

FMCでのFTDフェールオーバーイベントの特定と分析

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[FMCでのフェールオーバーイベント](#)

[ステップ 1: 正常性ポリシーの構成](#)

[ステップ 2: ポリシーの割り当て](#)

[ステップ 3: フェールオーバーイベントアラート](#)

[ステップ 4: 履歴フェールオーバーイベント](#)

[ステップ 5: ハイアベイラビリティダッシュボード](#)

[手順 6: 脅威対策CLI](#)

[関連情報](#)

概要

このドキュメントでは、Secure Firewall Management Center(FMC)GUIでSecure Firewall Threat Defenseのフェールオーバーイベントを識別して分析する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Firewall Threat Defense(FTD)のハイアベイラビリティ(HA)のセットアップ
- Cisco Firewall Management Center(FMC)の基本的な操作性

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco FMC v7.2.5
- Cisco Firepower9300シリーズv7.2.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して

ください。

背景説明

FMCは、管理オプションや設定オプションの他に、Firepowerデバイスの管理センターであるだけでなく、リアルタイムおよび過去のログやイベントの分析に役立つグラフィカルインターフェイスも提供します。

フェールオーバーに関しては、フェールオーバーのイベントを分析して障害を把握するのに役立つ新しい改良がインターフェイスに加えられています。

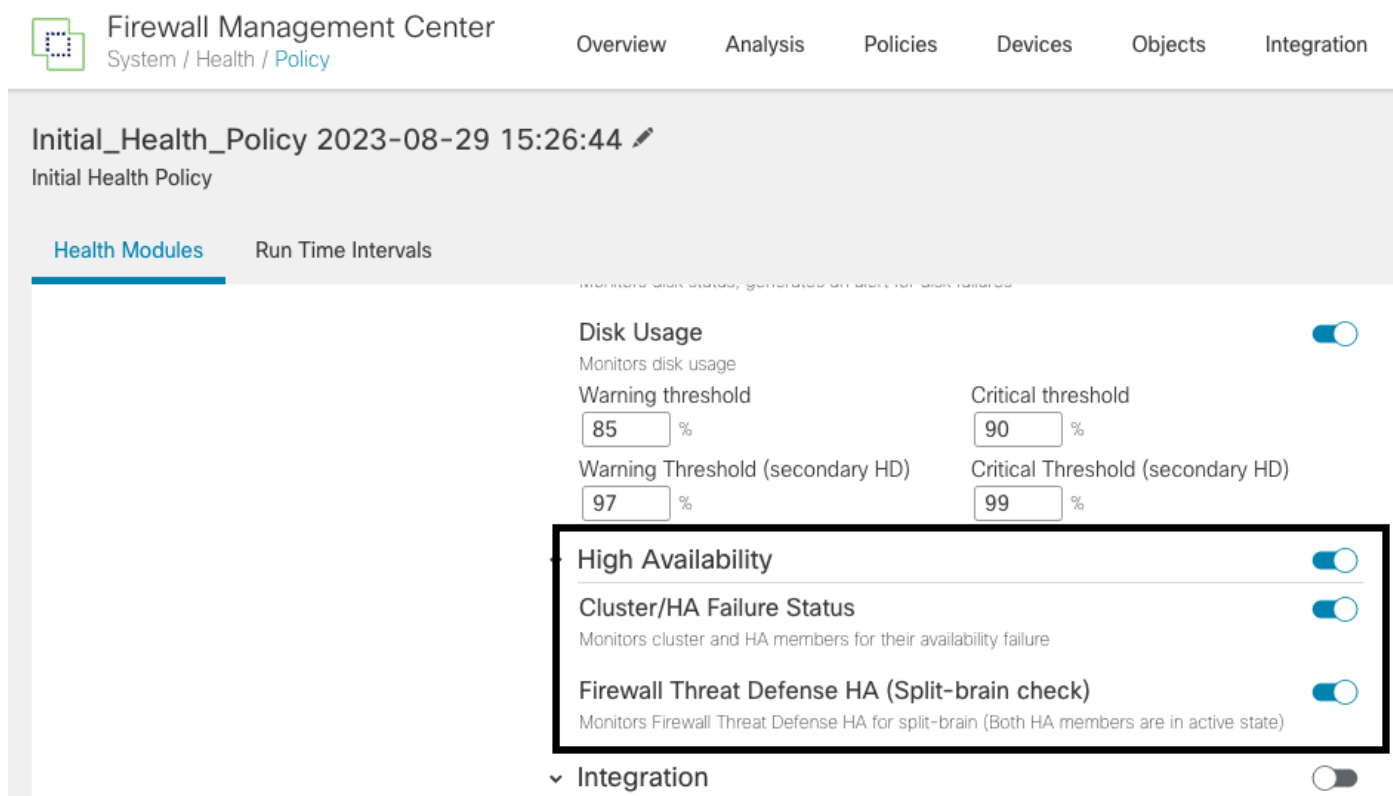
FMCでのフェールオーバーイベント

ステップ 1：正常性ポリシーの構成

ヘルスポリシーでは、モジュールCluster/HA Failure Statusがデフォルトで有効になっていますが、Split-brainチェックオプションを有効にすることもできます。

正常性ポリシーでHAのオプションを有効にするには、 System > Health > Policy > Firewall Threat Defense Health Policy > High Availability.

次の図に、正常性ポリシーのHA設定を示します。



The screenshot shows the FMC interface for configuring a health policy. The breadcrumb path is System / Health / Policy. The policy name is 'Initial_Health_Policy' with a timestamp of '2023-08-29 15:26:44'. The 'Health Modules' tab is selected, and the 'Run Time Intervals' sub-tab is active. The 'Disk Usage' module is configured with a warning threshold of 85% and a critical threshold of 90% for the primary HD, and 97% and 99% for the secondary HD. The 'High Availability' section is highlighted with a red box and shows three enabled options: 'High Availability', 'Cluster/HA Failure Status', and 'Firewall Threat Defense HA (Split-brain check)'. The 'Integration' section is currently collapsed.

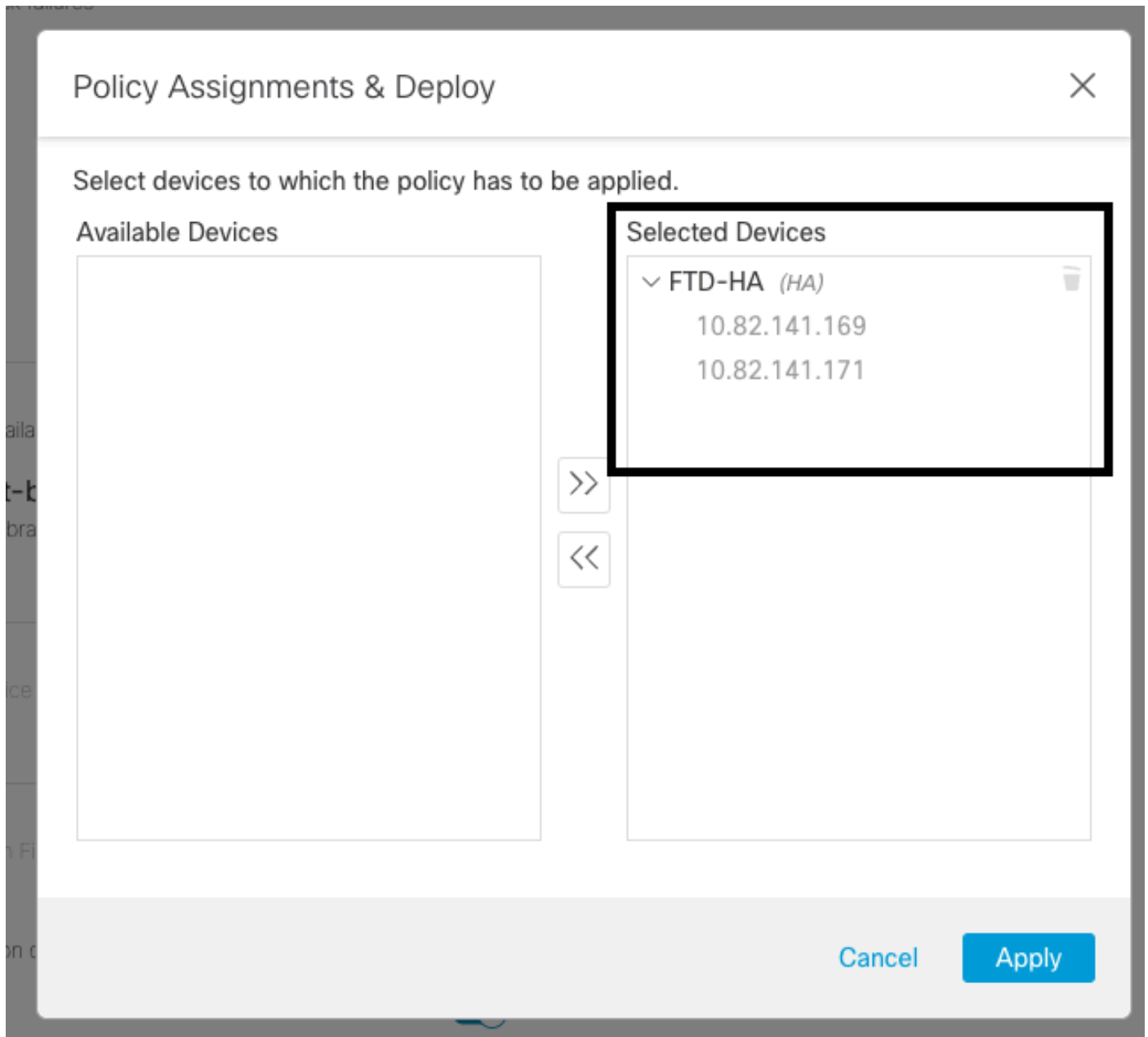
高可用性の正常性の設定

ステップ 2：ポリシーの割り当て

FMCから監視するHAペアにヘルスポリシーが割り当てられていることを確認します。

ポリシーを割り当てるには、 System > Health > Policy > Firewall Threat Defense Health Policy > Policy Assignments & Deploy.

次の図に、HAペアに正常性ポリシーを割り当てる方法を示します。



HA割り当て

ポリシーが割り当てられ、保存されると、FMCはそれをFTDに自動的に適用します。

ステップ 3 : フェールオーバーイベントアラート

HAの設定に応じて、フェールオーバーイベントがトリガーされると、フェールオーバー障害を説明するポップアップアラートが表示されます。

次の図に、生成されるフェールオーバーアラートを示します。

Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

t Pending (0) ● Upgrade (0)

	Version	Chassis	Licenses	Access Control P
with FTD	7.2.5	F241-24-04-FPR9K-1.cisco.com:443 Security Module - 1	Essentials, IPS (2 more...)	FTD HA
with FTD	7.2.5	F241-F241-24-4-FPR9K-2.cisco.com:4 Security Module - 1	Essentials, IPS (2 more...)	FTD HA

Dismiss all notifications

Cluster/Failover Status - 10.82.141.169 ✕
 SECONDARY (FLM1946BCEX)
 FAILOVER_STATE_ACTIVE (Inspection engine in other unit has failed(My failed services-. Peer failed services-diskstatus))
 PRIMARY (FLM19389LQR)
 FAILOVER_STATE_STANDBY (Check peer event for reason)

Cluster/Failover Status - 10.82.141.171 ✕
 PRIMARY (FLM19389LQR)
 FAILOVER_STATE_STANDBY (Other unit wants me Standby)
 PRIMARY (FLM19389LQR)
 FAILOVER_STATE_STANDBY_FAILED (Detect inspection engine failure(My failed services-diskstatus. Peer failed services-))

Disk Usage - 10.82.141.171 ✕
 /ngfw using 98%: 186G (5.5G Avail) of 191G

フェールオーバーアラート

また、次の場所にも移動することもできます [Notifications > Health](#) フェールオーバーのヘルスアラートを視覚化します。

次の図に、notificationsの下のフェールオーバーアラートを示します。

Firewall Management Center Overview Analysis Policies Devices Objects Integration Deploy 🔍 ⚙️ 👤 admin | cisco SECURE

View By: Group

All (2) ● Error (2) ● Warning (0) ● Offline (0) ● Normal (0) ● Deployment Pending (0) ● Upgrade (0)

Collaps All

Name	Model	Version	Chassis
Un grouped (1)			
FTD-HA High Availability			
10.82.141.169(Secondary, Active) 10.82.141.169 - Routed	Firepower 9300 with FTD	7.2.5	F241-24-04-FPR9K-1 Security Module - 1
10.82.141.171(Primary, Failed) 10.82.141.171 - Routed	Firepower 9300 with FTD	7.2.5	F241-F241-24-4-FPR Security Module - 1

Deployments Upgrades ● Health Tasks Show Notifications

20+ total 15 warnings 7 critical 0 errors Filter

- Smart License Monitor Smart Agent is not registered with Smart Licensing Cloud
- URL Filtering Monitor URL Filtering registration failure

Devices

10.82.141.169

- 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

10.82.141.171

- Disk Usage /ngfw using 98%: 186G (5.4G Avail) of 191G
- 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

HA通知

ステップ 4 : 履歴フェールオーバーイベント

FMCは、過去に発生したフェールオーバーイベントを視覚化する方法を提供します。イベントをフィルタリングするには、[System > Health > Events > Edit Search](#) Module NameにCluster/Failover Statusを指定します。また、ステータスに基づいてフィルタを適用することもできます。

次の図に、フェールオーバーイベントをフィルタリングする方法を示します。

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

フェールオーバーフィルタメッセージ

特定の日時のイベントを表示するように時間設定を調整できます。時刻の設定を変更するには、System > Health > Events > Time.

次の図に、時刻設定を編集する方法を示します。

The screenshot shows the Firewall Management Center interface. The main content area displays the 'Health Monitoring Time Window' configuration page. The page includes a table of health events on the left and a configuration window for the 'Expanding Time Window' on the right. The configuration window has fields for 'Start Time' (2023-09-27 11:02) and 'End Time' (2023-09-28 11:14). Below these fields are two calendar views for September 2023. To the right of the calendar views is a 'Presets' section with a list of time window options: '1 hour', '6 hours', '1 day', '1 week', '2 weeks', and '1 month'. The '1 day' option is currently selected. At the bottom of the configuration window, there are 'Reset' and 'Apply' buttons. The table on the left shows a list of health events with columns for 'Module Name X', 'Test Name X', 'Status X', and 'Device X'. The events listed are all for 'Cluster/Failover Status' with a status of 'Warning' and a device of '10.82.141.171'.

時間フィルタ

イベントが特定されたら、そのイベントの理由を確認するために、[Description]の下にカーソルを置きます。

次の図に、フェールオーバーの理由を示します。

Firewall Management Center
System / Health / Events

Overview Analysis Policies Devices Objects Integration

Deploy 🔍 ⚙️ admin 🔒 **SECURE**

Bookmark This Page | Reporting | Workflows | View Bookmarks | Search

2023-09-27 11:19:00 - 2023-09-28 12:38:42 Expanding

Search Constraints (Edit Search Save Search)

Health Monitor Table View of Health Events

Module Name X	Test Name X	Time X	Description X	Value X	Units X	Status X	Device X
Cluster/Failover Status	Cluster/Failover Status	2023-09-28 11:41:52	PRIMARY (FLM19389LOR) FAILOVER_STATE_STANDBY_FAIL... PRIMARY (FLM19389LOR) FAILOVER_STATE_STANDBY_FAILED (Detect inspection engine failure:My failed services-diskstatus. Peer failed services-}).	0		🚨	10.82.141.171

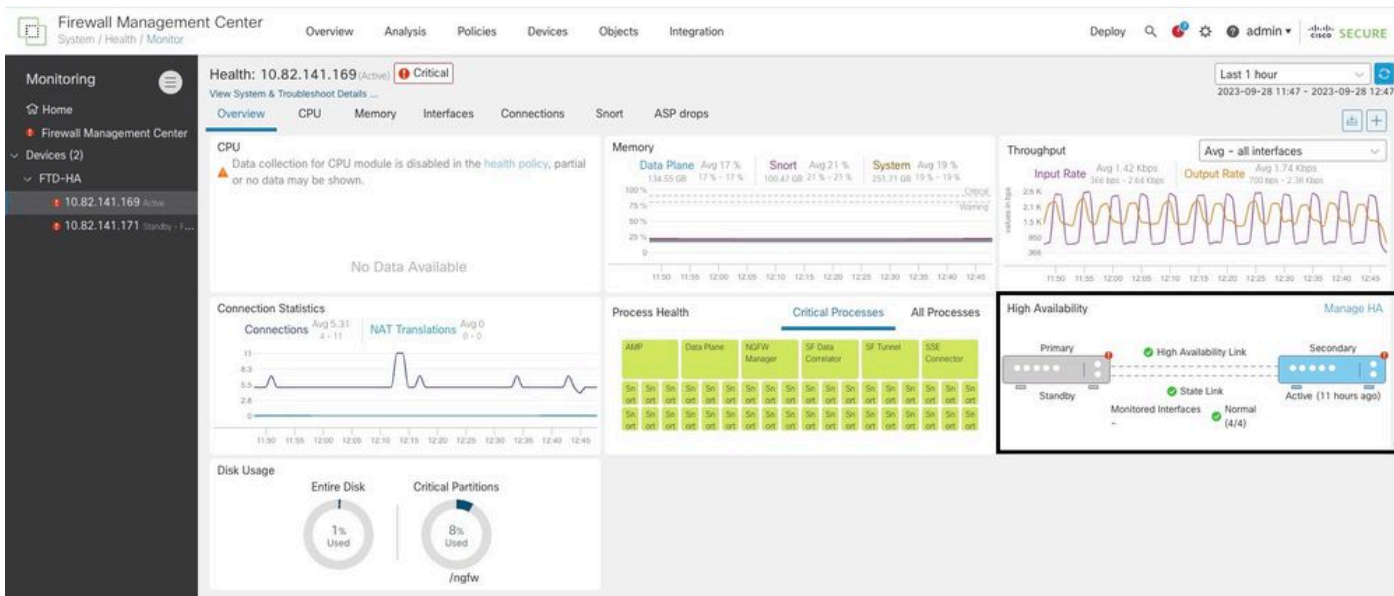
フェールオーバーの詳細

ステップ 5 : ハイアベイラビリティダッシュボード

フェールオーバーを監視するもう1つの方法は、 System > Health Monitor > Select Active or Standby Unit.

HAモニタは、HAおよび状態リンク、監視対象インターフェイス、ROL、各ユニットのアラートのステータスに関する情報を提供します。

次の図に、HAモニタを示します。



ヘルスグラフィック

アラートを視覚化するには、 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

アラート

アラートの詳細を表示するには、 [View all alerts > see more.](#)

次の図に、フェールオーバーの原因となったディスクステータスを示します。

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

Sep 28, 2023 12:47 PM

Appliance Heartbeat

All appliances are sending heartbeats correctly.

Sep 28, 2023 12:47 PM

Automatic Application Runas Status

Sep 28, 2023 12:47 PM

手順 6 : 脅威対策CLI

最後に、FMCに関する追加情報を収集するために、 Devices > Troubleshoot > Threat Defense CLIを参照。
Deviceや実行するコマンドなどのパラメータを設定し、 Execute.

次の図に、コマンドの例を示します show failover history フェールオーバーの障害を特定できるFMCで実行できます。

Firewall Management Center
Devices / Troubleshoot / Threat Defense CLI

Overview Analysis Policies **Devices** Objects Integration

Device: 10.82.141.169
Command: show Parameter: failover history

Output

```
other unit has failed due to disk failure  
05:28:05 UTC Sep 28 2023  
Active Drain Active Applying Config Inspection engine in  
other unit has failed due to disk failure  
05:28:05 UTC Sep 28 2023  
Active Applying Config Active Config Applied Inspection engine in  
other unit has failed due to disk failure  
05:28:05 UTC Sep 28 2023  
Active Config Applied Active Inspection engine in  
other unit has failed due to disk failure
```

Back Execute

フェールオーバー履歴

関連情報

- [FTDのハイアベイラビリティ](#)
- [Firepower アプライアンスでの FTD 高可用性の設定](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。