# فشل تسجيل حدث FTD الآمن الخاص بجدار الحماية إلى CDO/CDfmc بسبب دقة DNS

## مسألة

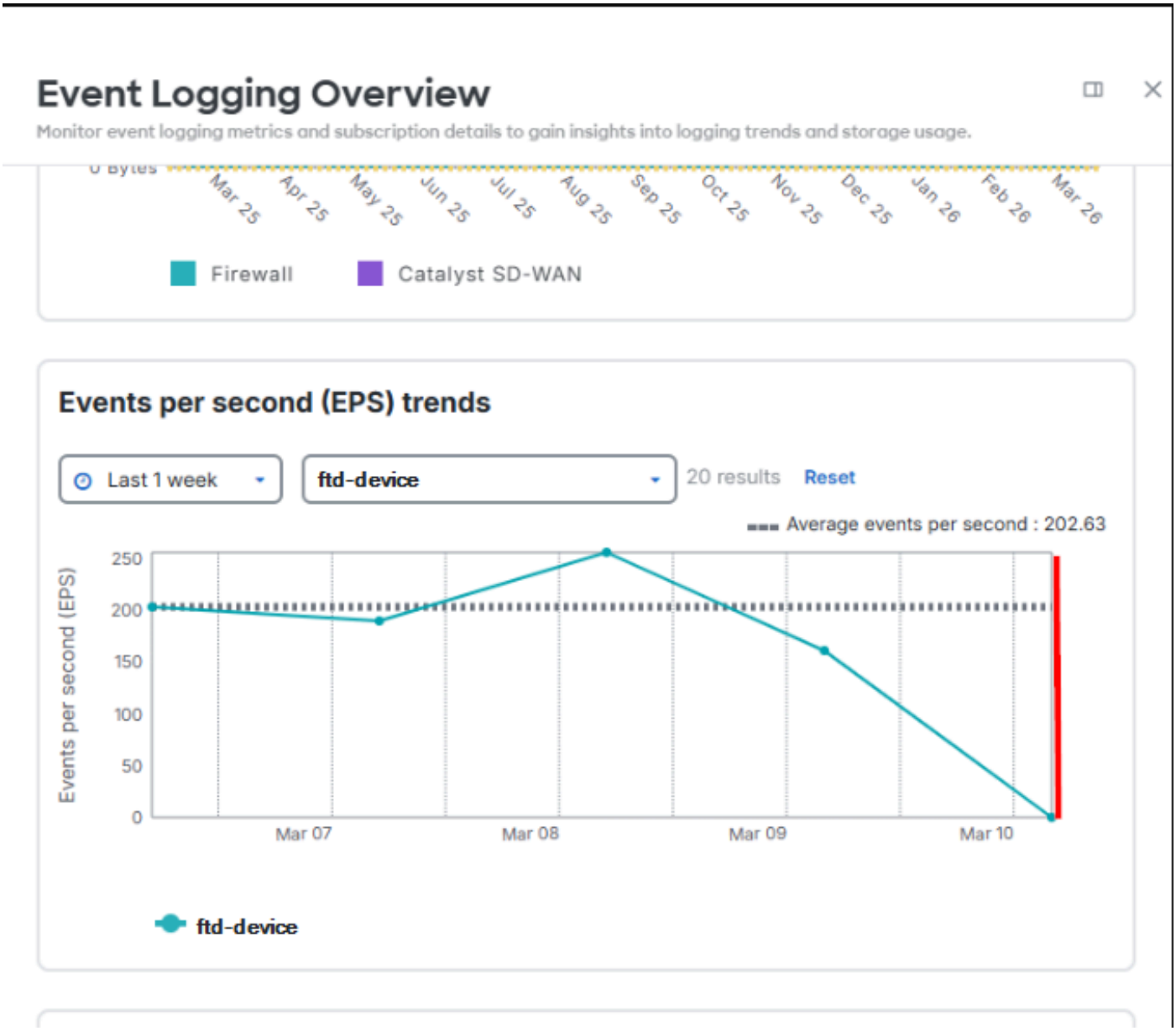
توقف تسجيل أحداث الاتصال عن الظهور في صفحات أحداث مركز إدارة جدار الحماية (CDfmc) الذي يتم تسليمه عبر السحابة لتسجيل أحداث Cisco Defense Orchestrator (CDO) للحصول على دفاع واحد ضد تهديد جدار الحماية (FTD). تعذر على الجهاز المتأثر إرسال سجلات أحداث الاتصال إلى النظام الأساسي لإدارة السحابة، مما يؤثر على إمكانية رؤية الإنتاج وإمكانات أستكشاف الأخطاء وإصلاحها. كشف التحليل عن أن FTD كان يواجه حالات فشل متكررة للاتصال بخدمات تصحيح الأخطاء من Cisco بسبب فشل تحليل الاسم المؤقت، مع ربط الطابع الزمني لفشل تحليل DNS تماما مع الوقت الذي توقفت فيه أحداث الاتصال عن الظهور في الصفحات.

## البيئة

- CDfmc باستخدام CDO بواسطة إدارته تتم Cisco Secure Firewall FTD
- FTD إدارة واجهة في تكوينه تم الذي DNS خادم
- بيئة الإنتاج التي تتطلب رؤية حدث الاتصال لاستكشاف الأخطاء وإصلاحها

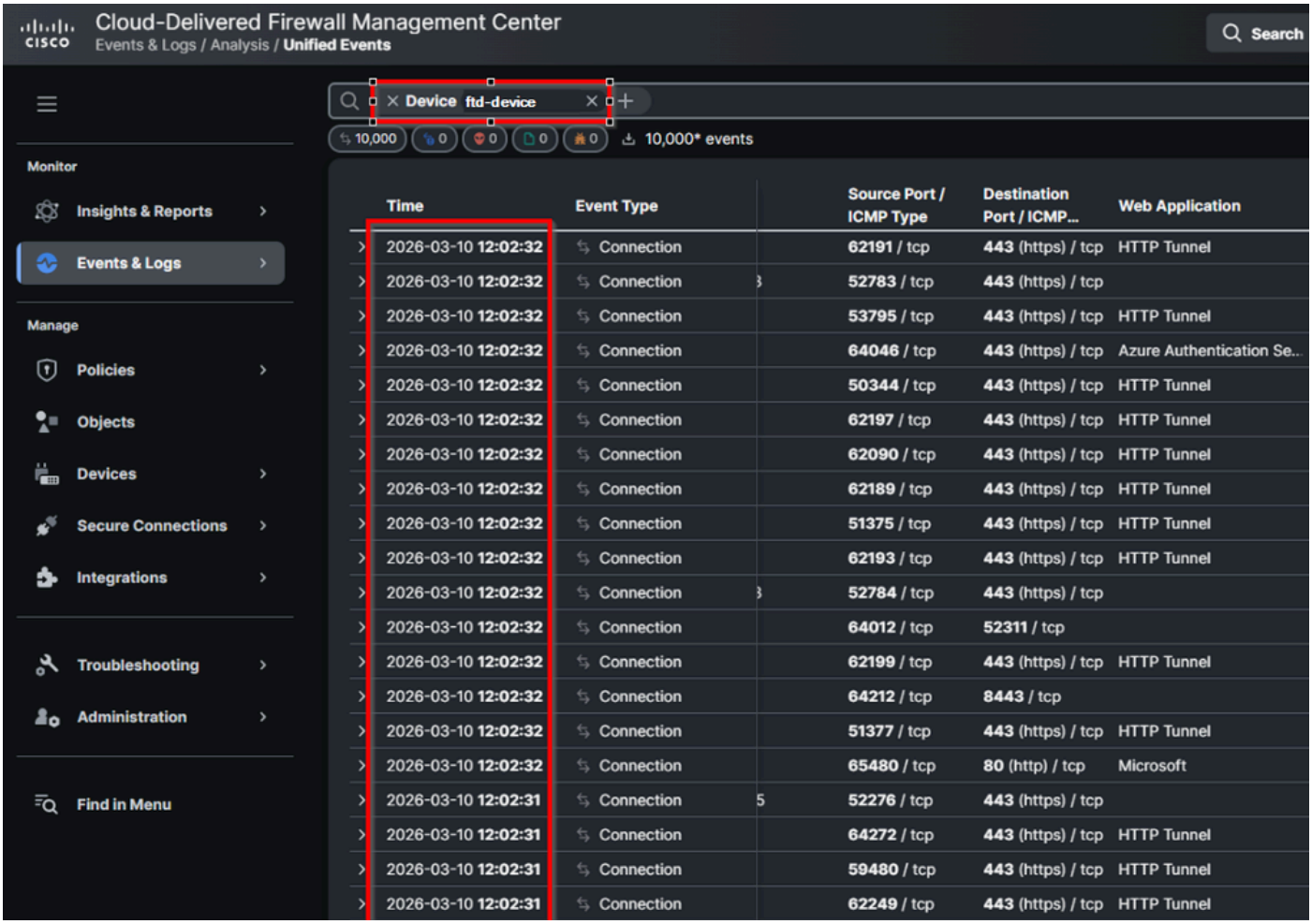
## قرار

1: راجع صفحات تسجيل أحداث CDO و CDfmc Unified/Connection Event لتحديد وقت التحقق من الخسارة.




inline_image_0.png

inline_image_0.png




inline_image_1.png

inline_image_1.png

2: تأكد من أن عمليات "برنامج الإرسال فائق السرعة (FTD)" اللازمة قيد التشغيل للسماح بإنشاء الحدث وإرساله:

<#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: راجع FTD للعثور على بيانات سجل الأحداث المرتبطة و الموصل التي تشير إلى السبب:

```
<#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: التحقق من خادم DNS الذي تم تكوينه لـ FTDs وإمكانية الوصول إليه:

```
<#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: تحقق من دقة DNS واتصال HTTPS من FTD إلى خدمات تصحيح 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
```

## الإجراءات

قام المستخدم بتعريف مشكلة داخلية وحلها مع خادم DNS الخاص به. بمجرد إستعادة وظيفة DNS:

- إستطاع FTD حل مجالات تصفية Cisco المطلوبة.
- أعاد "برنامج الإرسال فائق السرعة (FTD)" إنشاء الاتصال تلقائيا.
- تم إستئناف تشغيل سجلات أحداث الاتصال في CDfmc كما تم تصميمها.

تم تنفيذ كافة الإجراءات التصحيحية بواسطة المستخدم دون الحاجة إلى تغييرات في التكوين.

## السبب

كان السبب الجذري هو فشل تحليل DNS على واجهة إدارة FTD، والذي نتج تحديدا عن مشكلة مع خادم DNS الذي تم تكوينه. لأن FTD تعذر عليه حل مجالات تصفية Cisco المطلوبة، بما في ذلك eventing-ingest.sse.itd.cisco.com، تعذر عليه إنشاء إتصالات تصحيح صادرة، مما أدى إلى عدم تسليم أحداث الاتصال إلى سحابة أمان Cisco. بعد إستعادة تحليل DNS، أكد المستخدم أن تسجيل حدث الاتصال كان قيد التشغيل الكامل وأنه يعمل بشكل طبيعي في بيئة الإنتاج.

## المحتوى ذي الصلة

- حول الدفاع الآمن عن تهديد جدار الحماية وتكامل Cisco XDR
- الدعم الفني والتنزيلات من Cisco
- CSCwr75332 عيب محتمل يتجاوز هذه المقالة: في فشل معرف تصحيح الأخطاء من Cisco إعادة توجيه الأحداث إلى التحكم في سحابة الأمان FTD

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).