

Configuración Y Verificación De Syslog En El Administrador De Dispositivos Firepower

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar Syslog en el Administrador de dispositivos Firepower (FDM).

Prerequisites

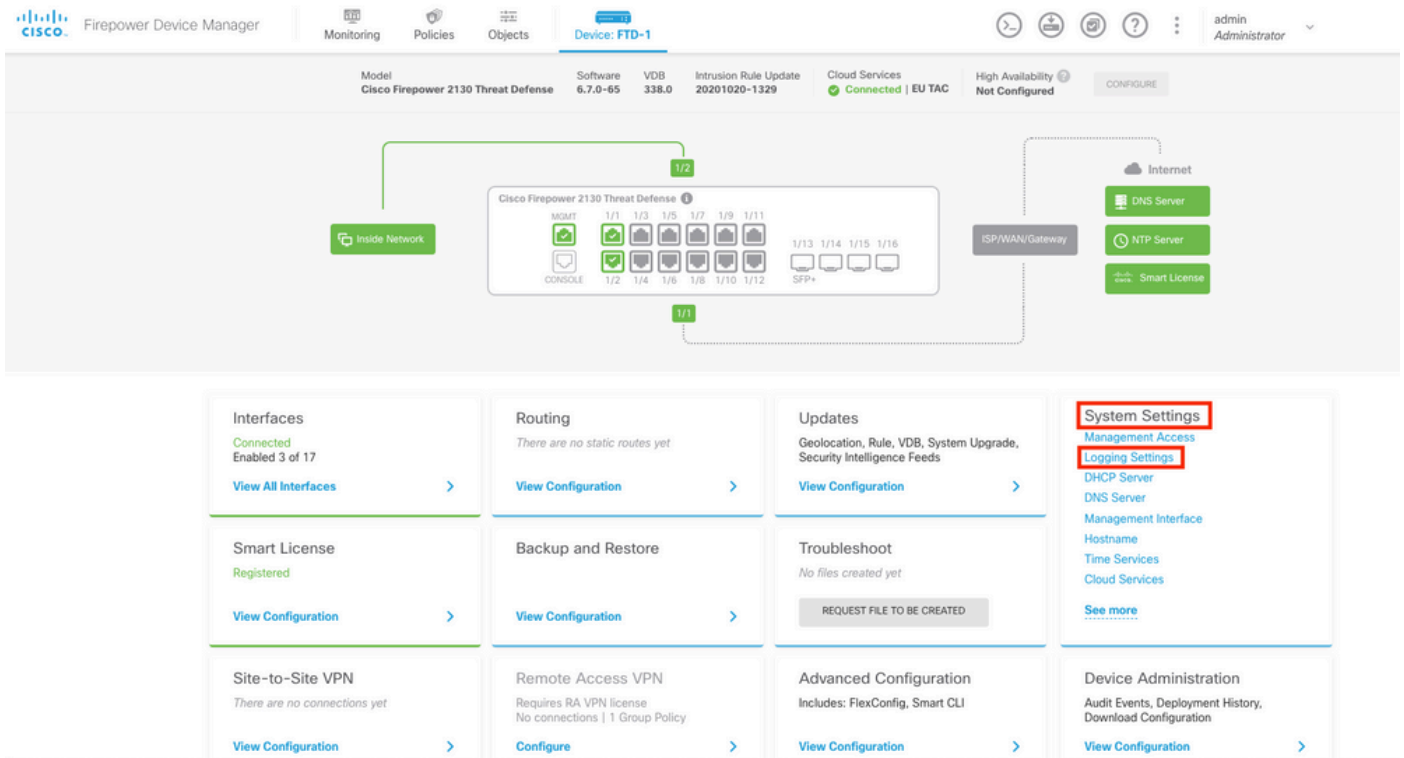
Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

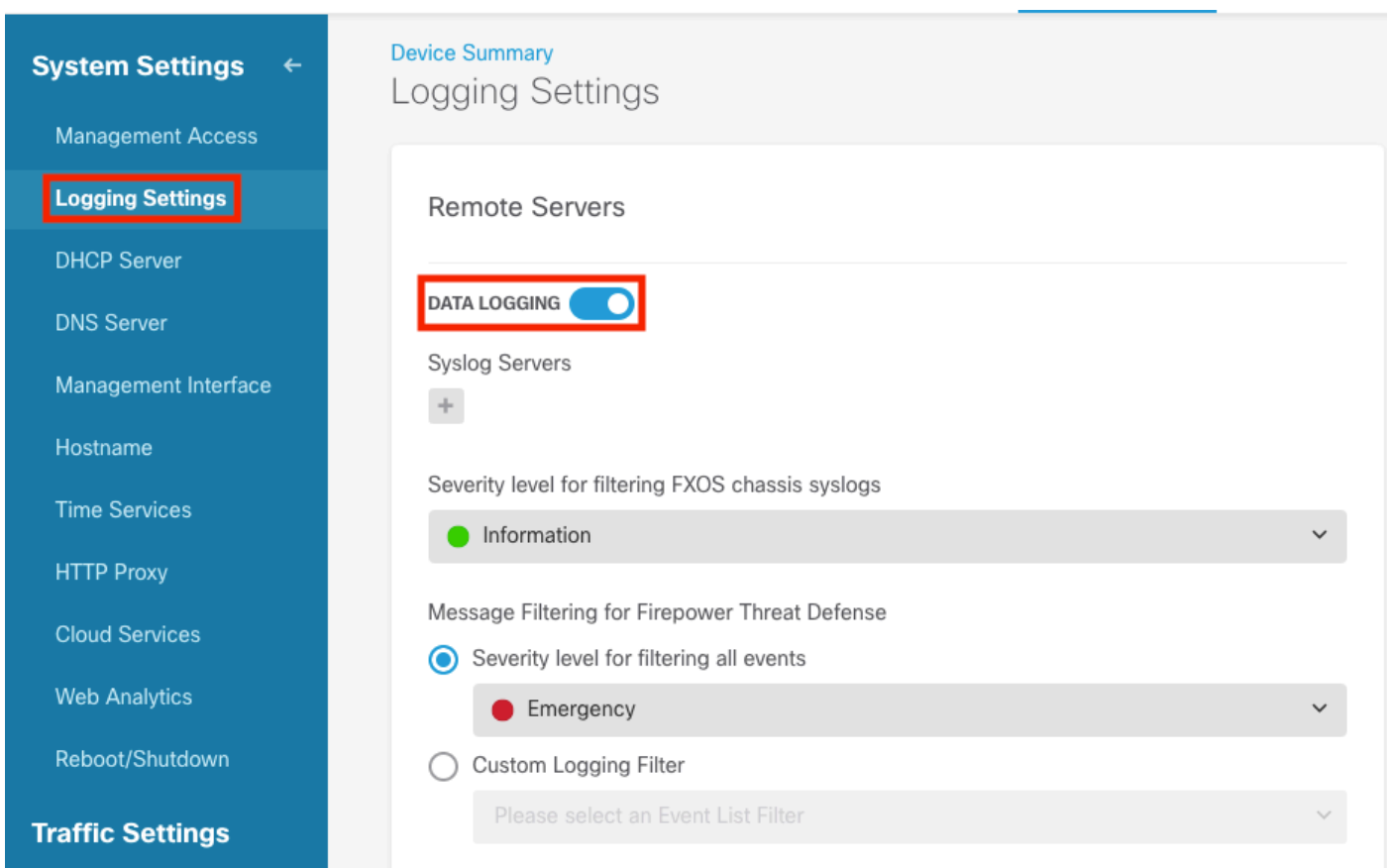
- Firepower Threat Defense
- Servidor Syslog que ejecuta el software Syslog para recopilar datos

Configuraciones

Paso 1. En la pantalla principal del administrador de dispositivos de Firepower, seleccione la configuración de registro en Configuración del sistema en la esquina inferior derecha de la pantalla.



Paso 2. En la pantalla System Settings (Parámetros del sistema), seleccione Logging Settings (Parámetros de registro) en el menú de la izquierda.



Paso 3. Establezca el interruptor de alternancia Registro de datos seleccionando el signo + en Servidores Syslog.

Paso 4. Seleccione Agregar servidor Syslog. Como alternativa, puede crear el objeto Servidor

Syslog en Objetos - Servidores Syslog.

Device Summary
Logging Settings

Remote Servers

DATA LOGGING

Syslog Servers

+

Filter

Nothing found

[Create new Syslog Server](#) CANCEL OK

Please select an Event List Filter

Paso 5. Introduzca la dirección IP del servidor Syslog y el número de puerto. Seleccione el botón de opción de Interfaz de datos y seleccione Aceptar.

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

Paso 6. A continuación, seleccione el nuevo servidor Syslog y haga clic en Aceptar.

Syslog Servers



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

[Create new Syslog Server](#) CANCEL OK

Paso 7. Seleccione el botón de opción Nivel de gravedad para filtrar todos los eventos y seleccione el nivel de registro que desee.

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

Paso 8. Seleccione Guardar en la parte inferior de la pantalla.

SAVE

Paso 9. Compruebe que la configuración se ha realizado correctamente.

Device Summary

Logging Settings

✔ **Successfully saved logging settings.**

Paso 10. Implementar la nueva configuración.



Y

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** ▾

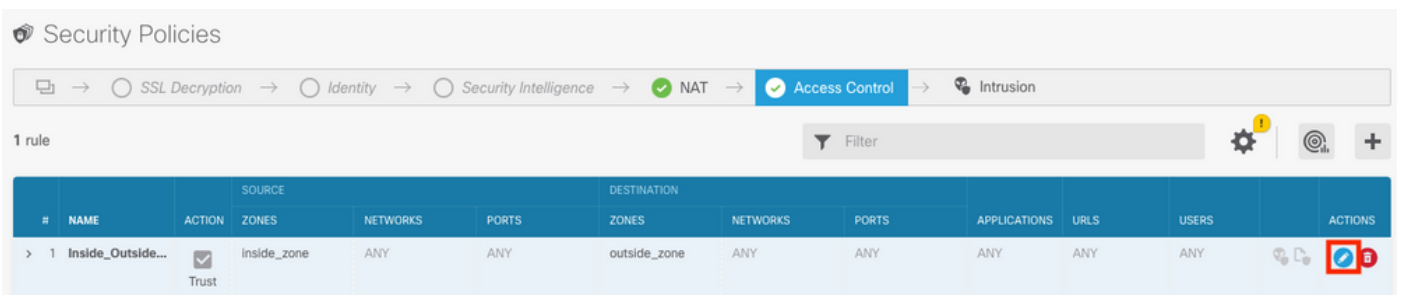
OPCIONAL.

Además, las reglas de control de acceso de la política de control de acceso se pueden configurar para iniciar sesión en el servidor Syslog:

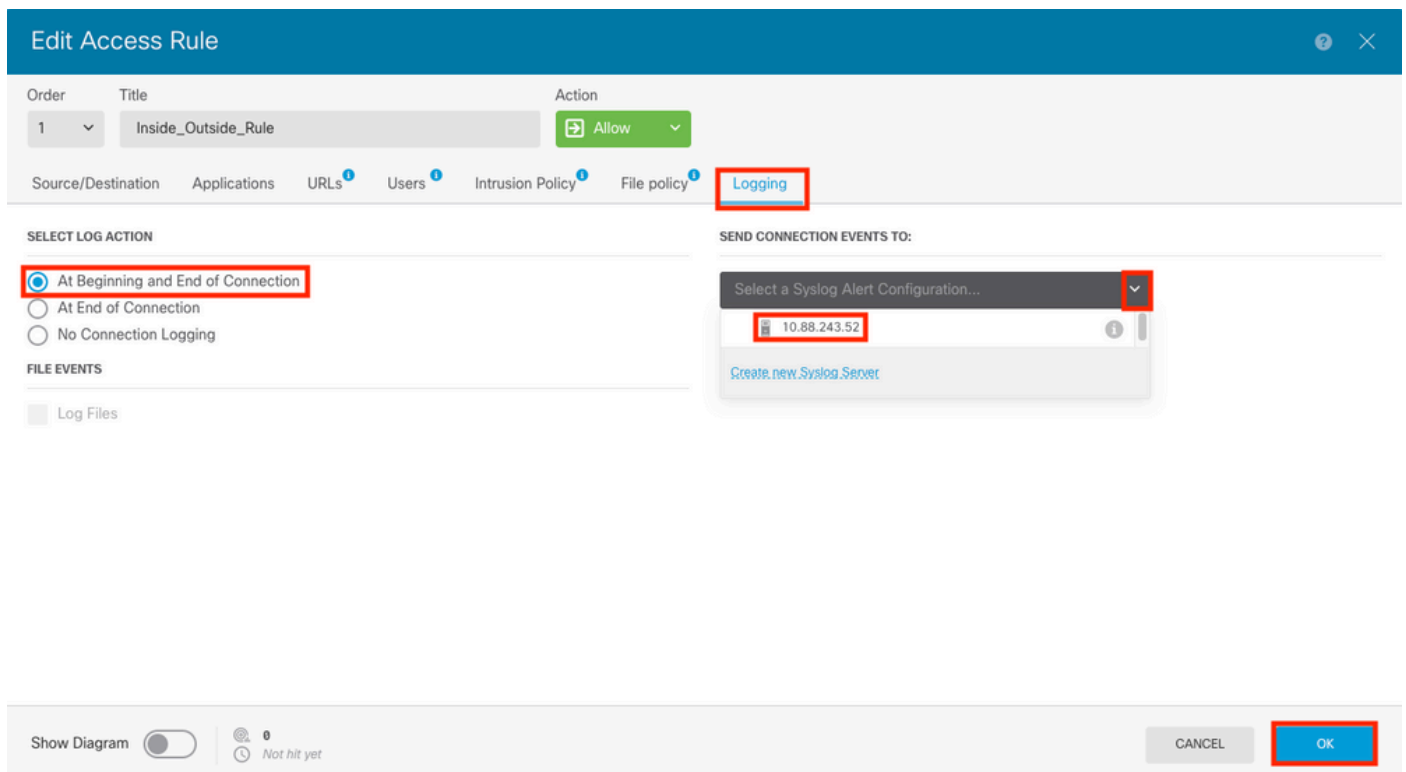
Paso 1. Haga clic en el botón Directivas situado en la parte superior de la pantalla.



Paso 2. Pase el ratón sobre el lado derecho de la regla ACP para agregar el registro y seleccione el icono del lápiz.



Paso 3. Seleccione la ficha Logging (Registro), seleccione el botón de opción At End of Connection (Al final de la conexión), seleccione la flecha desplegable bajo Select a Syslog Alert Configuration (Seleccionar una configuración de alerta de registro del sistema), Select on the Syslog Server (Seleccionar en el servidor de registro del sistema) y Select OK (Aceptar).



Paso 4. Implemente los cambios de configuración.

Verificación

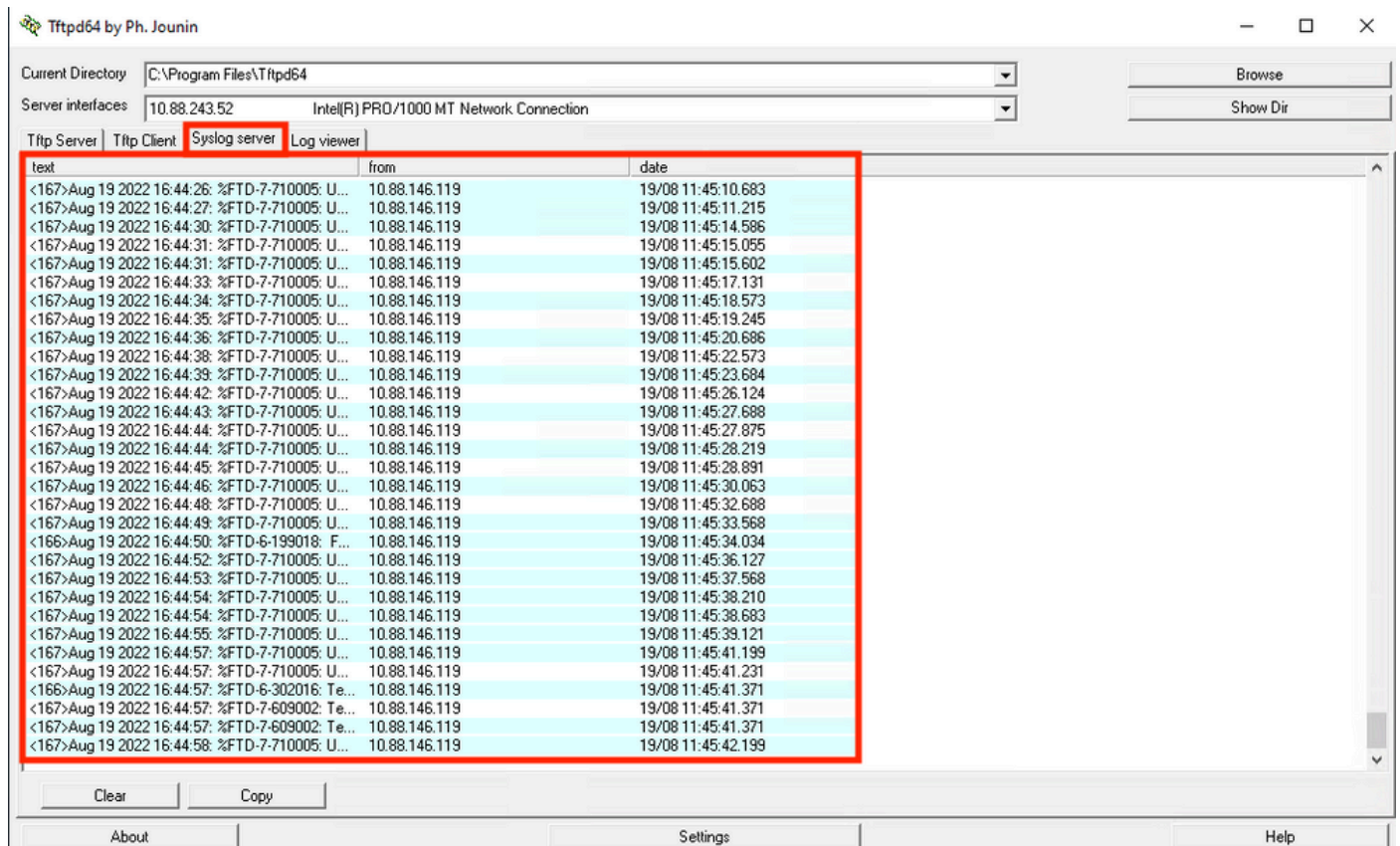
Paso 1. Una vez completada la tarea, puede verificar la configuración en el modo de suspensión CLI de FTD mediante el comando show running-config logging.

```
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
>
```

Paso 2. Desplácese hasta el servidor Syslog y compruebe que la aplicación del servidor Syslog acepta mensajes de Syslog.



Troubleshoot

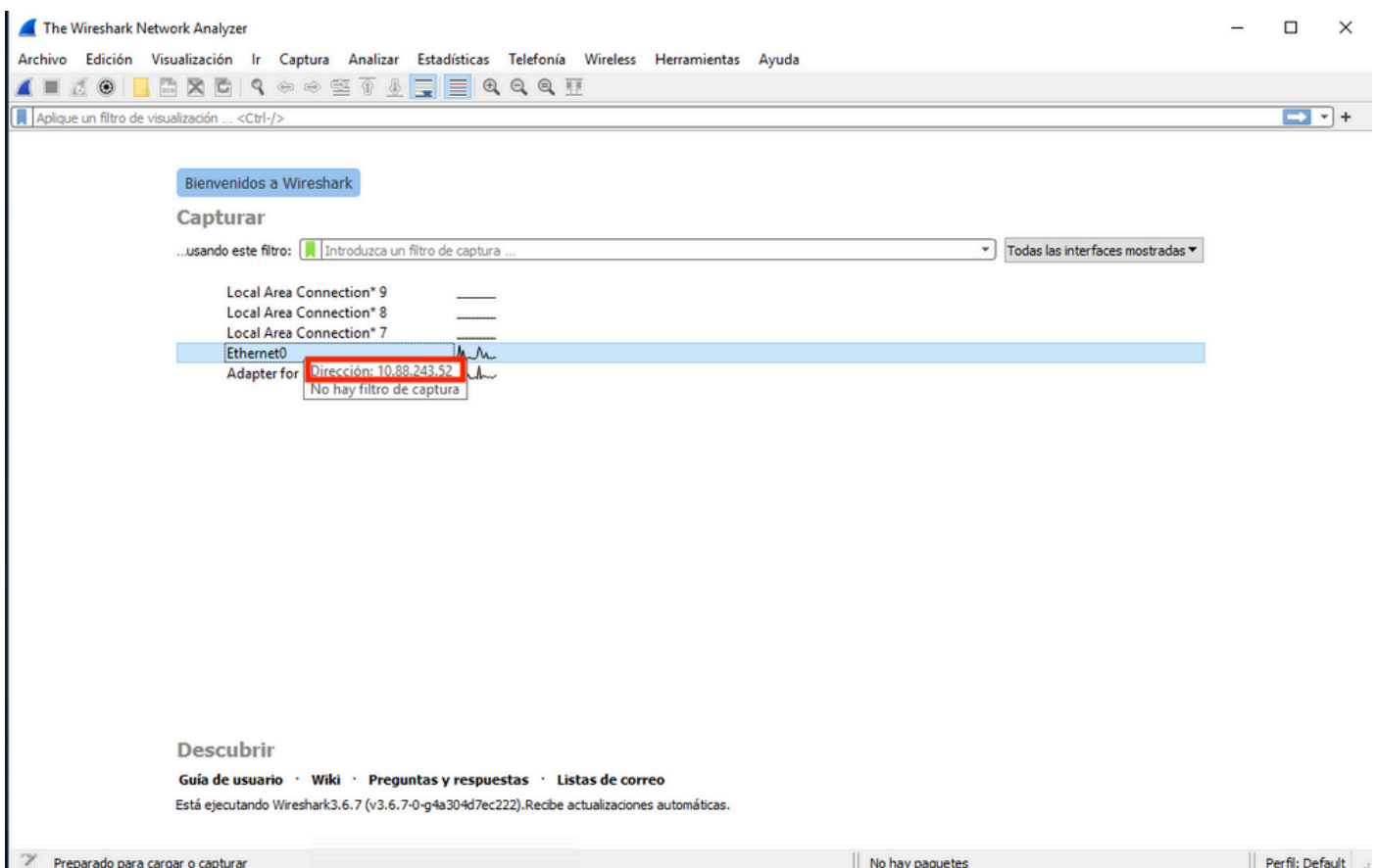
Paso 1. Si los mensajes Syslog de la aplicación Syslog generan algún mensaje, realice una captura de paquetes desde la CLI de FTD para comprobar si hay paquetes. Cambie del modo Clish a LINA ingresando el comando **system support diagnostic-cli** en la indicación de clish.

```
[> 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#
```

Paso 2. Cree una captura de paquetes para su udp 514 (o tcp 1468 si utilizó tcp)

Paso 3. Verifique que la comunicación esté llegando a la tarjeta de interfaz de red en el servidor Syslog. Utilice Wireshark u otra utilidad de captura de paquetes cargada. Haga doble clic en la interfaz de Wireshark para que el servidor Syslog comience a capturar paquetes.



Paso 4. Establezca un filtro de visualización en la barra superior para udp 514. Para ello, escriba `udp.port==514` y seleccione la flecha situada a la derecha de la barra. Desde la salida, confirme si los paquetes están llegando al servidor 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

Paso 5. Si la aplicación de servidor Syslog no muestra los datos, solucione el problema en la aplicación de servidor Syslog. Asegúrese de que se esté utilizando el protocolo correcto udp/tcp y el puerto correcto 514/1468.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).