由於DNS解析，安全防火牆FTD事件日誌記錄到CDO/cdFMC失敗

問題

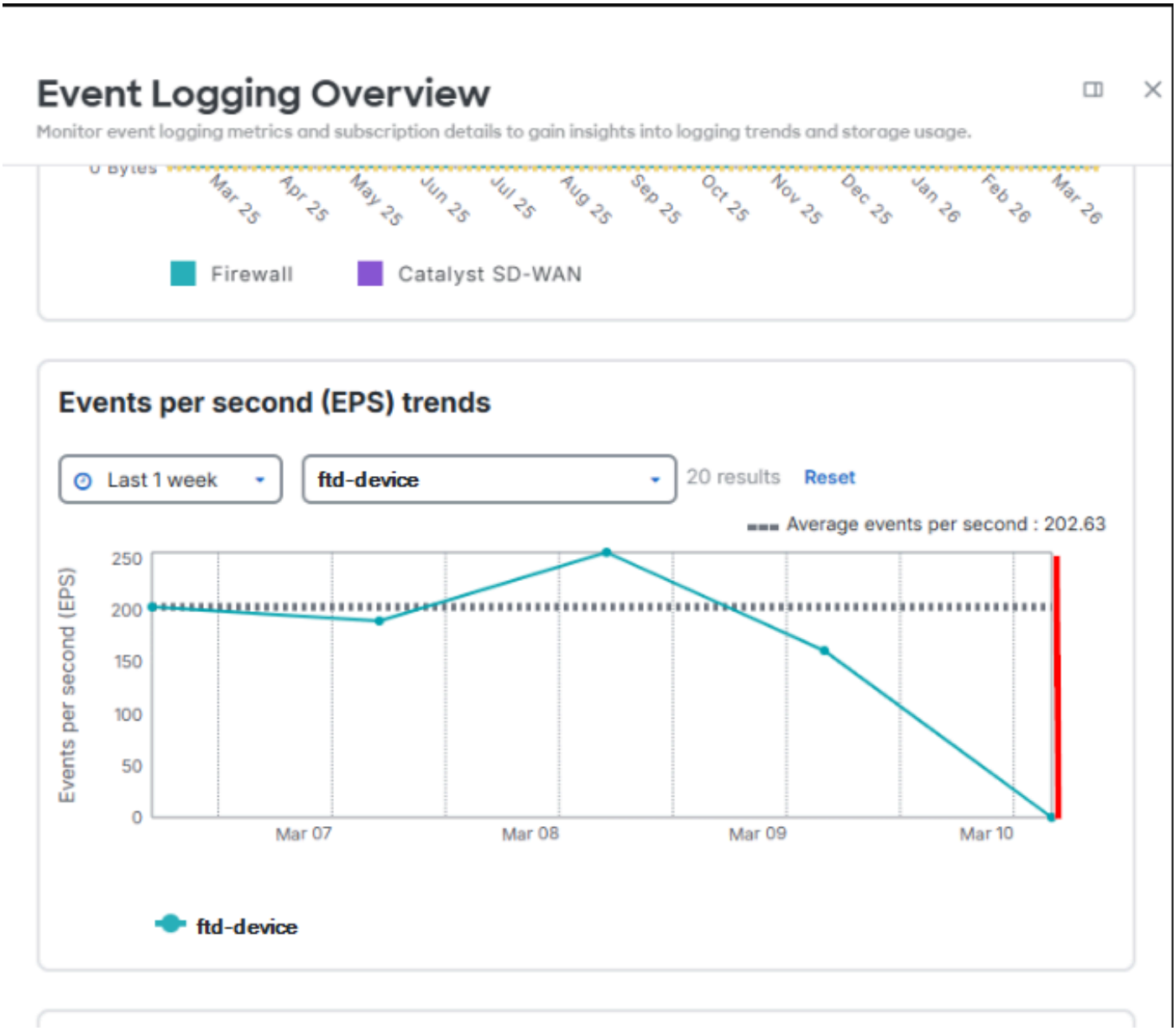
連線事件日誌記錄已停止出現在單個防火牆威脅防禦(FTD)的Cisco Defense Orchestrator(CDO)事件日誌和雲交付的防火牆管理中心(cdFMC)事件頁面中。 受影響的裝置無法將連線事件日誌傳送到雲管理平台，從而影響生產可見性和故障排除功能。分析顯示，由於臨時名稱解析失敗，FTD在連線到思科事件服務時反複遇到失敗，DNS解析失敗的時間戳與事件頁面中連線事件停止的時間完全相關。

環境

- 由CDO和cdFMC管理的Cisco安全防火牆FTD
- 在FTD管理介面上設定的DNS伺服器
- 需要連線事件可見性以進行故障排除的生產環境

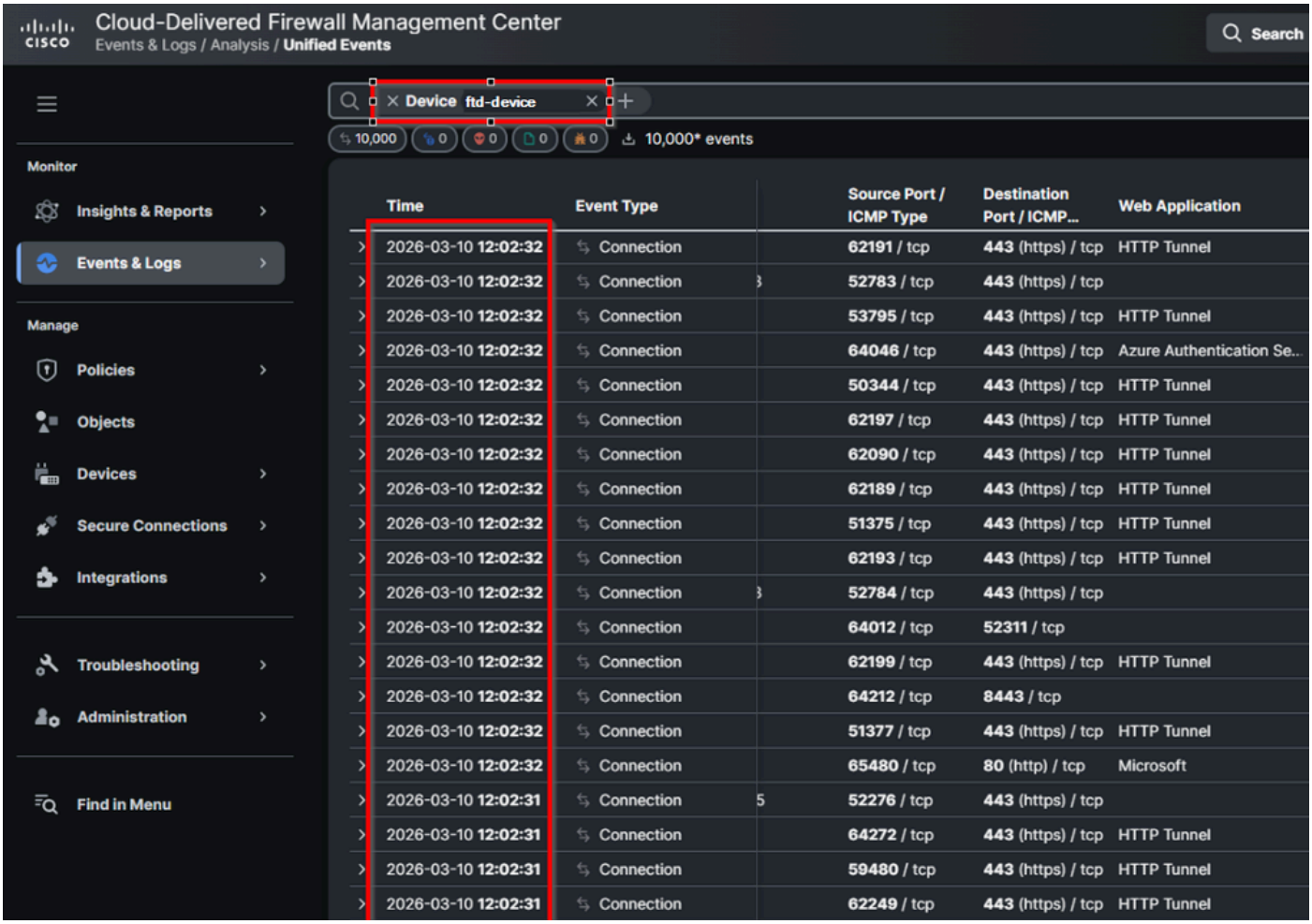
解析

1:檢視「CDO事件日誌記錄」和「cdFMC統一/連線事件」頁面，確定事件丟失的時間。



inline_image_0.png

inline_image_0.png



inline_image_1.png

inline_image_1.png

2:確保必要的FTD程式正在運行，以允許事件產生和傳送：

<#root>

```
root@ftd-device:/ngfw/var/log# pmtool status | grep Event
Required by: SFDataCorrelator,expire-session,TSS_Daemon,snapshot_manager,fpcollect,Syncd,Pruner,ActionQ

EventHandler (normal) - Running 17453

Command: /ngfw/usr/local/sf/bin/EventHandler
    LD_LIBRARY_PATH=/ngfw/usr/local/sf/lib64/EventHandlerModules
PID File: /ngfw/var/sf/run/EventHandler.pid
Enable File: /ngfw/etc/sf/EventHandler.run
--
root@ftd-device:/ngfw/var/log# pmtool status | grep SSE

SSEConnector (system) - Running 20697

Required by: ngfwManager,ASAConfig,tomcat,SSEConnector,rsyncd,hmdaemon,srt,UUID
```

3:檢視FTD以查詢指示原因的EventHandler和聯結器日誌資料的關聯：

<#root>

```
/ngfw/var/log/EventHandlerStat.* | grep -E "TotalEvents|SSEConnector"
{"Time": "2026-03-10T16:00:25Z", "TotalEvents": 104659, "PerSec": 348, "UserCPUSec": 9.242, "SysCPUSec"
{"Time": "2026-03-10T16:00:25Z",

"Consumer": "SSEConnector", "Events": 104649, "PerSec": 348, "CPUSec": 9.924, "%CPU": 3.3}

{"Time": "2026-03-10T16:00:25Z", "ConsumerEvent": "SSEConnector-ConnectionEvent", "InTransforms": 10464
{"Time": "2026-03-10T16:05:25Z", "TotalEvents": 57651, "PerSec": 192, "UserCPUSec": 5.382, "SysCPUSec":
{"Time": "2026-03-10T16:05:25Z",

 "Consumer": "SSEConnector", "Events": 57641, "PerSec": 192, "CPUSec": 5.900, "%CPU": 2.0, "OutputWaitSe

{"Time": "2026-03-10T16:05:25Z", "ConsumerEvent": "SSEConnector-ConnectionEvent", "InTransforms": 57641
{"Time": "2026-03-10T16:10:25Z", "TotalEvents": 24, "PerSec": 0, "UserCPUSec": 0.314, "SysCPUSec": 0.54
{"Time": "2026-03-10T16:10:25Z",

"Consumer": "SSEConnector", "Events": 14, "PerSec": 0, "CPUSec": 0.046, "%CPU": 0.0, "OutputWaitSec": 30

{"Time": "2026-03-10T16:10:25Z", "ConsumerEvent": "SSEConnector-ConnectionEvent", "InTransforms": 14, "
{"Time": "2026-03-10T16:15:25Z", "TotalEvents": 10, "PerSec": 0, "UserCPUSec": 0.214, "SysCPUSec": 0.60
{"Time": "2026-03-10T16:15:25Z",

 "Consumer": "SSEConnector", "Events": 0, "PerSec": 0, "CPUSec": 0.009, "%CPU": 0.0, "OutputWaitSec": 30

{"Time": "2026-03-10T16:10:25Z", "ConsumerEvent": "SSEConnector-ConnectionEvent", "InTransforms": 0, "O
---
/ngfw/var/log/messages | grep "SSEConnector"
Mar 12 11:36:01 ftd-device SF-IMS[62079]: [62112] EventHandler:EventHandler

[ERROR] Consumer SSEConnector publishing blocked for 330.801 sec: Resource temporarily unavailable

---
/ngfw/var/log/connector/connector.log | grep "failure in name resolution"
time="2026-03-10T12:02:44.329750985-04:00" level=error msg="[ftd-device][events.go:100 events:connectWe

dial tcp: lookup eventing-ingest.sse.itd.cisco.com: Temporary failure in name resolution"

time="2026-03-10T12:02:44.329830226-04:00" level=warning msg="[ftd-device][events.go:181 events:(*Servi

Could not connect to WebSocket endpoint wss://eventing-ingest.sse.itd.cisco.com:443/ingest: dial tcp: lo
```

4:驗證FTD已設定的DNS伺服器和可連線性：

<#root>

```
> show network
===============[System Information]===============
Hostname                  : ftd-device

DNS Servers               : 10.0.0.10

DNS from router           : enabled
Management port           : 8305
IPv4 Default route
  Gateway                 : 10.0.0.1
==================[management0]===================
Admin State               : Enabled
Admin Speed               : 40gbps
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : A1:A2:A3:A4:A5:A6
----------------------[IPv4]----------------------
Configuration             : Manual
Address                   : 10.0.0.2
Netmask                   : 255.255.255.0
Gateway                   : 10.0.0.1
----------------------[IPv6]----------------------
Configuration             : Disabled
> expert
admin@device:~$ sudo su
Password: [enter admin password]
root@device:/Volume/home/admin# ping 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10: icmp_seq=1 ttl=58 time=1.64 ms
64 bytes from 10.0.0.10: icmp_seq=2 ttl=58 time=1.72 ms
64 bytes from 10.0.0.10: icmp_seq=3 ttl=58 time=1.70 ms
^C
--- 10.0.0.10 ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 144ms

rtt min/avg/max/mdev = 1.639/1.678/1.724/0.033 ms
```

5:驗證從FTD到Cisco事件服務的DNS解析和HTTPS連線：

```
root@device:/Volume/home/admin# nslookup eventing-ingest.sse.itd.cisco.com
root@device:/Volume/home/admin# curl -v -k https://eventing-ingest.sse.itd.cisco.com
root@device:/Volume/home/admin# telnet eventing-ingest.sse.itd.cisco.com 443
```

動作

使用者發現並解決了DNS伺服器的一個內部問題。DNS功能恢復後：

- FTD能夠解析所需的思科事件網域。
- FTD會自動重新建立事件連線。
- 連線事件日誌繼續按設計出現在cdFMC中。

所有糾正操作均由使用者執行，無需更改配置。

原因

根本原因是FTD管理介面上的DNS解析失敗，尤其是因為已設定DNS伺服器發生問題所致。由於FTD無法解析所需的思科事件域，包括eventing-ingest.sse.itd.cisco.com，因此它無法建立傳出事件連線，導致連線事件無法傳遞到思科安全雲。在DNS解析恢復後，使用者確認連線事件日誌記錄已完全正常運行並在生產環境中正常運行。

相關內容

- 關於安全防火牆威脅防禦和Cisco XDR整合
- 思科技術支援與下載
- 本文以外可能存在的缺陷：思科錯誤ID CSCwr75332 FTD無法將事件轉送到安全雲控制

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）。