تكوين الأجهزة لإرسال رسائل الدخول إلى النظام الخاصة باستكشاف الأخطاء وإصلاحها وعرضها على FMC

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين الأجهزة المدارة لإرسال رسائل syslog التشخيصية إلى FMC وعرضها في عارض الأحداث الموحد.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:
· رسائل Syslog
•مركز إدارة Firepower (FMC)
•Firepower Threat Defense (FTD)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:
· ينطبق هذا المستند على جميع الأنظمة الأساسية Firepower.
· برنامج الدفاع الظاهري ضد تهديدات جدار الحماية الآمن (FTD) الذي يعمل ببرنامج الإصدار 7.6.0
· تطبيق Secure Firewall Management Center Virtual (FMC) الذي يشغل الإصدار 7.6.0 من البرنامج
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

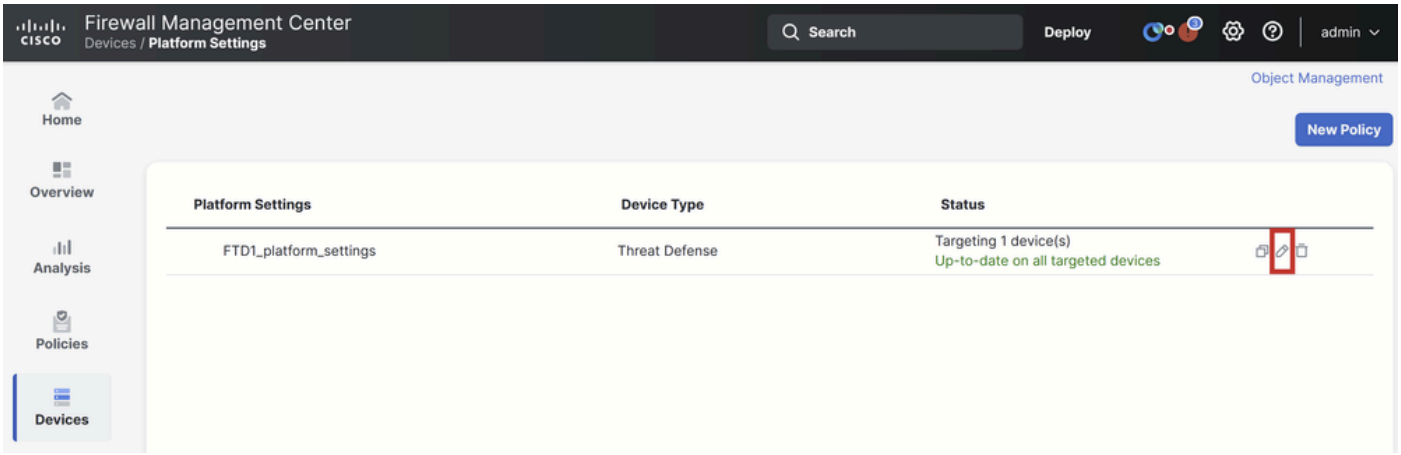
نظرة عامة على الميزة

في "جدار الحماية الآمن"، تتم إضافة نوع حدث جديد لاستكشاف الأخطاء وإصلاحها" في جدول "عارض الأحداث الموحدة". تم توسيع تكوين تسجيل إعدادات النظام الأساسي وهو يدعم إرسال رسائل syslog التشخيصية التي تم إنشاؤها بواسطة LINA إلى FMC بدلا من سجلات VPN فقط. يمكن تكوين هذه الميزة على أي FTD يشغل إصدار برنامج متوافق مع FMC 7.6.0. لا يتم دعم CDfmc لأن CDfmc لا يحتوي على أدوات تحليلات.

- يقتصر خيار جميع السجلات على الطوارئ والتنبيه ومستويات السجلات الحرجة بسبب حجم الحدث.
- تظهر سجلات أستكشاف الأخطاء وإصلاحها هذه أي syslog يتم إرسالها من الجهاز إلى FMC (VPN أو آخر).
- تتدفق سجلات أستكشاف الأخطاء وإصلاحها إلى وحدة التحكم في إدارة الشبكة (FMC) وتكون مرئية في عرض الحدث الموحد وتحت الأجهزة > أستكشاف الأخطاء وإصلاحها > سجلات أستكشاف الأخطاء وإصلاحها.

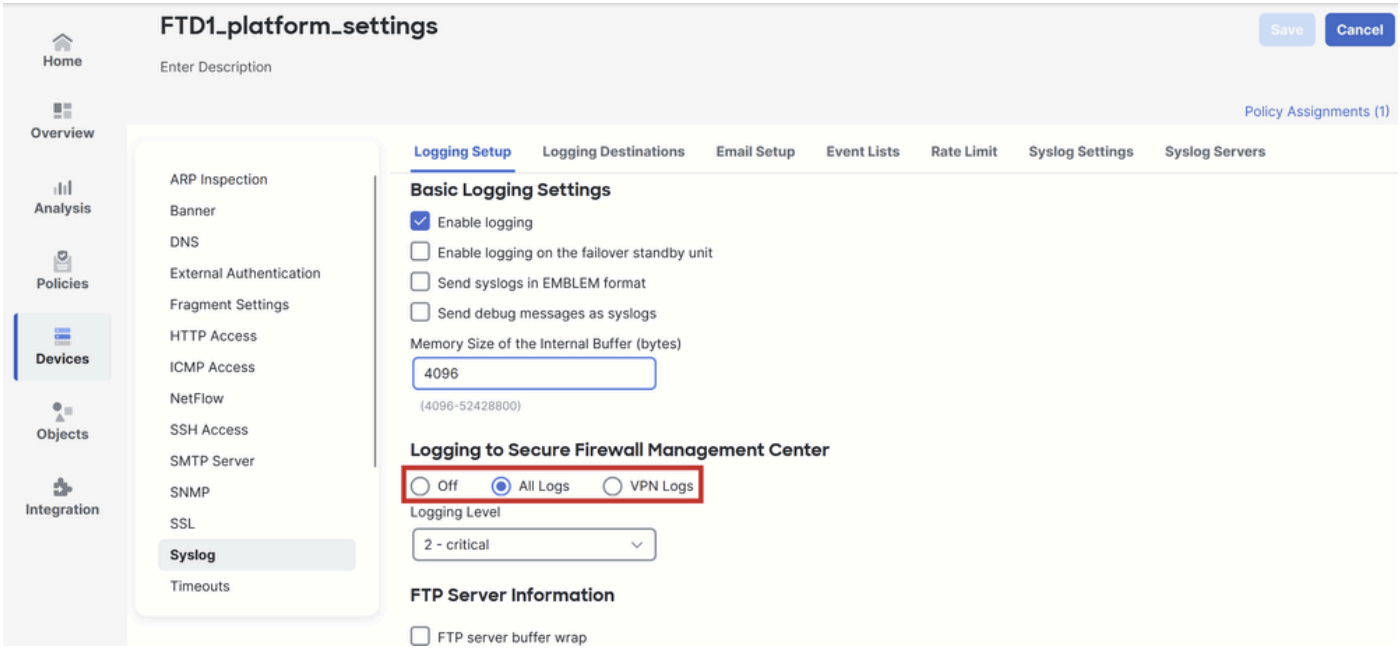
التكوين

انتقل إلى أجهزة FMC > إعدادات النظام الأساسي وانقر فوق أيقونة تحرير في الركن العلوي الأيمن من السياسة.



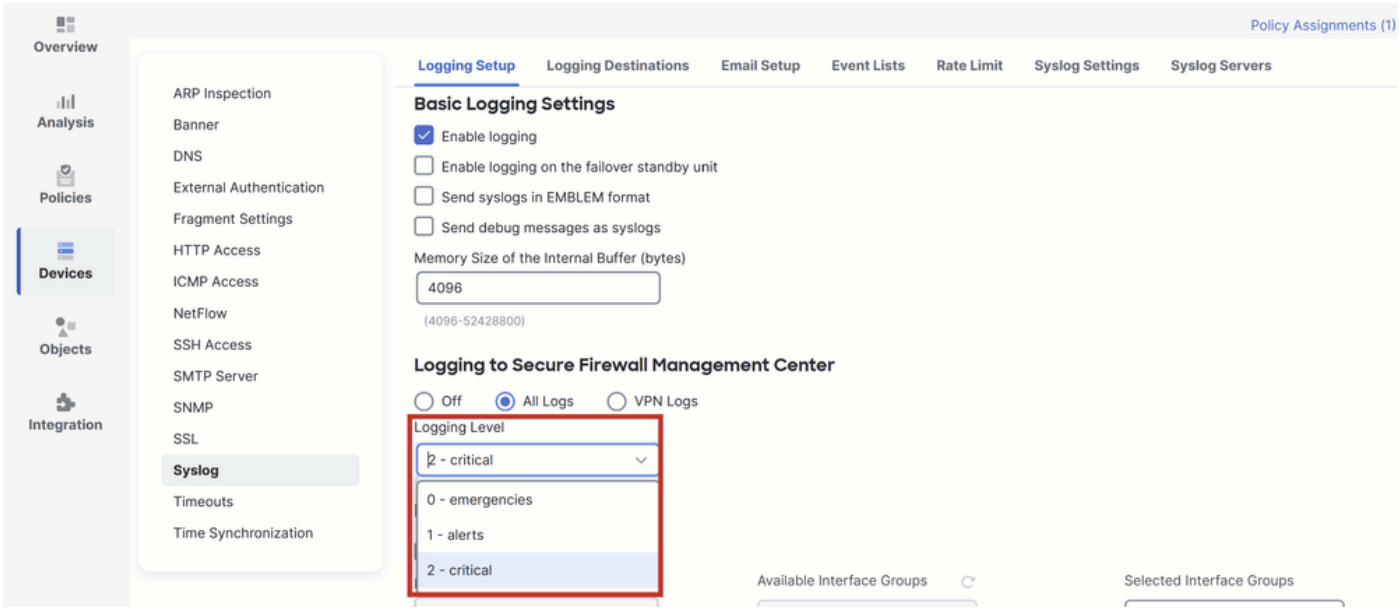
نهج إعدادات النظام الأساسي

انتقل إلى Syslog > إعداد التسجيل. يمكنك مشاهدة ثلاثة خيارات أسفل التسجيل إلى مركز إدارة جدار الحماية الآمن.



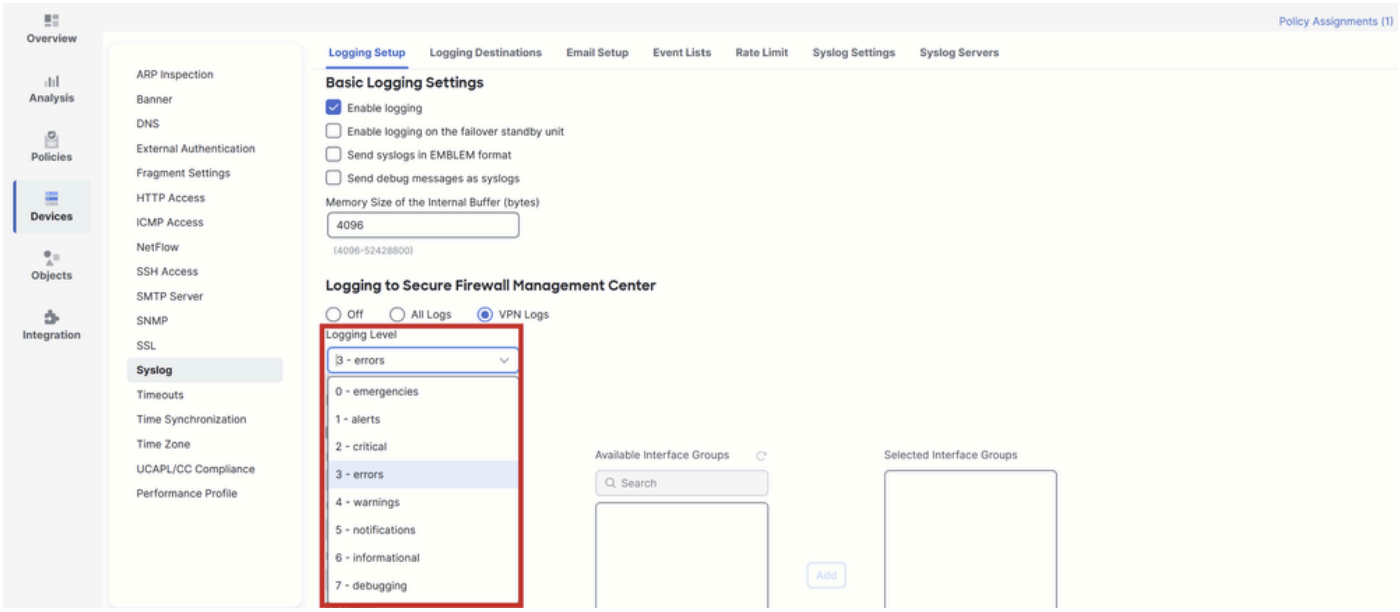
ثلاثة خيارات للتسجيل

إذا قمت باختيار جميع السجلات، فيمكنك تحديد أي من مستويات التسجيل الثلاثة المتوفرة: حالات الطوارئ والتنبيهات ورسائل syslog التشخيصية وإرسالها إلى FMC (بما في ذلك VPN).

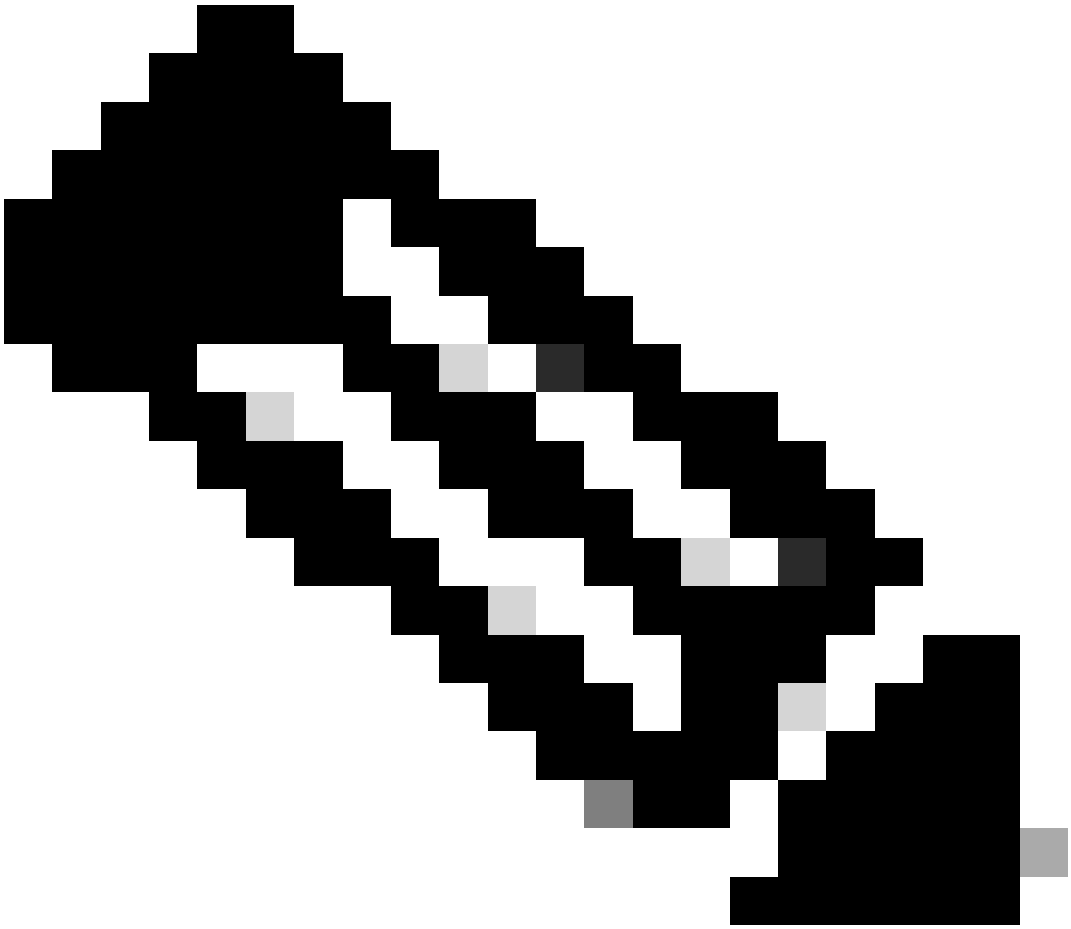


مستويات التسجيل المتاحة

إذا قمت باختيار سجلات الشبكة الخاصة الظاهرية (VPN)، فستتوفر جميع مستويات التسجيل ويمكن تحديد أحد هذه المستويات.



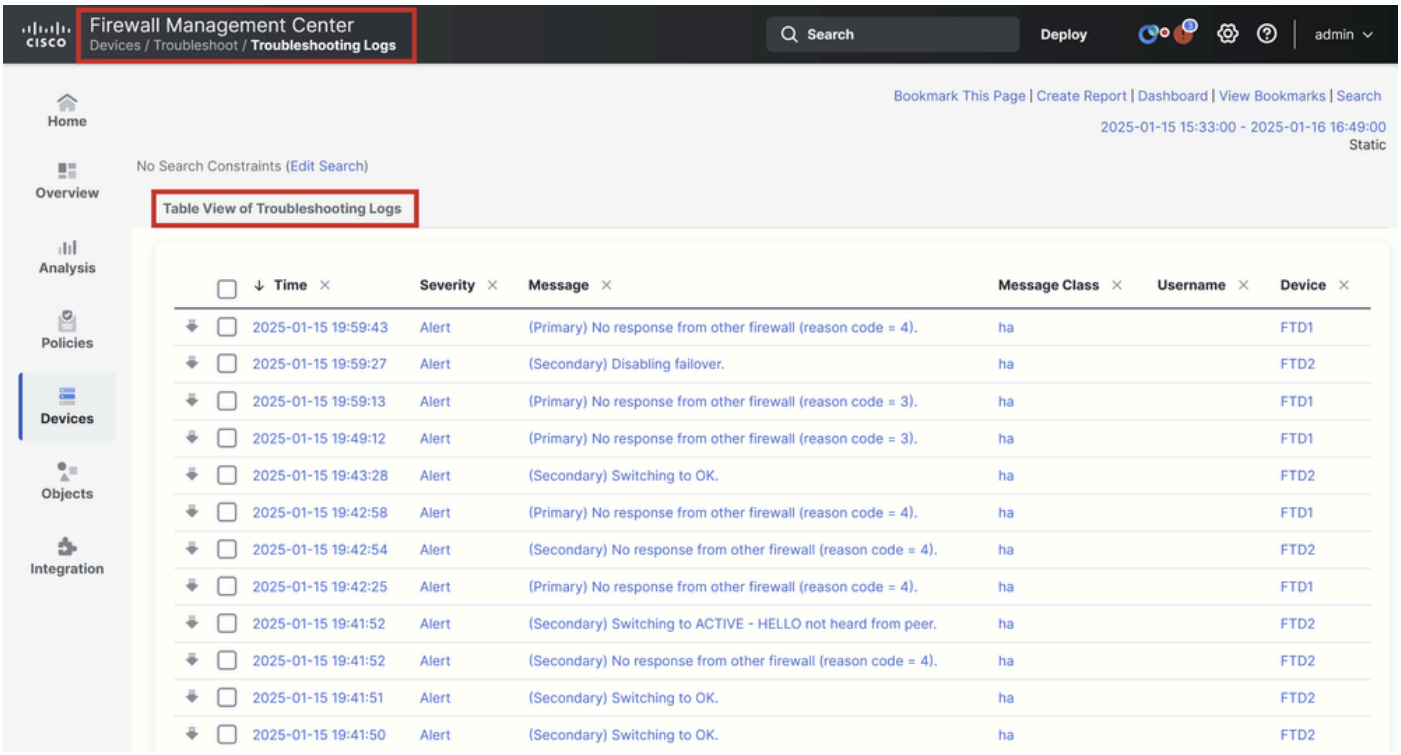
مستويات التسجيل المتاحة



ملاحظة: عندما تقوم بتكوين جهاز باستخدام شبكة VPN للوصول إلى موقع إلى

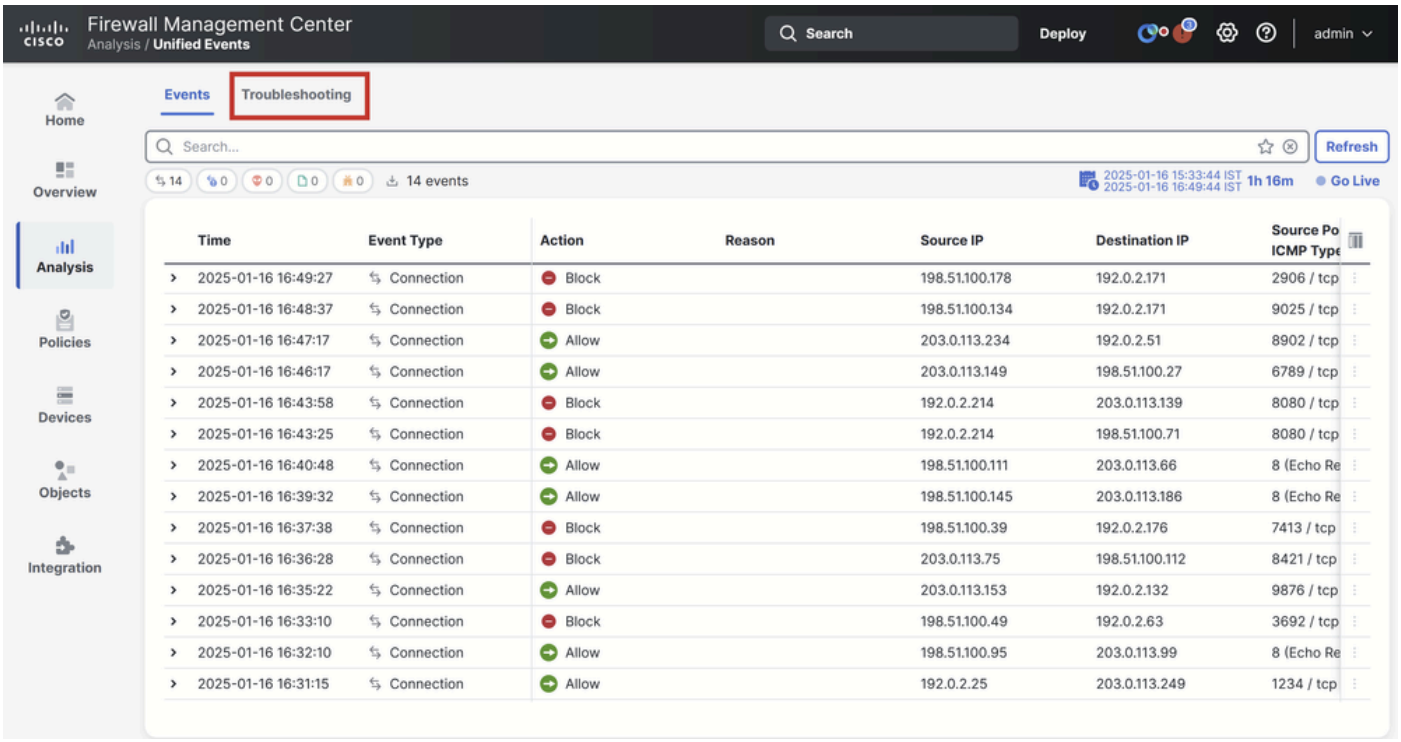
موقع أو وصول عن بعد، فإنه يقوم تلقائيا بتمكين إرسال حزم VPN إلى مركز الإدارة بشكل افتراضي. أنت يستطيع غيرت وه إلى كل سجل أن يرسل كل syslog بجانب VPN سجل إلى FMC.

يمكن الوصول إلى هذه السجلات من الأجهزة > أستكشاف الأخطاء وإصلاحها > سجلات أستكشاف الأخطاء وإصلاحها.



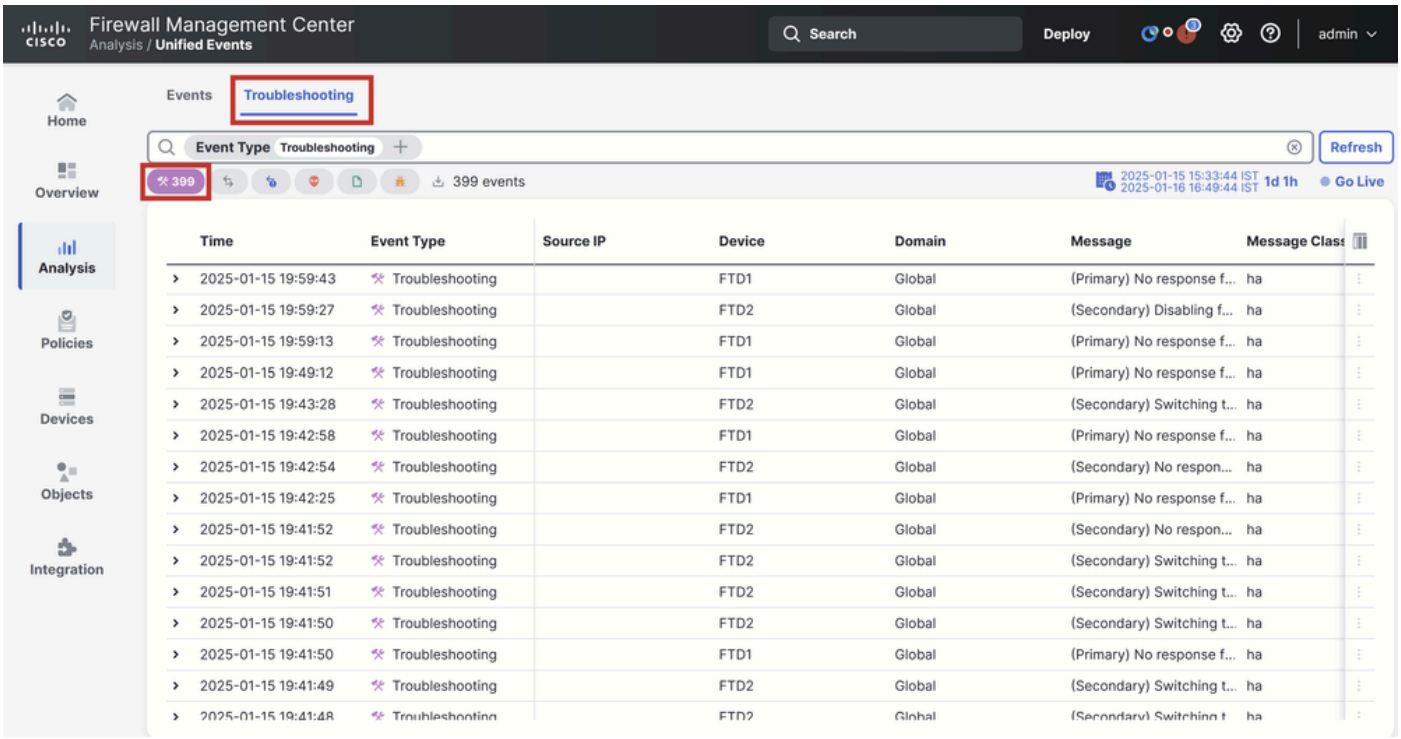
عرض الجدول لسجلات أستكشاف الأخطاء وإصلاحها

تتوفر الآن علامة تبويب عرض جديدة لاستكشاف الأخطاء وإصلاحها في صفحة عارض الأحداث الموحدة. لعرض هذه الأحداث، انتقل إلى Analysis (تحليل) > Unified Events (أحداث موحدة) > Troubleshooting (أستكشاف الأخطاء وإصلاحها).



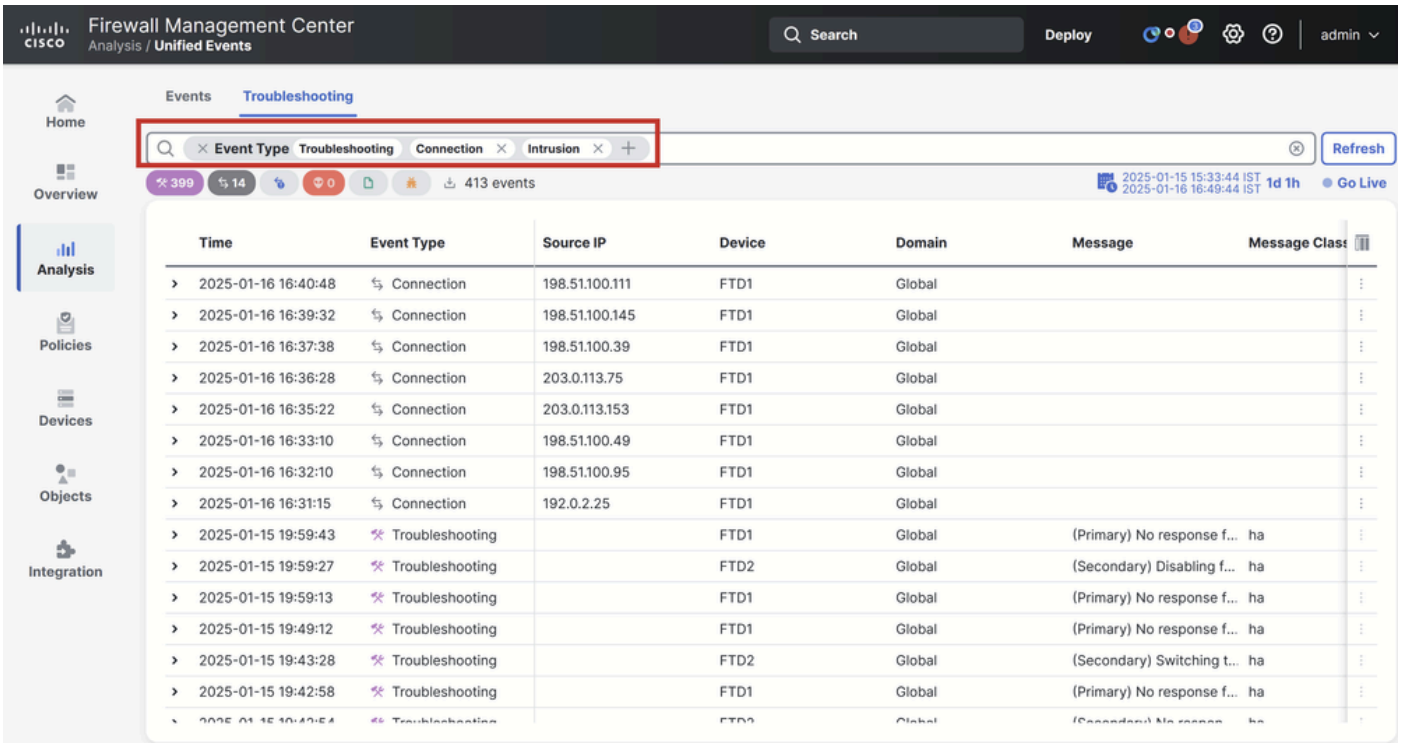
طريقة عرض أستكشاف الأخطاء وإصلاحها

يكون نوع حدث جديد مرئيا داخل الجدول بمجرد التبديل إلى علامة التبويب هذه. ال يمكن إضافتها أو إزالتها من طريقة العرض مثل الأنواع الأخرى لأنها أساسية لطريقة عرض أستكشاف الأخطاء وإصلاحها.



نوع حدث أستكشاف الأخطاء وإصلاحها

ال يزال من الممكن إضافة أنواع أحداث أخرى وإزالتها من طريقة عرض "أستكشاف الأخطاء وإصلاحها" هذه. وهذا يتيح لك عرض سجلات التشخيص جنبا إلى جنب مع بيانات الحدث الأخرى.



أنواع أحداث أخرى

التحقق من التكوين

بمجرد تنفيذ التكوين من واجهة المستخدم الرسومية (GUI) لـ FMC، يمكن التحقق من صحته من واجهة سطر الأوامر (CLI) لـ FTD من خلال تشغيل الأوامر show running-config logging وshow logging في وضع CLISH أو LINA.

```
FTD1# show running-config logging
logging enable
logging timestamp
logging list MANAGER_ALL_SYSLOG_EVENT_LIST level critical
logging buffered errors
logging FMC MANAGER_ALL_SYSLOG_EVENT_LIST
logging device-id hostname
logging permit-hostdown
no logging message 106015
no logging message 313001
no logging message 313008
no logging message 106023
no logging message 710003
no logging message 302015
no logging message 302014
no logging message 302013
no logging message 302018
no logging message 302017
no logging message 302016
no logging message 302021
no logging message 302020
```

رمأ CLI ل FTD

```
FTD1# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Timezone: disabled
    Logging Format: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level errors, 45 messages logged
    Trap logging: disabled
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: hostname "FTD1"
    Mail logging: disabled
    ASDM logging: disabled
    FMC logging: list MANAGER_ALL_SYSLOG_EVENT_LIST, 45 messages logged
```

رمأ CLI ل 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).