

Firepower アプライアンスでの FTD 高可用性の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[タスク 1.条件の確認](#)

[タスク 2.FTD HAの設定](#)

[条件](#)

[タスク 3.FTD HAとライセンスの確認](#)

[タスク 4.フェールオーバーロールの切り替え](#)

[タスク 5.HAペアの解除](#)

[タスク 6.HAペアの削除](#)

[タスク 7.HAの中断](#)

[よく寄せられる質問 \(FAQ\)](#)

[関連情報](#)

はじめに

このドキュメントでは、FirepowerデバイスでFirepower Threat Defense(FTD)ハイアベイラビリティ(HA) (アクティブ/スタンバイフェールオーバー) を設定および確認する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。


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 Firepower 9300 X 2
- Cisco Firepower 4100(7.2.8)X 2
- Firepower Management Center(FMC)(7.2.8)

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。

 注:FTDを使用するFPR9300アプライアンスでは、シャーシ間HAのみを設定できます。HA構成の2つのユニットは、ここに記載されている条件を満たしている必要があります。

タスク 1.条件の確認

タスク要件：

両方のFTDアプライアンスが注意事項の要件を満たし、HAユニットとして設定できることを確認します。

ソリューション：

ステップ 1：FPR9300管理IPに接続し、モジュールハードウェアを確認します。

FPR9300-1 のハードウェアを確認します。

<#root>

```
KSEC-FPR9K-1-A#
```

```
show server inventory
```

Server	Equipped	PID	Equipped VID	Equipped Serial (SN)	Slot	Status	Ackd Memory (MB)	Ackd Cores
1/1	FPR9K-SM-36	V01		FLM19216KK6		Equipped	262144	36
1/2	FPR9K-SM-36	V01		FLM19206H71		Equipped	262144	36
1/3	FPR9K-SM-36	V01		FLM19206H7T		Equipped	262144	36

```
KSEC-FPR9K-1-A#
```

FPR9300-2 のハードウェアを確認します。

<#root>

```
KSEC-FPR9K-2-A#
```

```
show server inventory
```

Server	Equipped	PID	Equipped VID	Equipped Serial (SN)	Slot	Status	Ackd Memory (MB)	Ackd Cores
1/1	FPR9K-SM-36	V01		FLM19206H9T		Equipped	262144	36
1/2	FPR9K-SM-36	V01		FLM19216KAX		Equipped	262144	36
1/3	FPR9K-SM-36	V01		FLM19267A63		Equipped	262144	36

```
KSEC-FPR9K-2-A#
```

ステップ 2：FPR9300-1 Chassis Managerにログインし、Logical Devicesに移動します。

ソフトウェアのバージョン、番号、およびインターフェイスのタイプを確認します。

タスク 2.FTD HAの設定

タスク要件：

次の図に示すように、アクティブ/スタンバイフェールオーバー（HA）を設定します。この場合は、41xxペアが使用されます。

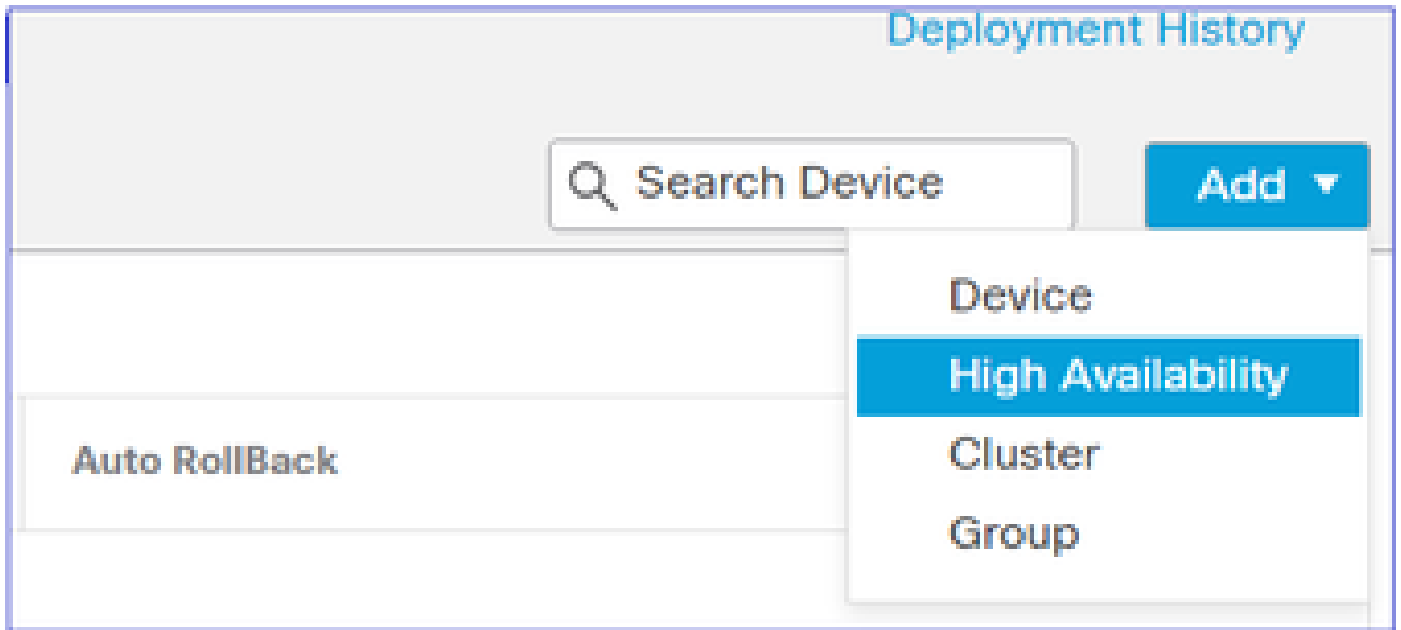


解決方法

次の図に示すように、両方の FTD デバイスは、すでに FMC に登録されています。

FTD4100-5 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	FP4100-5.443 Security Module - 1	Base, Threat (2 more...)	acp_simple	↻	✎
FTD4100-6 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	FP4100-6.443 Security Module - 1	Base, Threat (2 more...)	acp_simple	↻	✎

ステップ 1：FTDフェールオーバーを設定するには、図に示すように、Devices > Device Managementに移動し、Add High Availabilityを選択します。



ステップ 2 : 図に示すように、プライマリピアとセカンダリピアを入力し、Continueを選択します。

Version: 7.2 Channel: 7.2 License: 7.2

Add High Availability Pair ?

Name:*

FTD4100-HA

Device Type:

Firewall Threat Defense ▾

Primary Peer:

FTD4100-5 ▾

Secondary Peer:

FTD4100-6 ▾

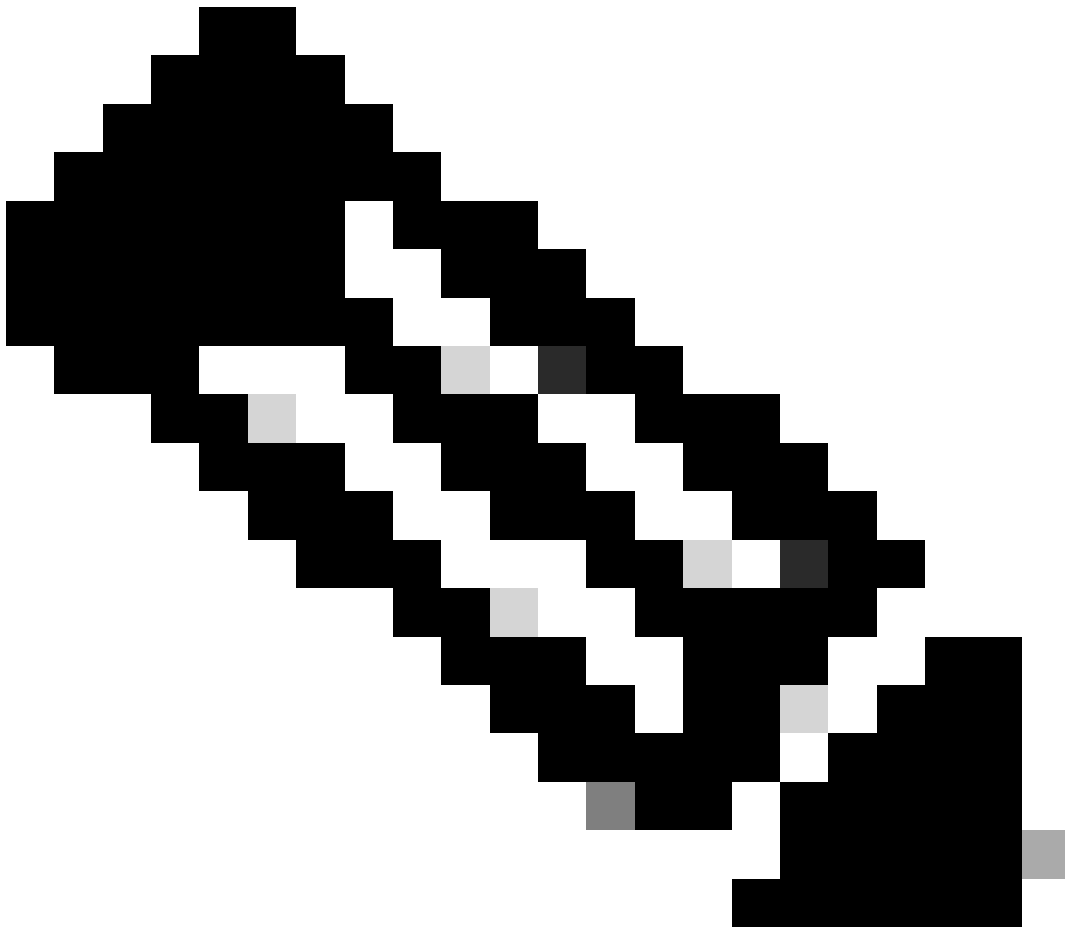
i Threat Defense High Availability pair will have primary configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.

⚠ 警告：正しいユニットをプライマリユニットとして選択してください。選択したプライマリユニットのすべての設定が、選択したセカンダリFTDユニットに複製されます。複製の結果として、セカンダリユニットの現在の設定を置き換えることができます。

条件

2つのFTDデバイス間にHAを作成するには、次の条件を満たす必要があります。

- 同じモデルである。
 - 同じバージョン：これはFXOSとFTDに適用されます。メジャー（1番目の番号）、マイナー（2番目の番号）、メンテナンス（3番目の番号）は同じでなければなりません。
 - インターフェイスの数が同じである。
 - インターフェイスのタイプが同じである。
 - FMCの同じグループ/ドメインの一部としての両方のデバイス。
 - Network Time Protocol（NTP；ネットワークタイムプロトコル）の設定が同一であること。
 - 未確定の変更を行わずにFMCに完全に導入されていること。
 - 同じファイアウォールモード（ルーテッドまたはトランスペアレント）である。
-



注:FTDデバイスとFMC GUIの両方で、このチェックボックスをオンにする必要があります。これは、FTDに同じモードがあった場合に、FMCがこれを反映しないためです。

- DHCP/Point-to-Point Protocol over Ethernet(PPPoE)が設定されているインターフェイスはありません。
- 両方のシャーシに異なるホスト名[完全修飾ドメイン名(FQDN)]があります。シャーシのホス

ト名を確認するには、FTD CLIに移動して次のコマンドを実行します。

```
<#root>
firepower#
show chassis-management-url

https://
KSEC-FPR9K-1.cisco.com

:443//
```



注:6.3以降のFTDでは、コマンドshow chassis detailを使用します。

```
<#root>
Firepower-module1#
show chassis detail

Chassis URL : https://FP4100-5:443//

Chassis IP : 10.62.148.187
Chassis IPv6 : ::
Chassis Serial Number : JAD19500BAB
Security Module : 1
```

両方のシャーシの名前が同じである場合は、次のコマンドを使用して、一方のシャーシの名前を変更します。

```
<#root>
KSEC-FPR9K-1-A#
scope system
KSEC-FPR9K-1-A /system #
set name FPR9K-1new
Warning: System name modification changes FC zone name and redeploys them non-disruptively
KSEC-FPR9K-1-A /system* #
commit-buffer
FPR9K-1-A /system #
exit
FPR9K-1new-A
```

#

シャーシ名を変更したら、FTD を FMC から登録解除し、再度登録します。その後に、HA ペアの作成に進んでください。

ステップ 3 : HAを設定し、リンクの設定を行います。

今回は、状態リンクの設定は高可用性リンクと同じです。

Addを選択し、図に示すように、HAペアが展開されるまで数分待ちます。

Add High Availability Pair

High Availability Link

Interface:* Port-channel3

Logical Name:* FOVER

Primary IP:* 172.16.51.1

Use IPv6 Address

Secondary IP:* 172.16.51.2

Subnet Mask:* 255.255.255.0

State Link

Interface:* Same as LAN Failover Link

Logical Name:* FOVER

Primary IP:* 172.16.51.1

Use IPv6 Address

Secondary IP:* 172.16.51.2

Subnet Mask:* 255.255.255.0

IPsec Encryption

Enabled

Key Generation: Auto

i LAN failover link is used to sync configuration, stateful failover link is used to sync application content between peers. Selected interface links and encryption settings cannot be changed later.

Cancel Add

ステップ 4 : データインターフェイス (プライマリおよびスタンバイIPアドレス) の設定

図に示すように、FMCのGUIでHAのEditを選択します。

HA Pair Name	Status	Device	Version	Security Module	Base, Threat	Policy	Actions
FTD4120-HA	High Availability						Edit
FTD4100-5(Primary, Active)	Short 3	Firepower 4120 with FTD	7.2.8	FP4100-5-443 Security Module - 1	Base, Threat (2 more...)	acp_simple	...
FTD4100-6(Secondary, Standby)	Short 3	Firepower 4120 with FTD	7.2.8	FP4100-6-443 Security Module - 1	Base, Threat (2 more...)	acp_simple	...

ステップ 5 : インターフェイスを設定します。

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Advanced

Name:

Enabled
 Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:

(64 - 9184)

Priority:
 (0 - 65535)

Propagate Security Group Tag:

NVE Only:

Edit Physical Interface

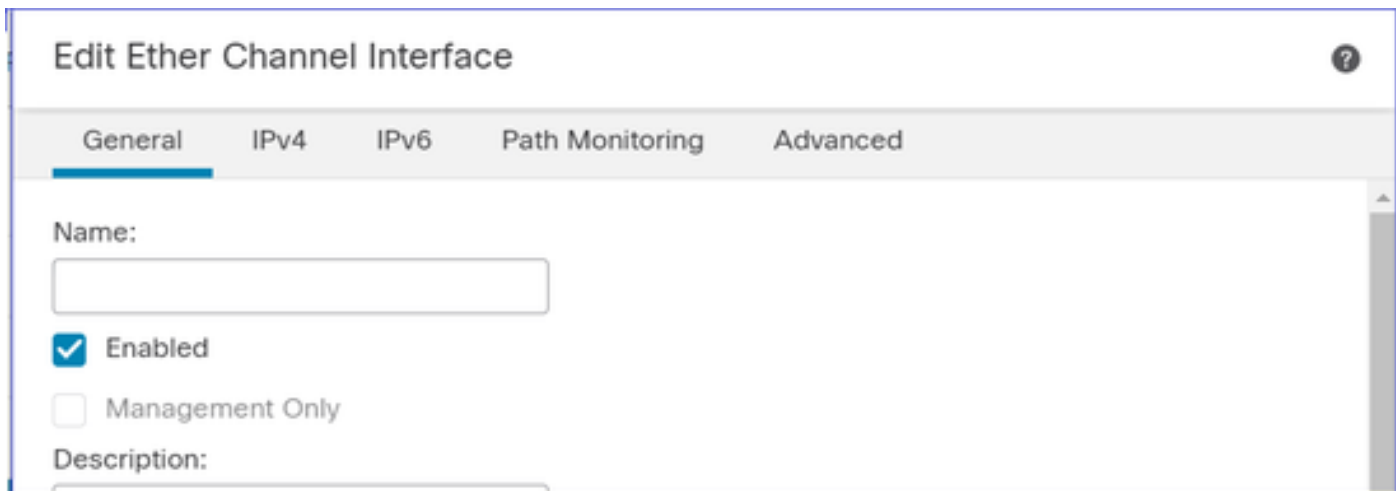
General IPv4 IPv6 Path Monitoring Advanced

IP Type:

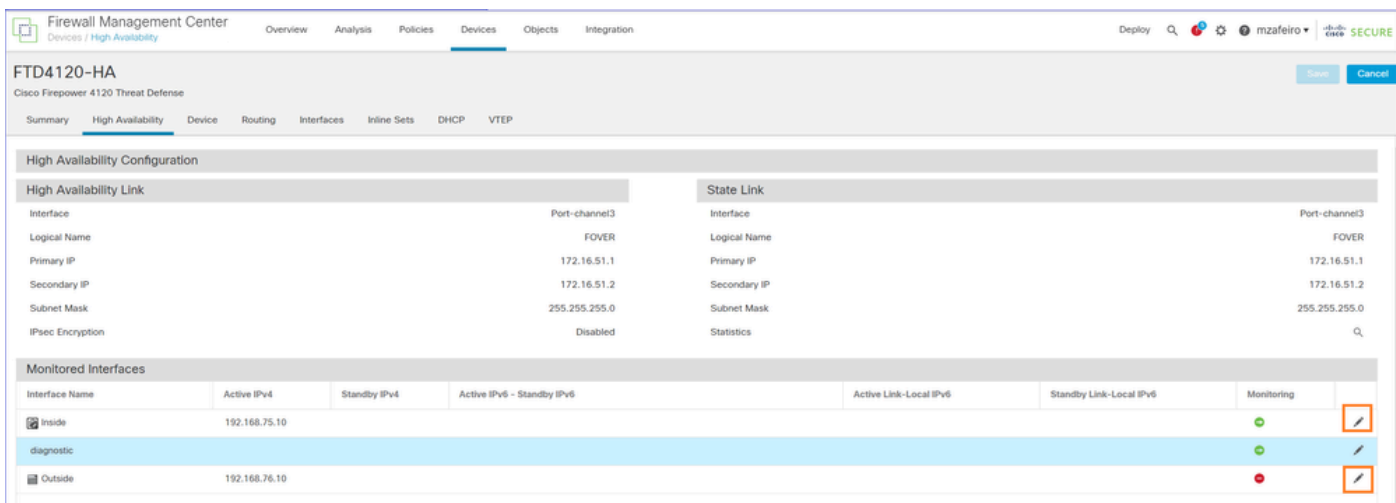
IP Address:

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

サブインターフェイスの場合は、最初に親インターフェイスを有効にする必要があります。



手順 6 : High Availabilityに移動し、インターフェイス名Editを選択して、図に示すようにスタンバイIPアドレスを追加します。



手順 7 : 図に示す内部インターフェイス用。

Edit Inside

Monitor this interface for failures

IPv4 IPv6

Interface Name:
Inside

Active IP Address:
192.168.75.10

Mask:
24

Standby IP Address:
192.168.75.11

Cancel OK

ステップ 8 : Outsideインターフェイスに対しても同じ操作を行います。

ステップ 9 : 図に示すように、結果を確認します。

Monitored Interfaces						
Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring
Inside	192.168.75.10	192.168.75.11				●
diagnostic						●
Outside	192.168.76.10	192.168.76.11				●

ステップ 10 : High Availabilityタブから離れずに、図に示すように仮想MACアドレスを設定します。

Interface MAC Addresses		
Physical Interface	Active Mac Address	Standby Mac Address
No records to display		

ステップ 11内部インターフェイスの場合は、図のように表示されます。

Add Interface Mac Address

Physical Interface:*

Ethernet1/4 

Active Interface Mac Address:*

aaaa.bbbb.1111

Standby Interface Mac Address:*

aaaa.bbbb.2222

-  Enter the Mac addresses in hexadecimal format such as 0123.4567.89ab

Cancel

OK

ステップ 12 Outsideインターフェイスに対しても同じ操作を行います。

ステップ 13 図に示すように、結果を確認します。

Interface MAC Addresses			+
Physical Interface	Active Mac Address	Standby Mac Address	
Ethernet1/4	aaaa.bbbb.1111	aaaa.bbbb.2222	
Port-channel2.202	aaaa.bbbb.3333	aaaa.bbbb.4444	

ステップ 14 : 変更を設定したら、SaveとDeployを選択します。

タスク 3.FTD HAとライセンスの確認

タスク要件 :

FMC GUI と FTD CLI から、FTD HA 設定と有効なライセンスを確認します。

ソリューション :

ステップ 1 : Summaryに移動し、図に示すように、HA設定と有効なライセンスを確認します。

The screenshot shows the FMC GUI for a Cisco Firepower 4120 Threat Defense device. The 'Summary' tab is selected, and the 'License' section is expanded. The 'Base' license is highlighted in orange, indicating it is active. Other license options like 'Export-Controlled Features', 'Malware', and 'Threat' are also visible with their respective status indicators.

ステップ 2 : FTDのCLISH CLIから、「show high-availability config」または「show failover」コマンドを実行します。

```
<#root>
```

```
>
```

```
show high-availability config
```

```
Failover On
Failover unit Primary
Failover LAN Interface: FOVER Port-channel13 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 2 of 1291 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.18(4)210, Mate 9.18(4)210
Serial Number: Ours FLM1949C5RR, Mate FLM2108V9YG
```

Last Failover at: 08:46:30 UTC Jul 18 2024

This host: Primary - Active

```
Active time: 1999 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)
  Interface diagnostic (0.0.0.0): Normal (Waiting)
  Interface Inside (192.168.75.10): Link Down (Shutdown)
  Interface Outside (192.168.76.10): Normal (Not-Monitored)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
```

Other host: Secondary - Standby Ready

```
Active time: 1466 (sec)
slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.18(4)210) status (Up Sys)
  Interface diagnostic (0.0.0.0): Normal (Waiting)
  Interface Inside (192.168.75.11): Link Down (Shutdown)
  Interface Outside (192.168.76.11): Normal (Not-Monitored)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
```

Stateful Failover Logical Update Statistics
<output omitted>

ステップ 3 : セカンダリデバイスでも同じ操作を行います。

ステップ 4 : LINA CLIからshow failover stateコマンドを実行します。

<#root>

firepower#

show failover state

	State	Last Failure Reason	Date/Time
This host -	Primary Active	None	
Other host -	Secondary Standby Ready	Comm Failure	18:32:56 EEST Jul 21 2016

====Configuration State====

Sync Done

====Communication State====

Mac set

firepower#

ステップ 5 : プライマリユニット(LINA CLI)から設定を確認します。

<#root>

```
>
show running-config failover

failover
failover lan unit primary
failover lan interface FOVER Port-channel3
failover replication http
failover mac address Ethernet1/4 aaaa.bbbb.1111 aaaa.bbbb.2222
failover mac address Port-channel2.202 aaaa.bbbb.3333 aaaa.bbbb.4444
failover link FOVER Port-channel3
failover interface ip FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2
```

```
>
show running-config interface
```

```
!
interface Port-channel2
no nameif
no security-level
no ip address
!
interface Port-channel2.202
vlan 202
nameif Outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
!
interface Port-channel3
description LAN/STATE Failover Interface
!
interface Ethernet1/1
management-only
nameif diagnostic
security-level 0
no ip address
!
interface Ethernet1/4
shutdown
nameif Inside
security-level 0
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
>
```

タスク 4. フェールオーバーロールの切り替え

タスク要件 :

FMC から、フェールオーバーの役割をプライマリ/アクティブ、セカンダリ/スタンバイからプライマリ/スタンバイ、セカンダリ/アクティブに切り替えます。

ソリューション :

ステップ 1 : 図に示すように、アイコンを選択します。



ステップ 2 : 操作を確認します。

show failover history コマンドの出力を使用できます。

<p>新しいアクティブ</p>	<p>新しい</p>
<pre>> フェールオーバー履歴の表示 0.===== 状態から状態への理由 0.===== 2024年7月18日09:27:11 UTC スタンバイレディ有効その他のユニットはアクティブにする (configコマンドで設定) 2024年7月18日09:27:11 UTC アクティブドレインのみ他のユニットはアクティブです (configコマンドで設定) 2024年7月18日09:27:11 UTC アクティブドレインアクティブ適用設定その他のユニットは私をアクティブにします (configコマンドで設定) 2024年7月18日09:27:11 UTC アクティブ設定適用アクティブ設定適用された他のユニットがアクティブを要求 (configコマンドで設定) 2024年7月18日09:27:11 UTC アクティブ構成が適用されたアクティブ他のユニットがアクティブを要求 (configコマンドで設定)</pre>	<p>> フェ 0.== 状態 0.== 2024 config パー</p>

ステップ 4 : 確認後、プライマリユニットを再度アクティブにします。

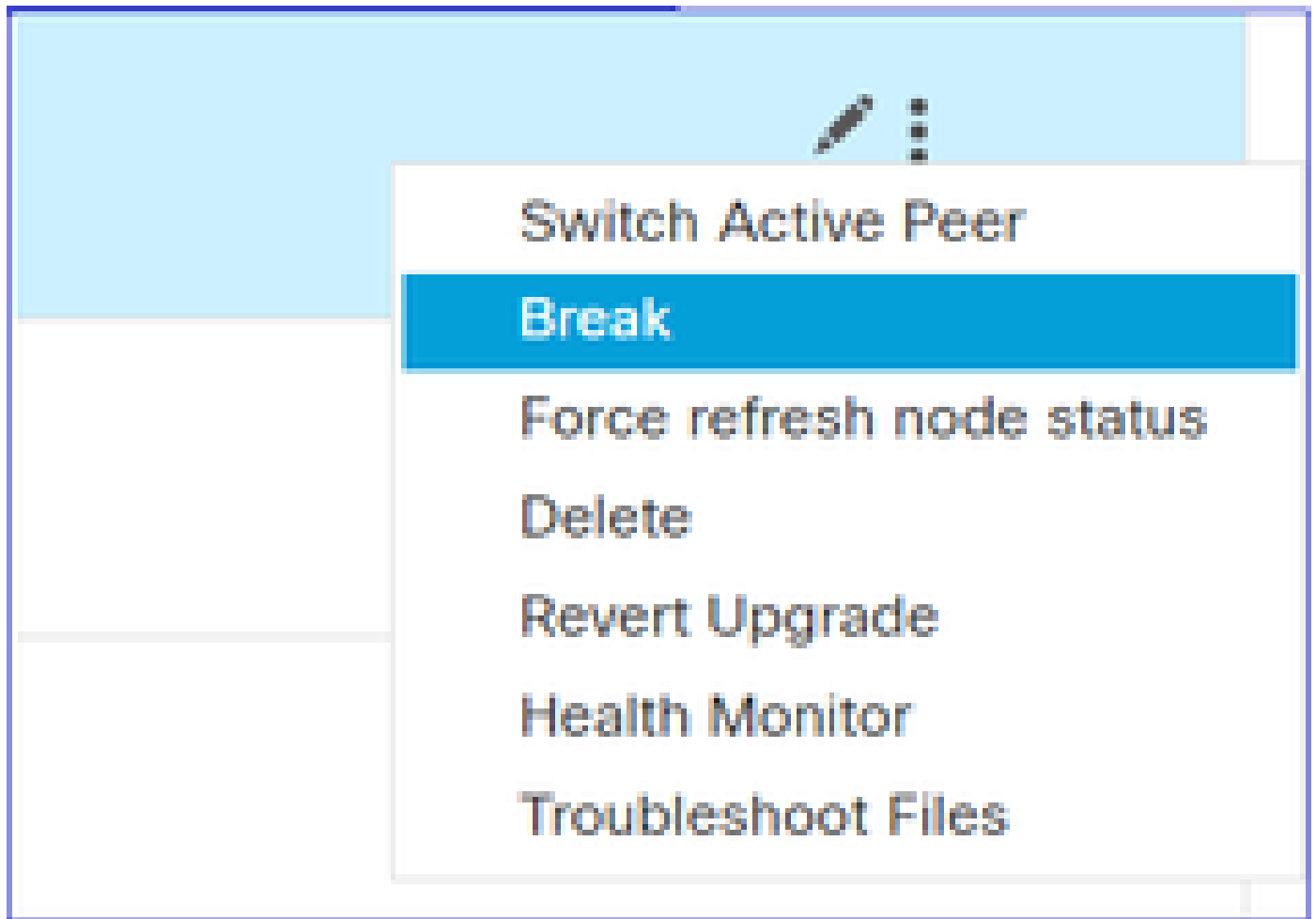
タスク 5.HAペアの解除

タスク要件 :

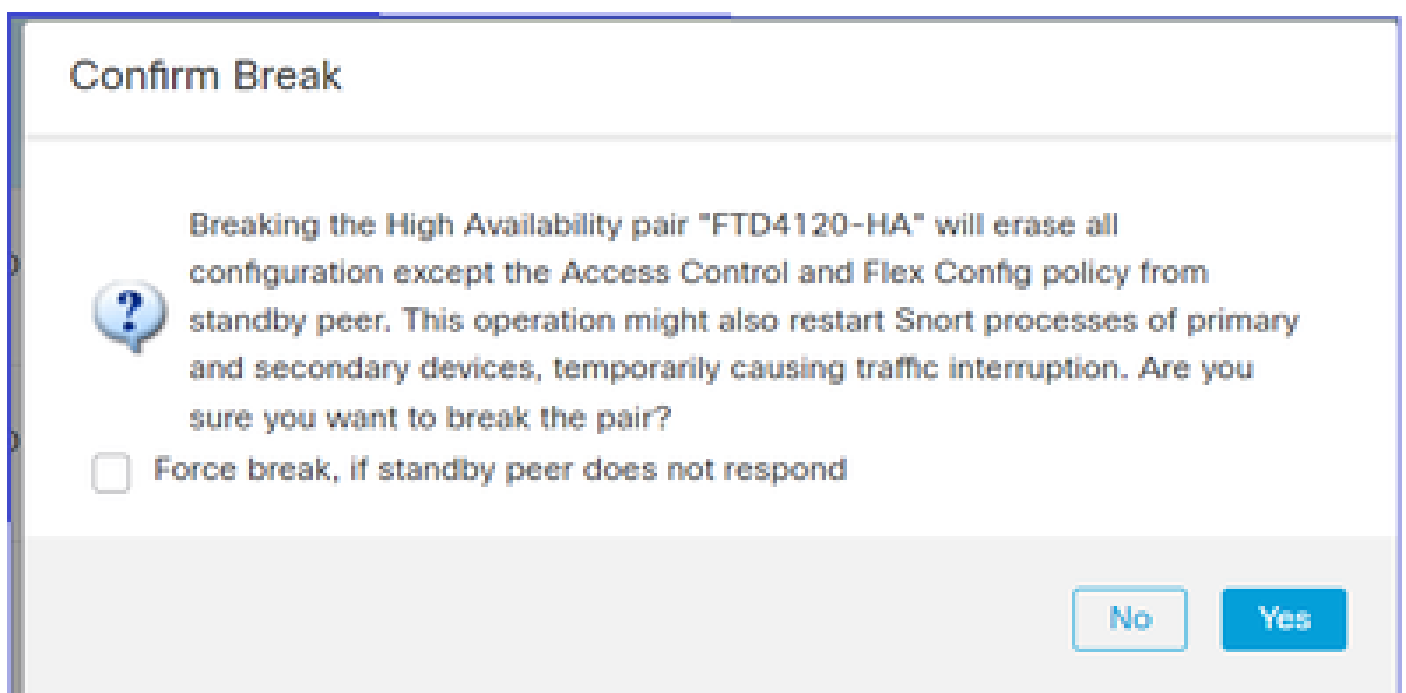
FMC から、フェールオーバーペアを解除します。

ソリューション :

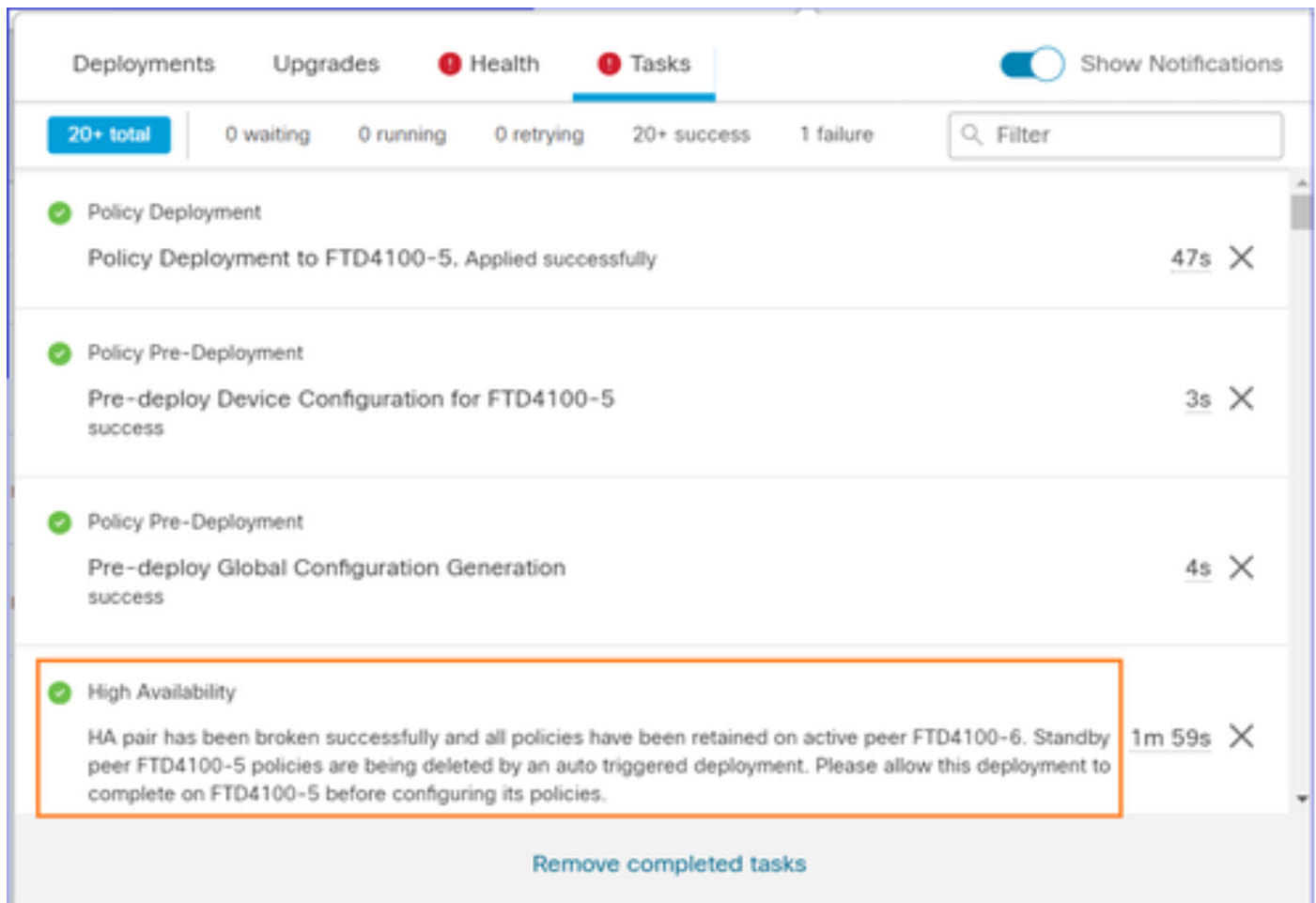
ステップ 1 : 図に示すように、アイコンを選択します。



ステップ 2 : 図に示すように、通知を確認します。



ステップ 3 : 次の図に示すメッセージに注意してください。



ステップ 4 : FMC GUIまたはCLIからの結果の確認

HA 解除の前後にプライマリユニットで show running-config コマンドを実行します。

HAブレイク前のプライマリ/スタンバイユニット	HAブレイク後のプライマリユニット
<pre>> show running-configコマンド : 保存済み : : シリアル番号 : FLM1949C5RR : ハードウェア : FPR4K-SM-24、73850 MB RAM、CPU Xeon E5シリーズ2200 MHz、2 CPU (48コア) : NGFWバージョン7.2.8 ! ホスト名firepower イネーブルパスワード*****暗号化 強力な暗号化を無効にする</pre>	<pre>>情報 : このユニットは現在スタンバイ状態です。フェールオーバーを無効にすると、このユニットはスタンバイ状態のままになります。 > show running-config : 保存済み : : シリアル番号 : FLM1949C5RR : ハードウェア : FPR4K-SM-24、73850 MB RAM、CPU Xeon E5シリーズ2200 MHz、2 CPU (48コア) : NGFWバージョン7.2.8</pre>

<pre> service-module 0キープアライブタイムアウト4 service-module 0キープアライブカウンタ6 names no mac-address auto (デフォルト) ! interface Port-channel2 nameifなし ctsマニュアル propagate sgt preserve-untag (sgtの保存/タグ解 除を伝播) policy static sgt disabled trusted (信頼できるポ リシースタティックsgt無効) セキュリティレベルなし IPアドレスがありません ! インターフェイスポートチャンネル2.202 vlan 202 nameif外部 ctsマニュアル propagate sgt preserve-untag (sgtの保存/タグ解 除を伝播) policy static sgt disabled trusted (信頼できるポ リシースタティックsgt無効) セキュリティレベル0 ipアドレス192.168.76.10 255.255.255.0スタンバ イ192.168.76.11 ! interface Port-channel3 説明LAN/ステートフェールオーバーインターフ ェイス ! interface Ethernet1/1 管理専用 nameif診断 ctsマニュアル propagate sgt preserve-untag (sgtの保存/タグ解 除を伝播) policy static sgt disabled trusted (信頼できるポ リシースタティックsgt無効) セキュリティレベル0 IPアドレスがありません ! interface Ethernet1/4 nameif内部 ctsマニュアル </pre>	<pre> ! ホスト名firepower イネーブルパスワード*****暗号化 強力な暗号化を無効にする service-module 0キープアライブタイムアウト4 service-module 0キープアライブカウンタ6 names no mac-address auto (デフォルト) ! interface Port-channel2 shutdown nameifなし セキュリティレベルなし IPアドレスがありません ! interface Port-channel3 shutdown nameifなし セキュリティレベルなし IPアドレスがありません ! interface Ethernet1/1 管理専用 shutdown nameifなし セキュリティレベルなし IPアドレスがありません ! interface Ethernet1/4 shutdown nameifなし セキュリティレベルなし IPアドレスがありません ! FTPモードパッシブ ngips conn-match vlan-id (オプション) オブジェクトグループ検索アクセスコントロー ル access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY : デフォルトトンネ ルとプライオリティポリシー access-list CSM_FW_ACL_ remark rule-id 9998 : ルール : デフォルトトンネルアクション ルール </pre>
---	---

<pre> propagate sgt preserve-untag (sgtの保存/タグ解除を伝播) policy static sgt disabled trusted (信頼できるポリシースタティックsgt無効) セキュリティレベル0 ipアドレス192.168.75.10 255.255.255.0スタンバイ192.168.75.11 ! FTPモードパッシブ ngips conn-match vlan-id (オプション) オブジェクトグループ検索アクセスコントロール access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY : デフォルトトンネルとプライオリティポリシー access-list CSM_FW_ACL_ remark rule-id 9998 : ルール : デフォルトトンネルアクションルール access-list CSM_FW_ACL_ advanced permit ipinip anyルールID 9998 access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544ルールID 9998 access-list CSM_FW_ACL_ advanced permit 41 anyルールID 9998 access-list CSM_FW_ACL_ advanced permit gre any anyルールID 9998 access-list CSM_FW_ACL_ remark rule-id 268434433 : アクセスポリシー : acp_simple - デフォルト access-list CSM_FW_ACL_ remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ advanced permit ip any any rule-id268434433 ! tcpマップUM_STATIC_TCP_MAP tcpオプション範囲6 7許可 tcpオプション範囲9 18許可 tcpオプション範囲20 255 : 許可 緊急フラグ許可 ! ポケットベルなし no logging message 106015 </pre>	<pre> access-list CSM_FW_ACL_ advanced permit ipinip anyルールID 9998 access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544ルール ID 9998 access-list CSM_FW_ACL_ advanced permit 41 anyルールID 9998 access-list CSM_FW_ACL_ advanced permit gre any anyルールID 9998 access-list CSM_FW_ACL_ remark rule-id 268439552 : アクセスポリシー : acp_simple - 必須 access-list CSM_FW_ACL_ remark rule-id 268439552: L7 RULE: rule1 access-list CSM_FW_ACL_ advanced permit ip any any rule-id268439552 ! tcpマップUM_STATIC_TCP_MAP tcpオプション範囲6 7許可 tcpオプション範囲9 18許可 tcpオプション範囲20 255 : 許可 緊急フラグ許可 ! ポケットベルなし no logging message 106015 no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100 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 フェールオーバーなし <output omitted> </pre>
---	---

<pre> no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100 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 mtu outside 1500 MTU診断1500 mtu inside 1500 フェールオーバー failover lan unit primary failover lan interface FOVERポートチャンネル3 フェールオーバーレプリケーションHTTP フェールオーバーmacアドレス : Ethernet1/4 aaaa.bbbb.1111 aaaa.bbbb.2222 フェールオーバーmacアドレス : Port- channel2.202 aaaa.bbbb.3333 aaaa.bbbb.4444 フェールオーバーリンクFOVERポートチャンネル 3 フェールオーバーインターフェイスIP FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 <output omitted> </pre>	
<p>HAブレイク前のセカンダリ/アクティブユニット</p>	<p>HAブレイク後のセカンダリユニット</p>
<pre> >show running-config : 保存済み : : シリアル番号 : FLM2108V9YG : ハードウェア : FPR4K-SM-24、73850 MB RAM、CPU Xeon E5シリーズ2200 MHz、2 CPU (48コア) : NGFWバージョン7.2.8 ! </pre>	<pre> > show running-config : 保存済み : : シリアル番号 : FLM2108V9YG : ハードウェア : FPR4K-SM-24、73850 MB RAM、CPU Xeon E5シリーズ2200 MHz、2 CPU (48コア) : NGFWバージョン7.2.8 </pre>

```
ホスト名firepower
イネーブルパスワード*****暗号化
強力な暗号化を無効にする
service-module 0キープアライブタイムアウト4
service-module 0キープアライブカウンタ6
names
no mac-address auto ( デフォルト )

!
interface Port-channel2
nameifなし
セキュリティレベルなし
IPアドレスがありません
!
インターフェイスポートチャンネル2.202
vlan 202
nameif外部
ctsマニュアル
propagate sgt preserve-untag ( sgtの保存/タグ
解除を伝播 )
policy static sgt disabled trusted ( 信頼できるポ
リシースタティックsgt無効 )
セキュリティレベル0
ipアドレス192.168.76.10 255.255.255.0スタン
バイ192.168.76.11
!
interface Port-channel3
説明LAN/ステートフェールオーバーインターフ
ェイス
!
interface Ethernet1/1
管理専用
nameif診断
セキュリティレベル0
IPアドレスがありません
!
interface Ethernet1/4
nameif内部
セキュリティレベル0
ipアドレス192.168.75.10 255.255.255.0スタン
バイ192.168.75.11
!
FTPモードパッシブ
ngips conn-match vlan-id ( オプション )
オブジェクトグループ検索アクセスコントロー
ル
```

```
!
ホスト名firepower
イネーブルパスワード*****暗号化
強力な暗号化を無効にする
service-module 0キープアライブタイムアウト4
service-module 0キープアライブカウンタ6
names
no mac-address auto ( デフォルト )

!
interface Port-channel2
nameifなし
セキュリティレベルなし
IPアドレスがありません
!
インターフェイスポートチャンネル2.202
vlan 202
nameif外部
ctsマニュアル
propagate sgt preserve-untag ( sgtの保存/タグ
解除を伝播 )
policy static sgt disabled trusted ( 信頼できるポ
リシースタティックsgt無効 )
セキュリティレベル0
ipアドレス192.168.76.10 255.255.255.0スタン
バイ192.168.76.11
!
interface Port-channel3
nameifなし
セキュリティレベルなし
IPアドレスがありません
!
interface Ethernet1/1
管理専用
nameif診断
セキュリティレベル0
IPアドレスがありません
!
interface Ethernet1/4
nameif内部
セキュリティレベル0
ipアドレス192.168.75.10 255.255.255.0スタン
バイ192.168.75.11
!
FTPモードパッシブ
ngips conn-match vlan-id ( オプション )
```

<p>access-group CSM_FW_ACL_global access-list CSM_FW_ACL_remark rule-id 9998: PREFIX POLICY : デフォルトトンネルとプ ライオリティポリシー access-list CSM_FW_ACL_remark rule-id 9998 : ルール : デフォルトトンネルアクシ ョン ルール access-list CSM_FW_ACL_advanced permit ipinip anyルールID 9998 access-list CSM_FW_ACL_advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any range 1025 65535 any eq 3544ルール ID 9998 access-list CSM_FW_ACL_advanced permit 41 anyルールID 9998 access-list CSM_FW_ACL_advanced permit gre any anyルールID 9998 access-list CSM_FW_ACL_remark rule-id 268439552 : アクセスポリシー : acp_simple - 必須 access-list CSM_FW_ACL_remark rule-id 268439552: L7 RULE: rule1 access-list CSM_FW_ACL_advanced permit ip any any rule-id268439552 ! tcpマップUM_STATIC_TCP_MAP tcpオプション範囲6 7許可 tcpオプション範囲9 18許可 tcpオプション範囲20 255 : 許可 緊急フラグ許可 ! ポケットベルなし no logging message 106015 no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100 no logging message 302015 no logging message 302014 no logging message 302013 no logging message 302018 no logging message 302017 no logging message 302016</p>	<p>オブジェクトグループ検索アクセスコントロー ル access-group CSM_FW_ACL_global access-list CSM_FW_ACL_remark rule-id 9998: PREFIX POLICY : デフォルトトンネルとプ ライオリティポリシー access-list CSM_FW_ACL_remark rule-id 9998 : ルール : デフォルトトンネルアクシ ョン ルール access-list CSM_FW_ACL_advanced permit ipinip anyルールID 9998 access-list CSM_FW_ACL_advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_advanced permit udp any range 1025 65535 any eq 3544ルール ID 9998 access-list CSM_FW_ACL_advanced permit 41 anyルールID 9998 access-list CSM_FW_ACL_advanced permit gre any anyルールID 9998 access-list CSM_FW_ACL_remark rule-id 268439552 : アクセスポリシー : acp_simple - 必須 access-list CSM_FW_ACL_remark rule-id 268439552: L7 RULE: rule1 access-list CSM_FW_ACL_advanced permit ip any any rule-id268439552 ! tcpマップUM_STATIC_TCP_MAP tcpオプション範囲6 7許可 tcpオプション範囲9 18許可 tcpオプション範囲20 255 : 許可 緊急フラグ許可 ! ポケットベルなし no logging message 106015 no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100 no logging message 302015 no logging message 302014 no logging message 302013 no logging message 302018</p>
--	--

no logging message 302021 no logging message 302020 mtu outside 1500 MTU診断1500 mtu inside 1500 フェールオーバー フェールオーバーLANユニットセカンダリ failover lan interface FOVERポートチャンネル3 フェールオーバーレプリケーションHTTP フェールオーバーリンクFOVERポートチャンネル3 フェールオーバーインターフェイスIP FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 <output omitted>	no logging message 302017 no logging message 302016 no logging message 302021 no logging message 302020 mtu outside 1500 MTU診断1500 mtu inside 1500 フェールオーバーなし no monitor-interface外部 no monitor-interfaceサービスモジュール <output omitted>
---	---

HA の解除に関する主な注意点 :

プライマリ/スタンバイユニット	セカンダリ/アクティブユニット
<ul style="list-style-type: none"> すべてのフェールオーバー設定が削除されます。 すべてのIP設定が削除される 	<ul style="list-style-type: none"> すべてのフェールオーバー設定が削除されます。 スタンバイIPは残りますが、次の展開では削除されます

ステップ 5 : この作業が終了したら、HAペアを再作成します。

タスク 6.HAペアの削除

このタスクは、7.2.8ソフトウェアを使用する41xxのHAセットアップに基づいています。この場合、最初はデバイスは次の状態でした。

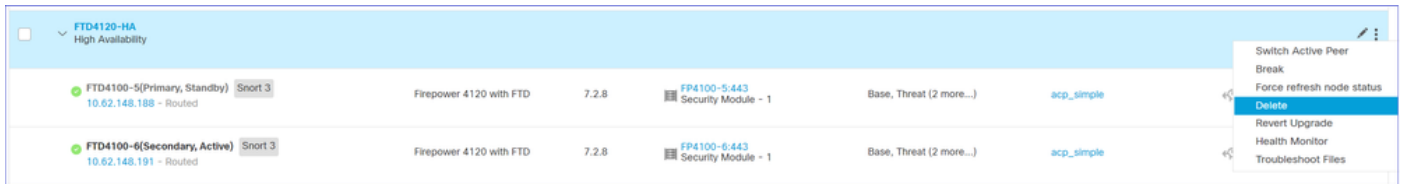
- プライマリ/スタンバイ
- セカンダリ/アクティブ

タスク要件 :

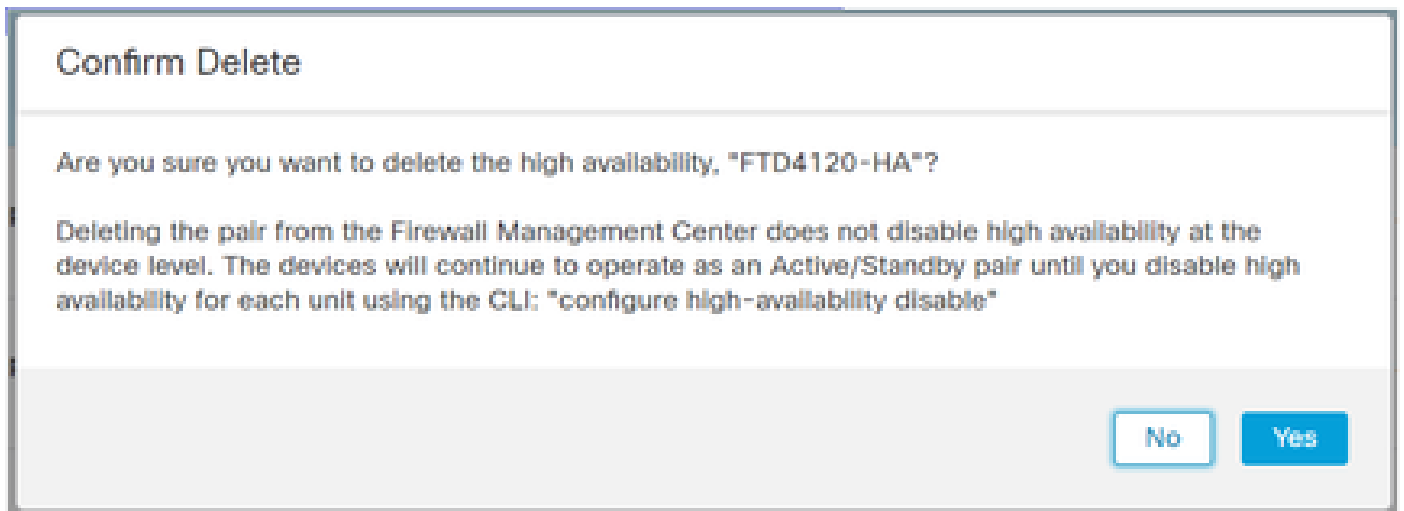
FMCから、フェールオーバーペアを削除します。

ソリューション :

ステップ 1 : 図に示すアイコンを選択します。



ステップ 2 : 次の図に示すように、通知を確認して確定します。



ステップ 3 : HAを削除すると、両方のデバイスがFMCから登録解除 (削除) されます。

LINA CLI からの show running-config コマンドの結果は、次の表のようになります。

プライマリユニット (スタンバイ)	セカンダリユニット (アクティブ)
<pre>> show running-config : 保存済み : : シリアル番号 : FLM1949C5RR : ハードウェア : FPR4K-SM-24、73853 MB RAM、CPU Xeon E5シリーズ2200 MHz、2 CPU (48コア) : NGFWバージョン7.2.8 ! ホスト名Firepower-module1 イネーブルパスワード*****暗号化 強力な暗号化を無効にする no asp inspect-dp ack-passthrough service-module 0キープアライブタイムアウト4 service-module 0キープアライブカウンタ6 names no mac-address auto (デフォルト)</pre>	<pre>> show running-config : 保存済み : : シリアル番号 : FLM2108V9YG : ハードウェア : FPR4K-SM-24、73853 MB RAM、CPU Xeon E5シリーズ2200 MHz、2 CPU (48コア) : NGFWバージョン7.2.8 ! ホスト名Firepower-module1 イネーブルパスワード*****暗号化 強力な暗号化を無効にする no asp inspect-dp ack-passthrough service-module 0キープアライブタイムアウト4 service-module 0キープアライブカウンタ6 names no mac-address auto (デフォルト)</pre>

<pre>! interface Port-channel2 nameifなし セキュリティレベルなし IPアドレスがありません ! インターフェイスポートチャンネル2.202 vlan 202 nameif NET202 ctsマニュアル propagate sgt preserve-untag (sgtの保存/タグ 解除を伝播) policy static sgt disabled trusted (信頼できるポ リシースタティックsgt無効) セキュリティレベル0 ipアドレス172.16.202.1 255.255.255.0スタンバ イ172.16.202.2 ! インターフェイスポートチャンネル2.203 vlan 203 nameif NET203 ctsマニュアル propagate sgt preserve-untag (sgtの保存/タグ 解除を伝播) policy static sgt disabled trusted (信頼できるポ リシースタティックsgt無効) セキュリティレベル0 ipアドレス172.16.203.1 255.255.255.0スタンバ イ172.16.203.2 ! interface Port-channel3 説明LAN/ステートフェールオーバーインターフ ェイス ! interface Ethernet1/1 管理専用 nameif診断 ctsマニュアル propagate sgt preserve-untag (sgtの保存/タグ 解除を伝播) policy static sgt disabled trusted (信頼できるポ リシースタティックsgt無効) セキュリティレベル0 IPアドレスがありません ! interface Ethernet1/4</pre>	<pre>! interface Port-channel2 nameifなし セキュリティレベルなし IPアドレスがありません ! インターフェイスポートチャンネル2.202 vlan 202 nameif NET202 ctsマニュアル propagate sgt preserve-untag (sgtの保存/タグ 解除を伝播) policy static sgt disabled trusted (信頼できるポ リシースタティックsgt無効) セキュリティレベル0 ipアドレス172.16.202.1 255.255.255.0スタンバ イ172.16.202.2 ! インターフェイスポートチャンネル2.203 vlan 203 nameif NET203 ctsマニュアル propagate sgt preserve-untag (sgtの保存/タグ 解除を伝播) policy static sgt disabled trusted (信頼できるポ リシースタティックsgt無効) セキュリティレベル0 ipアドレス172.16.203.1 255.255.255.0スタンバ イ172.16.203.2 ! interface Port-channel3 説明LAN/ステートフェールオーバーインターフ ェイス ! interface Ethernet1/1 管理専用 nameif診断 ctsマニュアル propagate sgt preserve-untag (sgtの保存/タグ 解除を伝播) policy static sgt disabled trusted (信頼できるポ リシースタティックsgt無効) セキュリティレベル0 IPアドレスがありません ! interface Ethernet1/4</pre>
---	---

nameif NET204 ctsマニュアル propagate sgt preserve-untag (sgtの保存/タグ解除を伝播) policy static sgt disabled trusted (信頼できるポリシースタティックsgt無効) セキュリティレベル0 ipアドレス172.16.204.1 255.255.255.0スタンバイ172.16.204.2 ! FTPモードパッシブ ngips conn-match vlan-id (オプション) no object-group-searchアクセスコントロール access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY : デフォルトトンネルとプライオリティポリシー access-list CSM_FW_ACL_ remark rule-id 9998 : ルール : デフォルトトンネルアクションルール access-list CSM_FW_ACL_ advanced permit ipinip anyルールID 9998 access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544ルールID 9998 access-list CSM_FW_ACL_ advanced permit 41 anyルールID 9998 access-list CSM_FW_ACL_ advanced permit gre any anyルールID 9998 access-list CSM_FW_ACL_ remark rule-id 268434433 : アクセスポリシー : acp_simple - デフォルト access-list CSM_FW_ACL_ remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ advanced permit ip any any rule-id268434433 ! tcpマップUM_STATIC_TCP_MAP tcpオプション範囲6 7許可 tcpオプション範囲9 18許可 tcpオプション範囲20 255 : 許可 tcpオプションmd5クリア	nameif NET204 ctsマニュアル propagate sgt preserve-untag (sgtの保存/タグ解除を伝播) policy static sgt disabled trusted (信頼できるポリシースタティックsgt無効) セキュリティレベル0 ipアドレス172.16.204.1 255.255.255.0スタンバイ172.16.204.2 ! FTPモードパッシブ ngips conn-match vlan-id (オプション) no object-group-searchアクセスコントロール access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY : デフォルトトンネルとプライオリティポリシー access-list CSM_FW_ACL_ remark rule-id 9998 : ルール : デフォルトトンネルアクションルール access-list CSM_FW_ACL_ advanced permit ipinip anyルールID 9998 access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544ルールID 9998 access-list CSM_FW_ACL_ advanced permit 41 anyルールID 9998 access-list CSM_FW_ACL_ advanced permit gre any anyルールID 9998 access-list CSM_FW_ACL_ remark rule-id 268434433 : アクセスポリシー : acp_simple - デフォルト access-list CSM_FW_ACL_ remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ advanced permit ip any any rule-id268434433 ! tcpマップUM_STATIC_TCP_MAP tcpオプション範囲6 7許可 tcpオプション範囲9 18許可 tcpオプション範囲20 255 : 許可 tcpオプションmd5クリア
--	--

緊急フラグ許可

!

ポケットベルなし

no logging message 106015

no logging message 313001

no logging message 313008

no logging message 106023

no logging message 710003

no logging message 106100

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

mtu NET202 1500

mtu NET203 1500

MTU診断1500

mtu NET204 1500

フェールオーバー

failover lan unit primary

failover lan interface FOVERポートチャンネル3

フェールオーバーレプリケーションHTTP

フェールオーバーリンクFOVERポートチャンネル

3

フェールオーバーインターフェイスIP FOVER

172.16.51.1 255.255.255.0 standby 172.16.51.2

モニタインターフェイスNET202

モニタインターフェイスNET203

icmp到達不能レート制限1バーストサイズ1

<output omitted>

> show ip

システムIPアドレス :

インターフェイス名IPアドレスサブネットマスク方式

Port-channel2.202 NET202 172.16.202.1

255.255.255.0設定

Port-channel2.203 NET203 172.16.203.1

255.255.255.0設定

Port-channel3 FOVER 172.16.51.1

255.255.255.0未設定

緊急フラグ許可

!

ポケットベルなし

no logging message 106015

no logging message 313001

no logging message 313008

no logging message 106023

no logging message 710003

no logging message 106100

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

mtu NET202 1500

mtu NET203 1500

MTU診断1500

mtu NET204 1500

フェールオーバー

フェールオーバーLANユニットセカンダリ

failover lan interface FOVERポートチャンネル3

フェールオーバーレプリケーションHTTP

フェールオーバーリンクFOVERポートチャンネル

3

フェールオーバーインターフェイスIP FOVER

172.16.51.1 255.255.255.0 standby 172.16.51.2

モニタインターフェイスNET202

モニタインターフェイスNET203

icmp到達不能レート制限1バーストサイズ1

<output omitted>

>show ip

システムIPアドレス :

インターフェイス名IPアドレスサブネットマスク方式

Port-channel2.202 NET202 172.16.202.1

255.255.255.0設定

Port-channel2.203 NET203 172.16.203.1

255.255.255.0設定

Port-channel3 FOVER 172.16.51.1

255.255.255.0未設定

<p>Ethernet1/4 NET204 172.16.204.1 255.255.255.0構成 現在のIPアドレス： インターフェイス名IPアドレスサブネットマスク方式 Port-channel2.202 NET202 172.16.202.2 255.255.255.0設定 Port-channel2.203 NET203 172.16.203.2 255.255.255.0設定 Port-channel3 FOVER 172.16.51.1 255.255.255.0未設定 Ethernet1/4 NET204 172.16.204.2 255.255.255.0構成</p> <p>> show failover フェールオーバーOn フェールオーバーユニットプライマリ フェールオーバーLANインターフェイス ：FOVER Port-channel3 (アップ) 再接続タイムアウト0:00:00 ユニットポーリング頻度1秒、ホールドタイム 15秒 インターフェイスポーリング頻度5秒、ホールド タイム25秒 インターフェイスポリシー1 監視対象インターフェイス4/1291 (最大) MACアドレス移動通知間隔が設定されていま せん フェールオーバーレプリケーションHTTP バージョン：9.18(4)210、Mate 9.18(4)210 シリアル番号：FLM1949C5RR、Mate FLM2108V9YG 最終フェールオーバー：2024年7月16日 13:56:37 UTC このホスト：プライマリ - スタンバイ準備完了 アクティブ時間：0 (秒) スロット0:UCSB-B200-M3-U hw/sw rev(0.0/9.18(4)210)ステータス (アップシステム) インターフェイスNET202(172.16.202.2)：正常 (モニタ済み) インターフェイスNET203(172.16.203.2)：正常 (モニタ済み) インターフェイス診断(0.0.0.0)：正常 (待機中) インターフェイスNET204(172.16.204.2)：正常</p>	<p>Ethernet1/4 NET204 172.16.204.1 255.255.255.0構成 現在のIPアドレス： インターフェイス名IPアドレスサブネットマスク ク方式 Port-channel2.202 NET202 172.16.202.1 255.255.255.0設定 Port-channel2.203 NET203 172.16.203.1 255.255.255.0設定 Port-channel3 FOVER 172.16.51.2 255.255.255.0未設定 Ethernet1/4 NET204 172.16.204.1 255.255.255.0構成</p> <p>> show failover フェールオーバーOn フェールオーバーユニットセカンダリ フェールオーバーLANインターフェイス ：FOVER Port-channel3 (アップ) 再接続タイムアウト0:00:00 ユニットポーリング頻度1秒、ホールドタイム 15秒 インターフェイスポーリング頻度5秒、ホールド タイム25秒 インターフェイスポリシー1 監視対象インターフェイス4/1291 (最大) MACアドレス移動通知間隔が設定されていま せん フェールオーバーレプリケーションHTTP バージョン：9.18(4)210、Mate 9.18(4)210 シリアル番号：FLM2108V9YG、Mate FLM1949C5RR 最終フェールオーバー：2024年7月16日 13:42:35 UTC このホスト：セカンダリ - アクティブ アクティブ時間：70312 (秒) スロット0:UCSB-B200-M3-U hw/sw rev(0.0/9.18(4)210)ステータス (アップシステム) インターフェイスNET202(172.16.202.1)：正常 (モニタ済み) インターフェイスNET203(172.16.203.1)：正常 (モニタ済み) インターフェイス診断(0.0.0.0)：正常 (待機中) インターフェイスNET204(172.16.204.1)：正常</p>
--	--

<p>(モニタ済み)</p> <p>スロット1:snort rev(1.0)ステータス (アップ)</p> <p>スロット2: diskstatus rev (1.0)ステータス (アップ)</p> <p>その他のホスト : セカンダリ - アクティブ</p> <p>アクティブ時間 : 70293 (秒)</p> <p>インターフェイスNET202(172.16.202.1) : 正常 (モニタ済み)</p> <p>インターフェイスNET203(172.16.203.1) : 正常 (モニタ済み)</p> <p>インターフェイス診断(0.0.0.0) : 正常 (待機中)</p> <p>インターフェイスNET204(172.16.204.1) : 正常 (モニタ済み)</p> <p>スロット1:snort rev(1.0)ステータス (アップ)</p> <p>スロット2: diskstatus rev (1.0)ステータス (アップ)</p> <p><output omitted></p>	<p>(モニタ済み)</p> <p>スロット1:snort rev(1.0)ステータス (アップ)</p> <p>スロット2: diskstatus rev (1.0)ステータス (アップ)</p> <p>その他のホスト : プライマリ - スタンバイ準備完了</p> <p>アクティブ時間 : 0 (秒)</p> <p>スロット0:UCSB-B200-M3-U hw/sw rev(0.0/9.18(4)210)ステータス (アップシステム)</p> <p>インターフェイスNET202(172.16.202.2) : 正常 (モニタ済み)</p> <p>インターフェイスNET203(172.16.203.2) : 正常 (モニタ済み)</p> <p>インターフェイス診断(0.0.0.0) : 正常 (待機中)</p> <p>インターフェイスNET204(172.16.204.2) : 正常 (モニタ済み)</p> <p>スロット1:snort rev(1.0)ステータス (アップ)</p> <p>スロット2: diskstatus rev (1.0)ステータス (アップ)</p> <p><output omitted></p>
---	--

ステップ 4 : 両方のFTDデバイスがFMCから登録解除されました。

<#root>

> show managers

No managers configured.

FMC の [HA の無効化 (Disable HA)] オプションに関する主な注意点 :

プライマリ ユニット	セカンダリ ユニット
<p>デバイスが FMC から削除されます。</p> <p>FTDデバイスから削除された設定はありません。</p>	<p>デバイスが FMC から削除されます。</p> <p>FTDデバイスから削除された設定はありません。</p>

シナリオ 1

configure high-availability disableコマンドを実行して、アクティブなFTDデバイスからフェール

オーバー設定を削除します。

```
<#root>
```

```
>
```

```
configure high-availability disable
```

```
?
```

```
Optional parameter to clear interfaces (clear-interfaces) optional parameter to clear interfaces (clear-interfaces)
<cr>
```

```
<#root>
```

```
>
```

```
configure high-availability disable
```

```
High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':
```

```
yes
```

```
Successfully disabled high-availability.
```

結果は、次のとおりです。

プライマリユニット(ex-Standby)	セカンダリユニット(ex-Active)
<pre>> INFO: This unit is currently in standby state. By disabling failover, this unit will remain in standby state. > show failover Failover Off (pseudo-Standby) Failover unit Primary Failover LAN Interface: FOVER Port-channel3 (up) Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 0 of 1291 maximum MAC Address Move Notification Interval not set failover replication http</pre>	<pre>> show failover Failover Off Failover unit Secondary Failover LAN Interface: not Configured Reconnect timeout 0:00:00 Unit Poll frequency 1 seconds, holdtime 15 seconds Interface Poll frequency 5 seconds, holdtime 25 seconds Interface Policy 1 Monitored Interfaces 4 of 1291 maximum MAC Address Move Notification Interval not set > show ip System IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG</pre>

<pre>> show ip System IP Addresses: Interface Name IP address Subnet mask Method Port-channel3 FOVER 172.16.51.1 255.255.255.0 unset Current IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG</pre>	<pre>Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG Current IP Addresses: Interface Name IP address Subnet mask Method Port-channel2.202 NET202 172.16.202.1 255.255.255.0 CONFIG Port-channel2.203 NET203 172.16.203.1 255.255.255.0 CONFIG Ethernet1/4 NET204 172.16.204.1 255.255.255.0 CONFIG</pre>
<p>プライマリ (以前のスタンバイ)</p>	<p>セカンダリ(ex-Active)</p>
<pre>> show running-config : 保存済み : : シリアル番号 : FLM1949C5RR : ハードウェア : FPR4K-SM-24、73853 MB RAM、CPU Xeon E5シリーズ2200 MHz、2 CPU (48コア) : NGFWバージョン7.2.8 ! ホスト名Firepower-module1 イネーブルパスワード*****暗号化 強力な暗号化を無効にする no asp inspect-dp ack-passthrough service-module 0キープアライブタイムアウト4 service-module 0キープアライブカウンタ6 names no mac-address auto (デフォルト) ! interface Port-channel2 shutdown nameifなし セキュリティレベルなし no ip address <- IPが削除されます。 ! interface Port-channel3 説明LAN/ステートフェールオーバーインターフ ェイス</pre>	<pre>> show running-config : 保存済み : : シリアル番号 : FLM2108V9YG : ハードウェア : FPR4K-SM-24、73853 MB RAM、CPU Xeon E5シリーズ2200 MHz、2 CPU (48コア) : NGFWバージョン7.2.8 ! ホスト名Firepower-module1 イネーブルパスワード*****暗号化 強力な暗号化を無効にする no asp inspect-dp ack-passthrough service-module 0キープアライブタイムアウト4 service-module 0キープアライブカウンタ6 names no mac-address auto (デフォルト) ! interface Port-channel2 nameifなし セキュリティレベルなし IPアドレスがありません ! インターフェイスポートチャンネル2.202 vlan 202 nameif NET202 ctsマニュアル</pre>

<pre> ! interface Ethernet1/1 管理専用 shutdown nameifなし セキュリティレベルなし IPアドレスがありません ! interface Ethernet1/4 shutdown nameifなし セキュリティレベルなし IPアドレスがありません ! FTPモードパッシブ ngips conn-match vlan-id (オプション) no object-group-searchアクセスコントロール access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY : デフォルトトンネルとプ ライオリティポリシー access-list CSM_FW_ACL_ remark rule-id 9998 : ルール : デフォルトトンネルアクション ルール access-list CSM_FW_ACL_ advanced permit ipinip anyルールID 9998 access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544ルール ID 9998 access-list CSM_FW_ACL_ advanced permit 41 anyルールID 9998 access-list CSM_FW_ACL_ advanced permit gre any anyルールID 9998 access-list CSM_FW_ACL_ remark rule-id 268434433 : アクセスポリシー : acp_simple - デフォルト access-list CSM_FW_ACL_ remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ advanced permit ip any any rule-id268434433 ! tcpマップUM_STATIC_TCP_MAP </pre>	<pre> propagate sgt preserve-untag (sgtの保存/タグ 解除を伝播) policy static sgt disabled trusted (信頼できるポ リシースタティックsgt無効) セキュリティレベル0 ipアドレス172.16.202.1 255.255.255.0スタンバ イ172.16.202.2 ! インターフェイスポートチャンネル2.203 vlan 203 nameif NET203 ctsマニュアル propagate sgt preserve-untag (sgtの保存/タグ 解除を伝播) policy static sgt disabled trusted (信頼できるポ リシースタティックsgt無効) セキュリティレベル0 ipアドレス172.16.203.1 255.255.255.0スタンバ イ172.16.203.2 ! interface Port-channel3 nameifなし セキュリティレベルなし IPアドレスがありません ! interface Ethernet1/1 管理専用 nameif診断 ctsマニュアル propagate sgt preserve-untag (sgtの保存/タグ 解除を伝播) policy static sgt disabled trusted (信頼できるポ リシースタティックsgt無効) セキュリティレベル0 IPアドレスがありません ! interface Ethernet1/4 nameif NET204 ctsマニュアル propagate sgt preserve-untag (sgtの保存/タグ 解除を伝播) policy static sgt disabled trusted (信頼できるポ リシースタティックsgt無効) セキュリティレベル0 ipアドレス172.16.204.1 255.255.255.0スタンバ イ172.16.204.2 </pre>
--	--

<pre> tcpオプション範囲6 7許可 tcpオプション範囲9 18許可 tcpオプション範囲20 255 : 許可 tcpオプションmd5クリア 緊急フラグ許可 ! ポケットベルなし no logging message 106015 no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100 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 フェールオーバーなし failover lan unit primary failover lan interface FOVERポートチャンネル3 フェールオーバーレプリケーションHTTP フェールオーバーリンクFOVERポートチャンネル3 フェールオーバーインターフェイスIP FOVER 172.16.51.1 255.255.255.0 standby 172.16.51.2 no monitor-interfaceサービスモジュール <output omitted> </pre>	<pre> ! FTPモードパッシブ ngips conn-match vlan-id (オプション) no object-group-searchアクセスコントロール access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ remark rule-id 9998: PREFIX FILTER POLICY : デフォルトトンネルとプ ライオリティポリシー access-list CSM_FW_ACL_ remark rule-id 9998 : ルール : デフォルトトンネルアクション ルール access-list CSM_FW_ACL_ advanced permit ipinip anyルールID 9998 access-list CSM_FW_ACL_ advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 access-list CSM_FW_ACL_ advanced permit udp any range 1025 65535 any eq 3544ルール ID 9998 access-list CSM_FW_ACL_ advanced permit 41 anyルールID 9998 access-list CSM_FW_ACL_ advanced permit gre any anyルールID 9998 access-list CSM_FW_ACL_ remark rule-id 268434433 : アクセスポリシー : acp_simple - デフォルト access-list CSM_FW_ACL_ remark rule-id 268434433: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ advanced permit ip any any rule-id268434433 ! tcpマップUM_STATIC_TCP_MAP tcpオプション範囲6 7許可 tcpオプション範囲9 18許可 tcpオプション範囲20 255 : 許可 tcpオプションmd5クリア 緊急フラグ許可 ! ポケットベルなし no logging message 106015 no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710003 no logging message 106100 </pre>
---	--


	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 mtu NET202 1500 mtu NET203 1500 MTU診断1500 mtu NET204 1500 フェールオーバーなし モニタインターフェイスNET202 モニタインターフェイスNET203 no monitor-interfaceサービスモジュール
--	---

アクティブなFTD CLIからHAを無効にするための主な注意事項：

アクティブユニット	スタンバイユニット
<ul style="list-style-type: none"> フェールオーバーの設定が削除される スタンバイIPは削除されない 	<ul style="list-style-type: none"> インターフェイス設定が削除されます。 フェールオーバー設定は削除されませんが、フェールオーバーは無効になります (擬似スタンバイ)。

この時点で、以前のスタンバイユニットでもHAを無効にできます。

シナリオ2(非推奨)

 **警告**：このシナリオではアクティブ/アクティブ状態になるため、お勧めしません。これは認識のためだけに表示されます。

configure high-availability disableコマンドを実行して、スタンバイFTDデバイスのフェールオーバー設定を解除します。

```
<#root>
```

```
>
```

```
configure high-availability disable
```

High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':

YES

Successfully disabled high-availability.

結果は、次のとおりです。

プライマリ (以前のスタンバイ)	セカンダリ (アクティブ)
<pre>> show failover フェールオーバーオフ フェールオーバーユニットセカンダリ フェールオーバーLANインターフェイス：未設定 再接続タイムアウト0:00:00 ユニットポーリング頻度1秒、ホールドタイム15秒 インターフェイスポーリング頻度5秒、ホールドタイム25秒 インターフェイスポリシー1 監視対象インターフェイス4/1291 (最大) MACアドレス移動通知間隔が設定されていません > show ip システムIPアドレス： インターフェイス名IPアドレスサブネットマスク方式 Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual ← デバイスがex-Active! ポートチャネル2.203 NET203 172.16.203.1 255.255.255.0手動 Ethernet1/4 NET204 172.16.204.1 255.255.255.0マニュアル 現在のIPアドレス： インターフェイス名IPアドレスサブネットマスク方式 ポートチャネル2.202 NET202 172.16.202.1 255.255.255.0手動 ポートチャネル2.203 NET203 172.16.203.1 255.255.255.0手動 Ethernet1/4 NET204 172.16.204.1</pre>	<pre>> show failover Failover On < : フェールオーバーが無効になっていません フェールオーバーユニットセカンダリ フェールオーバーLANインターフェイス : FOVER Port-channel3 (アップ) 再接続タイムアウト0:00:00 ユニットポーリング頻度1秒、ホールドタイム15秒 インターフェイスポーリング頻度5秒、ホールドタイム25秒 インターフェイスポリシー1 監視対象インターフェイス4/1291 (最大) MACアドレス移動通知間隔が設定されていません フェールオーバーレプリケーションHTTP バージョン : 9.18(4)210、Mate 9.18(4)210 シリアル番号 : FLM2108V9YG、Mate FLM1949C5RR 最終フェールオーバー : 2024年7月17日 12:44:06 UTC このホスト : セカンダリ - アクティブ アクティブ時間 : 632 (秒) スロット0:UCSB-B200-M3-U hw/sw rev(0.0/9.18(4)210)ステータス (アップシステム) インターフェイス診断(0.0.0.0) : 正常 (待機中) インターフェイスNET204(172.16.204.1) : 正常 (モニタ済み) インターフェイスNET203(172.16.203.1) : 正常 (モニタ済み) インターフェイスNET202(172.16.202.1) : 正常 (モニタ済み)</pre>

<p>255.255.255.0マニュアル</p>	<p> スロット1:snort rev(1.0)ステータス (アップ) スロット2: diskstatus rev (1.0)ステータス (アップ) その他のホスト : プライマリ - 無効 アクティブ時間 : 932 (秒) スロット0:UCSB-B200-M3-U hw/sw rev(0.0/9.18(4)210)ステータス (アップシステム) インターフェイス診断(0.0.0.0) : 不明 (待機中) インターフェイスNET204(172.16.204.2) : 不明 (監視対象) インターフェイスNET203(172.16.203.2) : 不明 (監視対象) インターフェイスNET202(172.16.202.2) : 不明 (監視対象) スロット1:snort rev(1.0)ステータス (アップ) スロット2: diskstatus rev (1.0)ステータス (アップ) > show ip システムIPアドレス : インターフェイス名IPアドレスサブネットマスク方式 Port-channel2.202 NET202 172.16.202.1 255.255.255.0 manual ← デバイスが以前のスタンバイと同じIPを使用している ! ポートチャネル2.203 NET203 172.16.203.1 255.255.255.0手動 Port-channel3 FOVER 172.16.51.1 255.255.255.0未設定 Ethernet1/4 NET204 172.16.204.1 255.255.255.0マニュアル 現在のIPアドレス : インターフェイス名IPアドレスサブネットマスク方式 ポートチャネル2.202 NET202 172.16.202.1 255.255.255.0手動 ポートチャネル2.203 NET203 172.16.203.1 255.255.255.0手動 Port-channel3 FOVER 172.16.51.2 255.255.255.0未設定 Ethernet1/4 NET204 172.16.204.1 255.255.255.0マニュアル </p>
---------------------------	---

アクティブなFTD CLIからHAを無効にするための主な注意事項 :

アクティブユニット	スタンバイユニット
<ul style="list-style-type: none"> フェールオーバー設定は削除されず、有効のままになります デバイスは、以前のスタンバイユニットと同じIPを使用します 	<ul style="list-style-type: none"> フェールオーバーの設定が削除される デバイスがアクティブユニットと同じIPを使用している

シナリオ 3

configure high-availability disable clear-interfacesコマンドを実行して、アクティブなFTDデバイスからフェールオーバーの設定を削除します。

```
<#root>
```

```
>
```

```
configure high-availability disable clear-interfaces
```

```
High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':
```

```
yes
```

```
Successfully disabled high-availability.
```

```
>
```

結果は、次のとおりです。

プライマリ (以前のスタンバイ)	セカンダリ(ex-Active)
<pre>> show failover フェイルオーバーオフ (擬似スタンバイ) フェールオーバーユニットプライマリ フェールオーバーLANインターフェイス : FOVER Port-channel3 (アップ) 再接続タイムアウト0:00:00 ユニットポーリング頻度1秒、ホールドタイム 15秒 インターフェイスポーリング頻度5秒、ホールド タイム25秒 インターフェイスポリシー1</pre>	<pre>> show failover フェールオーバーオフ フェールオーバーユニットセカンダリ フェールオーバーLANインターフェイス: 未設 定 再接続タイムアウト0:00:00 ユニットポーリング頻度1秒、ホールドタイム 15秒 インターフェイスポーリング頻度5秒、ホールド タイム25秒 インターフェイスポリシー1</pre>

<p>監視対象インターフェイス0/1291 (最大) MACアドレス移動通知間隔が設定されていません フェールオーバーレプリケーションHTTP</p> <pre>> show ip システムIPアドレス : インターフェイス名IPアドレスサブネットマスク方式 Port-channel3 FOVER 172.16.51.1 255.255.255.0未設定 現在のIPアドレス : インターフェイス名IPアドレスサブネットマスク方式 Port-channel3 FOVER 172.16.51.1 255.255.255.0未設定 ></pre>	<p>監視対象インターフェイス0/1291 (最大) MACアドレス移動通知間隔が設定されていません</p> <pre>> show ip システムIPアドレス : インターフェイス名IPアドレスサブネットマスク方式 現在のIPアドレス : インターフェイス名IPアドレスサブネットマスク方式 ></pre>
---	--

アクティブなFTD CLIの「clear-interfaces」とともに、Disable HAに関する主な注意事項：

アクティブユニット	スタンバイユニット
<ul style="list-style-type: none"> フェールオーバーの設定が削除される IPが削除されます 	<ul style="list-style-type: none"> フェールオーバー設定は削除されませんが、フェールオーバーは無効になります (擬似スタンバイ)。 IPが削除されます

シナリオ 4

configure high-availability disable clear-interfacesコマンドを実行して、スタンバイFTDデバイスからフェールオーバーコンフィギュレーションを削除します。

```
<#root>
```

```
>
```

```
configure high-availability disable clear-interfaces
```

```
High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':
```

```
YES
```

```
Successfully disabled high-availability.
```

>

結果は、次のとおりです。

プライマリ (以前のスタンバイ)	セカンダリ (アクティブ)
<pre>> show failover フェールオーバーオフ フェールオーバーユニットセカンダリ フェールオーバーLANインターフェイス : 未設定 再接続タイムアウト0:00:00 ユニットポーリング頻度1秒、ホールドタイム15秒 インターフェイスポーリング頻度5秒、ホールドタイム25秒 インターフェイスポリシー1 監視対象インターフェイス0/1291 (最大) MACアドレス移動通知間隔が設定されていません > show ip システムIPアドレス : インターフェイス名IPアドレスサブネットマスク方式 現在のIPアドレス : インターフェイス名IPアドレスサブネットマスク方式 ></pre>	<pre>> show failover フェールオーバーOn フェールオーバーユニットセカンダリ フェールオーバーLANインターフェイス : FOVER Port-channel3 (アップ) 再接続タイムアウト0:00:00 ユニットポーリング頻度1秒、ホールドタイム15秒 インターフェイスポーリング頻度5秒、ホールドタイム25秒 インターフェイスポリシー1 監視対象インターフェイス4/1291 (最大) MACアドレス移動通知間隔が設定されていません フェールオーバーレプリケーションHTTPバージョン : 9.18(4)210、Mate 9.18(4)210 シリアル番号 : FLM2108V9YG、Mate FLM1949C5RR 最終フェールオーバー : 07:06:56 UTC Jul 18 2024 このホスト : セカンダリ - アクティブ アクティブ時間 : 1194 (秒) スロット0:UCSB-B200-M3-U hw/sw rev(0.0/9.18(4)210)ステータス (アップシステム) インターフェイス診断(0.0.0.0) : 正常 (待機中) インターフェイスNET204(172.16.204.1) : 正常 (モニタ済み) インターフェイスNET202(172.16.202.1) : 正常 (モニタ済み) インターフェイスNET203(172.16.203.1) : 正常 (モニタ済み) スロット1:snort rev(1.0)ステータス (アップ) スロット2: diskstatus rev (1.0)ステータス (アップ) その他のホスト : プライマリ - 無効</pre>

	<p> アクティブ時間 : 846 (秒) スロット0:UCSB-B200-M3-U hw/sw rev(0.0/9.18(4)210)ステータス (アップシステム) インターフェイス診断(0.0.0.0) : 不明 (待機中) インターフェイスNET204(172.16.204.2) : 不明 (監視対象) インターフェイスNET202(172.16.202.2) : 不明 (監視対象) インターフェイスNET203(172.16.203.2) : 不明 (監視対象) スロット1:snort rev(1.0)ステータス (アップ) スロット2: diskstatus rev (1.0)ステータス (アップ) </p> <p> > show ip システムIPアドレス : インターフェイス名IPアドレスサブネットマスク方式 ポートチャンネル2.202 NET202 172.16.202.1 255.255.255.0手動 ポートチャンネル2.203 NET203 172.16.203.1 255.255.255.0手動 Port-channel3 FOVER 172.16.51.1 255.255.255.0未設定 Ethernet1/4 NET204 172.16.204.1 255.255.255.0マニュアル 現在のIPアドレス : インターフェイス名IPアドレスサブネットマスク方式 ポートチャンネル2.202 NET202 172.16.202.1 255.255.255.0手動 ポートチャンネル2.203 NET203 172.16.203.1 255.255.255.0手動 Port-channel3 FOVER 172.16.51.2 255.255.255.0未設定 Ethernet1/4 NET204 172.16.204.1 255.255.255.0マニュアル </p>
--	--

アクティブなFTD CLIの「clear-interfaces」とともに、Disable HAに関する主な注意事項 :

アクティブユニット	スタンバイユニット
-----------	-----------

- フェールオーバー設定は削除されません
- IPは削除されません

- フェールオーバーの設定が削除される
- IPが削除されます

手順 6 : タスクが完了したら、デバイスをFMCに登録し、HAペアを有効にします。

タスク 7.HAの中断

タスク要件 :

FTD CLISH CLI から HA を一時停止させます。

ソリューション :

ステップ 1 : プライマリFTDでコマンドを実行し、確認します(YESと入力)。

```
<#root>
```

```
> configure high-availability suspend
```

```
Please ensure that no deployment operation is in progress before suspending high-availability.  
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to
```

```
YES
```

```
Successfully suspended high-availability.
```

ステップ 2 : プライマリユニットの変更を確認します。

```
<#root>
```

```
>
```

```
show high-availability config
```

```
Failover Off
```

```
Failover unit Primary  
Failover LAN Interface: fover_link Ethernet1/4 (up)  
Reconnect timeout 0:00:00  
Unit Poll frequency 1 seconds, holdtime 15 seconds  
Interface Poll frequency 5 seconds, holdtime 25 seconds  
Interface Policy 1  
Monitored Interfaces 1 of 1041 maximum  
MAC Address Move Notification Interval not set  
failover replication http
```

ステップ 3 : セカンダリユニットでの結果 :

<#root>

>

```
show high-availability config
Failover Off (pseudo-Standby)

Failover unit Secondary
Failover LAN Interface: fover_link Ethernet1/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

ステップ 4 : プライマリユニットでのHAの再開 :

<#root>

>

```
configure high-availability resume

Successfully resumed high-availability.
```

> .

```
    No Active mate detected
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate
```

>

<#root>

>

```
show high-availability config

Failover On

Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

ステップ 5 : HAを再開した後のセカンダリユニットでの結果 :

```
<#root>
```

```
> ..
```

```
Detected an Active mate
```

```
Beginning configuration replication from mate.
```

```
WARNING: Failover is enabled but standby IP address is not configured for this interface.
```

```
WARNING: Failover is enabled but standby IP address is not configured for this interface.
```

```
End configuration replication from mate.
```

```
>
```

```
<#root>
```

```
>
```

```
show high-availability config
```

```
Failover On
```

```
Failover unit Secondary
```

```
Failover LAN Interface: fover_link Ethernet1/4 (up)
```

```
Reconnect timeout 0:00:00
```

```
Unit Poll frequency 1 seconds, holdtime 15 seconds
```

```
Interface Poll frequency 5 seconds, holdtime 25 seconds
```

```
Interface Policy 1
```

```
Monitored Interfaces 1 of 1041 maximum
```

```
MAC Address Move Notification Interval not set
```

```
failover replication http
```

```
>
```

よく寄せられる質問 (FAQ)

構成が複製されると、その構成は直ちに (1行ずつ) 保存されますか、それとも複製の最後に保存されますか。

複製の完了時です。設定/コマンドの複製を示す debug fover sync コマンドの出力の最後で、それを確認できます。

```
<#root>
```

```
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1506 remark rule-id 268442578: L7 RUL
```

```
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1507 advanced permit tcp object-group
```

```
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1508 remark rule-id 268442078: ACCESS
```

```
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1509 remark rule-id 268442078: L4 RUL
```

```
...
```

```
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_
```

```
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: ACC
```

```
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: L7
```

```
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: ACC
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: L4
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268442078
cli_xml_server: frep_write_cmd: Cmd: crypto isakmp nat-traversal
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_311
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_433
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_6
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_2
cli_xml_server: frep_write_cmd: Cmd:
```

```
write memory <--
```

ユニットが擬似スタンバイ状態（フェールオーバーがディセーブル）で、そのユニットをリロードした後、他方のユニットがフェールオーバーをイネーブルにしてアクティブになっている場合はどうなりますか。

最終的にアクティブ/アクティブシナリオになります（技術的にはアクティブ/フェールオーバーオフになります）。具体的には、ユニットが起動するとフェールオーバーは無効になりますが、そのユニットはアクティブユニットと同じ IP を使用します。そのため、事実上、次のようになります。

- ユニット1：アクティブ
- ユニット2：フェールオーバーがオフになっています。ユニットでは、ユニット1と同じデータIPが使用されますが、MACアドレスは異なります。

手でフェールオーバーを無効にし（ハイアベイラビリティ中断を設定し）、デバイスをリロードすると、フェールオーバー設定はどうなりますか。

フェールオーバーを無効にした場合、永続的な変更ではありません（明示的に変更しない限り、startup-configには保存されません）。ユニットのリブートとリロードは2通りの方法で実行できます。2つ目の方法では注意が必要です。

Case 1. CLISHからのリブート

CLISHからのリブートでは、確認は求められません。そのため、設定の変更はスタートアップ設定に保存されません。

```
<#root>
```

```
>
```

```
configure high-availability suspend
```

```
Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to
```

```
YES
```

```
Successfully suspended high-availability.
```

running-configではフェールオーバーが無効になっています。この例では、アクティブ/アクティブシナリオを回避するために、ユニットはスタンバイ状態で、期待どおりに擬似スタンバイ状態になりました。

```
<#root>
firepower#
show failover | include Failover
Failover Off (
pseudo-Standby
)
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

startup-configでは、フェールオーバーは引き続き有効になっています。

```
<#root>
firepower#
show startup | include failover
failover
failover lan unit secondary
failover lan interface FOVER Ethernet1/1
failover replication http
failover link FOVER Ethernet1/1
failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2
failover ipsec pre-shared-key *****
```

CLISH からデバイスをリブートします (reboot コマンド)。

```
<#root>
>
reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO':
YES
Broadcast message from root@
Threat Defense System: CMD=-stop, CSP-ID=cisco-ftd.6.2.2.81__ftd_001_JMX2119L05CYRIBVX1, FLAG=' '
Cisco FTD stopping ...
```

ユニットが起動すると、フェールオーバーが有効になっているため、デバイスはフェールオーバー ネゴシエーション フェーズに入り、リモートピアの検出を試みます。

```
<#root>
```

```
User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower> .
```

```
Detected an Active mate
```

Case 2.LINA CLIからのリポート

LINA からのリポート (reload コマンド) では、確認が求められます。したがって、Y(Yes)を選択した場合、設定変更はstartup-configに保存されます。

```
<#root>
```

```
firepower#
```

```
reload
```

```
System config has been modified. Save? [Y]es/[N]o:
```

```
Y <-- Be careful. This disables the failover in the startup-config
```

```
Cryptochecksum: 31857237 8658f618 3234be7c 854d583a
```

```
8781 bytes copied in 0.940 secs
```

```
Proceed with reload? [confirm]
```

```
firepower#
```

```
show startup | include failover
```

```
no failover
```

```
failover lan unit secondary
```

```
failover lan interface FOVER Ethernet1/1
```

```
failover replication http
```

```
failover link FOVER Ethernet1/1
```

```
failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2
```

```
failover ipsec pre-shared-key *****
```

ユニットが起動すると、フェールオーバーは無効になります。

```
<#root>
```


```
firepower#
```

```
show failover | include Fail
```

```
Failover Off
```

```
Failover unit Secondary
```

```
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

 注：このシナリオを回避するには、プロンプトが表示されたら、変更をstartup-configに保存しないようにしてください。

関連情報

- Cisco Firepower Management Center のすべてのバージョンの設定ガイドが、ここにありません。

[Cisco Secure Firewall Threat Defenseに関するドキュメントの参照](#)

- FXOS Chassis Manager および CLI のすべてのバージョンの設定ガイドが、ここにありません。

[Cisco Firepower 4100/9300 FXOSドキュメントの参照](#)

- Cisco Firepower次世代セキュリティテクノロジーに関する詳細な実践知識を得るために、Cisco Global Technical Assistance Center(TAC)は次のビジュアルガイドを強く推奨します。

[Cisco Firepower Threat Defense\(FTD\) : 次世代ファイアウォール\(NGFW\)、次世代侵入防御システム\(NGIPS\)、および高度なマルウェア防御\(AMP\)の設定とトラブルシューティングのベストプラクティス](#)

- Firepowerテクノロジーに関連するすべての設定およびトラブルシューティングテクニカルノート

[Cisco Secureファイアウォール管理センター](#)

- [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。