Échec de la journalisation des événements FTD du pare-feu sécurisé sur CDO/cdFMC en raison de la résolution DNS

Problème

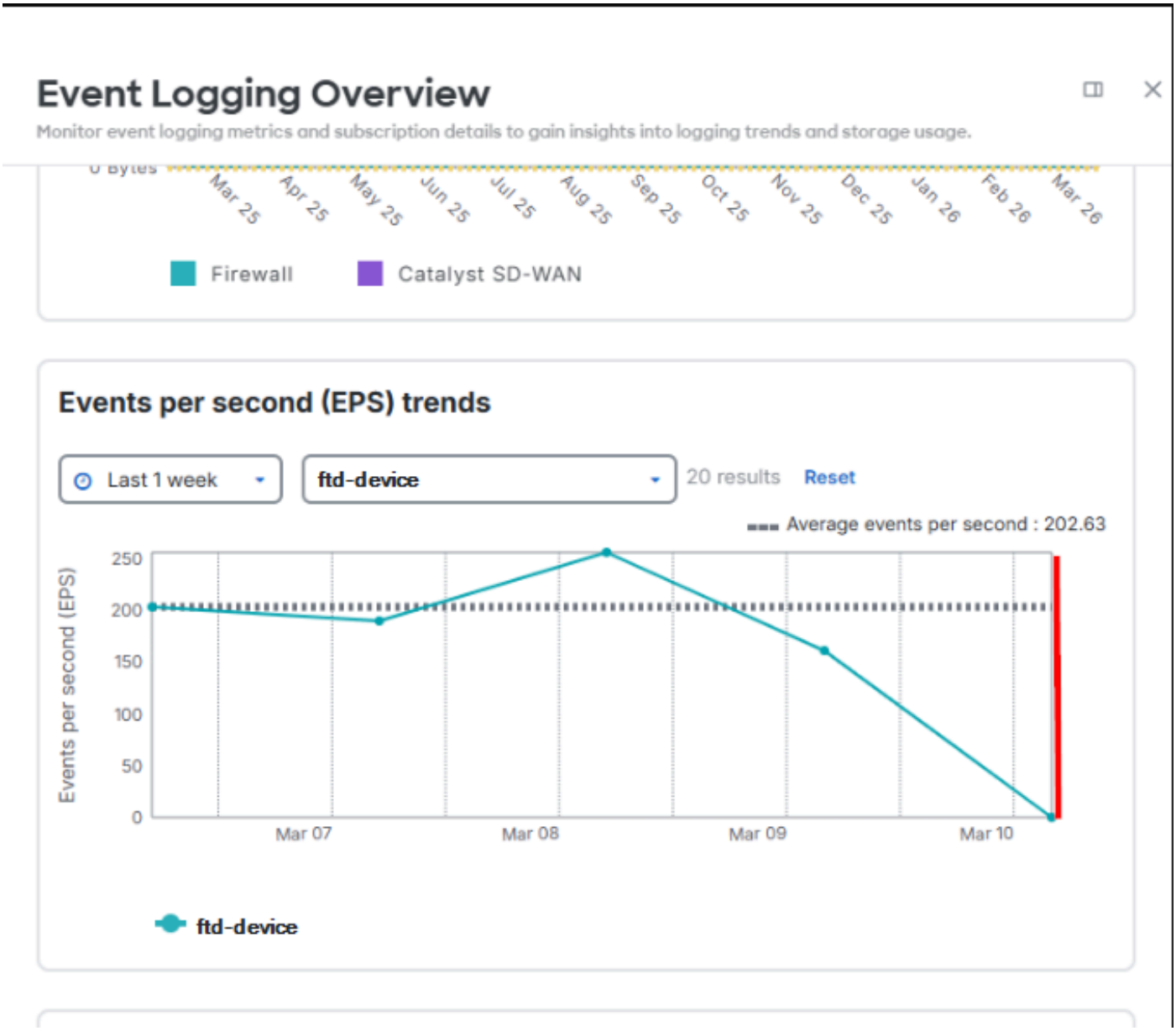
La journalisation des événements de connexion a cessé d'apparaître dans les pages Event Logging de Cisco Defense Orchestrator (CDO) et Firewall Management Center (cdFMC) Events livrées dans le cloud pour un seul pare-feu de défense contre les menaces (FTD). Le périphérique affecté n'a pas pu envoyer de journaux d'événements de connexion à la plate-forme de gestion du cloud, ce qui a affecté la visibilité de la production et les capacités de dépannage. L'analyse a révélé que le FTD rencontrait des échecs répétés de connexion aux services d'événements Cisco en raison d'échecs temporaires de résolution de noms, l'horodatage des échecs de résolution DNS étant corrélé exactement avec le moment où les événements de connexion cessaient d'apparaître dans les pages d'événements.

Environnement

- Cisco Secure Firewall FTD géré par CDO avec cdFMC
- Serveur DNS configuré sur l'interface de gestion FTD
- Environnement de production nécessitant une visibilité des événements de connexion pour le dépannage

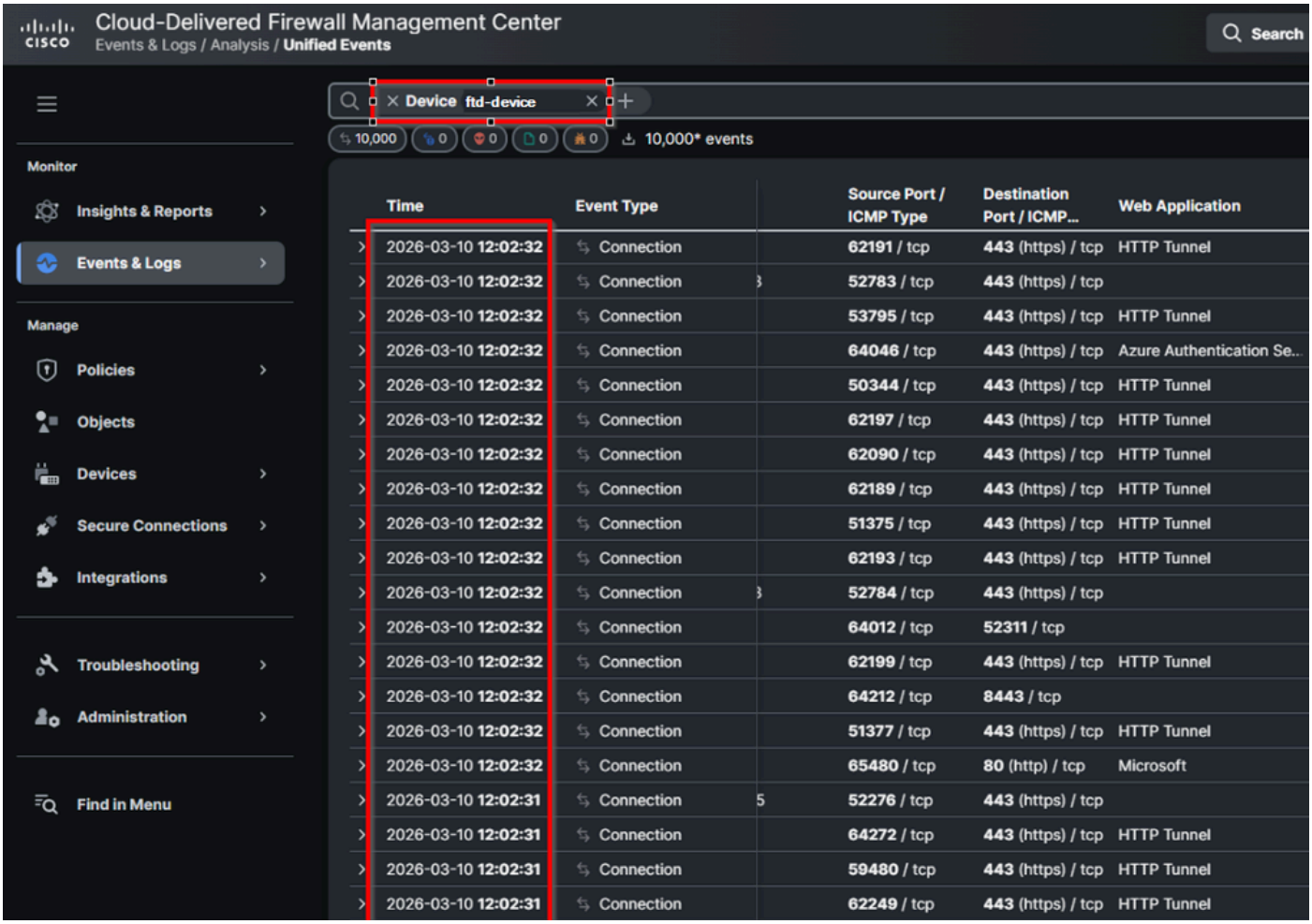
Résolution

1: Consultez les pages Journalisation des événements CDO et Événement cdFMC Unified/Connection pour déterminer l'heure de la perte d'événement.



image_en_ligne_0.png

image_en_ligne_0.png



image_inline_1.png

image_inline_1.png

2: Assurez-vous que les processus FTD nécessaires sont en cours d'exécution pour permettre la génération et l'envoi d'événements :

<#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: Vérifiez le FTD pour trouver les données de journal EventHandler et Connector corrélées indiquant la cause :

<#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: Vérifiez les FTD configurés pour le serveur DNS et l'accessibilité :

<#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: Vérifiez la résolution DNS et la connectivité HTTPS entre le FTD et les services d'événements 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
```

Actions

L'utilisateur a identifié et résolu un problème interne avec son serveur DNS. Une fois la fonctionnalité DNS restaurée :

- Le FTD a pu résoudre les domaines d'événements Cisco requis.
- Le FTD rétablit automatiquement la connectivité des événements.
- Les journaux des événements de connexion ont repris leur affichage dans cdFMC tel que conçu.

Toutes les actions correctives ont été effectuées par l'utilisateur sans qu'aucune modification de configuration ne soit requise.

Motif

La cause principale était un échec de résolution DNS sur l'interface de gestion FTD, causé spécifiquement par un problème avec le serveur DNS configuré. Comme le FTD n'a pas pu résoudre les domaines d'événements Cisco requis, y compris eventing-ingest.sse.itd.cisco.com, il n'a pas pu établir de connexions d'événements sortantes, ce qui a entraîné la non-transmission des événements de connexion au nuage de sécurité Cisco. Après la restauration de la résolution DNS, l'utilisateur a confirmé que la journalisation des événements de connexion était entièrement opérationnelle et fonctionnait normalement dans l'environnement de production.

Autres informations utiles

- À propos de Secure Firewall Threat Defense et de l'intégration de Cisco XDR
- Assistance technique de Cisco et téléchargements
- Défaut possible au-delà de cet article : Le bogue Cisco CSCwr75332 FTD ne parvient pas à transférer les événements au contrôle du cloud de sécurité

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.