

Secure Firewall 7.6 FTD HAアップグレード障害の軽減

内容

[はじめに](#)

[背景説明](#)

[問題](#)

[最新情報 \(ソリューション\)](#)

[前提条件](#)

[対応プラットフォーム](#)

[機能の概要](#)

[FTD HAの新しいアップグレードワークフロー](#)

[スタンバイユニットが最初にアップグレードされる](#)

[1台目のユニットのアップグレード \(スタンバイユニット\)](#)

[2台目のユニットのアップグレード \(アクティブユニット\)](#)

[HAアドバンストラブルシュート](#)

[HAアドバンストラブルシュートレポート](#)

[HA検証エラーの例](#)

[正常なHA検証の例](#)

[HAアドバンストラブルシュートの内容](#)

[HAアドバンストラブルシュートファイルの場所](#)

[HAアドバンストラブルシューティングの生成に関するヒント](#)

[HAアドバンストラブルシューティングでのリターンステータスとアクション](#)

[エラーコードと分類](#)

[ユーザの介入メッセージ](#)

[TAC介入メッセージ](#)

[ファイアウォール管理センターUIの変更](#)

[ソフトウェア アーキテクチャ](#)

[FAQ](#)

はじめに

このドキュメントでは、特にハイアベイラビリティ(HA)環境での、バージョン7.0から7.2へのFTDアップグレード障害に対処するためのトラブルシューティングについて説明します。

背景説明

これらの障害の半数以上は200_enable_maintenance_modeフェーズの問題に起因しており、既存のHA検証では主に基本的なアクティブ/スタンバイ状態のチェックが実行されますが、これは包括的なHA移行には不十分です。

Secure Firewall 7.6のアップデートでは、これらの問題に対処するために改善されたHA検証が導入されました。これらの機能拡張には、HA状態の遷移に対する徹底的なチェック、同期プロセスのタイムアウトの延長、および拡張されたエラー報告が含まれます。このアップデートの目的は、アップグレード後のHAの問題と全体的なアップグレードの失敗を大幅に減らし、HA導入のアップグレードプロセスをよりスムーズで信頼性の高いものにすることです。

移行元：<https://confluence-eng-rtp2.cisco.com/conf/display/IFT/FTD+HA+Upgrade+Failure+Reduction>

問題

- HA展開では、7.0、7.1、および7.2リリースにわたって、お客様から多数のFTDアップグレード障害が報告されています。
- 障害の50 %以上がFTD HAの導入によるものです。200_enable_maintenance_modeの障害は、HA障害の一因となります。
- 既存のHA状態の検証は、アクティブ/スタンバイ状態のチェックなどの基本的な検証であり、HA移行を完全に検証するものではありません。

最新情報 (ソリューション)

FTDアップグレードのHA検証の改善：

- HA状態遷移の検証
- config sync (7200秒)、app sync (1200秒)、bulk sync (7200秒) などのHA移行状態のFTD HAアップグレードタイムアウトの改善
- FTDアップグレードの開始または失敗のタイミングをFMCにより詳細に制御できるようにする
- FTD HAアップグレードのエラーレポートおよびリカバリメッセージの改善

以前のリリースと比較して、次の機能があります。

- HA検証の改善により、HA導入におけるアップグレード後のHA作成の問題を軽減
- 検証の改善により、FTDアップグレードの失敗を削減

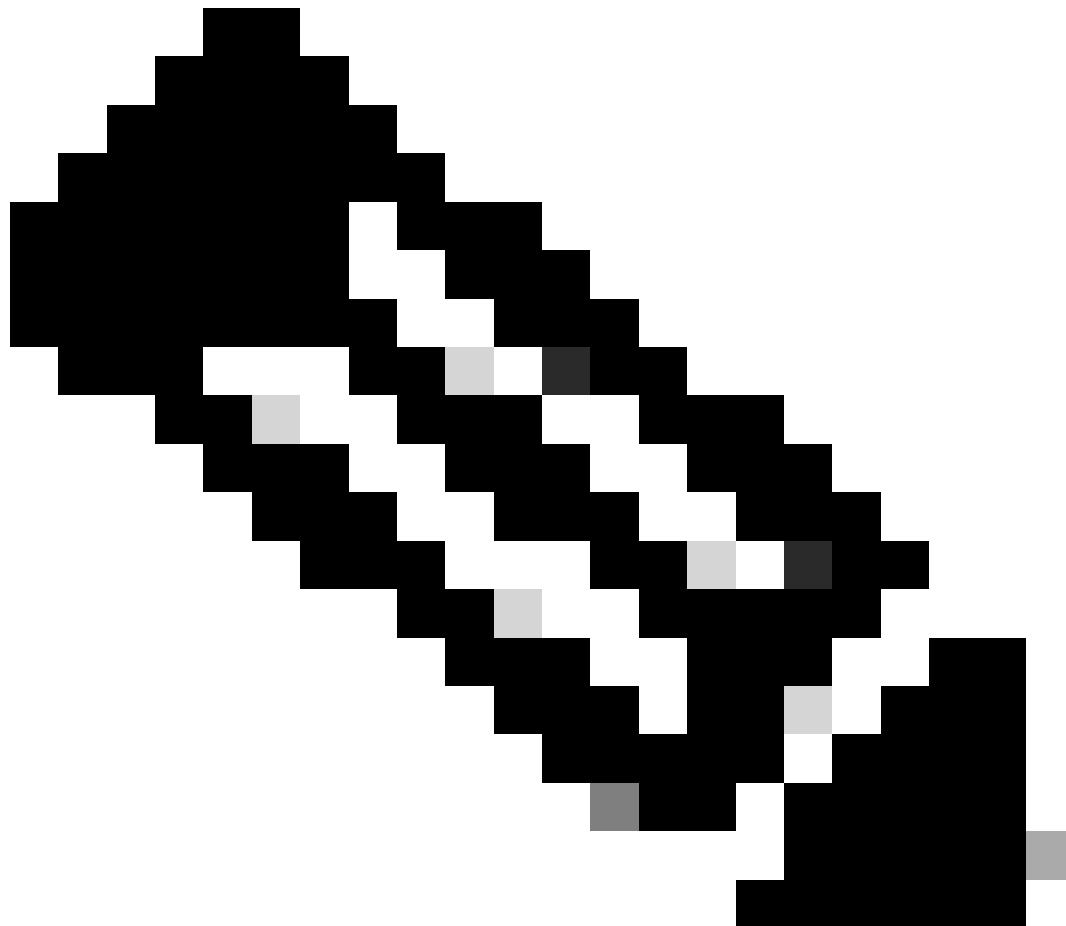
前提条件

対応プラットフォーム

- マネージャおよびバージョン：FMC 7.6.0
- アプリケーション(ASA/FTD)およびアプリケーションの最小バージョン：FTD 7.6.0、FMC

7.6.0 FTD HAの管理

- サポート対象プラットフォーム：FTD HAを実行するすべてのプラットフォーム
-



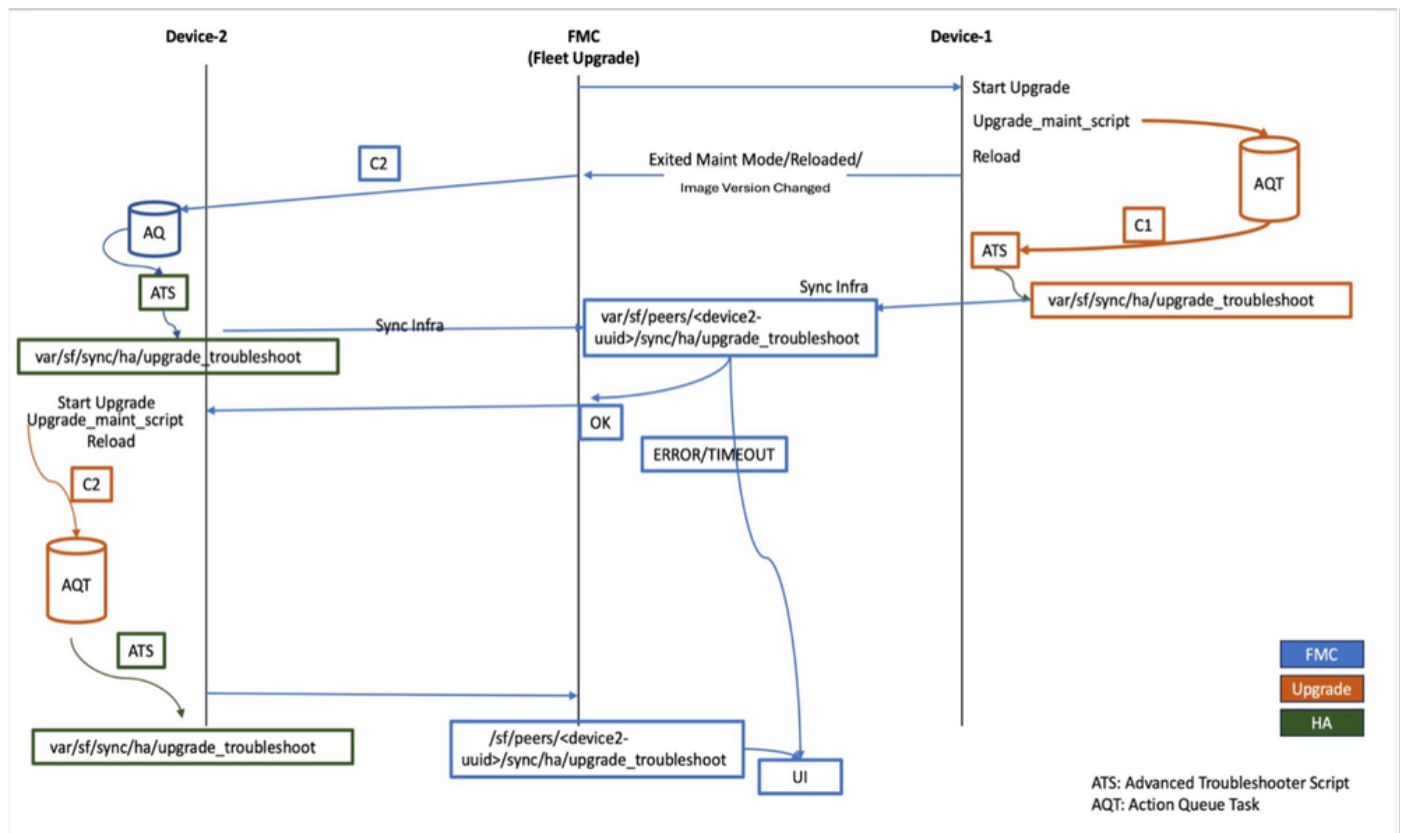
注：この機能は、FMCで管理されるFTD HA展開にのみ適用されます。この機能は、FDMで管理されるFTD HAまたはクラスタ化されたデバイスには適用されません。

機能の概要

- この機能は、アップグレードプロセスのリポート部分の後にFMCによってアップグレードされたユニットのHA状態をチェックすることによって、HA展開でのFTDアップグレードの失敗を減らすのに役立ちます。
- アップグレードのリポート後、FMCはアクティブ/スタンバイ状態およびHA同期の障害をチェックします。
- FTDは、新しいHAアドバンストラブルシュートの形式で、2番目のノードのアップグレードをいつ開始または失敗するかをFMCに通知します。

- アップグレード後のリポートでHAへの参加に失敗した場合は、FMCのUIに適切なメッセージが表示されます。

FTD HAの新しいアップグレードワークフロー



スタンバイユニットが最初にアップグレードされる

1台目のユニットのアップグレード (スタンバイユニット)

- 最初のユニットアップグレード中に、アップグレードスクリプトはaction_queueタスクを開始して、999_finish段階でHAアドバンストラブルシューティングデータを収集します。
- 挿入されたタスク実行は、アップグレード後の再起動後に開始され、JSONファイルの形式でトラブルシューティング情報を収集します。
- 同じJSONファイルがFMCに同期されます。
- 最初のノードがメンテナンスモードから抜けると、HAアドバンストラブルシューティングを収集するために、FMCによってアクティブユニットでリモートaction_queueタスクがトリガーされます (アクティブユニットは7.6以上である必要があります)。アクティブユニットが7.6より前であることが検出された場合、アクティブユニットからはトラブルシューティングは収集されず、スタンバイユニットから収集されたトラブルシューティングのみに基づいてFMCが判断を行います。

両方のユニットからHAアドバンストラブルシューティングが収集されると、FMCは、アップグレードを開始するか、2番目のノード (アクティブユニット) でアップグレードをブロックするかを決定します。

2台目のユニットのアップグレード (アクティブユニット)

- スタンバイユニットと同様に、アップグレードスクリプトは999_finish段階でHAアドバンストラブルシューティングを収集するためのaction_queueタスクを開始します。
- 挿入されたタスクの実行は、アップグレード後の再起動のみを開始し、JSONファイルの形式でトラブルシューティング情報を生成します。
- 同じファイルがFMCに同期されます。
- いずれかのユニットでHA障害が報告された場合は、FMCのUIのアップグレードタブにHA障害データが表示されます。
- アップグレード後のリブートでHAへの参加に失敗した場合、アップグレードは完了とマークされ、同じアップグレードタブでHA検証の失敗が報告されます。

HAアドバンストラブルシューティング

- HAアドバンストラブルシューティングは、この機能の一部として導入された新しい単一のJSONファイルで、HA情報が含まれています。アップグレード後のリブート後に生成され、FTDからFMCに送信されます。
- ファイル名とパス : /ngfw/var/sf/sync/ha/upgrade_troubleshoot
- FMCが最初の (スタンバイ) ユニットからHAアドバンストラブルシューティングを収集するとすぐに、FMCはリモートタスクをトリガーしてアクティブユニットから同じ情報を収集します。
 - このリモートデータ収集は、デバイスが7.6以降を実行している場合にのみサポートされます。
 - 7.6より前のバージョンを実行しているデバイスが見つかった場合、リモートデータ収集はスキップされます。そのため、この場合、FMCはスタンバイユニットからデータを収集し、次のアクションを決定するだけです。
- HAの高度なトラブルシューティングの生成は迅速です。Linaがダウンしてレポートの生成に失敗した場合、ただちに終了します。
 - デバイスのリブート時間はプラットフォームによって異なり、リブート時間は各プラットフォームで説明した時間と同じです。

HAアドバンストラブルシューティングレポート

各HAユニットは、アップグレード後のリブートでJSONファイル形式のHAアドバンストラブルシューティングデータを生成し、FMCと共有します。失敗と成功が発生した場合の検証例を次に示します。

HA検証エラーの例

ファイル : /ngfw/var/sf/sync/ha/upgrade_troubleshoot

```
{
"failover_lan" : "NA",
"error_code" : "1046 -
```

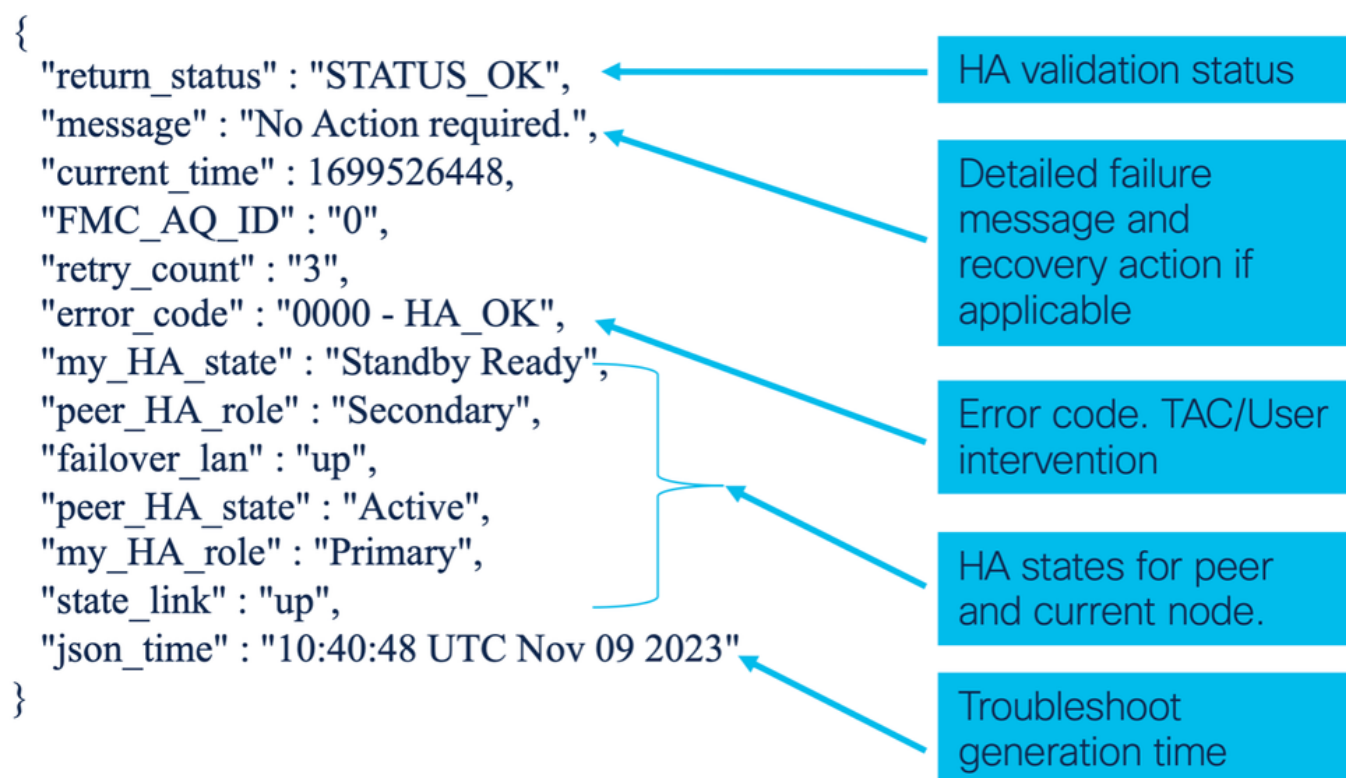
```
STARTUP_FAILOVER_CONFIG_NOT_PRESENT",
"current_time" : 1701369637,
"peer_HA_state" : "Not Detected",
"FMC_AQ_ID" : "0",
"state_link" : "NA",
"json_time" : "18:40:37 UTC Nov 30 2023",
"my_HA_state" : "Disabled",
"my_HA_role" : "Secondary",
"return_status" : "STATUS_ERROR",
"message" : "Failover config is not present on the startup
config. Device is in standalone state. Please configure failover.",
"peer_HA_role" : "Primary"
}
```

正常なHA検証の例

ファイル : /ngfw/var/sf/sync/ha/upgrade_troubleshoot

```
{
"return_status" : "STATUS_OK",
"message" : "No Action required.",
"current_time" : 1699526448,
"my_HA_state" : "Standby Ready",
"FMC_AQ_ID" : "0",
"retry_count" : "3",
"error_code" : "0000 - HA_OK",
"peer_HA_role" : "Secondary",
"failover_lan" : "up",
"peer_HA_state" : "Active",
"my_HA_role" : "Primary",
"state_link" : "up",
"json_time" : "10:40:48 UTC Nov 09 2
}
```

HAアドバンストラブルシュートの内容



HAアドバンストラブルシューティングファイルの場所

HAアドバンストラブルシューティングJSONファイルの場所：

On FTD: `/ngfw/var/sf/sync/ha/upgrade_troubleshoot`
On FMC: `/var/sf/peers/`

`/sync/ha/upgrade_troubleshoot`

- HAのトラブルシューティングはlinaコマンドに依存します。
 - トラブルシューティングで`/ngfw/var/sf/sync/ha/upgrade_troubleshoot`での生成に失敗した場合は、`/ngfw/var/log/ha_upgrade_troubleshoot.log`でログを参照できます。
- `/ngfw/var/sf/sync/ha/upgrade_troubleshoot`および`/ngfw/var/log/ha_upgrade_troubleshoot.log`ファイルは、FTDトラブルシューティングファイルの一部です。

HAアドバンストラブルシューティングの生成に関するヒント

システム状態が原因でHAアドバンストラブルシューティングが生成されない場合があります、その理由は回線ダウンまたはアップグレード後のアクションキュープロセスのダウンである可能性があります。

ります。回線またはアクションキューがダウンしている場合、これは問題です。

このような場合は、エキスパートモードで次のコマンドを使用して、linaおよびActionQueueプロセスが実行されているかどうかを確認してください。

<#root>

pmtool status | grep lina

lina (system) - Running 5503 * Indicates Lina is up and running

pmtool status | grep ActionQueueScrape

ActionQueueScrape (system) - Running 5268 * Indicates action queue is up and

HAアドバンストラブルシューティングでのリターンステータスとアクション

- STATUS_INIT：これは、HAのトラブルシューティングがトリガーされたことを示します。
- STATUS_OK：デバイスは安定した状態です。必要な操作はありません。
- STATUS_ERROR：これにより、HAが形成されていないためにエラーが発生したことがわかります。表示されたメッセージに基づいてアクションを実行するか、TACに問い合わせる必要があります。
- STATUS_RETRY：デバイスは中間状態のいずれかになります。HAのトラブルシューティングは、状態に基づく固定間隔の後、STATUS_ERRORまたはSTATUS_OKが発生するまで再試行を続けます。
 - STATUS_ERRORが発生した障害に基づいて、HA障害は次の2つのケースに分類されます。
 - ユーザによる介入：これらのHA障害はユーザが修正でき、ユーザはアップグレードを再開できます。TACによる介入は必要ありません。
 - TACによる介入：これらのHA障害では、ユーザが自分で修正することはできません。TACによる介入が必要です。

エラーコードと分類

エラーコードに基づいて、エラーは次のように分類されます。

return_statusを返します。	error_code (エラー・コード)	説明	再試行または回復メカニズム
ステータス_OK	「0000 - HA_OK」 (予約済み値は0001 ~	これは成功シナリオ用です。 (HA状態が	(該当なし)

	1023です)	ActiveおよびStandby Readyの場合)	
ステータス_エラー	「1024:2047 - ERROR_REASON」	エラーシナリオ(ユーザの介入)の場合は、次のようにします	ユーザおよびアップグレードフレームワークに表示されるアクション可能なメッセージにより、将来 (存在する場合) 再試行または回復メカニズムが追加される可能性があります。 。
ステータス_エラー	「2048:3071 - ERROR_REASON」	エラーシナリオ (TAC介入) 用です。	回復にはTACの介入が必要です。

ユーザの介入メッセージ

エラー	エラー メッセージ	エラー コード
「FAILOVER_CONFIG_NOT_PRSENT」	「Failover config is not present on the device (デバイスにフェールオーバー設定がありません) 」	"1024"
'FAILOVER_IS_NOT_ENABLED'	“デバイスでフェールオーバーが有効になっていません。Please enable failover」	"1025"
'フェールオーバー_LAN_ダウン'	「デバイスのフェールオーバーLANがダウンしています」	"1026"
'STATE_LINK_DOWN'	「デバイスのステートリンクがダウンしています」	"1027"

'FAILOVER_BLOCK_DEPRESSION' (フェールオーバーのブロック除去)	"デバイス内の次のブロックの空き領域が不足しています : \n"	"1028"
'APP_SYNC_TIMEOUT'	「デバイス上のアプリケーション同期タイムアウト」	"1029"
'CD_APP_SYNC_ERROR'	「デバイスでCDアプリの同期エラーが検出されました」	"1030"
'CONFIG_SYNC_TIMEOUT'	「デバイスのConfig sync timeout」	"1031"
「FAILED_TO_APPLY_CONFIG」	「Failed to apply configuration on the device (デバイスに設定を適用できませんでした) 」	"1032"
'BULK_SYNC_TIMEOUT'	「デバイスの一括同期タイムアウト」	"1033"
「BULK_SYNC_CLIENT_ISSUE」	“デバイス上の次のクライアントをチェックしてください : \n"	"1034"
'IFC_CHECK_FAILED'	“デバイスの次のインターフェイスでフェールオーバーインターフェイスのチェックに失敗しました : \n"	"1035"
'IFC_FAILED_CHECK_VLAN_SPANTREE'	「インターフェイスがアップしているため、VLANがスイッチ側で許可されているかどうか、またはスパニングツリーの問題があるかどうかを確認してください。」	"1036"

'バージョンの不一致'	「他のデバイスの異なるソフトウェアバージョン」	"1037"
'モード_不一致'	「他のデバイスで動作モードが異なる」	"1038"
'LIC_MISMATCH'	「別のデバイス上の別のライセンス」	"1039"
'CHASSIS_MISMATCH'	「他のデバイスでの異なるシャーシ構成」	"1040"
'CARD_MISMATCH' (カードミスマッチ)	「他のデバイスでの異なるカード設定」	"1041"
'PEER_NOT_OK'	“このデバイスは正常な状態です。ピアデバイスを確認してください。	"1042"

TAC介入メッセージ

エラー	エラー メッセージ	エラー コード
'RUN_CMD_FAILED'	「Failed to run command (コマンドの実行に失敗)」	"2048"
'LINA_NOT_STARTED'	「Linaがデバイスで起動していません。しばらくしてからもう一度お試しください」	"2049" '
'HWIDB_MISMATCH'	「HWIDBインデックスがデバイス上で異なる」	"2050"
'バックプレーン_障害'	“デバイスのバックプレーンに障害があります。バックプレーンをチェックしてください」	"2051"

'HA_PROGR_FAILURE'	「デバイス上のHA進行障害」	"2052"
'SVM_FAILURE'	「Service Module failed on the device」 (デバイスでサービスモジュールに障害が発生しました)	"2053"
『SVM_MIO_HB_FAILURE』	「デバイス上のMIOとアプリケーションエージェント間のハートビート障害」	"2054"
'SVM_MIO_CRUZ_FAILED'	「MIO-blade network adapter failure on the device (デバイスのMIOブレードネットワークアダプタの障害) 」	"2055"
『SVM_MIO_HB_CRUZ_FAILED』	「MIO-blade Heartbeat and network adapter failure on the device (デバイス上のMIOブレードのハートビートとネットワークアダプタの障害) 」	"2056"
'SSM_CARD_FAILURE'	「Service card failure on the device (デバイスのサービスカード障害) 」	"2057"
『MY_COMM_FAILURE』	「Communication failure on the device (デバイスの通信障害) 」	"2058"
『CRITICAL_PROCESS_DIED』	「デバイス上で重要なプロセスが停止した」	"2059"
'SNORT_FAILURE'	「デバイスでSnortが失敗した」	"2060"
'PEER_SVM_FAILURE'	「NGFWサービスモジュールが他のデバイスで失敗した」	"2061"

『FAULT_MON_BLOCK_DEP』	「障害モニタリングにより、デバイス上のブロックの枯渇が報告されました」	"2062"
'DISK_FAILURE'	「デバイスのディスクに障害が発生しました」	"2063"
「SNORT_DiSK_FAILURE」	“デバイスでSnortとDiskに障害が発生しました	"2064"
'INACTIVE_MATE_FOUND'	“起動中にアクティブでないメイトを検出しました	"2065"
'SCRIPT_TIMEOUT'	"Retry limit exceeded.スクリプトを終了しています"	"2066"
'ERROR_UNKNOWN'	「Failed to identify error (エラーの識別に失敗しました) 」	"2067"

ファイアウォール管理センターUIの変更

▲ Upgrade Completed with Validation Errors

auto_hdaguba_ftd3
10.10.1.106
Cisco Secure Firewall Threat Defense for VMware (Version: 7.6.0-1312)

Version: 7.6.0.8123-1311 | Size: 1,009.41 MB | Build Date: Jan 7, 2024 10:38 PM UTC
Initiated By: admin | Initiated At: Jan 9, 2024 9:12 PM EST

Upgrade to Version 7.6.0.8123-1311 completed with some post-upgrade validation errors.

Log Details

Post-Upgrade Validation Errors:

```
FMC_AQ_ID : 0
error_code : 1024 - FAILOVER_CONFIG_NOT_PRESENT
failover_lan : up
message : Failover config is not present on the device. Please configure failover.
mock_data : 1
my_HA_role : Secondary
my_HA_state : App Sync
peer_HA_role : Primary
```

- There are no UI workflow changes.
- The HA validation error logs will be displayed under existing Log Details field on FMC UI.

Close

ソフトウェア アーキテクチャ

この機能は、既存のアクションキューフレームワークに大きく依存します。この機能は、基盤となる回線CLIを使用して、HAアドバンストラブルシューティングデータを生成します。

FAQ

Q：この機能はFTDアップグレードの復元機能に適用できますか。

A：いいえ。FTD復元は1対1ではなく並行して動作するため、この機能は復元機能には適用されません。

Q:200_enable_maintenance_mode.plでアップグレードが失敗した場合、高度なトラブルシューティングデータが生成されますか。

A：いいえ。HAアドバンストラブルシューティングは、アップグレード後のリブート後にのみ生成され、アップグレードの失敗時には生成されません

Q:2番目のユニットでのHA検証が原因でアップグレードがブロックされた場合、2番目のユニットだけでアップグレードをトリガーできますか。

A：はい。ユーザはアップグレードのためにHAペアを再度選択する必要があり、FMCはアップグレードされていないユニットでのみアップグレードをトリガーします。

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。