firepower脅威対策のハイアベイラビリティに関 する問題のトラブルシューティング

内容
前提条件
<u>要件</u>
<u>使用するコンポーネント</u>
<u>背景説明</u>
<u>設計オプション</u>
HA用語
HA状態
<u>HA状態のフロー図</u>
<u>UIの検証</u>
<u>Firepower Management CenterマネージドFTD HA</u>
FDM管理対象FTD HA
ASDMマネージドASA HA
<u>FTD/ASA HAを実行する4100/9300用Firepowerシャーシマネージャ</u>
<u>CLIの確認</u>
トラブルシュート
シナリオ
<u>アプリ同期エラー</u>
<u>スタンバイノードが「CD App Sync error is App Config Apply Failed」でHAに参加できない</u>
<u>スタンバイノードが「APP SYNC timeoutが原因でHA状態の進行が失敗した」というメッセ</u> ージでHAに参加できない
ー スタンバイノードが「CD App Sync error is Failed to apply SSP config on standby」でHAに 参加できない
<u>ヘルスチェックの失敗</u>
<u>Snortのダウンまたはディスク障害</u>
<u>検出エンジン(SNORTインスタンス)がダウンしている</u>
<u>デバイスのディスク使用率が高い</u>
<u>サービスカードの障害</u>
<u>MIOハートビート障害</u>
<u>関連情報</u>

概要

このドキュメントでは、Firepower Threat Defense(FTD)のハイアベイラビリティ(HA)の運用、検 証、およびトラブルシューティングの手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- FTDおよびASAプラットフォーム
- FTDアプライアンスでのパケットキャプチャ

このドキュメントで説明されているコンセプトをよりよく理解するために、『<u>Firepower設定ガイ</u> <u>ド : FirepowerアプライアンスでのFTDハイアベイラビリティの設定</u>』を参照することを強くお勧 めします。

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。

- ・シスコFTD
- Cisco Firepower Management Center (FMC)

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

背景説明

情報と例はFTDに基づいていますが、概念のほとんどは適応型セキュリティアプライアンス (ASA)にも完全に適用できます。

FTDは、次の2つの主要な管理モードをサポートしています。

- FMC経由のオフボックス:リモート管理とも呼ばれます。
- ・ firepower Device Manager(FDM)経由のオンボックス ローカル管理とも呼ばれます。

◆ 注:FDMで管理されるFTDは、Firepowerバージョンコードv6.3.0以降からハイアベイラビリ ティに追加できます。

設計オプション

FTDの設計上の観点からは、次の図に示すように直接接続できます。



または、次の図に示すように、レイヤ2(L2)スイッチを介して接続できます。

Primary Unit	-@-	Failover Link	-@-	Secondary Unit
		IPSEC Tunnel		

HA用語

アクティブ	アクティブASAはすべてのトラフィックフローを受信し、すべてのネッ トワークトラフィックをフィルタリングします。設定の変更はアクティ ブASAで行われます。
HAリンク	フェールオーバーペアの2台のユニットは、フェールオーバーリンクを 通じて常に通信し、各ユニットの動作ステータスを判別して、設定変更 を同期します。リンク上で共有される情報は次のとおりです。 ・ ユニット状態(アクティブまたはスタンバイ) ・ Helloメッセージ(キープアライブ) ・ ネットワーク リンク ステータス ・ MACアドレス交換 ・ 設定の複製と同期
プライマリ	これは、通常、HAを作成するときに最初に設定されるユニットです。こ の重要な点は、ASA HAの両方のデバイスがまったく同じ瞬間に起動し た場合、プライマリがアクティブな役割を担うことです。

セカンダリ	これは、HAを作成するときに通常2番目に設定されるユニットです。こ の重要な点は、ASA HAの両方のデバイスがまったく同じ瞬間に起動し た場合、セカンダリがスタンバイロールを引き継ぐことです。
スタンバイ	スタンバイASAはライブトラフィックを処理せず、アクティブデバイス からの接続と設定を同期し、フェールオーバーが発生した場合にアクテ ィブロールを引き継ぎます。
状態リンク	アクティブユニットは、状態リンクを使用して、接続の状態情報をスタ ンバイデバイスに渡します。したがって、スタンバイユニットは特定の タイプの接続を維持でき、ユーザには影響しません。この情報は、フェ ールオーバーが発生したときに存在する接続をスタンバイユニットが維 持するのに役立ちます。注:フェールオーバーとステートフルフェール オーバーに同じリンクを使用すると、インターフェイスを最適に維持で きます。ただし、大規模な設定でトラフィック量の多いネットワークを 使用している場合は、ステートリンクとフェールオーバーリンク用に専 用のインターフェイスを検討する必要があります。ステートフルフェー ルオーバーリンクの帯域幅は、デバイスのデータインターフェイスの最 大帯域幅と一致する必要があることを推奨します。

HA状態

アクティブ	デバイスは現在ネットワーク上のライブトラフィックを処理しており、 実行する必要があるすべての設定変更をこのデバイスで実行する必要が あります。
アプリの同期	この状態のデバイスは、アクティブデバイスの設定を同期します。
一括同期	この状態のデバイスは、アクティブデバイスの設定を同期します。
Disabled	ユニットのフェールオーバーがディセーブルになっている(コマンド :no failover)。
ネゴシエーション	デバイスはアクティブデバイスの可用性をチェックし、アクティブデバ イスがスタンバイ状態でないとアクティブロールを引き継ぎます。
スタンバイ準備完了	現在、デバイスはトラフィックを処理しませんが、アクティブデバイス にヘルスチェックの問題が発生した場合はアクティブロールが引き継が

	れます。
同期の設定	設定は、アクティブデバイスからスタンバイデバイスに複製されます。
コールドスタンバイ	デバイスはフェールオーバー時にアクティブとして引き継ぎますが、接 続イベントは複製しません。

HA状態のフロー図

プライマリ (ピアが接続されていない):



セカンダリ(アクティブ接続ピアあり):



UIの検証

Firepower Management CenterマネージドFTD HA

FTD HAの状態は、次の図に示すように、Device > Device Managementの順に移動するとFMC UIから確認できます。

cisco (Firepower Management Center Overvi	ew Analysis Policies	Devices Obje	ects AMP Intelligence		Deplay Q 💕	🌣 🎯 admin 🔻
View By:	Group					Dej	ployment History
All (2)	Error (0) Warning (0) Offline (0)	Normal (2) Deployment Pe	nding (0) 🔹 L	Jpgrade (0) • Snort 3 (2)		Q Search Device	Add 💌
Collapse Al	1						
	ame	Model	Version	Chassis	Licenses	Access Control Policy	
•	Ungrouped (1)						
0	FTD-HA High Availability						11
	FTD01(Primary, Active) Snort 3 10.197.224.69 - Routed	FTDv for VMware	7.0.0	N/A	Base	Base	:
	FTD02(Secondary, Standby) Snort 3 10,197.224.89 - Routed	FTDv for VMware	7.0.0	N/A	Base	Base	1

FDM管理対象FTD HA

プライマリFDM概要ページ:

alialia cisco.	Firepower Device Manager	त्राय Monitoring	Ø Policies	證王 Objects	Device: FTD01			dmin 🗸
	Model Cisco Firepov	ver Threat Defense f	or VMwa	Software 7.0.0-46	VDB Intrusion Rule Update 338.0 20210203-2335	Cloud Services	High Availability Primary Device: Active 🖉 Peer: Standby	
		C						
			Ci	ico Firepower 1	DV1	MOMT	E (Nit's Server	
		G Inside Netw	ork.				V/USAN/Cathowey	
					ava	CONSIGLE		

セカンダリFDM概要ページ:

	🛈 Th	is device is part of a high avai	lability (HA) pair and To make any	is currently in standby star changes, please log into	te. With few exceptions, y the active unit. Learn Mo	you cannot edit the configuration for this device. ne C
cisco.	Firepower Device Manager	Monitoring Policies	₩E Objects	Device: FTD01		O₂ △ (@) ⑦ ⋮ admin Administrator ~
	Model Cisco Firepower	Threat Defense for VMwa	Software VDB 7.0.0-46 338.0	Intrusion Rule Update 20210203-2335	Cloud Services Connected	High Availability Secondary Device: Standby 🤃 Peer; Active
		C	isco Firepower Threat D	0/1 Defense for VMware ①		DNS Server
		😰 Inside Network	C/I			P/MANUGateway
					connou	Suit Americane
				τ		

ASDMマネージドASA HA

プライマリASAへのASDMホームページ:

100 - 10 - 10 - 10 - 10 - 10 - 10 - 10	Configuration	3		back Oronward	Y Help Type topic	Home				cis
C Dev	vice Dashboard									
Device In	nformation					Interface Status				
Hos ASA ASD Fire Tota	st Name: ciscoasa A Version: 9.12(3) DM Version: 7.12(2) wall Mode: Routed al Flash: 8192 M	Ceneral 2 4	License Virtual Resou Device Uptime: 30 Device Type: A5 Number of vCPUs: 8 Total Memory: 83	rces Id 20h 36m 28s Av 92 M8		Interface backup inside management outside	IP Addres/Mask 109.106.53.100/24 10.106.60.55/24 10.106.47.62/24 10.106.48.65/24	Line O up O up O up O up	Unk Oup Oup Oup	Kbps 3 1 5 1
						Select an interface b	o view input and output k	lops		
PN Sum	nmary				Details	Failover Status				Details
IPsec U	U Clientiess	SL VPN: U	AnyConnect Client(SSL		SCREWILZ.	This Host PRIMAP	(Active)	Other Host: SECON	DART (Standby Ready)	Sector 1
ystem R	Resources Status					Traffic Status				
Memory	/ Usage (MB)					2-				Å
1977ME	5000 5000 4000 2000					02-36 UDP: 0 backup 'backup' interface'	02:37 TCP: 0 Total: 0	02'38	62.39	02:40 ©
1977MB 02:40:41	7000 6000 4000 2000 1000 0 02.36	02.37	02'38	02'39	02.40	UDP: 0	02:37 TCP: 0 Total: 0 Traffic Usage (Kbps) 02:37 3 Output Kbps: 0	02'18 02'18	02'39 02'39 02'39	02:40
1977ME	7000 6000 5000 2000 0 02.36	02-37	02'38	02'39	02.40 Latest ASDM	UDP: 0 UD	02:37 TCP: 0 Total: 0 Traffic Usage (Kbps) 02:37 3 Output Kbps: 0	02'18 02'18	02'39 02'39 02'39	02:40

セカンダリASAへのASDMホームページ:

0 0	Home
evice Information	Interface Status
General License Virtual Resources Host Name: clscoasa ASA Version: 9.12(3)12 Device Uptime: 30d 20h 39m 10s ASDW Version: 7.12(2)14 Device Type: ASAv Firewall Mode: Routed Number of VCPUs: 8 Total Flash: 8192 MB Total Memory: 8192 MB	Interface IP Address/Mask Line Link Kbps backup no ip address 0 up 0 up 2 inside no ip address 0 up 0 up 1 management 10.106.47.64/24 0 up 0 up \$\$9 outside no ip address 0 up 0 up \$\$9
	Select an interface to view input and output Kbps
PN Summary	Fallover Status
IPsec 0 Clientless SSL VPN: 0 AnyConnect Client(SSL,TLS,DTLS): 0 Details	This Host: SECONDARY (Standby Ready) Other Host: PRIMARY (Active)
Total Memory Usage Total CPU Usage Core Usage Details Memory Usage 000<	Connections Per Second Usage 3 2 1 0 02:29 02:40 02:41 02:42 02:43 02:44 02:45 02:46 02:47 02:48 02:49 02:40 02:41 02:42 02:43 02:44 02:45 02:40 02:41 02:42 02:43 02:44 02:45 02:46 02:47 02:48 02:49 02:49 02:40 02:41 02:42 02:43 02:44 02:45 02:47 02:48 02:49 02:49 02:40 02:41 02:42 02:43 02:44
224322 0 ¹ 0239 0240 0241 0242 0243 O O Latest 4	02.29 02.40 02.43 02.42 02.43 Input Kbps: 2 OUtput Kbps: 0
O O Latest / ASDM logging is disabled.To enable ASDM logging is disabled.To enableASDM logging is disabled.To enable A	ISDM Syslog Messages ogging with informational level, click the button below. sable Logging

FTD/ASA HAを実行する4100/9300用Firepowerシャーシマネージャ

プライマリFCM論理デバイスページ:

Overviev	Interfaces	Logical Devices	Security Engine	Platform Setting	IS				System Tools Help admin
Logical De	vice List	1			(1 instances) 0% (0 of 70) Cores Av	allable			C Refresh O Add +
ASA			Standalone	Status:ok					1
Appli	cation	Version	Res	ource Profile	Management IP	Gateway	Management Port	Status	
[™] ASA		9.12.4.16			10.197.216.7	10.197.216.1	Ethernet1/7	Online	
	Interface Name Ethernet1/1 Ethernet1/2 Ethernet1/3 Ethernet1/4 Ethernet1/4 Ethernet1/6 Ethernet1/8 Ethernet3/8 Ethernet3/8				Type data data data data data data data dat	Attri NU NU NU	Butes User Operational Status : not-applicable ALING-UNTF : Ethernet3/7 ALING-UNTF : Ethernet3/7 ALING-UNTF : Ethernet3/7 ALING : active		

セカンダリFCM論理デバイスページ:

Overview	Interfaces	Logical Devices	Security Engine	Platform Settings	k)				System Tools Help admin
Logical Dev	ice List	t			(1 instances) 0% (0 of 70) Cores Ava	liable			C Rotrosh 🔘 Add •
ASA			Standalone	Statustok					2 I
Applic	ation	Version	Reso	urce Profile	Management IP	Gateway	Management Port	Status	
[™] ASA		9.12.4.18			10.197.216.8	10.197.216.1	Ethernet1/7	Online	Carlo Me Carla
	Interface Name Ethernet1/1 Ethernet1/2 Ethernet1/2 Ethernet1/2 Ethernet1/3 Ethernet1/3 Ethernet1/5 Ethernet1/6 Ethernet1/6 Ethernet3/7 Ethernet3/7 Ethernet3/7				Type dota data data data data data data data	ALLAN Chi HAA HAA HAA	butes ster Operational Status : not-applicable -UNC-INTF : Ethernet3/7 -UNC-INTF : Ethernet3/7 -ROLE : standby		

CLIの確認

<#root>

>

show running-config failover

failover
failover lan unit secondary
failover lan interface failover-link GigabitEthernet0/2
failover replication http
failover link failover-link GigabitEthernet0/2
failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89

ここで考慮すべき重要なポイントは次のとおりです。

フェールオーバー failover lan unit secondary —>ユニットがプライマリかセカンダリか failover lan interface failover-link GigabitEthernet0/2 —>デバイスのフェールオーバーリンク物理 インターフェイス 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failover-link GigabitEthernet0/2 failover interface ip failover-link 10.10.69.49 255.255.255.0 standby 10.10.69.89 —>プライマリお よびスタンバイデバイスフェールオーバーリンクのipアドレス。

<#root>

>

show failover

Failover On Failover unit Secondary Failover LAN Interface: failover-link GigabitEthernetO/2 (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 311 maximum MAC Address Move Notification Interval not set failover replication http Version: Ours 9.16(0)26, Mate 9.16(0)26 Serial Number: Ours 9A1JSSKW48J, Mate 9ABR3HWFG12 Last Failover at: 01:18:19 UTC Nov 25 2021 This host: Secondary - Standby Ready Active time: 0 (sec) slot 0: ASAv hw/sw rev (/9.16(0)26) status (Up Sys) Interface outside (0.0.0.0): Normal (Not-Monitored) Interface inside (192.168.45.2): Normal (Not-Monitored) Interface diagnostic (0.0.0.0): Normal (Not-Monitored) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up) Other host: Primary - Active Active time: 707216 (sec) Interface outside (0.0.0.0): Normal (Not-Monitored) Interface inside (192.168.45.1): Normal (Not-Monitored) Interface diagnostic (0.0.0.0): Normal (Not-Monitored) slot 1: snort rev (1.0) status (up) slot 2: diskstatus rev (1.0) status (up) Stateful Failover Logical Update Statistics Link : failover-link GigabitEthernet0/2 (up) Stateful Obj xmit xerr rcv rerr General sys cmd up time RPC services TCP conn UDP conn ARP tbl Xlate_Timeout IPv6 ND tbl VPN IKEv1 SA VPN IKEv1 P2 VPN IKEv2 SA VPN IKEv2 P2 VPN CTCP upd VPN SDI upd VPN DHCP upd SIP Session SIP Tx SIP Pinhole Route Session Router ID User-Identity CTS SGTNAME CTS PAC TrustSec-SXP IPv6 Route STS Table Rule DB B-Sync Rule DB P-Sync Rule DB Delete Logical Update Queue Information Cur Max Total Recv Q: 0

Xmit Q: 0

Failover On:フェールオーバーは有効または無効です。

このホスト:セカンダリ – Standby Ready このデバイスの役割とインターフェイスの状態。

その他のホスト:プライマリ – アクティブ。 もう1つのデバイスはアクティブ状態で、現在のデ バイスと通信します。

<#root>

>

show failover history

From State	To State	Reason	
01:18:14 UTC Nov 25 2021 Not Detected	Negotiation	No Error	
01:18:27 UTC Nov 25 2021 Negotiation	Just Active	No Active unit foun	d
01:18:27 UTC Nov 25 2021 Just Active	Active Drain	No Active unit foun	d
01:18:27 UTC Nov 25 2021 Active Drain	Active Applying Config	No Active unit foun	d
01:18:27 UTC Nov 25 2021 Active Applying Config	Active Config Applied	No Active unit foun	d
01:18:27 UTC Nov 25 2021 Active Config Applied	Active	No Active unit foun	d

デバイスの過去の状態と、それらの状態変更の理由を確認するには、次のコマンドを使用します。

<#root>

>

show failover state

State	Last Failure Reason	Date/Time			
This host - Secondary					
Standby Ready	None				
Other host - Primary					
Active	None				
====Configuration State===					
Sync Done - STANDBY					
====Communication State===					

デバイスの現在の状態と最後のフェールオーバーの理由を確認します。

フィールド	説明
設定状態	設定同期の状態を表示します。 スタンバイユニットで可能な設定状態: ・ Config Syncing - STANDBY:同期された設定の実行中に設定されます。 ・ インターフェイス設定の同期 – スタンバイ ・ Sync Done - STANDBY:スタンバイユニットがアクティブユニットからの設 定同期を完了したときに設定されます。 アクティブユニットで可能な設定状態: ・ Config Syncing:スタンバイユニットに対して設定の同期を実行するときに、 アクティブユニットに設定されます。 ・ インターフェイス設定の同期 ・ Sync Done:アクティブユニットがスタンバイユニットへの設定の同期を正 常に完了した時点を設定します。 ・ Ready for Config Sync:スタンバイユニットが設定同期を受信する準備がで きたことを通知したときに、アクティブユニットに設定されます。
通信状態	MACアドレスの同期のステータスを表示します。 ・ Mac set:MACアドレスは、ピアユニットからこのユニットに同期されていま す。 ・ Updated Mac:MACアドレスが更新され、他のユニットと同期する必要がある 場合に使用します。また、ユニットがピアユニットから同期されたローカル MACアドレスを更新する移行時にも使用されます。
日付/時刻	失敗の日付とタイムスタンプが表示されます。
最後の失敗 の理由	最後に報告された障害の理由が表示されます。この情報は、障害状態がクリアされ てもクリアされません。この情報は、フェールオーバーが発生した場合にのみ変更 されます。

フィールド	説明
	考えられる障害の原因: ・ Interface Failure:フェールオーバー条件を満たしていて、フェールオーバー が発生したインターフェイスの数。 ・ Comm Failure:フェールオーバーリンクで障害が発生したか、ピアがダウン しています。 ・ バックプレーンの障害
都道府県	ユニットのプライマリ/セカンダリおよびアクティブ/スタンバイのステータスを表 示します。
このホスト /その他のホ スト	このホストは、コマンドが実行されたデバイスの情報を示します。別のホストは、 フェールオーバーペアの他のデバイスの情報を示します。

٦

<#root>

>

show failover descriptor

outside send: 00020000ffff0000 receive: 00020000ffff0000 inside send: 00020100ffff0000 receive: 00020100ffff0000 diagnostic send: 01020000ffff0000 receive: 01020000ffff0000

トラブルシュート

デバッグ

<#root>

>

debug fover ?

cableFailover LAN statuscmd-execFailover EXEC command executionfailFailover internal exceptionfmsgFailover messageifcNetwork interface status traceopenFailover device open

rx	Failover Message receive
rxdmp	Failover recv message dump (serial console only)
rxip	IP network failover packet recv
snort	Failover NGFW mode snort processing
switch	Failover Switching status
sync	Failover config/command replication
tx	Failover Message xmit
txdmp	Failover xmit message dump (serial console only)
txip	IP network failover packet xmit
verify	Failover message verify

キャプチャ :

フェールオーバーインターフェイスのキャプチャ:

このキャプチャを参照すると、フェールオーバーhelloパケットが送信された速度でフェールオー バーリンクに送信されているかどうかを確認できます。

<#root>

>

show capture

capture capfail type raw-data interface Failover [Capturing - 452080 bytes]
match ip host 10.197.200.69 host 10.197.200.89
>

show capture capfail

15 packets captured

```
1: 09:53:18.506611 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
2: 09:53:18.506687 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
3: 09:53:18.813800 10.197.200.89 > 10.197.200.69 ip-proto-105, length 46
4: 09:53:18.814121 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
5: 09:53:18.814151 10.197.200.69 > 10.197.200.89 ip-proto-105, length 62
6: 09:53:18.815143 10.197.200.89 > 10.197.200.69 ip-proto-105, length 62
7: 09:53:18.815158 10.197.200.89 > 10.197.200.69 ip-proto-105, length 50
8: 09:53:18.815372 10.197.200.69 > 10.197.200.89 ip-proto-105, length 50
9: 09:53:19.514530 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
10: 09:53:19.514972 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
11: 09:53:19.718041 10.197.200.69 > 10.197.200.89 ip-proto-9, length 70
12: 09:53:20.533084 10.197.200.69 > 10.197.200.89 ip-proto-105, length 54
13: 09:53:20.533999 10.197.200.89 > 10.197.200.69 ip-proto-105, length 54
14: 09:53:20.686625 10.197.200.89 > 10.197.200.69 ip-proto-9, length 74
15: 09:53:20.686732 10.197.200.69 > 10.197.200.89 ip-proto-9, length 74
15 packets shown
```

フェールオーバーリンクでのARPキャプチャ:

このキャプチャを取得して、ピアのARPテーブルにMacエントリが含まれているかどうかを確認 できます。

<#root>

>

show capture

capture caparp type raw-data ethernet-type arp interface Failover [Capturing - 1492 bytes] >

show capture caparp

22 packets captured

```
1: 11:02:38.235873 arp who-has 10.197.200.69 tell 10.197.200.89
2: 11:02:38.235934 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
3: 11:03:47.228793 arp who-has 10.197.200.69 tell 10.197.200.89
4: 11:03:47.228870 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
5: 11:08:52.231296 arp who-has 10.197.200.69 tell 10.197.200.89
6: 11:08:52.231387 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
7: 11:32:49.134163 arp who-has 0.0.0.0 (ff:ff:ff:ff:ff:ff) tell 0.0.0.0 (0:0:0:0:0:0)
8: 11:32:50.226443 arp who-has 10.197.200.1 tell 10.197.200.28
9: 11:42:17.220081 arp who-has 10.197.200.89 tell 10.197.200.69
10: 11:42:17.221652 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
11: 11:42:20.224124 arp who-has 10.197.200.89 tell 10.197.200.69
12: 11:42:20.225726 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
13: 11:42:25.288849 arp who-has 10.197.200.69 tell 10.197.200.89
14: 11:42:25.288956 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
15: 11:46:17.219638 arp who-has 10.197.200.89 tell 10.197.200.69
16: 11:46:17.220295 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
17: 11:47:08.135857 arp who-has 10.197.200.69 tell 10.197.200.89
18: 11:47:08.135994 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
19: 11:47:11.142418 arp who-has 10.197.200.89 tell 10.197.200.69
20: 11:47:11.143150 arp reply 10.197.200.89 is-at 0:50:56:a0:72:4d
21: 11:47:18.213993 arp who-has 10.197.200.69 tell 10.197.200.89
22: 11:47:18.214084 arp reply 10.197.200.69 is-at 0:50:56:a0:85:6c
22 packets shown
```

/

シナリオ

アクティブユニットから変更を展開する際に、ピアユニットがHAグループへの参加に失敗したり 失敗したりする場合は、失敗したユニットにログインし、High Availabilityページに移動して、 Failover Historyリンクをクリックします。

アプリ同期エラー

show failover historyの出力にアプリケーション同期の失敗が示されている場合、HA検証フェーズ

の時点で問題が発生しています。このフェーズでは、ユニットが高可用性グループとして正しく 機能できるかどうかをシステムがチェックします。

「From State is App Sync」というメッセージが表示され、ノードが「Standby Ready」状態に移 行すると、「All validation passed」というメッセージが表示されます。

検証が失敗すると、ピアは無効(失敗)状態に移行します。問題を解決して、ピアをハイアベイ ラビリティグループとして再度機能させます。

App Syncエラーを修正してアクティブユニットに変更を加えた場合は、それらを展開してから、 ピアノードが参加できるようにHAを再開する必要があることに注意してください。

このメッセージは、問題の解決方法を説明するエラーを示します。これらのエラーは、ノードの 参加と、その後の各展開で発生する可能性があります。

ノードの参加時に、アクティブユニットに最後に展開されたコンフィギュレーションに対してチェックが実行されます。

スタンバイノードが「CD App Sync error is App Config Apply Failed」でHAに参加できない

スタンバイFTDコマンドラインで、/ngfw/var/log/action_queue.logに設定エラーの理由が設定され ている必要があります。 修復:設定エラーを特定し、必要な変更を行った後に、HAを再開できます。 Cisco Bug IDCSCvu15611を参照してください。

<#root>

From State	To State	Reason			
15:10:16 CDT Sep 28 2021					
Not Detected	Disabled	No Error			
15:10:18 CDT Sep 28 2021					
Disabled	Negotiation	Set by the config command			
15:10:24 CDT Sep 28 2021					
Negotiation	Cold Standby	Detected an Active mate			
15:10:25 CDT Sep 28 2021					
Cold Standby	App Sync	Detected an Active mate			
15:10:55 CDT Sep 28 2021					
App Sync	Disabled				
CD App Sync error is App Config Apply Failed					

スタンバイノードが「APP SYNC timeoutが原因でHA状態の進行が失敗した」というメッセージ でHAに参加できない スタンバイFTDコマンドラインで、/ngfw/var/log/ngfwmanager.logにapp-sync timeoutの理由が設 定されている必要があります。

この段階では、アクティブユニットがアプリケーションの同期がまだ進行中であると認識してい るため、ポリシーの展開も失敗します。

ポリシーの導入により、「newNode join/AppSyncプロセスが進行中であるため、設定の変更は許 可されず、導入要求が拒否されます。しばらくしてから展開を再試行してください。」

修復:スタンバイノードでハイアベイラビリティを再開すると、問題が解決する場合があります 。

Cisco Bug ID <u>CSCvt48941</u>を参照してください。 Cisco Bug ID <u>CSCvx11636</u>を参照してください。

<#root>

From State	To State	Reason			
19:07:01 EST MAY 31 2021					
Not Detected	Disabled	No Error			
19:07:04 EST MAY 31 2021					
Disabled	Negotiation	Set by the config command			
19:07:06 EST MAY 31 2021	-				
Negotiation	Cold Standby	Detected an Active mate			
19:07:07 EST MAY 31 2021					
Cold Standby	App Sync	Detected an Active mate			
21:11:18 EST Jun 30 2021					
App Sync	Disabled				
A state progression failed due to APP SYNC timeout					

スタンバイノードが「CD App Sync error is Failed to apply SSP config on standby」でHAに参加 できない

スタンバイFTDコマンドラインで、/ngfw/var/log/ngfwmanager.logに障害の正確な理由が示されている必要があります。

修復:スタンバイノードでハイアベイラビリティを再開すると、問題が解決する場合があります 。

Cisco Bug IDを参照 <u>CSCvy04965</u>

<#root>

From StateTo StateReason04:15:15 UTC Apr 17 2021DisabledNo Error04:15:24 UTC Apr 17 2021Vo Error

Disabled	Negotiation	Set by the config command
04:16:12 UTC Apr 17 2021		
Negotiation	Cold Standby	Detected an Active mate
04:16:13 UTC Apr 17 2021		
Cold Standby	App Sync	Detected an Active mate
04:17:44 UTC Apr 17 2021		
App Sync	Disabled	
CD App Sync error is Failed	d to apply SSP config on sta	andby

ヘルスチェックの失敗

「HELLO not heard from mate」とは、相手がオフラインであるか、フェールオーバーリンクが HELLOキープアライブメッセージを通信していないことを意味します。

もう一方のデバイスにログインしてみます。SSHが機能しない場合は、コンソールアクセスを取得し、デバイスが動作しているかオフラインであるかを確認します。

動作している場合は、show failover stateコマンドを使用して障害の原因を特定します。

正常に動作しない場合は、グレースフルリブートを実行して、コンソールにブートログが表示されるかどうかを確認します。表示されない場合は、デバイスにハードウェア障害がある可能性があります。

<#root>

From State	To State	Reason
04:53:36 UTC Feb 6 2021 Failed	Standby Ready	
Interface check		
02:12:46 UTC Jul 11 2021		
Standby Ready 02:12:46 UTC Jul 11 2021	JUST ACTIVE	HELLU not neard from mate
Active Config Applied	Active	HELLO not heard from mate

Snortのダウンまたはディスク障害

FTDで「Detect Inspection engine failure due to disk failure」というエラーが表示される場合は、 2つの可能性があります。

検出エンジン(SNORTインスタンス)がダウンしている

これは、Linux側でコマンドpmtool statusを使用して検証できます。 | grep -i de,

修復:いずれかのインスタンスがダウンしている場合は、/ngfw/var/log/messagesを確認して原因 を特定します。

デバイスのディスク使用率が高い

これは、Linux側でコマンドdf-Thを使用して検証できます。

修復:ディスクの大半を消費しているディレクトリを特定し、TACに連絡して不要なファイルを 削除してください。

<#root>

From State	To State	Reason
Active Config Applied 16:07:18 UTC Dec 5 2020	Active	No Active unit found
Active 16:07:20 UTC Dec 5 2020	Standby Ready	Other unit wants me Standby
Standby Ready	Failed	
Detect Inspection engine	failure due to disk failure	
16:07:29 UTC Dec 5 2020 Failed	Standby Ready	My Inspection engine is as good as peer due to d

サービスカードの障害

このような問題は、通常、ASA 5500-XデバイスのFirepowerモジュールの障害が原因で報告され ます。show module sfr detailsを使用して、モジュールの健全性を確認してください。

修復:障害発生時にASA Syslogを収集します。これには、コントロールプレーンやデータプレーンの障害などの詳細が含まれる場合があります。

これは、SFRモジュールのさまざまな理由が原因である可能性があります。TACを開いてIPSの この問題の根本原因を見つけることを推奨します。

<#root>

From State	To State	Reason		
21:48:19 CDT Aug 1 2021				
Active 21:48:19 CDT Aug 1 2021	Standby Ready	Set by the config command		
Standby Ready	Just Active			
ervice card in other unit has failed				

MIOハートビート障害

Firepower脅威対策/ASAは、FPR1K、2K、4K、9Kで「MIOブレードのハートビート障害」による 障害を報告します。

Cisco Bug IDを参照 <u>CSCvy14484</u> Cisco Bug IDを参照 <u>CSCvh26447</u>

<#root>

To State	Reason
Active	No Active unit found
Failed	
2	
Negotiation	MIO-blade heartbeat reco
	To State Active Failed P Negotiation

関連情報

- <u>https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/S/asa-command-ref-S/show-f-to-show-ipu-commands.html</u>
- <u>https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-ha.html#id_72185</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。