El registro de eventos FTD de firewall seguro para CDO/cdFMC falla debido a la resolución DNS

Problema

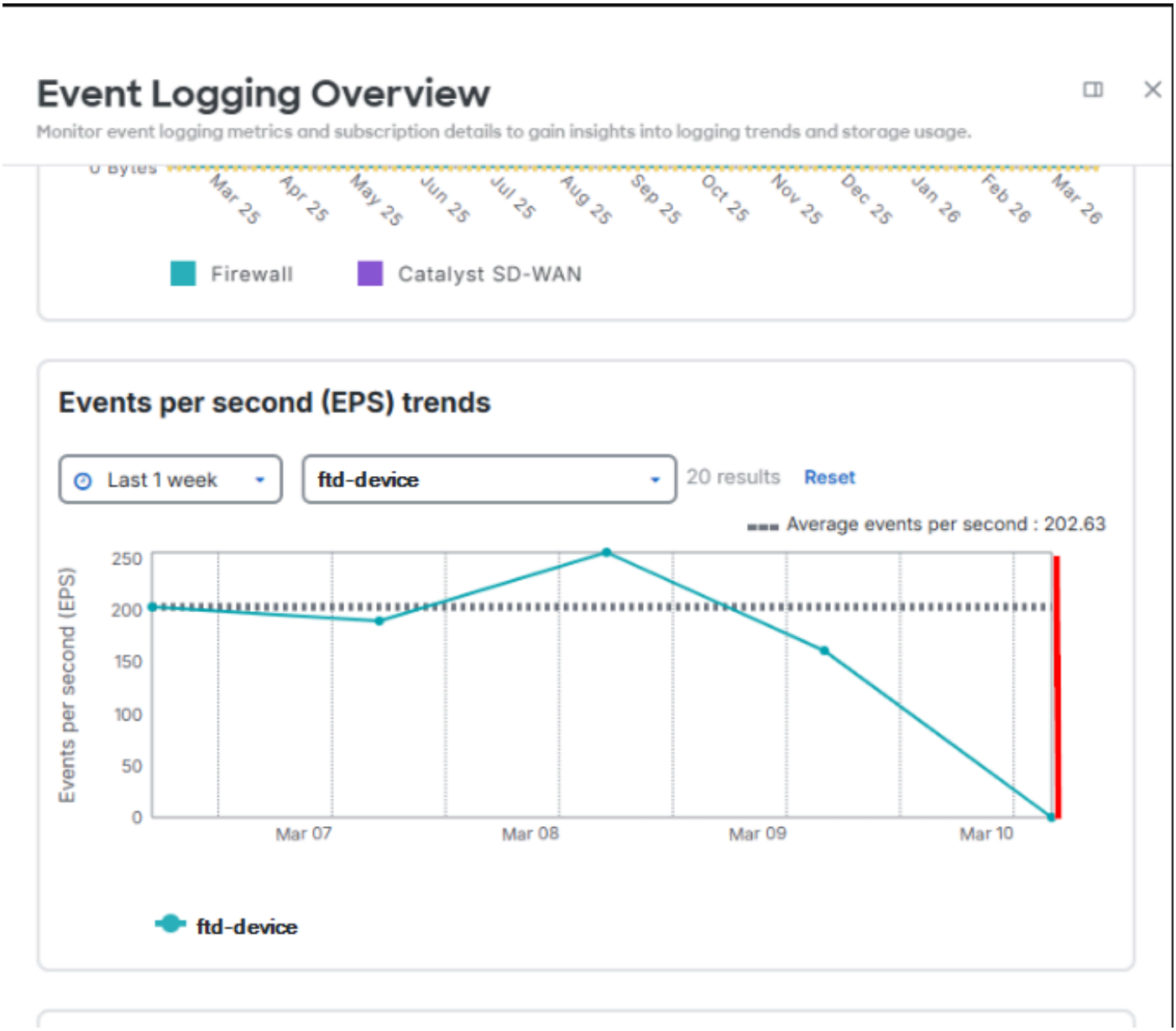
El registro de eventos de conexión dejó de aparecer en las páginas de eventos de Cisco Defense Orchestrator (CDO) Event Logging y en las páginas de eventos del centro de gestión de firewall (cdFMC) proporcionadas en la nube para crear un único firewall Threat Defence (FTD). El dispositivo afectado no pudo enviar los registros de eventos de conexión a la plataforma de gestión en la nube, lo que afectó a la visibilidad de la producción y a las capacidades de solución de problemas. El análisis reveló que el FTD estaba experimentando fallos repetidos para conectarse a los servicios de eventos de Cisco debido a fallos temporales en la resolución de nombres, con el registro de hora de los fallos de resolución DNS que se correlaciona exactamente con el momento en que los eventos de conexión dejaron de aparecer en las páginas de eventos.

Entorno

- Cisco Secure Firewall FTD gestionado por CDO con cdFMC
- Servidor DNS configurado en la interfaz de administración de FTD
- Entorno de producción que requiere visibilidad de eventos de conexión para solucionar problemas

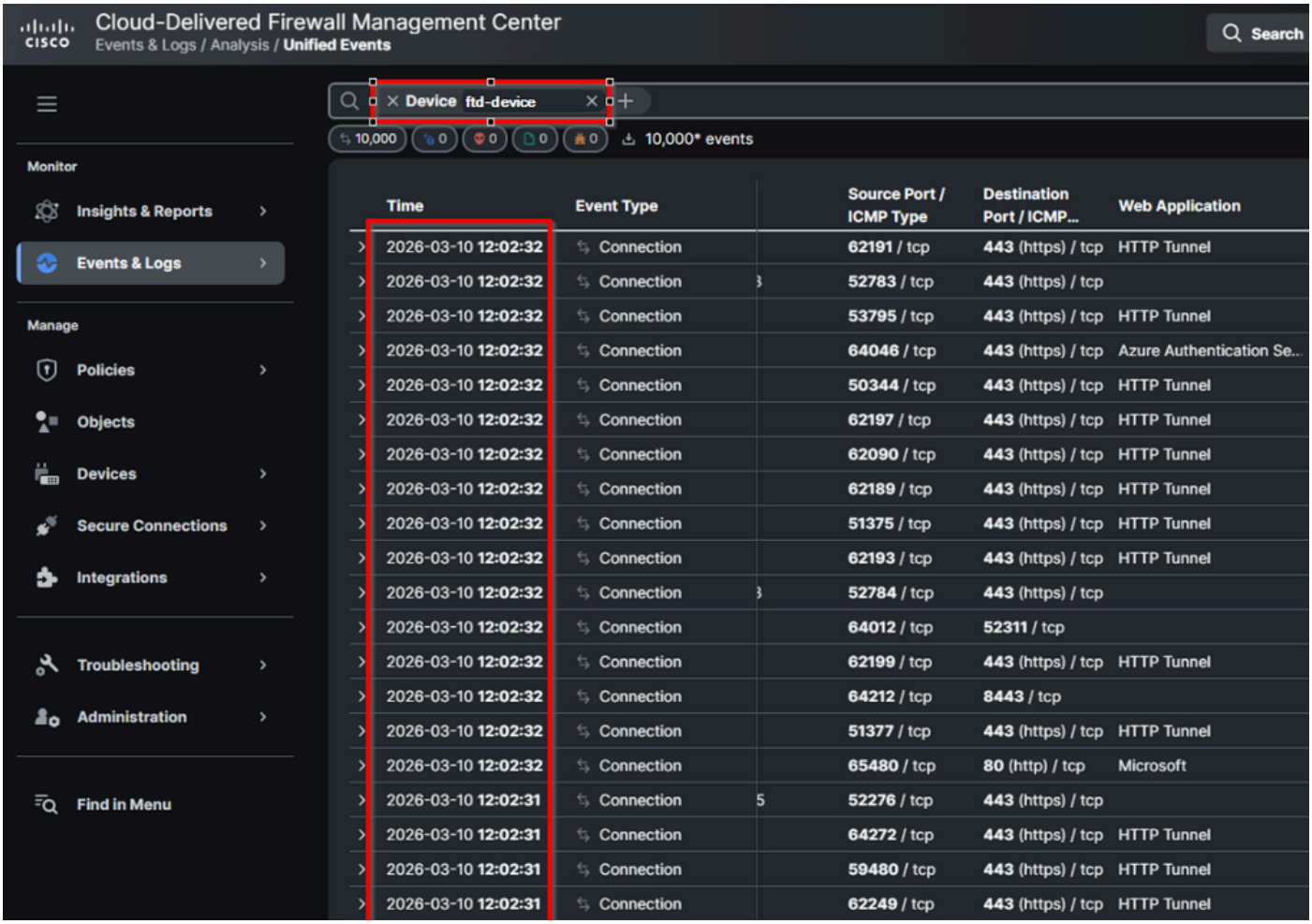
Resolución

1: Revise las páginas Registro de eventos de CDO y cdFMC Unified/Connection Event para determinar el tiempo de pérdida de eventos.



inline_image_0.png

inline_image_0.png



inline_image_1.png

inline_image_1.png

2: Asegúrese de que se estén ejecutando los procesos de FTD necesarios para permitir la generación y el envío de eventos:

<#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: Revise el FTD para encontrar los datos de registro de EventHandler y Connector correlacionados que indican 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: Verifique el servidor DNS configurado y la disponibilidad de los FTD:

<#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: Verifique la resolución DNS y la conectividad HTTPS desde el FTD a los servicios de eventos de 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
```

Acciones

El usuario identificó y resolvió un problema interno con su servidor DNS. Una vez restaurada la funcionalidad de DNS:

- El FTD ha podido resolver los dominios de eventos de Cisco requeridos.
- El FTD restableció automáticamente la conectividad de eventos.
- Los registros de eventos de conexión se reanudaron y aparecieron en cdFMC según lo diseñado.

El usuario realizó todas las acciones correctivas sin necesidad de realizar cambios en la configuración.

Causa

La causa raíz fue un error de resolución de DNS en la interfaz de administración de FTD, causado específicamente por un problema con el servidor DNS configurado. Debido a que el FTD no pudo resolver los dominios de eventos de Cisco requeridos, incluido eventing-ingest.sse.itd.cisco.com, no pudo establecer conexiones de eventos salientes, por lo que los eventos de conexión no se entregaron a Cisco Security Cloud. Después de restaurar la resolución DNS, el usuario confirmó que el registro de eventos de conexión estaba completamente operativo y funcionando normalmente en el entorno de producción.

Contenido relacionado

- Acerca de Secure Firewall Threat Defence e integración con Cisco XDR
- Soporte técnico y descargas de Cisco
- Posible defecto más allá de este artículo: El ID de bug de Cisco CSCwr75332 FTD no reenvía los eventos al control de la nube de seguridad

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).