

Firepower Device Manager(FDM)でのSyslogの設定と確認

内容

[概要](#)

[前提条件](#)

[要件](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、Firepower Device Manager(FDM)内でSyslogを設定する方法について説明します。

前提条件

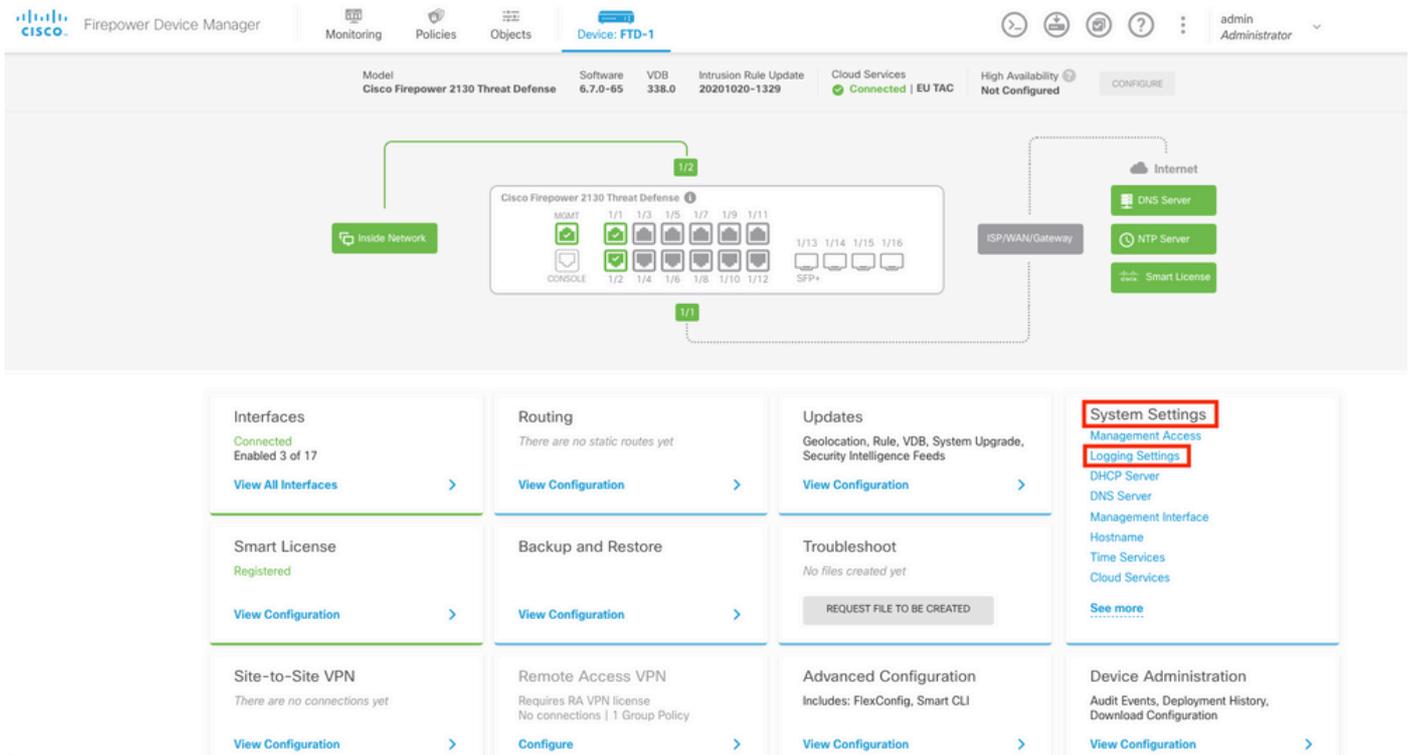
要件

次の項目に関する知識があることが推奨されます。

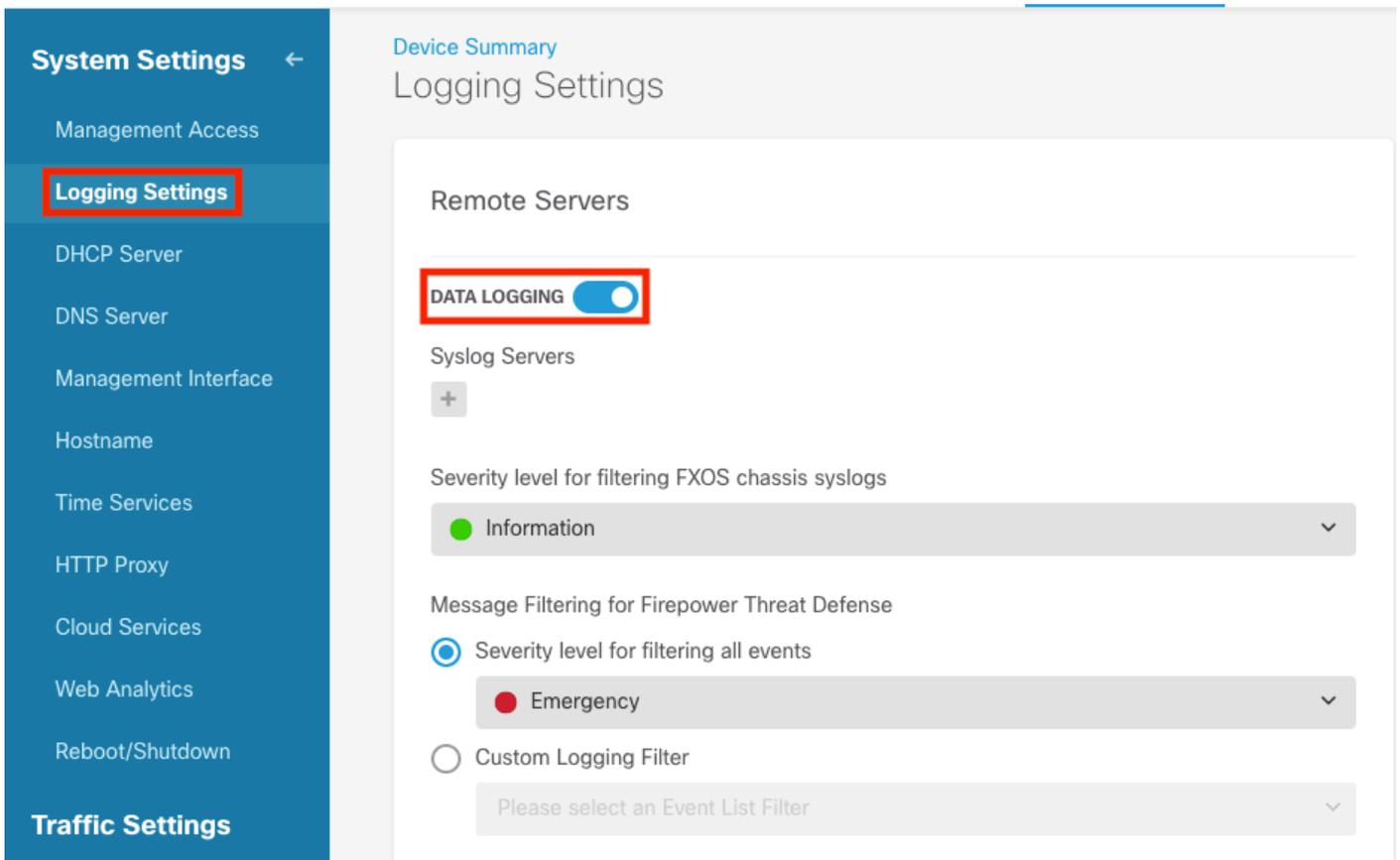
- Firepower脅威防御
- Syslogソフトウェアを実行してデータを収集するSyslogサーバ

設定

ステップ 1 : Firepowerデバイスマネージャのメイン画面から、画面の右下隅にある[System Settings]の下の[Logging Settings]を選択します。



ステップ 2 : [System Settings]画面で、左側のメニューから[Logging Settings]を選択します。



ステップ 3 : Syslog Serversの下の+記号を選択して、Data Loggingトグルスイッチを設定します。

ステップ 4 : [Add Syslog Server]を選択します。または、[Objects] - [Syslog Servers]でSyslog Serverオブジェクトを作成することもできます。

Logging Settings

Remote Servers

DATA LOGGING

Syslog Servers



Filter

Nothing found

[Create new Syslog Server](#)

CANCEL

OK

Please select an Event List Filter

ステップ 5 : SyslogサーバのIPアドレスとポート番号を入力します。Data Interfaceのオプションボタンを選択し、OKを選択します。

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.

i 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

CANCEL

OK

手順 6 : 次に、新しいSyslogサーバを選択し、[OK]を選択します。

Syslog Servers



Filter

<input checked="" type="checkbox"/>		10.88.243.52	
-------------------------------------	--	--------------	--

[Create new Syslog Server](#) CANCEL OK

手順 7 : [Severity level for filtering all events]オプションボタンを選択し、必要なログレベルを選択します。

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

ステップ 8 : 画面の下部にある[Save]を選択します。

SAVE

ステップ 9 : 設定が正常に行われたことを確認します。

Device Summary

Logging Settings

✔ Successfully saved logging settings.

ステップ 10 : 新しい設定を展開します。



および

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	LEGEND
Access Rule Edited: <i>Inside_Outside_Rule</i>		
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: <i>Device-Log-Settings</i>		
syslogServerLogFilter.dataLogging.loggingEnabled: true	true	
syslogServerLogFilter.dataLogging.platformLogLevel: INFORMATIONAL	INFORMATIONAL	
-	syslogServerLogFilter.fileMalwareLogging.loggingEn: true	
-	syslogServerLogFilter.fileMalwareLogging.severityL: true	
syslogServerLogFilter.dataLogging.syslogServers:		
-	172.16.1.250:514	
Access Policy Edited: <i>NGFW-Access-Policy</i>		

MORE ACTIONS ▾

CANCEL

DEPLOY NOW ▾

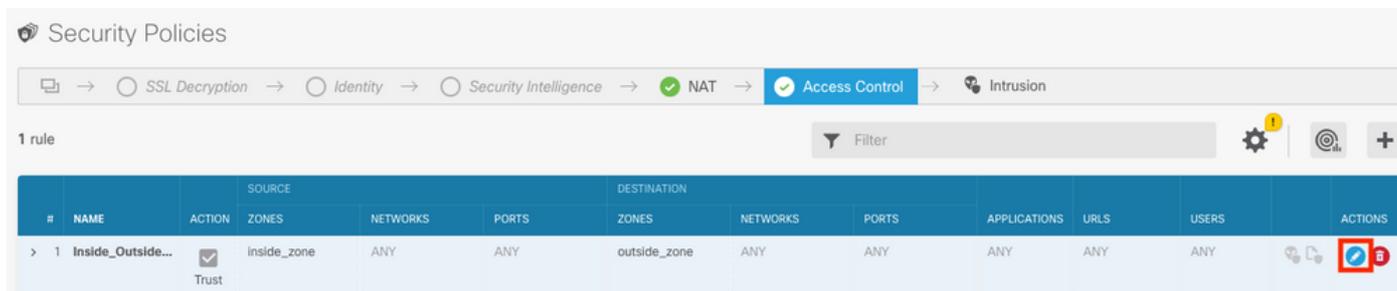
オプション。

さらに、Syslogサーバにログインするようにアクセスコントロールポリシーのアクセスコントロールルールを設定できます。

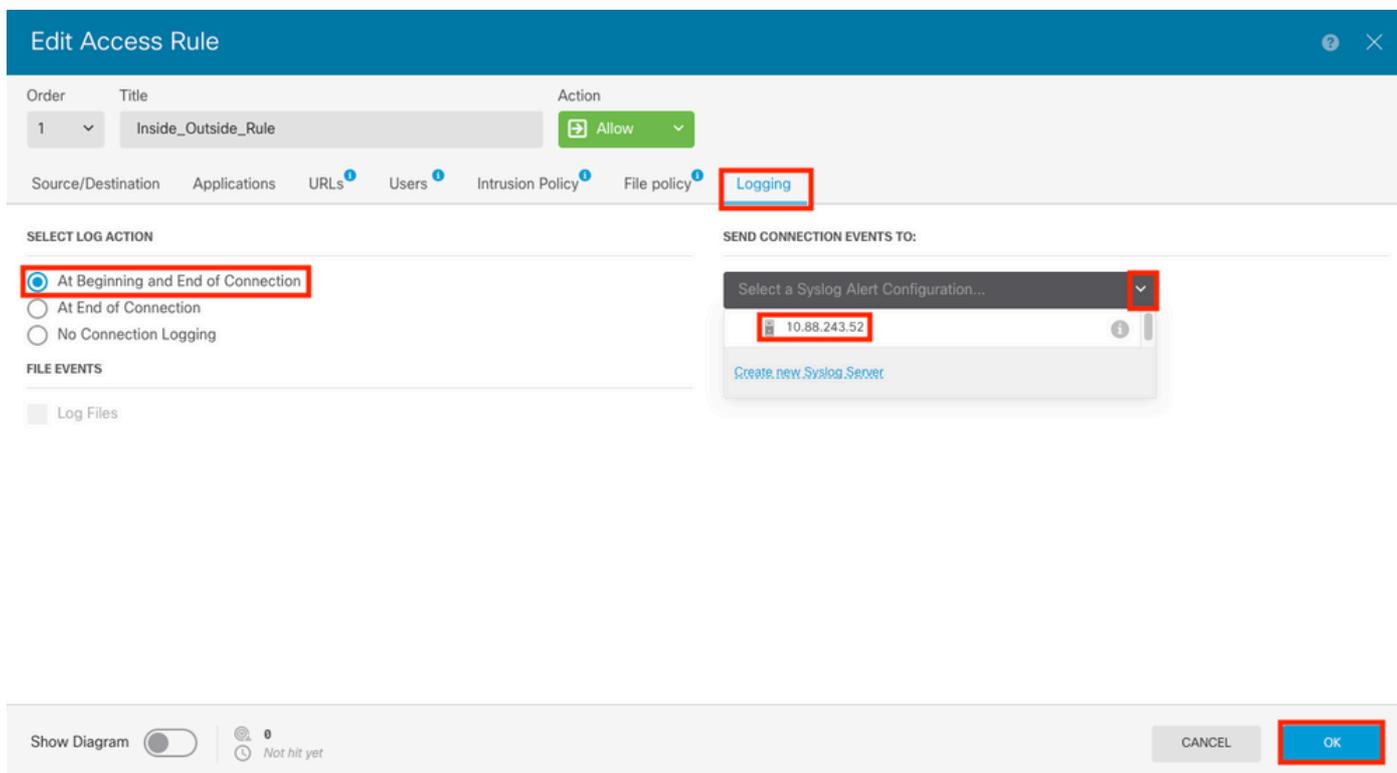
ステップ 1：画面上部の[Policies]ボタンをクリックします。



ステップ 2：ACPルールの右側にマウスを移動して、ロギングを追加し、鉛筆アイコンを選択します。



ステップ 3：[Logging]タブを選択し、[At End of Connection]のオプションボタンを選択し、[Select a Syslog Alert Configuration]の下のドロップダウン矢印を選択し、Syslogサーバでを選択して、[OK]を選択します。



ステップ 4：設定の変更を導入します。

確認

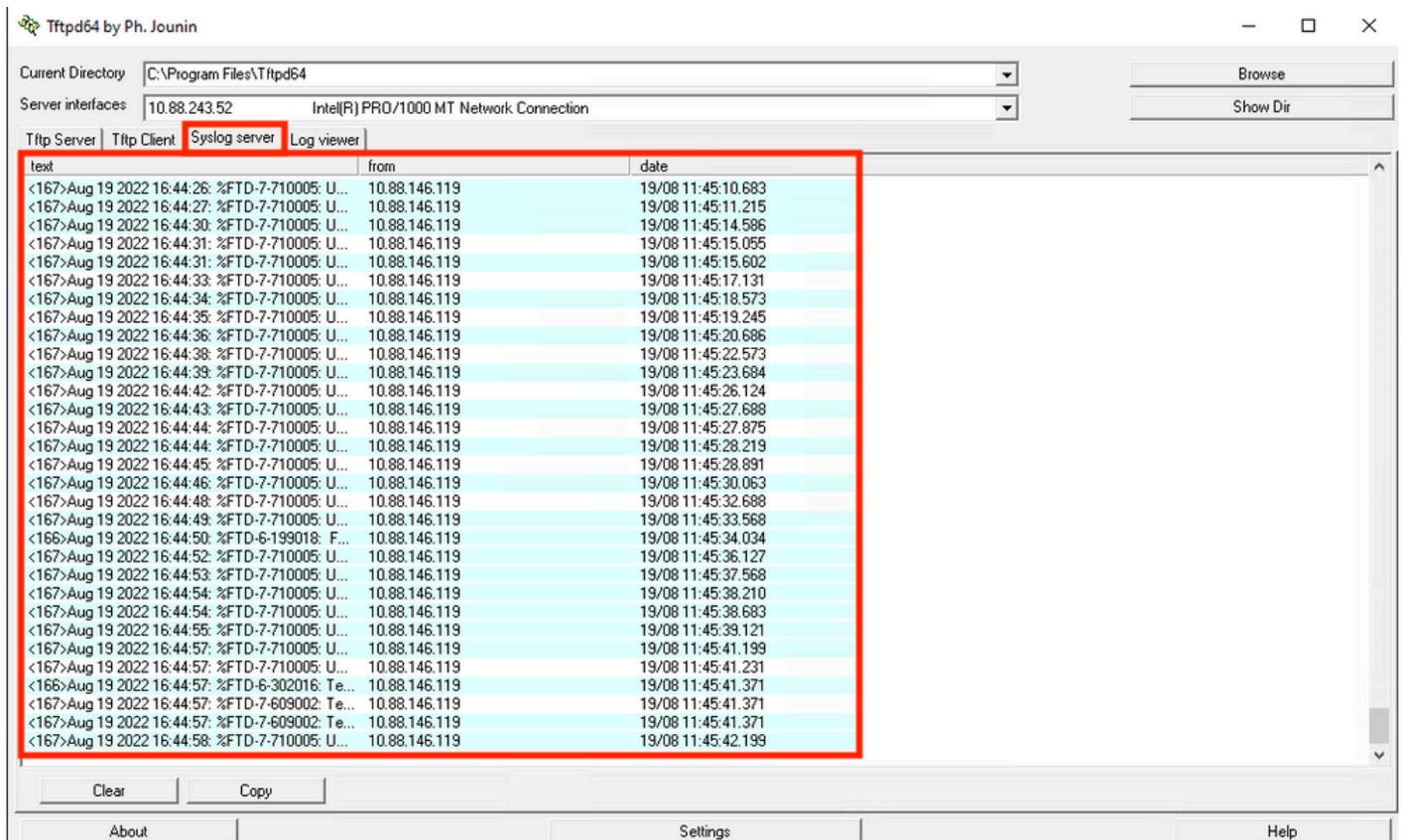
ステップ 1: タスクが完了したら、show running-config logging コマンドを使用して、FTD CLI のクリックモードの設定を確認できます。

```
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
>
```

ステップ 2: Syslog サーバに移動し、Syslog サーバアプリケーションが Syslog メッセージを受け入れていることを確認します。



トラブルシューティング

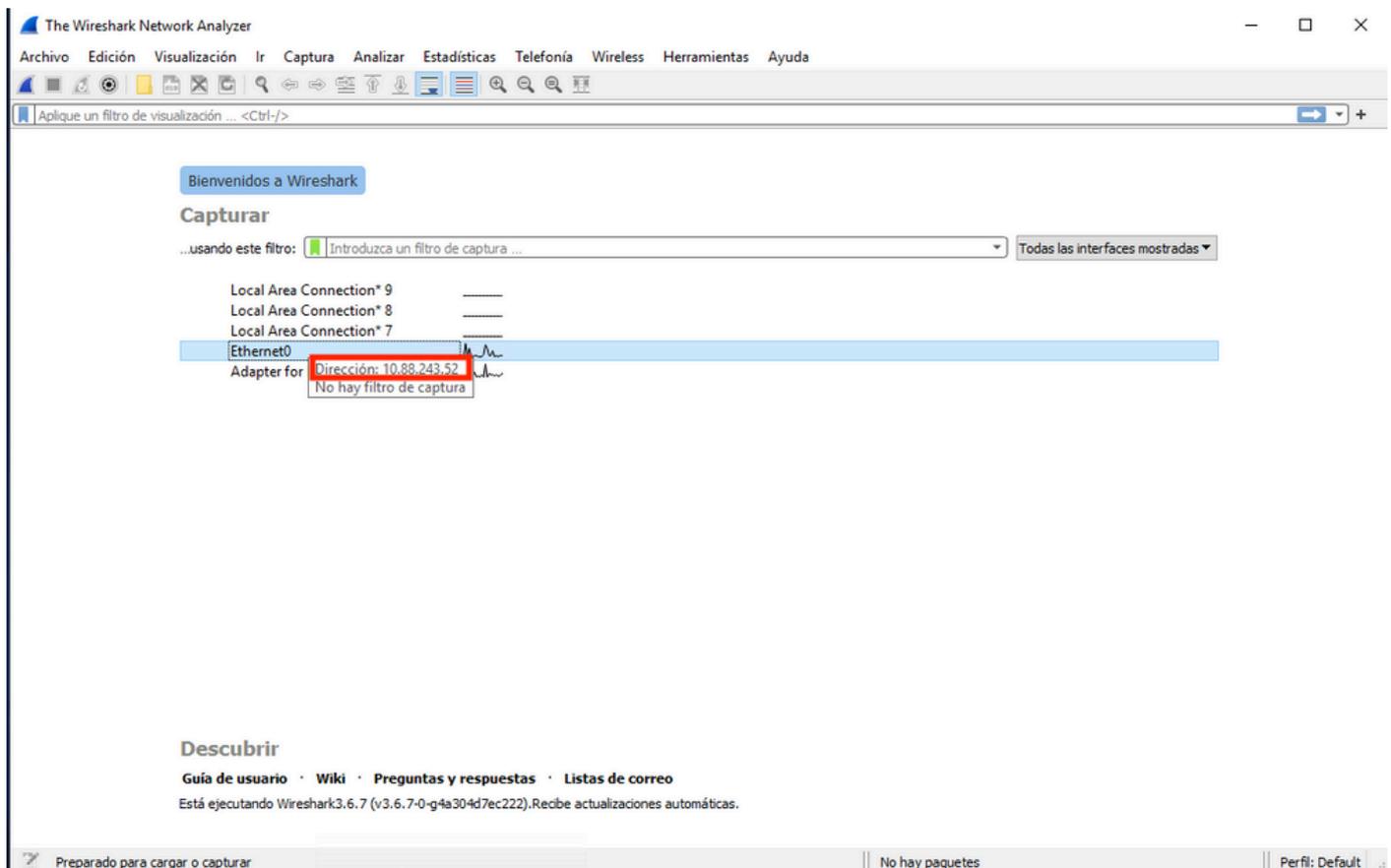
ステップ 1 : SyslogアプリケーションのSyslogメッセージで何らかのメッセージが生成された場合は、FTD CLIからパケットキャプチャを実行してパケットを確認します。clishプロンプトでsystem support diagnostic-cliコマンドを入力して、ClishモードからLINAに変更します。

```
[> 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#
```

ステップ 2 : udp 514 (tcpを使用している場合はtcp 1468) 用に1つのパケットキャプチャを作成します

ステップ 3 : 通信がSyslogサーバのネットワークインターフェイスカード(NIC)に到達していることを確認します。ロードされたWiresharkまたは別のパケットキャプチャユーティリティを使用します。SyslogサーバのWiresharkのインターフェイスをダブルクリックして、パケットのキャプチャを開始します。



ステップ 4 : udp.port==514と入力し、バーの右側にある矢印を選択して、udp 514の上部バーに表示フィルタを設定します。出力から、パケットがSyslogサーバに送信されているかどうかを確認します。

*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

ステップ 5 : Syslogサーバアプリケーションにデータが表示されない場合は、Syslogサーバアプリケーション内の設定をトラブルシューティングします。正しいプロトコルがudp/tcpと正しいポート514/1468で使用されていることを確認します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。