Configurare i dispositivi per l'invio e la visualizzazione dei syslog di risoluzione dei problemi in FMC

Sommario

Introduzione

In questo documento viene descritto come configurare i dispositivi gestiti in modo che inviino messaggi di syslog di diagnostica a FMC e li visualizzino nel Visualizzatore eventi unificato.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:
· Messaggi Syslog
•Firepower Management Center (FMC)
•Firepower Threat Defense (FTD)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:
· Questo documento è valido per tutte le piattaforme Firepower.
· Secure Firewall Threat Defense Virtual (FTD) con software versione 7.6.0
· Secure Firewall Management Center Virtual (FMC) con software versione 7.6.0
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

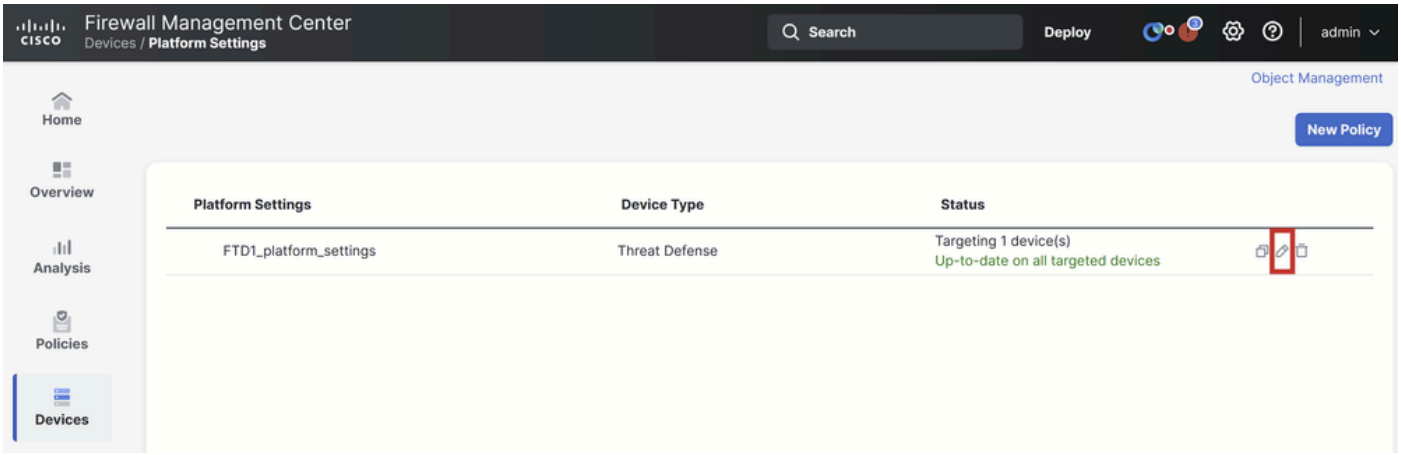
Panoramica delle funzionalità

In Secure Firewall 7.6, nella tabella del Visualizzatore eventi unificato viene aggiunto un nuovo tipo di evento Risoluzione dei problemi. La configurazione di registrazione syslog delle impostazioni della piattaforma è stata estesa e supporta l'invio di messaggi syslog di diagnostica generati da LINA al FMC anziché ai soli log VPN. Questa funzionalità può essere configurata su qualsiasi FTD che esegue una versione software compatibile con FMC 7.6.0. cdFMC non è supportato perché non dispone di strumenti di analisi.

- L'opzione Tutti i registri è limitata ai livelli di registro di emergenza, di avviso e critico a causa del volume degli eventi.
- Nei log di risoluzione dei problemi vengono visualizzati tutti i syslog inviati dal dispositivo al FMC (VPN o altro).
- I registri di risoluzione dei problemi vengono inviati al FMC e sono visibili nella Vista eventi unificata e in Dispositivi > Risoluzione dei problemi > Registri di risoluzione dei problemi.

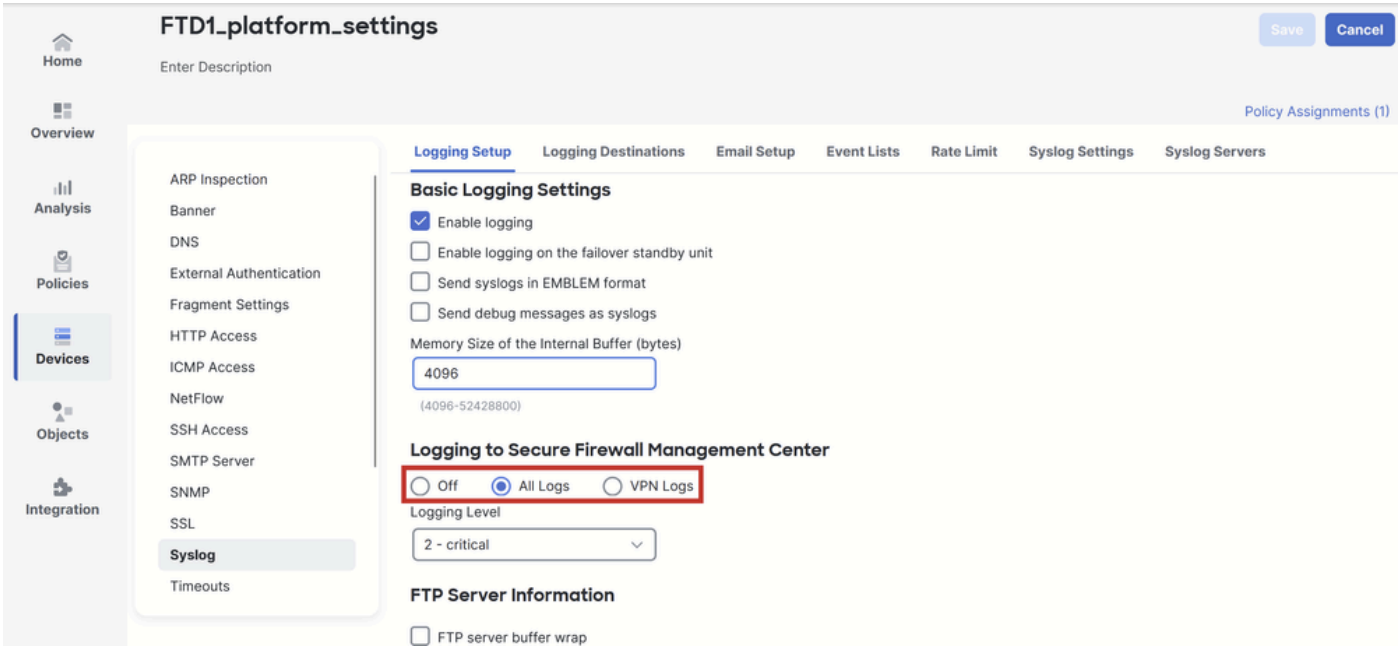
Configurazione

Passare a Dispositivi FMC > Impostazioni piattaforma e fare clic su Icona Modifica nell'angolo superiore destro del criterio.



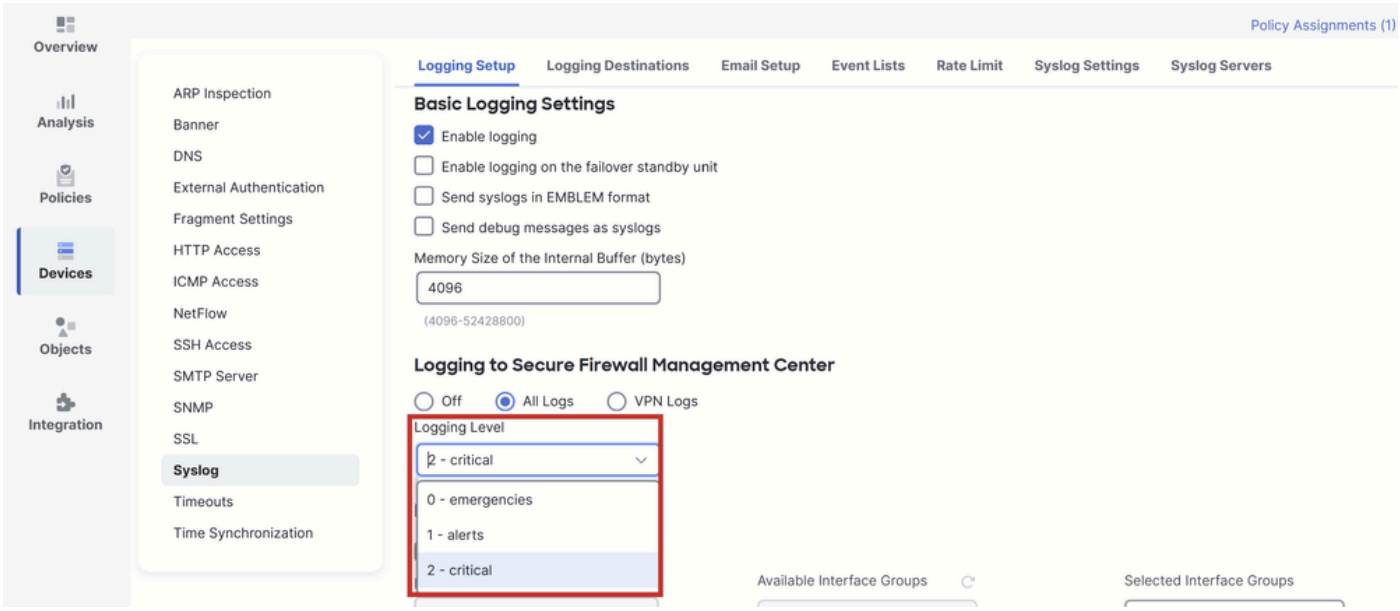
Criterio impostazioni piattaforma

Passare a Syslog > Impostazione registrazione. In Accesso a Centro gestione firewall protetto sono disponibili tre opzioni.



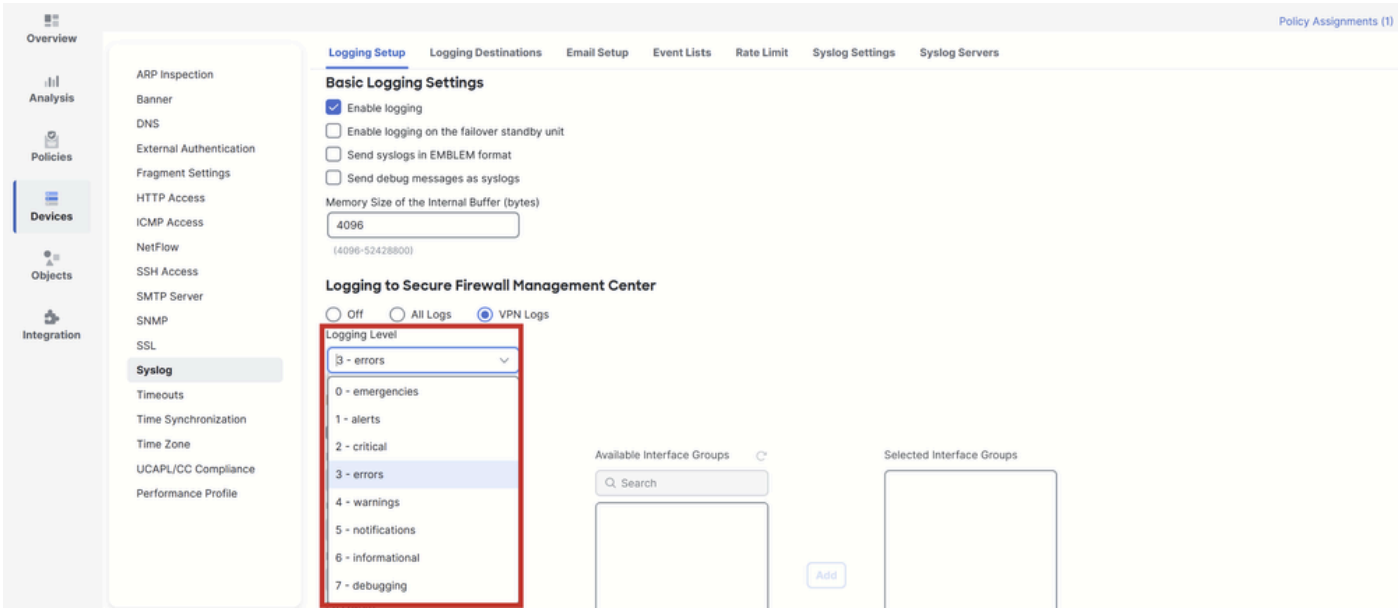
Tre opzioni di registrazione

Se si sceglie Tutti i registri, è possibile selezionare uno dei tre livelli di registrazione disponibili: emergenze, avvisi e messaggi critici e inviare tutti i messaggi di syslog diagnostici al FMC (VPN inclusa).

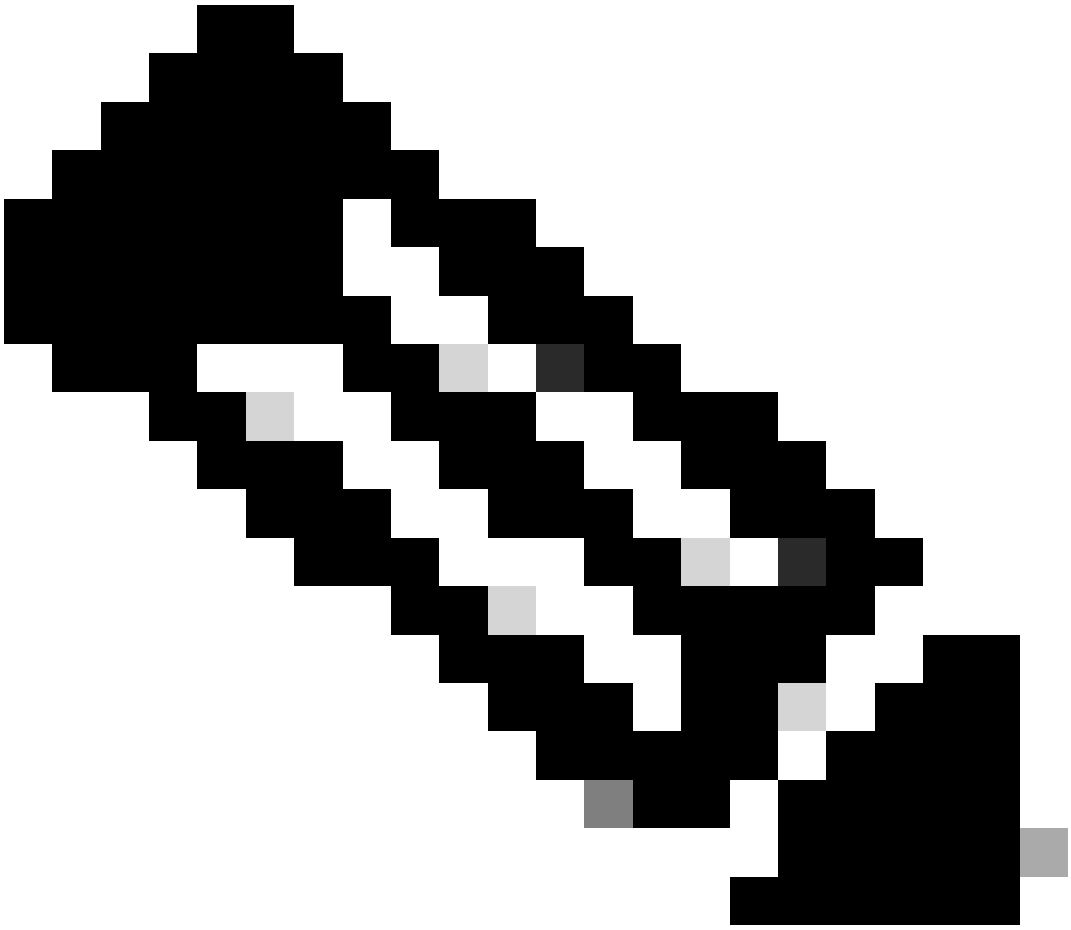


Livelli di registrazione disponibili

Se si sceglie Registri VPN, saranno disponibili tutti i livelli di registrazione e sarà possibile selezionarne uno.



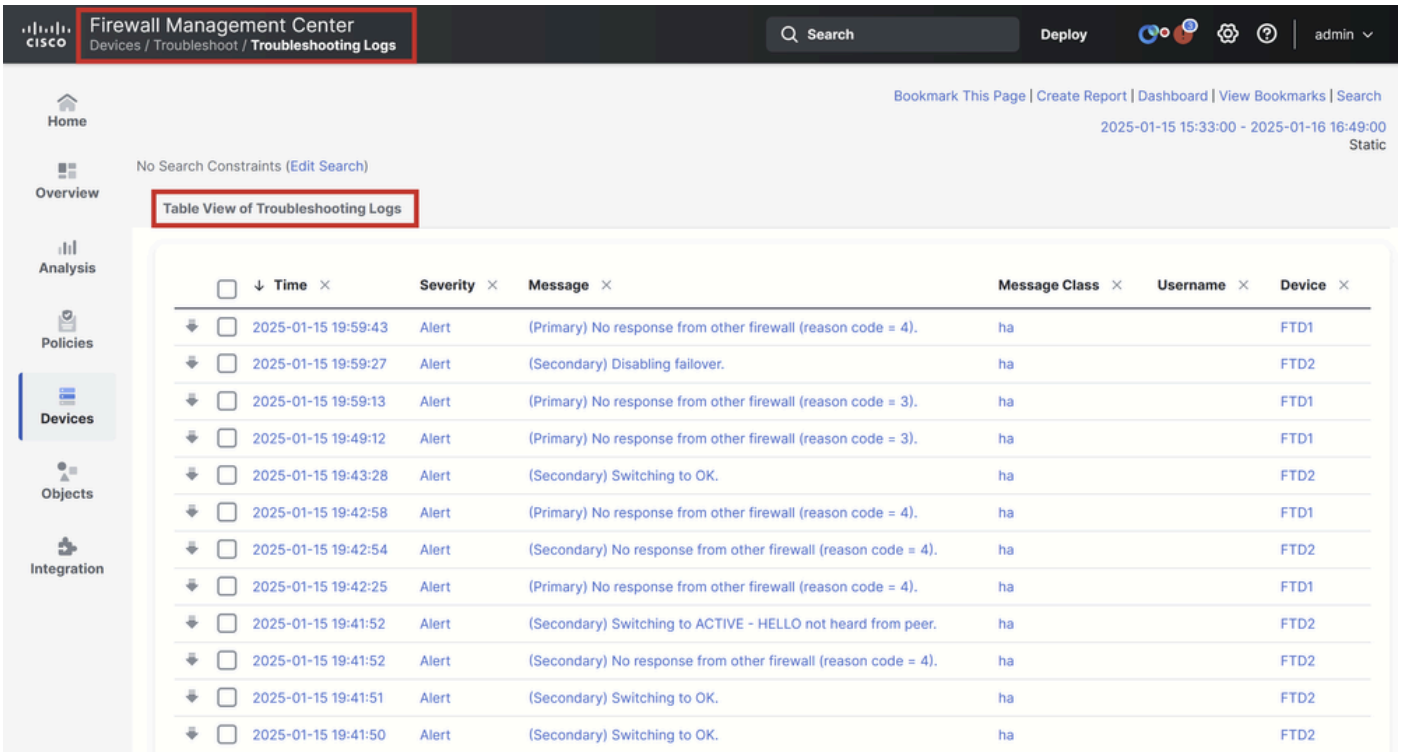
Livelli di registrazione disponibili



Nota: Quando si configura un dispositivo con una VPN da sito a sito o con accesso

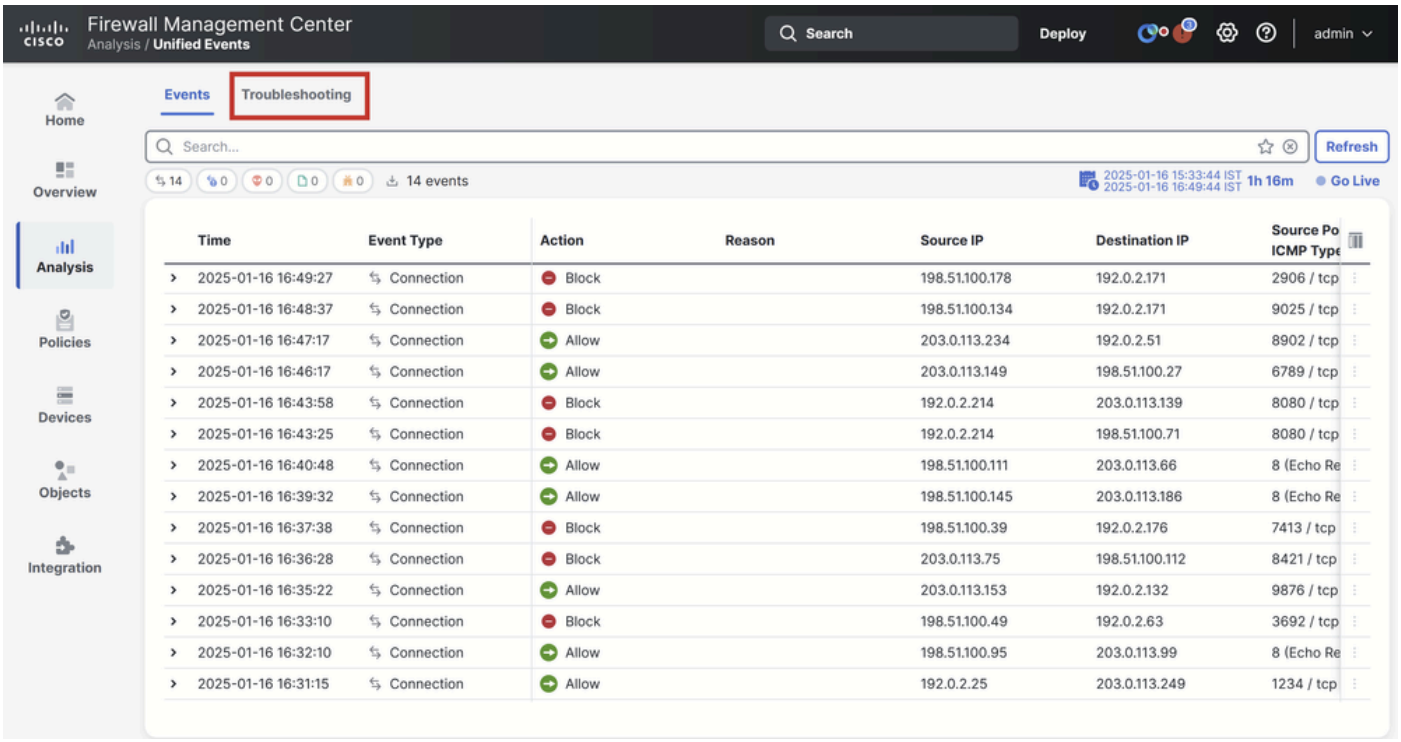
remoto, per impostazione predefinita viene attivato automaticamente l'invio di syslog VPN al centro di gestione. È possibile modificarlo in Tutti i log per inviare tutti i syslog oltre ai log VPN a FMC.

È possibile accedere a questi log da Dispositivi > Risoluzione dei problemi > Log per la risoluzione dei problemi.



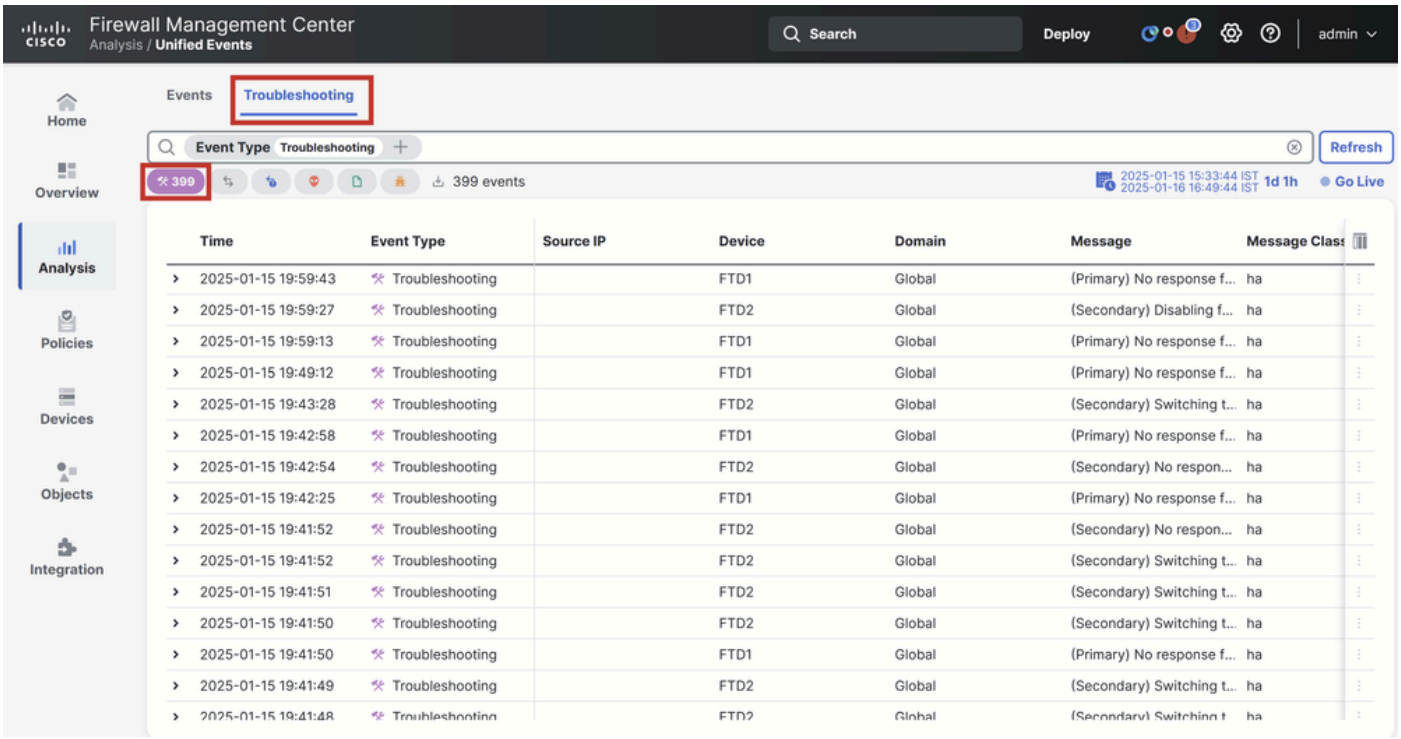
Visualizzazione per tabella dei log per la risoluzione dei problemi

Nella pagina Visualizzatore eventi unificato è ora disponibile una nuova scheda Visualizzazione Risoluzione problemi. Per visualizzare questi eventi, selezionare Analisi > Eventi unificati > Risoluzione dei problemi.



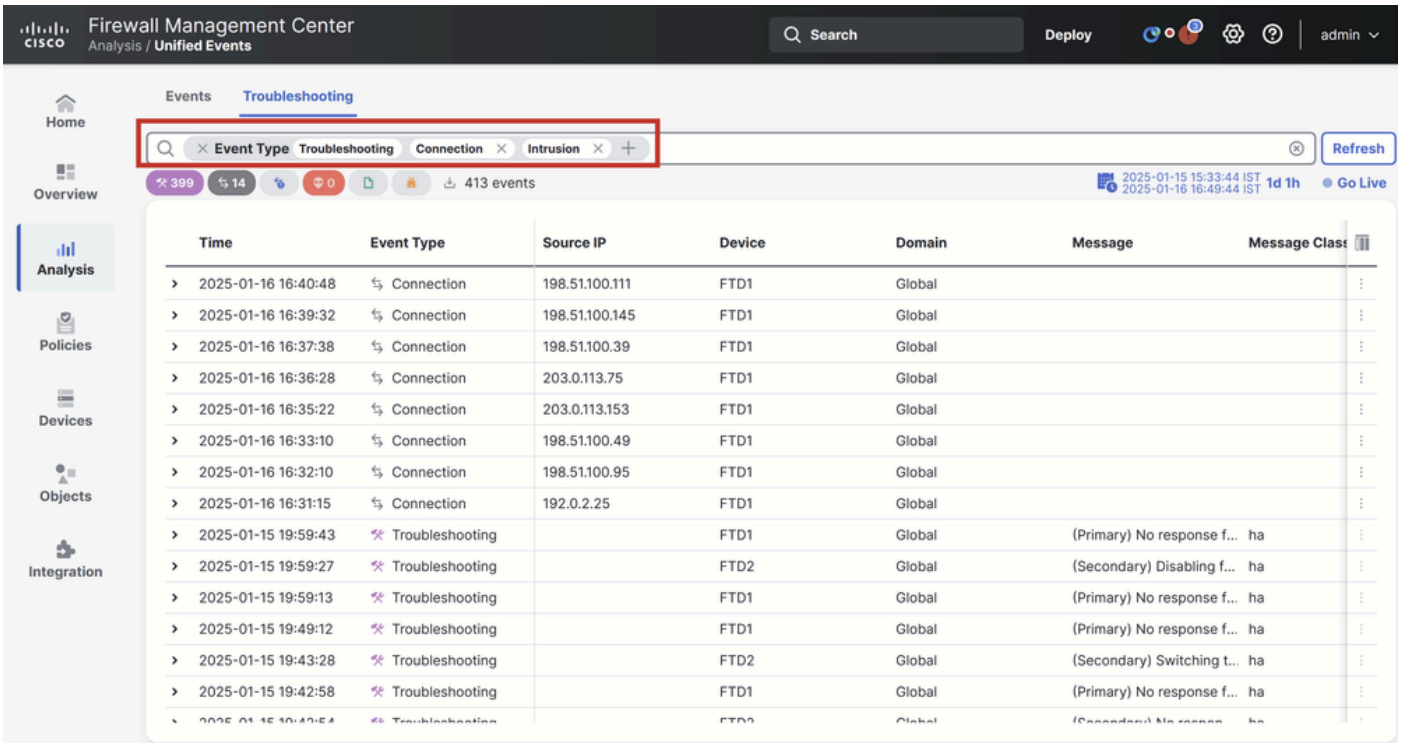
Visualizzazione Risoluzione problemi

Quando si passa a questa scheda, nella tabella viene visualizzato un nuovo tipo di evento. Non può essere aggiunto o rimosso dalla vista come gli altri tipi poiché è centrale nella vista Risoluzione problemi (Troubleshooting).



Tipo di evento risoluzione dei problemi

È comunque possibile aggiungere e rimuovere altri tipi di eventi da questa visualizzazione Risoluzione problemi. In questo modo è possibile visualizzare i log di diagnostica insieme ad altri dati degli eventi.



Altri tipi di evento

Verifica della configurazione

Una volta eseguita la configurazione dalla GUI del FMC, è possibile verificarla dalla CLI del FTD eseguendo i comandi show running-config log e show log in modalità 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 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 FTD

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).