配置设备以发送和查看FMC上的系统日志故障排除

目录

简介

本文档介绍如何配置受管设备以将诊断系统日志消息发送到FMC并在统一事件查看器中查看这些消息。

先决条件

要求

Cisco 建议您了解以下主题：
·系统日志消息
•Firepower Management Center (FMC)
•Firepower Threat Defense (FTD)

使用的组件

本文档中的信息基于以下软件和硬件版本：
·本文档适用于所有Firepower平台。
·运行软件版本7.6.0的安全防火墙威胁防御虚拟(FTD)
·运行软件版本7.6.0的安全防火墙管理中心虚拟(FMC)
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

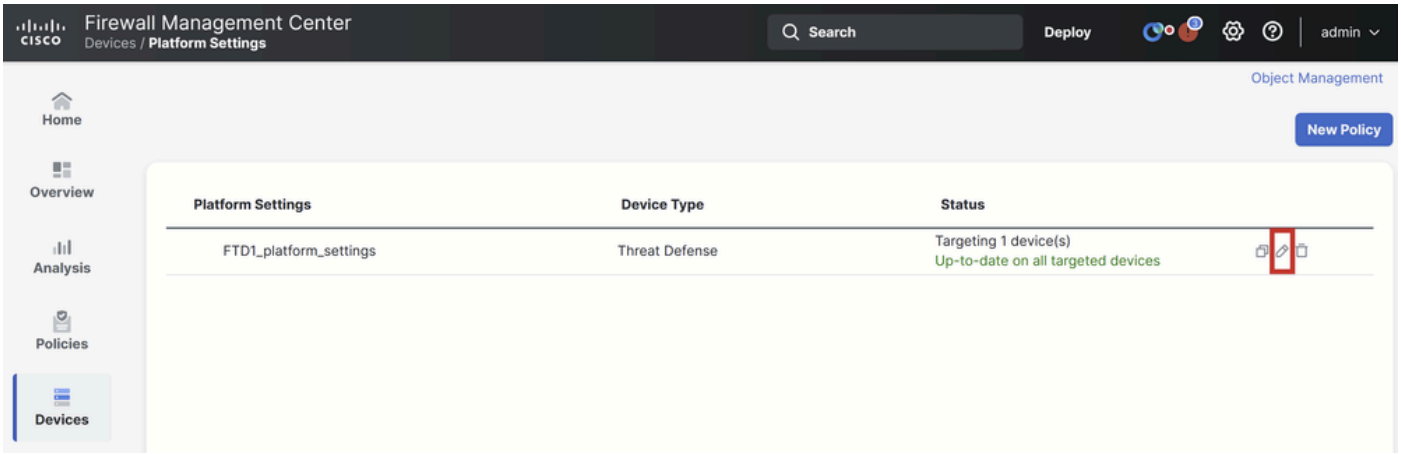
功能概述

在Secure Firewall 7.6中，新的Troubleshoot事件类型被添加到Unified Event Viewer表中。平台设置syslog日志记录配置已扩展，它支持将LINA生成的诊断系统日志消息发送到FMC，而不仅仅是VPN日志。此功能可在运行与FMC 7.6.0兼容的软件版本的任何FTD上配置。由于cdFMC没有分析工具，因此不支持cdFMC。

- 由于存在事件量，“所有日志”选项限制为紧急、警报和严重日志级别。
- 这些故障排除日志显示从设备发送到FMC（VPN或其他）的任何系统日志。
- 故障排除日志流向FMC，并且在Unified Event View中和Devices > Troubleshoot > Troubleshooting Logs下可见。

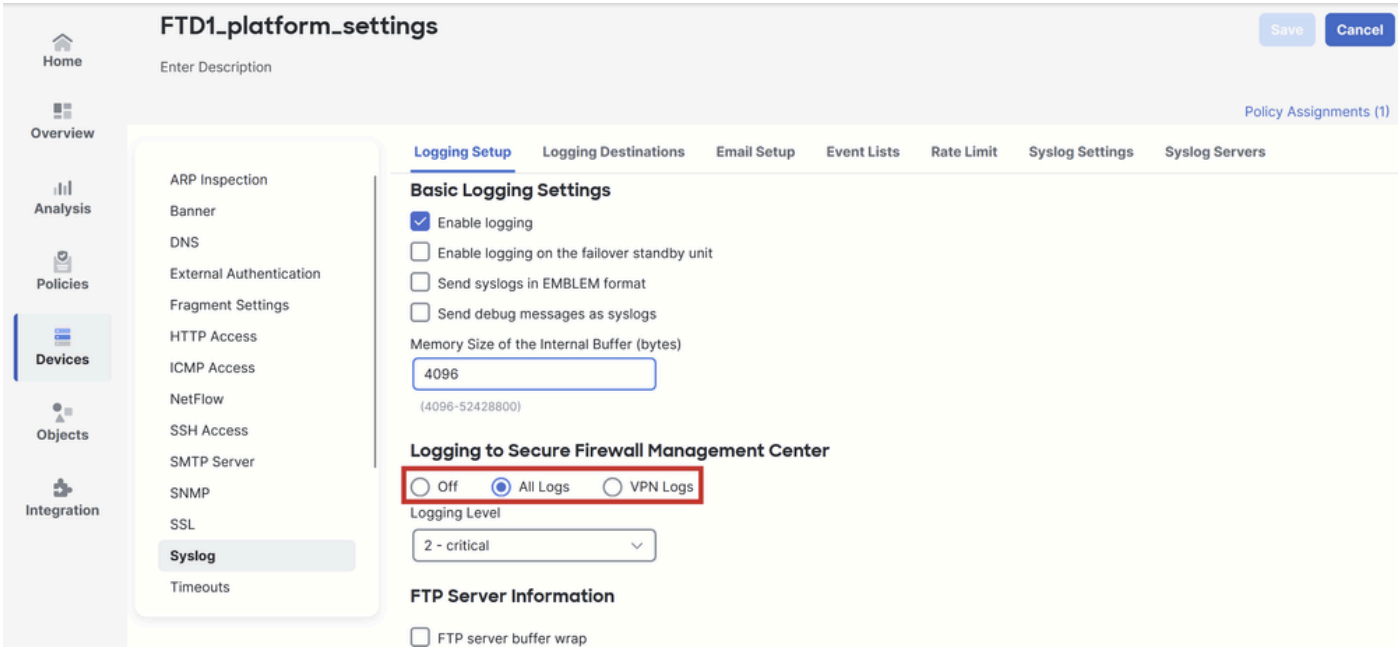
配置

导航到FMC Devices > Platform Settings，然后点击策略右上角的Edit图标。



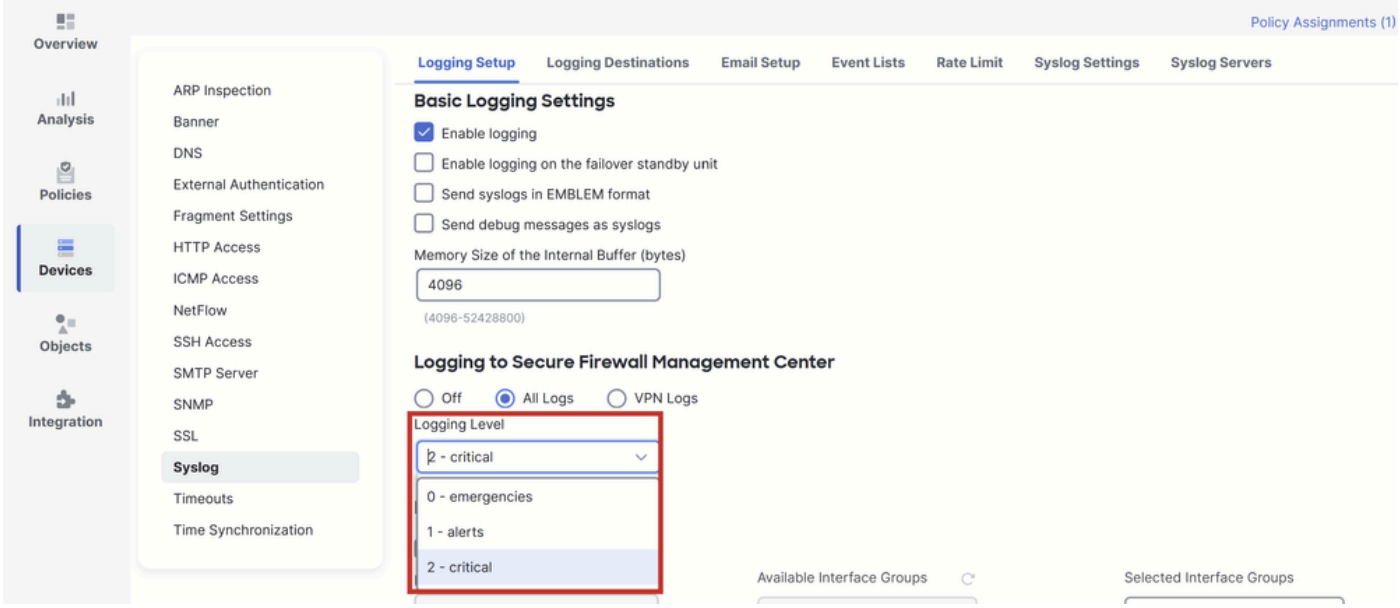
平台设置策略

转到Syslog > Logging Setup。在Logging to Secure Firewall Management Center下可以看到三个选项。



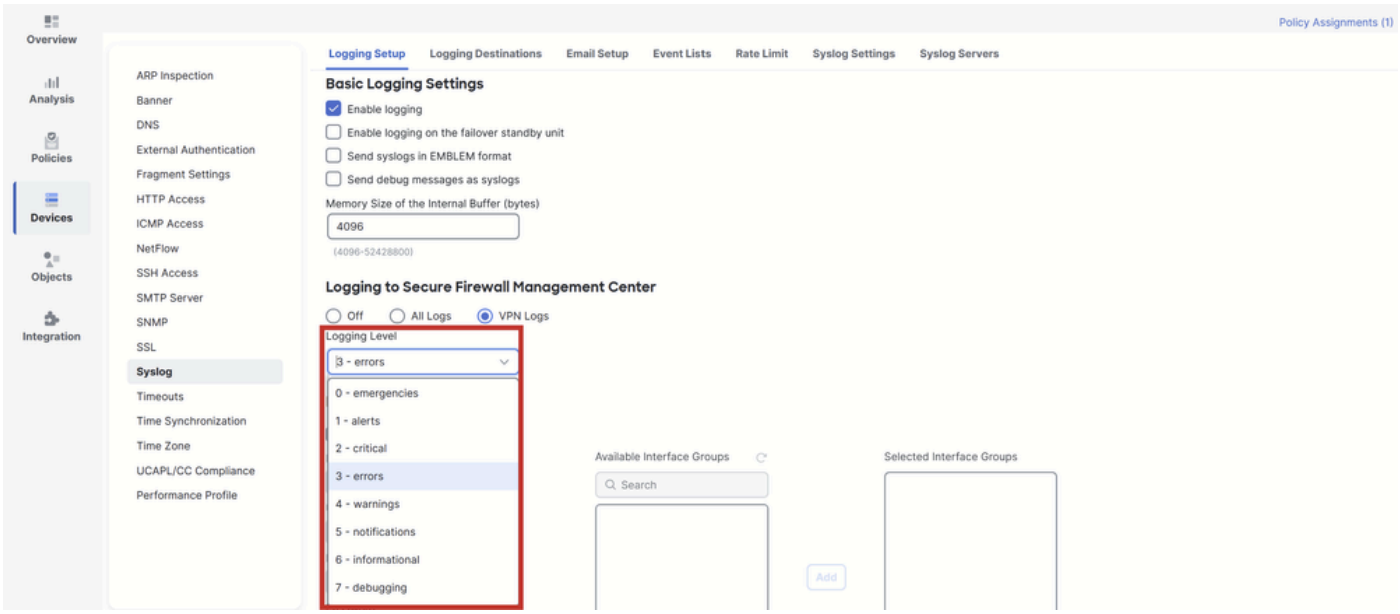
三个日志记录选项

如果选择All Logs，则可以选择以下三个可用日志记录级别中的任意一个：紧急、警报和严重并向FMC（包括VPN）发送所有诊断系统日志消息。

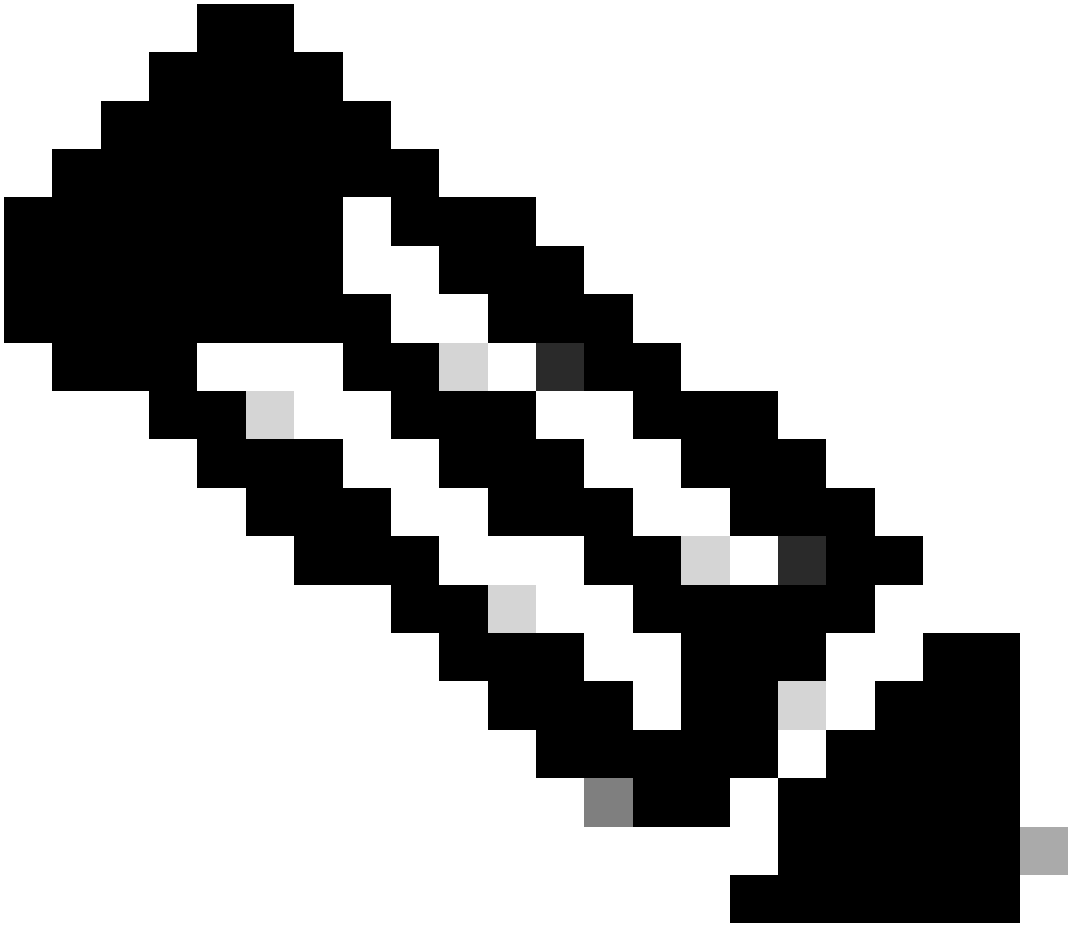


可用的日志记录级别

如果选择VPN Logs，则所有日志记录级别均可用，并且可以选择其中一个日志记录级别。

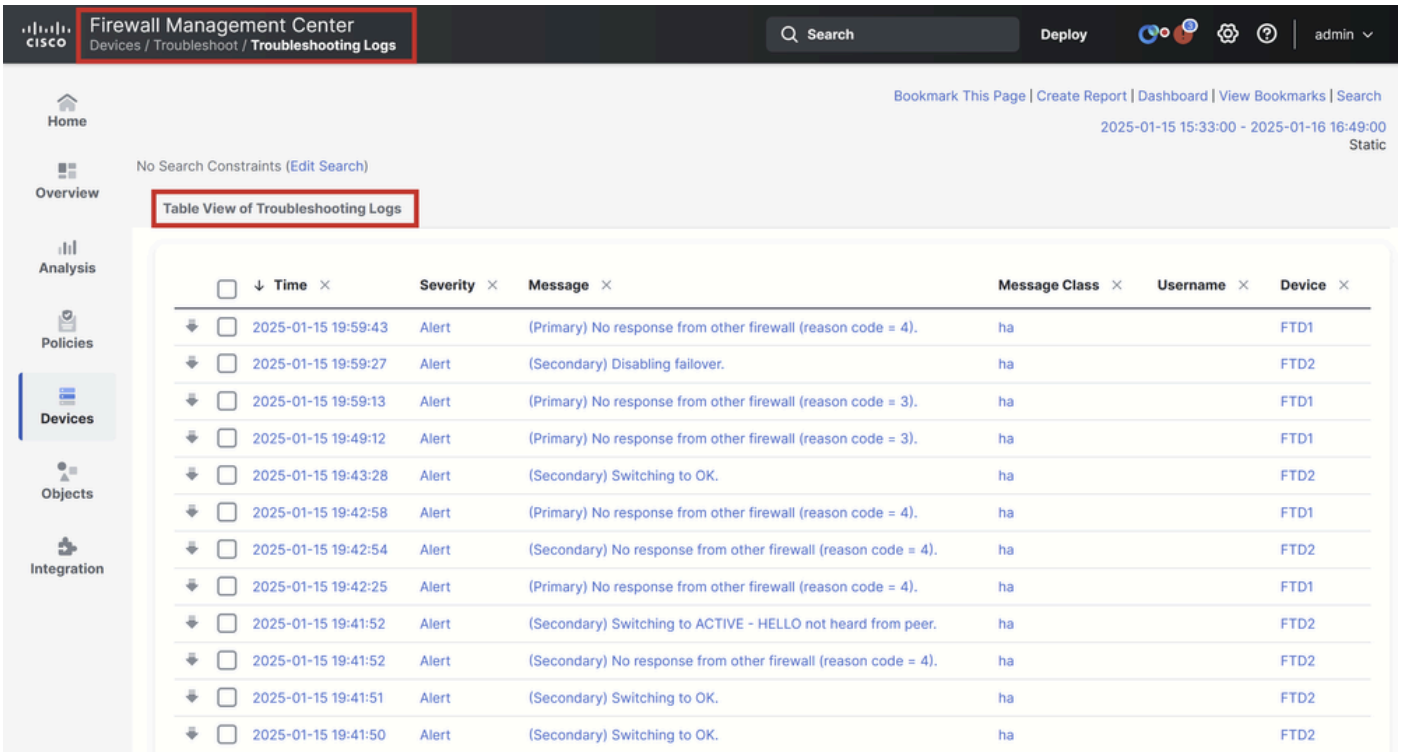


可用的日志记录级别



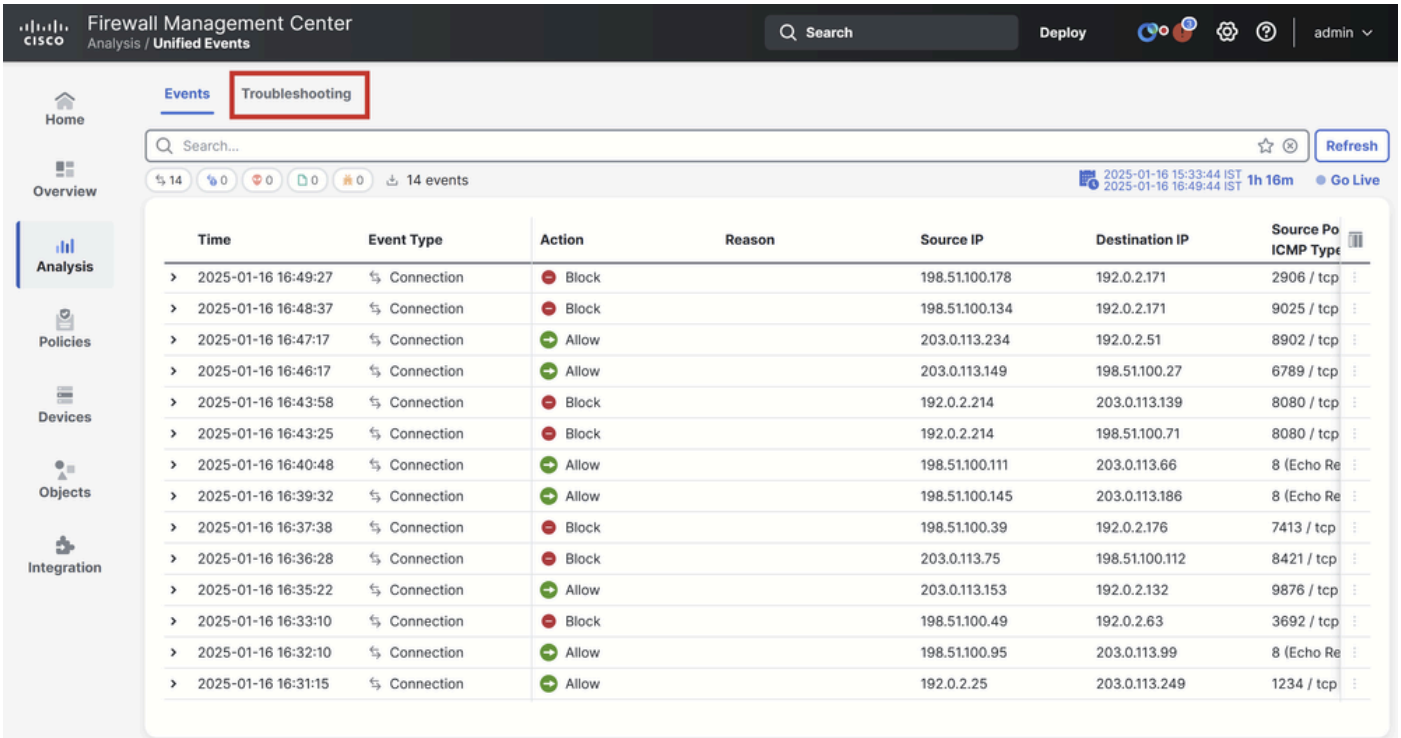
注意：当您为设备配置站点到站点或远程访问VPN时，默认情况下，它会自动启用向管理中心发送VPN系统日志。您可以将其更改为All Logs以将除VPN日志之外的所有系统日志发送到FMC。

可以从设备>故障排除>故障排除日志访问这些日志。



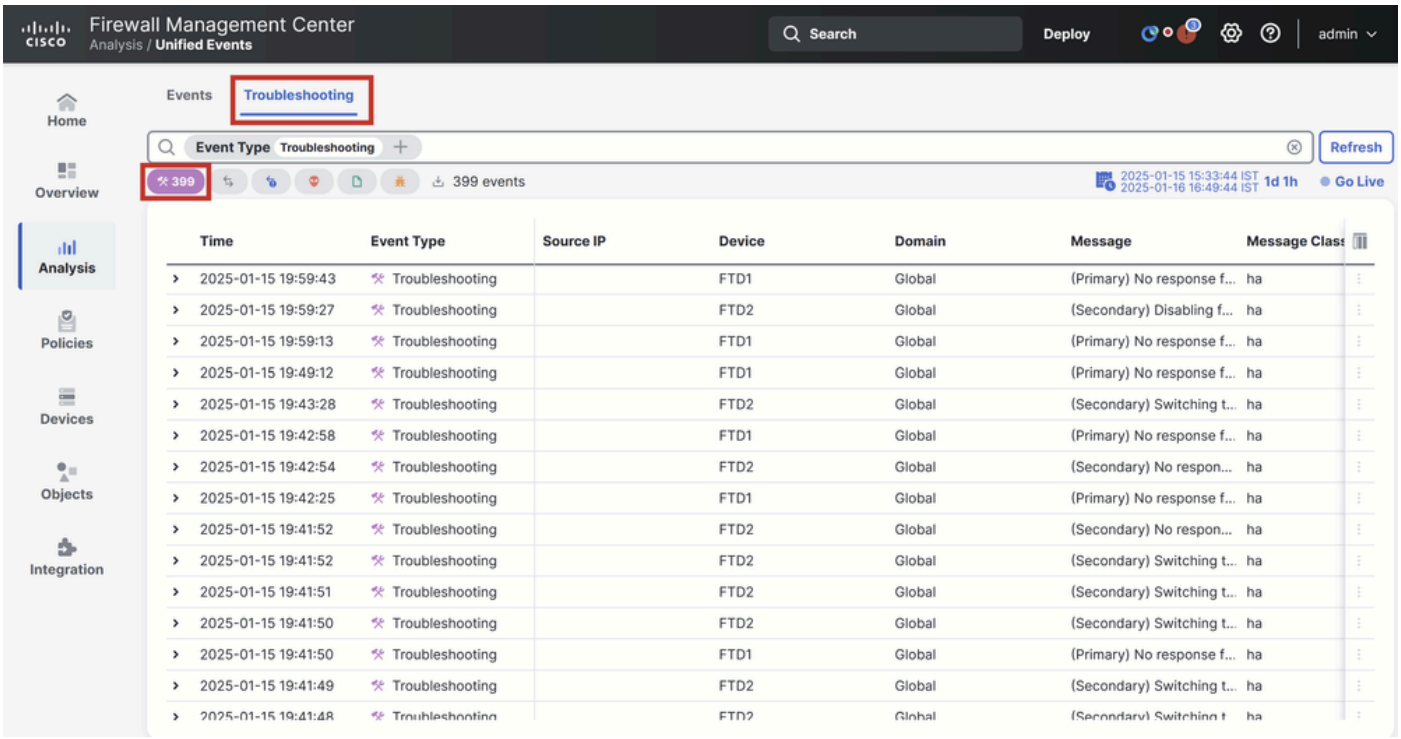
故障排除日志的表视图

Unified Event Viewer页面上现在有一个新的Troubleshooting view选项卡。要查看这些事件，请导航到分析>统一事件>故障排除。



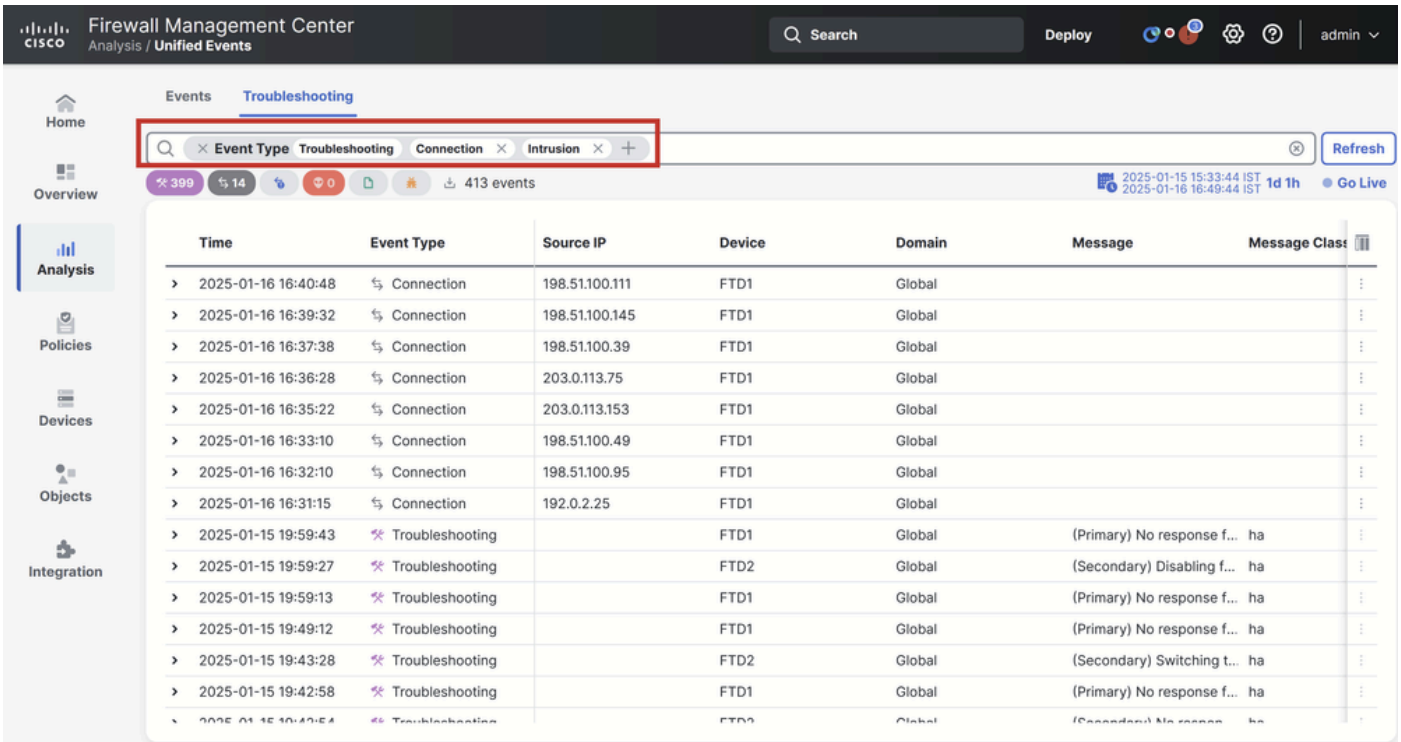
故障排除视图

切换到此选项卡后，新的事件类型在表中可见。无法像其他类型一样在视图中添加或删除该视图，因为它在故障排除视图中很重要。



故障排除事件类型

仍然可以在此“故障排除”视图中添加和删除其他事件类型。这允许您查看诊断日志以及其他事件数据。



其他事件类型

检查配置

从FMC GUI完成配置后，可以通过在CLISH或LINA模式下运行show running-config logging和show logging命令从FTD CLI进行验证。

```
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
```

FTD CLI命令

```
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
```

FTD CLI命令

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）。