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
 使用するコンボーネント
 タスク 1.条件の確認
 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 5.HAペアの解除
 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 PIC	Equipped	VID Equipped Serial	(SN) Slot Status	Ackd Memory (MB) Ack	1 Cores
1/1	FPR9K-SM-36	5 V01	FLM19216KK6	Equipped	262144	36
1/2	FPR9K-SM-36	5 V01	FLM19206H71	Equipped	262144	36
1/3	FPR9K-SM-36	5 V01	FLM19206H7T	Equipped	262144	36
KSEC-EI	PR9K-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-FP	R9K-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 Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	FP4100-5:443 El Security Module - 1	Base, Threat (2 more)	acp_simple	ę,	1:
FTD4100-6 Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	Executive Module - 1	Base, Threat (2 more)	acp_simple	Q+	1:

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。

	Deployme	ent History
Q Search De	evice	Add 🔻
	Device	
	High A	vailability
Auto RollBack	Cluster	r
	Group	

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。

Ver	rion Charala Liannaa	
	Add High Availability Pair	ľ
	Name:*	
7.2	Device Type:	n (:
7.2	Firewall Threat Defense 🔹	n (:
	Primary Peer:	
	FTD4100-5	
	Secondary Peer:	
	FTD4100-6 v	
	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.	
	Cancel Continue	

▲ 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 デバイスの間に 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。

ligh Availabi	ility Link	State Link		
Interface:*	Port-channel3 v	Interface:*	Same as LAN Failover Link	٣
ogical Name:*	FOVER	Logical Name:*	FOVER	
Primary IP:*	172.16.51.1	Primary IP:*	172.16.51.1	
1	Use IPv6 Address		Use IPv6 Address	
Secondary IP:*	172.16.51.2	Secondary IP:*	172.16.51.2	
Subnet Mask:*	255.255.255.0	Subnet Mask:*	255.255.255.0	
Psec Encryp	ition			
Key Generation:	Auto 👻			
LAN failover l between peers.	link is used to sync configuration, statefu Selected interface links and encryption :	ul failover link is used settings cannot be cl	I to sync application content hanged later.	

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。

V FTD4120-HA High Availability							1
FTD4100-5(Primary, Active) Short 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	E Security Module - 1	Base, Threat (2 more)	acp_simple	4Ø	:
FTD4100-6(Secondary, Standby) Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	EP4100-6:443 Security Module - 1	Base, Threat (2 more)	acp_simple	40	:

ステップ5:インターフェイスを設定します。

Edit Physic	al Inter	face			0
General	IPv4	IPv6	Path Monitoring	Advanced	
Name:					
Inside					
Enabled					
Managem	ent Only				
Description:					
Mode:					
None			*		
Security Zone:					
			*		
Interface ID:					
Ethernet1/4					
MTU:					
1500					
(64 - 9184)					
Priority:					
0			(0 - 65535)		
Propagate Sec	ourity Gro	sup Tag:	0		
NVE Only:					
0					
					Cancel OK
Edit Physic	al Inter	face			٥

Ealt Physi	cal inter	Tace						0
General	IPv4	IPv6	Path Monitoring	Advanced				
IP Type:								
Use Static	IP		Ŧ					
IP Address:								
192.168.7	5.10/24							
							Cancel	ОК

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。

Edit Ether	Edit Ether Channel Interface							
General	IPv4	IPv6	Path Monitoring	Advanced				
Name:					Í			
Enabled								
Manager	ment Only							
Description:								

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。

Firewall Management Cer Devices / High Availability	nter _{Overview}	Analysis Policies	Devices Objects Integra	tion			Deploy Q 🚱 🔅	🛛 mzafeiro 🕶	tesce SECURE
FTD4120-HA Cisco Firepower 4120 Threat Defense								Sav	Cancel
Summary High Availability Dev	ice Routing Interfa	ces Inline Sets DI	HCP VTEP						
High Availability Configuration									
High Availability Link					State Link				
Interface			Port-channel3		Interface			Port-	channel3
Logical Name			FOVER		Logical Name				FOVER
Primary IP			172.16.51.1		Primary IP			17:	2.16.51.1
Secondary IP			172.16.51.2		Secondary IP			17:	2.16.51.2
Subnet Mask			255.255.255.0		Subnet Mask			255.2	55.255.0
IPsec Encryption			Disabled		Statistics				Q,
Monitored Interfaces									
Interface Name	Aution (Ded	Standard Dud	Author (Ded Standby (Ded.			Asthus Link, Local Phot	Classifier Link, Local Phyl.	Manifesing	
	ACTAG IS AC	Standoy in ve	Active IPvo - acanoby IPvo			Active Link-Local IP40	standoy Link-Local IPY0	Monitoring	
inside	192.168.75.10							•	
diagnostic								•	1
Outside	192.168.76.10							•	1

手順7:図に示す内部インターフェイス用。

Edit Inside	0
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	ок

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 IIPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitoring	
😭 Inside	192.168.75.10	192.168.75.11				•	/
diagnostic						•	/
Cutside	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 12Outside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	/1
Port-channel2.202	aaaa.bbbb.3333	aaaa.bbbb.4444	/1

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。



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-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 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

This hast	State	Last Failure Reason	Date/Time
This nost -	Active	None	
Other host -	Secondary		
	Standby Ready	Comm Failure	18:32:56 EEST Jul 21 2016
====Configurat Sync Done ====Communicat Mac set	ion State===		

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。

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
Т
interface Port-channel2
no nameif
no security-level
no ip address
1
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
Т
interface Port-channel3
description LAN/STATE Failover Interface
interface Ethernet1/1
management-only
nameif diagnostic
security-level 0
no ip address
I.
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。

FTD4120-HA High Availability							Switch Active Peer
FTD4100-5(Primary, Active) Snort 3 10.62.148.188 - Routed	Firepower 4120 with FTD	7.2.8	EP4100-5:443 Security Module - 1	Base, Threat (2 more)	acp_simple	Q9	Break Force refresh node status Delete Revert Upgrade
FTD4100-6(Secondary, Standby) Snort 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	E Security Module - 1	Base, Threat (2 more)	acp_simple	Q.	Health Monitor Troubleshoot Files

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。

新しいアクティブ	新しり
>フェールオーバー履歴の表示 0	
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)	> 7
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)	0.=== 状態; 0.===
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 config バー:
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)	

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。

Confirm Break
Breaking the High Availability pair "FTD4120-HA" will erase all configuration except the Access Control and Flex Config policy from standby peer. This operation might also restart Snort processes of primary and secondary devices, temporarily causing traffic interruption. Are you sure you want to break the pair? Force break, if standby peer does not respond
No Yes

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。

0	Deployments	Upgra	des	Health	Tasks		Sho	ow Notific	ation	s
2	0+ total	0 waiting	0 running	0 retrying	20+ success	1 failure	Q. Filter]
0	Policy Deployr Policy Deplo	nent syment to F	TD4100-5	. Applied succ	cessfully			<u>47s</u>	×	ĺ
0	Policy Pre-Dep Pre-deploy I success	ployment Device Cor	nfiguration	for FTD4100)-5			35	×	
0	Policy Pre-Dep Pre-deploy success	oloyment Global Con	figuration	Generation				4s	×	
0	High Availabili HA pair has be peer FTD4100 complete on F	ty een broken s -5 policies a TD4100-5 b	uccessfully a re being del vefore config	and all policies leted by an aut uring its policie	have been retained to triggered deployr es.	l on active peer l nent. Please allo	FTD4100-6. Standby w this deployment to	<u>1m 59s</u>	×	
_				Rem	ove completed ta	asks		·		

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ブレーク前のプライマリ/スタンバイユニット	HAブレーク後のプライマリユニット
>show running-configコマンド :保存済み :	>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。
: 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	 > 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) <li:< li=""> NGFWバージョン7.2.8 </li:<>

service-module 0キープアライブタイムアウト4	
service-module $0 + - \nabla P = 7 - 7 - 7 - 7 - 7 - 7 - 7 - 7 - 7 - 7$	。 ホスト名firepower
names	イネーブルパスワード*****暗号化
no mac-address auto(デフォルト)	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
interface Port-channel2	names
nameifなし	no mac-address auto(デフォルト)
ctsマニュアル	
propagate sgt preserve-untag(sgtの保存/タグ解	!
除を伝播)	interface Port-channel2
policy static sgt disabled trusted(信頼できるボ	shutdown
リシー人タティックsgt無効)	nameifなし
	セキュリティレベルなし
IPアドレスかありません	IPアドレスかありません
! _ /ヽ. ケーフェ /フヂート チャ チョ り 000	! interface Dart sharped?
インダーノエイスホートティズル2.202 vien 202	Interface Port-channel3
vian 202 namaif办 部	
	$+\pm_1 \pm_1 \pm_1 = + + + + + + + + +$
uss、ニュアル propagate sat preserve_untag(satの保存/タグ解	
propagate syt preserve-unitag(sytw) 本中クク麻 除を伝播)	
policy static set disabled trusted (信頼できるポ	interface Ethernet1/1
リシースタティックsqt無効)	管理専用
セキュリティレベル0	shutdown
ipアドレス192.168.76.10 255.255.255.0スタンバ	nameifなし
・ イ192.168.76.11	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	!
説明LAN/ステートフェールオーバーインターフ	interface Ethernet1/4
エイス	shutdown
!	nameifなし
interface Ethernet1/1	セキュリティレベルなし
管理専用	IPアドレスがありません
nameif診断	!
ctsマニュアル	FTPモードパッシフ
propagate sgt preserve-untag(sgtの保存/タグ解	ngips conn-match vlan-id(オブション)
除を伝播)	オフジェクトクループ検索アクセムコントロー
policy static sgt disabled trusted(信頼できるホ	
リンースダティックsgt無効)	access-group CSM_FW_ACL_ global
IF / トレヘルのりません I	ッッシュ・ドトロードコード POLIGY テノタルトトノネ ルとプライオリティポリシー
ا interface Ethernet1/۸	access_list CSM_FW_ACL_remark rule_id
nameif内部	000035-1131 00101_1 W_AOL_ Ternark Tule-10 9998 ・ルール・デフォルトトンネルアクション
ctsマーュアル	$\mathbb{L} = \mathbb{L}$

ſ

propagate sgt preserve-untag(sgtの保存/タグ解	access-list CSM_FW_ACL_ advanced permit
除を伝播)	ipinip anyルールD 9998
policy static sgt disabled trusted(信頼できるポ	access-list CSM_FW_ACL_ advanced permit
リシースタティックsgt無効)	udp any eq 3544 any range 1025 65535 rule-id
セキュリティレベル0	9998
ipアドレス192.168.75.10 255.255.255.0スタンバ	access-list CSM_FW_ACL_ advanced permit
イ192.168.75.11	udp any range 1025 65535 any eq 3544ルール
: 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-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-group CSM_FW_ACL_ global	access-list CSM_FW_ACL_ remark rule-id
access-list CSM_FW_ACL_ remark rule-id 9998:	268439552:アクセスポリシー: acp_simple –
PREFILTER POLICY:デフォルトトンネルとプ	必須
ライオリティポリシー	access-list CSM_FW_ACL_ remark rule-id
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	268439552: L7 RULE: rule1 access-list CSM_FW_ACL_ advanced permit ip any any rule-id268439552 ! ten Z w Z LIM_STATIC_TCP_MAP
access-list CSM_FW_ACL_ advanced permit udp	tcpオプション範囲6 7許可
any eq 3544 any range 1025 65535 rule-id 9998	tcpオプション範囲9 18許可
access-list CSM_FW_ACL_ advanced permit udp	tcpオプション範囲20 255 : 許可
any range 1025 65535 any eq 3544/L-/LID	緊急フラグ許可
9998	!
access-list CSM_FW_ACL_ advanced permit 41	ポケットベルなし
anyルールID 9998	no logging message 106015
access-list CSM_FW_ACL_ advanced permit gre	no logging message 313001
any anyルールID 9998	no logging message 313008
access-list CSM_FW_ACL_ remark rule-id	no logging message 106023
268434433:アクセスポリシー: acp_simple –	no logging message 710003
デフォルト	no logging message 106100
access-list CSM_FW_ACL_ remark rule-id	no logging message 302015
268434433: L4 RULE: DEFAULT ACTION RULE	no logging message 302014
access-list CSM_FW_ACL_ advanced permit ip	no logging message 302013
any any rule-id268434433	no logging message 302018
!	no logging message 302017
tcpマップUM_STATIC_TCP_MAP	no logging message 302016
tcpオプション範囲6 7許可	no logging message 302021
tcpオプション範囲9 18許可	no logging message 302020
tcpオプション範囲20 255 : 許可	フェールオーバーなし
緊急フラグ許可	<output omitted=""></output>
! 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 302015 no logging message 302015 no logging message 302014 no logging message 302017 no logging message 302017 no logging message 302021 no logging message 302020 mtu outside 1500 MTU診断1500 mtu inside 1500 $7 = -\mathcal{N} \vec{x} - \mathcal{N} -$ failover lan unit primary failover lan unit primary failover lan unit primary failover lan unit primary failover lan unit primary ドレス : Ethernet1/4 aaaa.bbbb.1111 aaaa.bbbb.2222 $7 = -\mathcal{N} \vec{x} - \mathcal{N} - \mathcal$	
HAブレーク前のセカンダリ/アクティブユニッ ト	HAブレーク後のセカンダリユニット
>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 !	> 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

ホスト名firepower	!
イネーブルパスワード*****暗号化	ー ホスト名firepower
強力な暗号化を無効にする	イネーブルパスワード*****暗号化
service-module 0キープアライブタイムアウト4	強力な暗号化を無効にする
service-module 0キープアライブカウンタ6	service-module 0キープアライブタイムアウト4
names	service-module 0キープアライブカウンタ6
no mac-address auto(デフォルト)	names
	no mac-address auto(デフォルト)
!	
interface Port-channel2	
	Interface Port-channel2
セキュリティレベルなし	
IPアドレスかありません	
	IPアドレスかありません L
インダーノエイスホートナヤネル2.202	
vlan 202	インダーノエイスホートナヤネル2.202
nameif/阶部	vlan 202
cts イニュアル	
propagate sgt preserve-untag (sgtの保存/タク	
解际を広播)	propagate sgt preserve-untag (sgtの保存/タク
policy static sgt disabled trusted(信頼できるホ	解际を伝播)
リシースダティックsgt無効)	policy static sgt disabled trusted(信頼できる示
セキュリティレベルU	リシースダティックsgt無効)
IPアトレス192.108.76.10 255.255.255.0スタノ	セイユリティレベルU
11 192.108.70.11	IP アレス 192.108.70.10 255.255.255.0スタノ
! interface Dart channel?	111 192.108.70.11
Intenace Port-channels 説明LAN/フニートフェールオーバーインターフ	! interface Dort channel?
読明LAN/スノードノェールオーバーインヌーノ ェイフ	
: interface Ethernet1/1	
管理車田	
nameif診断	interface Ethernet1/1
セキュリティレベル0	管理専用
IPアドレスがありません	nameif診断
!	セキュリティレベル0
interface Ethernet1/4	IPアドレスがありません
nameif内部	! !
セキュリティレベル0	interface Ethernet1/4
ipアドレス192.168.75.10 255.255.255.0スタン	nameif内部
バイ192.168.75.11	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
FTPモードパッシブ	バイ192.168.75.11
ngips conn-match vlan-id(オプション)	<u>!</u>
オブジェクトグループ検索アクセスコントロー	FTPモードパッシブ
้ม	ngips conn-match vlan-id(オプション)

Т

access-group CSM_FW_ACL_ global	オブジェクトグループ検索アクセスコントロー
access-list CSM_FW_ACL_ remark rule-id 9998:	ル
PREFILTER POLICY:デフォルトトンネルとプ	access-group CSM_FW_ACL_ global
ライオリティポリシー	access-list CSM_FW_ACL_ remark rule-id 9998:
access-list CSM_FW_ACL_ remark rule-id	PREFILTER POLICY:デフォルトトンネルとプ
9998:ルール:デフォルトトンネルアクション	ライオリティポリシー
ルール	access-list CSM_FW_ACL_ remark rule-id
access-list CSM_FW_ACL_ advanced permit	9998:ルール:デフォルトトンネルアクション
ipinip anyルールID 9998	ルール
access-list CSM_FW_ACL_ advanced permit	access-list CSM_FW_ACL_ advanced permit
udp any eq 3544 any range 1025 65535 rule-id	ipinip anyルールID 9998
9998	access-list CSM_FW_ACL_ advanced permit
access-list CSM_FW_ACL_ advanced permit	udp any eq 3544 any range 1025 65535 rule-id
udp any range 1025 65535 any eq 3544ルール	9998
ID 9998	access-list CSM_FW_ACL_ advanced permit
access-list CSM_FW_ACL_ advanced permit 41	udp any range 1025 65535 any eq 3544ルール
anyルールID 9998	ID 9998
access-list CSM_FW_ACL_ advanced permit gre	access-list CSM_FW_ACL_ advanced permit 41
any anyルールID 9998	anyルールID 9998
access-list CSM_FW_ACL_ remark rule-id	access-list CSM_FW_ACL_ advanced permit gre
268439552:アクセスポリシー: acp_simple –	any anyルールID 9998
必須	access-list CSM_FW_ACL_ remark rule-id
access-list CSM_FW_ACL_ remark rule-id	268439552:アクセスポリシー: acp_simple -
268439552: L7 RULE: rule1	必須
access-list CSM_FW_ACL_ advanced permit ip	access-list CSM_FW_ACL_ remark rule-id
any any rule-id268439552	268439552: L7 RULE: rule1
!	access-list CSM_FW_ACL_ advanced permit ip
tcpマップUM_STATIC_TCP_MAP	any any rule-id268439552
tcpオプション範囲67許可	
tcpオプション範囲9 18許可	tcpマップUM_STATIC_TCP_MAP
tcpオブション範囲20 255:許可	
緊急フラク許可 -	
	tcpオブション範囲20 255:許可
ホケットベルなし	緊急ノフク計可 .
no logging message 106015	
no logging message 313001	ホケットベルなし 400045
no logging message 313008	no logging message 106015
no logging message 106023	no logging message 313001
no logging message /10003	no logging message 313008
no logging message 106100	no logging message 106023
no logging message 302015	no logging message 710003
no logging message 302014	no logging message 106100
no logging message 302013	no logging message 302015
no logging message 302018	no logging message 302014
no logging message 302017	no logging message 302013
no logging message 302016	no logging message 302018

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

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
 すべてのフェールオーバ	・ すべてのフェールオーバー設定が削除されます。
一設定が削除されます。 すべてのIP設定が削除される	・ 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。

V FTD4120-HA High Availability							Switch Active Peer
 FTD4100-5(Primary, Standby) Snort 3 10.62.148.188 - Routed 	Firepower 4120 with FTD	7.2.8	III FP4100-5:443 Security Module - 1	Base, Threat (2 more)	acp_simple	45	Break Force refresh node status Delete
FTD4100-6(Secondary, Active) Short 3 10.62.148.191 - Routed	Firepower 4120 with FTD	7.2.8	EFP4100-6:443 Security Module - 1	Base, Threat (2 more)	acp_simple	45	Health Monitor Troubleshoot Files

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。

Confirm Delete	
Are you sure you want to delete the high availability, "FTD4120-HA"? Deleting the pair from the Firewall Management Center does not disable high availability at the device level. The devices will continue to operate as an Active/Standby pair until you disable high availability for each unit using the CLI: "configure high-availability disable"	
No Yes	

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)
> show running-config	> show running-config
:保存済み	: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)	: :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	NGFWバージョン7.2.8
I	I
ホスト名Firepower-module1	ホスト名Firepower-module1
イネーブルパスワード****暗号化	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	強力な暗号化を無効にする
no asp inspect-dp ack-passthrough	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キープアライブタイムアウト4
service-module 0キープアライブカウンタ6	service-module 0キープアライブカウンタ6
names	names
no mac-address auto(デフォルト)	no mac-address auto(デフォルト)

1	
' interface Port-channel?	: interface Port-channel?
セキュリティレベルなし	ー ヤキュリティレベルなし
· インターフェイスポートチャネル2.202	ー インターフェイスポートチャネル2.202
vlan 202	vlan 202
nameif NET202	nameif NET202
ctsマニュアル	ctsマニュアル
propagate sgt preserve-untag(sgtの保存/タグ	propagate sgt preserve-untag(sgtの保存/タグ
解除を伝播)	解除を伝播)
policy static sgt disabled trusted(信頼できるポ	policy static sgt disabled trusted(信頼できるポ
リシースタティックsgt無効)	リシースタティックsgt無効)
セキュリティレベル0	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	ipアドレス172.16.202.1 255.255.255.0スタンバ
イ172.16.202.2	172.16.202.2
!	!
インターフェイスポートチャネル2.203	インターフェイスポートチャネル2.203
vlan 203	vlan 203
nameif NET203	nameif NET203
ctsマニュアル	ctsマニュアル
propagate sgt preserve-untag(sgtの保存/タク 解除を伝播)	propagate sgt preserve-untag(sgtの保存/タク 解除を伝播)
policy static sgt disabled trusted(信頼できるポ	policy static sgt disabled trusted(信頼できるポ
リシースタティックsgt無効)	リシースタティックsgt無効)
セキュリティレベル0	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	ipアドレス172.16.203.1 255.255.255.0スタンバ
イ172.16.203.2	172.16.203.2
!	!
interface Port-channel3	interface Port-channel3
説明LAN/ステートノエールオーハーインターノ	説明LAN/ステートノェールオーハーインターノ
! interface Ethernet1/1	! interface Ethernet1/1
menace Linemennin 答理 由 田	milenace Linemet // 1 答理 由 田
nameif診断	nameif診断
ctsマーュアル	ctsマーュアル
propagate sgt preserve-untag (sgtの保存/タグ	propagate sgt preserve-untag (sgtの保存/タグ
ment for the second s	ment of the second se
policy static sgt disabled trusted(信頼できるポ	policy static sgt disabled trusted(信頼できるポ
リシースタティックsgt無効)	リシースタティックsgt無効)
セキュリティレベル0	セキュリティレベル0
IPアドレスがありません	IPアドレスがありません
!	!
interface Ethernet1/4	interface Ethernet1/4

nameif NET204	nameif NET204
ctsマニュアル	ctsマニュアル
propagate sgt preserve-untag(sgtの保存/タグ	propagate sgt preserve-untag(sgtの保存/タグ
知险をにぜい	図除ちに振い
聨隊を伝播) 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	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	ipアドレス172.16.204.1 255.255.255.0スタンバ
・	
イ172.16.204.2	イ172.16.204.2
·	·
FTPモードパッシブ	FTPモードパッシブ
ngips conn-match vian-id(オノション)	ngips conn-match vian-id(オノション)
no object-group-searchアクセスコントロール	no object-group-searchアクセスコントロール
access-group CSM_FW_ACL_ global	access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ remark rule-id 9998:	access-list CSM_FW_ACL_ remark rule-id 9998:
PREFILTER POLICY:デフォルトトンネルとプ	PREFILTER POLICY:デフォルトトンネルとプ
ライオリティポリシー	ライオリティポリシー
access-list CSM_FW_ACL_ remark rule-id	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	9998:ルール:デフォルトトンネルアクション
ルール	ルール
access-list CSM_FW_ACL_ advanced permit	access-list CSM_FW_ACL_ advanced permit
IPINIP ANY//-//ID 9998	IDINIP any/2-7210 9998
udp any eq 3544 any range 1025 65535 rule-id	udp any eq 3544 any range 1025 65535 rule-id
9998	9998
access-list CSM_FW_ACL_ advanced permit	access-list CSM_FW_ACL_ advanced permit
udp any range 1025 65535 any eq 3544ルール	udp any range 1025 65535 any eq 3544ルール
ID 9998	ID 9998
access-list CSM_FW_ACL_ advanced permit 41	access-list CSM_FW_ACL_ advanced permit 41
anyルールID 9998	anyルールID 9998
access-list CSM_FW_ACL_ advanced permit gre	access-list CSM_FW_ACL_ advanced permit gre
any anyルールID 9998	any anyルールID 9998
access-list CSM_FW_ACL_ remark rule-id	access-list CSM_FW_ACL_ remark rule-id
268434433:アクセスポリシー: acp_simple –	268434433:アクセスポリシー: acp_simple –
デフォルト	デフォルト
access-list CSM_FW_ACL_ remark rule-id	access-list CSM_FW_ACL_ remark rule-id
268434433: L4 RULE: DEFAULT ACTION	268434433: L4 RULE: DEFAULT ACTION
RULE	
access-list CSM_FW_ACL_ advanced permit ip	access-list CSM_FW_ACL_ advanced permit ip
any any rule-id268434433	any any rule-id268434433
!	!
tcpマップUM_STATIC_TCP_MAP	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6 7許可
tcpオブション範囲9 18許可	tcpオブション範囲9 18許可
ICPオノンヨン範囲20 255:計り	tcpオノンヨン範囲20 255:計り
tanオプションmdEクリア	topオプションmd5クリア
	icpッファコンmuoフリア

緊急フラグ許可	 緊急フラグ許可
!	!
ポケットベルなし	ポケットベルなし
no logging message 106015	no logging message 106015
no logging message 313001	no logging message 313001
no logging message 313008	no logging message 313008
no logging message 106023	no logging message 106023
no logging message 710003	no logging message 710003
no logging message 106100	no logging message 106100
no logging message 302015	no logging message 302015
no logging message 302014	no logging message 302014
no logging message 302013	no logging message 302013
no logging message 302018	no logging message 302018
no logging message 302017	no logging message 302017
no logging message 302016	no logging message 302016
no logging message 302021	no logging message 302021
no logging message 302020	no logging message 302020
mtu NET202 1500	mtu NET202 1500
mtu NET203 1500	mtu NET203 1500
MTU診断1500	MTU診断1500
mtu NET204 1500	mtu NET204 1500
フェールオーバー	フェールオーバー
failover lan unit primary	フェールオーバーLANユニットセカンダリ
failover lan interface FOVERポートチャネル3	failover lan interface FOVERポートチャネル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ポートチャネル	フェールオーバーリンクFOVERポートチャネル
	っ フェールオーバーインターフェイフID EOV/EP
$7 \pm -773 - 77 - 775 = 7 \pm 7577 = 75777 = 7577 = 75777 = 75777 = 75777 = 75777 = 75777 = 75777 = 75777 = 75777 = 75777 = 75777 = 75777 = 75777 = 757777 = 75777 = 75777 = 757777 = 757777 = 757777 = 757777 = 757777 = 757777 = 757777 = 7577777 = 75777777 = 7577777777$	72 - 773 - 77 - 773 - 723 - 724 - 727 -
$T_{2.10.51.1255.255.255.05}$ standby $T_{2.10.51.2}$	$T_{2.10.51.1255.255.255.0511009172.10.51.2}$
$\Box = \mathcal{A} + \mathcal{A} \mathcal{A} = \mathcal{A} + \mathcal{A} + \mathcal{A} = \mathcal{A} + \mathcal{A} + \mathcal{A} = \mathcal{A} + \mathcal{A} + \mathcal{A} + \mathcal{A} = \mathcal{A} + \mathcal{A} $	$ \mathbf{L} = \mathbf{y}^{T} - \mathbf{y}^{T} - \mathbf{y}^{T} + \mathbf{z}^{T} - \mathbf{z}^{T} + $
レーダインダーノエイスNEI203	L _ ダインダーノェイへNET203
<output omitted=""></output>	<output omitted=""></output>
> show ip	>show ip
システムIPアドレス:	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	インターフェイス名IPアドレスサブネットマス
ク方式	ク方式
Port-channel2.202 NET202 172.16.202.1	Port-channel2.202 NET202 172.16.202.1
255.255.255.0設定	255.255.255.0設定
Port-channel2.203 NET203 172.16.203.1	Port-channel2.203 NET203 172.16.203.1
255.255.255.0設定	255.255.255.0設定
Port-channel3 FOVER 172.16.51.1	Port-channel3 FOVER 172.16.51.1
255.255.255.0未設定	255.255.255.0未設定

Ethernet1/4 NET204 172.16.204.1	Ethernet1/4 NET204 172.16.204.1
255.255.255.0構成 現在の10アドレフ・	255.255.255.0構成 現在の10アドレフ・
境任のIFファレス: インターフェイス名IPアドレスサブネットマス	成任のIFファレス: インターフェイス名IPアドレスサブネットマス
Port-channel2.202 NET202 172.16.202.2	Port-channel2.202 NET202 172.16.202.1
255.255.255.0設定	255.255.255.0設定
Port-channel2.203 NET203 172.16.203.2	Port-channel2.203 NET203 172.16.203.1
255.255.255.0設定	255.255.255.0設定
Port-channel3 FOVER 172.16.51.1	Port-channel3 FOVER 172.16.51.2
255.255.255.0未設定	255.255.255.0未設定
Ethernet1/4 NET204 172.16.204.2	Ethernet1/4 NET204 172.16.204.1
255.255.255.0構成	255.255.255.0構成
> show failover	> show failover
フェールオーバーOn	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	フェールオーバーLANインターフェイス
:FOVER Port-channel3(アップ)	:FOVER Port-channel3(アップ)
再接続タイムアウト0:00:00	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	ユニットポーリング頻度1秒、ホールドタイム
インターノエイスホーリンク頻度5秒、ホールド タッノ oc 手体	インターノエイスホーリンク頻度5秒、ホールド タノノ 05秒
メイム25秒 インターフェイフポルシー1	ダイム25秒 ノンターフェイフポルシー1
1 ノダーノェ1 ス小リシー 陸祖対象インターフェイフ //1201(是土)	1 ノダーノェ1 スホリシー 啓祖対象インターフェイフ4/1201 (是 +)
単代内家インスーノエイス4/1251(取八) MACアドレス移動通知問隔が設定されていませ	血代内家インスーノェイス4/1291(取八) MΔCアドレス移動通知問隔が設定されていませ
フェールオーバーレプリケーションHTTP	フェールオーバーレプリケーションHTTP
バージョン:9.18(4)210、Mate 9.18(4)210	バージョン:9.18(4)210、Mate 9.18(4)210
シリアル番号:FLM1949C5RR、Mate	シリアル番号:FLM2108V9YG、Mate
FLM2108V9YG	FLM1949C5RR
最終フェールオーバー:2024年7月16日	最終フェールオーバー:2024年7月16日
13:56:37 UTC	13:42:35 UTC
このホスト:プライマリ-スタンバイ準備完了	このホスト:セカンダリ – アクティブ
アクティブ時間:0(秒)	アクティブ時間: 70312 (秒)
スロット0:UCSB-B200-M3-U hw/sw	スロット0:UCSB-B200-M3-U hw/sw
rev(0.0/9.18(4)210)ステーダス(アッノンステム 、	rev(0.0/9.18(4)210)ステーダス(アッノンステム
<i>)</i> インターフェイスNET202(172-16-202-2)・正営	/ インターフェイスNET202(172-16-202-1)・正覚
($T = q$ 済み)	(+- 232) (+- 232)
(ビーク海&) インターフェイスNFT203(172 16 203 2)・正常	(ビーク/4007) インターフェイスNFT203(172 16 203 1)・正常
(モニタ済み)	(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	インターフェイスNET204(172.16.204.1):正常

ſ

(モニタ済み)	(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	スロット2: diskstatus rev (1.0)ステータス(アッ
プ)	プ)
その他のホスト:セカンダリ – アクティブ	その他のホスト:プライマリ – スタンバイ準備
アクティブ時間: 70293 (秒)	完了
インターフェイスNET202(172.16.202.1):正常	アクティブ時間:0(秒)
(モニタ済み)	スロット0:UCSB-B200-M3-U hw/sw
インターフェイスNET203(172.16.203.1):正常	rev(0.0/9.18(4)210)ステータス(アップシステム
(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NET202(172.16.202.2):正常
	(モニタ済み)
/ インターフェイスNET204(172.16.204.1):正常	インターフェイスNET203(172.16.203.2):正常
(モニタ済み)	(モニタ済み)
$\nabla = 2 \sqrt{2} \sqrt{2}$	インターフェイス診断(0000)・正常(待機中
$\nabla \Pi^{\nu} h^{2}$ diskstatus rev (1.0) $\nabla T - \nabla X$ (T^{ν}	
	^ インターフェイスNFT204(172 16 204 2)・正常
	「「デジージー」「ジェージ」(H
<output omitted=""></output>	$\left(\begin{array}{c} 2 \\ - \end{array} \right)$
	$\nabla \Pi = \nabla \Lambda (T, V)$
	\neg
	<pre>coutput omitted></pre>

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
デバイスが FMC から削除されます。	デバイスが FMC から削除されます。
FTDデバイスから削除された設定はありません	FTDデバイスから削除された設定はありません
o	0

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 <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.

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

結果は、次のとおりです。

> 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-channel3 FOVER 172.16.51.1 255.255.255.0 unset	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
プライマリ(以前のスタンバイ)	セカンダリ(ex-Active)
> show running-config	> show running-config
:保存済み	: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)	: :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	NGFWバージョン7.2.8
ホスト名Firepower-module1	ホスト名Firepower-module1
イネーブルパスワード*****暗号化	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	強力な暗号化を無効にする
no asp inspect-dp ack-passthrough	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キープアライブタイムアウト4
service-module 0キープアライブカウンタ6	service-module 0キープアライブカウンタ6
names	names
no mac-address auto(デフォルト)	no mac-address auto(デフォルト)
!	!
interface Port-channel2	interface Port-channel2
shutdown	nameifなし
nameifなし	セキュリティレベルなし
セキュリティレベルなし	IPアドレスがありません
no ip address <- IPが削除されます。	!
!	インターフェイスポートチャネル2.202
interface Port-channel3	vlan 202
説明LAN/ステートフェールオーバーインターフ	nameif NET202
ェイス	ctsマニュアル

Т

ſ

!	propagate sgt preserve-untag (sgtの保存/タク
interface Ethernet1/1	解除を伝播)
官埋専用	policy static sgt disabled trusted(信頼できるホ
shutdown	リシースタティックsgt無効)
	セキュリティレベル0
セキュリティレベルなし	ipアドレス172.16.202.1 255.255.255.0スタンバ
IPアドレスがありません	1 172.16.202.2
interface Ethernet1/4	インターフェイスポートチャネル2.203
shutdown	vlan 203
nameifなし	nameif NET203
セキュリティレベルなし	ctsマニュアル
IPアドレスがありません	propagate sgt preserve-untag(sgtの保存/タグ
!	解除を伝播)
FTPモードパッシブ	policy static sgt disabled trusted(信頼できるポ
ngips conn-match vlan-id(オプション)	リシースタティックsgt無効)
no object-group-searchアクセスコントロール	セキュリティレベル0
access-group CSM_FW_ACL_ global	ipアドレス172.16.203.1 255.255.255.0スタンバ
access-list CSM_FW_ACL_ remark rule-id 9998:	イ172.16.203.2
PREFILTER POLICY:デフォルトトンネルとプ	!
ライオリティポリシー	interface Port-channel3
access-list CSM_FW_ACL_ remark rule-id	nameifなし
9998:ルール:デフォルトトンネルアクション	セキュリティレベルなし
ルール	IPアドレスがありません
access-list CSM_FW_ACL_ advanced permit	!
ipinip anyルールID 9998	interface Ethernet1/1
access-list CSM_FW_ACL_ advanced permit	管理専用
udp any eq 3544 any range 1025 65535 rule-id	nameif診断
9998	ctsマニュアル
access-list CSM_FW_ACL_ advanced permit	propagate sgt preserve-untag(sgtの保存/タグ
udp any range 1025 65535 any eq 3544ルール	解除を伝播)
ID 9998	policy static sgt disabled trusted(信頼できるポ
access-list CSM_FW_ACL_ advanced permit 41	リシースタティックsgt無効)
anyルールID 9998	セキュリティレベル0
access-list CSM_FW_ACL_ advanced permit gre	IPアドレスがありません
any anyルールID 9998	!
access-list CSM_FW_ACL_ remark rule-id	interface Ethernet1/4
268434433:アクセスポリシー: acp_simple –	nameif NET204
デフォルト	ctsマニュアル
access-list CSM_FW_ACL_ remark rule-id	propagate sgt preserve-untag(sgtの保存/タグ
268434433: L4 RULE: DEFAULT ACTION	解除を伝播)
RULE	policy static sgt disabled trusted(信頼できるポ
access-list CSM_FW_ACL_ advanced permit ip	リシースタティックsgt無効)
any any rule-id268434433	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
tcpマップUM_STATIC_TCP_MAP	1172.16.204.2

tenオプション節囲6.7許可	
topオプション範囲9 18許可	゚ FTPモードパッシブ
lcp/ファンコン範囲20 255 · 許可	$\frac{1}{2} = \frac{1}{2} $
topオプションmd5クリア	ngips conn-match vian-id (377537)
lcpオノノコンIIIUSノリア 取刍フラガ社可	
	access-group CSM_FW_ACL_ global
! ポケット ベリ たし	
	$= \chi + \mu = \chi + \mu z$
no logging message 313001	
no logging message 313008	9998:ルール:テノオルトトノネルドクショノ
no logging message 106023	
no logging message /10003	access-list CSM_FW_ACL_ advanced permit
no logging message 106100	ipinip anyルールID 9998
no logging message 302015	access-list CSM_FW_ACL_ advanced permit
no logging message 302014	udp any eq 3544 any range 1025 65535 rule-id
no logging message 302013	9998
no logging message 302018	access-list CSM_FW_ACL_ advanced permit
no logging message 302017	udp any range 1025 65535 any eq 3544ルール
no logging message 302016	ID 9998
no logging message 302021	access-list CSM_FW_ACL_ advanced permit 41
no logging message 302020	anyルールID 9998
フェールオーバーなし	access-list CSM_FW_ACL_ advanced permit gre
failover lan unit primary	any anyルールID 9998
failover lan interface FOVERポートチャネル3	access-list CSM_FW_ACL_ remark rule-id
フェールオーバーレプリケーションHTTP	268434433:アクセスポリシー: acp_simple –
フェールオーバーリンクFOVERポートチャネル	デフォルト
3	access-list CSM FW ACL remark rule-id
フェールオーバーインターフェイスIP FOVER	268434433: L4 RULE: DEFAULT ACTION
172.16.51.1 255.255.255.0 standby 172.16.51.2	RULE
no monitor-interfaceサービスモジュール	access-list CSM FW ACL advanced permit ip
	any any rule-id268434433
<output omitted=""></output>	
	ぃ tcpマップUM_STATIC_TCP_MAP
	tcpオプション節囲6 7許可
	topオプション範囲Q 18許可
	topオプション範囲20.255 · 許可
	topオプションmd5クリア
	ICPJ ノノコノIIIUSノリノ 取刍フラガ払可
	! ポケット ゕ µ ゎ !
	ホノントバンレムし no logging monogen 106015
	no logging message 313008
	no logging message 106023
	no logging message 710003
	no logging message 106100
	1

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
・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	 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。

	1
プライマリ(以前のスタンバイ)	セカンダリ(アクティブ)
> 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 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イ/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	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)

255.255.255.0マニュアル	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
	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) (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
	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
	curenteur/4 NET204 172.10.204.1 255.255.255.0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

Г

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 	 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)
> show failover	> show failover
フェイルオーバーオフ(擬似スタンバイ)	フェールオーバーオフ
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	フェールオーバーLANインターフェイス:未設
: FOVER Port-channel3(アップ)	定
再接続タイムアウト0:00:00	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	ユニットポーリング頻度1秒、ホールドタイム
15秒	15秒
インターフェイスポーリング頻度5秒、ホールド	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	タイム25秒
インターフェイスポリシー1	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 フェールオーバーレプリケーションHTTP	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 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 >	> 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 >

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
・フェールオーバーの設定が削 除される ・ IP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)。 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)
> 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 ユニットボーリング頻度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の/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 >	> 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) 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: 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)
> 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 172.16.51.1 255.255.255.0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

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	• フェールオーバーの設定が
されません	削除される
・ IPは削除されません	・ 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-availablity.

> .

>

<#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

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 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: ACC

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

手動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。

フェイ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 192.0.2.1 255.255.0 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からのリブート LINA からのリブート(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:

 \mathtt{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 192.0.2.1 255.255.0 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、ここにあります。

<u>Cisco Secure Firewall Threat Defenseに関するドキュメントの参照</u>

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

<u>Cisco Firepower 4100/9300 FXOSドキュメントの参照</u>

 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。

<u>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</u> 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

<u>Cisco Secureファイアウォール管理センター</u>

• <u>テクニカル サポートとドキュメント - Cisco Systems</u>

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。