

Configuration de Syslog sur les appliances Firepower FXOS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Configurer Syslog à partir de l'interface utilisateur FXOS \(FPR4100/FPR9300\)](#)

[Configurer Syslog à partir de l'interface de ligne de commande FXOS \(FPR4100/FPR9300\)](#)

[Vérification de la configuration via l'interface de ligne de commande](#)

[Vérifier que les messages Syslog apparaissent sous Terminal Monitor](#)

[Vérification du service pour les hôtes distants configurés](#)

[Vérifier que le fichier journal local est correctement consigné à partir de FXOS](#)

[Générer des messages Syslog de test](#)

[Syslog FXOS dans les appliances Firepower 2100](#)

[Périphérique logique ASA dans FPR2100](#)

[Périphérique logique FTD dans FPR2100](#)

[Forum aux questions](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer, vérifier et dépanner Syslog sur les appliances FXOS (Firepower eXtensible Operating System).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- 1x FPR4120 avec logiciel FXOS version 2.2(1.70)
- 1x FPR2110 avec logiciel ASA version 9.9(2)
- 1x FPR2110 avec logiciel FTD version 6.2.3
- 1 serveur Syslog

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

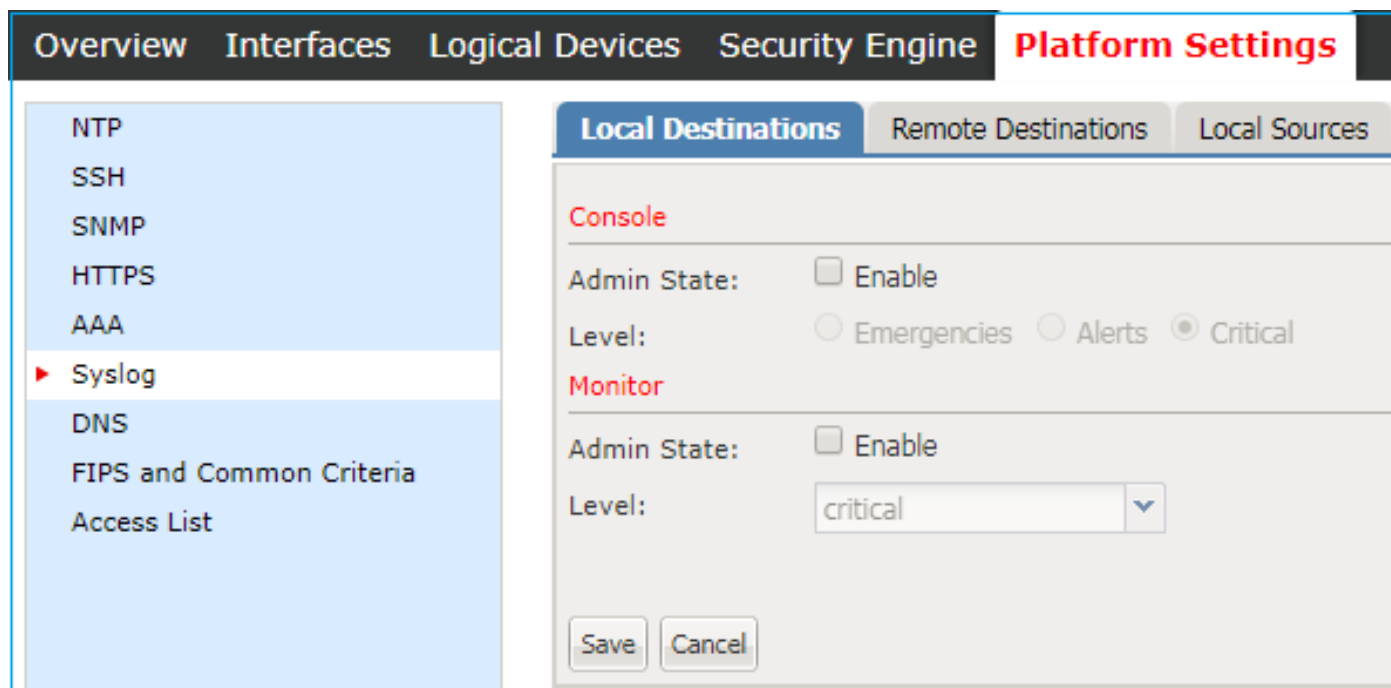
est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Configurer Syslog à partir de l'interface utilisateur FXOS (FPR4100/FPR9300)

FXOS possède son propre jeu de messages Syslog qui peuvent être activés et configurés à partir du Firepower Chassis Manager (FCM).

Étape 1. Accédez à **Paramètres de la plate-forme > Syslog**.



The screenshot shows the 'Platform Settings' page in the FXOS interface. The left sidebar contains a menu with the following items: NTP, SSH, SNMP, HTTPS, AAA, Syslog (highlighted with a red arrow), DNS, FIPS and Common Criteria, and Access List. The main content area is titled 'Platform Settings' and has three tabs: 'Local Destinations' (selected), 'Remote Destinations', and 'Local Sources'. Under the 'Local Destinations' tab, there are two sections: 'Console' and 'Monitor'. The 'Console' section has an 'Admin State' checkbox (unchecked) labeled 'Enable', and a 'Level' section with three radio buttons: 'Emergencies', 'Alerts', and 'Critical' (selected). The 'Monitor' section has an 'Admin State' checkbox (unchecked) labeled 'Enable', and a 'Level' dropdown menu currently set to 'critical'. At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

Étape 2. Sous **Destinations locales**, vous pouvez activer les messages Syslog sur la console pour les niveaux 0 à 2 ou la surveillance locale de Syslog pour tout niveau stocké localement. Considérez que tous les niveaux de gravité sélectionnés sont également affichés pour les deux méthodes : console et moniteur.

Overview Interfaces Logical Devices Security Engine **Platform Settings**

NTP
SSH
SNMP
HTTPS
AAA
► **Syslog**
DNS
FIPS and Common Criteria
Access List

Local Destinations Remote Destinations Local Sources

Console

Admin State: **1** Enable

Level: Emergencies **2** Alerts Critical

Monitor

Admin State: Enable

Level: errors

3 Save Cancel

Overview Interfaces Logical Devices Security Engine **Platform Settings**

NTP
SSH
SNMP
HTTPS
AAA
► **Syslog**
DNS
FIPS and Common Criteria
Access List

Local Destinations Remote Destinations Local Sources

Console

Admin State: Enable

Level: Emergencies Alerts Critical

Monitor

Admin State: **1** Enable

Level: errors

errors
emergencies
alerts
critical
errors
warnings
notifications
information
debugging

Save Cancel **2**

3

À partir de la version 2.3.1 de FXOS, vous pouvez également configurer via l'interface utilisateur graphique une destination de fichier locale pour les messages Syslog :

- NTP
- SSH
- SNMP
- HTTPS
- AAA
- ▶ **Syslog**
- DNS
- FIPS and Common Criteria
- Access List
- MAC Pool
- Resource Profiles
- Network Control Policy
- Chassis URL

Local Destinations
Remote Destinations
Local Sources

Console

Admin State: Enable

Level: Emergencies Alerts Critical

Monitor

Admin State: Enable

Level:

File

Admin State: Enable

Level:

Name:

Size: *

Note: La taille du fichier ne peut avoir qu'une taille comprise entre 4096 et 4194304 octets.

Note: Dans la version FXOS antérieure à la version 2.3.1, la configuration de fichier est disponible uniquement via l'interface de ligne de commande.

Vous pouvez également configurer jusqu'à 3 serveurs Syslog distants à partir de l'onglet **Destinations distantes**. Chaque serveur peut être défini comme une destination pour différents messages de niveau de gravité Syslog et marqué avec une fonction locale différente.

- NTP
- SSH
- SNMP
- HTTPS
- AAA
- **Syslog**
- DNS
- FIPS and Common Criteria
- Access List
- MAC Pool
- Resource Profiles
- Network Control Policy
- Chassis URL

Local Destinations **Remote Destinations** Local Sources

Server 1

Admin State: Enable

Level: Warnings

Hostname/IP Address:* 10.61.161.235

Facility: Local1

Server 2

Admin State: Enable

Level: Critical

Hostname/IP Address:* none

Facility: Local7

Server 3

Admin State: Enable

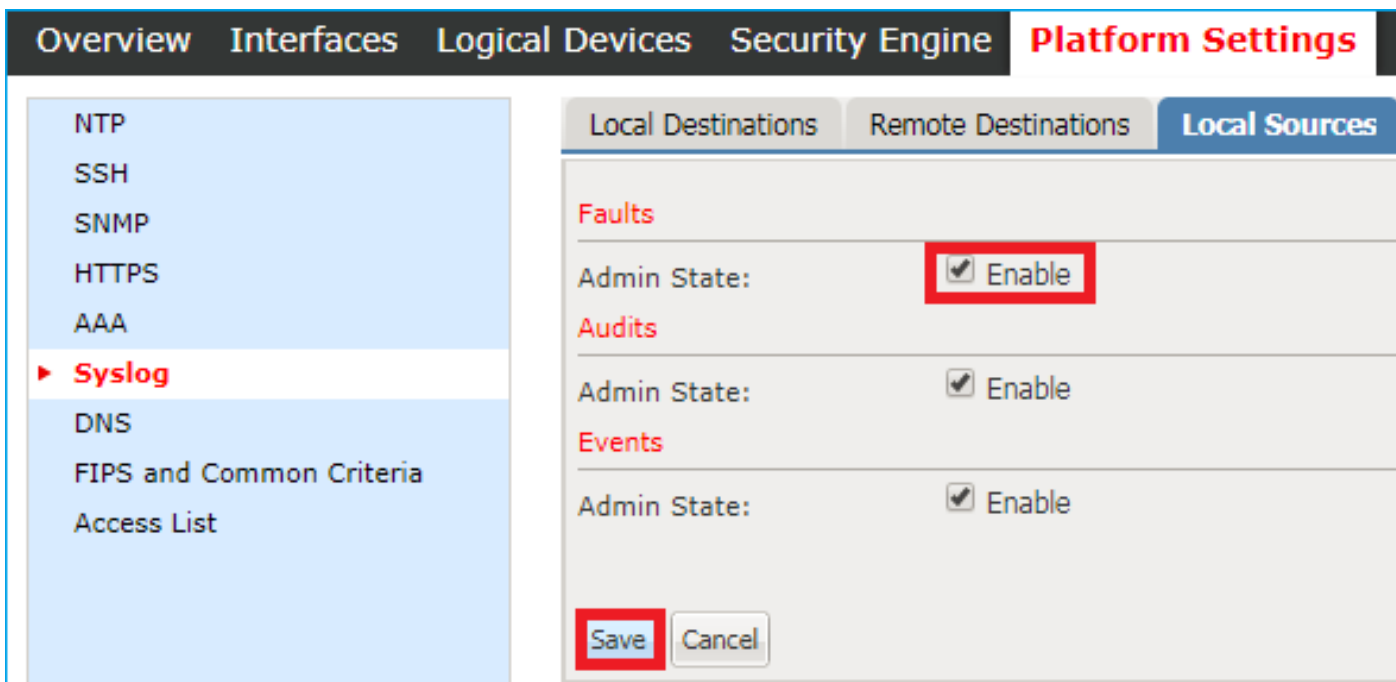
Level: Critical

Hostname/IP Address:* none

Facility: Local7

Save Cancel

Étape 3. Enfin, sélectionnez **Sources locales** supplémentaires pour les messages Syslog. FXOS peut être utilisé comme source Syslog Faults, messages d'audit et/ou événements.



Configurer Syslog à partir de l'interface de ligne de commande FXOS (FPR4100/FPR9300)

Configurez via CLI l'équivalent de la section **Destinations locales** :

```
FP4120-A /monitoring # enable syslog console
FP4120-A /monitoring* # set syslog console level critical
FP4120-A /monitoring* # enable syslog monitor
FP4120-A /monitoring* # set syslog monitor level warning
FP4120-A /monitoring* # commit-buffer
```

Configurez via CLI l'équivalent de la section **Destinations distantes** :

```
FP4120-A /monitoring # enable syslog remote-destination server-1
FP4120-A /monitoring* # set syslog remote-destination server-1 facility local1
FP4120-A /monitoring* # set syslog remote-destination server-1 level warning
FP4120-A /monitoring* # set syslog remote-destination server-1 hostname 10.61.161.235
FP4120-A /monitoring* # commit-buffer
```

Configurez via CLI l'équivalent de la section **Sources locales** :

```
FP4120-A /monitoring # enable syslog source audits
FP4120-A /monitoring* # enable syslog source events
FP4120-A /monitoring* # enable syslog source faults
FP4120-A /monitoring* # commit-buffer
```

En outre, vous pouvez activer un fichier local en tant que destination Syslog. Ces messages Syslog peuvent être affichés à l'aide des commandes **show logging** ou **show logging logfile** :

```
FP4120-A /monitoring # enable syslog file
FP4120-A /monitoring* # set syslog file level warning
FP4120-A /monitoring* # set syslog file name Logging
```

FP4120-A /monitoring* # **commit-buffer**

Note: La taille par défaut de ce fichier est la taille maximale (4194304 octets).

Vérification de la configuration via l'interface de ligne de commande

La configuration peut être vérifiée et configurée à partir de la **surveillance** de la portée :

```
FP4120-A# scope monitoring  
FP4120-A /monitoring # show syslog
```

console

```
state: Enabled  
level: Critical
```

monitor

```
state: Enabled  
level: warning
```

file

```
state: Enabled  
level: warning  
name: Logging  
size: 4194304
```

remote destinations

Name	Hostname	State	Level	Facility
Server 1	10.61.161.235	Enabled	warning	Local1
Server 2	none	Disabled	Critical	Local7
Server 3	none	Disabled	Critical	Local7

sources

```
faults: Enabled  
audits: Enabled  
events: Enabled
```

Vous pouvez également obtenir une sortie plus complète de l'interface de ligne de commande FXOS avec la commande **show logging** :

```
FP4120-A(fxos)# show logging
```

```
Logging console:           enabled (Severity: critical)  
Logging monitor:          enabled (Severity: warning)  
Logging linecard:         enabled (Severity: notifications)  
Logging fex:              enabled (Severity: notifications)  
Logging timestamp:        Seconds  
Logging server:           enabled  
{10.61.161.235}  
server severity:          warning  
server facility:          local1  
server VRF:               management  
Logging logfile:          enabled  
Name - Logging: Severity - warning Size - 4194304
```

Facility	Default Severity	Current Session Severity
-----	-----	-----
aaa	3	7
acllog	2	7
aclmgr	3	7
afm	3	7
assoc_mgr	7	7
auth	0	7
authpriv	3	7
bcm_usd	3	7
bootvar	5	7
callhome	2	7
capability	2	7
capability	2	7
cdp	2	7
cert_enroll	2	7
cfs	3	7
clis	7	7
confcheck	2	7
copp	2	7
cron	3	7
daemon	3	7
device-alias	3	7
epp	5	7
eth_port_channel	5	7
eth_port_sec	2	7
ethpc	2	7
ethpm	5	7
evmc	5	7
fabric_start_cfg_mgr	2	7
fc2d	2	7
fcdomain	3	7
fcns	2	7
fcpc	2	7
fcs	2	7
fdmi	2	7
feature-mgr	2	7
fex	5	7
flogi	2	7
fspf	3	7
ftp	3	7
fwm	6	7
ifmgr	5	7
igmp_1	5	7
ip	3	7
ipqosmgr	4	7
ipv6	3	7
kern	3	7
l3vm	5	7
lacp	2	7
ldap	2	7
ldap	2	7
licmgr	6	7
lldp	2	7
local0	3	7
local1	3	7
local2	3	7
local3	3	7
local4	3	7
local5	3	7
local6	3	7
local7	3	7
lpr	3	7
m2rib	2	7

mail	3	7
mcm	2	7
monitor	3	7
mrrib	5	7
msh	5	7
mvsh	2	7
news	3	7
nfp	2	7
nohms	2	7
nsmgr	5	7
ntp	2	7
otm	3	7
pfstat	2	7
pim	5	5
platform	5	7
plugin	2	7
port	5	7
port-channel	5	7
port-profile	2	7
port-resources	5	7
private-vlan	3	7
qd	2	7
radius	3	7
rdl	2	7
res_mgr	5	7
rib	2	7
rlir	2	7
rpm	5	7
rscn	2	7
sal	2	7
scsi-target	2	7
securityd	3	7
smm	4	7
snmpd	2	7
span	3	7
stp	3	7
syslog	3	7
sysmgr	3	7
tacacs	3	7
u6rib	5	7
udld	5	7
urib	5	7
user	3	7
uucp	3	7
vdc_mgr	6	7
vim	5	7
vlan_mgr	2	7
vmm	5	7
vms	5	7
vntag_mgr	6	7
vsan	2	7
vshd	5	7
wwn	3	7
xmlma	3	7
zone	2	7
zschk	2	7

0(emergencies)	1(alerts)	2(critical)
3(errors)	4(warnings)	5(notifications)
6(information)	7(debugging)	

2017 Nov 26 16:49:19 FP4120-5-A %\$ VDC-1 %\$ %LOCAL0-2-SYSTEM_MSG: Test-Syslog - ucssh[18553]

Vérifier que les messages Syslog apparaissent sous Terminal Monitor

Lorsque le moniteur Syslog est activé, les messages Syslog sont sous l'interface de ligne de commande FXOS lorsque le terminal de surveillance est activé.

```
FP4120-A(fxos)# terminal monitor
2017 Nov 26 16:39:35 FP4120-5-A %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1910369168]
[client 127.0.0.1:34975] AH01964: Connection to child 40 established (server 10.62.148.187:443)
- httpd[23982]
2017 Nov 26 16:39:36 FP4120-5-A %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1908272016]
[client 127.0.0.1:34977] AH01964: Connection to child 42 established (server 10.62.148.187:443)
- httpd[23982]
2017 Nov 26 16:39:36 FP4120-5-A %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1911417744]
(70014)End of file found: [client 127.0.0.1:34972] AH01991: SSL input filter read failed. -
httpd[23982]
```

Vérification du service pour les hôtes distants configurés

Vérifiez que les messages sont reçus sur le serveur Syslog.

Date	Time	Priority	Hostname	Message
11-26-2017	16:03:03	Local1.Info	10.62.148.187	: 2017 Nov 26 15:40:46 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid
11-26-2017	16:03:03	Local1.Info	10.62.148.187	: 2017 Nov 26 15:40:46 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid
11-26-2017	16:03:01	Local1.Info	10.62.148.187	: 2017 Nov 26 15:40:44 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid

Capturez le trafic sur l'interface de ligne de commande FXOS à l'aide de l'outil Ethalyzer pour confirmer que les messages Syslog sont générés et envoyés par FXOS.

Dans cet exemple, la destination du message correspond au serveur Syslog local (10.61.161.235), à l'indicateur d'installation (Local1) et à la gravité du message (6) :

```
FP4120-A(fxos)# ethalyzer local interface mgmt capture-filter "host 10.61.161.235 && udp port
514"
Capturing on eth0
wireshark-broadcom-rcpu-dissector: ethertype=0xde08, devicetype=0x0
2017-11-26 16:01:38.881829 10.62.148.187 -> 10.61.161.235 Syslog LOCAL1.INFO: : 2017 Nov 26
16:01:38 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1799220112] (70014)End of file
found: [client 127.0.0.1:51015] AH01991: SSL input filter read failed. - httpd[23982]
2017-11-26 16:01:38.882574 10.62.148.187 -> 10.61.161.235 Syslog LOCAL1.INFO: : 2017 Nov 26
16:01:38 UTC: Nov 26 16:01:37 %KERN-6-SYSTEM_MSG: [363494.943876] device eth0 entered
promiscuous mode - kernel
2017-11-26 16:01:38.883333 10.62.148.187 -> 10.61.161.235 Syslog LOCAL1.INFO: : 2017 Nov 26
16:01:38 UTC: %USER-6-SYSTEM_MSG: [ssl:info] [pid 23982:tid 1782442896] (70014)End of file
found: [client 127.0.0.1:51018] AH01991: SSL input filter read failed. - httpd[23982]
```

Vérifier que le fichier journal local est correctement consigné à partir de FXOS

```
FP4120-A(fxos)# show logging logfile
2017 Nov 26 15:20:22 FP4120-5-A %SYSLOG-1-SYSTEM_MSG : Logging logfile (messages) cleared by
user
2017 Nov 26 16:24:21 FP4120-5-A %USER-7-SYSTEM_MSG: Semaphore lock success - aaad
2017 Nov 26 16:24:21 FP4120-5-A %USER-7-SYSTEM_MSG: accounting_sem_unlock Semaphore unlock
succeeded - aaad
2017 Nov 26 16:24:21 FP4120-5-A %USER-7-SYSTEM_MSG: Semaphore lock success - aaad
```

Générer des messages Syslog de test

Il est également possible de générer des messages Syslog de n'importe quelle gravité à la demande à des fins de test via CLI. Ainsi, dans les serveurs Syslog très actifs, vous pouvez définir un filtre plus spécifique pour vous aider à confirmer que les messages Syslog sont correctement envoyés :

```
FP4120-A /monitoring # send-syslog critical Test-Syslog
```

Ce message est transmis à n'importe quelle destination Syslog et peut être utile dans les scénarios où le filtrage d'une source Syslog spécifique n'est pas possible :

```
FP4120-A(fxos)# show logging logfile
```

```
2017 Nov 26 16:49:19 FP4120-5-A %$ VDC-1 %$ %LOCAL0-2-SYSTEM_MSG: Test-Syslog - ucssh[18553]
```

Date	Time	Priority	Hostname	Message
11-26-2017	17:11:36	Local1.Critical	10.62.148.187	: 2017 Nov 26 16:49:19 UTC: %LOCAL0-2-SYSTEM_MSG: Testing-Syslog - ucssh[18553]

Syslog FXOS dans les appliances Firepower 2100

Périphérique logique ASA dans FPR2100

Il existe deux différences principales entre la configuration Syslog pour les appliances Firepower 4100/9300 et Firepower 2100 avec le logiciel ASA.

1. Dans Firepower 2100, la journalisation de la plate-forme est activée par défaut et ne peut pas être désactivée.
2. Il n'y a pas de journalisation du moniteur en raison du fait que le terminal du moniteur n'existe pas dans les plates-formes FP2100.

Les sections **Destinations distantes** et **Sources locales** sont identiques aux autres plates-formes.

Le fichier journal et les journaux en direct de la plate-forme ne sont pas accessibles via les commandes CLI.

Périphérique logique FTD dans FPR2100

Dans le FPR2100 où le dispositif FTD est installé, il y a deux différences majeures par rapport aux autres topologies :

1. L'adresse IP source est identique à celle utilisée pour les messages Syslog du périphérique logique.
2. Tous les messages FXOS sont utilisés pour l'ID Syslog du message pour les processus génériques d'ASA 199013-199019

```
firepower# show logging | include 1990
%ASA-6-199018: May 11 18:10:55 fp2100a port-manager: Informational: Ethernet1/12: admin state changed to down
%ASA-7-199019: May 11 18:10:55 fp2100a port-manager: LINK STATE CHANGE: port 50, new state 0/0/0
%ASA-2-199014: May 11 18:10:56 fp2100a port-manager: Alert: Ethernet1/12 link changed to DOWN
%ASA-6-199018: May 11 18:10:56 fp2100a port-manager: Informational: Ethernet1/12 speed changed to Unknown
```

Dans cet exemple, il y a les messages Syslog d'arrêt d'interface.

Forum aux questions

Quel est le port par défaut utilisé par Syslog ?

Par défaut, Syslog utilise le port UDP 514

Pouvez-vous configurer Syslog via TCP ?

Syslog via TCP est uniquement pris en charge pour FPR2100 avec les appliances FTD où les Syslogs FXOS sont intégrés aux messages ASA

Informations connexes

- [Guide de configuration de la CLI FXOS](#)
- [Support et documentation techniques - Cisco Systems](#)