Die sichere Firewall FTD-Ereignisprotokollierung zu CDO/cdFMC schlägt aufgrund der DNS-Auflösung fehl

Problem

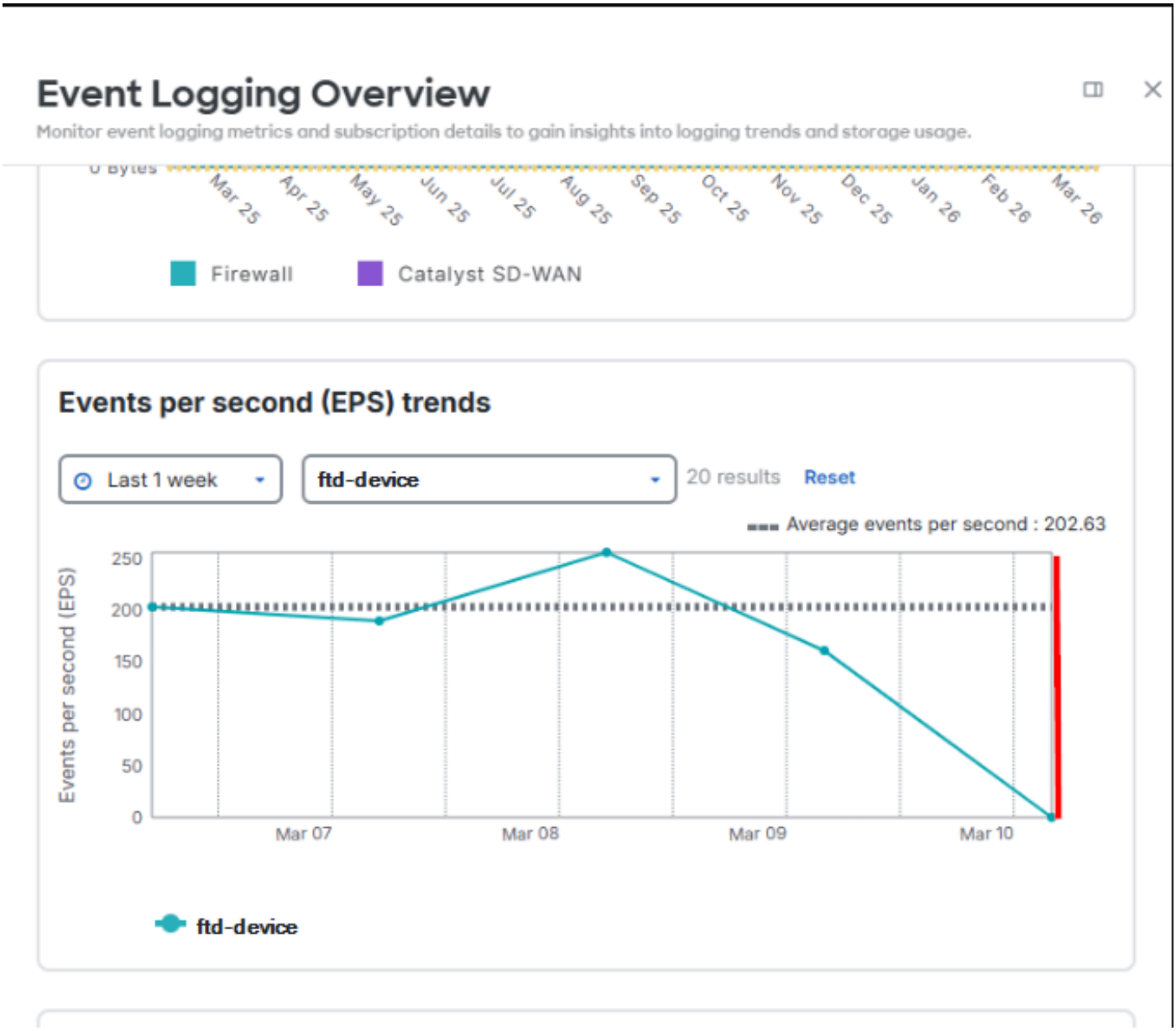
Die Protokollierung von Verbindungsereignissen wurde auf den Seiten Cisco Defense Orchestrator (CDO) Event Logging (Ereignisprotokollierung) und Cloud-gestütztes Firewall Management Center (cdFMC) Events (Ereignisse) für eine einzelne Firewall Threat Defense (FTD)-Seite beendet. Das betroffene Gerät konnte keine Verbindungsereignisprotokolle an die Cloud-Management-Plattform senden, was sich auf die Produktionstransparenz und die Fehlerbehebungsfunktionen auswirkte. Die Analyse ergab, dass die FTD aufgrund von temporären Fehlern bei der Namensauflösung wiederholt keine Verbindung zu den Cisco Ereignisdiensten herstellen konnte. Der Zeitstempel der DNS-Auflösungsfehler korrelierte genau mit dem Zeitpunkt, an dem Verbindungsereignisse nicht mehr auf Ereignisseiten angezeigt wurden.

Umwelt

- Cisco Secure Firewall FTD verwaltet durch CDO mit cdFMC
- DNS-Server an FTD-Management-Schnittstelle konfiguriert
- Produktionsumgebung, die eine transparente Fehlerbehebung für Verbindungsereignisse erfordert

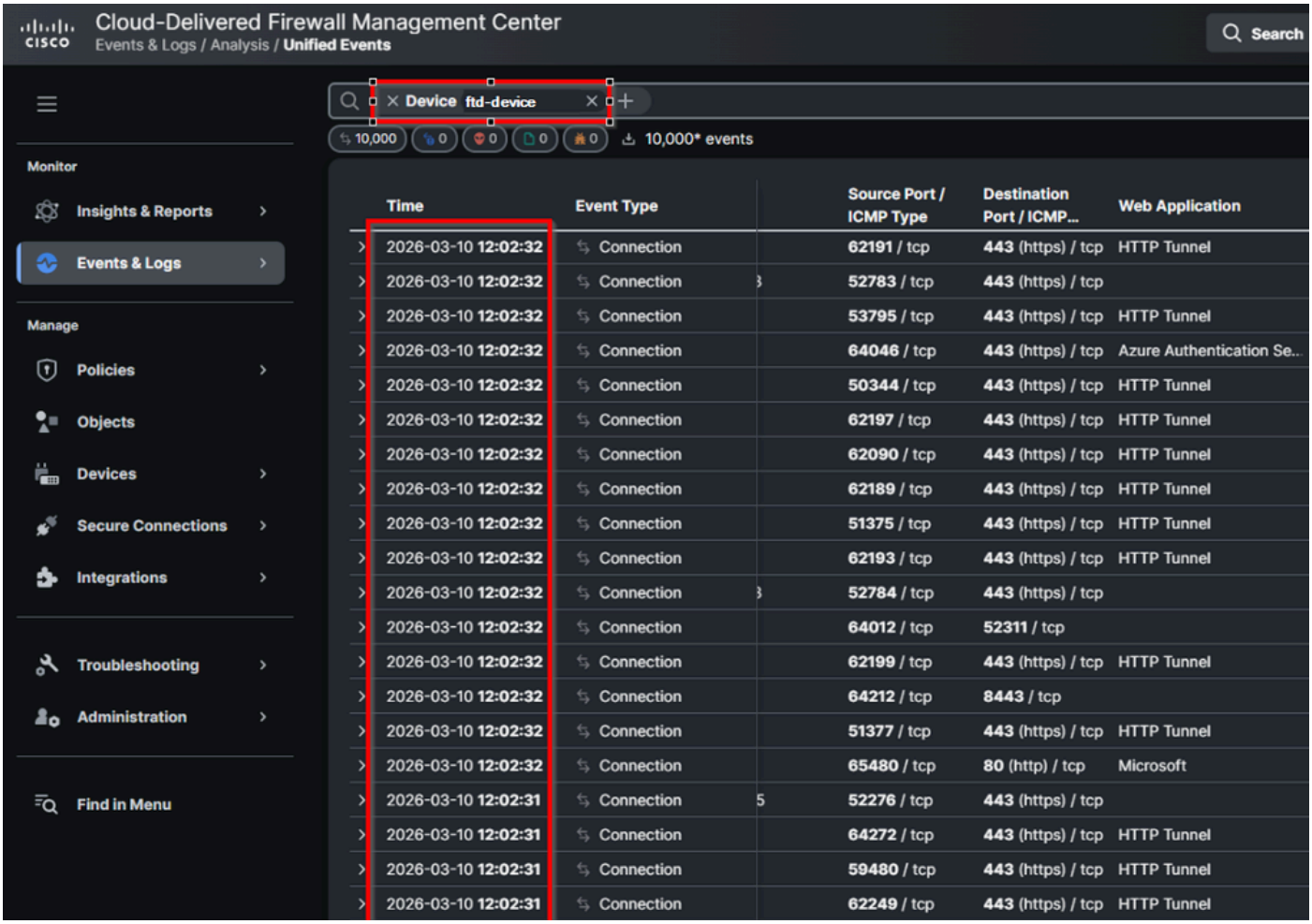
Auflösung

1: Auf den Seiten CDO Event Logging (CDO-Ereignisprotokollierung) und cdFMC Unified/Connection Event (cdFMC-Unified/Connection-Ereignis) können Sie den Zeitpunkt eines Ereignisverlusts ermitteln.



inline_image_0,png

inline_image_0,png



inline_image_1.png

inline_image_1.png

2: Stellen Sie sicher, dass die erforderlichen FTD-Prozesse ausgeführt werden, damit Ereignisse generiert und gesendet werden können:

<#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: Überprüfen Sie die FTD, um die entsprechenden EventHandler- und Connector-Protokolldaten zur Ursache zu finden:

<#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: Überprüfen Sie, ob die FTDs den DNS-Server konfiguriert haben und ob er erreichbar ist:

<#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: Überprüfung der DNS-Auflösung und HTTPS-Verbindung vom FTD zu den Cisco Ereignisdiensten:

```
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
```

Aktionen

Der Benutzer hat ein internes Problem mit seinem DNS-Server identifiziert und behoben. Sobald die DNS-Funktionalität wiederhergestellt wurde:

- Die FTD konnte die erforderlichen Cisco Ereignisdomänen beheben.
- Die FTD stellte die Ereignisverbindung automatisch wieder her.
- Verbindungsereignisprotokolle wurden wieder aufgenommen und werden wie vorgesehen in cdFMC angezeigt.

Alle Korrekturmaßnahmen wurden vom Benutzer durchgeführt, ohne dass Konfigurationsänderungen erforderlich waren.

Ursache

Die Ursache war ein DNS-Auflösungsfehler auf der FTD-Verwaltungsschnittstelle, der speziell durch ein Problem mit dem konfigurierten DNS-Server verursacht wurde. Da die FTD nicht in der Lage war, die erforderlichen Cisco Ereignising-Domänen, einschließlich eventing-ingest.sse.itd.cisco.com, aufzulösen, konnte sie keine ausgehenden Ereignisverbindungen herstellen, was dazu führte, dass Verbindungsereignisse nicht an die Cisco Security Cloud übermittelt wurden. Nachdem die DNS-Auflösung wiederhergestellt wurde, bestätigte der Benutzer, dass die Protokollierung der Verbindungsereignisse voll funktionsfähig ist und in der Produktionsumgebung normal funktioniert.

Verwandte Inhalte

- Informationen zu Secure Firewall Threat Defense und zur Cisco XDR-Integration
- Technischer Support und Downloads von Cisco
- Möglicher Mangel über diesen Artikel hinaus: Cisco Bug-ID CSCwr75332 FTD leitet Ereignisse nicht an Security Cloud Control weiter

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.