排除外部威脅源故障的最主要原因

目錄

簡介

本文檔介紹外部威脅源實施過程中失敗的幾個原因、錯誤分析和解決操作。

必要條件

沒有特定要求，因此思科建議您瞭解以下主題：

- 思科安全電子郵件閘道(ESA)
- 外部威脅來源(ETF)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體12.x或更高版本的思科安全電子郵件網關(ESA)

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。

失敗原因：

ETF服務已禁用或沒有有效的服務功能金鑰

<#root>

```
(Machine esa03.taclab.krk) (SERVICE)> tail threatfeeds

Press Ctrl-C to stop.
Wed Sep 8 16:15:26 2021 Info: THREAT_FEEDS: A delta poll is scheduled for the source: Test_Poll_Path
Machine: ‘esa03.taclab.krk'. A failure was encountered for the source 'Test_Poll_Path'.

Reason for failure: The ETF service is either disabled or there is no valid feature key for the service.
```

解決方案

確保：

1. ETF功能金鑰已正確安裝。
2. 已接受EULA並全域性啟用功能金鑰。
3. 已在電腦級別應用許可證。

註：如果存在群集級別，則需要將設定複製到電腦級別。

無法建立新連線： [錯誤110]連線超時

```
(Machine esa03.taclab.krk) (SERVICE)> tail threatfeeds

Press Ctrl-C to stop.
Reason for failure: Taxii Error: HTTPSConnectionPool(host= otx.alienvault.comport, port=443): Max retri
Failed to establish a new connection: [Errno 110] Connection timed out',))
```

注意：連線超時通常表示與網路相關的問題，這會阻止ESA獲取響應。建議使用防火牆/代理檢查以及資料包捕獲，以便進行更深入的分析。

解決方案

1. 確認防火牆和代理不阻止流量。
   可以在GUI > Security Services > Service Updates下檢查代理。
2. 確認與資料包捕獲的連線。導覽至GUI > Help and Support > Packet Capture。

提示：當出現網路相關問題的跡象時，謹慎的做法是運行資料包捕獲，以確認已正確建立連線。

失敗原因：「400」

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 6 13:38" threatfeeds
Mon Sep 6 13:38:16 2021 Debug: THREAT_FEEDS: Failed to fetch observables from the source: Test_Poll_Pat
Mon Sep 6 13:38:55 2021 Info: THREAT_FEEDS: The source 'Test_Poll_Path' is currently in a polling state
```

註:RFC7231錯誤400（錯誤請求），表示伺服器由於某種被視為客戶端錯誤而無法或不處理請求。 大多數情況下，出現此錯誤的原因在於請求語法格式不正確或請求消息幀無效。

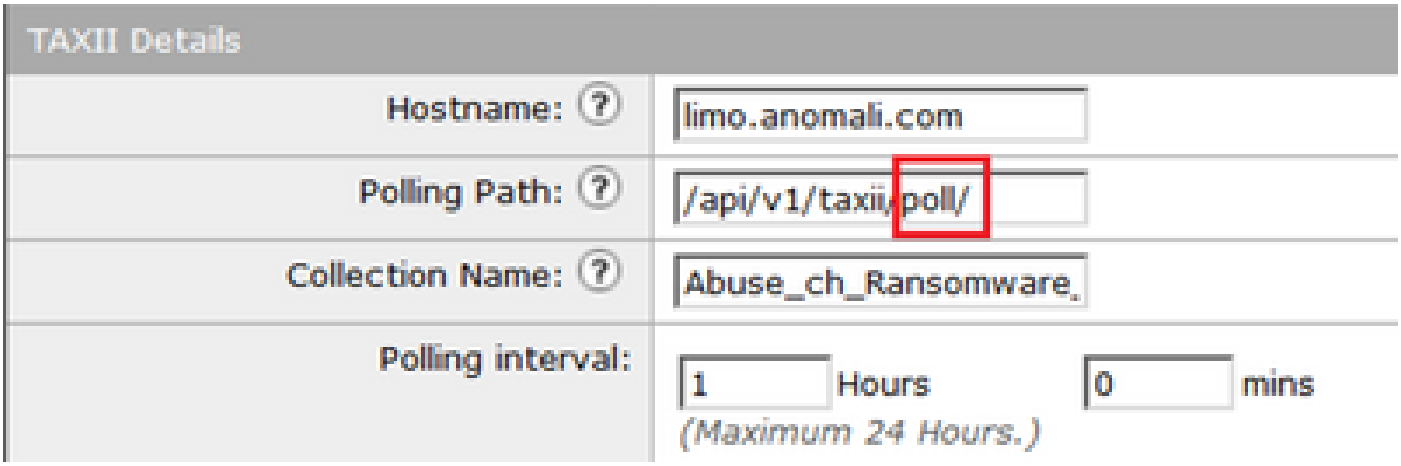
解決方案

錯誤「400」表示存在此輪詢路徑，但它指向TAXII伺服器提供的其他服務。

1. 確認輪詢路徑配置配置了輪詢請求而不是發現請求。
2. 在GUI > Mail Policies > External Threat Feeds Manager > Use HTTPS下，確認HTTPS已啟用。

注意：通常，當輪詢路徑配置有發現請求時（如：/api/v1/taxii/taxii-discovery-service/）會發生此問題
輪詢路徑可以配置為對源使用輪詢請求，例如：/api/v1/taxii/poll

注意：輪詢和發現請求之間的差異：
- 輪詢URL實際上就是您從中使用源的位置。
- Discovery Service URL用於查詢Taxii服務提供的服務。



HTTP錯誤：狀態代碼401身份驗證失敗

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 8 16:35" threatfeeds
Wed Sep 8 16:35:39 2021 Debug: THREAT_FEEDS: Updating the timestamp: 2021-09-08 16:31:36.071684 for the
Wed Sep 8 16:35:39 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name. Reason
```

解決方案

此錯誤代碼表明它缺少目標資源的有效身份驗證憑據。

確認憑據配置正確。
還可以選擇不為使用者配置憑據。

Taxii錯誤： HTTP錯誤：狀態代碼404請求的資源不可用

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 27 08:51" threatfeeds
Fri Aug 27 08:51:16 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: Test a
Fri Aug 27 08:51:16 2021 Info: THREAT_FEEDS: Job failed with exception : Source: Test. Reason for failu
```

註:404（未找到）狀態代碼表示源伺服器未找到目標資源的當前表示形式，或者不願意透露該表示形式存在。這顯示可能存在無效的URL，在大多數情況下，找不到由於資源路徑而發生的錯誤。

解決方案

在ESA GUI> Mail Policies > External Threat Feeds Manager > Choose the proper Source Name(在ESA GUI>郵件策略>外部威脅源管理器>選擇正確的源名稱)下確認源上的輪詢路徑/收集名稱。

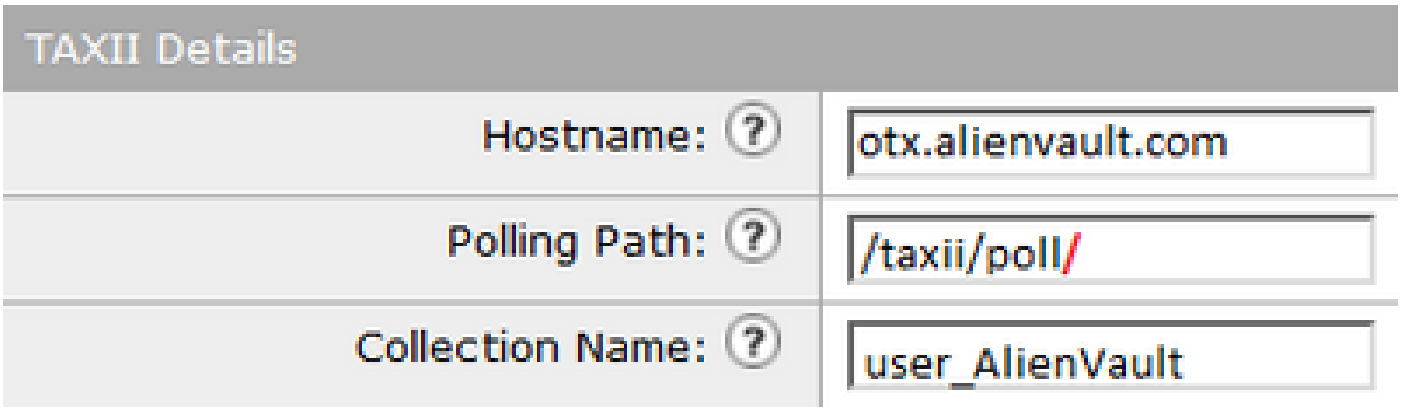
失敗原因：「405」

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 13 00:2" threatfeeds
Mon Sep 13 00:20:21 2021 Debug: THREAT_FEEDS: Failed to fetch observables from the source: Anomali. Rea
```

注意：根據RFC7231，錯誤405(Method Not Allowed)表示在請求行中接收的方法是源伺服器已知的，但目標資源不支援該方法。

解決方案

由於輪詢路徑末尾缺少跟蹤「/」斜線，因此存在語法錯誤。
在路徑/taxii/poll/的末尾新增軌跡斜線。



HTTP錯誤：狀態代碼503服務不可用

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Nov 10 13:45" threatfeeds
Sun Nov 10 13:45:21 2020 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name. Reaso
Sun Nov 10 13:45:22 2020 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
```

注意：根據RFC7231，錯誤503「服務不可用」是HTTP響應狀態代碼，表示伺服器暫時無法處理請求。

解決方案

錯誤代碼表明目標TAXII伺服器出現問題，需要進一步調查。
當伺服器超載時，可能會發生這種情況。聯絡供應商以瞭解更多資訊。

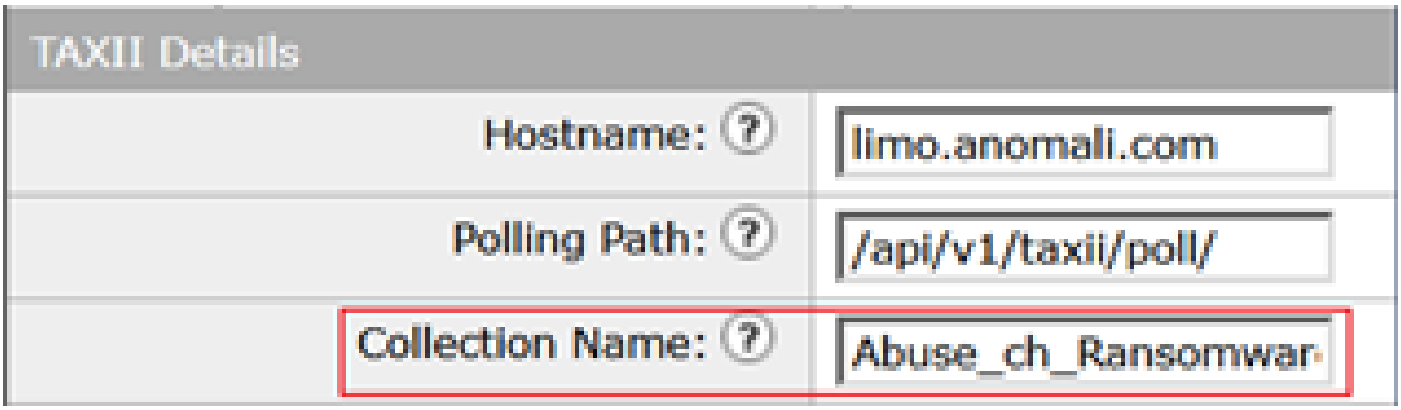
NOT_FOUND：找不到請求的集合

```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 7 12:53" threatfeeds
Tue Sep 7 12:53:16 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: Test_Po
Tue Sep 7 12:53:16 2021 Debug: THREAT_FEEDS: Updating the timestamp: 2021-09-07 12:49:12.648625 for the
```

解決方案

此錯誤表示集合名稱拼寫正確，但是，集合下的TAXII伺服器出現問題，該伺服器拒絕請求。

可能的原因可能是集合名稱上的過期計時器。
聯絡供應商檢查此類不一致。



[SSL: CERTIFICATE_VERIFY_FAILED]證書驗證失敗(_ssl.c:590)

<#root>

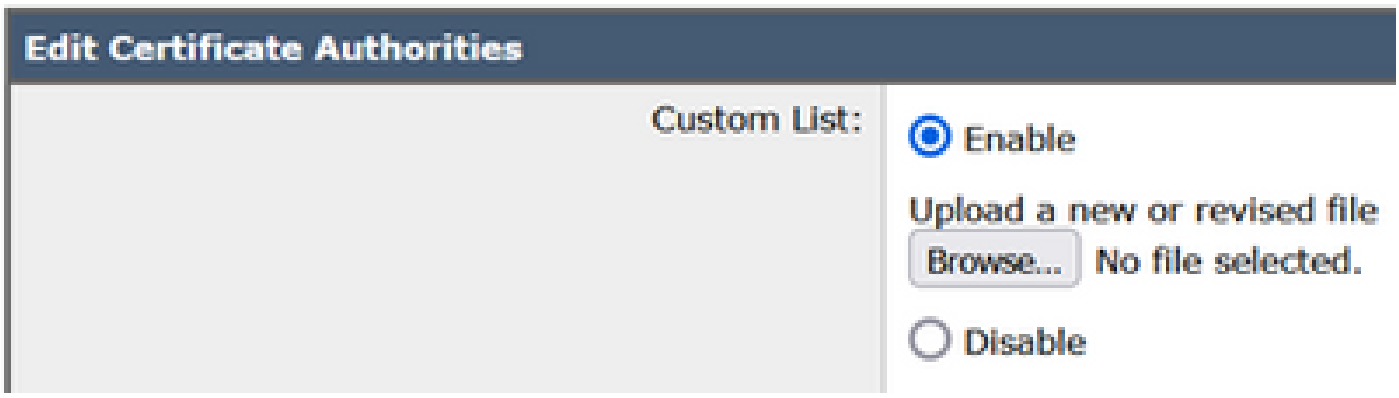
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Sep 8 16:35" threatfeeds
Wed Sep 8 16:35:26 2021 Info: THREAT_FEEDS: A delta poll is scheduled for the source: ETF_Source_Name
Wed Sep 8 16:35:33 2019 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_Sou
```

Reason for failure: Taxii Error: [SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed (_ssl.c:590)

解決方案

此錯誤表示憑證失敗。

若要解決此問題，請匯入證書頒發機構(CA)中的證書。
導覽至GUI > Network > Certificates > Edit Settings > Custom List >
選擇Enable模式並上傳憑證。



XML解析錯誤：找不到元素（第0行）

<#root>

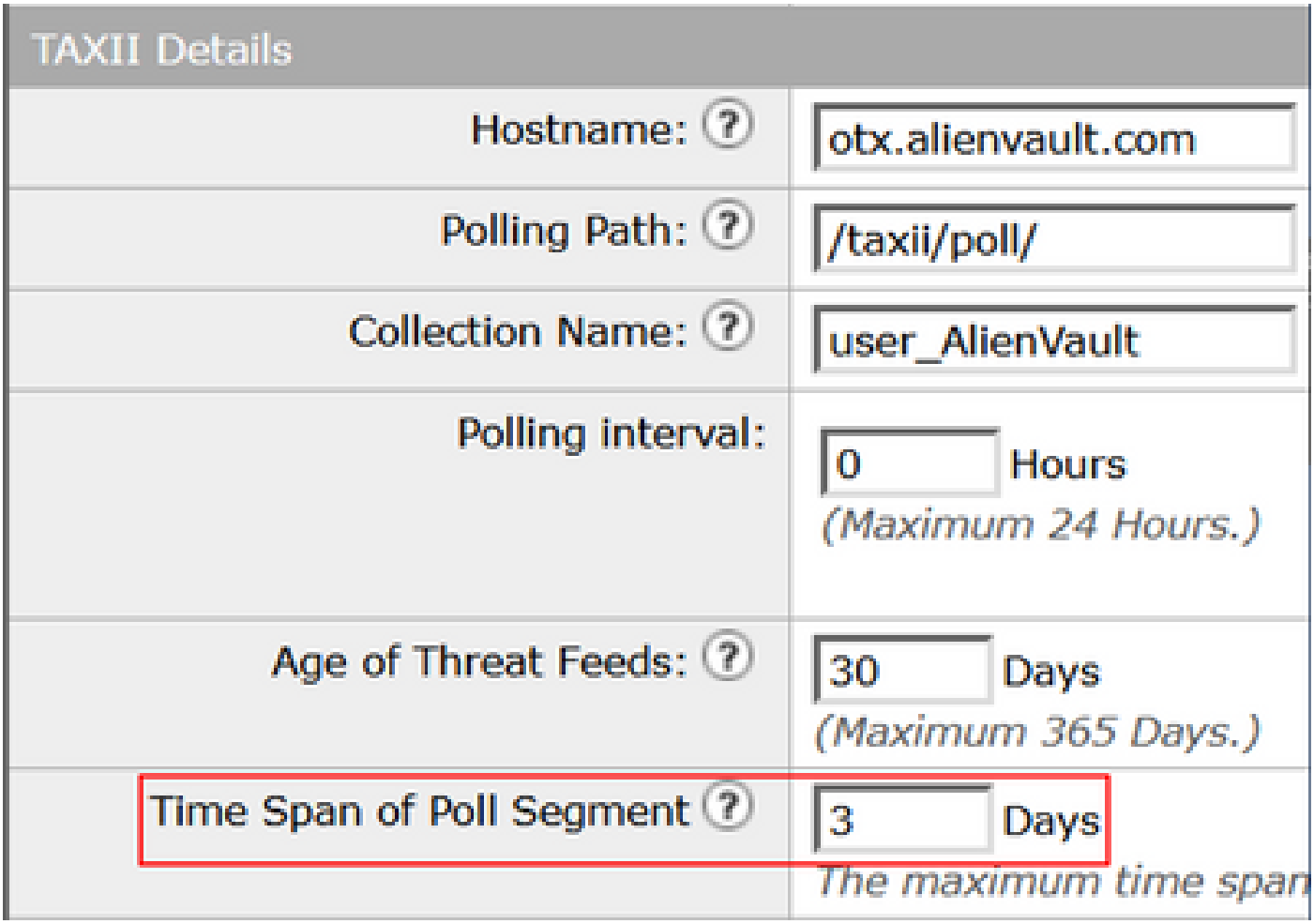
```
(Machine esa03.taclab.krk) (SERVICE)> grep "Aug 21 02:39" threatfeeds
Fri Aug 21 02:39:37 2021 Warning: THREAT_FEEDS: Unable to fetch the observables from the source: ETF_So
Fri Aug 21 02:39:37 2021 Info: THREAT_FEEDS: Job failed with exception : Source: ETF_Source_Name.
```

```
Reason for failure: Taxii Error: XML Parising Error: no element found (line 0)
```

解決方案

將輪詢段的Time Span值從ESA配置縮短到3-4天。

> 注意：對於某些特定源（其中未傳送結束資料標誌以停止源），這與Anomali伺服器不一致。
> 在這種情況下，配置了Anomali的ETF源的ESA無法輪詢超過5天時間跨度的資料。
> 有效的解決方法是從ESA配置中減小輪詢段的時間跨度值。



無法建立新連線： [錯誤11]連線被拒絕

<#root>

```
(Machine esa03.taclab.krk) (SERVICE)> tail threatfeeds

Press Ctrl-C to stop.
Reason for failure: Taxii Error: HTTPSConnectionPool(host=otx.alienvault.comport=443): Max retries exce
```

```
Failed to establish a new connection: [Errno 111] Connection refused',))
```

注意：「連線被拒絕」表示客戶端無法連線到正在運行的伺服器上的埠。通常情況下，當伺服器在錯誤的埠上偵聽或埠不可用時，會發生這種情況。

解決方案

1. 通過CLI使用telnet或netstat命令驗證適當的埠是否正在監聽。
2. 確認Firewall沒有阻止該埠。
3. 確保運行的服務上不存在埠配置錯誤/埠陳舊。

相關資訊

- 思科電子郵件安全裝置最終使用手冊
- 什麼是STIX和TAXII
- RFC2741 — 錯誤代碼
- TAC研討會外部威脅源

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）。