排除FMC與CTR的整合故障

目錄

簡介

本文說明當安全服務交換(SSE)聯結器進程在Firepower管理中心(FMC)或Firepower威脅防禦(FTD)裝置上被禁用以便與思科威脅響應(CTR)整合時，對其進行故障排除的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- FMC
- FTD
- CTR整合

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 6.4.0或更高版本軟體上的FMC
- 6.4.0或更高版本軟體上的FTD
- 思科安全服務交換
- CTR帳戶

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。

背景資訊

SSEConnector

SSEConnector是6.4.0之後的Firepower裝置上的一個進程，它將裝置註冊到SSE門戶。當思科雲配置設定為「開啟」或「關閉」時，FMC會廣播到所有受管FTD。啟用思科雲後，SSEConnector服務將啟動SSE門戶與Firepower裝置之間的通訊。每個FTD向FMC請求註冊令牌，以讓裝置整合到SSE入口中。在此整合之後，將在裝置上啟用SSE上下文，並重新配置EventHandler以將入侵事件傳送到Cisco Cloud。

CTR

威脅響應是一個威脅事件響應協調中心，它支援多個思科安全產品之間的整合並實現自動化。威脅響應加快了關鍵安全任務：檢測、調查和補救，並且是我們整合安全架構中的一個關鍵元素。

威脅響應的目標是幫助網路運營團隊和事件響應人員通過思科和第三方收集並組合提供的所有威脅情報瞭解其網路上的威脅。

但是，威脅響應的用途絕不僅僅是降低安全工具的複雜性、幫助識別威脅和加快事件響應速度。

威脅響應是一個整合平台(https://visibility.amp.cisco.com/)。 系統通過「模組」工作，模組是獨立的代碼片段，處理不同整合系統（如Threat Grid或AMP）的通訊。 這些模組處理整合系統所能提供的全部3項功能（豐富、本地環境和響應）。

CTR可用於什麼？

- 事件響應
- 調查
- 威脅搜尋
- 事件管理

當您搜尋可觀察對象時，所有已配置的模組都會要求它們負責搜尋這些可觀察對象的任何記錄的系統。然後，他們將提供的響應傳遞回Threat Response，然後提取所有模組（本例中為Stealthwatch模組）的收集結果，並對資料進行分類和組織並將其顯示在圖形中。

要將CTR與不同的產品整合，還需要兩個門戶「https://castle.amp.cisco.com/」(Castle)和「https://admin.sse.itd.cisco.com/app/devices」（安全服務交換）

城堡門戶

您可以在此處管理思科安全帳戶：

思科安全帳戶允許您管理思科安全產品組合中的多個應用。根據您的許可權利，這可以包括：

- AMP端點版
- Threat Grid
- 威脅響應

安全服務交換門戶

此門戶是CTR門戶的擴展，您可以在其中管理已在CTR門戶中註冊的裝置，以便在此處建立整合產品所需的令牌。

在將某些思科安全產品與思科威脅響應整合時，安全服務Exchange可提供裝置、服務和事件管理，包括以下產品和功能：

- 管理與思科威脅響應整合的安全管理裝置清單。
- 從整合的Cisco Firepower裝置收集事件資料，準備將其轉發（自動或手動）到思科威脅響應。

疑難排解

驗證是否已啟用雲服務

在FMC上，首先在**System > Licenses > Smart Licenses** 上驗證您未處於評估模式。

現在，在**Smart Software Satellite**索引標籤上的**System > Integration**下，驗證選擇的選項是否為**Connect directly to Cisco Smart Software Manager**，因為氣隙環境中不支援此功能。

導覽至**Cloud Services** 索引標籤上的**System > Integration**，並檢查**Cisco Cloud Event Configuration**選項是否已啟用。

驗證FMC/FTD和SSE門戶之間的連線

由於IP可以更改，需要允許這些下一個URL:

美國地區

- api-sse.cisco.com
- est.sco.cisco.com（在各地域中通用）
- mx*.sse.itd.cisco.com(目前僅適用於mx01.sse.itd.cisco.com)
- dex.sse.itd.cisco.com（客戶成功）
- eventing-ingest.sse.itd.cisco.com（用於CTR和CDO）

歐盟地區

- api.eu.sse.itd.cisco.com
- est.sco.cisco.com（在各地域中通用）
- mx*.eu.sse.itd.cisco.com(目前僅適用於mx01.eu.sse.itd.cisco.com)
- dex.eu.sse.itd.cisco.com（客戶成功）
- eventing-ingest.eu.sse.itd.cisco.com（適用於CTR和CDO）

亞太及日本地區

- api.apj.sse.itd.cisco.com
- est.sco.cisco.com（在不同地區通用）
- mx*.apj.sse.itd.cisco.com(目前僅適用於mx01.apj.sse.itd.cisco.com)
- dex.apj.sse.itd.cisco.com（客戶成功）

- eventing-ingest.apj.sse.itd.cisco.com（適用於CTR和CDO）

FMC和FTD都需要連線到其管理介面上的SSE URL，要測試連線，請在具有根訪問許可權的Firepower CLI上輸入以下命令：

```
curl -v https://api-sse.cisco.com/providers/sse/services/registration/api/v2/clients --cacert
/ngfw/etc/ssl/connectorCA.pem
curl -v https://est.sco.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem

curl -v https://eventing-ingest.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
curl -v https://mx01.sse.itd.cisco.com --cacert /ngfw/etc/ssl/connectorCA.pem
```

執行完每個指令後，您必須在連線結尾看到以下行：**Connection #0 to host "URL"保留原樣。**

如果連線超時或您在輸出中沒有收到此行，請驗證是否允許管理介面訪問這些URL，以及是否沒有任何上游裝置阻止或修改裝置與這些URL之間的連線。

可以使用以下命令繞過證書檢查：

```
root@ftd01:~# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying 52.4.85.66...
* Connected to api-sse.cisco.com (52.4.85.66) port 443 (#0)
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
* CAfile: none
CApath: /etc/ssl/certs
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Request CERT (13):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Certificate (11):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Client hello (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
* subject: C=US; ST=California; L=San Jose; O=Cisco Systems, Inc.; CN=api -sse.cisco.com
* start date: 2019-12-03 20:57:56 GMT
* expire date: 2021-12-03 21:07:00 GMT
* issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID S SL ICA G2
* SSL certificate verify result: self signed certificate in certificate c hain (19), continuing
anyway.
>GET / HTTP/1.1
>Host: api-sse.cisco.com
>User-Agent: curl/7.44.0
>Accept: */*
>
<HTTP/1.1 403 Forbidden
<Date: Wed, 08 Apr 2020 01:27:55 GMT
<Content-Type: text/plain; charset=utf-8
<Content-Length: 9
```

```
<Connection: keep-alive
<Keep-Alive: timeout=5
<ETag: "5e17b3f8-9"
<Cache-Control: no-store
<Pragma: no-cache
<Content-Security-Policy: default-src 'self'
<X-Content-Type-Options: nosniff
<X-XSS-Protection: 1; mode=block
<Strict-Transport-Security: max-age=31536000; includeSubdomains;
```

> **附註**：您會收到403 Forbidden報文，因為從測試傳送的引數不是SSE期望的，但這一點足以驗證連通性。

驗證SSEConnector狀態

您可以按如下所示驗證聯結器屬性。

```
# more /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
connector_fqdn=api-sse.cisco.com
```

為了檢查SSConnector和EventHandler之間的連線，可以使用此命令，以下是連線錯誤的示例：

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 3022791165 11204/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.sock
```

在已建立的連線的範例中，可以看到串流狀態為已連線：

```
root@firepower:/etc/sf# netstat -anlp | grep EventHandler_SSEConnector.sock
unix 2 [ ACC ] STREAM LISTENING 382276 7741/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.sock
unix 3 [ ] STREAM CONNECTED 378537 7741/EventHandler
/ngfw/var/sf/run/EventHandler_SSEConnector.soc
```

驗證傳送到SSE門戶和CTR的資料

若要從FTD裝置傳送事件以瞭解TCP連線需要使用https://eventing-ingest.sse.itd.cisco.com建立，以下是SSE入口和FTD之間未建立連線的範例：

```
root@firepower:/ngfw/var/log/connector# lsof -i | grep conn
connector 60815 www 10u IPv4 3022789647 0t0 TCP localhost:8989 (LISTEN)
connector 60815 www 12u IPv4 110237499 0t0 TCP firepower.cisco.com:53426->ec2-100-25-93-
234.compute-1.amazonaws.com:https (SYN_SENT)
```

在connector.log日誌中：

```
time="2020-04-13T14:34:02.88472046-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 18.205.49.246:443: getsockopt: connection timed out"
time="2020-04-13T14:38:18.244707779-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
time="2020-04-13T14:42:42.564695622-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 18.205.49.246:443: getsockopt: connection timed out"
time="2020-04-13T14:47:48.484762429-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
```

```
time="2020-04-13T14:52:38.404700083-05:00" level=error msg="[firepower.cisco.com][events.go:90
events:connectWebSocket] dial tcp 100.25.93.234:443: getsockopt: connection timed out"
```

> **附註**：請注意，所顯示的18.205.49.246和18.205.49.246屬於https://eventing-ingest.sse.itd.cisco.com的IP地址可能會更改，因此建議允許基於URL而非IP地址的SSE門戶流量。

如果沒有建立此連線，則事件不會傳送到SSE門戶，以下是FTD和SSE門戶之間已建立連線的示例：

```
root@firepower:# lsof -i | grep conn
connector 13277   www   10u  IPv4 26077573      0t0  TCP localhost:8989 (LISTEN)
connector 13277   www   19u  IPv4 26077679      0t0  TCP 192.168.1.200:56495->ec2-35-172-147-
246.compute-1.amazonaws.com:https (ESTABLISHED)
```

常見問題

升級到6.4後，SSE聯結器不與SSE門戶通訊。Connector.log提供類似於以下事件的錯誤：(*Service)。Start]無法連線到ZeroMQ PUSH終結點：無法撥打\"ipc:///ngfw/var/sf/run/EventHandler_SSEConnector.sock\":撥打unix /ngfw/var/sf/run/EventHandler_SSEConnector.sock:connect:沒有這樣的檔案或目錄\n"

重新啟動SSEConnector服務：

1)sudo pmtool disableby SSEConnector

2)sudo pmtool enablebyid SSEConnector

3)重新啟動裝置。重啟後，裝置與雲通訊。

重要日誌檔案位置

調試日誌 — 顯示成功連線或失敗消息

```
/ngfw/var/log/connector/connector.log
```

配置設定

```
/ngfw/etc/sf/connector.properties
```

配置設定

```
curl localhost:8989/v1/contexts/default
```

相關資訊

- https://docs.castle.amp.cisco.com/CiscoSecurityAccountUserGuide.pdf
- 技術支援與文件 - Cisco Systems