أستكشاف أخطاء دفق الحدث وإصالحها عىل السحابة الخاصة

المحتويات

المقدمة

يصف هذا المستند كيفية أستكشاف أخطاء تدفقات ألأحداث وإصالحها في السحابة الخاصة لنقطة النهاية ألآمنة للحماية المتقدمة من البرامج الضارة.

المتطلبات ألأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من الموضوع:

- السحابة الخاصة بنقطة النهاية الآمنة
- استعلام API

المكونات المستخدمة

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

- Secure Endpoint Private Cloud الإصدار 3.9.0
- cURL v7.87.0
- cURL الإصدار 8.0.1

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.

التكوين

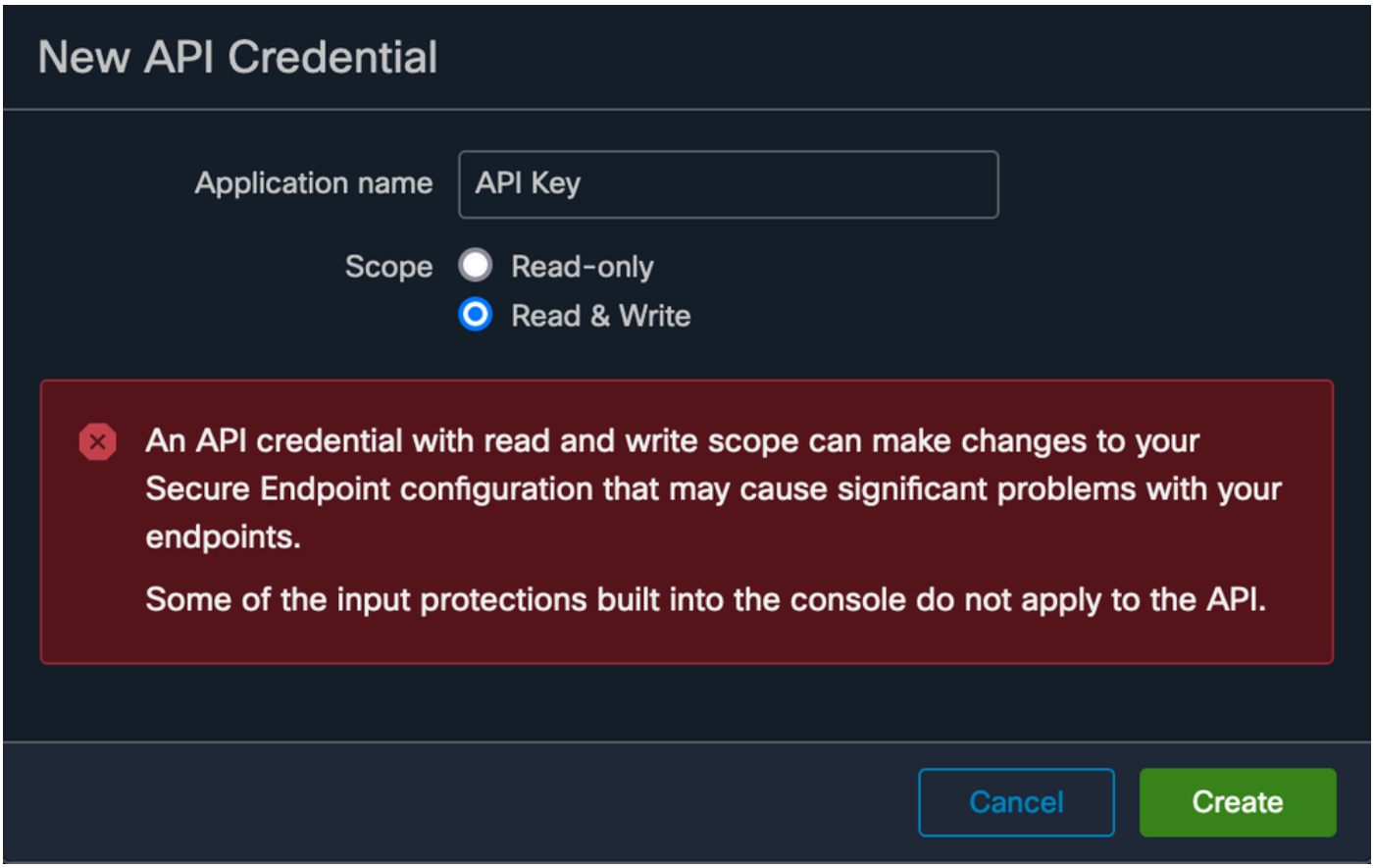
إنشاء مفتاح واجهة برمجة تطبيقات

الخطوة 1. تسجيل الدخول إلى وحدة تحكم السحابة الخاصة.

الخطوة 2. انتقل إلى Accounts > API Credentials.

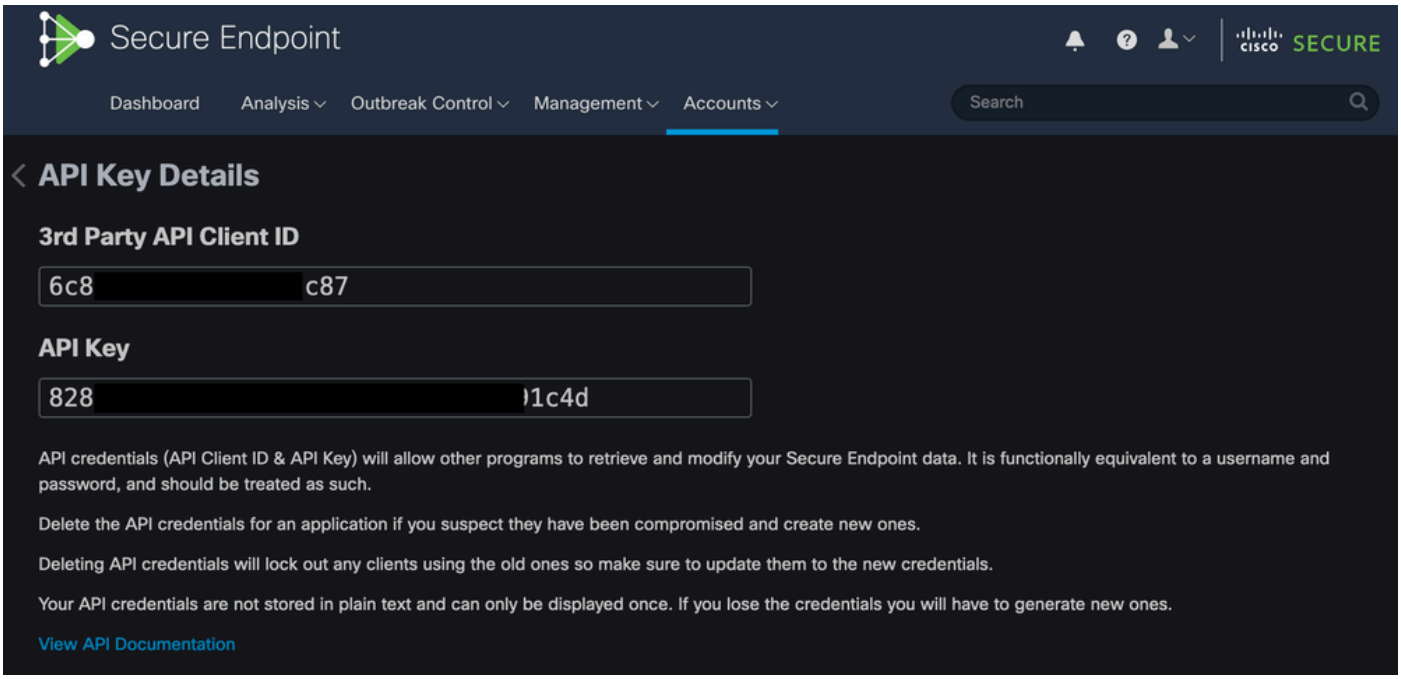
الخطوة 3. انقر New API Credential.

الخطوة 4. إضافة Application name وانقر فوق Read & Write النطاق.



الخطوة 5. انقر Create.

الخطوة 6. حفظ بيانات اعتماد واجهة برمجة التطبيقات.



مفتاح API

تحذير: لا يمكن إسترداد مفتاح API إذا قمت بترك هذه الصفحة.

إنشاء تدفق حدث

يؤدي هذا إلى إنشاء دفق رسائل جديد لبروتوكول خدمة "وضع الرسائل في قائمة انتظار" (AMQP) المتقدم لمعلومات الحدث.

يمكنك إنشاء "دفق حدث" لأنواع الأحداث والمجموعات المحددة:

```
--data '{"name":"EVENT_STREAM_NAME","event_type":["EVENT_TYPE_1", "EVENT_TYPE_2"],"group_guid":["GROUP_
```

يمكنك إنشاء دفق حدث لكافة أنواع الأحداث وكافة المجموعات بواسطة:

```
--data '{"name":"EVENT_STREAM_NAME","event_type":[],"group_guid":[]}'
```

نظام التشغيل MacOS/Linux

يمكنك إنشاء تدفق أحداث على MacOS/Linux باستخدام:

```
curl -X POST -k -H 'Accept: application/json' -H 'Content-Type: application/json' -u 'CLIENT_ID:API_KEY
```

ويندوز

يمكنك إنشاء دفق حدث على Windows باستخدام:

```
curl -X POST -k -H "Accept: application/json" -H "Content-Type: application/json" -u "CLIENT_ID:API_KEY
```

إستجابة

```
HTTP/1.1 201 Created
(...)
"data": {
  "id": 17,
  "name": "EVENT_STREAM_NAME",
  "amqp_credentials": {
    "user_name": "17-1bfXXXXXXXXX",
    "queue_name": "event_stream_17",
    "password": "3961XXXXXXXXXXXXXXXXXXXX814a77",
    "host": "FMC_SERVICE_URL",
    "port": 443,
    "proto": "https"
  }
}
```

قائمة تدفقات الأحداث

يعرض هذا قائمة بتدفقات الأحداث التي تم إنشاؤها على Private Cloud.

نظام التشغيل MacOS/Linux

يمكنك سرد تدفقات الأحداث على نظام التشغيل MacOS/Linux باستخدام:

```
curl -k -H 'Accept: application/json' -H 'Content-Type: application/json' -u 'CLIENT_ID:API_KEY' -i 'ht
```

ويندوز

يمكنك سرد تدفقات الأحداث على Windows باستخدام:

```
curl -k -H "Accept:application/json" -H "Content-Type:application/json" -u "CLIENT_ID:API_KEY" -i "http
```

إستجابة

```
HTTP/1.1 200 OK
(...)
"data": {
  "id": 17,
  "name": "EVENT_STREAM_NAME",
  "amqp_credentials": {
    "user_name": "17-1bfXXXXXXXXX",
    "queue_name": "event_stream_17",
    "host": "FMC_SERVICE_URL",
    "port": 443,
    "proto": "https"
  }
}
```

حذف تدفقات الأحداث

حذف دفق حدث نشط.

نظام التشغيل MacOS/Linux

يمكنك حذف تدفقات الأحداث على MacOS/Linux باستخدام:

```
curl -X DELETE -k -H 'Accept: application/json' -H 'Content-Type: application/json' -u 'CLIENT_ID:API_K
```

ويندوز

يمكنك حذف تدفقات الأحداث على Windows باستخدام:

```
curl -X DELETE -k -H "Accept:application/json" -H "Content-Type:application/json" -u "CLIENT_ID:API_KEY
```

إستجابة

```
HTTP/1.1 200 OK
(...)
 "data": {}
```

التحقق من الصحة

الخطوة 1. انسخ برنامج Python النصي إلى جهازك واحفظه باسم EventStream.py.

```
import pika
import ssl

user_name = "USERNAME"
queue_name = "QUEUE_NAME"
password = "PASSWORD"
host = "FMC_SERVICE_URL"
port = 443
proto = "https"

def callback(channel, method, properties, body):
print(body)

amqp_url = f"amqps://{user_name}:{password}@{host}:{port}"

context = ssl.SSLContext(ssl.PROTOCOL_TLSv1_2)
amqp_ssl = pika.SSLOptions(context)

params = pika.URLParameters(amqp_url)
params.ssl_options = amqp_ssl

connection = pika.BlockingConnection(params)
channel = connection.channel()

channel.basic_consume(
   queue_name,
   callback,
   auto_ack = False
)

channel.start_consuming()
```

الخطوة 2. قم بتنفيذه في المحطة الطرفية على هيئة python3 EventStream.py.

الخطوة 3. قم بتشغيل أي حدث تتم إضافته إلى قائمة انتظار تدفق الأحداث.

الخطوة 4. تحقق مما إذا كانت الأحداث تظهر في المحطة الطرفية.

استكشاف الأخطاء وإصلاحها

لتنفيذ هذه الأوامر، يجب عليك تسجيل الدخول عبر SSH إلى السحابة الخاصة.

فحص خدمة AMQP

تحقق مما إذا تم تمكين الخدمة:

```
[root@fireamp rabbitmq]# amp-ctl service status rabbitmq
running enabled rabbitmq
```

التحقق من تشغيل الخدمة:

```
[root@fireamp ~]# svstat /service/rabbitmq
/service/rabbitmq: up (pid 25504) 7402137 seconds
```

التحقق من الاتصال بمتلقي تدفق الحدث

تنفيذ الأمر:

```
tail /data/log/rabbitmq/rabbit@fireamp.log
```

تم تأسيس الاتصال:

```
=INFO REPORT==== 19-Apr-2023::08:40:12 ===
accepting AMQP connection <0.17588.27> (127.0.0.1:32946 -> 127.0.0.1:5672)
```

تم إغلاق الاتصال:

```
=WARNING REPORT==== 19-Apr-2023::08:41:52 ===
closing AMQP connection <0.17588.27> (127.0.0.1:32946 -> 127.0.0.1:5672):
connection_closed_abruptly
```

التحقق من الأحداث في قائمة الانتظار

تكون الأحداث الموجودة في قائمة الانتظار جاهزة للإرسال على دفق الحدث هذا إلى المستلم بعد تأسيس الاتصال. في هذا المثال، هناك 14 حدثا لمعرف تدفق الحدث 23.

<#root>

```
[root@fireamp rabbitmq]# rabbitmqctl list_queues
Listing queues ...
1acb0eb6-39f7-4b11-bd9b-fc4dd0e3bd77_60b15rn8mpftaico6or6l8zxavl1usm 26
1acb0eb6-39f7-4b11-bd9b-fc4dd0e3bd77_61984nlu8p11eeopmgmtcjra1v8gf5p 26
1acb0eb6-39f7-4b11-bd9b-fc4dd0e3bd77_iesRAgVoOh287mO_DetOx9PdDu8MxkS6kL4oSTeBm9s 26
event_decoration 0
event_log_store 0
```

event_stream_23 14

```
event_streams_api 0
events_delayed 0
events_retry 0
mongo_event_consumer 0
out_events_q1 0
tevent_listener 0
```

تجميع ملف حركة مرور الشبكة

للتحقق من حركة مرور تدفق الأحداث من السحابة الخاصة، يمكنك تجميع الالتقاط باستخدام tcpdump الأداة:

الخطوة 1. SSH إلى السحابة الخاصة.

الخطوة 2. تنفيذ الأمر:

```
tcpdump -vvv -i eth1 host <Event_Stream_Receiver_IP> -w file.pcap
```

الخطوة 3. إيقاف الالتقاط باستخدام Ctrl+C (في Windows) وأ Command-C (MAC).

الخطوة 4. إستخراج pcap ملف من السحابة الخاصة.

معلومات ذات صلة

- [تكوين AMP لميزة تدفق حدث نقاط النهاية]
- [الدعم التقني والمستندات - Cisco Systems]

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).