Registrazione eventi FTD firewall sicuro su CDO/cdFMC non riuscita a causa della risoluzione DNS

Problema

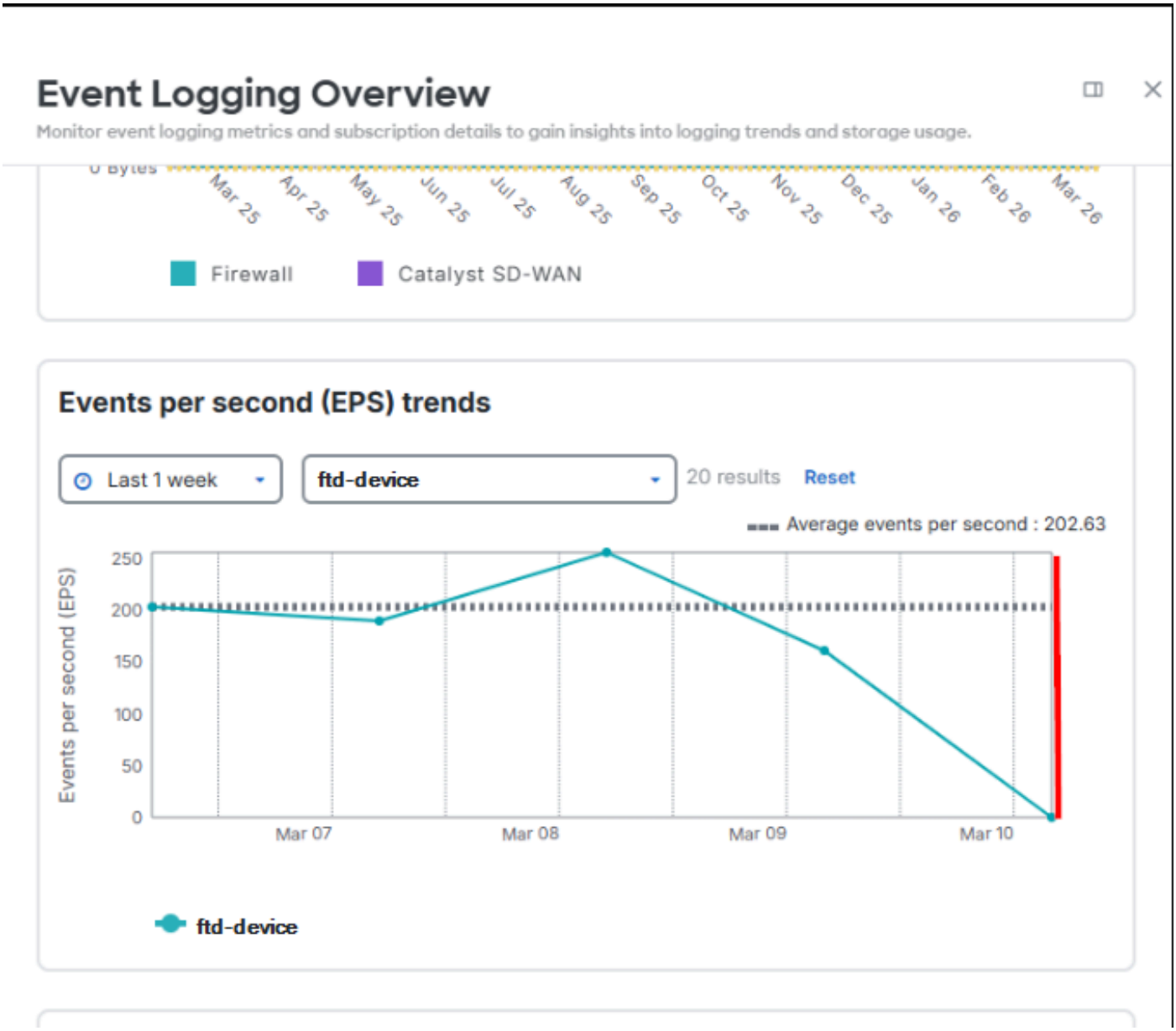
La registrazione degli eventi di connessione non è più visualizzata nelle pagine degli eventi di Cisco Defense Orchestrator (CDO) Event Logging e Firewall Management Center (cdFMC) recapitati nel cloud per un singolo FTD (Firewall Threat Defense). Il dispositivo interessato non è stato in grado di inviare i registri degli eventi di connessione alla piattaforma di gestione cloud, con effetti sulla visibilità della produzione e sulle funzionalità di risoluzione dei problemi. Dall'analisi è emerso che l'FTD stava riscontrando ripetuti errori di connessione ai servizi eventi Cisco a causa di errori temporanei di risoluzione dei nomi, con il timestamp degli errori di risoluzione DNS esattamente correlato al momento in cui gli eventi di connessione non vengono più visualizzati nelle pagine degli eventi.

Ambiente

- Cisco Secure Firewall FTD gestito da CDO con cdFMC
- Server DNS configurato nell'interfaccia di gestione FTD
- Ambiente di produzione che richiede visibilità degli eventi di connessione per la risoluzione dei problemi

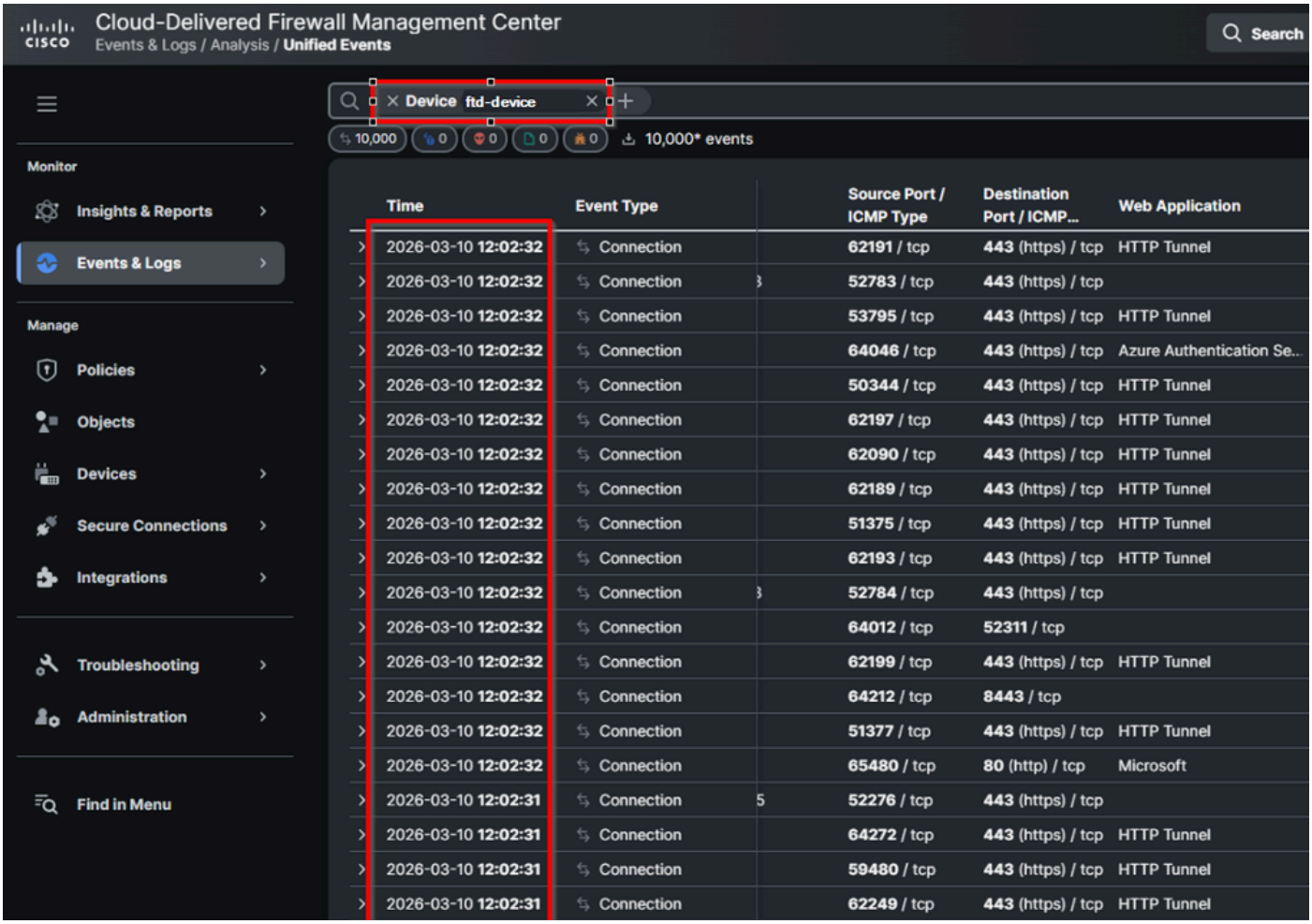
Risoluzione

1: Esaminare le pagine Registrazione eventi CDO e Evento connessione CdFMC unificato per determinare il tempo di perdita degli eventi.



inline_image_0.png

inline_image_0.png



inline_image_1.png

inline_image_1.png

2: Assicurarsi che i processi FTD necessari siano in esecuzione per consentire la generazione e l'invio degli eventi:

<#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: Esaminare l'FTD per trovare i dati di registro EventHandler e Connector correlati che indicano la causa:

<#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: Verificare il server DNS configurato per gli FTD e la raggiungibilità:

<#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: Verificare la risoluzione DNS e la connettività HTTPS dall'FTD ai servizi eventi Cisco:

```
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
```

Azioni

L'utente ha identificato e risolto un problema interno con il server DNS. Dopo il ripristino della funzionalità DNS:

- L'FTD è stato in grado di risolvere i domini degli eventi Cisco richiesti.
- L'FTD ristabilisce automaticamente la connettività degli eventi.
- Registri eventi di connessione ripresi visualizzati in cdFMC come progettati.

Tutte le azioni correttive sono state eseguite dall'utente senza la necessità di apportare modifiche alla configurazione.

Causa

La causa principale è un errore di risoluzione DNS sull'interfaccia di gestione FTD, causato in modo specifico da un problema con il server DNS configurato. Poiché l'FTD non è in grado di risolvere i domini di eventi Cisco richiesti, incluso eventing-ingest.sse.itd.cisco.com, non è stato in grado di stabilire connessioni di eventi in uscita. Gli eventi di connessione non verranno pertanto recapitati a Cisco Security Cloud. Dopo il ripristino della risoluzione DNS, l'utente ha confermato che la registrazione degli eventi di connessione era completamente operativa e funzionava normalmente nell'ambiente di produzione.

Contenuto correlato

- Informazioni su Secure Firewall Threat Defense e sull'integrazione di Cisco XDR
- Supporto tecnico Cisco e download
- Possibile difetto oltre questo articolo: Cisco ID bug CSCwr75332 FTD non riesce a inoltrare gli eventi al controllo del cloud di sicurezza

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).