在Firepower裝置管理器中配置並驗證系統日誌

目錄

簡介

本文檔介紹如何在Firepower裝置管理器(FDM)中配置系統日誌。

必要條件

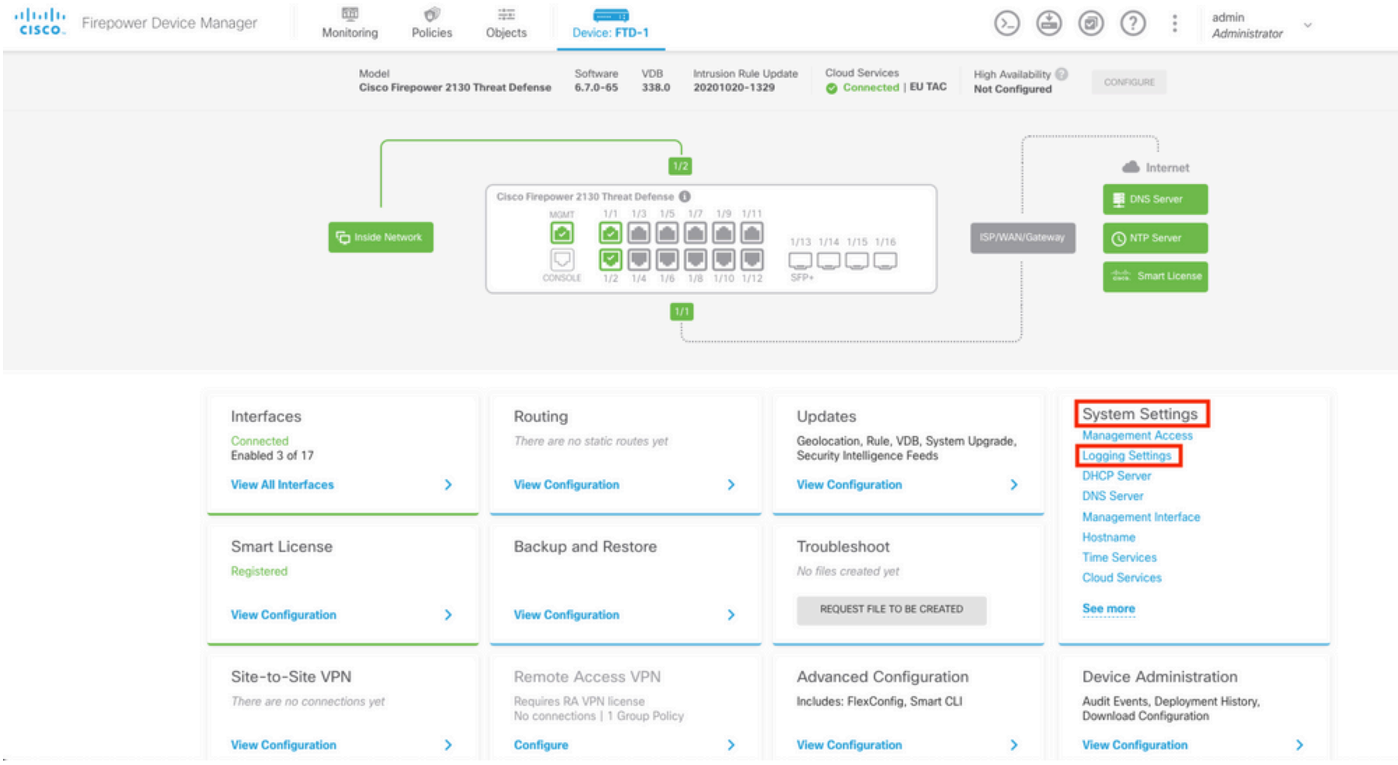
需求

思科建議您瞭解以下主題：

- Firepower威脅防禦
- 運行Syslog軟體以收集資料的Syslog伺服器

組態

步驟1.在Firepower裝置管理器主螢幕中，選擇螢幕右下角「System Settings（系統設定）」下的「Logging Settings（日誌記錄設定）」。



Model
Cisco Firepower 2130 Threat Defense

Software
6.7.0-65

VDB
338.0

Intrusion Rule Update
20201020-1329

Cloud Services
Connected | EU TAC

High Availability
Not Configured

Interfaces: Connected, Enabled 3 of 17

Routing: *There are no static routes yet*

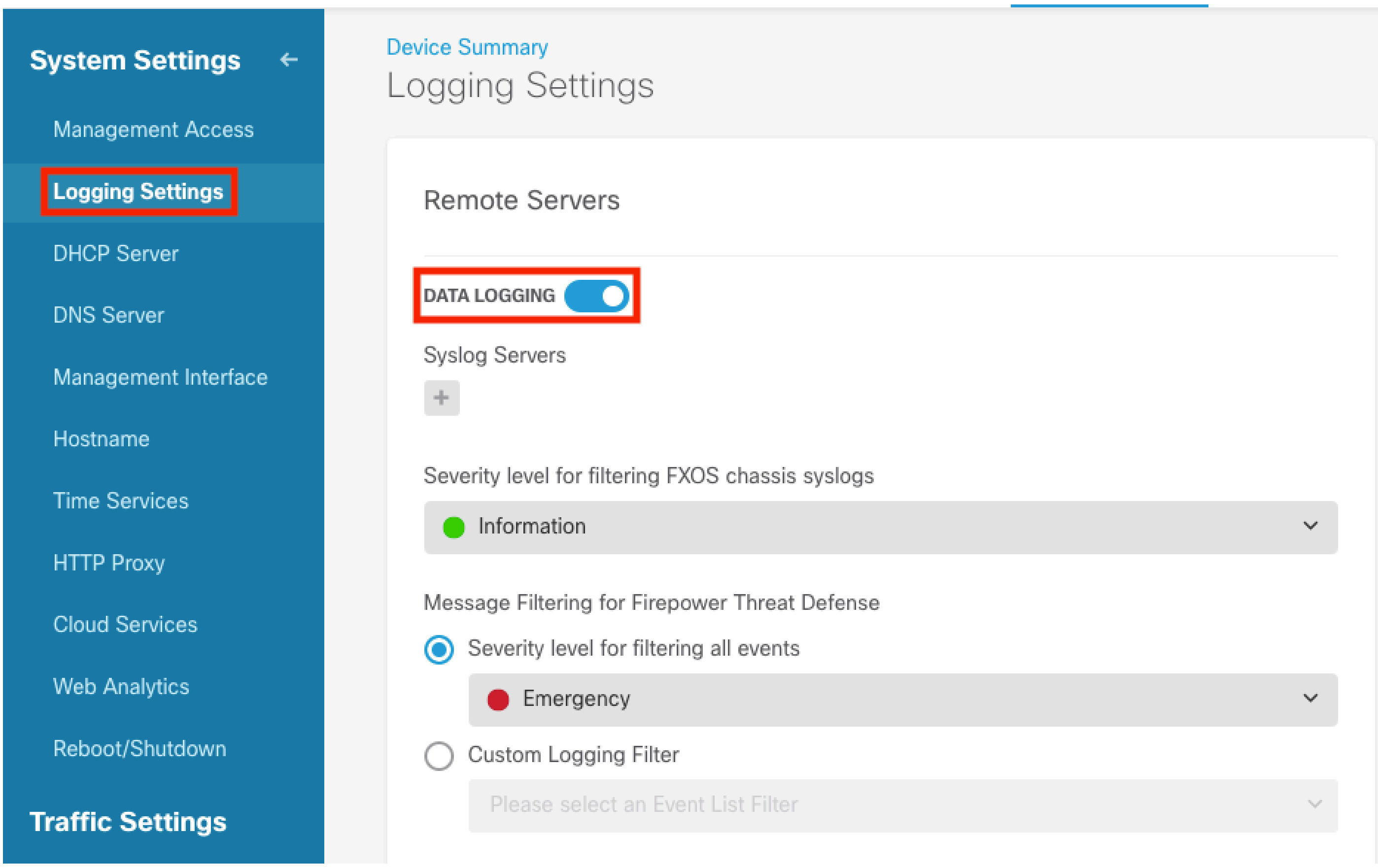
Smart License: Registered

Troubleshoot: *No files created yet*

Site-to-Site VPN: *There are no connections yet*

Remote Access VPN: Requires RA VPN license, No connections | 1 Group Policy

步驟2.在「System Settings（系統設定）」螢幕上，選擇左側選單中的Logging Settings（日誌記錄設定）。



DATA LOGGING: on

Severity level for filtering FXOS chassis syslogs: Information

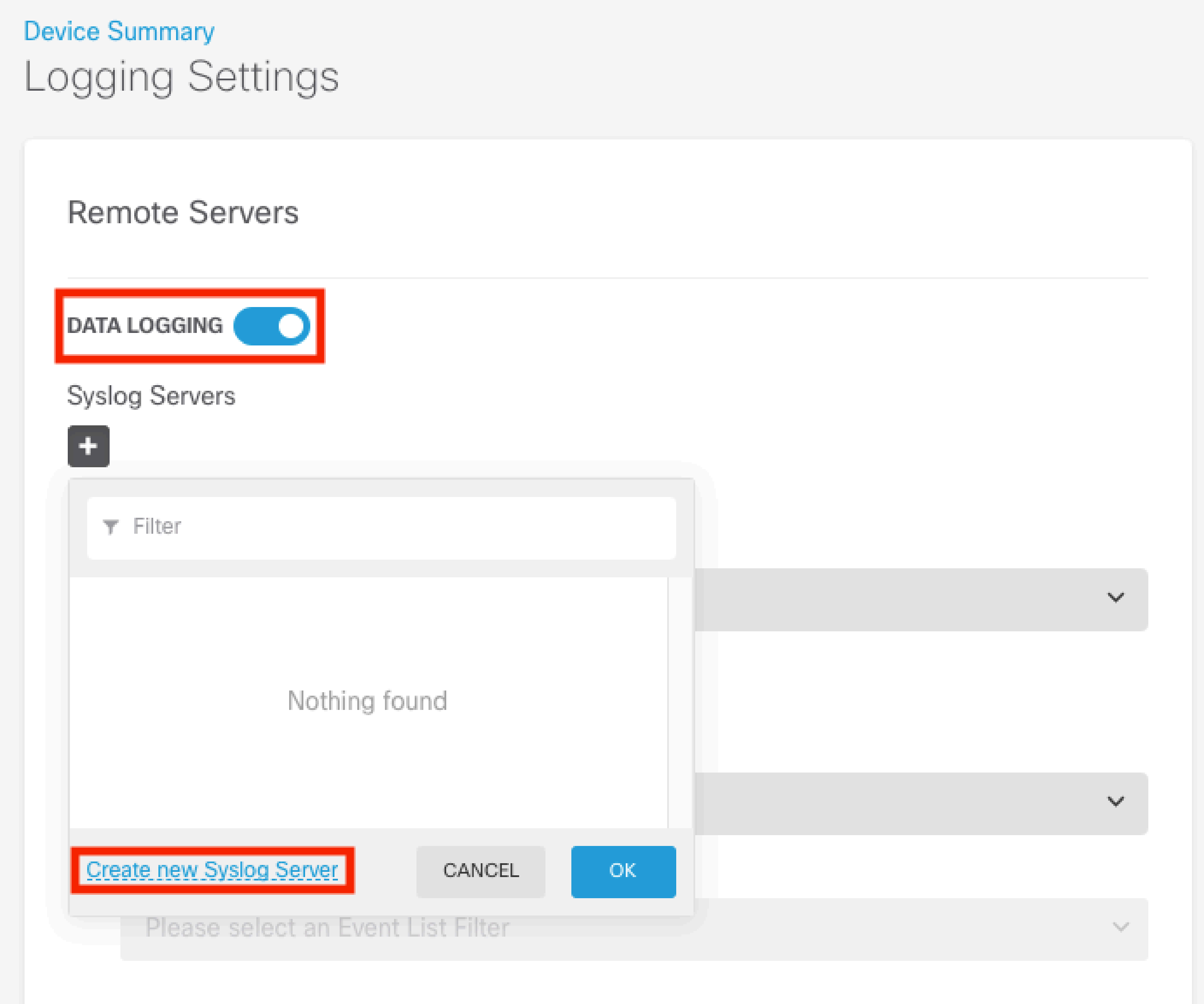
Message Filtering for Firepower Threat Defense

● Severity level for filtering all events: Emergency

○ Custom Logging Filter: Please select an Event List Filter

步驟3.選擇Syslog Servers下的+號以設定Data Logging切換開關。

步驟4.選擇Add Syslog Server。或者，您也可以在對象 — Syslog伺服器中建立系統日誌伺服器對象。



Device Summary

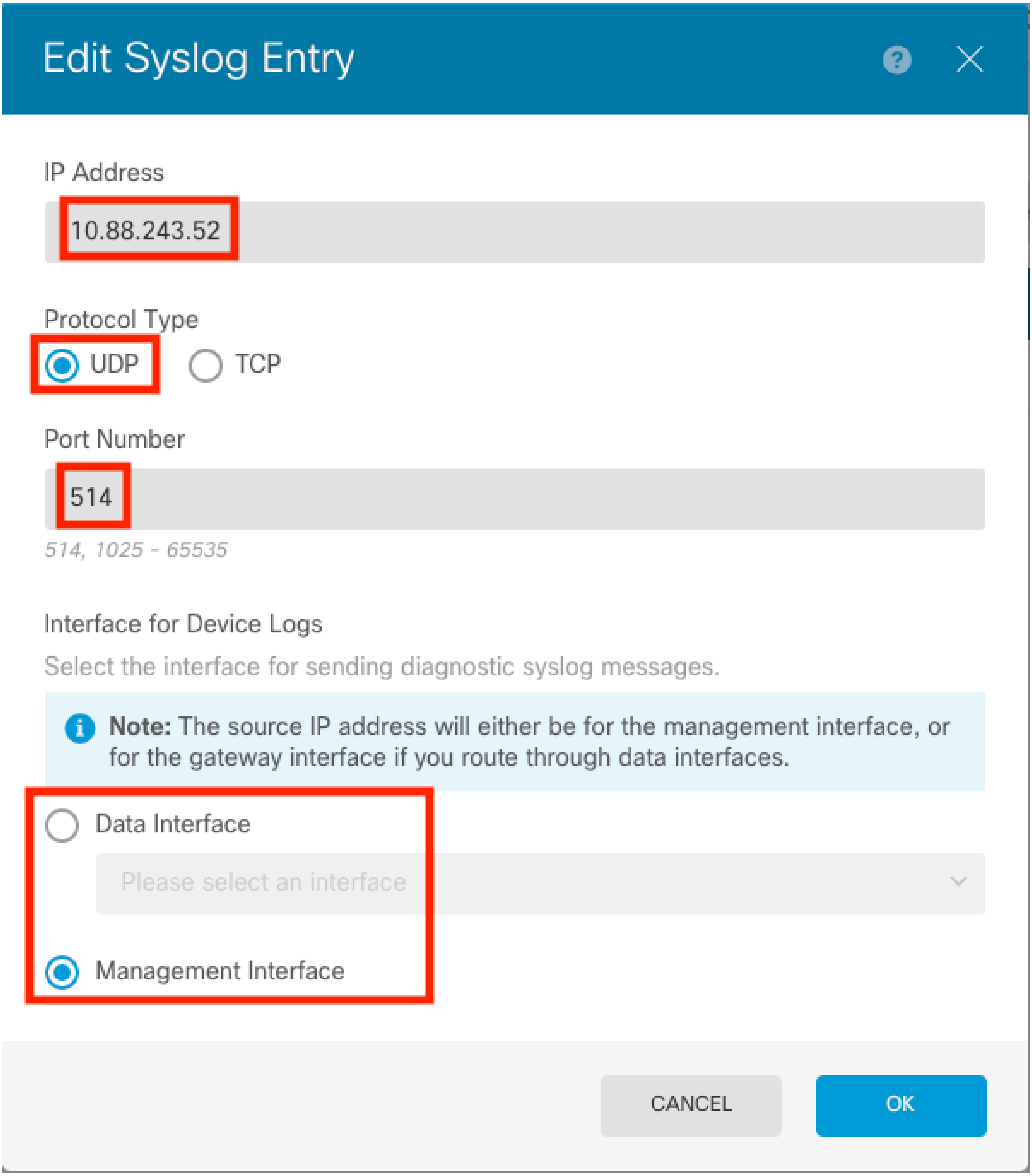
Logging Settings

Remote Servers

DATA LOGGING

Syslog Servers

步驟5.輸入系統日誌伺服器的IP地址和埠號。選擇「資料介面」的單選按鈕，然後選擇「確定」。



Edit Syslog Entry

IP Address

10.88.243.52

Protocol Type

● UDP ○ TCP

Port Number

514

514, 1025 - 65535

Interface for Device Logs

Select the interface for sending diagnostic syslog messages.

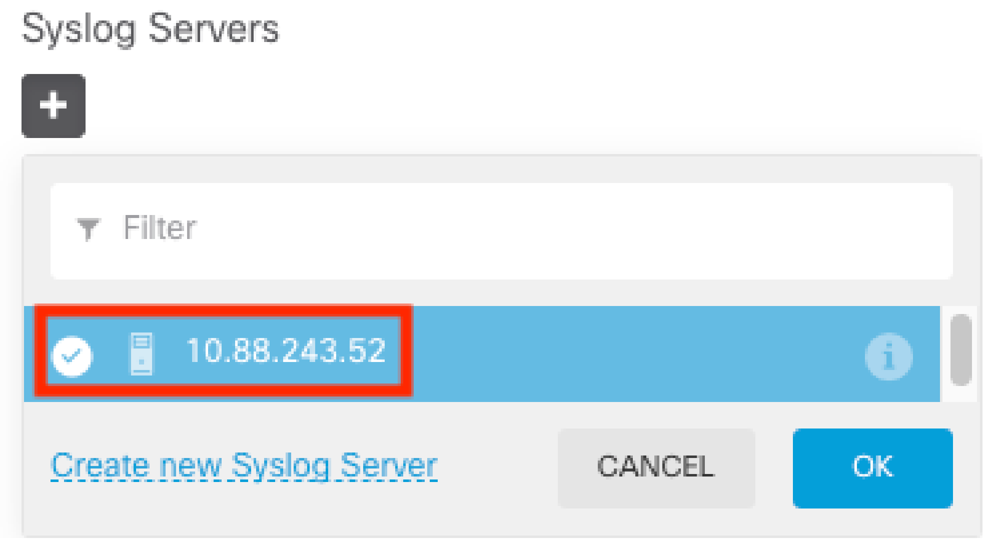
Note: The source IP address will either be for the management interface, or for the gateway interface if you route through data interfaces.

○ Data Interface

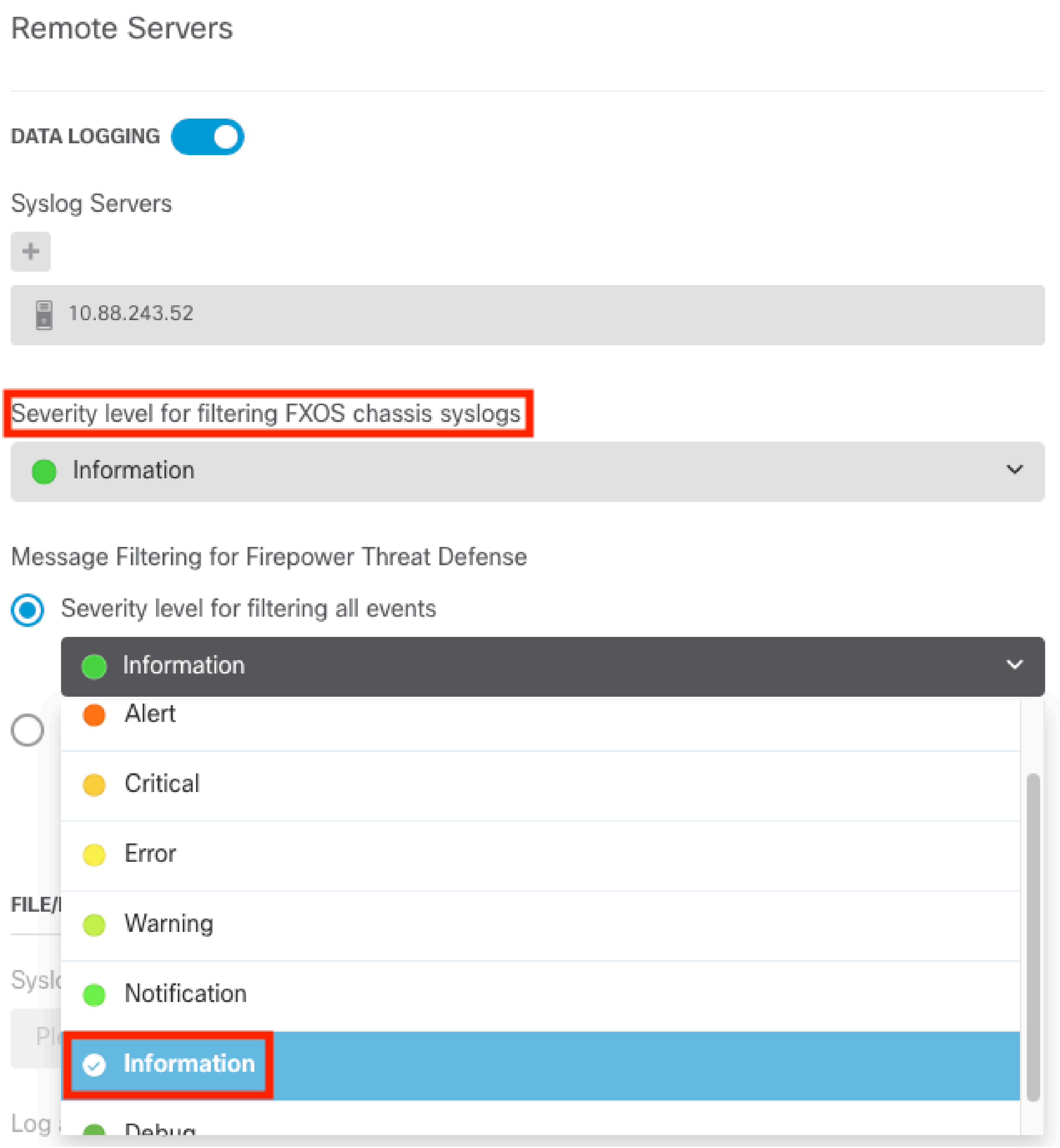
Please select an interface

● Management Interface

步驟6.接下來，選擇新的Syslog伺服器並選擇OK。



步驟7.選擇用於過濾所有事件的嚴重性級別單選按鈕，然後選擇所需的日誌記錄級別。



Remote Servers

DATA LOGGING ●

Syslog Servers

10.88.243.52

Severity level for filtering FXOS chassis syslogs

● Information

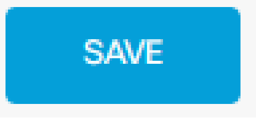
Message Filtering for Firepower Threat Defense

● Severity level for filtering all events

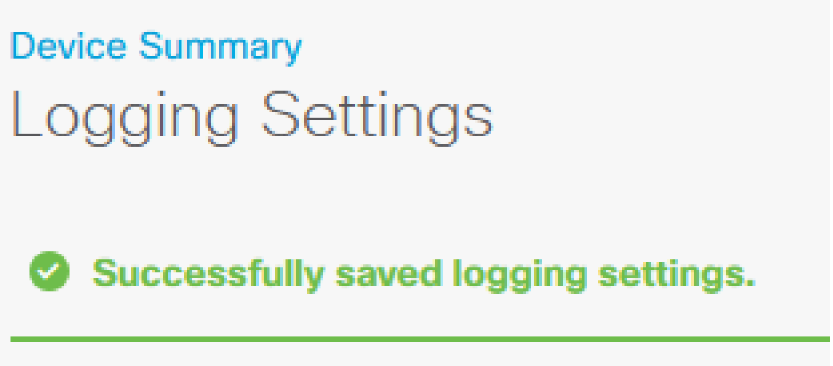
● Information

- Alert
- Critical
- Error
- Warning
- Notification
- ✓ Information
- Debug

步驟8.選擇螢幕底部的儲存。



步驟9.驗證設定是否成功。

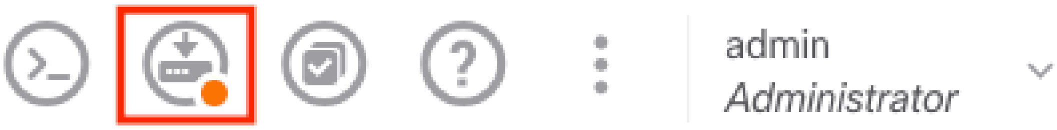


Device Summary

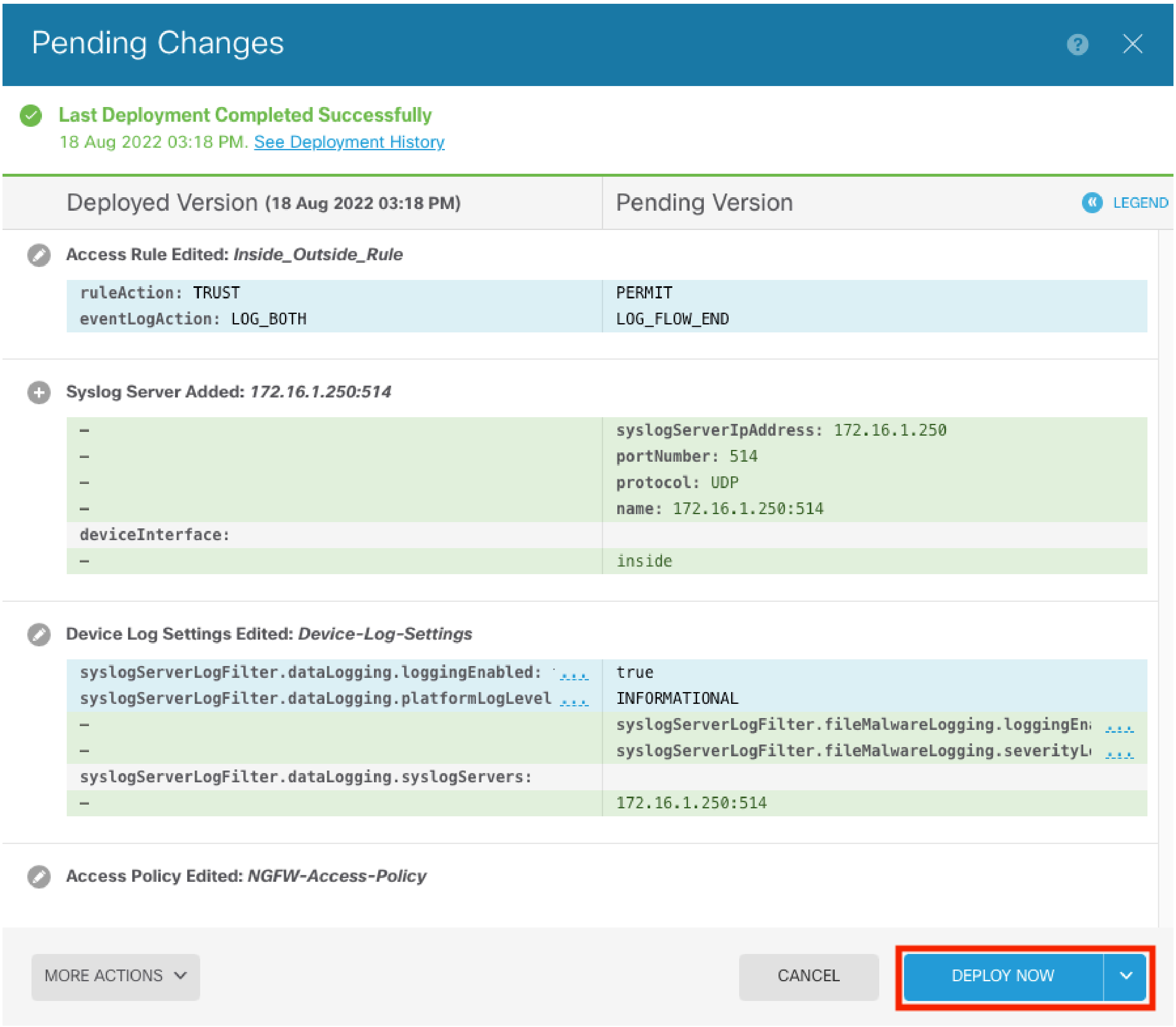
Logging Settings

Successfully saved logging settings.

步驟10.部署新設定。



和



Pending Changes

Last Deployment Completed Successfully
18 Aug 2022 03:18 PM. See Deployment History

Deployed Version (18 Aug 2022 03:18 PM)	Pending Version

Access Rule Edited: *Inside_Outside_Rule*

```
ruleAction: TRUST                          PERMIT
eventLogAction: LOG_BOTH                   LOG_FLOW_END
```

Syslog Server Added: *172.16.1.250:514*

```
-                                          syslogServerIpAddress: 172.16.1.250
-                                          portNumber: 514
-                                          protocol: UDP
-                                          name: 172.16.1.250:514
deviceInterface:
-                                          inside
```

Device Log Settings Edited: *Device-Log-Settings*

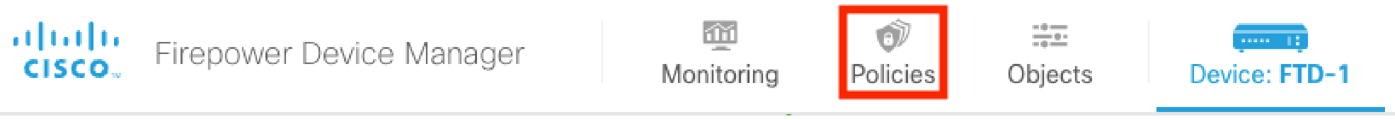
```
syslogServerLogFilter.dataLogging.loggingEnabled: ...   true
syslogServerLogFilter.dataLogging.platformLogLevel ...  INFORMATIONAL
-                                          syslogServerLogFilter.fileMalwareLogging.loggingEn ...
-                                          syslogServerLogFilter.fileMalwareLogging.severityL ...
syslogServerLogFilter.dataLogging.syslogServers:
-                                          172.16.1.250:514
```

Access Policy Edited: *NGFW-Access-Policy*

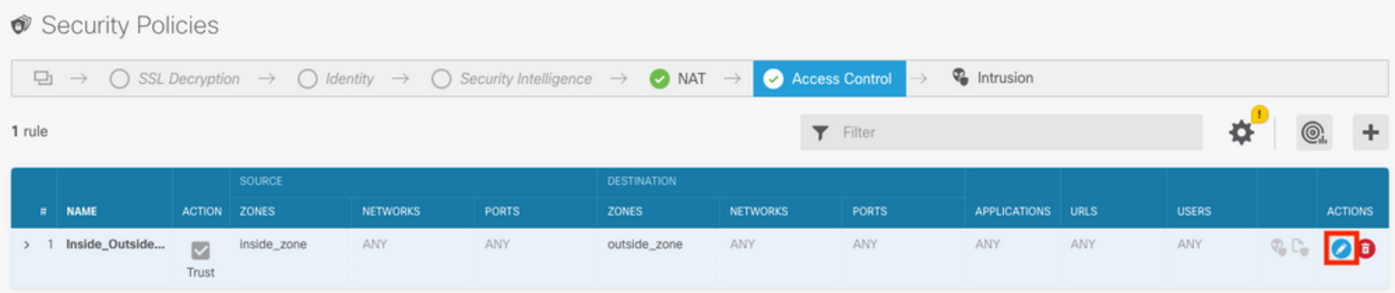
可選。

此外，還可以將訪問控制策略訪問控制規則設定為登入到系統日誌伺服器：

步驟1.按一下螢幕頂部的Policies（策略）按鈕。



步驟2. 將滑鼠懸停在ACP規則的右側以新增日誌記錄並選擇鉛筆圖示。

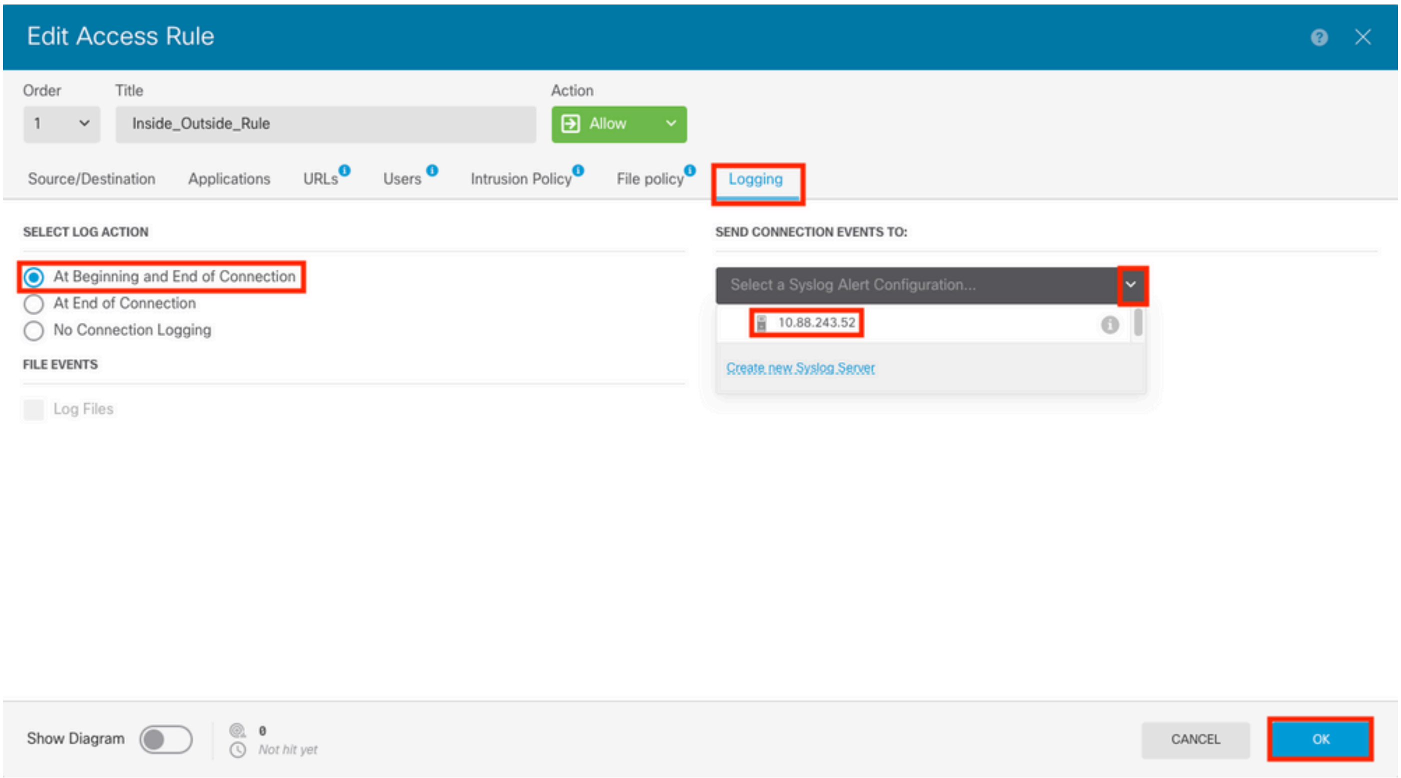

Security Policies

SSL Decryption → Identity → Security Intelligence → NAT → Access Control → Intrusion

1 rule

#	NAME	ACTION	SOURCE ZONES	SOURCE NETWORKS	SOURCE PORTS	DESTINATION ZONES	DESTINATION NETWORKS	DESTINATION PORTS	APPLICATIONS	URLS	USERS	ACTIONS
1	Inside_Outside...	Trust	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	ANY	

步驟3.選擇Logging頁籤，選擇At End of Connection的單選按鈕，選擇Select a Syslog Alert Configuration下的下拉箭頭，在Syslog Server上選擇，然後選擇OK。


Edit Access Rule

Order: 1
Title: Inside_Outside_Rule
Action: Allow

SELECT LOG ACTION
- ● At Beginning and End of Connection
- ○ At End of Connection
- ○ No Connection Logging

FILE EVENTS
- □ Log Files

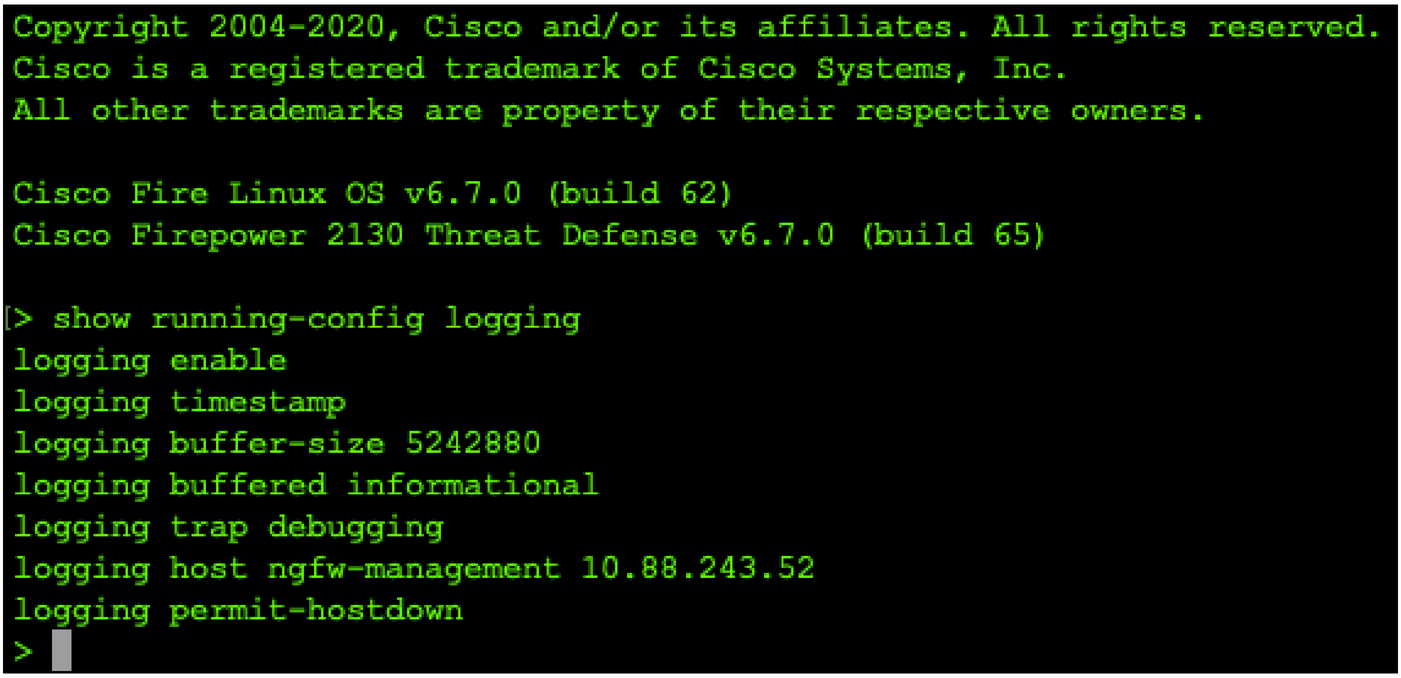
SEND CONNECTION EVENTS TO:
Select a Syslog Alert Configuration...
10.88.243.52
Create new Syslog Server

Show Diagram
0
Not hit yet

步驟4.部署配置更改。

驗證

步驟1.任務完成後，可以使用show running-config logging命令驗證FTD CLI清除模式中的設定。

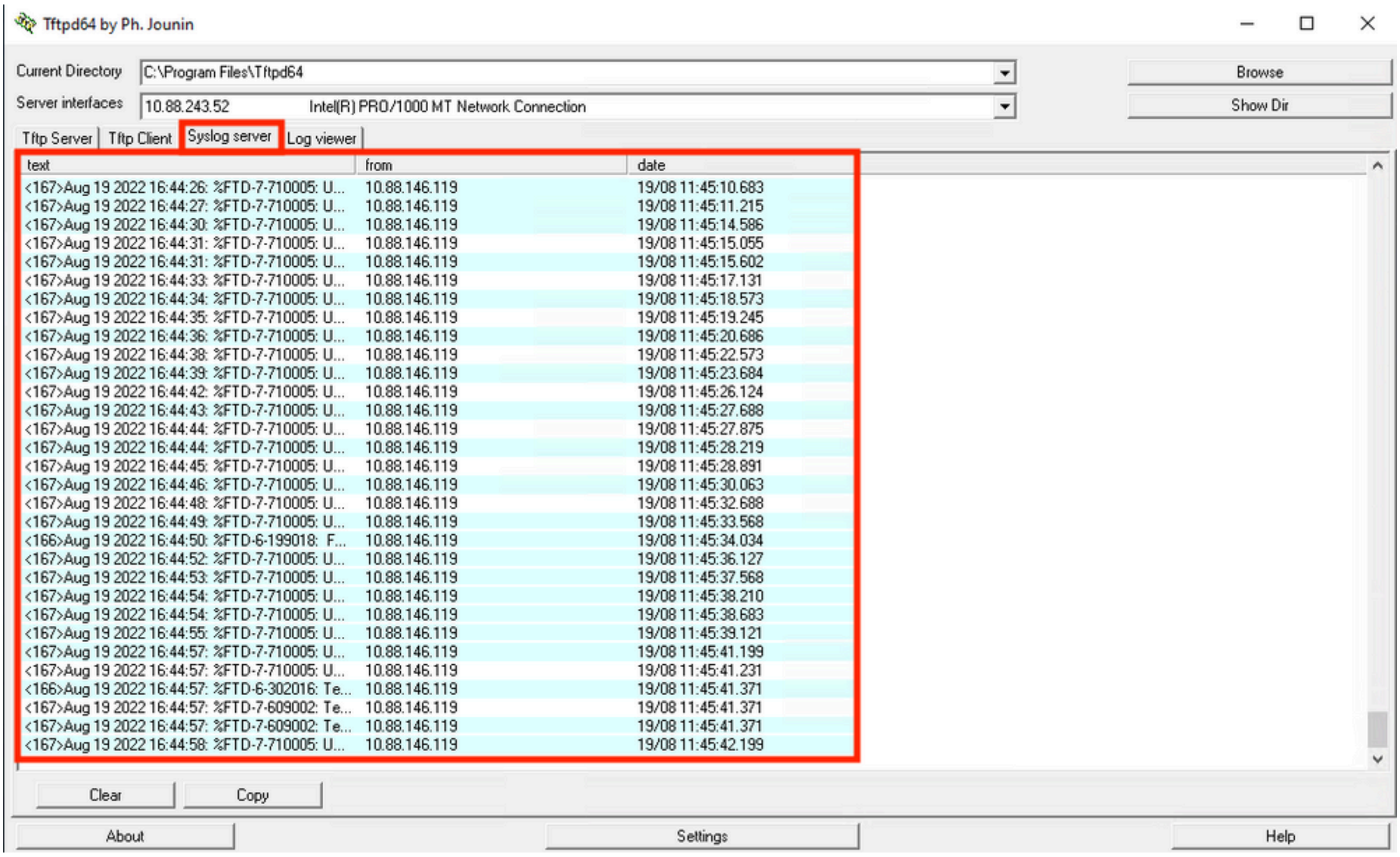


```
Copyright 2004-2020, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.7.0 (build 62)
Cisco Firepower 2130 Threat Defense v6.7.0 (build 65)

> show running-config logging
logging enable
logging timestamp
logging buffer-size 5242880
logging buffered informational
logging trap debugging
logging host ngfw-management 10.88.243.52
logging permit-hostdown
> 
```

步驟2.導航到Syslog伺服器並驗證Syslog伺服器應用程式是否正在接受Syslog消息。



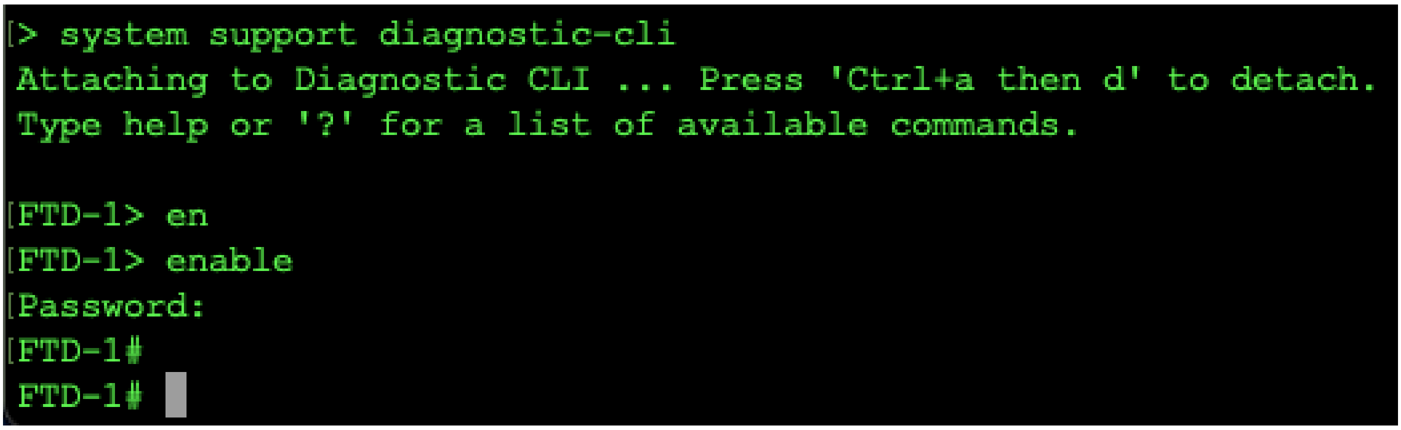
Current Directory: C:\Program Files\Tftpd64

Server interfaces: 10.88.243.52 Intel(R) PRO/1000 MT Network Connection

text	from	date
<167>Aug 19 2022 16:44:26: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:10.683
<167>Aug 19 2022 16:44:27: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:11.215
<167>Aug 19 2022 16:44:30: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:14.586
<167>Aug 19 2022 16:44:31: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:15.055
<167>Aug 19 2022 16:44:31: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:15.602
<167>Aug 19 2022 16:44:33: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:17.131
<167>Aug 19 2022 16:44:34: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:18.573
<167>Aug 19 2022 16:44:35: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:19.245
<167>Aug 19 2022 16:44:36: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:20.686
<167>Aug 19 2022 16:44:38: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:22.573
<167>Aug 19 2022 16:44:39: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:23.684
<167>Aug 19 2022 16:44:42: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:26.124
<167>Aug 19 2022 16:44:43: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:27.688
<167>Aug 19 2022 16:44:44: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:27.875
<167>Aug 19 2022 16:44:44: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:28.219
<167>Aug 19 2022 16:44:45: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:28.891
<167>Aug 19 2022 16:44:46: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:30.063
<167>Aug 19 2022 16:44:48: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:32.688
<167>Aug 19 2022 16:44:49: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:33.568
<166>Aug 19 2022 16:44:50: %FTD-6-199018: F...	10.88.146.119	19/08 11:45:34.034
<167>Aug 19 2022 16:44:52: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:36.127
<167>Aug 19 2022 16:44:53: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:37.568
<167>Aug 19 2022 16:44:54: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:38.210
<167>Aug 19 2022 16:44:54: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:38.683
<167>Aug 19 2022 16:44:55: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:39.121
<167>Aug 19 2022 16:44:57: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:41.199
<167>Aug 19 2022 16:44:57: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:41.231
<166>Aug 19 2022 16:44:57: %FTD-6-302016: Te...	10.88.146.119	19/08 11:45:41.371
<167>Aug 19 2022 16:44:57: %FTD-7-609002: Te...	10.88.146.119	19/08 11:45:41.371
<167>Aug 19 2022 16:44:57: %FTD-7-609002: Te...	10.88.146.119	19/08 11:45:41.371
<167>Aug 19 2022 16:44:58: %FTD-7-710005: U...	10.88.146.119	19/08 11:45:42.199

疑難排解

步驟1.如果Syslog應用程式上的Syslog消息生成任何消息，請從FTD CLI執行資料包捕獲以檢查資料包。在clish提示符下輸入**system support diagnostic-cli**命令，從Clish模式更改為LINA。

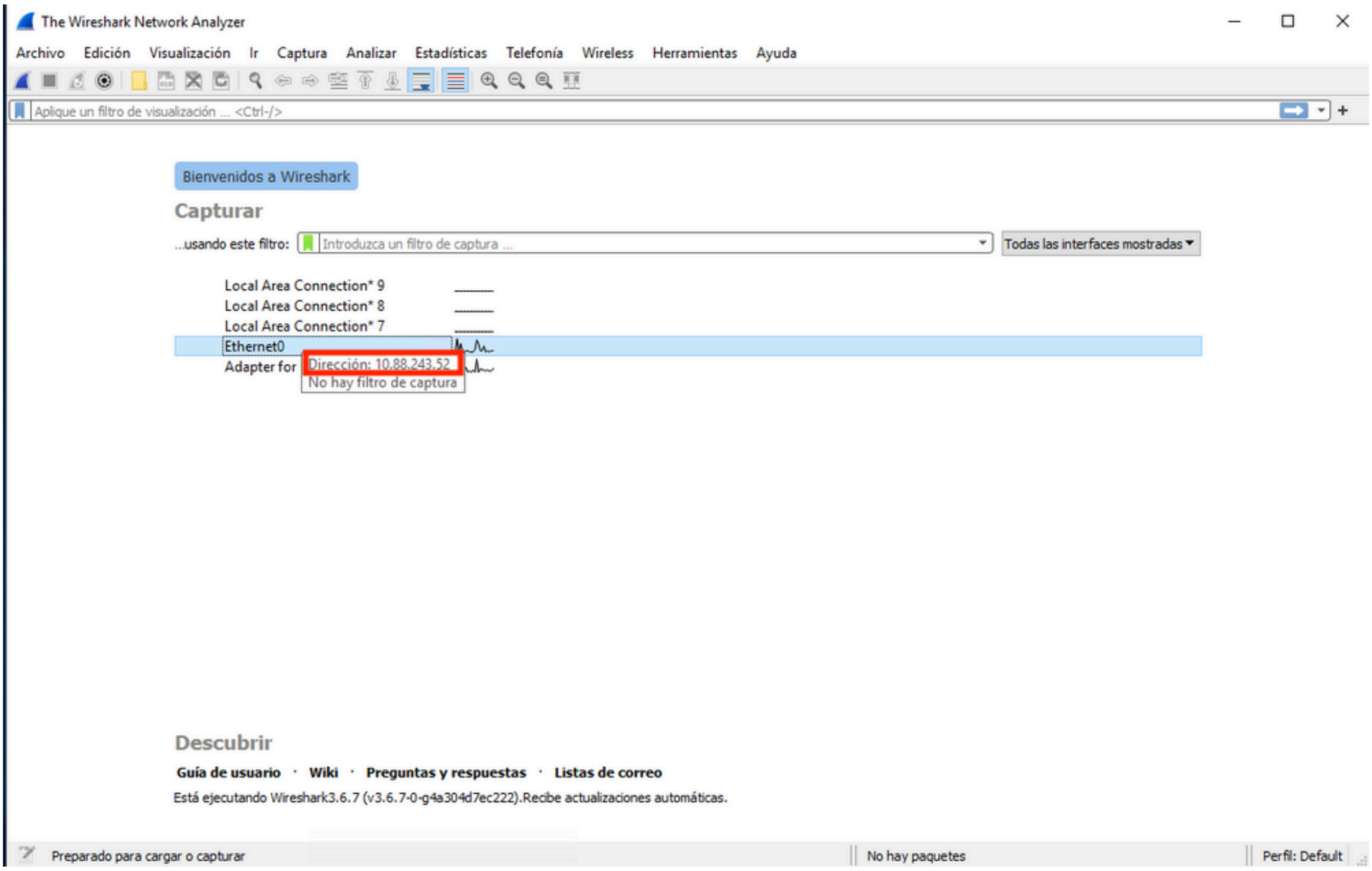


```
[> system support diagnostic-cli
 Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
 Type help or '?' for a list of available commands.

[FTD-1> en
[FTD-1> enable
[Password:
[FTD-1#
 FTD-1#
```

步驟2.為udp 514建立一個資料包捕獲（如果使用tcp，則為tcp 1468）

步驟3.驗證通訊是否與Syslog伺服器上的網路介面卡進行通訊。使用Wireshark或載入的其他資料包捕獲實用程式。按兩下Wireshark中的介面，讓系統日誌伺服器開始捕獲資料包。


The Wireshark Network Analyzer
Archivo
Edición
Visualización
Ir
Captura
Analizar
Estadísticas
Telefonía
Wireless
Herramientas
Ayuda
Aplique un filtro de visualización ... <Ctrl-/>
Bienvenidos a Wireshark
Capturar
...usando este filtro:
Introduzca un filtro de captura ...
Todas las interfaces mostradas
Descubrir
Guía de usuario · Wiki · Preguntas y respuestas · Listas de correo

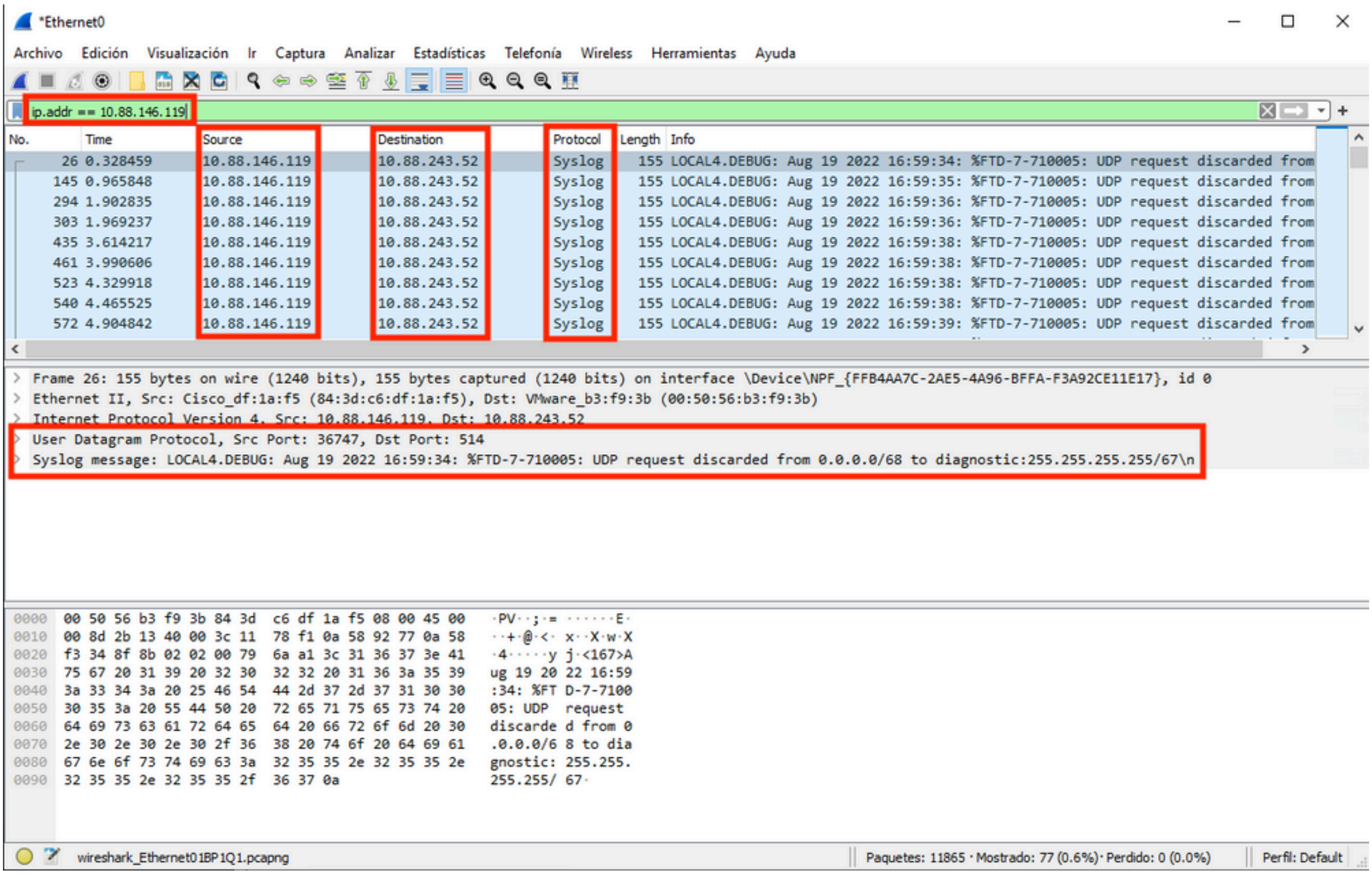
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 7
Ethernet0
Adapter for

Dirección: 10.88.243.52
No hay filtro de captura

Está ejecutando Wireshark3.6.7 (v3.6.7-0-g4a304d7ec222).Recibe actualizaciones automáticas.

Preparado para cargar o capturar | No hay paquetes | Perfil: Default

步驟4.鍵入udp.port==514並選擇該欄右側的箭頭，在頂部欄中為udp 514設定顯示過濾器。從輸出中，確認資料包是否進入系統日誌伺服器。



*Ethernet0
Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

```
ip.addr == 10.88.146.119
```

```
No.   Time      Source         Destination    Protocol Length Info
  26 0.328459  10.88.146.119  10.88.243.52   Syslog    155 LOCAL4.DEBUG: Aug 19 2022 16:59:34: %FTD-7-710005: UDP request discarded from
 145 0.965848  10.88.146.119  10.88.243.52   Syslog    155 LOCAL4.DEBUG: Aug 19 2022 16:59:35: %FTD-7-710005: UDP request discarded from
 294 1.902835  10.88.146.119  10.88.243.52   Syslog    155 LOCAL4.DEBUG: Aug 19 2022 16:59:36: %FTD-7-710005: UDP request discarded from
 303 1.969237  10.88.146.119  10.88.243.52   Syslog    155 LOCAL4.DEBUG: Aug 19 2022 16:59:36: %FTD-7-710005: UDP request discarded from
 435 3.614217  10.88.146.119  10.88.243.52   Syslog    155 LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7-710005: UDP request discarded from
 461 3.990606  10.88.146.119  10.88.243.52   Syslog    155 LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7-710005: UDP request discarded from
 523 4.329918  10.88.146.119  10.88.243.52   Syslog    155 LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7-710005: UDP request discarded from
 540 4.465525  10.88.146.119  10.88.243.52   Syslog    155 LOCAL4.DEBUG: Aug 19 2022 16:59:38: %FTD-7-710005: UDP request discarded from
 572 4.904842  10.88.146.119  10.88.243.52   Syslog    155 LOCAL4.DEBUG: Aug 19 2022 16:59:39: %FTD-7-710005: UDP request discarded from
```

```
> Frame 26: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits) on interface \Device\NPF_{FFB4AA7C-2AE5-4A96-BFFA-F3A92CE11E17}, id 0
> Ethernet II, Src: Cisco_df:1a:f5 (84:3d:c6:df:1a:f5), Dst: VMware_b3:f9:3b (00:50:56:b3:f9:3b)
> Internet Protocol Version 4, Src: 10.88.146.119, Dst: 10.88.243.52
> User Datagram Protocol, Src Port: 36747, Dst Port: 514
> Syslog message: LOCAL4.DEBUG: Aug 19 2022 16:59:34: %FTD-7-710005: UDP request discarded from 0.0.0.0/68 to diagnostic:255.255.255.255/67\n
```

```
0000  00 50 56 b3 f9 3b 84 3d  c6 df 1a f5 08 00 45 00   ·PV··;·= ······E·
0010  00 8d 2b 13 40 00 3c 11  78 f1 0a 58 92 77 0a 58   ··+·@·<· x··X·w·X
0020  f3 34 8f 8b 02 02 00 79  6a a1 3c 31 36 37 3e 41   ·4·····y j·<167>A
0030  75 67 20 31 39 20 32 30  32 32 20 31 36 3a 35 39   ug 19 20 22 16:59
0040  3a 33 34 3a 20 25 46 54  44 2d 37 2d 37 31 30 30   :34: %FT D-7-7100
0050  30 35 3a 20 55 44 50 20  72 65 71 75 65 73 74 20   05: UDP  request
0060  64 69 73 63 61 72 64 65  64 20 66 72 6f 6d 20 30   discarde d from 0
0070  2e 30 2e 30 2e 30 2f 36  38 20 74 6f 20 64 69 61   .0.0.0/6 8 to dia
0080  67 6e 6f 73 74 69 63 3a  32 35 35 2e 32 35 35 2e   gnostic: 255.255.
0090  32 35 35 2e 32 35 35 2f  36 37 0a                  255.255/ 67·
```

wireshark_Ethernet01BP1Q1.pcapng
Paquetes: 11865 · Mostrado: 77 (0.6%) · Perdido: 0 (0.0%)
Perfil: Default

步驟5.如果Syslog伺服器應用程式未顯示資料，請排除Syslog伺服器應用程式中的設定故障。確保使用的是正確的udp/tcp協定和正確的埠514/1468。

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）。