

Identifier et analyser les événements de basculement FTD sur FMC

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Événements de basculement sur FMC](#)

[Étape 1. Configuration de la stratégie de santé](#)

[Étape 2. Affectation de stratégie](#)

[Étape 3. Alertes d'événements de basculement](#)

[Étape 4. Événements de basculement historiques](#)

[Étape 5. Tableau de bord haute disponibilité](#)

[Étape 6. CLI Threat Defense](#)

[Informations connexes](#)

Introduction

Ce document décrit comment identifier et analyser les événements de basculement pour Secure Firewall Threat Defense sur l'interface utilisateur graphique de Secure Firewall Management Center.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration haute disponibilité (HA) pour Cisco Secure Firewall Threat Defense (FTD)
- Facilité d'utilisation de base de Cisco Firewall Management Center (FMC)

Composants utilisés

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

- Cisco FMC v7.2.5
- Gamme Cisco Firepower 9300 v7.2.5

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.

Informations générales

Le FMC n'est pas seulement le centre administratif des périphériques Firepower, au-delà des options de gestion et de configuration, il fournit également une interface graphique qui permet d'analyser les journaux et les événements en temps réel et passé.

En matière de basculement, l'interface présente de nouvelles améliorations qui permettent d'analyser les événements de basculement afin de comprendre les pannes.

Événements de basculement sur FMC

Étape 1. Configuration de la stratégie de santé

Le module Cluster/HA Failure Status est activé par défaut sur la politique d'intégrité, mais en outre, vous pouvez activer l'option Split-brain check.

Afin d'activer les options pour la haute disponibilité dans la politique de santé, accédez à [System > Health > Policy > Firewall Threat Defense Health Policy > High Availability](#).

Cette image décrit la configuration haute disponibilité de la politique d'intégrité :

The screenshot shows the Firewall Management Center interface. The breadcrumb navigation is System / Health / Policy. The main heading is 'Initial_Health_Policy 2023-08-29 15:26:44' with a sub-heading 'Initial Health Policy'. There are two tabs: 'Health Modules' (selected) and 'Run Time Intervals'. Under 'Health Modules', there are three items, each with a toggle switch:

- Disk Usage** (toggle on):
 - Monitors disk usage
 - Warning threshold: 85 %
 - Critical threshold: 90 %
 - Warning Threshold (secondary HD): 97 %
 - Critical Threshold (secondary HD): 99 %
- High Availability** (toggle on)
- Cluster/HA Failure Status** (toggle on):
 - Monitors cluster and HA members for their availability failure
- Firewall Threat Defense HA (Split-brain check)** (toggle on):
 - Monitors Firewall Threat Defense HA for split-brain (Both HA members are in active state)

Below these is an 'Integration' section with a toggle switch that is currently off.

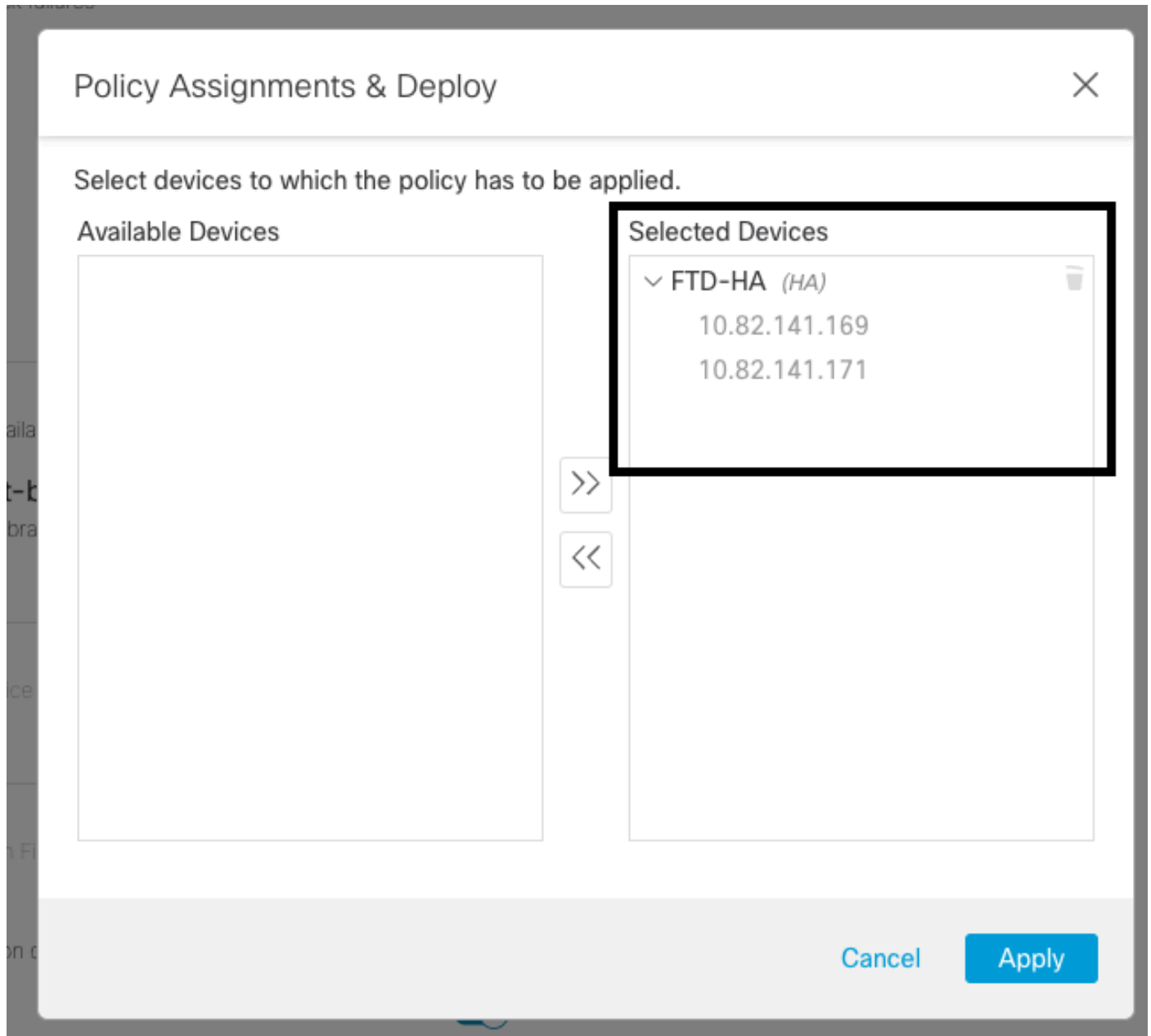
Paramètres d'intégrité haute disponibilité

Étape 2. Affectation de stratégie

Assurez-vous que la politique d'intégrité est attribuée aux paires haute disponibilité que vous souhaitez surveiller à partir du FMC.

Afin d'attribuer la stratégie, accédez à `System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy`.

Cette image montre comment attribuer la stratégie d'intégrité à la paire haute disponibilité :



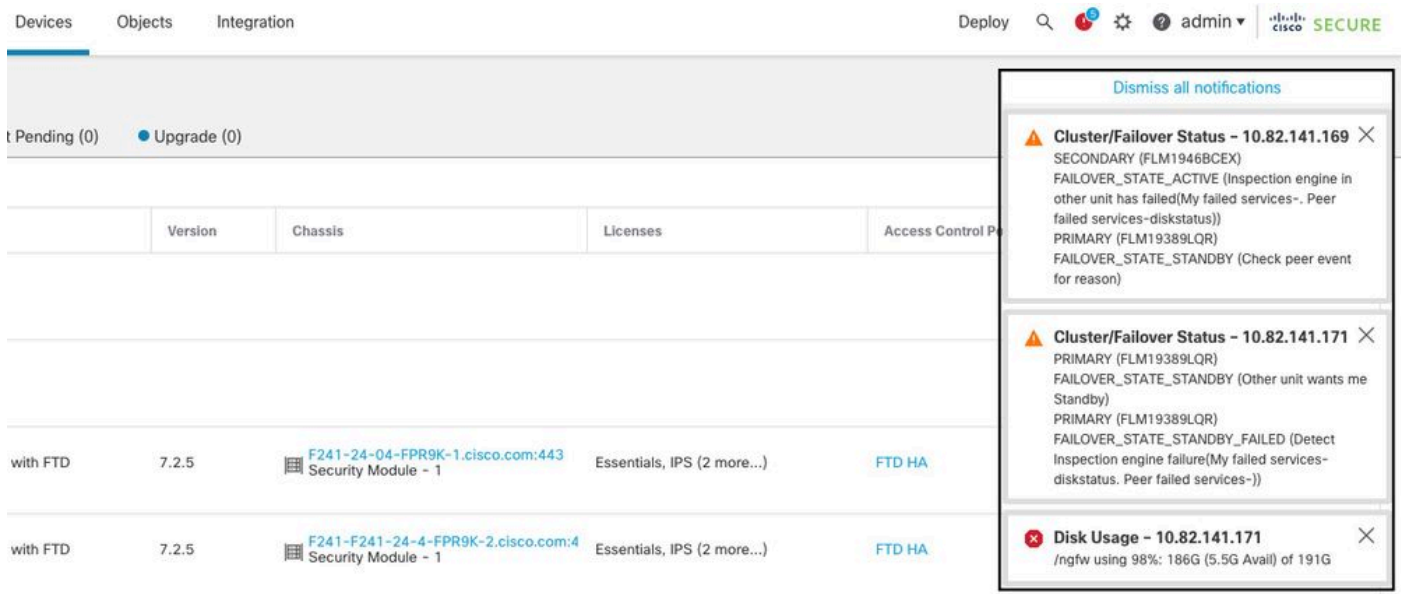
Affectation haute disponibilité

Une fois la stratégie attribuée et enregistrée, le FMC l'applique automatiquement au FTD.

Étape 3. Alertes d'événements de basculement

Selon la configuration de la haute disponibilité, une fois qu'un événement de basculement est déclenché, les alertes contextuelles qui décrivent l'échec du basculement s'affichent.

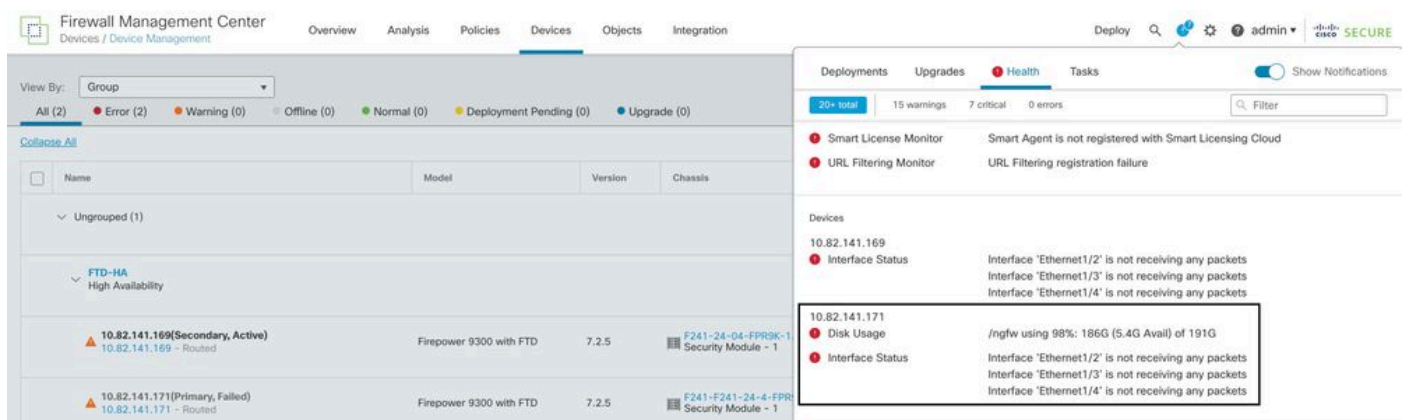
Cette image présente les alertes de basculement générées :



Alertes de basculement

Vous pouvez également accéder à Notifications > Health afin de visualiser les alertes d'intégrité de basculement.

Cette image présente les alertes de basculement sous les notifications :



Notifications HA

Étape 4. Événements de basculement historiques

Le FMC permet de visualiser les événements de basculement qui se sont produits dans le passé. Pour filtrer les événements, accédez à System > Health > Events > Edit Search et spécifiez le nom du module en tant qu'état de cluster/basculement. En outre, le filtre peut être appliqué en fonction de l'état.

Cette image montre comment filtrer les événements de basculement :

General Information

Module Name	<input type="text" value="Cluster/Failover Status"/>	Disk Status, Interface Status
Value	<input type="text"/>	25
Description	<input type="text"/>	Sample Description
Units	<input type="text"/>	unit
Status	<input type="text" value="Warning"/>	Critical, Warning, Normal, Recovered
Device	<input type="text"/>	device1.example.com, *.example.com, 192.168.1.3

Messages de filtre de basculement

Vous pouvez ajuster les paramètres d'heure afin d'afficher les événements pour une date et une heure spécifiques. Pour modifier les paramètres d'heure, accédez à [System > Health > Events > Time](#).

Cette image montre comment modifier les paramètres d'heure :

The screenshot displays the Firewall Management Center interface. The main content area shows a 'Table View of Health Events' with a list of events. A modal dialog titled 'Health Monitoring Time Window' is open, allowing for time range configuration. The 'Expanding Time Window' dropdown is selected. The 'Start Time' is set to 2023-09-27 11:02 and the 'End Time' is set to 2023-09-28 11:14. The 'Presets' section shows '1 hour' selected under 'Last' and 'Day' under 'Current'. The background table shows multiple rows of 'Cluster/Failover Status' events for device '10.82.141.171'.

Filtre de temps

Une fois que les événements ont été identifiés, afin de confirmer la raison de l'événement, pointez le curseur sous Description.

Cette image montre comment la raison du basculement peut être vue.



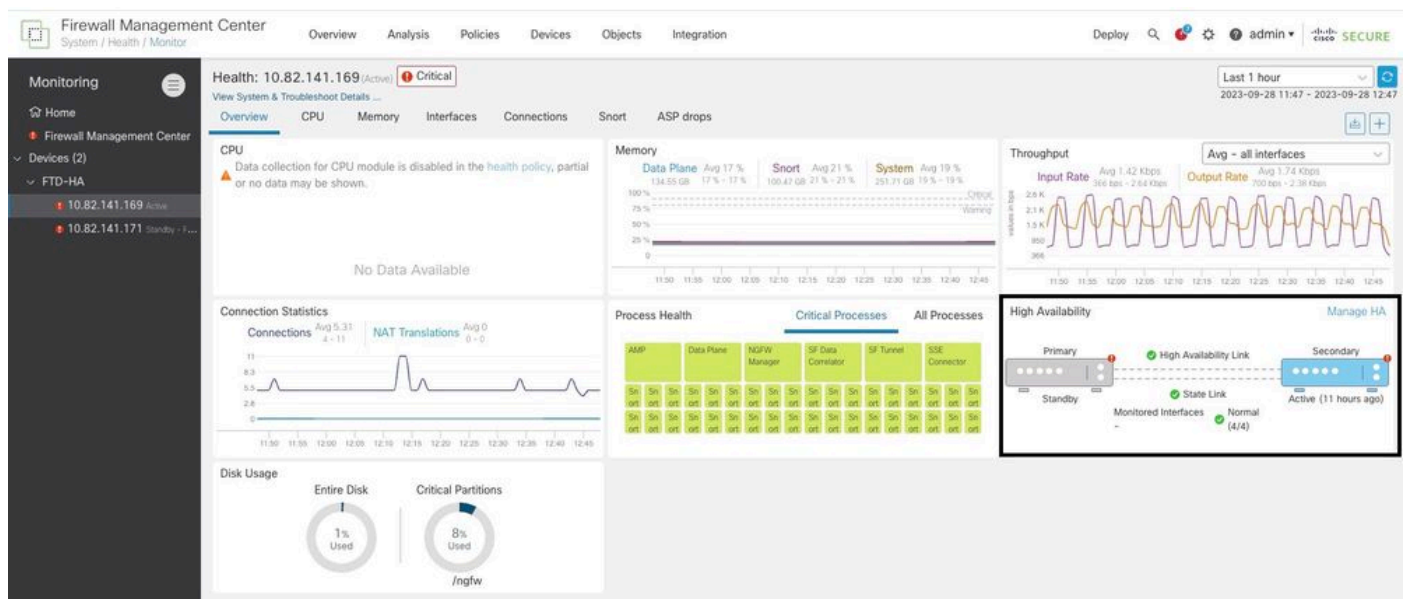
détails du basculement

Étape 5. Tableau de bord haute disponibilité

Une autre méthode de surveillance du basculement est disponible sous System > Health Monitor > Select Active or Standby Unit.

Le moniteur de haute disponibilité fournit des informations sur l'état de la haute disponibilité et de la liaison d'état, des interfaces surveillées, du ROL et de l'état des alertes sur chaque unité.

Cette image montre le moniteur haute disponibilité :



Graphiques de santé

Afin de visualiser les alertes, accédez à System > Health Monitor > Select Active or Standby Unit > Select the Alerts.



Monitoring

- Home
- Firewall Management Center
- Devices (2)
 - FTD-HA
 - 10.82.141.169 Active
 - 10.82.141.171 Standby - F...

Health: 10.82.141.171 (Standby - Failed) **Critical**

View System & Troubleshoot Det

Overview CPU

CPU

▲ Data collection for CPU or no data may be show

FTD-HA (HA-Standby - Failed)

10.82.141.171 - Critical

Alerts: 2 | 0 | 17

Top 5 Alerts

- Disk Usage
- Interface Status
- Firewall Threat Defense HA (Split-brain check)
- Snort Identity Memory Usage
- Configuration Resource Utilization

[View all alerts](#)

No Data Available

Alertes

Pour obtenir plus de détails sur les alertes, sélectionnez [View all alerts > see more.](#)

Cette image montre l'état du disque à l'origine du basculement :

Health Alerts - 10.82.141.171

19 total 2 critical 0 warnings 7 normal

[Export](#) [Run All](#)

Sep 28, 2023 12:47 PM

Disk Usage

/ngfw using 98%: 186G (5.4G Avail) of 191G [see less](#)

Local Disk Partition Status

Mount	Size	Free	Used	Percent
/mnt/boot	7.5G	7.3G	208M	3%
/opt/cisco/config	1.9G	1.8G	3.4M	1%
/opt/cisco/platform/logs	4.6G	4.3G	19M	1%
/var/data/cores	46G	43G	823M	2%
/opt/cisco/csp	684G	498G	187G	28%
/ngfw	191G	5.4G	186G	98%

Interface Status

Interface 'Ethernet1/2' is not receiving any packets
Interface 'Ethernet1/3' is not receiving any packets
Interface 'Ethernet1/4' is not receiving any packets [see more](#)

Appliance Heartbeat

All appliances are sending heartbeats correctly.

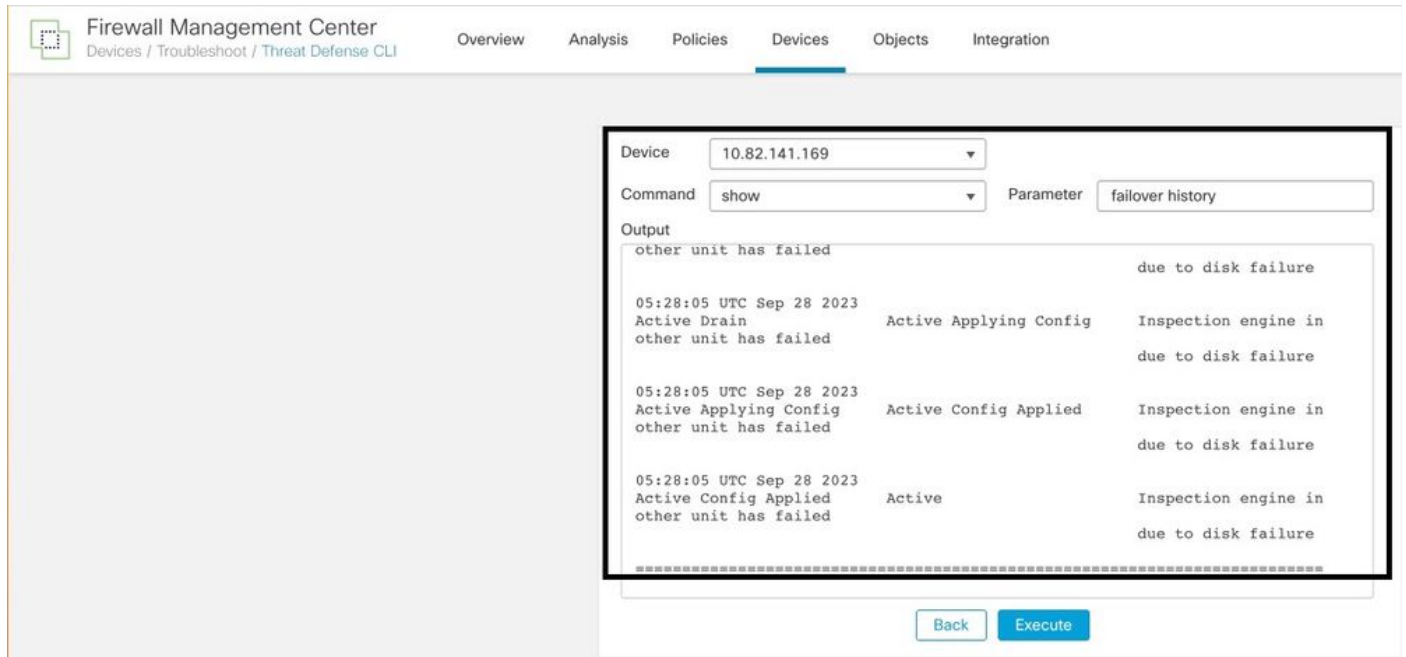
Automatic Application Runas Status

Sep 28, 2023 12:47 PM

Étape 6. CLI Threat Defense

Enfin, afin de collecter des informations supplémentaires sur FMC, vous pouvez accéder à **Devices > Troubleshoot > Threat Defense CLI**. Configurez les paramètres tels que **Device** et la commande à exécuter, puis cliquez sur **Execute**.

Cette image présente un exemple de la commande `show failover history` qui peut être exécuté sur le FMC où vous pouvez identifier l'échec du basculement.



historique de basculement

Informations connexes

- [Haute disponibilité pour FTD](#)
- [Configurer la haute disponibilité FTD sur les appareils Firepower](#)
- [Assistance et documentation techniques - Cisco Systems](#)

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.