配置裝置以傳送和檢視FMC上的故障排除系統日誌

目錄

簡介

本文檔介紹如何將受管裝置配置為將診斷系統日誌消息傳送到FMC，並在統一事件檢視器中檢視這些消息。

必要條件

需求

思科建議您瞭解以下主題：
·系統日誌消息
•Firepower Management Center (FMC)
•Firepower Threat Defense (FTD)

採用元件

本文中的資訊係根據以下軟體和硬體版本：
·本文檔適用於所有Firepower平台。
·執行軟體版本7.6.0的安全防火牆威脅防禦虛擬(FTD)
·運行軟體版本7.6.0的安全防火牆管理中心虛擬(FMC)
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

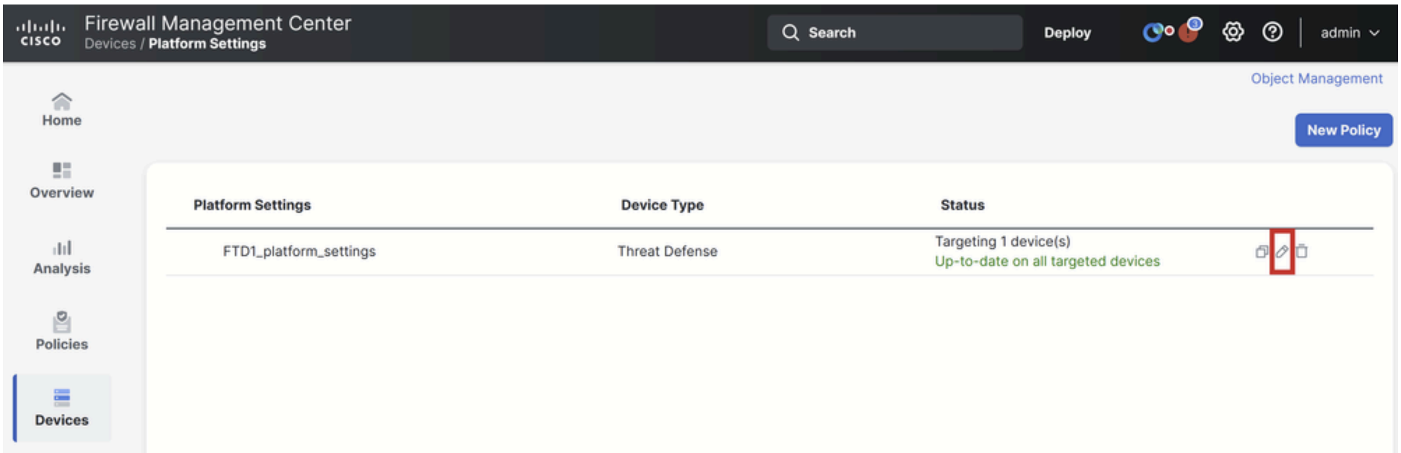
功能概述

在Secure Firewall 7.6中，將在統一事件檢視器表中新增新的故障排除事件型別。平台設定syslog日誌記錄配置已擴展，它支援將LINA生成的診斷系統日誌消息傳送到FMC，而不只是傳送VPN日誌。您可以在運行與FMC 7.6.0相容的軟體版本的任何FTD上配置此功能。由於cdFMC沒有分析工具，因此不支援cdFMC。

- 由於存在事件卷，「所有日誌」選項限製為緊急、警報和嚴重日誌級別。
- 這些故障排除日誌顯示從裝置傳送到FMC（VPN或其他）的任何系統日誌。
- 故障排除日誌流向FMC，並且在「統一事件檢視」和裝置>故障排除>故障排除日誌下可見。

設定

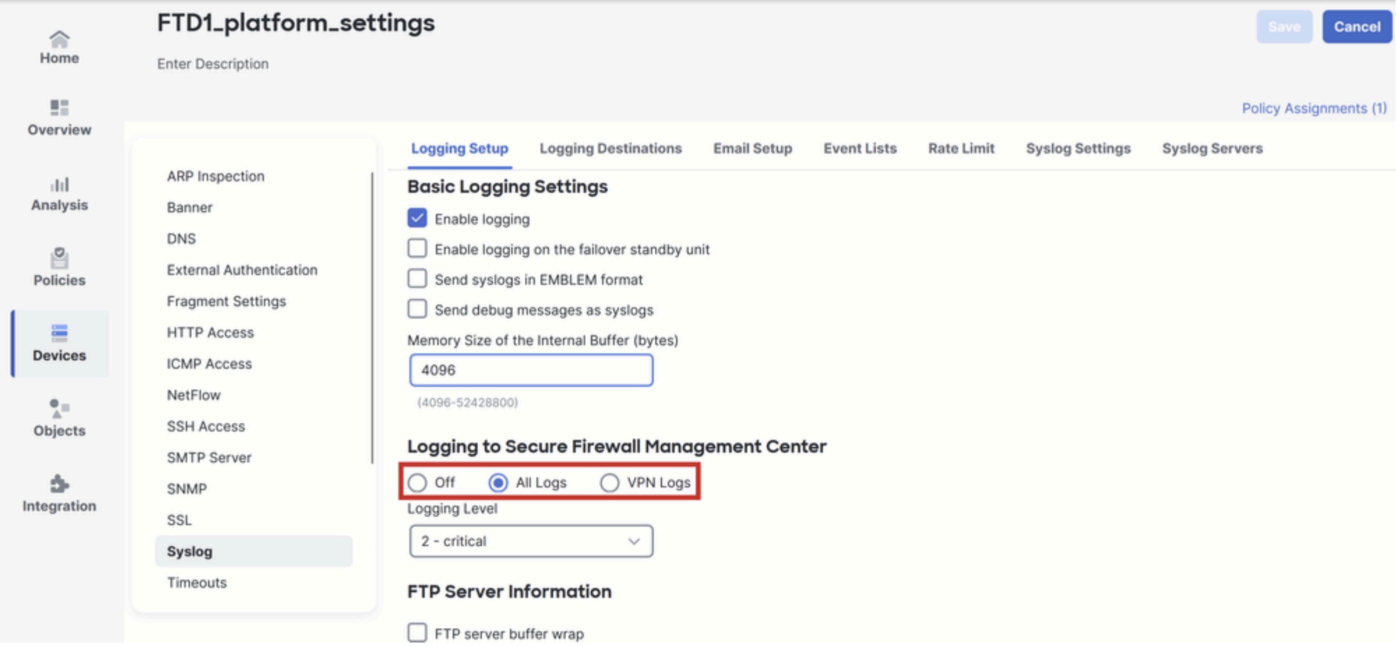
導覽至FMC Devices > Platform Settings，然後點選策略右上角的Edit圖示。



Platform Settings	Device Type	Status
FTD1_platform_settings	Threat Defense	Targeting 1 device(s) Up-to-date on all targeted devices

平台設定策略

移至Syslog > Logging Setup。在Logging to Secure Firewall Management Center下可以看到三個選項。



Basic Logging Settings

☑ Enable logging
☐ Enable logging on the failover standby unit
☐ Send syslogs in EMBLEM format
☐ Send debug messages as syslogs

Memory Size of the Internal Buffer (bytes)
4096
(4096-52428800)

Logging to Secure Firewall Management Center

○ Off ● All Logs ○ VPN Logs

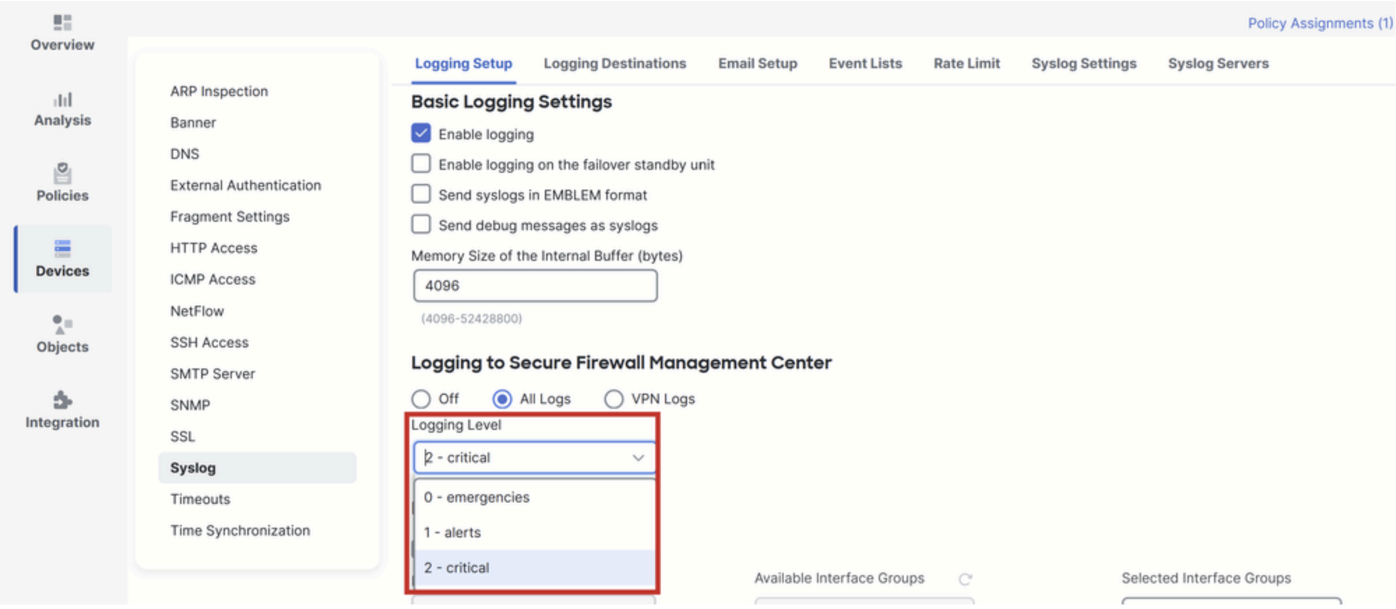
Logging Level
2 - critical

FTP Server Information

☐ FTP server buffer wrap

三個日誌記錄選項

如果選擇All Logs，則可以選擇三個可用日誌記錄級別中的任意一個：緊急事件、警報和嚴重事件，並將所有診斷系統日誌消息傳送到FMC（包括VPN）。



Basic Logging Settings

☑ Enable logging

□ Enable logging on the failover standby unit

□ Send syslogs in EMBLEM format

□ Send debug messages as syslogs

Memory Size of the Internal Buffer (bytes): 4096 (4096-52428800)

Logging to Secure Firewall Management Center

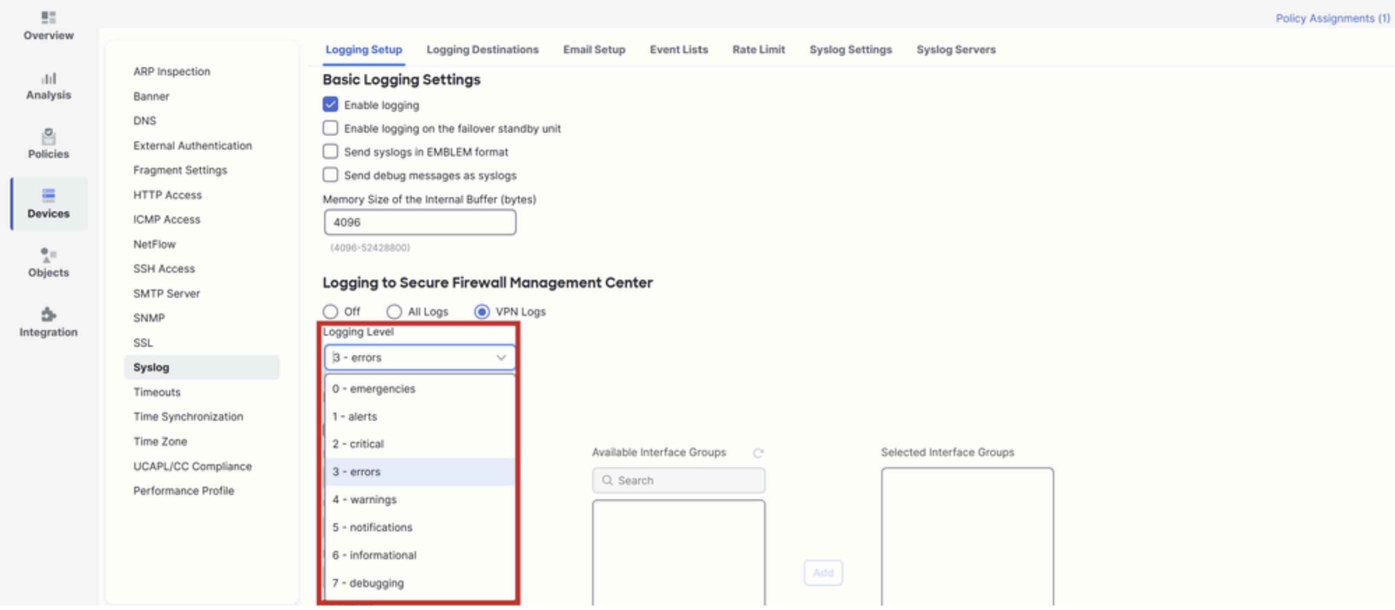
○ Off ● All Logs ○ VPN Logs

Logging Level: 2 - critical

- 0 - emergencies
- 1 - alerts
- 2 - critical

可用的日誌記錄級別

如果選擇VPN Logs，則所有日誌記錄級別均可用，並且可以選擇其中一個。



Basic Logging Settings

☑ Enable logging

□ Enable logging on the failover standby unit

□ Send syslogs in EMBLEM format

□ Send debug messages as syslogs

Memory Size of the Internal Buffer (bytes): 4096 (4096-52428800)

Logging to Secure Firewall Management Center

○ Off ○ All Logs ● VPN Logs

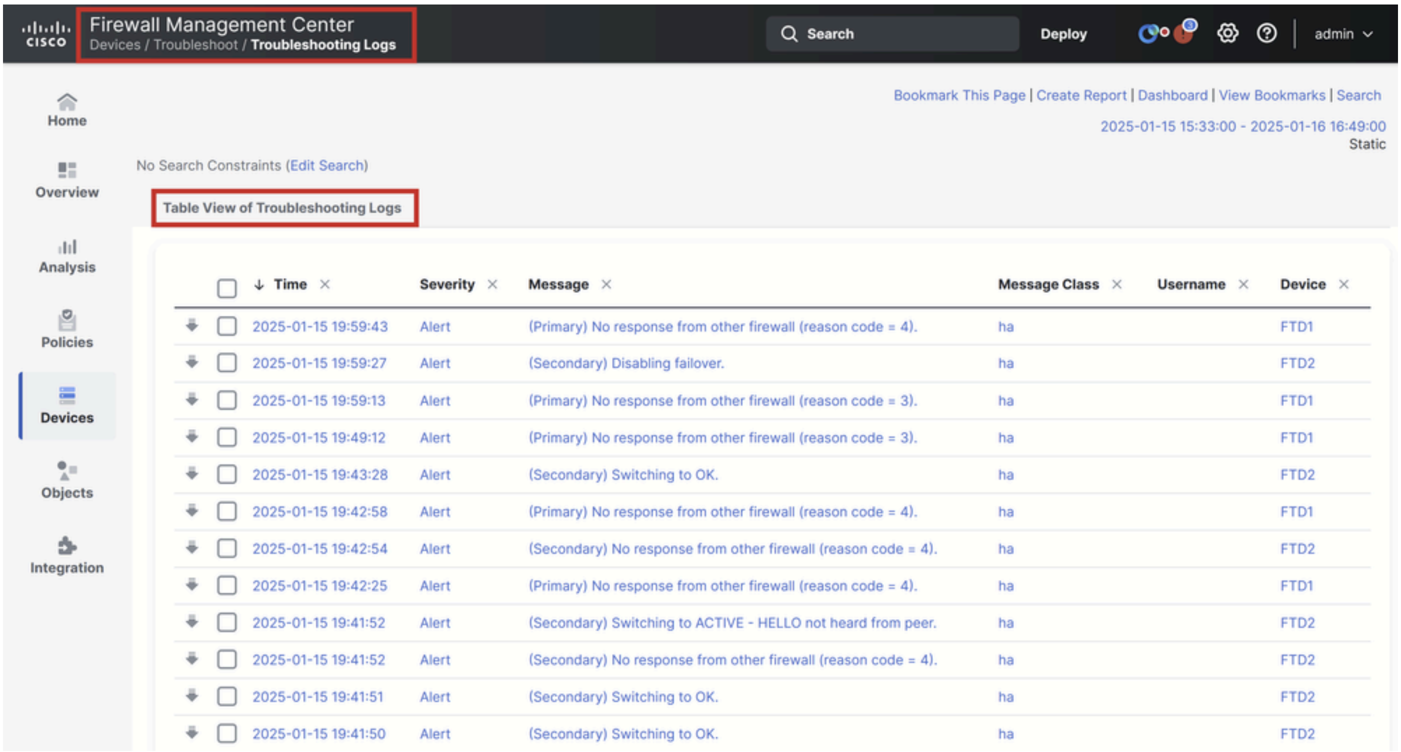
Logging Level: 3 - errors

- 0 - emergencies
- 1 - alerts
- 2 - critical
- 3 - errors
- 4 - warnings
- 5 - notifications
- 6 - informational
- 7 - debugging

可用的日誌記錄級別

附註：當您使用站點到站點或遠端訪問VPN配置裝置時，預設情況下，它會自動啟用向管理中心傳送VPN系統日誌的功能。您可以將其更改為「所有日誌」，以將除VPN日誌之外的所有系統日誌傳送到FMC。

可從Devices > Troubleshoot > Troubleshooting Logs訪問這些日誌。


Firewall Management Center
Devices / Troubleshoot / Troubleshooting Logs
Search
Deploy
admin
Home
Overview
Analysis
Policies
Devices
Objects
Integration
Bookmark This Page | Create Report | Dashboard | View Bookmarks | Search
Static
Table View of Troubleshooting Logs

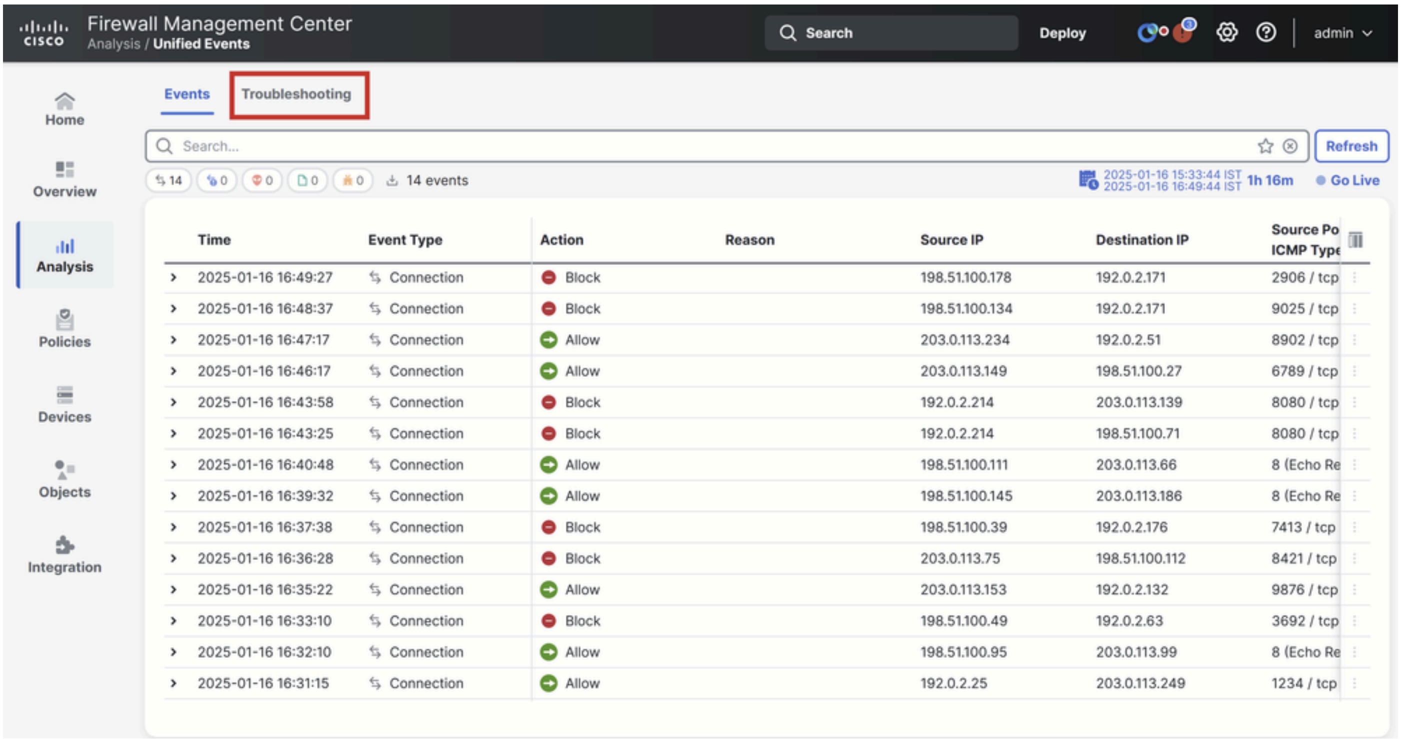
2025-01-15 15:33:00 - 2025-01-16 16:49:00

No Search Constraints (Edit Search)

Time	Severity	Message	Message Class	Username	Device
2025-01-15 19:59:43	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
2025-01-15 19:59:27	Alert	(Secondary) Disabling failover.	ha		FTD2
2025-01-15 19:59:13	Alert	(Primary) No response from other firewall (reason code = 3).	ha		FTD1
2025-01-15 19:49:12	Alert	(Primary) No response from other firewall (reason code = 3).	ha		FTD1
2025-01-15 19:43:28	Alert	(Secondary) Switching to OK.	ha		FTD2
2025-01-15 19:42:58	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
2025-01-15 19:42:54	Alert	(Secondary) No response from other firewall (reason code = 4).	ha		FTD2
2025-01-15 19:42:25	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
2025-01-15 19:41:52	Alert	(Secondary) Switching to ACTIVE - HELLO not heard from peer.	ha		FTD2
2025-01-15 19:41:52	Alert	(Secondary) No response from other firewall (reason code = 4).	ha		FTD2
2025-01-15 19:41:51	Alert	(Secondary) Switching to OK.	ha		FTD2
2025-01-15 19:41:50	Alert	(Secondary) Switching to OK.	ha		FTD2

故障排除日誌的表檢視

Unified Event Viewer頁面上現在有一個新的「故障排除」檢視頁籤。要檢視這些事件，請導航到分析>統一事件>故障排除。



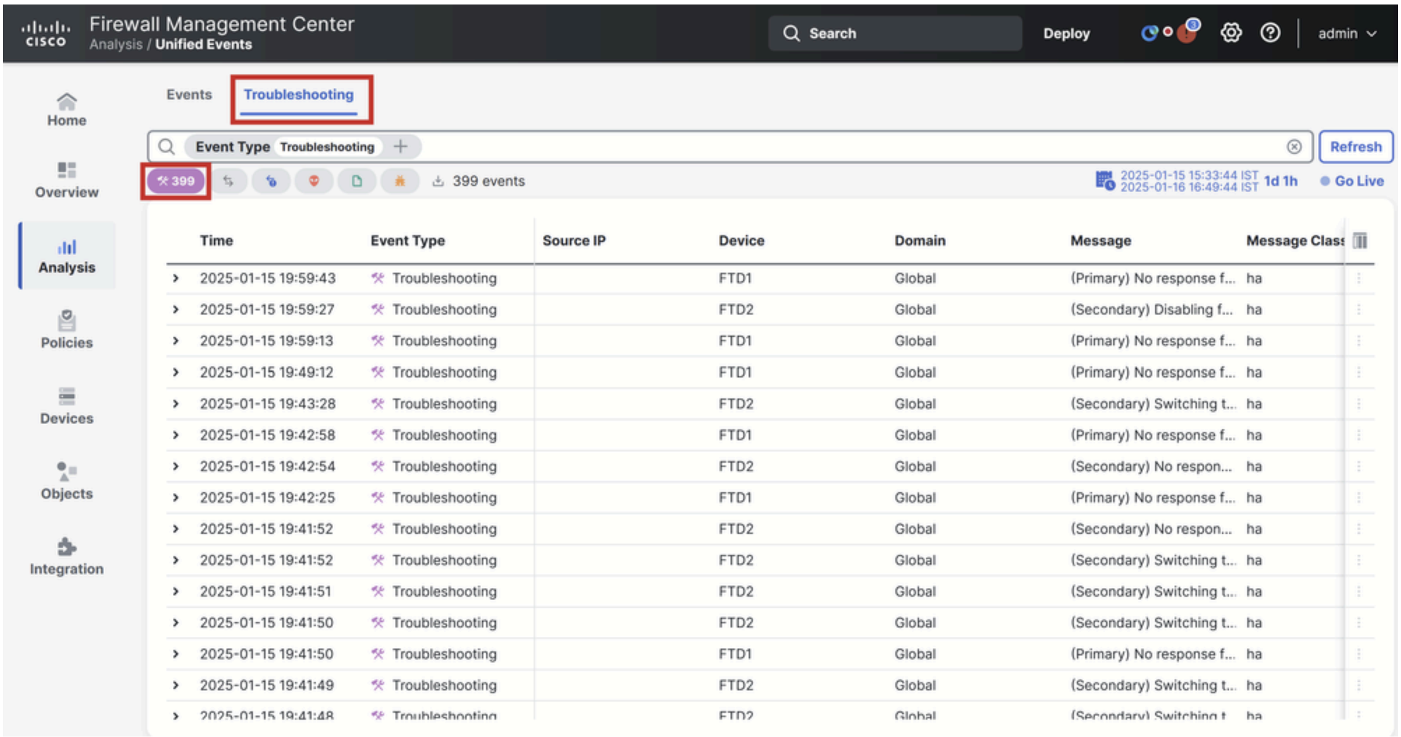
14 events

2025-01-16 15:33:44 IST
2025-01-16 16:49:44 IST 1h 16m

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Po ICMP Type
2025-01-16 16:49:27	Connection	Block		198.51.100.178	192.0.2.171	2906 / tcp
2025-01-16 16:48:37	Connection	Block		198.51.100.134	192.0.2.171	9025 / tcp
2025-01-16 16:47:17	Connection	Allow		203.0.113.234	192.0.2.51	8902 / tcp
2025-01-16 16:46:17	Connection	Allow		203.0.113.149	198.51.100.27	6789 / tcp
2025-01-16 16:43:58	Connection	Block		192.0.2.214	203.0.113.139	8080 / tcp
2025-01-16 16:43:25	Connection	Block		192.0.2.214	198.51.100.71	8080 / tcp
2025-01-16 16:40:48	Connection	Allow		198.51.100.111	203.0.113.66	8 (Echo Re
2025-01-16 16:39:32	Connection	Allow		198.51.100.145	203.0.113.186	8 (Echo Re
2025-01-16 16:37:38	Connection	Block		198.51.100.39	192.0.2.176	7413 / tcp
2025-01-16 16:36:28	Connection	Block		203.0.113.75	198.51.100.112	8421 / tcp
2025-01-16 16:35:22	Connection	Allow		203.0.113.153	192.0.2.132	9876 / tcp
2025-01-16 16:33:10	Connection	Block		198.51.100.49	192.0.2.63	3692 / tcp
2025-01-16 16:32:10	Connection	Allow		198.51.100.95	203.0.113.99	8 (Echo Re
2025-01-16 16:31:15	Connection	Allow		192.0.2.25	203.0.113.249	1234 / tcp

故障排除檢視

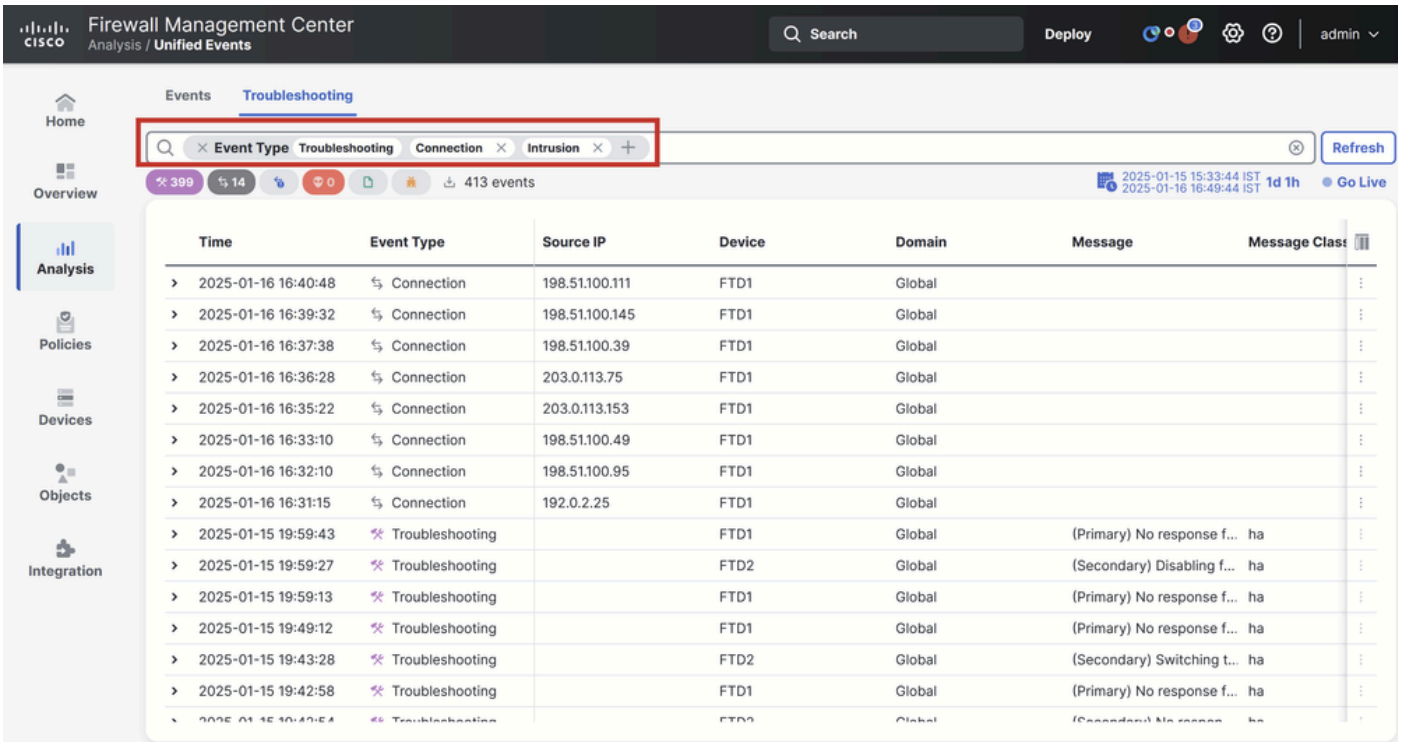
切換到此頁籤後，新的事件型別在表中可見。不能像其他型別那樣在檢視中新增或刪除它，因為它在故障排除檢視的中心。



	Time	Event Type	Source IP	Device	Domain	Message	Message Class
›	2025-01-15 19:59:43	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
›	2025-01-15 19:59:27	Troubleshooting		FTD2	Global	(Secondary) Disabling f...	ha
›	2025-01-15 19:59:13	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
›	2025-01-15 19:49:12	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
›	2025-01-15 19:43:28	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
›	2025-01-15 19:42:58	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
›	2025-01-15 19:42:54	Troubleshooting		FTD2	Global	(Secondary) No respon...	ha
›	2025-01-15 19:42:25	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
›	2025-01-15 19:41:52	Troubleshooting		FTD2	Global	(Secondary) No respon...	ha
›	2025-01-15 19:41:52	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
›	2025-01-15 19:41:51	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
›	2025-01-15 19:41:50	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
›	2025-01-15 19:41:50	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
›	2025-01-15 19:41:49	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
›	2025-01-15 19:41:48	Troubleshooting		FTD2	Global	(Secondary) Switching t	ha

故障排除事件型別

仍然可以在此「故障排除」檢視中新增和刪除其他事件型別。這樣，您就可以檢視診斷日誌以及其他事件資料。

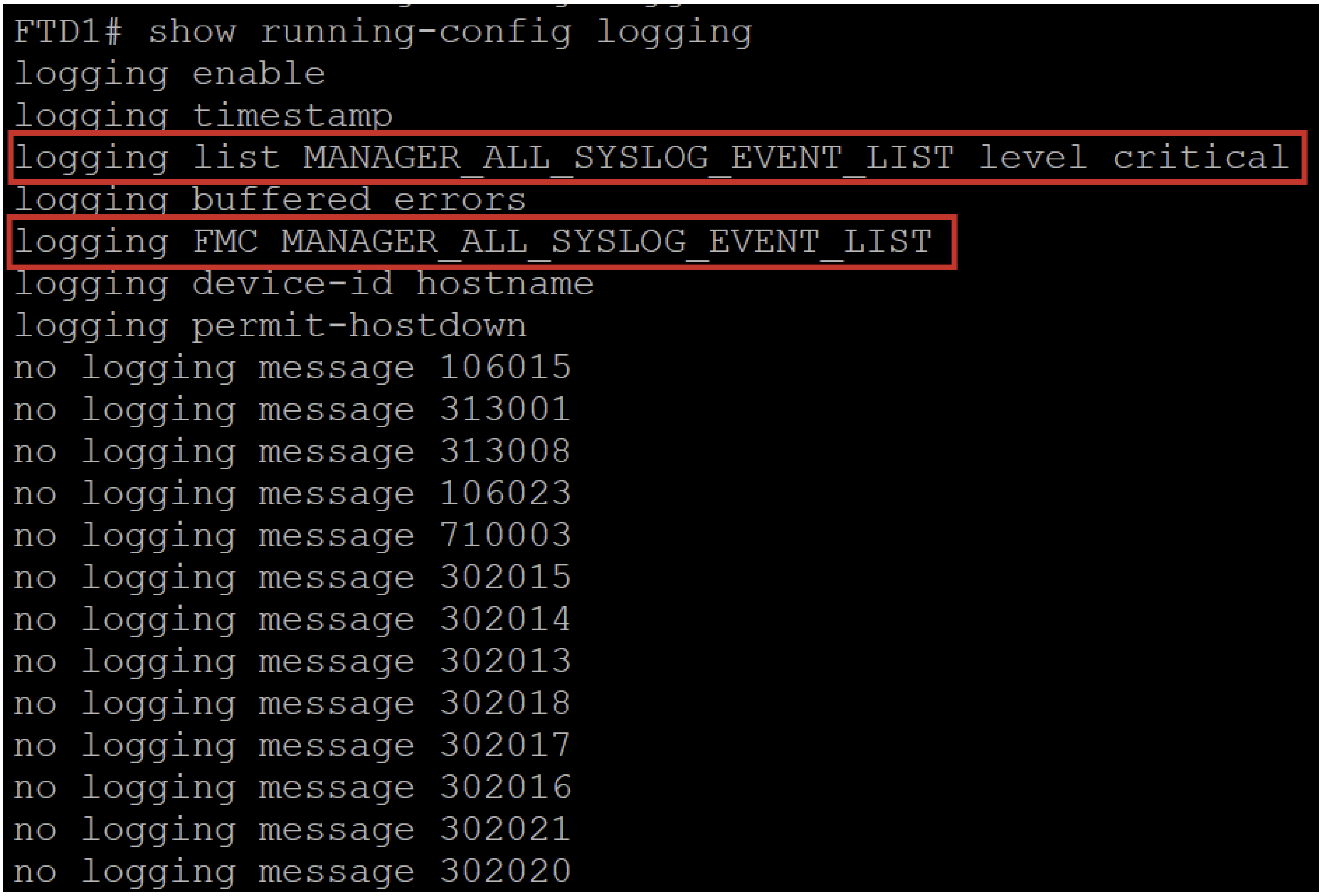


	Time	Event Type	Source IP	Device	Domain	Message	Message Class
›	2025-01-16 16:40:48	Connection	198.51.100.111	FTD1	Global		
›	2025-01-16 16:39:32	Connection	198.51.100.145	FTD1	Global		
›	2025-01-16 16:37:38	Connection	198.51.100.39	FTD1	Global		
›	2025-01-16 16:36:28	Connection	203.0.113.75	FTD1	Global		
›	2025-01-16 16:35:22	Connection	203.0.113.153	FTD1	Global		
›	2025-01-16 16:33:10	Connection	198.51.100.49	FTD1	Global		
›	2025-01-16 16:32:10	Connection	198.51.100.95	FTD1	Global		
›	2025-01-16 16:31:15	Connection	192.0.2.25	FTD1	Global		
›	2025-01-15 19:59:43	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
›	2025-01-15 19:59:27	Troubleshooting		FTD2	Global	(Secondary) Disabling f...	ha
›	2025-01-15 19:59:13	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
›	2025-01-15 19:49:12	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
›	2025-01-15 19:43:28	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
›	2025-01-15 19:42:58	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
›	2025-01-15 19:42:54	Troubleshooting		FTD2	Global	(Secondary) No respon	ha

其他事件型別

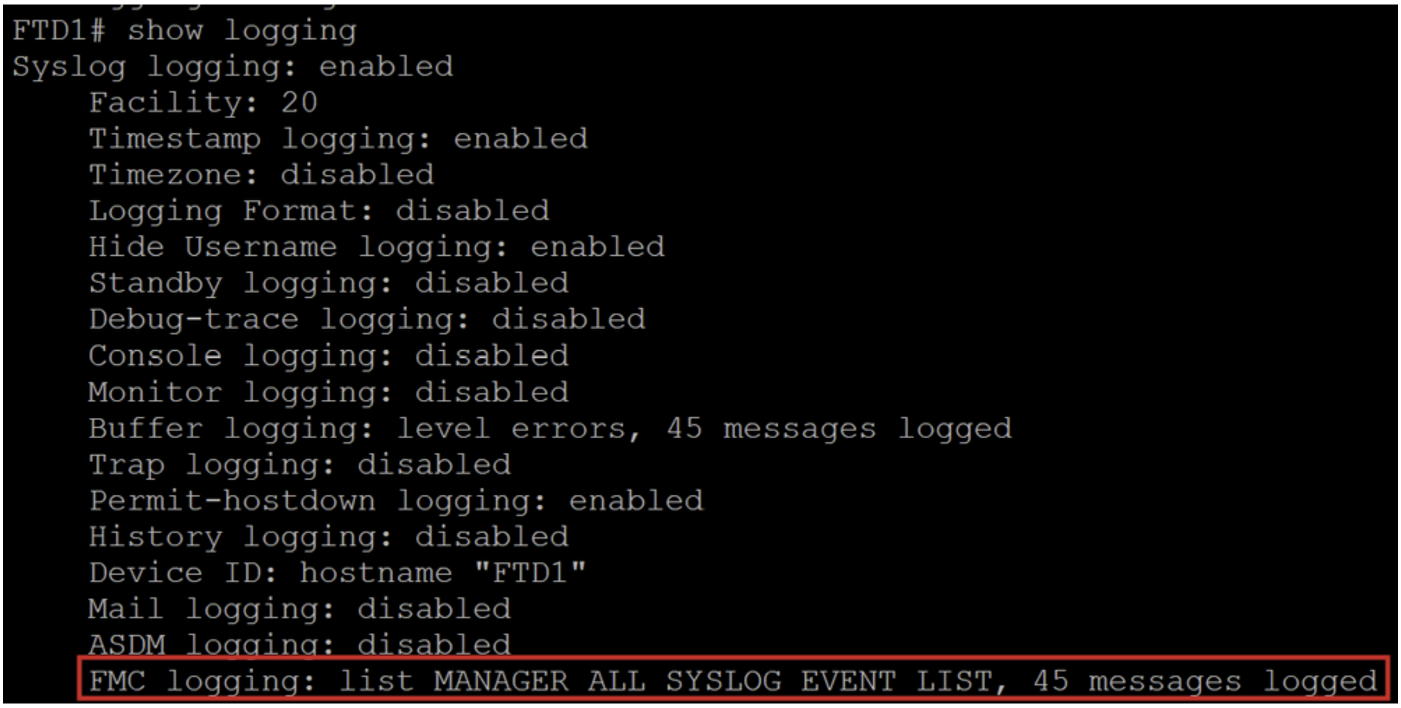
驗證設定

從FMC GUI完成組態後，即可在FTD CLI中，在CLISH或LINA模式下執行show running-config logging和show logging指令以驗證組態。



```
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指令



```
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指令

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。