

Configuration et vérification de Syslog dans le Gestionnaire de périphériques Firepower

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Configurations](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer Syslog dans Firepower Device Manager (FDM).

Conditions préalables

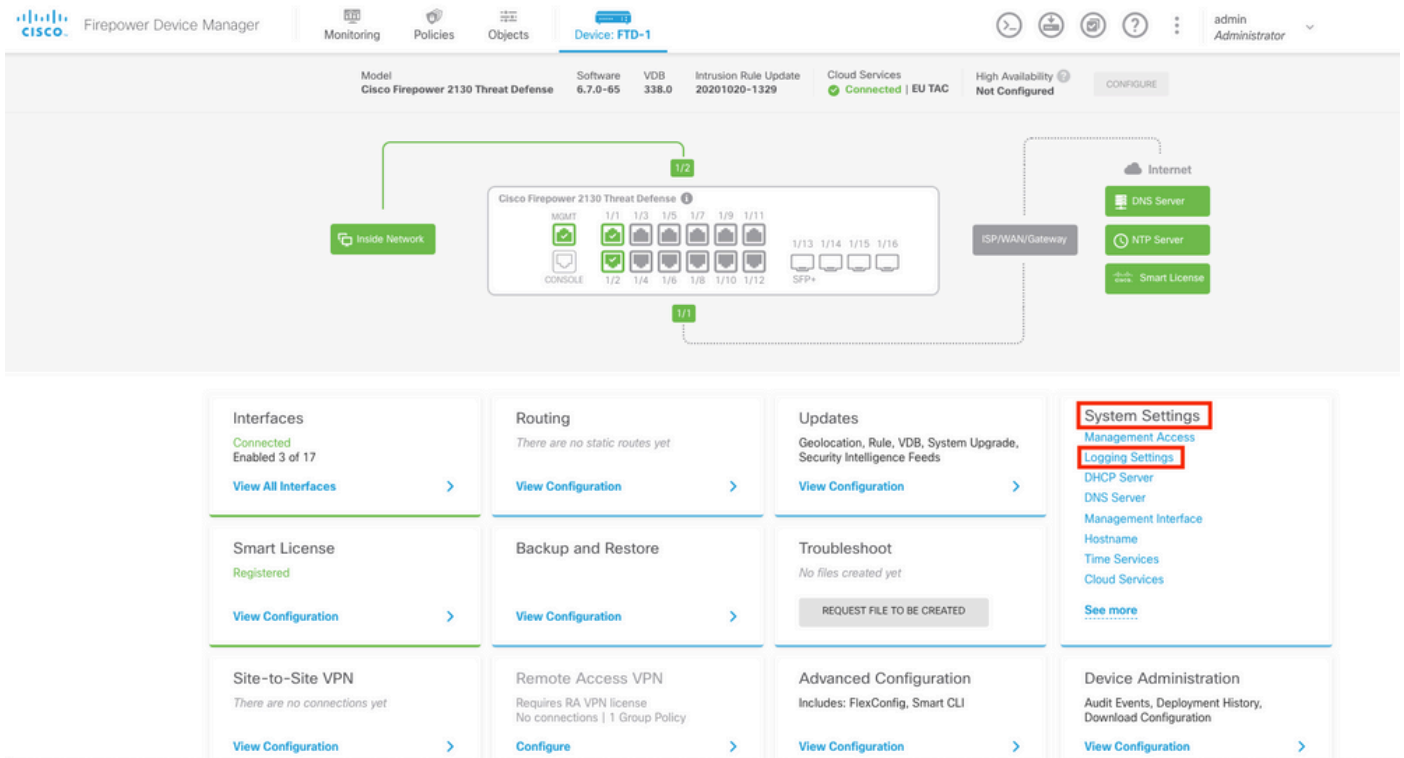
Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

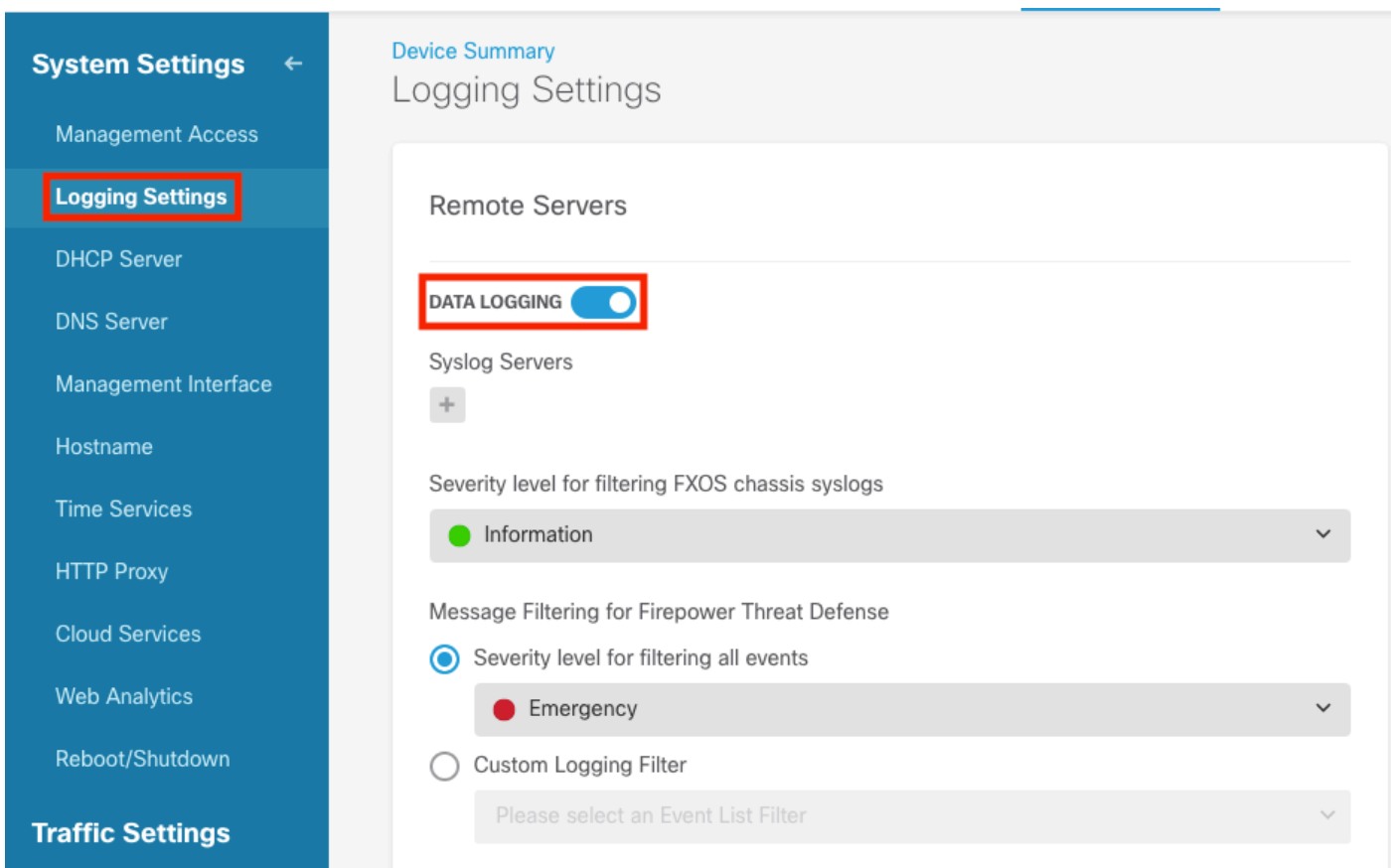
- Firepower Threat Defense
- Serveur Syslog exécutant le logiciel Syslog pour collecter des données

Configurations

Étape 1. Dans l'écran Main Firepower Device Manager (Gestionnaire principal de périphériques Firepower), sélectionnez Logging Settings (Paramètres de journalisation) sous System Settings (Paramètres système) dans le coin inférieur droit de l'écran.

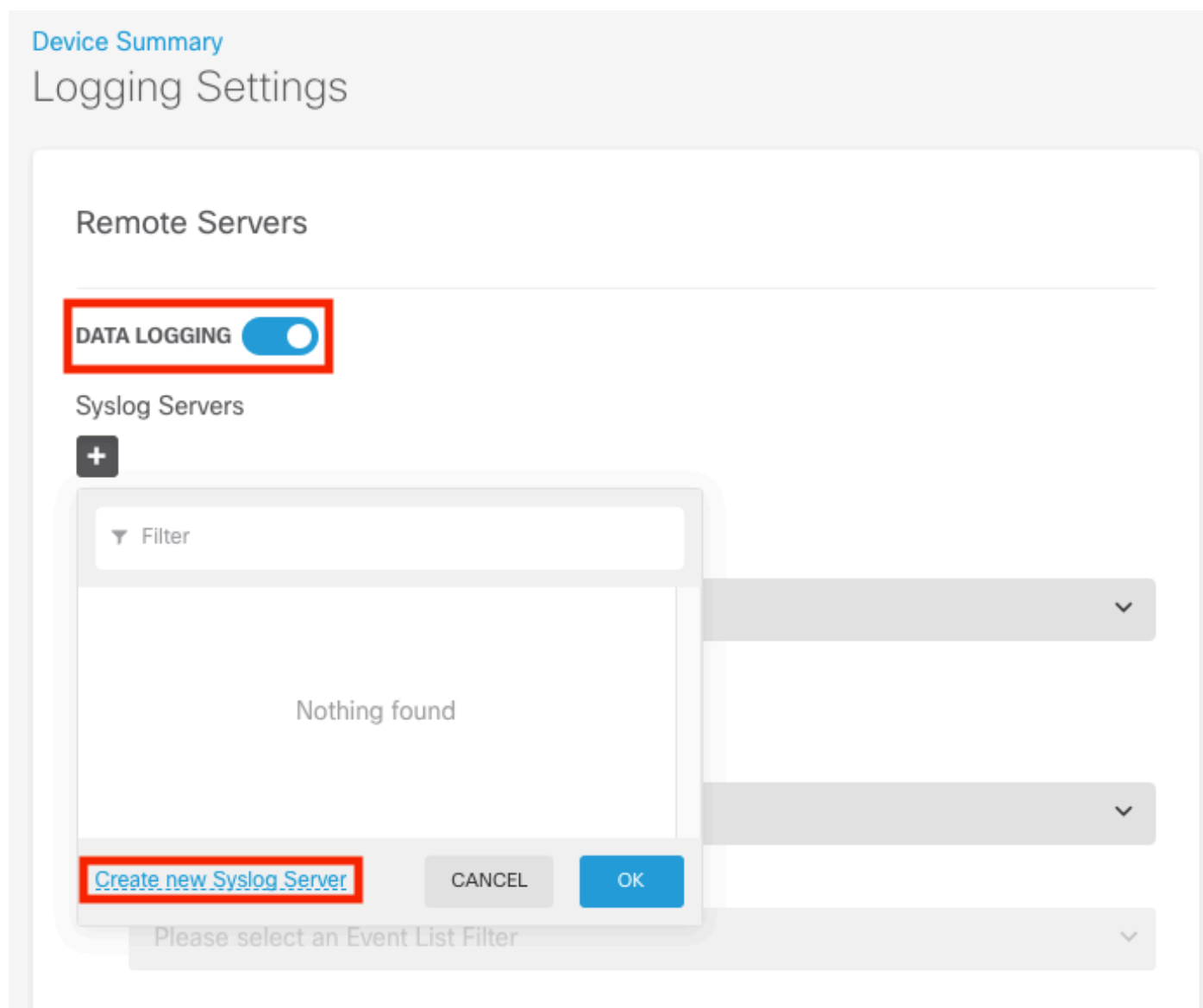


Étape 2. Dans l'écran System Settings (Paramètres système), sélectionnez Logging Settings (Paramètres de journalisation) dans le menu de gauche.



Étape 3. Définissez le commutateur à bascule Journalisation des données en sélectionnant le signe + sous Serveurs Syslog.

Étape 4. Sélectionnez Ajouter un serveur Syslog. Vous pouvez également créer l'objet Serveur



Étape 5. Saisissez l'adresse IP de votre serveur Syslog et le numéro de port. Sélectionnez la case d'option Interface de données, puis cliquez sur OK.

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

Étape 6. Sélectionnez ensuite le nouveau serveur Syslog, puis cliquez sur OK.

Syslog Servers



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

[Create new Syslog Server](#)

Étape 7. Sélectionnez la case d'option Niveau de gravité pour le filtrage de tous les événements et sélectionnez le niveau de journalisation souhaité.

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

Étape 8. Sélectionnez Enregistrer en bas de l'écran.

SAVE

Étape 9. Vérifiez que les paramètres ont réussi.

Device Summary

Logging Settings

✔ **Successfully saved logging settings.**

Étape 10. Déployez les nouveaux paramètres.



ET

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: <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** ▾

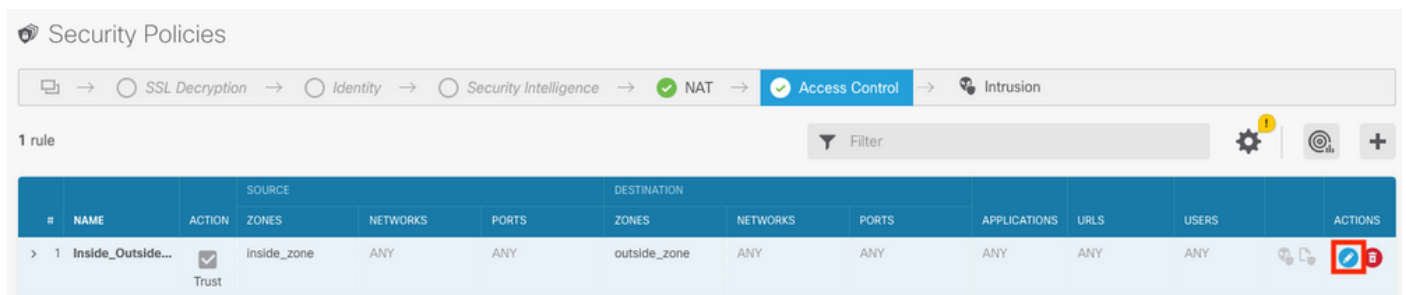
FACULTATIF.

En outre, les règles de contrôle d'accès de la stratégie de contrôle d'accès peuvent être définies pour se connecter au serveur Syslog :

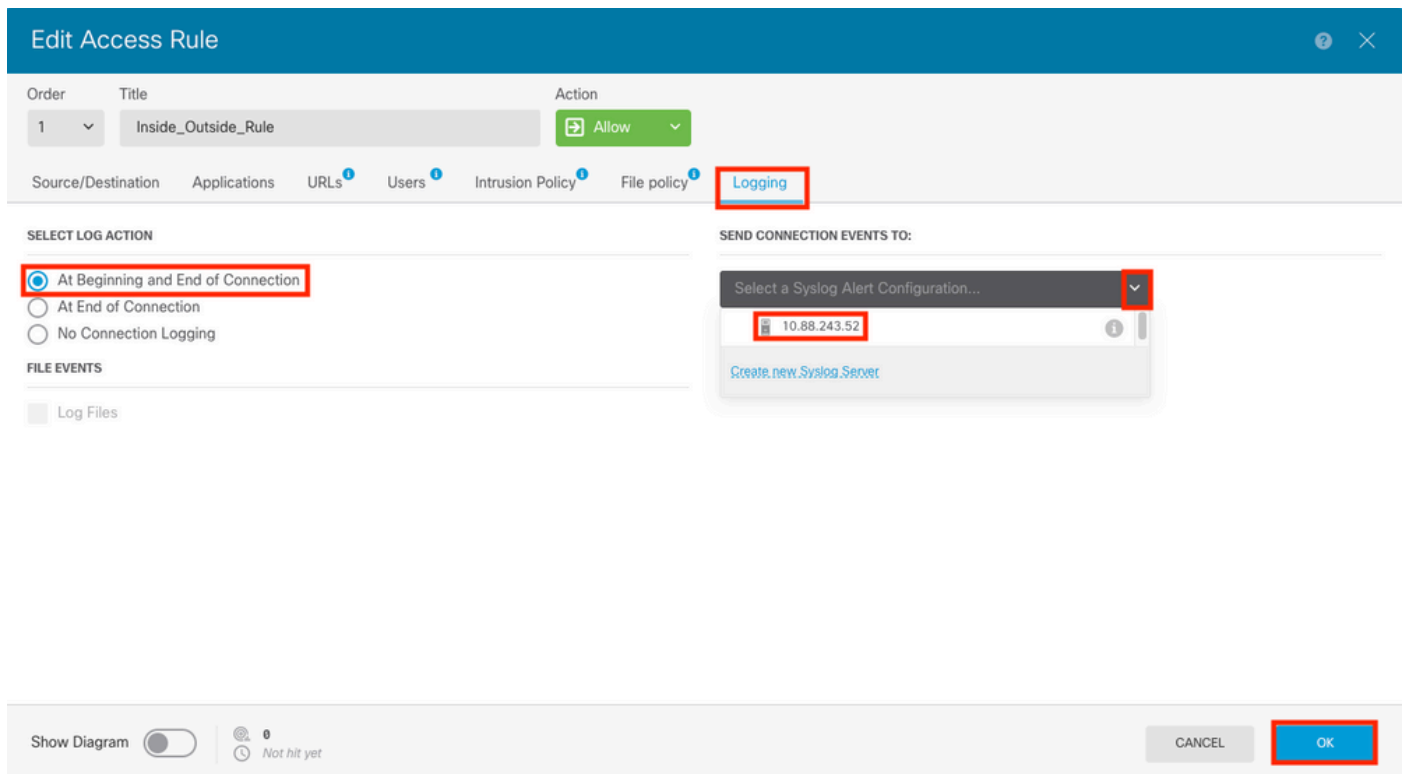
Étape 1. Cliquez sur le bouton Politiques en haut de l'écran.



Étape 2. Passez le curseur sur le côté droit de la règle ACP pour ajouter la journalisation et sélectionnez l'icône représentant un crayon.



Étape 3. Sélectionnez l'onglet Logging, sélectionnez la case d'option At End of Connection, sélectionnez la flèche de la liste déroulante sous Select a Syslog Alert Configuration, sélectionnez sur le serveur Syslog et cliquez sur OK.



Étape 4. Déployez les modifications de configuration.

Vérifier

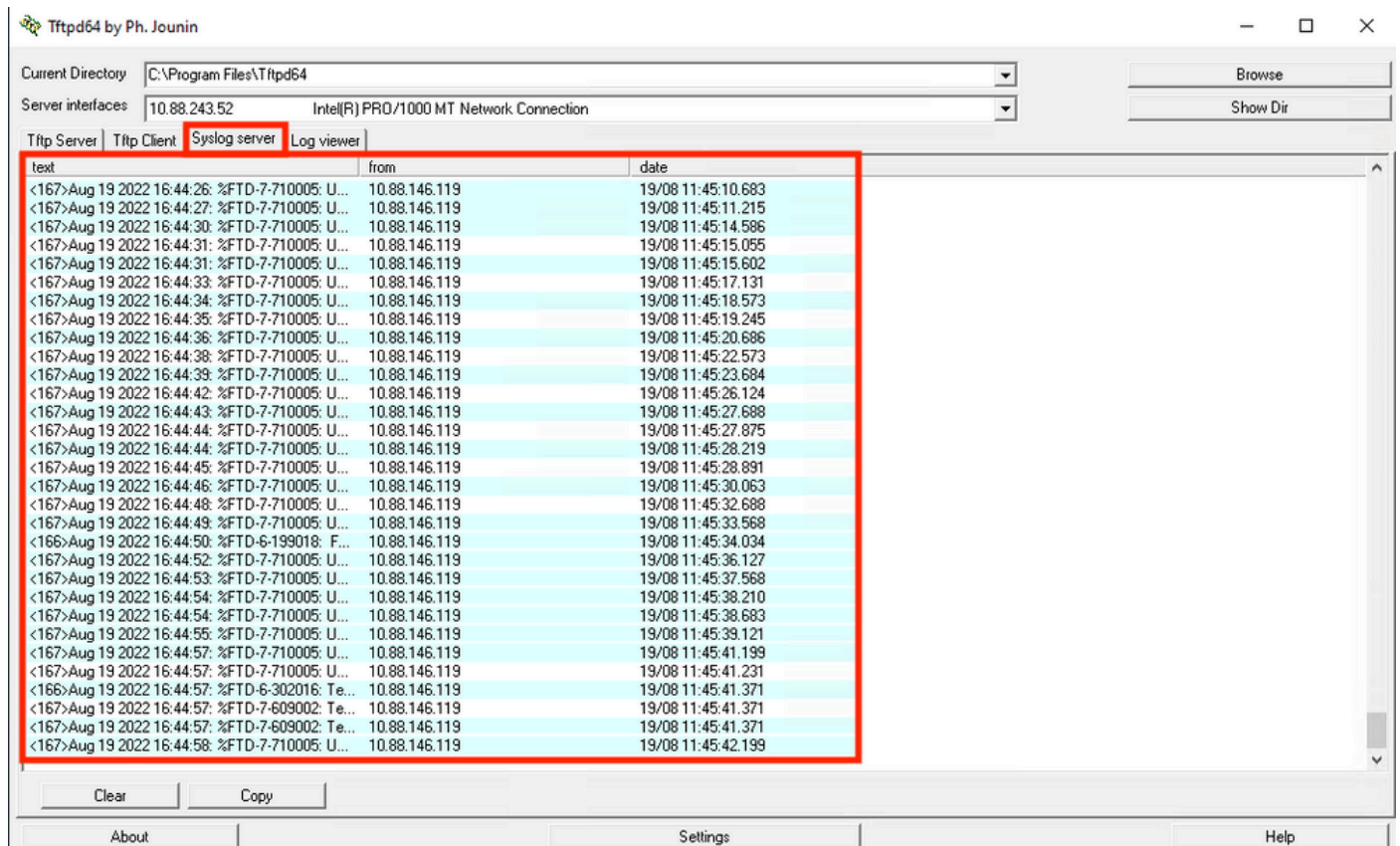
Étape 1. Une fois la tâche terminée, vous pouvez vérifier les paramètres du mode de configuration CLI FTD à l'aide de la commande show running-config logging.

```
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
>
```

Étape 2. Accédez au serveur Syslog et vérifiez que l'application du serveur Syslog accepte les messages Syslog.



Dépannage

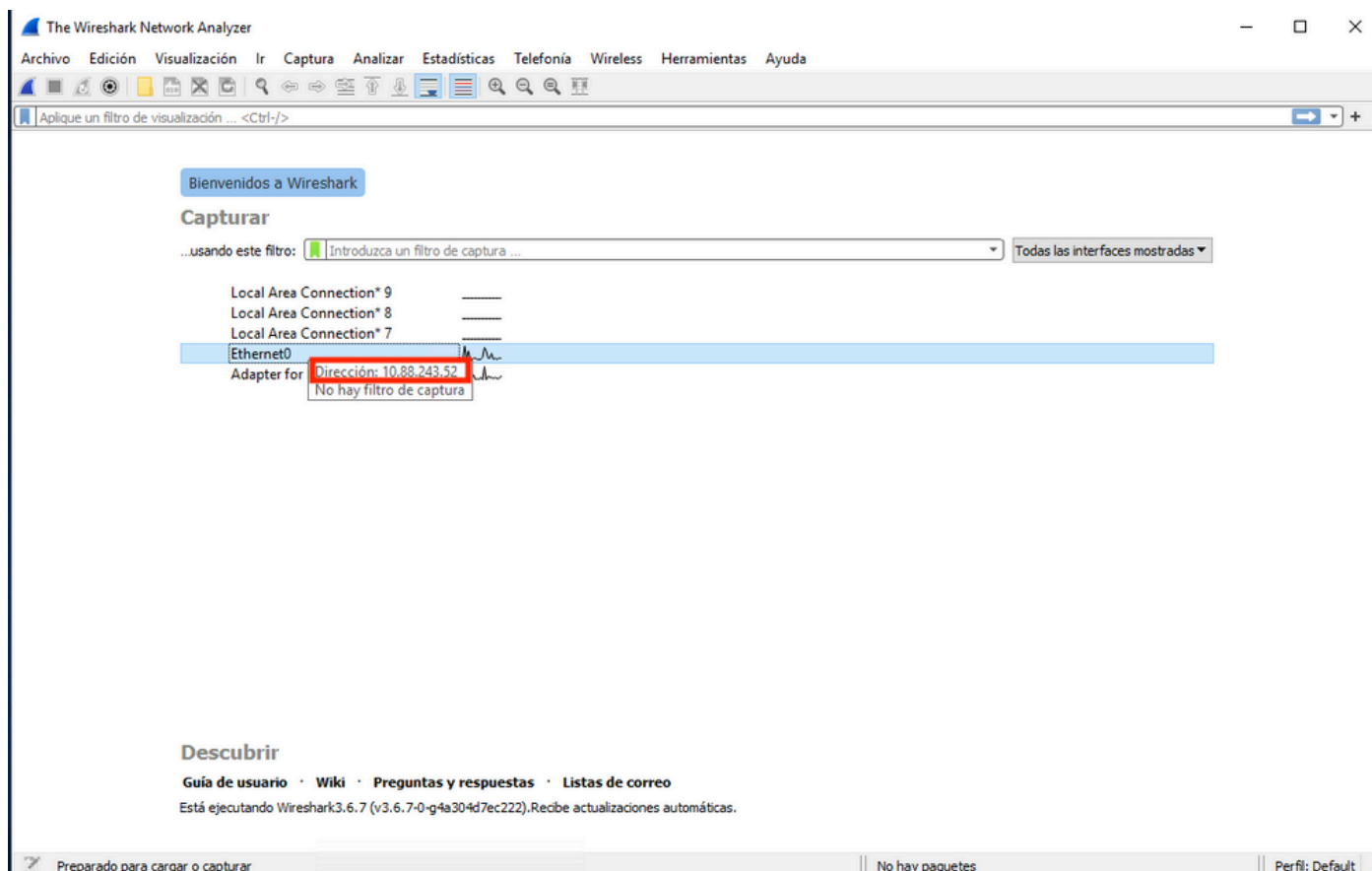
Étape 1. Si les messages Syslog de l'application Syslog produisent des messages, effectuez une capture de paquets à partir de l'interface de ligne de commande FTD pour vérifier la présence de paquets. Passez du mode Clish au mode LINA en entrant la commande **system support diagnostic-cli** à l'invite de commande clish.

```
[> 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#
```

Étape 2. Créez une capture de paquets pour votre udp 514 (ou tcp 1468 si vous avez utilisé tcp)

Étape 3. Vérifiez que la communication est établie avec la carte d'interface réseau sur le serveur Syslog. Utilisez Wireshark ou un autre utilitaire de capture de paquets chargé. Double-cliquez sur l'interface dans Wireshark pour que le serveur Syslog commence à capturer des paquets.



Étape 4. Définissez un filtre d'affichage dans la barre supérieure pour udp 514 en tapant `udp.port==514` et en sélectionnant la flèche à droite de la barre. À partir du résultat, vérifiez si les paquets sont transmis au serveur Syslog.

*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

Étape 5. Si l'application serveur Syslog n'affiche pas les données, dépannez le paramètre dans l'application serveur Syslog. Assurez-vous que le bon protocole est utilisé avec udp/tcp et le bon port 514/1468.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.