對Firepower裝置上的雲配置故障進行故障排除"

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[網路圖表](#)
[問題](#)
[疑難排解](#)
[選項1.DNS配置不存在](#)
[選項2.客戶DNS無法解析https://api-sse.cisco.com](#)
[更多疑難排解選項](#)
[已知的問題](#)
[[影片] Firepower — 將FMC註冊到SSE](#)

簡介

本文檔介紹Firepower系統觸發運行狀況警報「威脅資料更新 — 思科雲配置 — 故障」的常見場景。

必要條件

需求

思科建議您瞭解以下主題：

- Firepower系統
- 雲整合
- DNS解析和代理連線
- 思科威脅回應(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：

- Firepower管理中心(FMC)版本6.4.0或更高版本
- Firepower威脅防禦(FTD)或Firepower感測器模組(SFR)版本6.4.0或更高版本
- 思科安全服務交換(SSE)
- 思科智慧帳戶入口網站

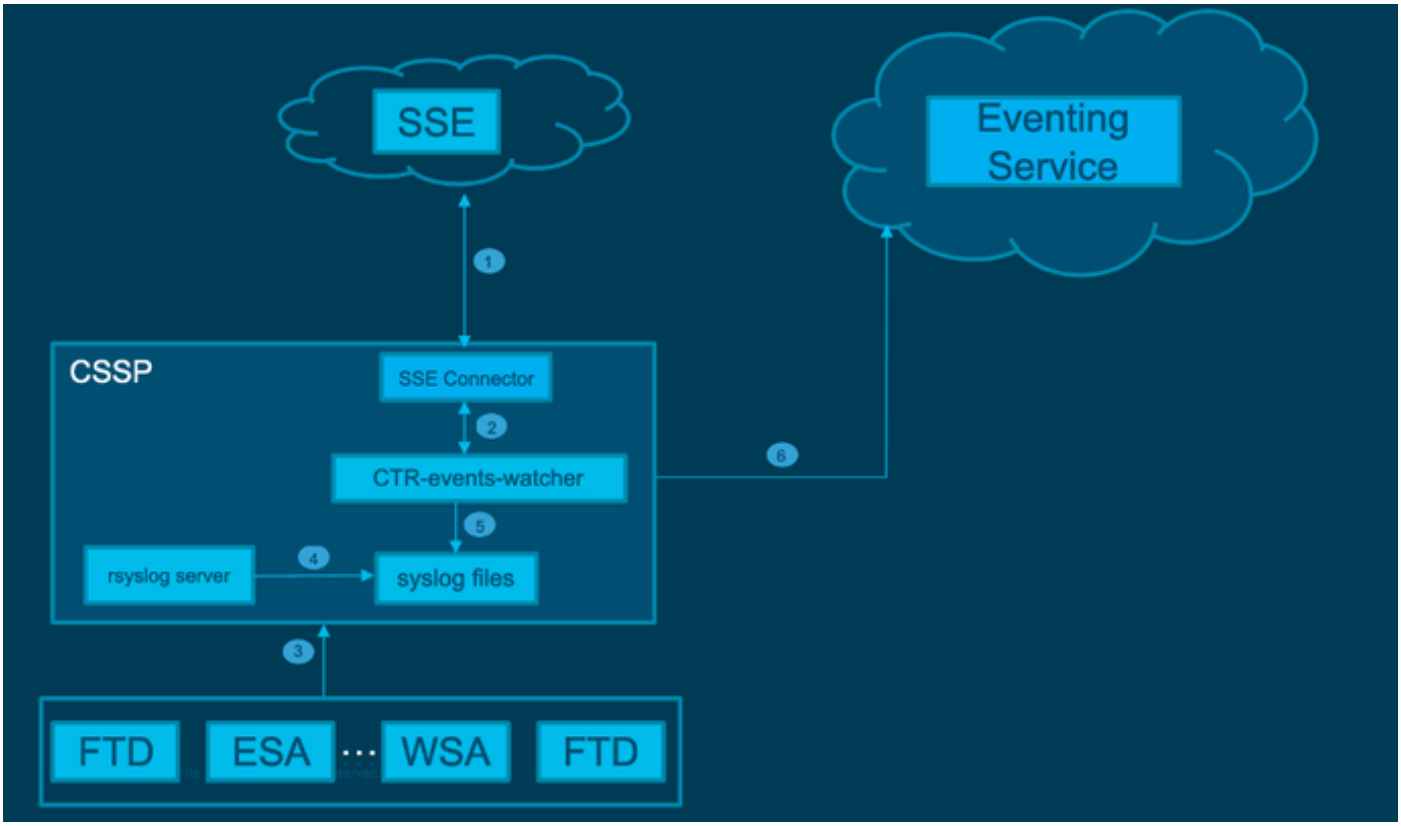
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

觀察到雲配置錯誤是因為FTD無法與api-sse.cisco.com通訊。Firepower裝置需要訪問該網站以與SecureX和雲服務整合。

此警報是快速威脅遏制(RTC)功能的一部分，在新的Firepower版本中預設啟用，其中FTD需要能夠在Internet上與api-sse.cisco.com通訊。如果此通訊無法使用，FTD的健康監控模組會顯示此錯誤訊息。

網路圖表



問題

增強功能思科錯誤ID CSCvr46845描述了Firepower系統何時觸發運行狀況警報「思科雲配置 — 故障」，大多數情況下，問題與FTD和api-sse.cisco.com之間的連線相關。但是，此警報非常普遍，將重點放在必要的故障排除上沒有什麼幫助，因為它可以指向各種問題（即使仍與連線有關），但位於不同的環境中。

有兩種主要可能情況：

案例 1.未啟用雲整合。如果存在任何雲整合，則完全應該會收到此警報。因為不允許連線到雲門戶。

案例 2.已啟用雲整合。在這種情況下，必須進行更詳細的分析，以排除涉及連線故障的不同情況。

運行狀況故障警報示例如下圖所示：

運行狀況故障警報示例

疑難排解

案例1的解決方案。由於FTD無法與https://api-sse.cisco.com/通訊，因此觀察到了雲端組態錯誤

要禁用「Cisco Cloud Configuration-Failure」警報，請導航至**System > Health > Policy > Edit policy > Threat Data Updates on Devices > Choose Enabled(Off)> Save Policy and Exit**。以下是內嵌組態的參考准則。

案例2的解決方案。必須啟用雲整合的時間。

疑難排解的主要實用命令：

```
curl -v -k https://api-sse.cisco.com <-- To verify connection with the external site
nslookup api-sse.cisco.com <-- To dicard any DNS error
/ngfw/etc/sf/connector.properties <-- To verify is configure properly the FQDN settings
lsof -i | grep conn <-- To verify the outbound connection to the cloud on port 8989/tcp is ESTABLISHED
```

選項1.DNS配置不存在

步驟1.確認FTD上已設定DNS伺服器。如果沒有DNS配置，您可以按照以下步驟繼續：

```
> show network
```

步驟2.使用以下命令新增DNS伺服器：

```
> configure network dns servers dns_ip_addresses
```

配置DNS後，運行狀況警報被修復，裝置顯示為正常。可能需要一段時間才能反映更改並設定配置的DNS伺服器。

選項2.客戶DNS無法解析https://api-sse.cisco.com

使用**curl**命令進行測試。如果裝置無法到達雲站點，則您會收到類似於此示例的輸出。

```
FTD01:/home/ldap/abbac# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* getaddrinfo(3) failed for api-sse.cisco.com:443
* Couldn't resolve host 'api-sse.cisco.com'
* Closing connection 0
curl: (6) Couldn't resolve host 'api-sse.cisco.com'
```

> **提示**：從選項1中提供的相同故障排除方法開始。首先驗證DNS配置是否已正確設定。執行curl指令後，您可以注意到DNS問題。

良好且正確的curl輸出必須如下所示：

```
root@fp:/home/admin# curl -v -k https://api-sse.cisco.com
* Rebuilt URL to: https://api-sse.cisco.com/
* Trying 10.6.187.110...
* Connected to api-sse.cisco.com (10.6.187.110) 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, Server finished (14):
* 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 SSL ICA G2
* SSL certificate verify result: self signed certificate in certificate chain (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, 30 Dec 2020 21:41:15 GMT
<Content-Type: text/plain; charset=utf-8
<Content-Length: 9
<Connection: keep-alive
<Keep-Alive: timeout=5
<ETag: "5fb40950-9"
<Cache-Control: no-store
<Pragma: no-cache
<Content-Security-Policy: default-src https: ;
<X-Content-Type-Options: nosniff
<X-XSS-Protection: 1; mode=block
<X-Frame-Options: SAMEORIGIN
<Strict-Transport-Security: max-age=31536000; includeSubDomains
<
* Connection #0 to host api-sse.cisco.com left intact
Forbidden
```

捲曲到伺服器主機名。

```
# curl -v -k https://cloud-sa.amp.cisco.com
*   Trying 10.21.117.50...
* TCP_NODELAY set
* Connected to cloud-sa.amp.cisco.com (10.21.117.50) port 443 (#0)
* ALPN, offering http/1.1
```

```
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
 CApath: none
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
```

使用**nslookup、telnet**和**ping**命令等基本連線工具驗證思科雲站點的正確DNS解析。

注意:Firepower雲服務必須在埠8989/tcp上擁有到雲的出站連線。

將nslookup應用於伺服器主機名。

```
# nslookup cloud-sa.amp.sourcefire.com
# nslookup cloud-sa.amp.cisco.com
# nslookup api.amp.sourcefire.com
# nslookup panacea.threatgrid.com

root@fp:/home/admin# nslookup api-sse.cisco.com
Server: 10.25.0.1
Address: 10.25.0.1#53

Non-authoritative answer:
api-sse.cisco.com canonical name = api-sse.cisco.com.akadns.net.
Name: api-sse.cisco.com.akadns.net
Address: 10.6.187.110
Name: api-sse.cisco.com.akadns.net
Address: 10.234.20.16
```

對於AMP雲的連線問題，可能是由於DNS解析。驗證DNS設定或從FMC執行nslookup。

```
nslookup api.amp.sourcefire.com
```

Telnet

```
root@fp:/home/admin# telnet api-sse.cisco.com 8989
root@fp:/home/admin# telnet api-sse.cisco.com 443
root@fp:/home/admin# telnet cloud-sa.amp.cisco.com 443
```

Ping

```
root@fp:/home/admin# ping api-sse.cisco.com
```

更多疑難排解選項

驗證**/ngfw/etc/sf/connector.properties**下的聯結器屬性。您必須使用正確的聯結器埠(8989)和connector_fqdn使用正確的URL看到此輸出。

```
root@Firepower-module1:sf# cat /ngfw/etc/sf/connector.properties
registration_interval=180
connector_port=8989
region_discovery_endpoint=https://api-sse.cisco.com/providers/sse/api/v1/regions
connector_fqdn=api-sse.cisco.com
```

請參閱Firepower配置指南以獲得更好的參考。

已知的問題

思科錯誤ID CSCvs05084 FTD思科雲配置因代理失敗

思科錯誤ID CSCvp56922使用update-context sse-connector API更新裝置主機名和版本

思科錯誤ID CSCvu02123 DOC錯誤：在CTR配置指南中將Firepower裝置可訪問的URL更新為SSE

思科漏洞ID CSCvr46845 ENH：運行狀況消息「Cisco Cloud Configuration - Failure」需要改進

[影片] Firepower — 將FMC註冊到SSE

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）。