Falha no registro de eventos do FTD do Secure Firewall para CDO/cdFMC devido à resolução do DNS

Problema

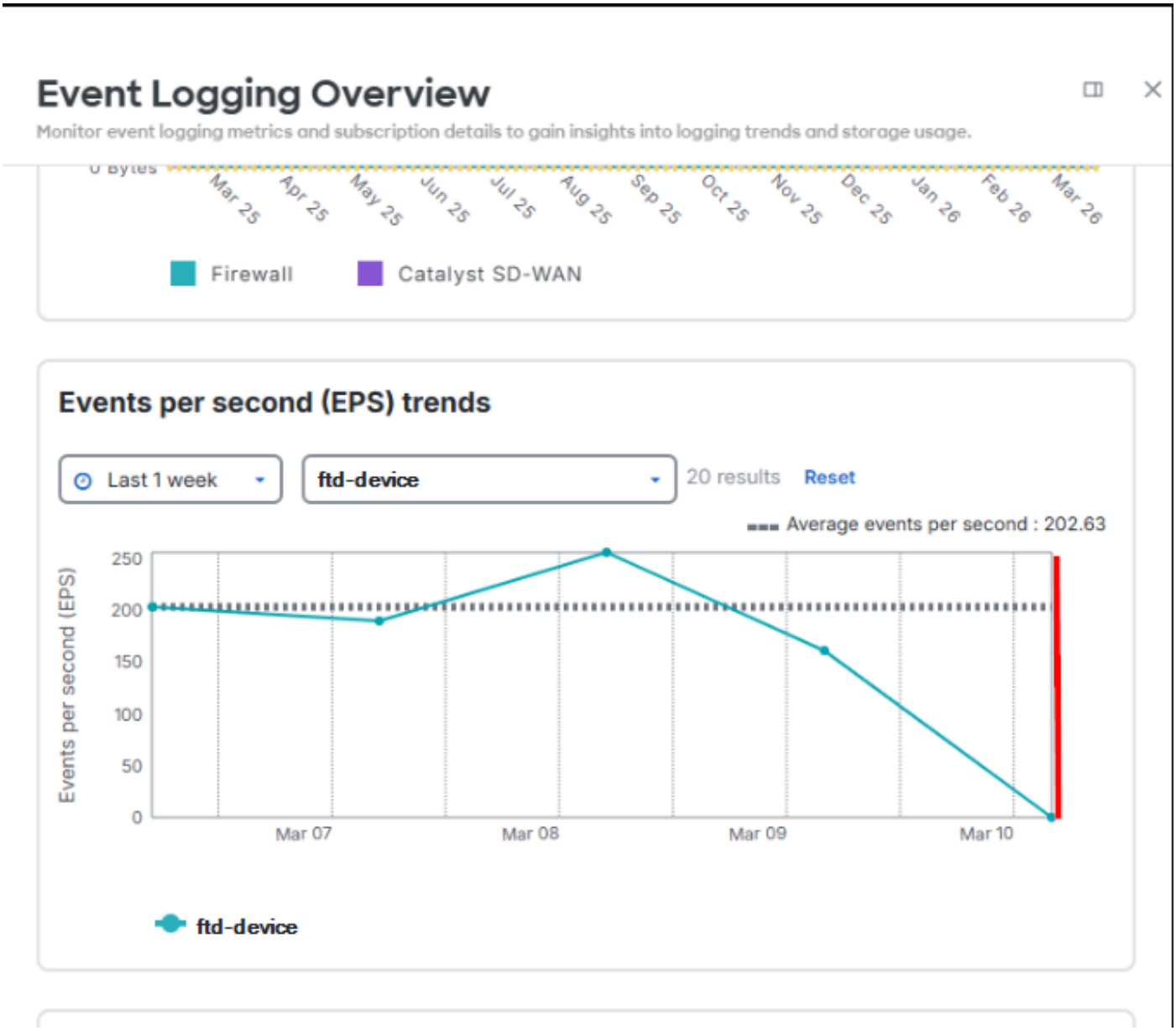
O registro de eventos do Connection parou de aparecer no registro de eventos do Cisco Defense Orchestrator (CDO) e nas páginas de eventos do Firewall Management Center (cdFMC) disponibilizadas na nuvem para um único Firewall Threat Defense (FTD). O dispositivo afetado não conseguiu enviar logs de eventos de conexão para a plataforma de gerenciamento de nuvem, afetando a visibilidade de produção e os recursos de solução de problemas. A análise revelou que o FTD estava enfrentando repetidas falhas de conexão com os serviços de eventos da Cisco devido a falhas temporárias de resolução de nomes, com o carimbo de data/hora das falhas de resolução DNS correlacionando exatamente com o momento em que os eventos de conexão pararam de aparecer nas páginas de eventos.

Ambiente

- FTD do Cisco Secure Firewall gerenciado por CDO com cdFMC
- Servidor DNS configurado na interface de gerenciamento FTD
- Ambiente de produção que requer visibilidade de eventos de conexão para solução de problemas

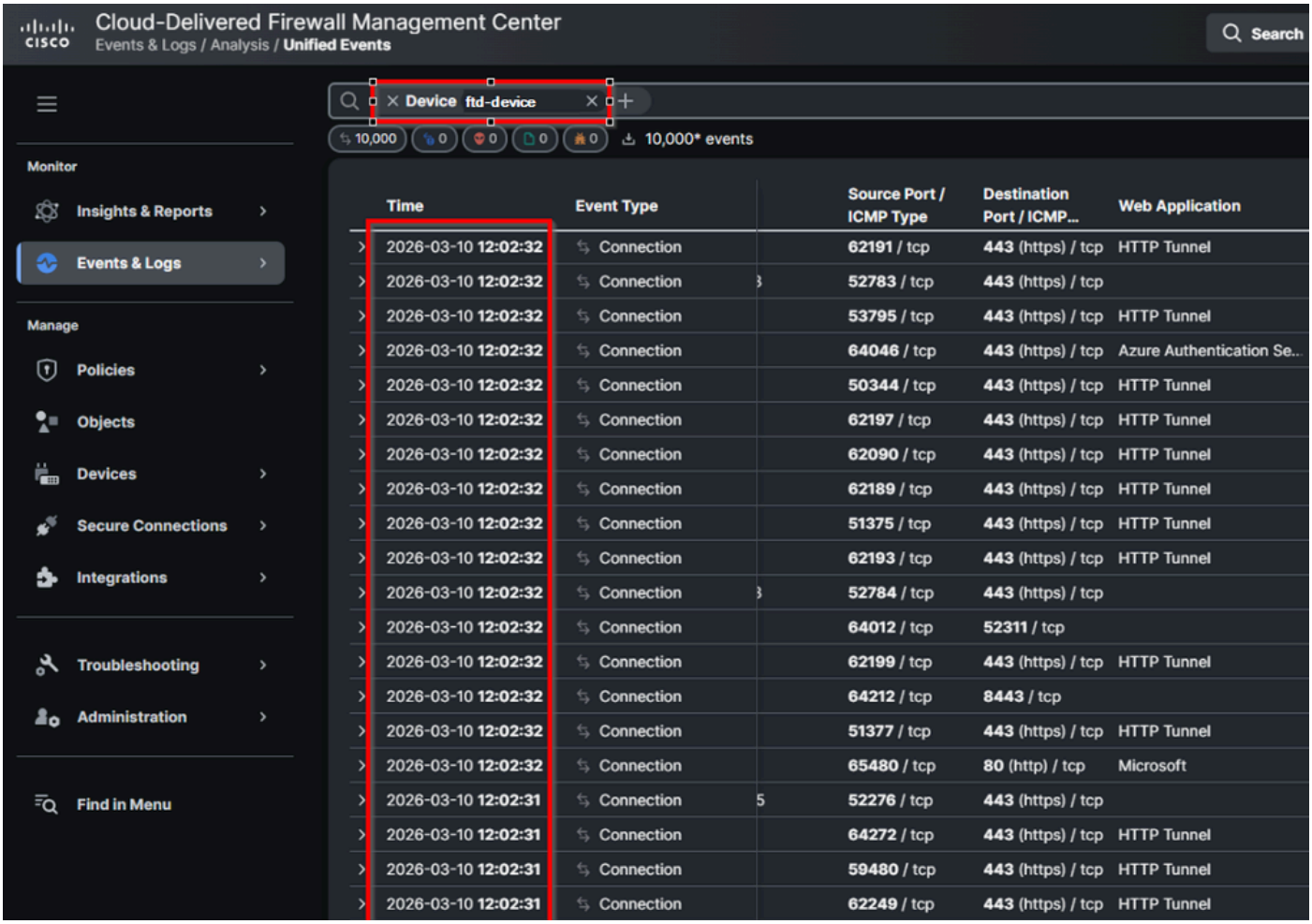
Resolução

1: Revise as páginas CDO Event Logging e cdFMC Unified/Connection Event para determinar o tempo de perda de eventos.



inline_image_0.png

inline_image_0.png



inline_image_1.png

inline_image_1.png

2: Verifique se os processos de FTD necessários estão em execução para permitir a geração e o envio do evento:

<#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 o FTD para localizar os dados de log correlacionados do EventHandler e do Connector que indicam a 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 o servidor DNS configurado dos FTDs e a acessibilidade:

<#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 a resolução DNS e a conectividade HTTPS do FTD para os serviços de eventos da 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
```

Ações

O usuário identificou e resolveu um problema interno com seu servidor DNS. Depois que a funcionalidade DNS for restaurada:

- O FTD conseguiu resolver os domínios de eventos Cisco necessários.
- O FTD restabeleceu automaticamente a conectividade de eventos.
- Os logs de eventos de conexão foram retomados e aparecem no cdFMC conforme designado.

Todas as ações corretivas foram executadas pelo usuário sem a necessidade de alterações na configuração.

Causa

A causa raiz foi uma falha de resolução de DNS na interface de gerenciamento do FTD, causada especificamente por um problema com o servidor DNS configurado. Como o FTD não pôde resolver os domínios de eventos obrigatórios da Cisco, incluindo eventing-ingest.sse.itd.cisco.com, ele não pôde estabelecer conexões de eventos de saída, resultando em eventos de conexão não entregues ao Cisco Security Cloud. Depois que a resolução DNS foi restaurada, o usuário confirmou que o registro de eventos de conexão estava totalmente operacional e funcionando normalmente no ambiente de produção.

Conteúdo relacionado

- Sobre o Secure Firewall Threat Defense e a integração com o Cisco XDR
- Suporte técnico e downloads da Cisco
- Possível defeito além deste artigo: O bug da Cisco ID CSCwr75332 FTD não consegue encaminhar eventos para o controle de segurança em nuvem

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.