# DNS解決が原因でCDO/cdFMCへのセキュアファイアウォールFTDイベントロギングが失敗する

## お問い合わせ内容

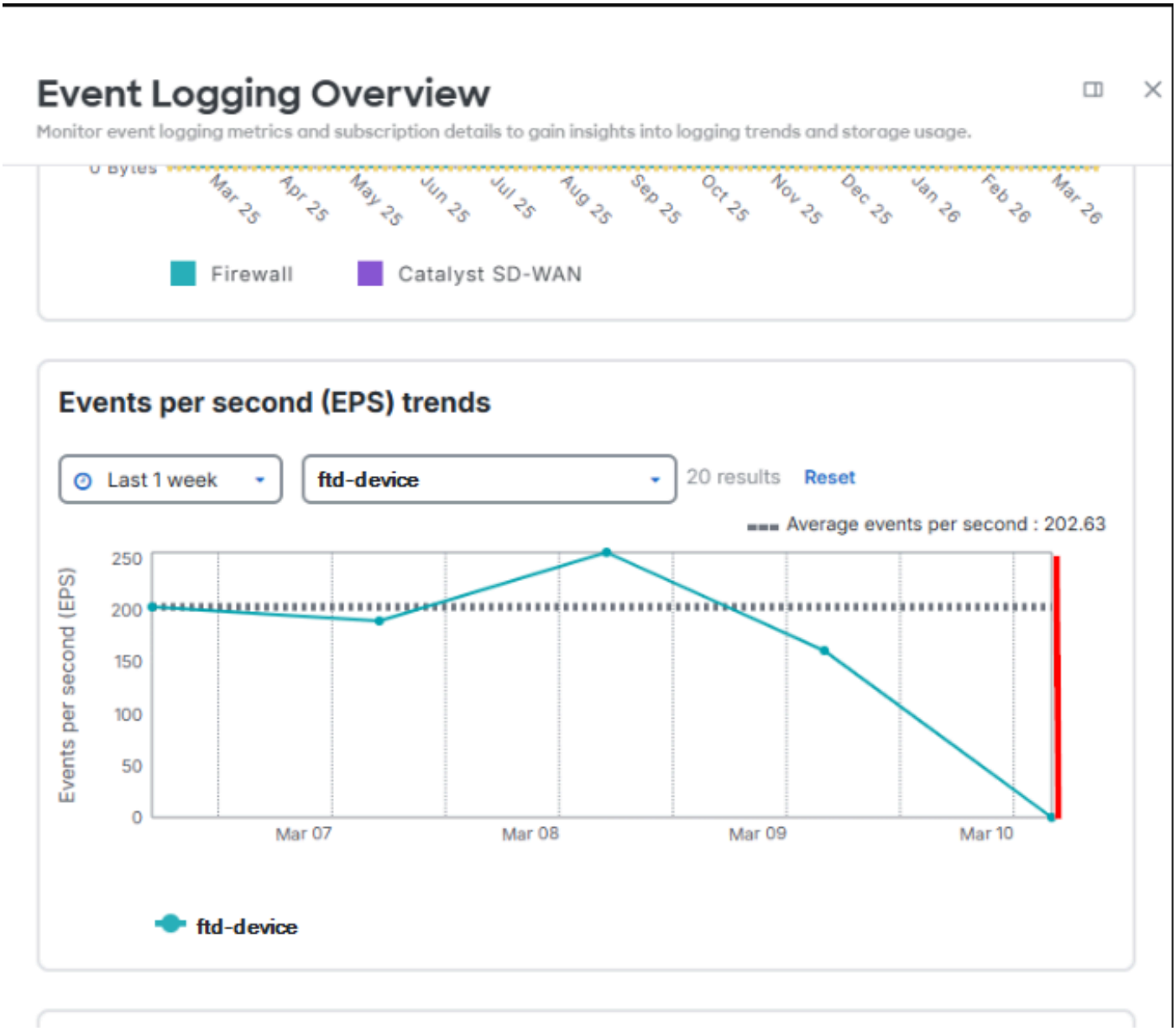
単一のファイアウォール脅威対策(FTD)のCisco Defense Orchestrator(CDO)のEvent Loggingおよびクラウド配信のFirewall Management Center(cdFMC)Eventsページに表示される接続イベントの口ギングが停止しました。 影響を受けるデバイスは、接続イベントログをクラウド管理プラットフォームに送信できなくなり、製品の可視性とトラブルシューティング機能に影響を与えました。分析の結果、FTDで、一時的な名前解決の失敗が原因でCiscoイベントサービスへの接続の失敗が繰り返されていることが判明しました。DNS解決失敗のタイムスタンプは、接続イベントがイベントページに表示されなくなったときと正確に相関しています。

## 環境

- cdFMCを使用したCDOによって管理されるCisco Secure Firewall FTD
- FTD管理インターフェイスで設定されたDNSサーバ
- トラブルシューティングのために接続イベントの可視性を必要とする実稼働環境

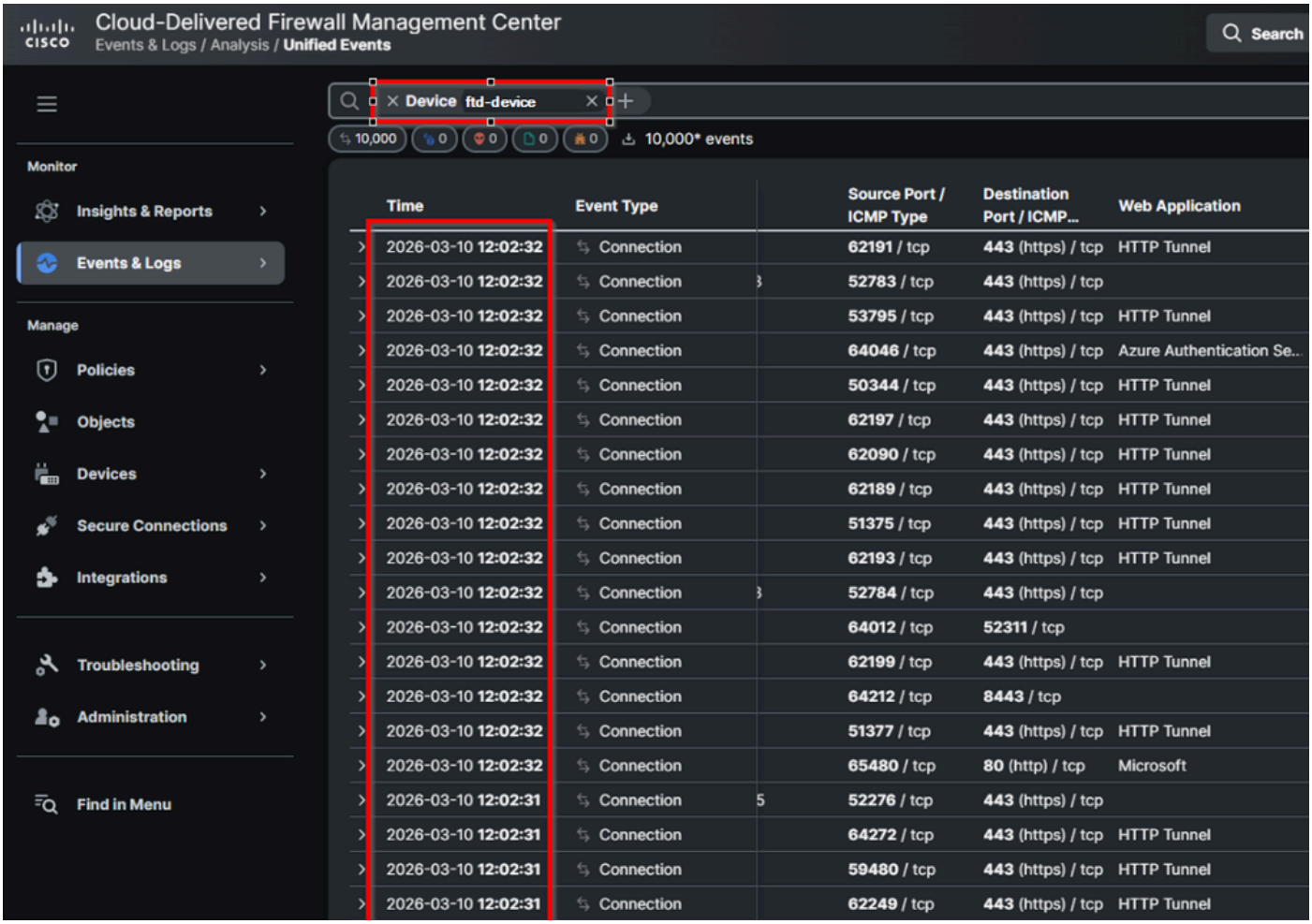
## 解決策

1: CDO Event LoggingおよびcdFMC Unified/Connection Eventページを確認して、イベント損失の時間を判断します。




inline_image_0.png ( インラインイメージ_0.png )

inline_image_0.png ( インラインイメージ_0.png )




inline_image_1.pngファイル

inline_image_1.pngファイル

2：イベントの生成と送信を許可するために必要なFTDプロセスが実行されていることを確認します。

<#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:FTDを確認し、原因を示す関連するEventHandlerおよびConnectorの口グデータを見つけます。

<#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, "Ou
---
/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:FTDの設定済みDNSサーバと到達可能性を確認します。

<#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:FTDからCiscoイベントサービスへのDNS解決およびHTTPS接続を確認します。

```
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
```

## [アクション（Actions）]

ユーザは、DNSサーバの内部の問題を特定し、解決しました。DNS機能が復元された後：

- FTDは、必要なシスコのイベントドメインを解決できました。
- FTDはイベント接続を自動的に再確立しました。
- 設計どおりに、接続イベントログがcdFMCに表示され始めました。

すべての修正操作は、設定の変更なしでユーザが実行しました。

## 原因

根本的な原因は、FTD管理インターフェイスでのDNS解決の失敗で、特に設定されているDNSサーバの問題が原因です。FTDがeventing-ingest.sse.itd.cisco.comを含む必要なシスコイベントドメインを解決できなかったため、発信イベントコネクションを確立できず、その結果、接続イベントがCisco Security Cloudに配信されません。DNS解決が復元された後、ユーザは接続イベントのロギングが完全に動作しており、実稼働環境で正常に機能していることを確認しました。

## 関連コンテンツ

- セキュアファイアウォール脅威対策とCisco XDRの統合について
- シスコのテクニカルサポートとダウンロード
- この記事の先にある考えられる不具合:Cisco Bug ID CSCwr75332 FTDがSecurity Cloud Controlにイベントを転送できない

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。