由于DNS解析，安全防火墙FTD事件日志记录到CDO/cdFMC失败

问题

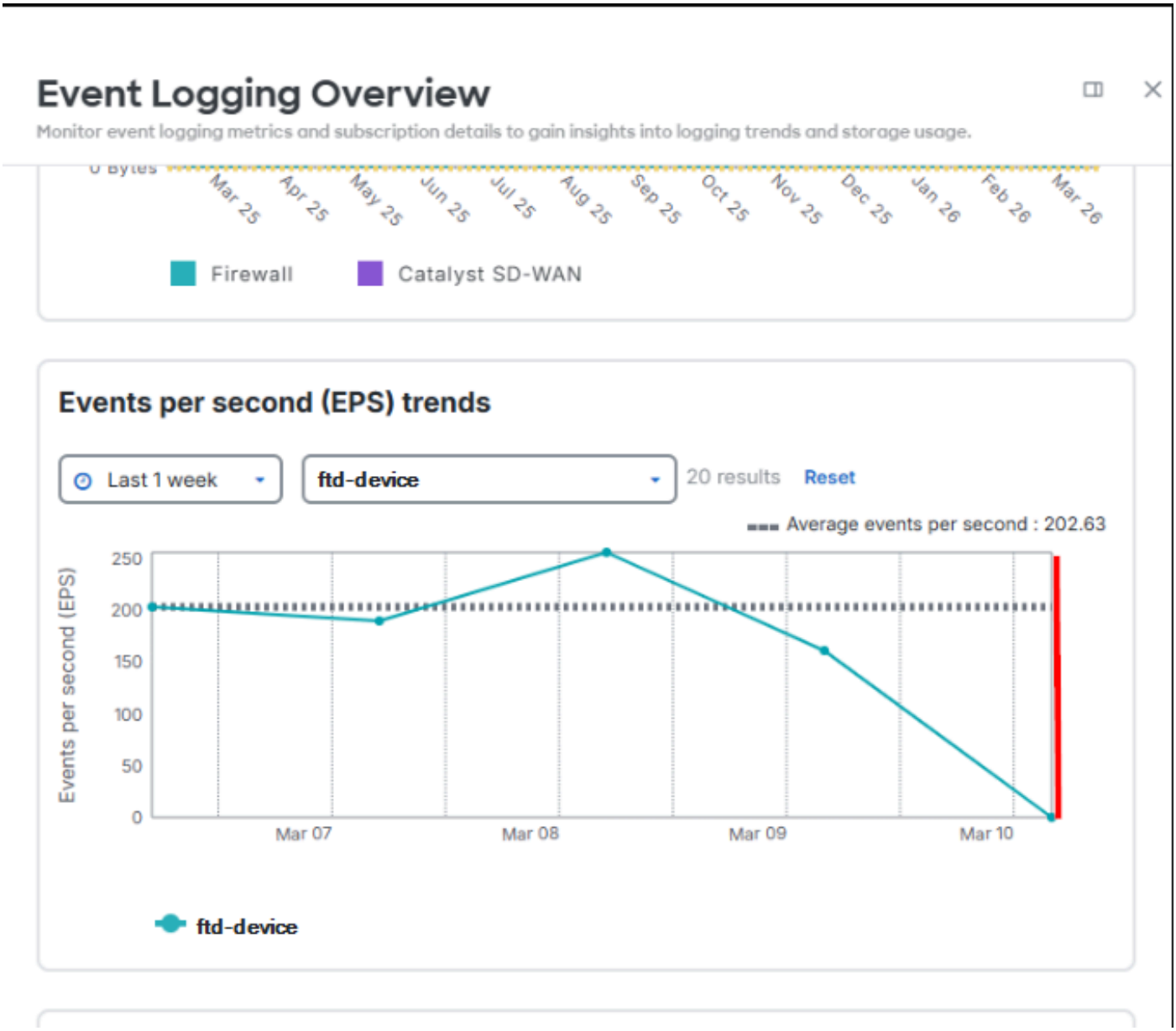
连接事件日志已停止出现在单个防火墙威胁防御(FTD)的Cisco Defense Orchestrator(CDO)事件日志和云交付的防火墙管理中心(cdFMC)事件页面中。 受影响的设备无法将连接事件日志发送到云管理平台，从而影响生产可见性和故障排除功能。分析显示，由于临时名称解析失败，FTD在连接到思科事件服务时反复遇到故障，DNS解析失败的时间戳与事件页面中连接事件停止的时间完全相关。

环境

- 由CDO和cdFMC管理的思科安全防火墙FTD
- 在FTD管理接口上配置的DNS服务器
- 需要连接事件可视性的生产环境以进行故障排除

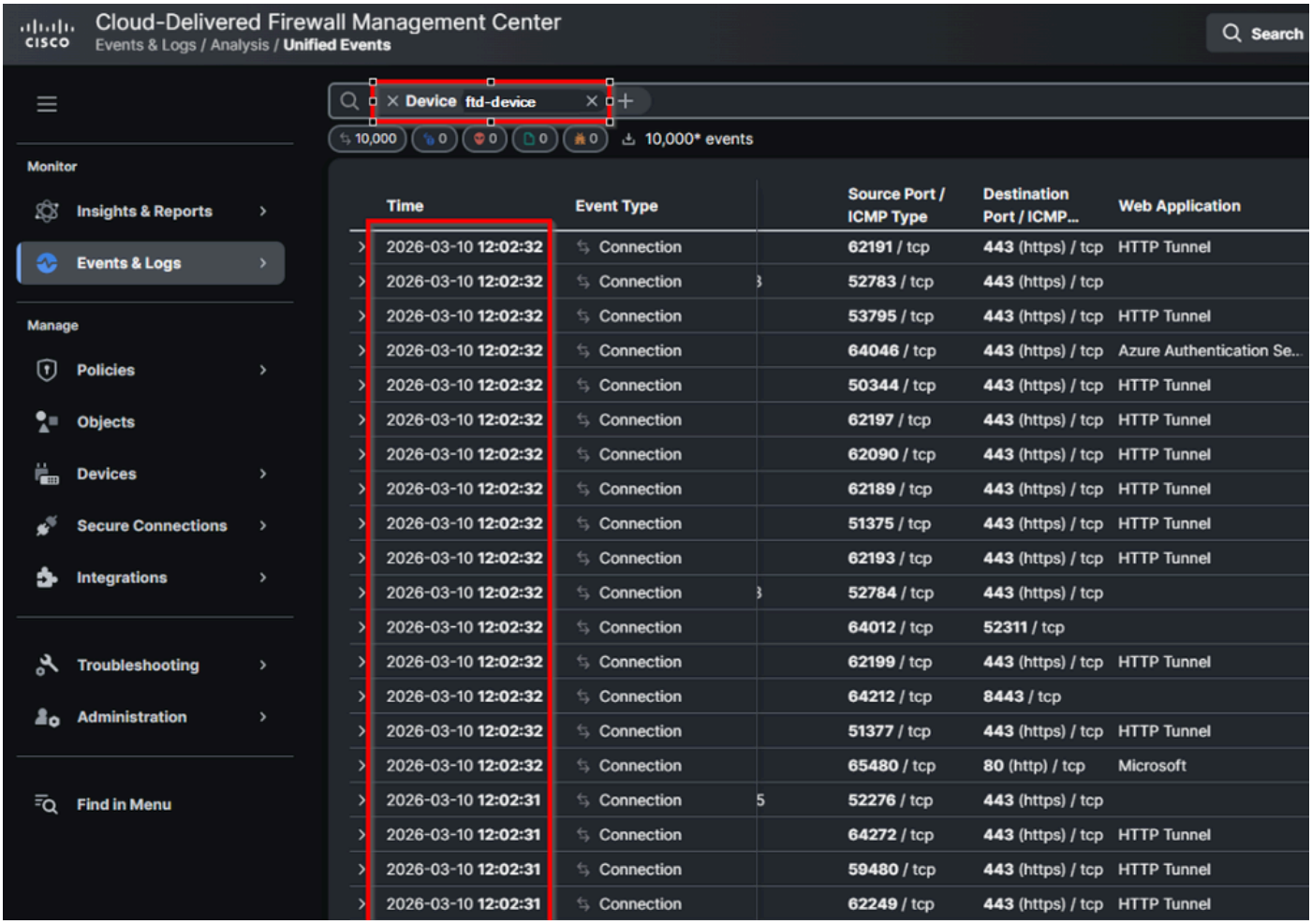
分辨率

1:查看CDO Event Logging（CDO事件记录）和cdFMC Unified/Connection Event（cdFMC统一/连接事件）页面，确定事件丢失的时间。



inline_image_0.png

inline_image_0.png



inline_image_1.png

inline_image_1.png

2:确保必要的FTD进程正在运行，以允许事件生成和发送：

<#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:查看FTD，查找指示原因的相关EventHandler和连接器日志数据：

<#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:验证已配置的FTD的DNS服务器和可达性：

<#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:验证从FTD到Cisco事件服务的DNS解析和HTTPS连接：

```
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
```

操作

用户发现并解决了DNS服务器的一个内部问题。DNS功能恢复后：

- FTD能够解析所需的思科事件域。
- FTD自动重新建立事件连接。
- 连接事件日志继续按设计出现在cdFMC中。

所有纠正操作均由用户执行，无需更改配置。

原因

根本原因是FTD管理接口上的DNS解析故障，特别是由配置的DNS服务器问题引起的。由于FTD无法解析所需的思科事件域，包括eventing-ingest.sse.itd.cisco.com，因此无法建立出站事件连接，导致连接事件无法传送到思科安全云。在DNS解析恢复后，用户确认连接事件日志记录已完全运行并在生产环境中正常运行。

相关内容

- 关于安全防火墙威胁防御和思科XDR集成
- 思科技术支持和下载
- 本文后面可能存在的缺陷：Cisco Bug ID CSCwr75332 FTD无法将事件转发到安全云控制

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。