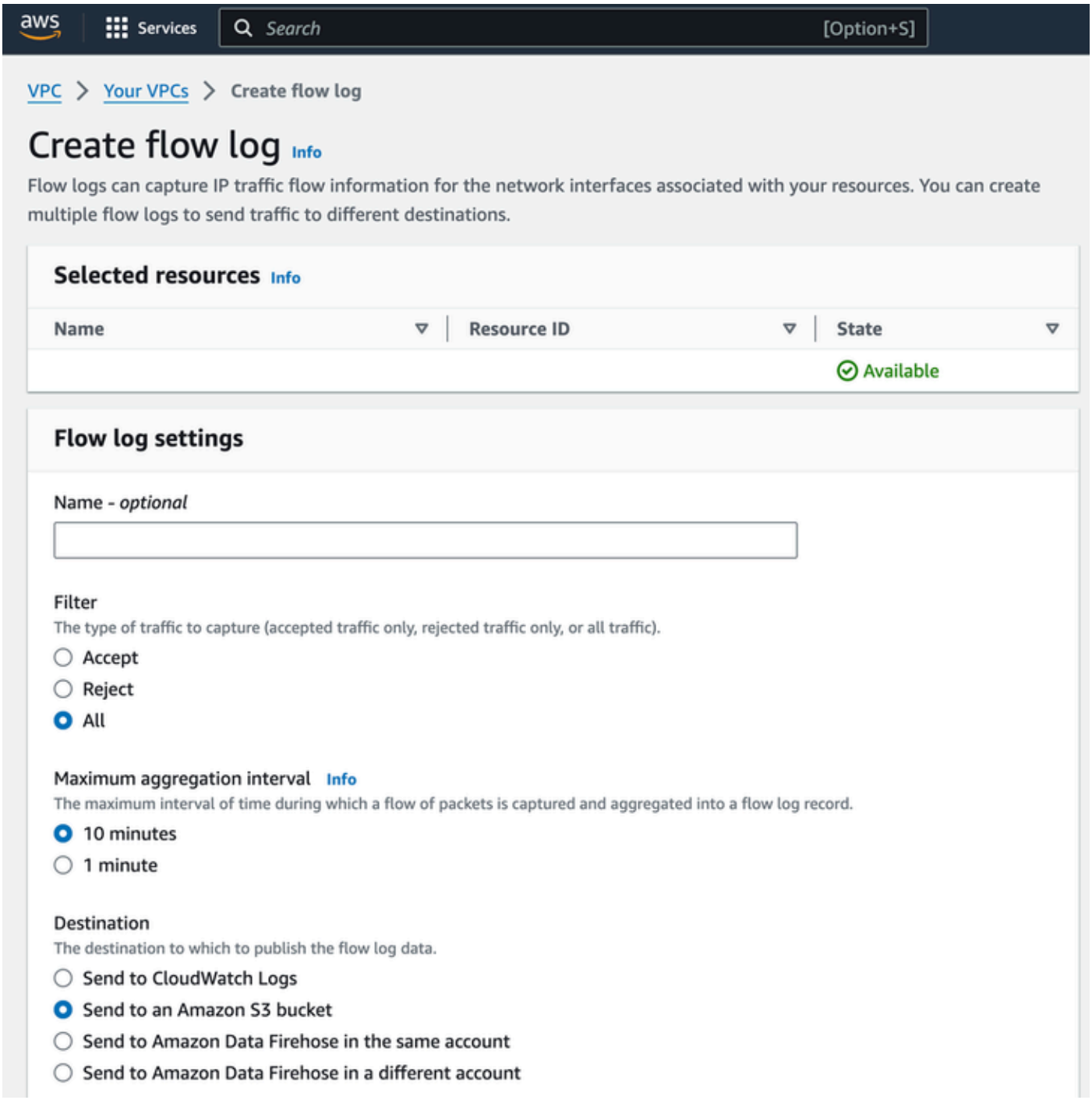

AWS-Flow-LOG

4: امنح سجلات التدفق الخاصة بك اسما وشارك S3 Cket ARN الذي تم إنشاؤه سابقا.

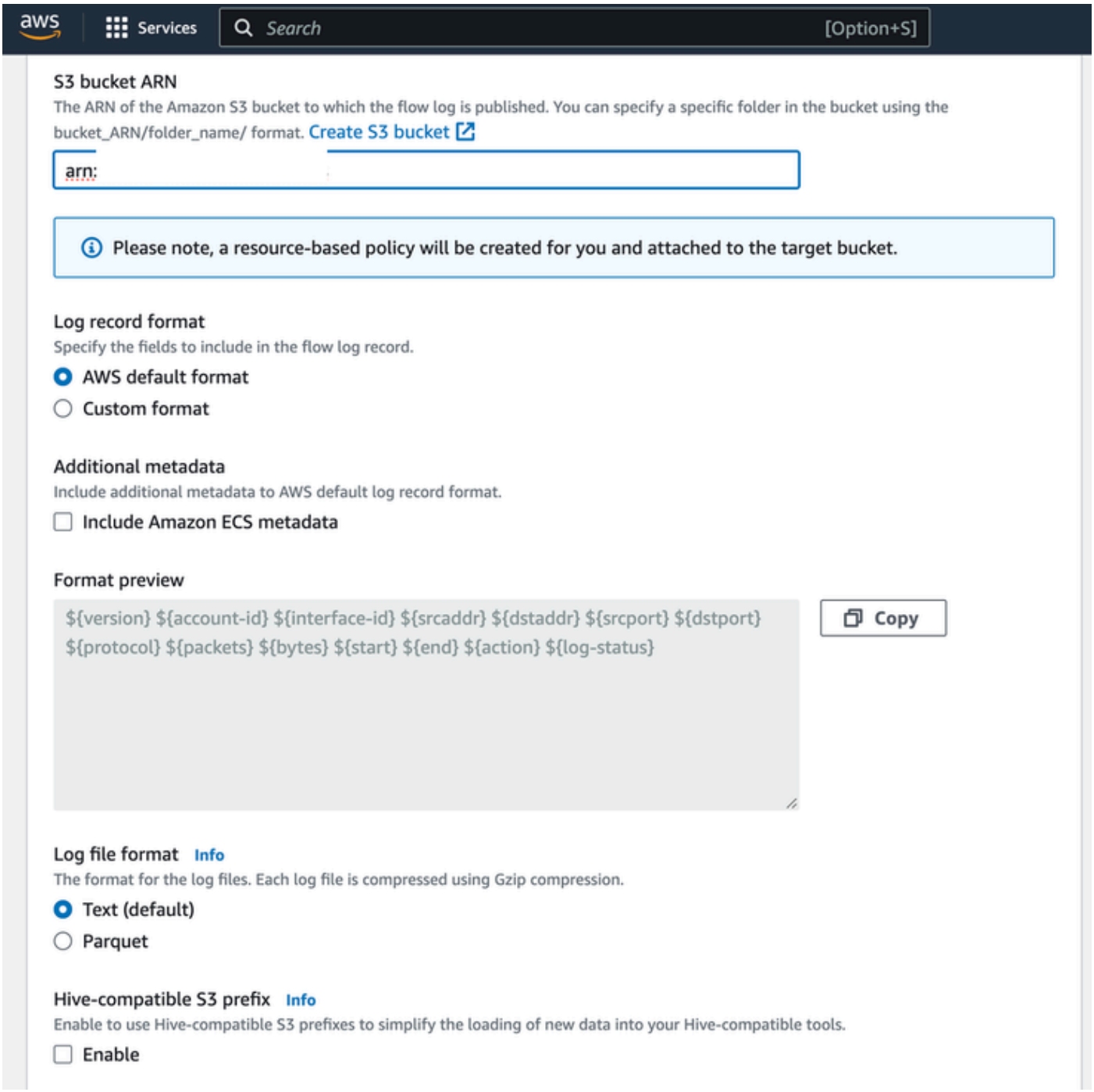


مالحظة: ل ARN، راجع تكوين دلو S3 - الخطوة 6

5: لديك خيار للذهاب بتنسيق السجل الافتراضي ل AWS أو إنشاء تنسيق سجل مخصص في حالة الحاجة إلى مزيد من الحقول.

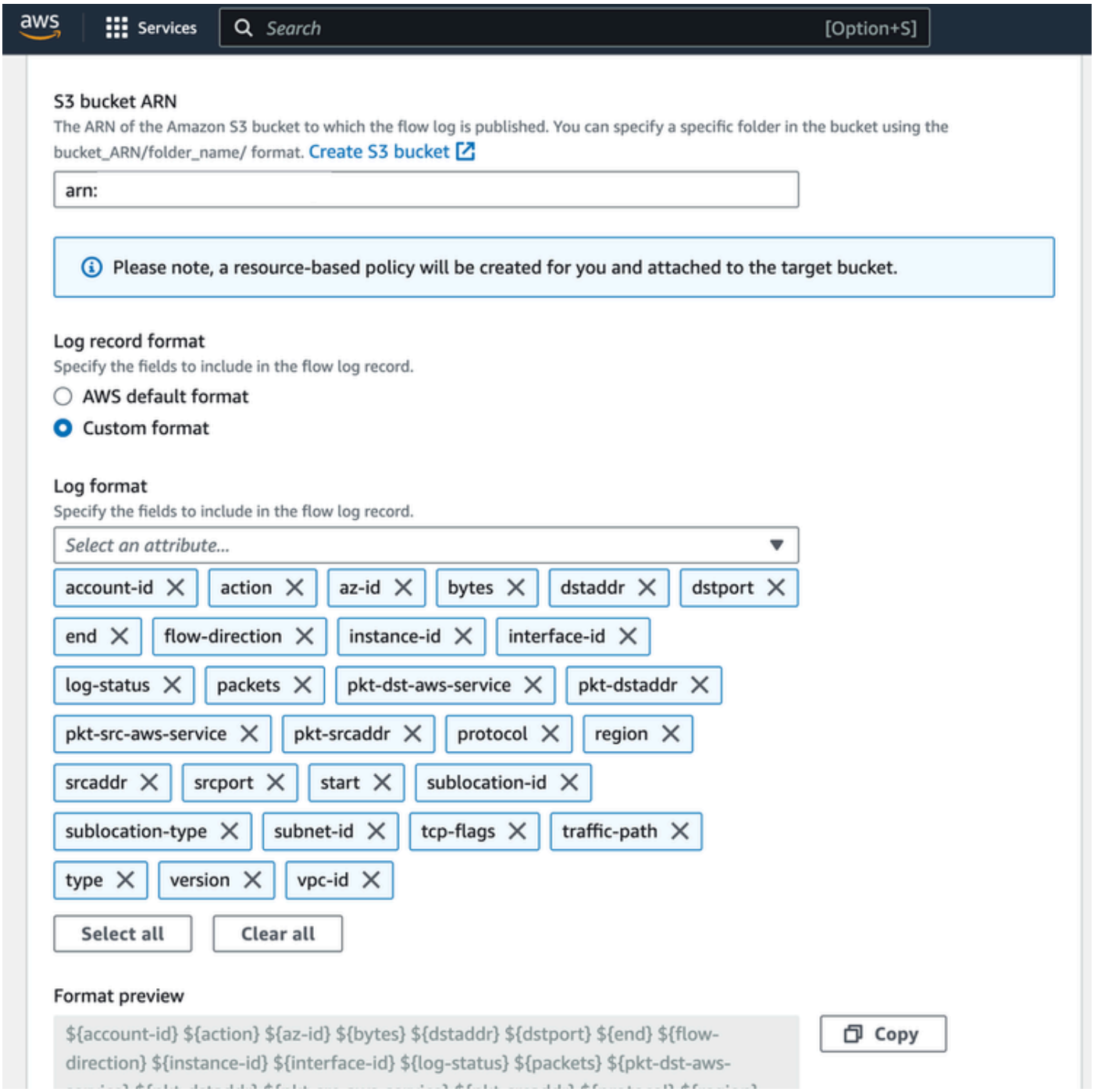

aws
Services
Search
[Option+S]
VPC > Your VPCs > Create flow log
Create flow log Info
Flow logs can capture IP traffic flow information for the network interfaces associated with your resources. You can create multiple flow logs to send traffic to different destinations.
Selected resources Info
Name
Resource ID
State
Available
Flow log settings
Name - optional
Filter
The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).
Accept
Reject
All
Maximum aggregation interval Info
The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.
10 minutes
1 minute
Destination
The destination to which to publish the flow log data.
Send to CloudWatch Logs
Send to an Amazon S3 bucket
Send to Amazon Data Firehose in the same account
Send to Amazon Data Firehose in a different account

AWS-Flow-LOG

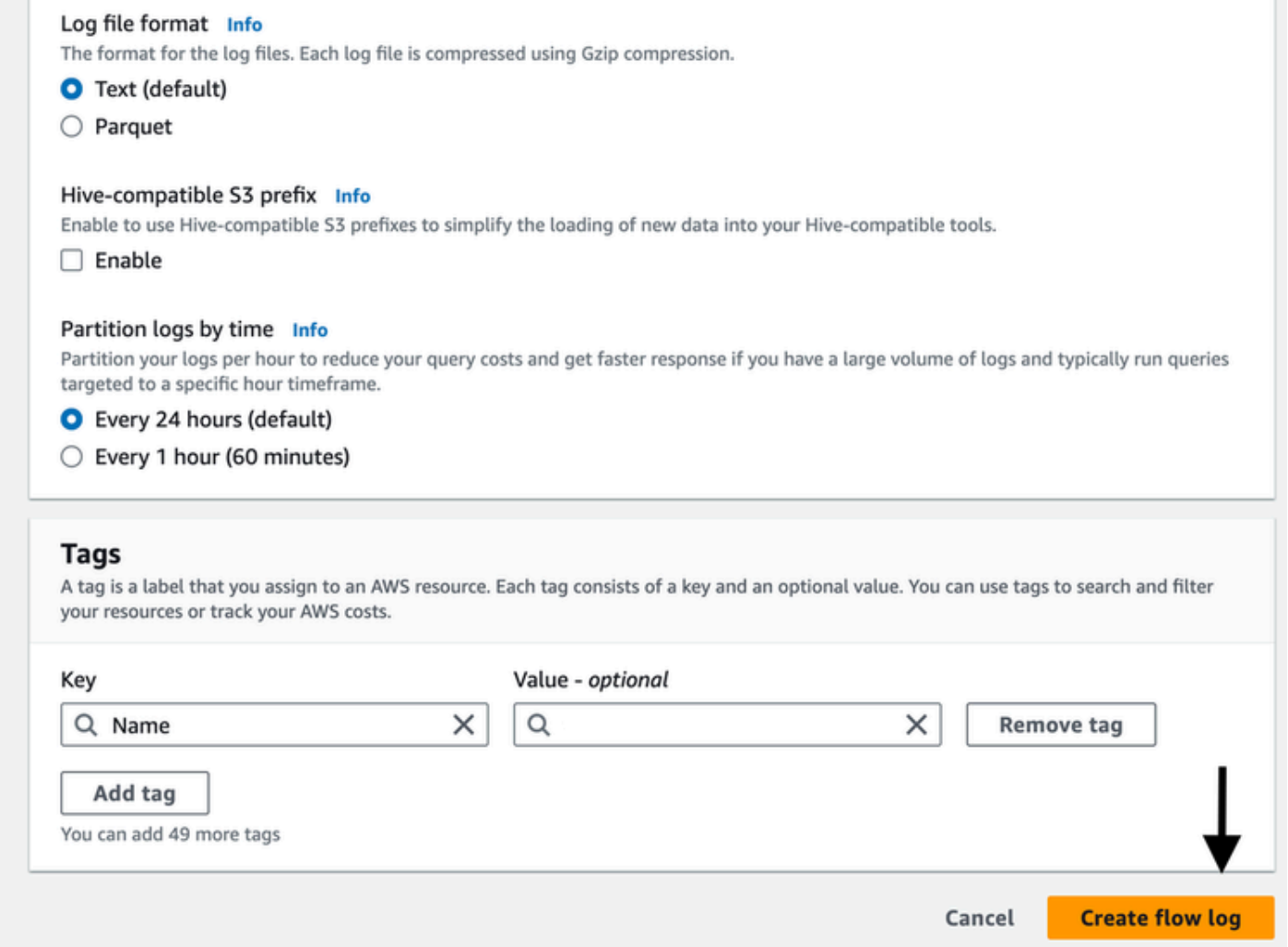



AWS-Flow-LOG

7: انقر فوق إنشاء سجلات التدفق.


aws
Services
Search
[Option+S]
S3 bucket ARN
The ARN of the Amazon S3 bucket to which the flow log is published. You can specify a specific folder in the bucket using the bucket_ARN/folder_name/ format. Create S3 bucket
arn:
Please note, a resource-based policy will be created for you and attached to the target bucket.
Log record format
Specify the fields to include in the flow log record.
AWS default format
Custom format
Log format
Specify the fields to include in the flow log record.
Select an attribute...
account-id
action
az-id
bytes
dstaddr
dstport
end
flow-direction
instance-id
interface-id
log-status
packets
pkt-dst-aws-service
pkt-dstaddr
pkt-src-aws-service
pkt-srcaddr
protocol
region
srcaddr
srcport
start
sublocation-id
sublocation-type
subnet-id
tcp-flags
traffic-path
type
version
vpc-id
Select all
Clear all
Format preview
${account-id} ${action} ${az-id} ${bytes} ${dstaddr} ${dstport} ${end} ${flow-direction} ${instance-id} ${interface-id} ${log-status} ${packets} ${pkt-dst-aws-
Copy

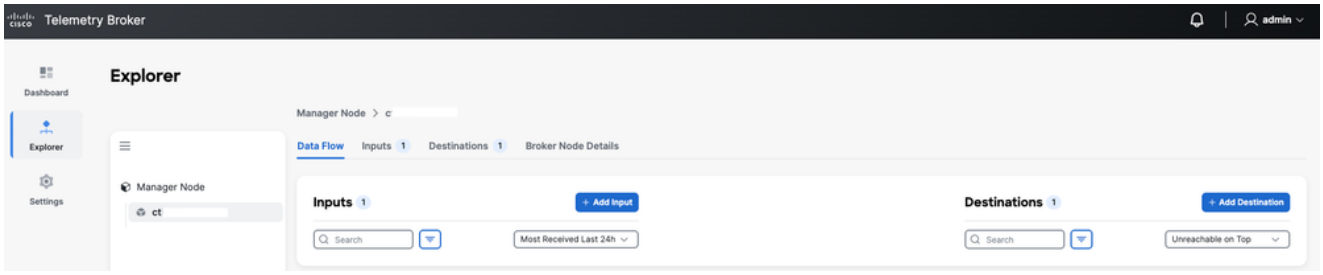
AWS-Flow-LOG




AWS-Flow-LOG

## الخطوة 4. تكوين إدخال VPC إلى CTB

1: Access CTB Web UI، انتقل إلى Explorer> علامة التبويب Broker Node > انقر فوق فتح عقدة الوسيط >Data FlowTab > انقر فوق إضافة إدخال.




CTB-Input-UI

2: حدد نوع الإدخال كسجل تدفق AWS VPC وانقر فوق التالي.

# 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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).