

Configuration des périphériques pour envoyer et afficher les journaux système de dépannage sur FMC

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Présentation des fonctionnalités](#)

[Configurer](#)

[Vérifier la configuration](#)

Introduction

Ce document décrit comment configurer des périphériques gérés pour envoyer des messages syslog de diagnostic à FMC et les afficher dans Unified Event Viewer.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- périodiques
- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Ce document s'applique à toutes les plates-formes Firepower.
- Secure Firewall Threat Defense Virtual (FTD) qui exécute la version 7.6.0 du logiciel
- Secure Firewall Management Center Virtual (FMC) qui exécute la version 7.6.0 du logiciel

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Présentation des fonctionnalités

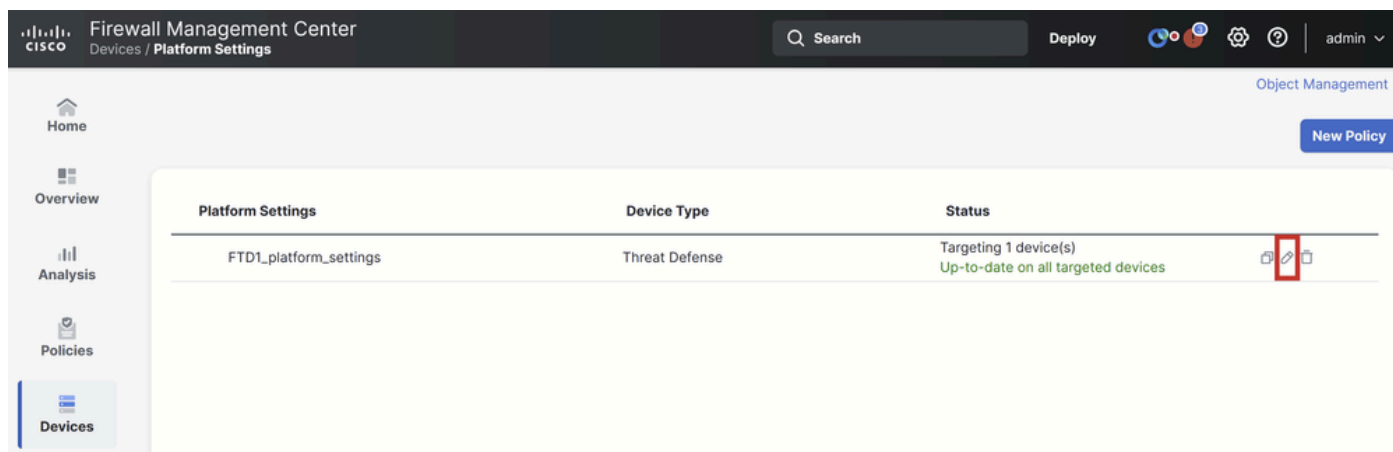
Dans Secure Firewall 7.6, un nouveau type d'événement Troubleshoot est ajouté dans la table

Unified Event Viewer. La configuration de journalisation syslog des paramètres de la plate-forme a été étendue et prend en charge l'envoi de messages syslog de diagnostic générés par LINA au FMC au lieu de simples journaux VPN. Cette fonctionnalité peut être configurée sur n'importe quel FTD exécutant une version logicielle compatible avec FMC 7.6.0. cdFMC n'est pas pris en charge car cdFMC ne dispose pas d'outils d'analyse.


- L'option Tous les journaux est limitée aux niveaux d'urgence, d'alerte et de journal critique en raison du volume d'événements.
- Ces journaux de dépannage affichent tous les Syslog envoyés par le périphérique au FMC (VPN ou autre).
- Les journaux de dépannage sont transmis au FMC et sont visibles dans la vue Unified Event View et sous Devices > Troubleshoot > Troubleshooting Logs.

Configurer

Accédez à Périphériques FMC > Paramètres de la plate-forme et cliquez sur l'icône Modifier dans l'angle supérieur droit de la stratégie.

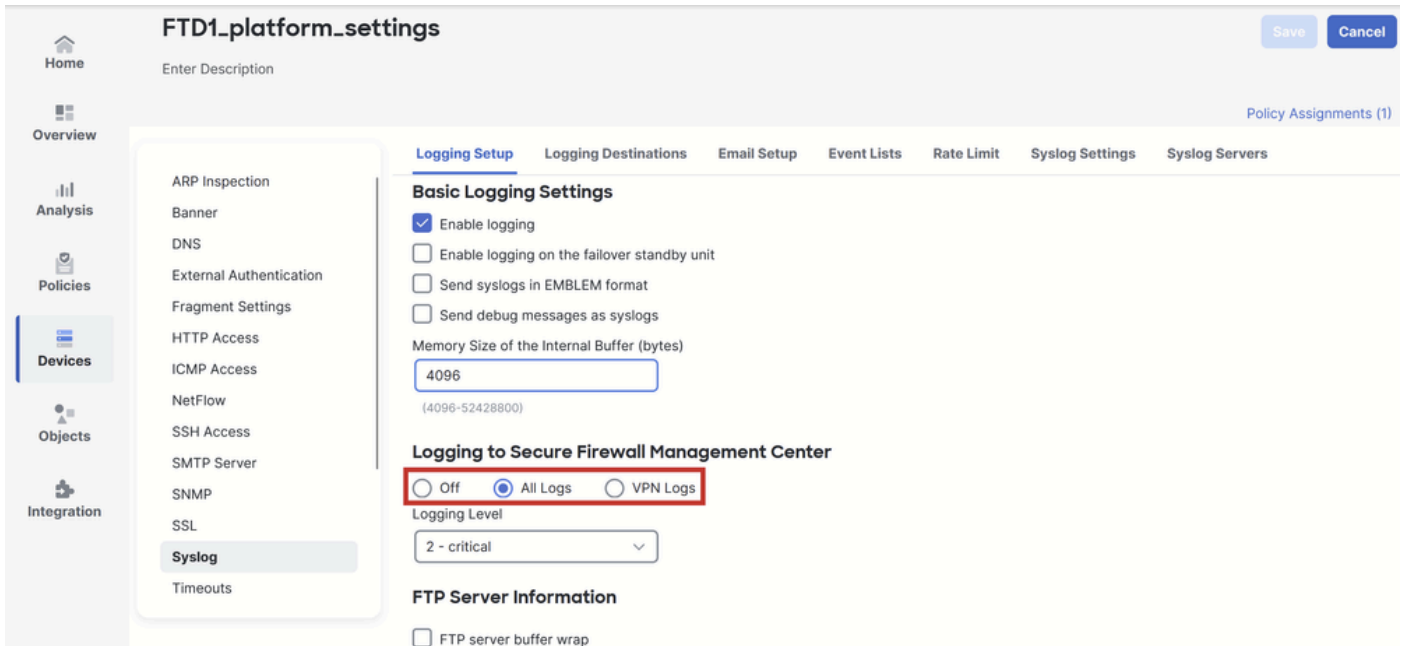


The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the title 'Firewall Management Center', and the breadcrumb 'Devices / Platform Settings'. A search bar, a 'Deploy' button, and user information 'admin' are also visible. The left sidebar contains navigation options: Home, Overview, Analysis, Policies, and Devices. The main content area displays a table with the following data:

Platform Settings	Device Type	Status	
FTD1_platform_settings	Threat Defense	Targeting 1 device(s) Up-to-date on all targeted devices	

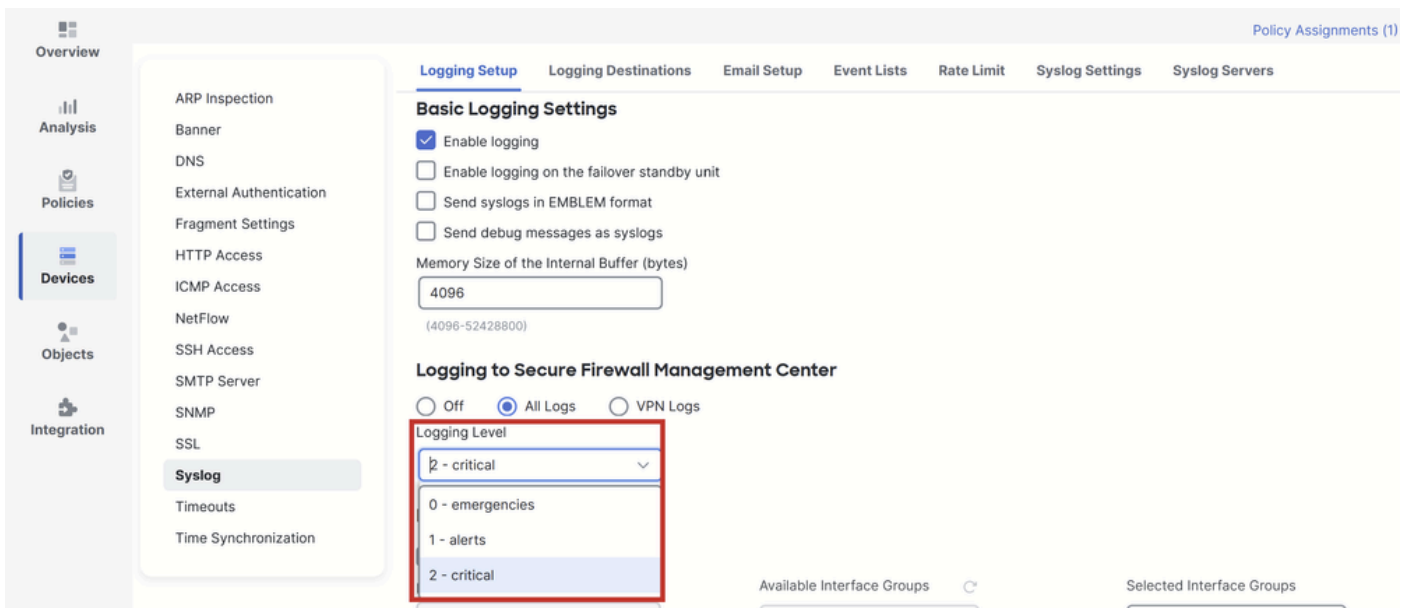
Stratégie des paramètres de plateforme

Accédez à Syslog > Logging Setup. Vous pouvez voir trois options sous Logging to Secure Firewall Management Center.



Trois options de journalisation

Si vous sélectionnez Tous les journaux, vous pouvez sélectionner l'un des trois niveaux de journalisation disponibles : urgences, alertes et critiques et envoyer tous les messages syslog de diagnostic à FMC (y compris VPN).



Niveaux de journalisation disponibles

Si vous choisissez VPN Logs, tous les niveaux de journalisation sont disponibles et l'un de ceux-ci peut être sélectionné.

Policy Assignments (1)

Overview

Analysis

Policies

Devices

Objects

Integration

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

NetFlow

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Performance Profile

Logging Setup | Logging Destinations | Email Setup | Event Lists | Rate Limit | Syslog Settings | Syslog Servers

Basic Logging Settings

- Enable logging
- Enable logging on the failover standby unit
- Send syslogs in EMBLEM format
- Send debug messages as syslogs

Memory Size of the Internal Buffer (bytes)

4096
(4096-52428800)

Logging to Secure Firewall Management Center

Off | All Logs | VPN Logs

Logging Level

3 - errors

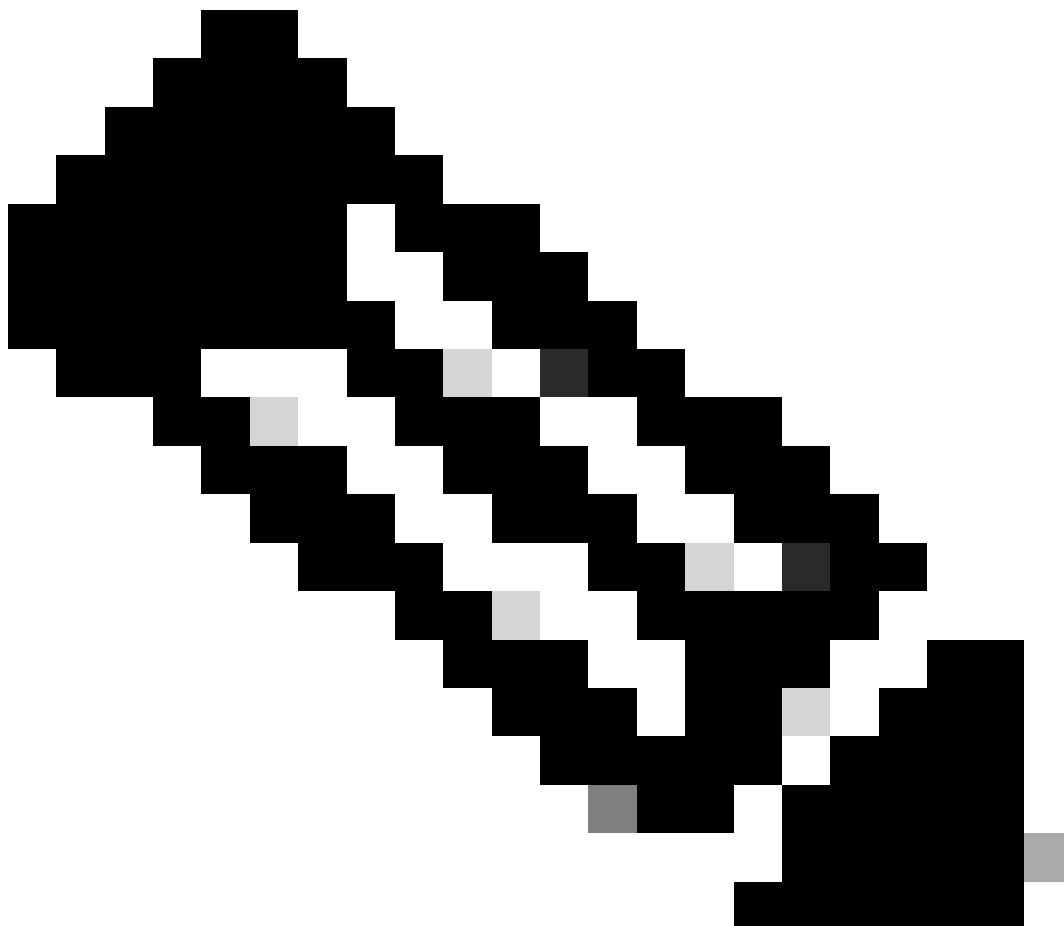
- 0 - emergencies
- 1 - alerts
- 2 - critical
- 3 - errors
- 4 - warnings
- 5 - notifications
- 6 - informational
- 7 - debugging

Available Interface Groups

Selected Interface Groups

Add

Niveaux de journalisation disponibles



Remarque : Lorsque vous configurez un périphérique avec un VPN de site à site ou

d'accès à distance, il active automatiquement l'envoi des syslog VPN au centre de gestion par défaut. Vous pouvez le modifier en All Logs pour envoyer tous les syslog à FMC en plus des journaux VPN.

Ces journaux sont accessibles depuis Périphériques > Dépannage > Journaux de dépannage.

The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the title 'Firewall Management Center', and the breadcrumb 'Devices / Troubleshoot / Troubleshooting Logs'. A search bar and a 'Deploy' button are also visible. The left sidebar contains navigation options: Home, Overview, Analysis, Policies, Devices (highlighted), Objects, and Integration. The main content area displays a table titled 'Table View of Troubleshooting Logs'. The table has columns for Time, Severity, Message, Message Class, Username, and Device. The data rows show various alerts from devices FTD1 and FTD2, with messages such as 'No response from other firewall' and 'Switching to OK'.

<input type="checkbox"/>	↓ Time ×	Severity ×	Message ×	Message Class ×	Username ×	Device ×
<input type="checkbox"/>	2025-01-15 19:59:43	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
<input type="checkbox"/>	2025-01-15 19:59:27	Alert	(Secondary) Disabling failover.	ha		FTD2
<input type="checkbox"/>	2025-01-15 19:59:13	Alert	(Primary) No response from other firewall (reason code = 3).	ha		FTD1
<input type="checkbox"/>	2025-01-15 19:49:12	Alert	(Primary) No response from other firewall (reason code = 3).	ha		FTD1
<input type="checkbox"/>	2025-01-15 19:43:28	Alert	(Secondary) Switching to OK.	ha		FTD2
<input type="checkbox"/>	2025-01-15 19:42:58	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
<input type="checkbox"/>	2025-01-15 19:42:54	Alert	(Secondary) No response from other firewall (reason code = 4).	ha		FTD2
<input type="checkbox"/>	2025-01-15 19:42:25	Alert	(Primary) No response from other firewall (reason code = 4).	ha		FTD1
<input type="checkbox"/>	2025-01-15 19:41:52	Alert	(Secondary) Switching to ACTIVE - HELLO not heard from peer.	ha		FTD2
<input type="checkbox"/>	2025-01-15 19:41:52	Alert	(Secondary) No response from other firewall (reason code = 4).	ha		FTD2
<input type="checkbox"/>	2025-01-15 19:41:51	Alert	(Secondary) Switching to OK.	ha		FTD2
<input type="checkbox"/>	2025-01-15 19:41:50	Alert	(Secondary) Switching to OK.	ha		FTD2

Tableau des journaux de dépannage

Un nouvel onglet d'affichage Dépannage est désormais disponible sur la page Unified Event Viewer. Pour afficher ces événements, accédez à Analysis > Unified Events > Troubleshooting.

Firewall Management Center
Analysis / Unified Events

Search Deploy admin

Events Troubleshooting

Search... Refresh

14 0 0 0 14 events 2025-01-16 15:33:44 IST 1h 16m Go Live

Time	Event Type	Action	Reason	Source IP	Destination IP	Source Po ICMP Type
> 2025-01-16 16:49:27	Connection	Block		198.51.100.178	192.0.2.171	2906 / tcp
> 2025-01-16 16:48:37	Connection	Block		198.51.100.134	192.0.2.171	9025 / tcp
> 2025-01-16 16:47:17	Connection	Allow		203.0.113.234	192.0.2.51	8902 / tcp
> 2025-01-16 16:46:17	Connection	Allow		203.0.113.149	198.51.100.27	6789 / tcp
> 2025-01-16 16:43:58	Connection	Block		192.0.2.214	203.0.113.139	8080 / tcp
> 2025-01-16 16:43:25	Connection	Block		192.0.2.214	198.51.100.71	8080 / tcp
> 2025-01-16 16:40:48	Connection	Allow		198.51.100.111	203.0.113.66	8 (Echo Re
> 2025-01-16 16:39:32	Connection	Allow		198.51.100.145	203.0.113.186	8 (Echo Re
> 2025-01-16 16:37:38	Connection	Block		198.51.100.39	192.0.2.176	7413 / tcp
> 2025-01-16 16:36:28	Connection	Block		203.0.113.75	198.51.100.112	8421 / tcp
> 2025-01-16 16:35:22	Connection	Allow		203.0.113.153	192.0.2.132	9876 / tcp
> 2025-01-16 16:33:10	Connection	Block		198.51.100.49	192.0.2.63	3692 / tcp
> 2025-01-16 16:32:10	Connection	Allow		198.51.100.95	203.0.113.99	8 (Echo Re
> 2025-01-16 16:31:15	Connection	Allow		192.0.2.25	203.0.113.249	1234 / tcp

Vue Dépannage

Un nouveau type d'événement est visible dans le tableau une fois que vous passez à cet onglet. Il ne peut pas être ajouté ou supprimé de la vue comme les autres types, car il est au centre de la vue Dépannage.

Firewall Management Center
Analysis / Unified Events

Search Deploy admin

Events Troubleshooting

Event Type Troubleshooting + Refresh

399 399 events 2025-01-15 15:33:44 IST 1d 1h Go Live

Time	Event Type	Source IP	Device	Domain	Message	Message Class
> 2025-01-15 19:59:43	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
> 2025-01-15 19:59:27	Troubleshooting		FTD2	Global	(Secondary) Disabling f...	ha
> 2025-01-15 19:59:13	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
> 2025-01-15 19:49:12	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
> 2025-01-15 19:43:28	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
> 2025-01-15 19:42:58	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
> 2025-01-15 19:42:54	Troubleshooting		FTD2	Global	(Secondary) No respon...	ha
> 2025-01-15 19:42:25	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
> 2025-01-15 19:41:52	Troubleshooting		FTD2	Global	(Secondary) No respon...	ha
> 2025-01-15 19:41:52	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
> 2025-01-15 19:41:51	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
> 2025-01-15 19:41:50	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
> 2025-01-15 19:41:50	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
> 2025-01-15 19:41:49	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
> 2025-01-15 19:41:48	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha

Type d'événement de dépannage

D'autres types d'événements peuvent toujours être ajoutés et supprimés de cette vue Dépannage. Cela vous permet d'afficher les journaux de diagnostic avec d'autres données d'événements.

Firewall Management Center
Analysis / Unified Events

Search Deploy admin

Events Troubleshooting

Event Type Troubleshooting Connection Intrusion + Refresh

399 14 0 413 events 2025-01-15 15:33:44 IST 1d 1h Go Live

Time	Event Type	Source IP	Device	Domain	Message	Message Class
2025-01-16 16:40:48	Connection	198.51.100.111	FTD1	Global		
2025-01-16 16:39:32	Connection	198.51.100.145	FTD1	Global		
2025-01-16 16:37:38	Connection	198.51.100.39	FTD1	Global		
2025-01-16 16:36:28	Connection	203.0.113.75	FTD1	Global		
2025-01-16 16:35:22	Connection	203.0.113.153	FTD1	Global		
2025-01-16 16:33:10	Connection	198.51.100.49	FTD1	Global		
2025-01-16 16:32:10	Connection	198.51.100.95	FTD1	Global		
2025-01-16 16:31:15	Connection	192.0.2.25	FTD1	Global		
2025-01-15 19:59:43	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:59:27	Troubleshooting		FTD2	Global	(Secondary) Disabling f...	ha
2025-01-15 19:59:13	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:49:12	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:43:28	Troubleshooting		FTD2	Global	(Secondary) Switching t...	ha
2025-01-15 19:42:58	Troubleshooting		FTD1	Global	(Primary) No response f...	ha
2025-01-15 19:42:54	Troubleshooting		FTD2	Global	(Secondary) No response f...	ha

Autres types d'événements

Vérifier la configuration

Une fois la configuration effectuée à partir de l'interface utilisateur graphique FMC, elle peut être vérifiée à partir de l'interface de ligne de commande FTD en exécutant les commandes `show running-config logging` et `show logging` en mode 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
```

Commande 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
```

Commande CLI FTD

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.