Beveiligde firewall FTD-gebeurtenisregistratie naar CDO/cdFMC mislukt vanwege DNS-resolutie

uitgeven

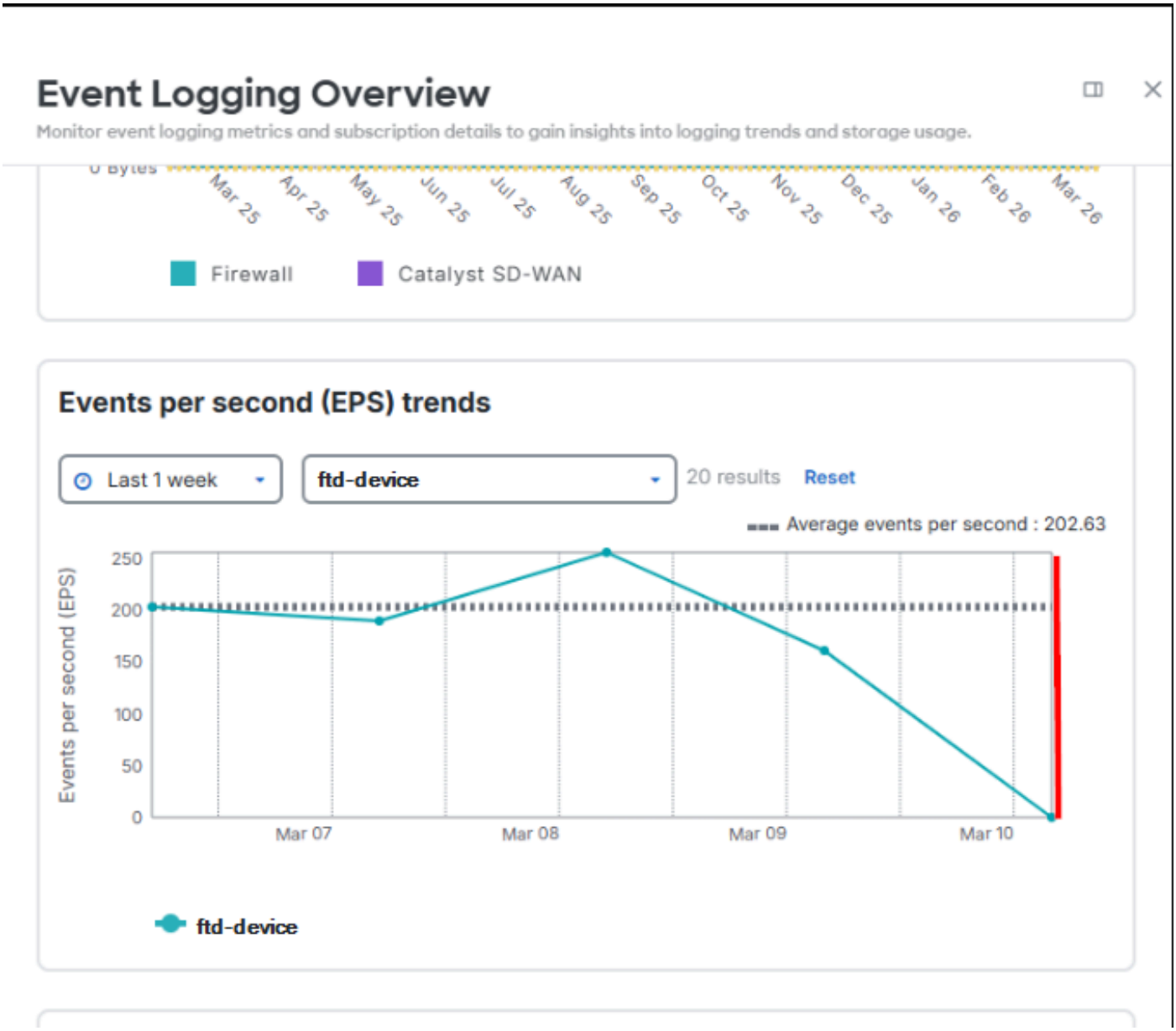
Logboekregistratie van verbindingsgebeurtenissen is niet meer weergegeven in de gebeurtenislogboekregistratie van Cisco Defense Orchestrator (CDO) en de door de cloud geleverde pagina's van het Firewall Management Center (cdFMC) voor gebeurtenissen voor één Firewall Threat Defense (FTD). Het getroffen apparaat kon geen logboeken van verbindingsgebeurtenissen naar het cloudbeheerplatform verzenden, waardoor de zichtbaarheid van de productie en de mogelijkheden voor probleemoplossing werden beïnvloed. Analyse toonde aan dat de FTD herhaaldelijk problemen ondervond om verbinding te maken met Cisco-eventingservices vanwege tijdelijke naamoplossingsfouten, waarbij de tijdstempel van DNS-resolutiefouten precies correleerde met wanneer verbindingsgebeurtenissen niet meer op eventingpagina's verschenen.

milieu

- Cisco Secure Firewall FTD beheerd door CDO met cdFMC
- DNS-server geconfigureerd via FTD-beheerinterface
- Productieomgeving die zichtbaarheid van verbindingsgebeurtenissen vereist voor probleemoplossing

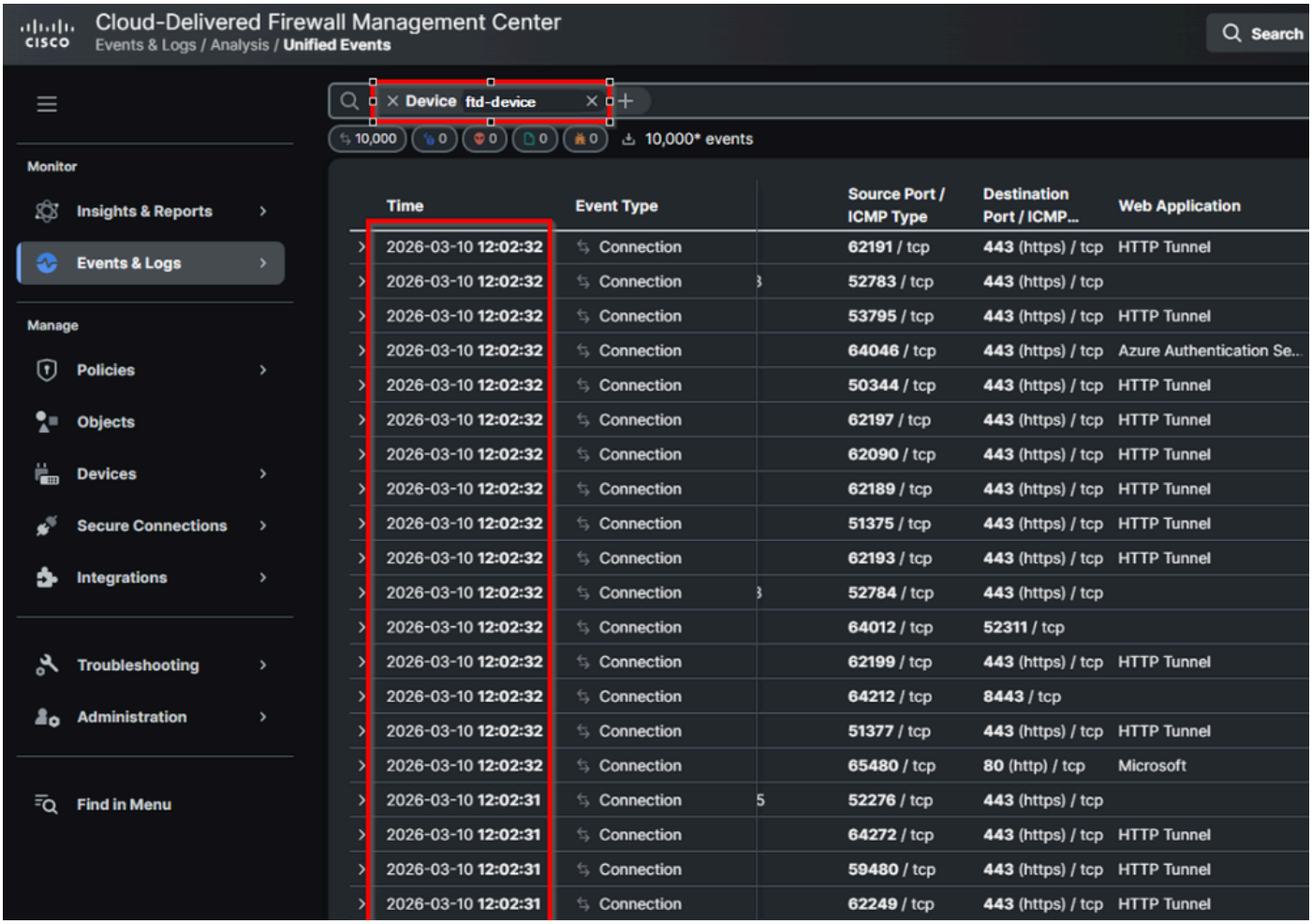
resolutie

1: Controleer de pagina's CDO Event Logging en cdFMC Unified/Connection Event om het tijdstip van gebeurtenisverlies te bepalen.



inline_image_0.png

inline_image_0.png



inline_image_1.png

inline_image_1.png

2: Zorg ervoor dat de nodige FTD-processen worden uitgevoerd om het genereren en verzenden van gebeurtenissen mogelijk te maken:

<#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: Controleer de FTD om de correlerende loggegevens van EventHandler en Connector te vinden die de oorzaak aangeven:

<#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: Controleer de door de FTD's geconfigureerde DNS-server en bereikbaarheid:

<#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: Controleer de DNS-resolutie en HTTPS-connectiviteit van de FTD naar Cisco-eventingservices:

```
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
```

Acties

De gebruiker heeft een intern probleem met zijn DNS-server geïdentificeerd en opgelost. Nadat de DNS-functionaliteit is hersteld:

- De FTD kon de vereiste Cisco eventing-domeinen oplossen.
- De FTD herstelde automatisch de eventing-connectiviteit.
- Logboeken van verbindingsgebeurtenissen worden opnieuw weergegeven in cdFMC zoals ontworpen.

Alle corrigerende acties werden door de gebruiker uitgevoerd zonder dat er configuratiewijzigingen nodig waren.

Oorzaak

De hoofdoorzaak was een DNS-oplossingsfout op de FTD-beheerinterface, die specifiek werd veroorzaakt door een probleem met de geconfigureerde DNS-server. Omdat de FTD de vereiste Cisco eventing-domeinen, waaronder eventing-ingest.sse.itd.cisco.com, niet kon oplossen, kon deze geen uitgaande eventing-verbindingen tot stand brengen, waardoor verbindingsgebeurtenissen niet werden geleverd aan de Cisco Security Cloud. Nadat de DNS-resolutie was hersteld, bevestigde de gebruiker dat de logboekregistratie van verbindingsgebeurtenissen volledig operationeel was en normaal functioneerde in de productieomgeving.

Verwante inhoud

- Informatie over Secure Firewall Threat Defense en Cisco XDR-integratie
- Cisco Technical Support en downloads
- Mogelijk defect buiten dit artikel: Cisco bug ID CSCwr75332 FTD kan gebeurtenissen niet doorsturen naar Security Cloud Control

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.