

對私有雲上的事件流進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[組態](#)

[建立API金鑰](#)

[建立事件流](#)

[MacOS/Linux](#)

[Windows](#)

[響應](#)

[事件流清單](#)

[MacOS/Linux](#)

[Windows](#)

[響應](#)

[刪除事件流](#)

[MacOS/Linux](#)

[Windows](#)

[響應](#)

[驗證](#)

[疑難排解](#)

[檢查AMQP服務](#)

[檢查到事件流接收器的連線](#)

[檢查隊列中的事件](#)

[收集網路流量檔案](#)

[相關資訊](#)

簡介

本文檔介紹如何對高級惡意軟體防護安全終結點私有雲中的事件流進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- [安全端點私有雲](#)
- [API查詢](#)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 安全端點私有雲v3.9.0
- cURL v7.87.0
- cURL v8.0.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

組態

建立API金鑰

步驟1. 登入到私有雲控制檯。

步驟2. 導航至 `Accounts > API Credentials`.

步驟3. 按一下 `New API Credential`.

步驟4. 新增 `Application name` 然後按一下 `Read & Write` 範圍。

New API Credential

Application name

Scope Read-only
 Read & Write

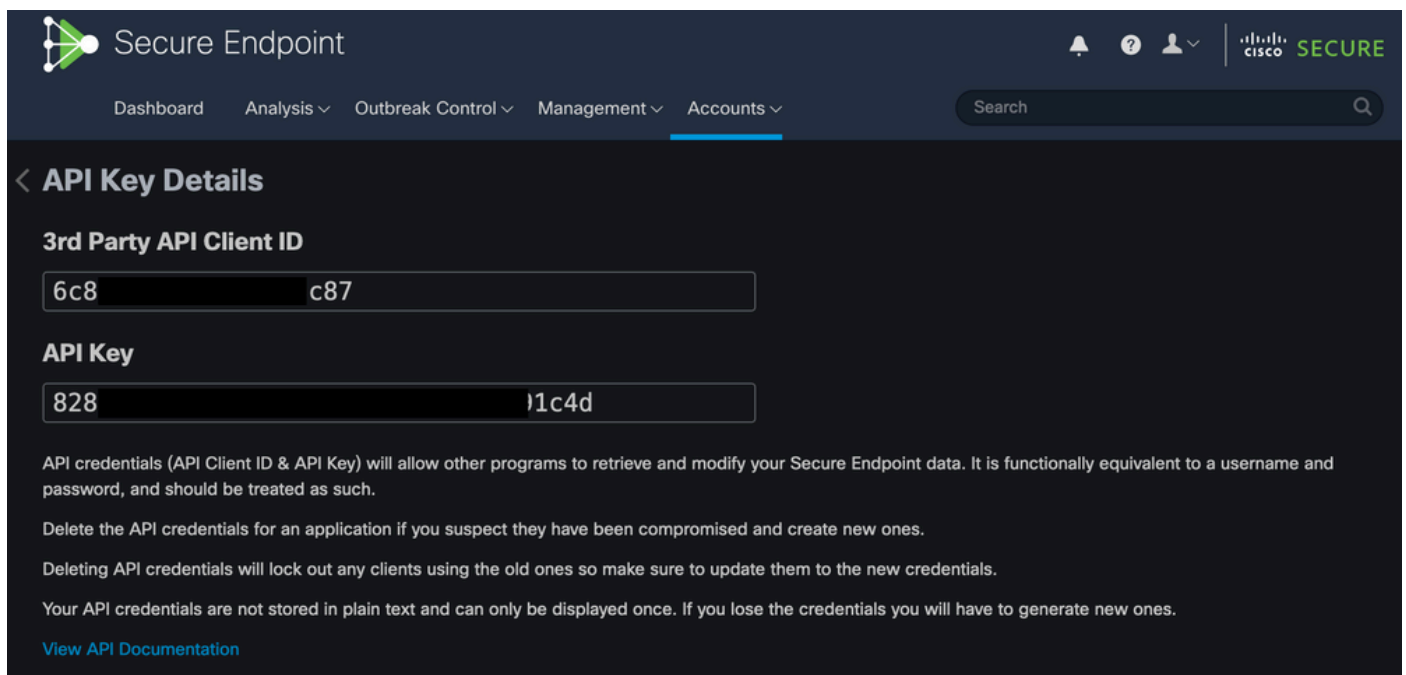
⊗ An API credential with read and write scope can make changes to your Secure Endpoint configuration that may cause significant problems with your endpoints.

Some of the input protections built into the console do not apply to the API.

建立API金鑰

步驟5. 按一下 `Create`.

步驟6.儲存API憑據。



The screenshot shows the Cisco Secure Endpoint web interface. The top navigation bar includes 'Dashboard', 'Analysis', 'Outbreak Control', 'Management', and 'Accounts'. A search bar is located on the right. The main content area is titled '< API Key Details'. It features two input fields: '3rd Party API Client ID' with the value '6c8c87' and 'API Key' with the value '8281c4d'. Below the fields, there is explanatory text: 'API credentials (API Client ID & API Key) will allow other programs to retrieve and modify your Secure Endpoint data. It is functionally equivalent to a username and password, and should be treated as such.' It also includes instructions on deleting credentials and a link to 'View API Documentation'.

API金鑰

注意：如果您離開此頁面，則無法恢復API金鑰。

建立事件流

這將為事件資訊建立新的高級消息隊列協定(AMQP)消息流。

可以為指定的事件型別和組建立事件流：

```
--data '{"name":"EVENT_STREAM_NAME","event_type":["EVENT_TYPE_1", "EVENT_TYPE_2"],"group_guid":["GROUP_1", "GROUP_2"]}'
```

您可以通過以下方式為所有事件型別和所有組建立事件流：

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

MacOS/Linux

您可以使用以下功能在MacOS/Linux上建立事件流：

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

Windows

您可以使用以下功能在Windows上建立事件流：

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

響應

```
HTTP/1.1 201 Created
```

```
(...)
```

```
"data": {  
  "id": 17,  
  "name": "EVENT_STREAM_NAME",  
  "amqp_credentials": {  
    "user_name": "17-1bfXXXXXXXXXX",  
    "queue_name": "event_stream_17",  
    "password": "3961XXXXXXXXXXXXXXXXXXXX814a77",  
    "host": "FMC_SERVICE_URL",  
    "port": 443,  
    "proto": "https"  
  }  
}
```

事件流清單

這顯示在私有雲上建立的事件流的清單。

MacOS/Linux

您可以使用以下內容列出MacOS/Linux上的事件流：

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

Windows

您可以使用以下內容列出Windows上的事件流：

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

響應

HTTP/1.1 200 OK

(...)

```
"data": {  
  "id": 17,  
  "name": "EVENT_STREAM_NAME",  
  "amqp_credentials": {  
    "user_name": "17-1bfXXXXXXXXXX",  
    "queue_name": "event_stream_17",  
    "host": "FMC_SERVICE_URL",  
    "port": 443,  
    "proto": "https"  
  }  
}
```

刪除事件流

刪除活動事件流。

MacOS/Linux

您可以使用以下內容刪除MacOS/Linux上的事件流：

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

Windows

您可以使用以下方法刪除Windows上的事件流：

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

響應

HTTP/1.1 200 OK

(...)

```
"data": {}
```

驗證

步驟1.將Python指令碼複製到裝置並將其另存為 `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()
```

步驟2.在終端中執行它作為 `python3 EventStream.py`.

步驟3.觸發新增到事件流隊列中的任何事件。

步驟4.檢查終端中是否顯示事件。

疑難排解

為了執行這些命令，您必須通過SSH登入到私有雲。

檢查AMQP服務

驗證服務是否已啟用：

```
[root@fireamp rabbitmq]# ampctl service status rabbitmq
running enabled rabbitmq
```

驗證服務是否正在運行：

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

檢查到事件流接收器的連線

執行命令：

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

已建立連線：

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

連線已關閉：

```
=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
```

檢查隊列中的事件

隊列中的事件已準備就緒，可以在建立連線後通過此事件流傳送到接收器。在此示例中，事件流ID 23有14個事件。

<#root>

```
[root@fireamp rabbitmq]# rabbitmqctl list_queues
Listing queues ...
1acb0eb6-39f7-4b11-bd9b-fc4dd0e3bd77_60b15rn8mpftai6or6l8zxav11usm 26
1acb0eb6-39f7-4b11-bd9b-fc4dd0e3bd77_61984nlu8p11eeopmgmtcjra1v8gf5p 26
1acb0eb6-39f7-4b11-bd9b-fc4dd0e3bd77_iesRAGVo0h287m0_Det0x9PdDu8MxkS6kL4oSTeBm9s 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
```

收集網路流量檔案

為了驗證來自私有雲的事件流流量，可以使用 `tcpdump` 工具：

步驟1.通過SSH連線到私有雲。

步驟2.執行命令：

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

步驟3.停止捕獲 `Ctrl+C` (Windows)或 `Command-C` (Mac)。

步驟4.提取 `pcap` 私有雲中的檔案。

相關資訊

- [配置面向終端的AMP事件流功能](#)
- [技術支援與文件 - Cisco Systems](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。