Configurar dispositivos para enviar e visualizar syslogs de solução de problemas no FMC

Contents

Introdução

Este documento descreve como configurar dispositivos gerenciados para enviar mensagens de syslog de diagnóstico ao FMC e visualizá-las no Visualizador de Eventos Unificado.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:
•Mensagens de syslog
•Firepower Management Center (FMC)
•Firepower Threat Defense (FTD)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:
· Este documento se aplica a todas as plataformas Firepower.
· Secure Firewall Threat Defense Virtual (FTD), que executa a versão 7.6.0 do software
· Secure Firewall Management Center Virtual (FMC), que executa a versão 7.6.0 do software
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Visão geral do recurso

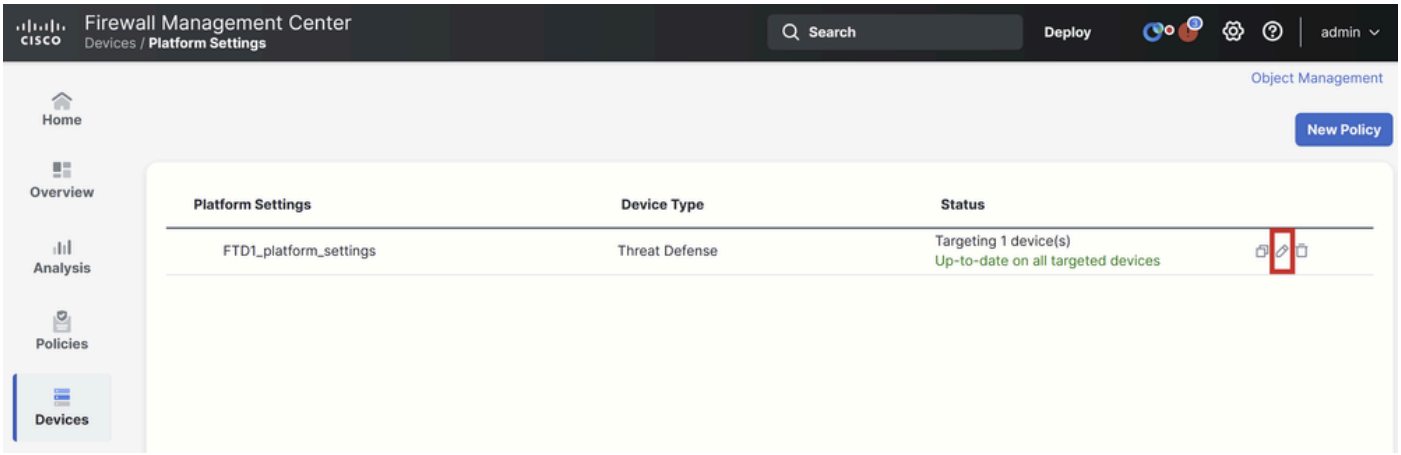
No Secure Firewall 7.6, um novo tipo de evento Solução de problemas é adicionado à tabela Unified Event Viewer. A configuração de registro de syslog de configurações de plataforma foi estendida e suporta o envio de mensagens de syslog de diagnóstico geradas por LINA para o

FMC, em vez de apenas registros VPN. Este recurso pode ser configurado em qualquer FTD que execute uma versão de software compatível com o FMC 7.6.0. O cdFMC não é suportado porque o cdFMC não tem ferramentas de análise.

- A opção Todos os registros está limitada aos níveis de registro de emergência, alerta e crítico devido ao volume de eventos.
- Esses registros de solução de problemas mostram qualquer syslog enviado do dispositivo para o FMC (VPN ou outro).
- Os registros de solução de problemas fluem para o FMC e são visíveis no Unified Event View e em Devices > Troubleshoot > Troubleshooting Logs.

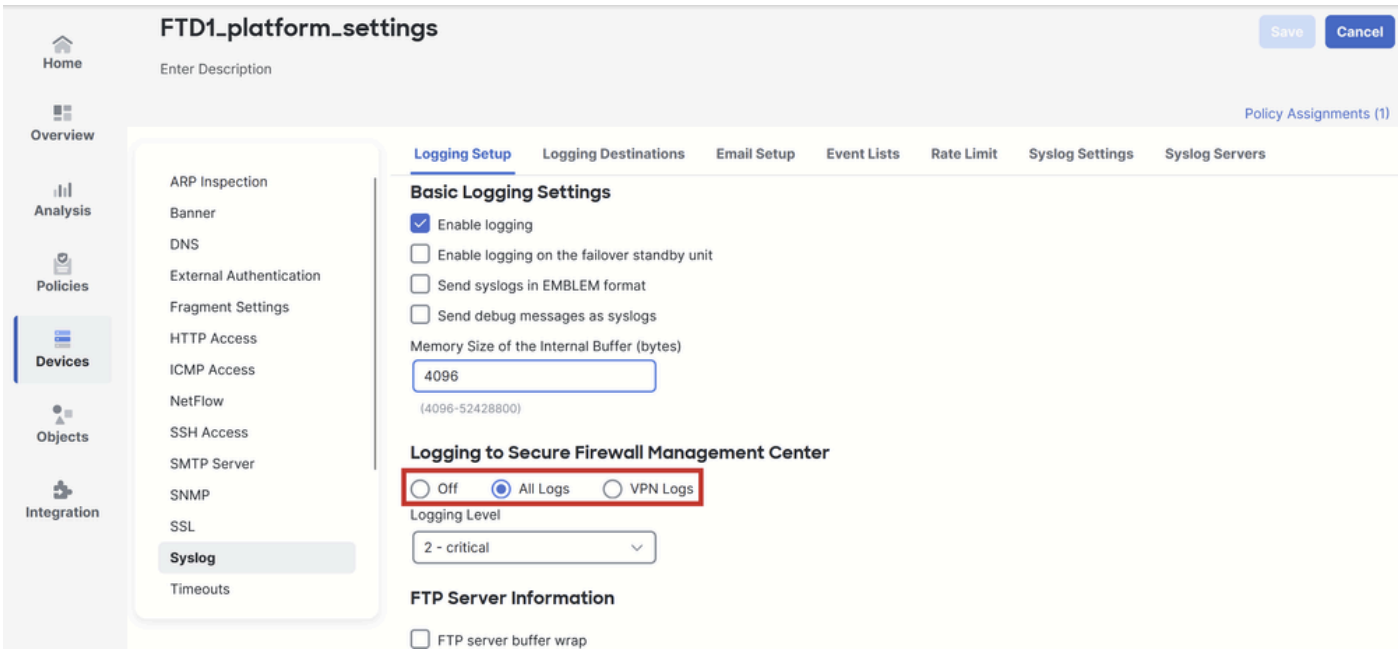
Configurar

Navegue até FMC Devices > Platform Settings e clique no ícone Edit no canto superior direito da política.



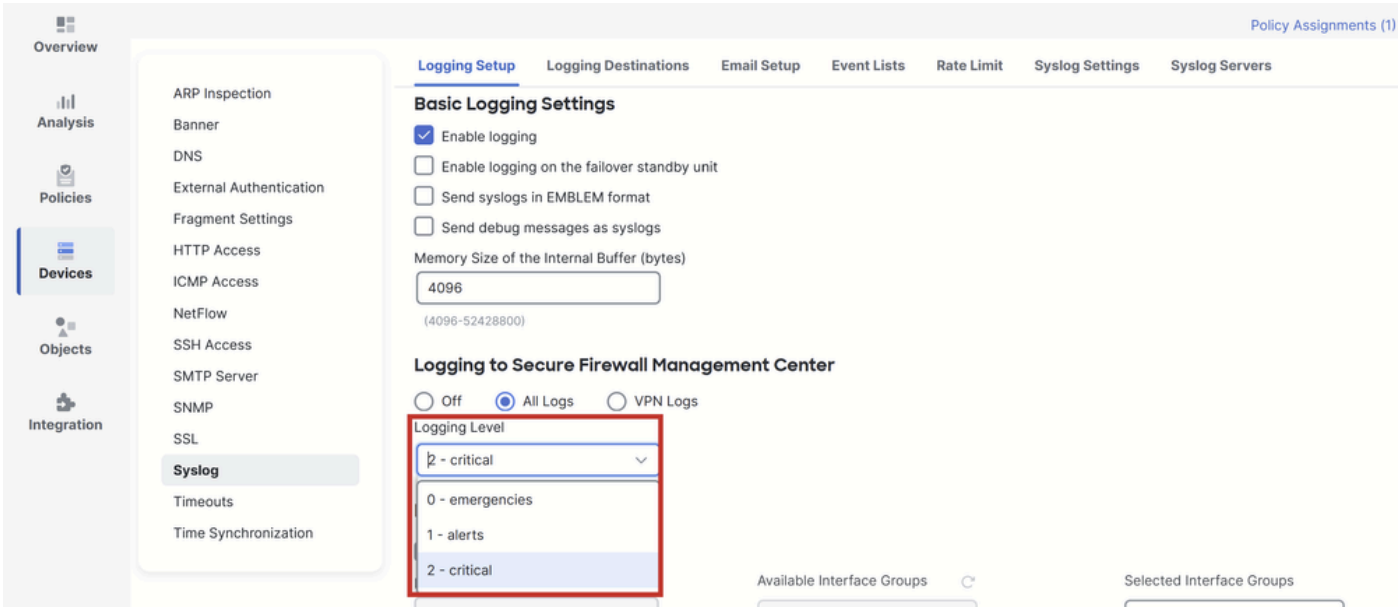
Política de Configurações de Plataforma

Vá para Syslog > Logging Setup. Você pode ver três opções em Logging to Secure Firewall Management Center.



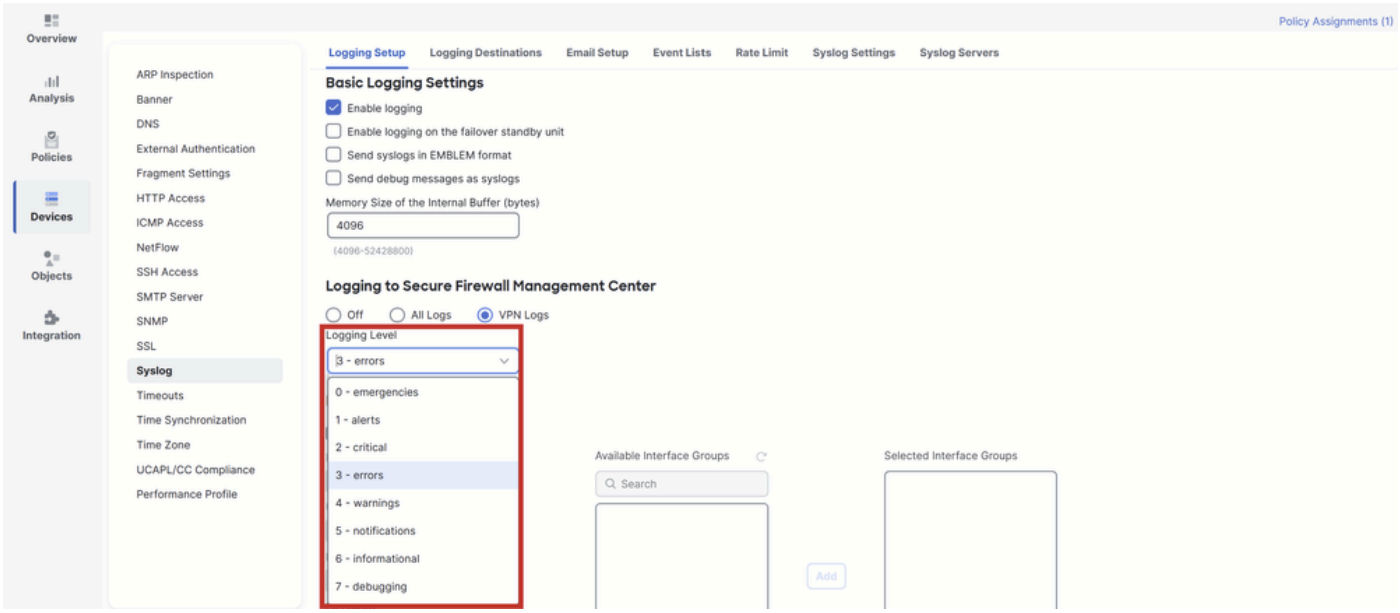
Três opções de registro

Se você selecionar All Logs, poderá selecionar qualquer um dos três níveis de log disponíveis: emergências, alertas e mensagens críticas e enviar todas as mensagens de syslog de diagnóstico para o FMC (incluindo VPN).

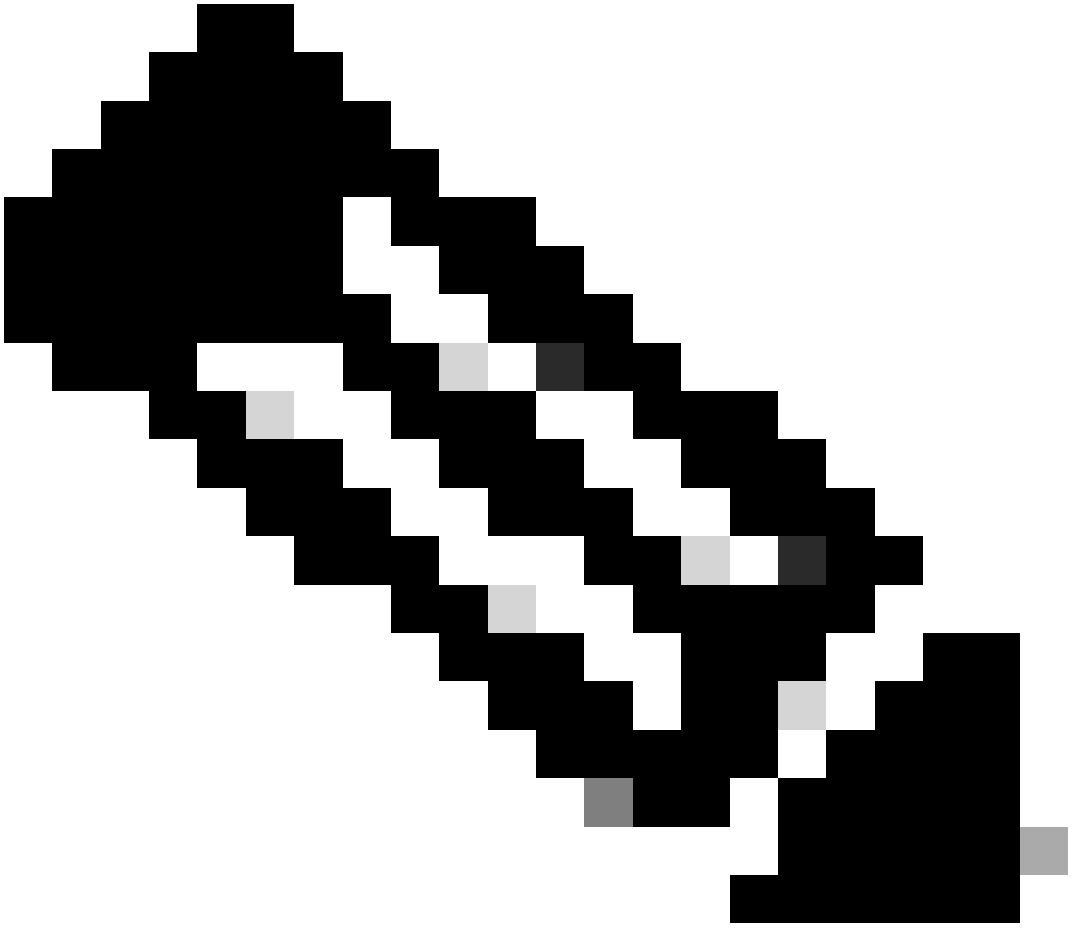


Níveis de log disponíveis

Se você selecionar VPN Logs, todos os níveis de registro estarão disponíveis e um deles poderá ser selecionado.

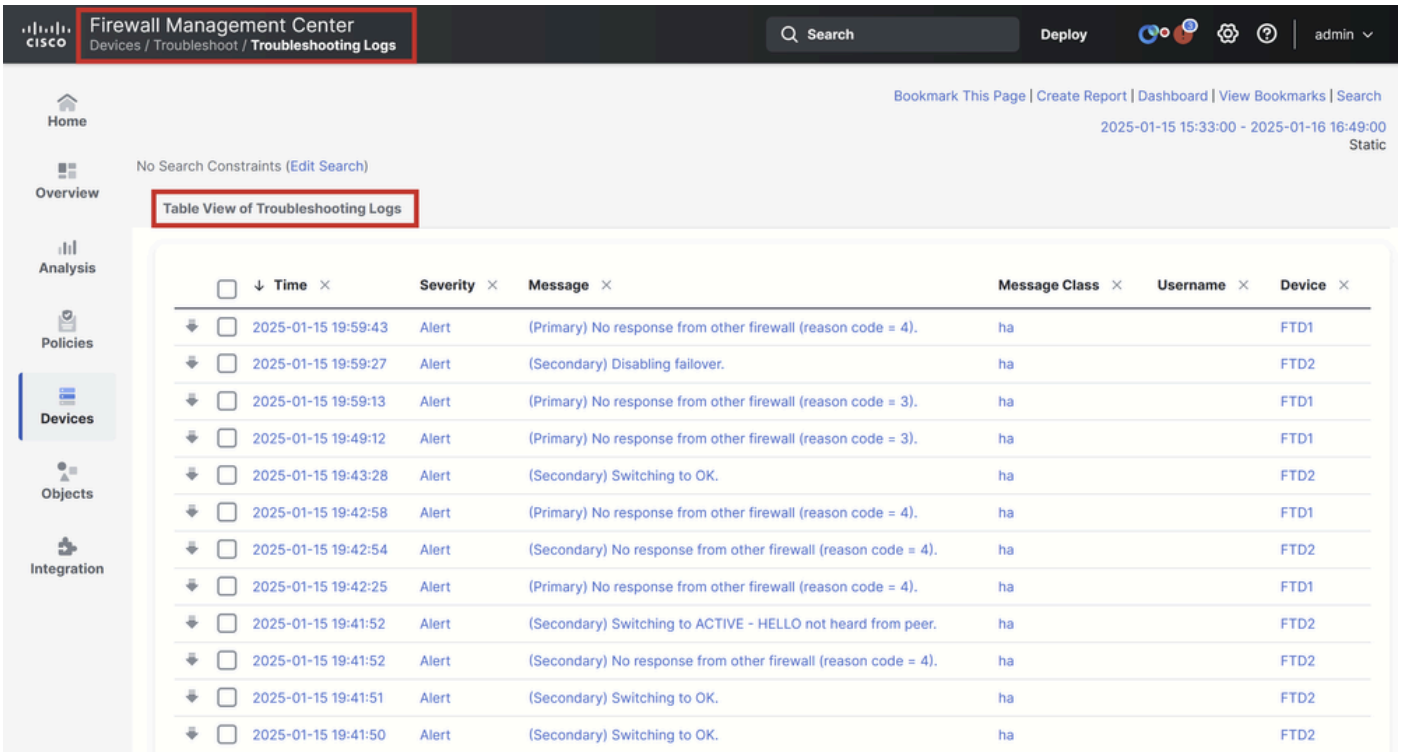


Níveis de log disponíveis



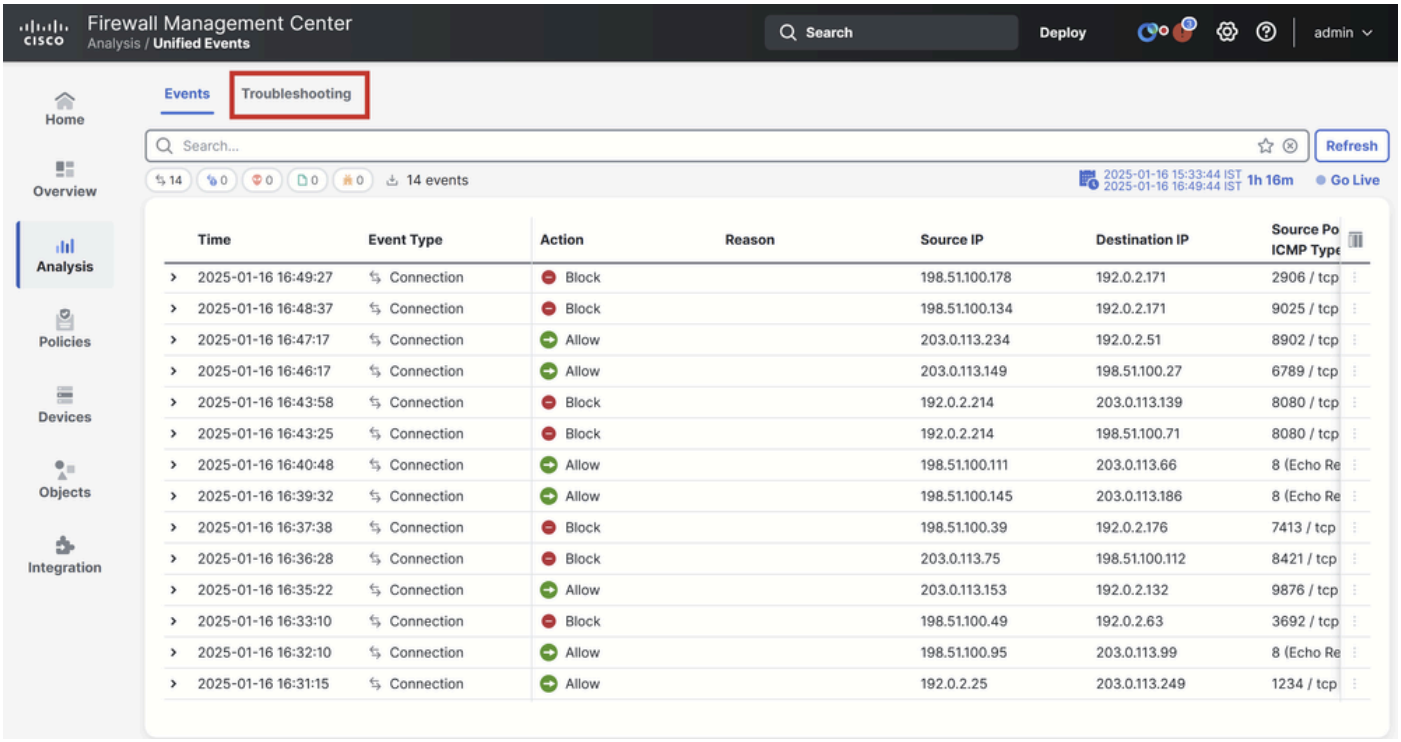
Note: Quando você configura um dispositivo com VPN de acesso remoto ou de site a site, ele permite automaticamente o envio de syslogs de VPN para o centro de gerenciamento por padrão. Você pode alterá-lo para All Logs (Todos os registros) para enviar todos os syslogs além dos registros VPN ao FMC.

Esses registros podem ser acessados em Devices > Troubleshoot > Troubleshooting Logs.



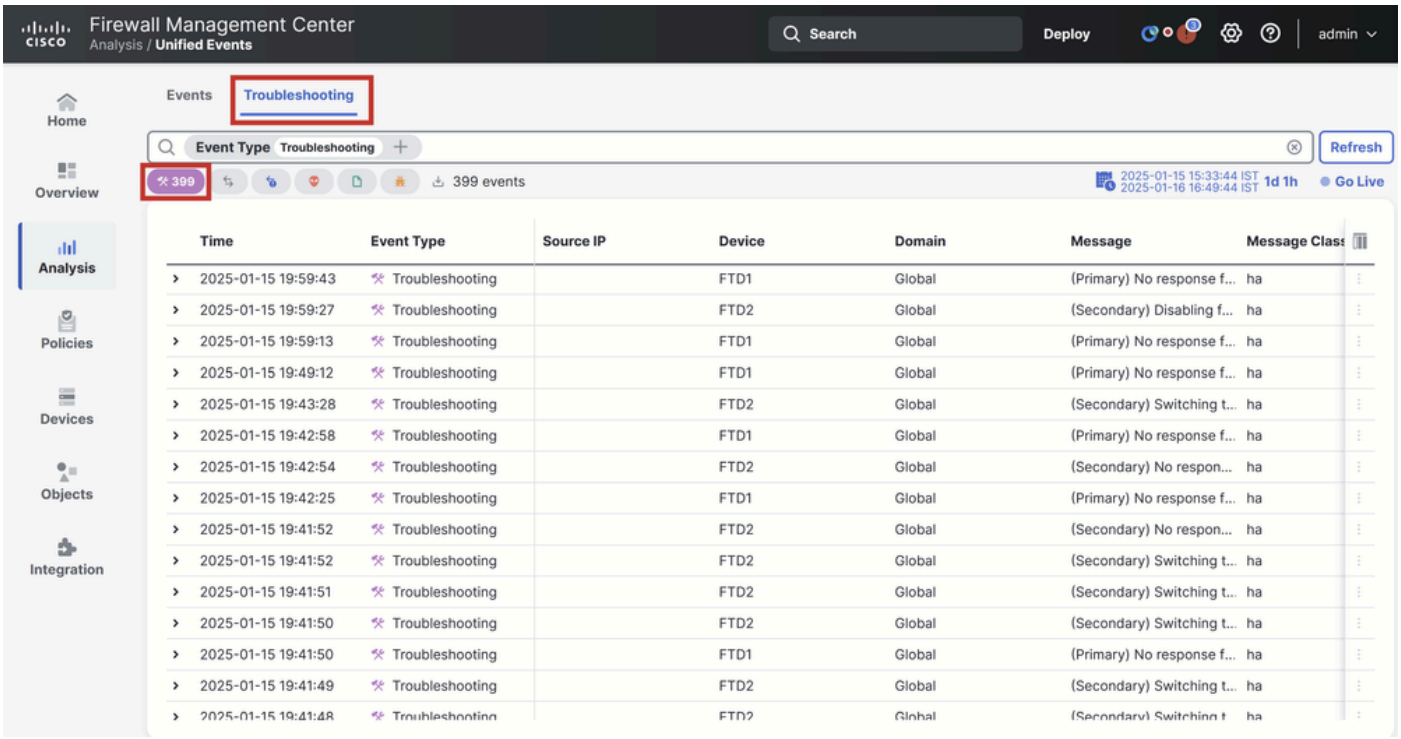
Visão em Tabela dos Logs de Troubleshooting

Uma nova guia de exibição Solução de problemas agora está disponível na página Unified Event Viewer. Para exibir esses eventos, navegue até Análise > Eventos unificados > Solução de problemas.



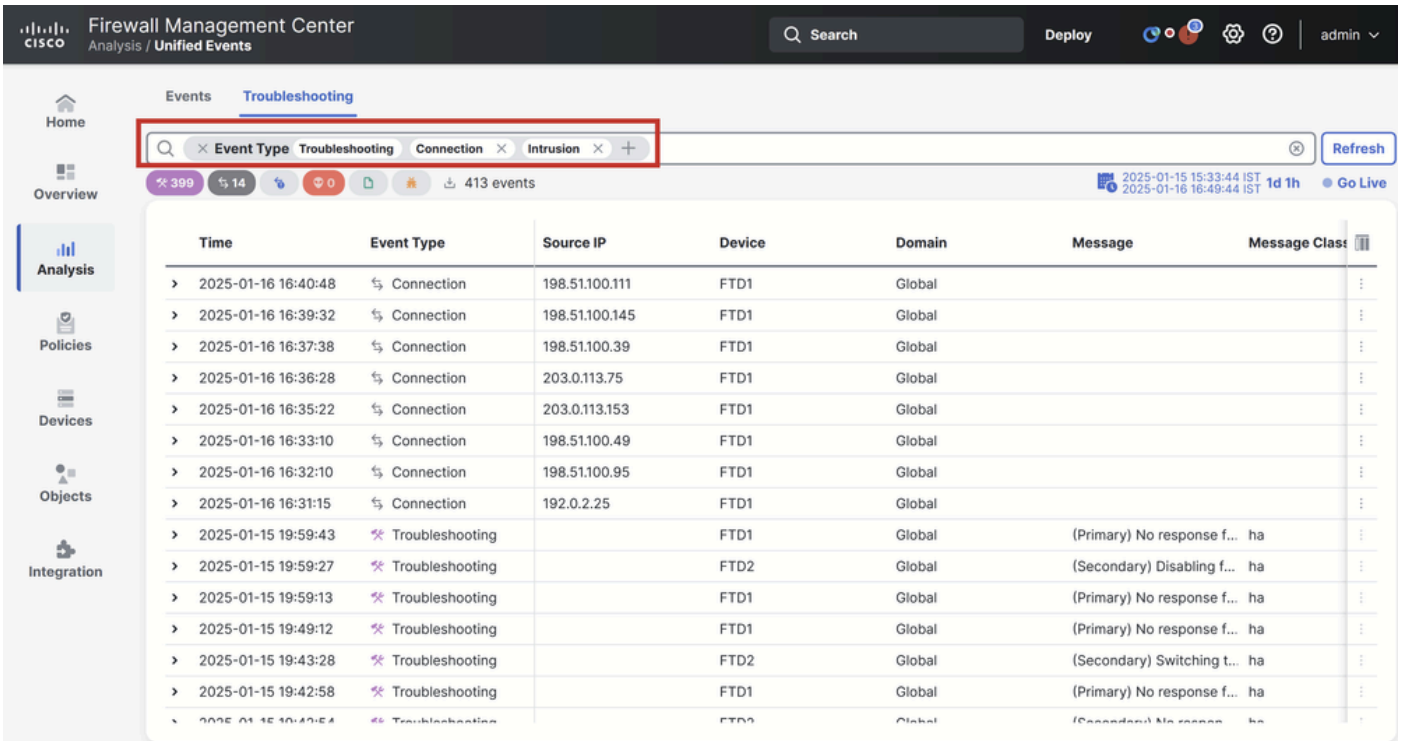
Exibição de Solução de Problemas

Um novo tipo de evento estará visível na tabela quando você alternar para esta guia. Ele não pode ser adicionado ou removido da exibição como os outros tipos, pois é central para a exibição Solução de problemas.



Troubleshooting de Tipo de Evento

Outros tipos de evento ainda podem ser adicionados e removidos desta exibição de Solução de problemas. Isso permite que você visualize logs de diagnóstico juntamente com outros dados de evento.



Outros tipos de evento

Verificar a configuração

Depois que a configuração é feita na GUI do FMC, ela pode ser verificada na CLI do FTD

executando os comandos show running-config logging e show logging no modo CLISH ou 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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.