Configuración de dispositivos para enviar y ver los registros del sistema de resolución de problemas en FMC

Contenido

Introducción

Este documento describe cómo configurar los dispositivos administrados para enviar mensajes de syslog de diagnóstico a FMC y verlos en el Visor de Eventos Unificado.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:
•Mensajes de Syslog
•Centro de administración Firepower (FMC)
•Firepower Threat Defense (FTD)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.
· Este documento se aplica a todas las plataformas Firepower.
· Secure Firewall Threat Defence Virtual (FTD), que ejecuta la versión de software 7.6.0
· Secure Firewall Management Center Virtual (FMC), que ejecuta la versión de software 7.6.0
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

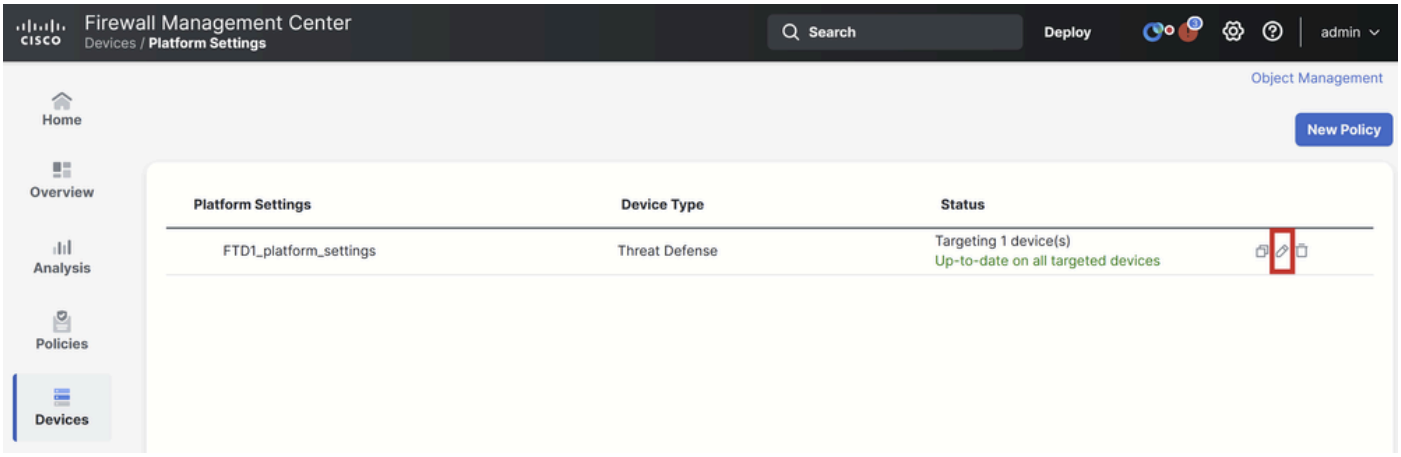
Descripción general de características

En Secure Firewall 7.6, se agrega un nuevo tipo de evento de Troubleshooting en la tabla del visor de eventos de Unified. La configuración de la plataforma syslog logging configuration se ha ampliado y admite el envío de mensajes de syslog de diagnóstico generados por LINA al FMC en lugar de solamente registros de VPN. Esta función se puede configurar en cualquier FTD que ejecute una versión de software compatible con FMC 7.6.0. cdFMC no es compatible porque cdFMC no tiene herramientas de análisis.

- La opción Todos los registros está limitada a los niveles de registro crítico, de alerta y de emergencia debido al volumen de eventos.
- Estos registros de solución de problemas muestran cualquier registro del sistema enviado desde el dispositivo al FMC (VPN u otro).
- Los registros de solución de problemas se envían al FMC y son visibles en la vista de eventos unificada y en Dispositivos > Solución de problemas > Registros de solución de problemas.

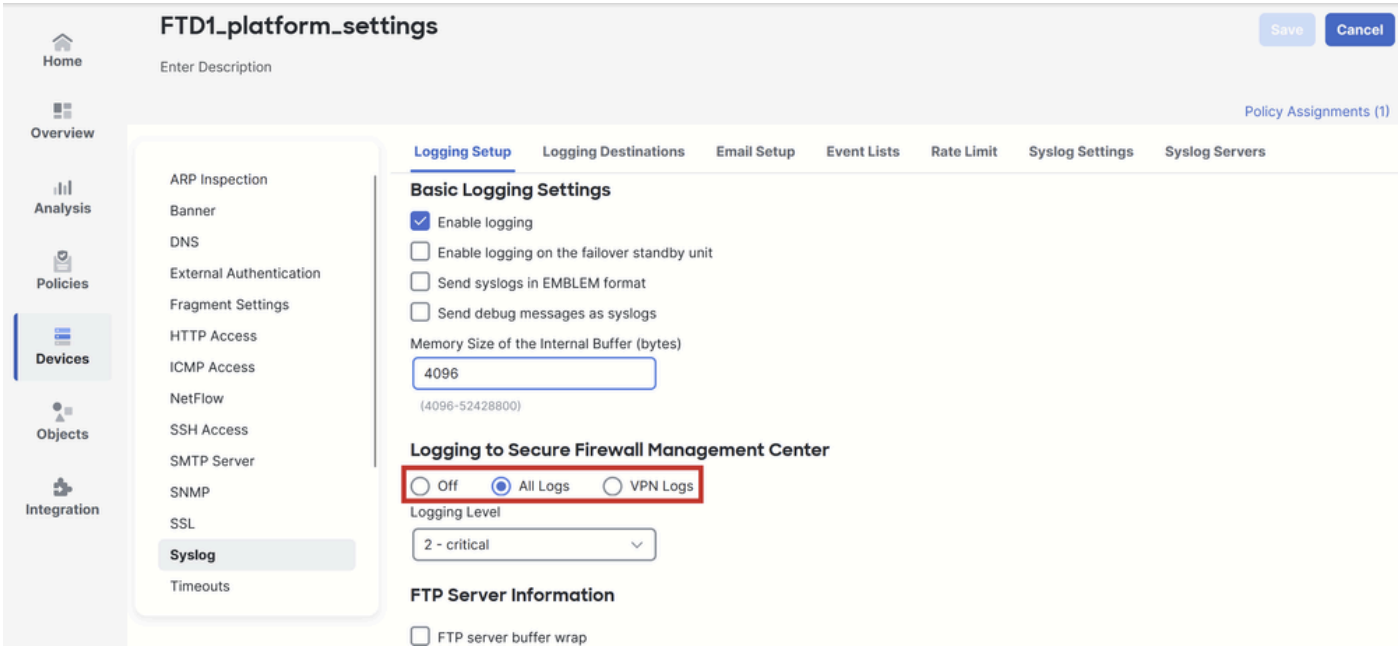
Configurar

Navegue hasta FMC Devices > Platform Settings y haga clic en el icono Edit en la esquina superior derecha de la política.



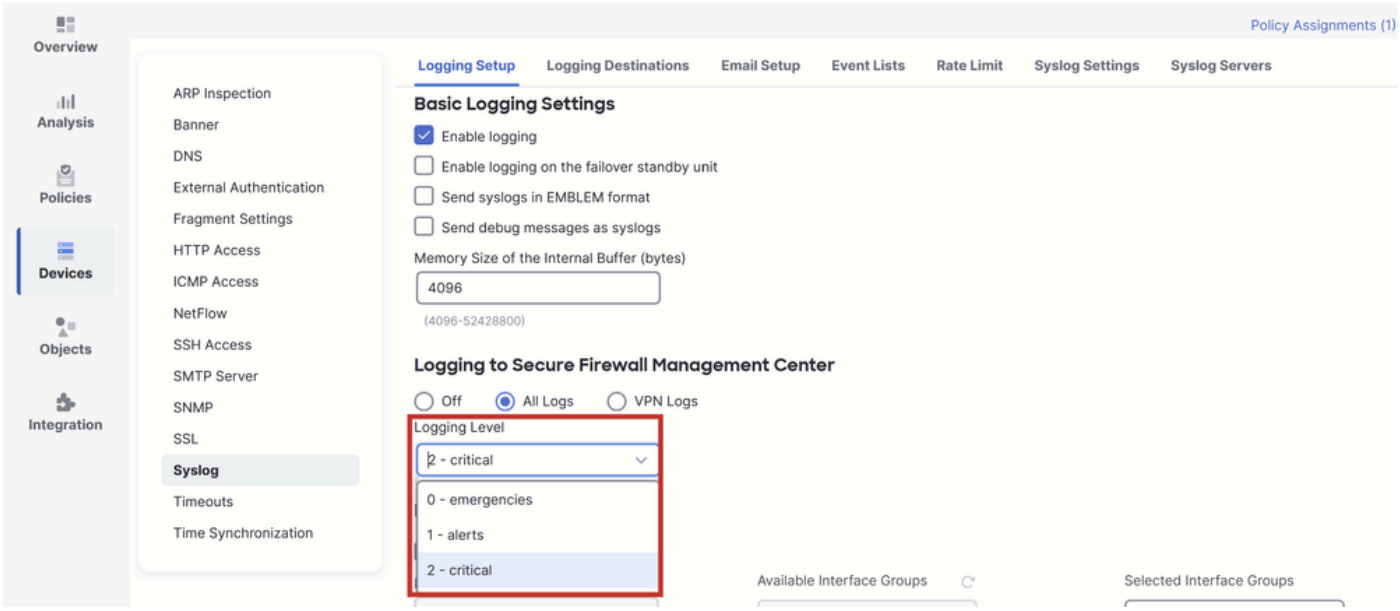
Directiva de configuración de plataforma

Vaya a Syslog > Configuración de registro. Puede ver tres opciones en Registro en Secure Firewall Management Center.



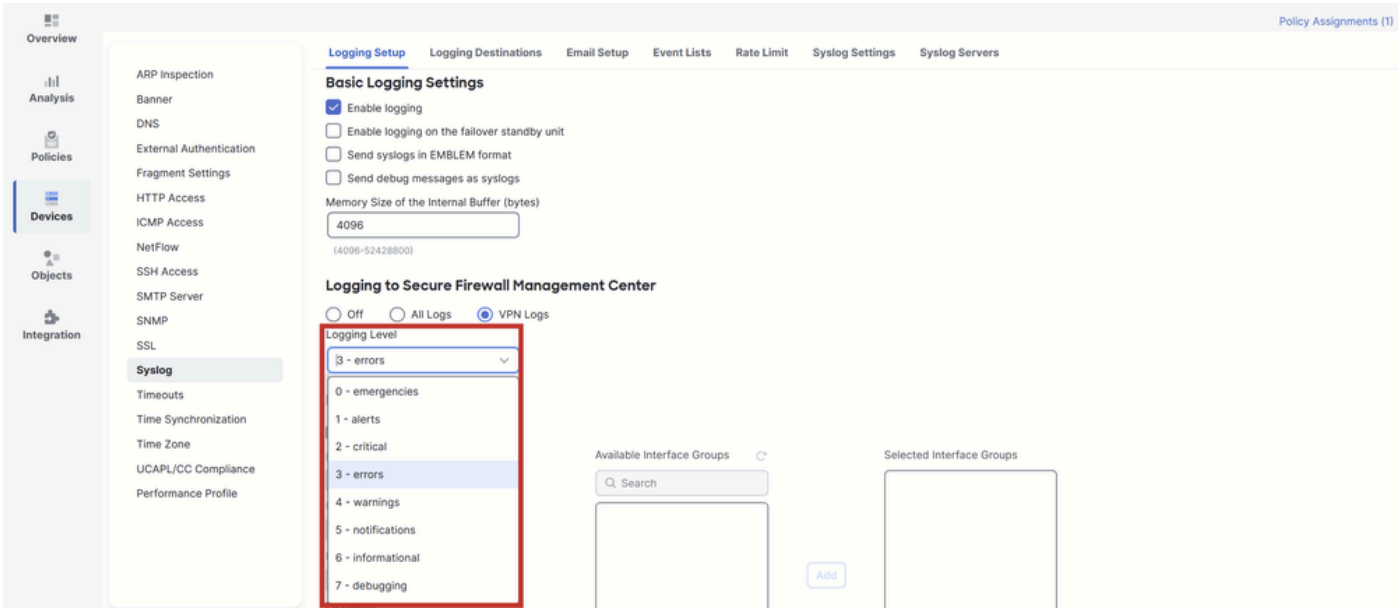
Tres opciones de registro

Si selecciona All Logs, puede seleccionar cualquiera de los tres niveles de registro disponibles: emergencias, alertas y mensajes críticos y enviar todos los mensajes de syslog de diagnóstico a FMC (incluida VPN).

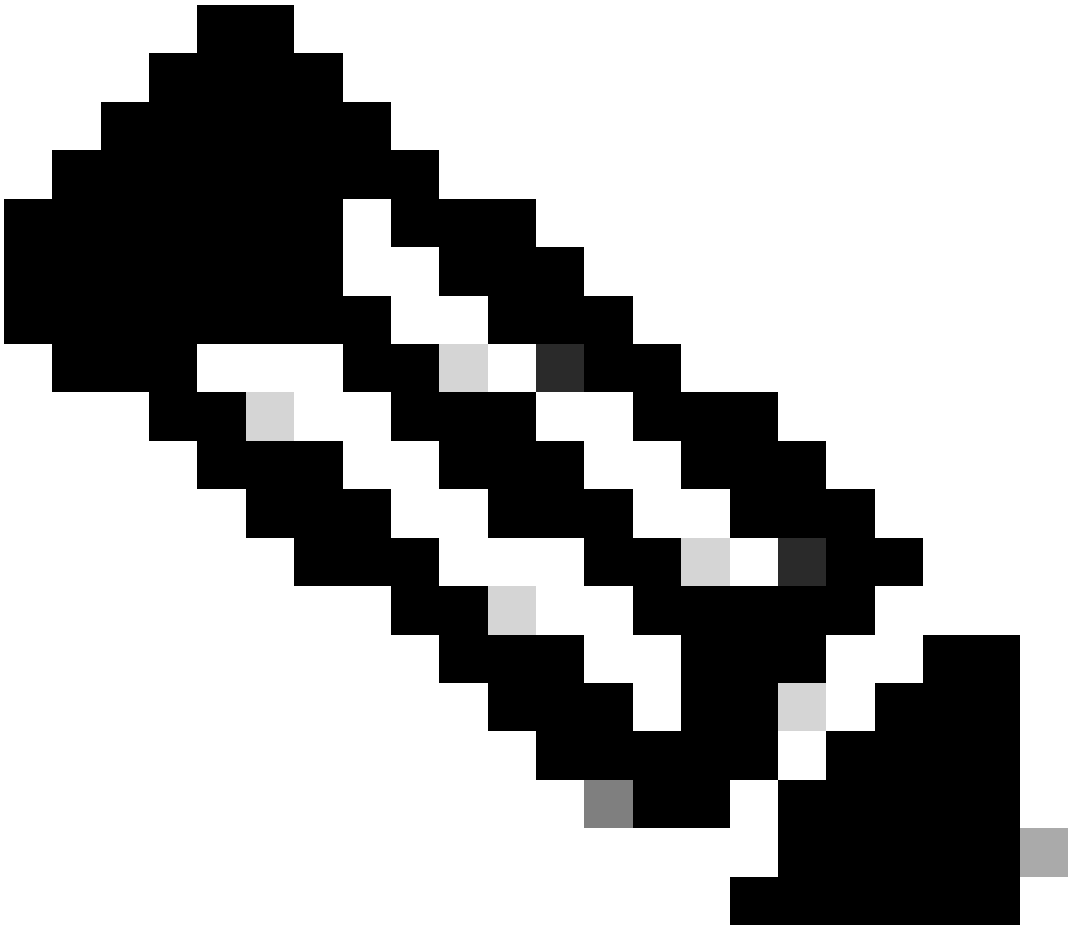


Niveles de registro disponibles

Si elige VPN Logs, todos los niveles de registro están disponibles y se puede seleccionar uno de ellos.



Niveles de registro disponibles

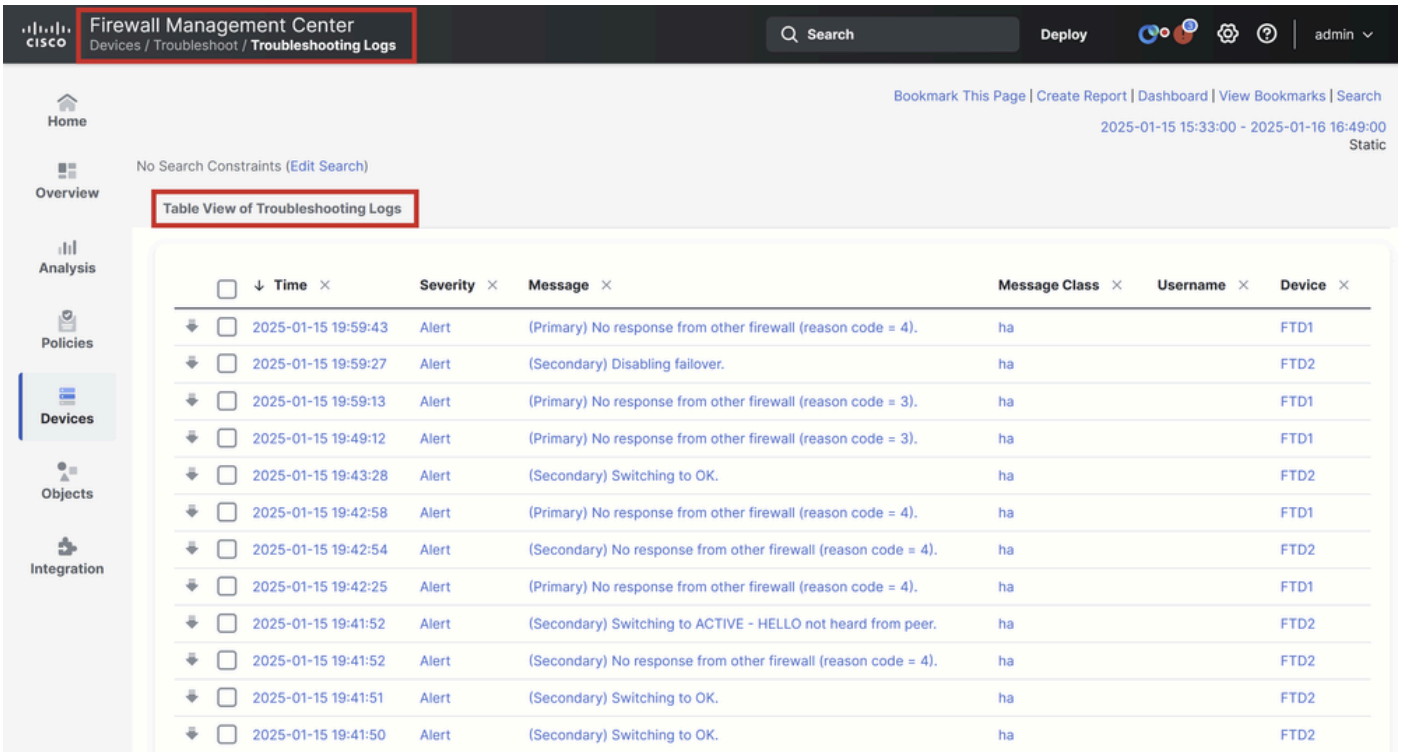


Nota: Al configurar un dispositivo con VPN de sitio a sitio o de acceso remoto, se habilita

---

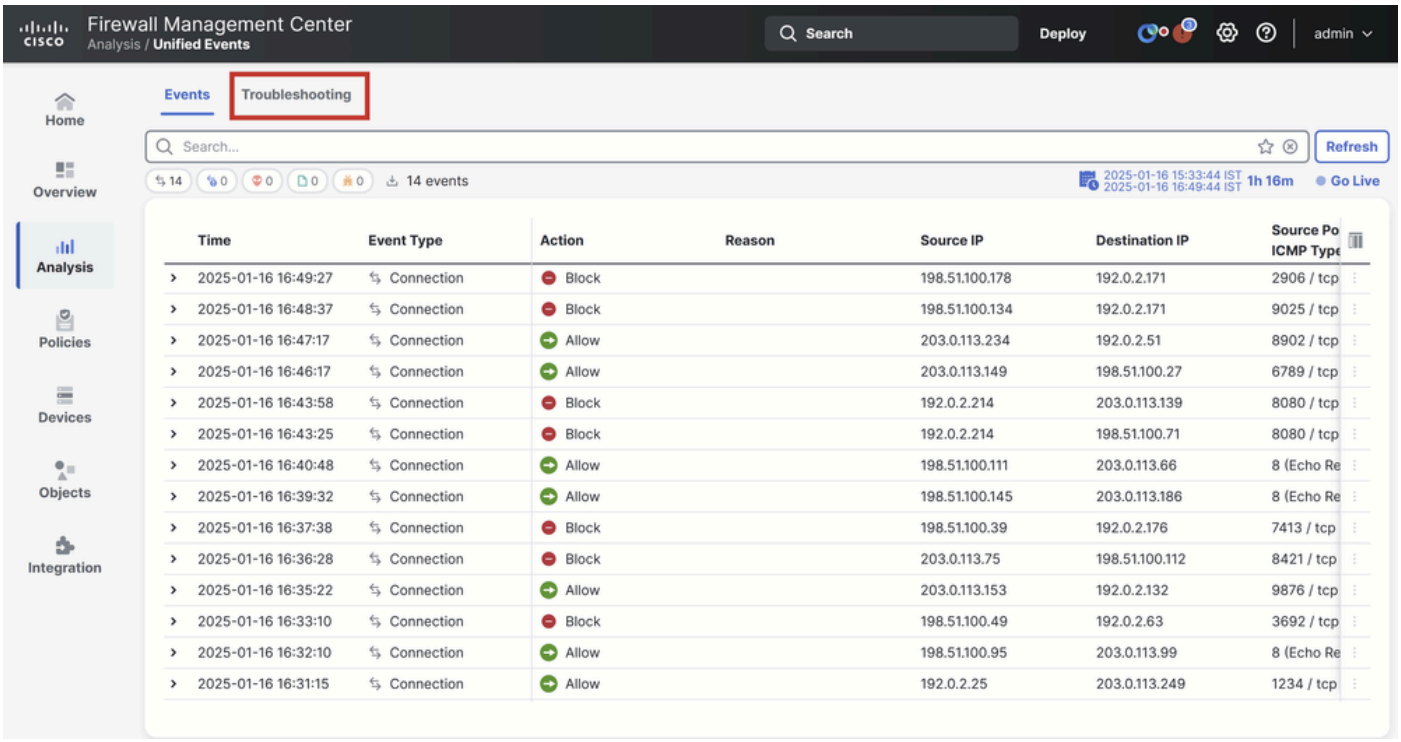
automáticamente el envío de registros del sistema VPN al centro de administración de forma predeterminada. Puede cambiarlo a Todos los registros para enviar todos los registros del sistema además de los registros de VPN a FMC.

Se puede acceder a estos registros desde Devices > Troubleshoot > Troubleshooting Logs.



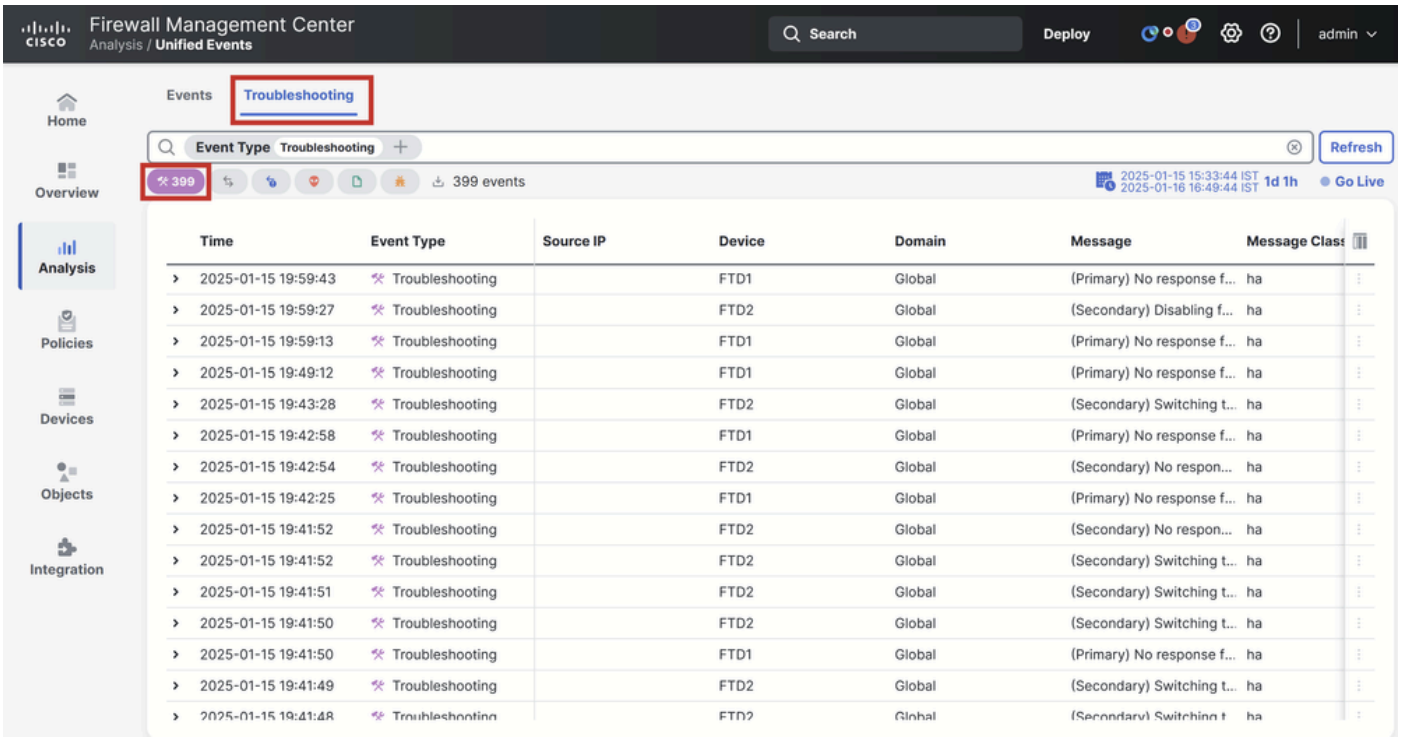
Vista de tabla de registros de solución de problemas

Ahora hay disponible una nueva ficha de vista de solución de problemas en la página Visor de sucesos de Unified. Para ver estos eventos, vaya a Análisis > Eventos unificados > Solución de problemas.



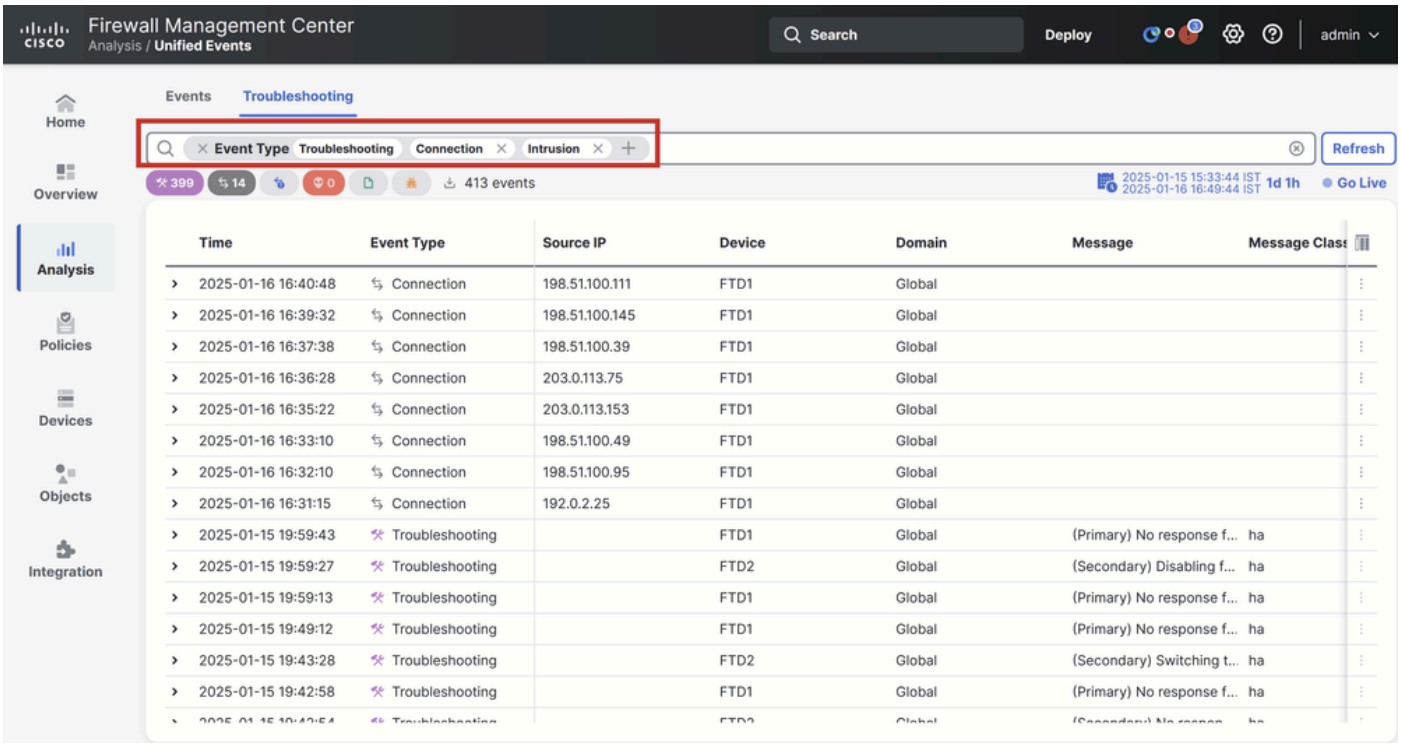
Vista de solución de problemas

Un nuevo tipo de evento es visible dentro de la tabla una vez que cambie a esta ficha. No se puede agregar ni quitar de la vista como los demás tipos, ya que es fundamental para la vista Solución de problemas.



Tipo de evento de resolución de problemas

Aún se pueden agregar y quitar otros tipos de eventos de esta vista Solución de problemas. Esto permite ver los registros de diagnóstico junto con otros datos de eventos.



Otros tipos de eventos

Verifique la Configuración

Una vez que la configuración se realiza desde la GUI de FMC, se puede verificar desde la CLI de FTD ejecutando los comandos show running-config logging y show logging en el modo CLISH o LINA.

```
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
```

Comando CLI de FTD

```
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
```

Comando CLI de FTD

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).