

Reduzieren des Fehlers eines Secure Firewall

7.6 FTD HA Upgrade

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Problem](#)

[Neuerungen \(Lösung\)](#)

[Voraussetzungen](#)

[Unterstützte Plattformen](#)

[Funktionsüberblick](#)

[Neuer Upgrade-Workflow für FTD HA](#)

[Standby-Gerät ist die erste Upgrade-Einheit](#)

[Upgrade der ersten Einheit \(Standby-Einheit\)](#)

[Upgrade der zweiten Einheit \(aktive Einheit\)](#)

[HA Vorzeitige Fehlerbehebung](#)

[HA-Bericht zur erweiterten Fehlerbehebung](#)

[Beispiel für HA-Validierungsfehler](#)

[Beispiel für erfolgreiche HA-Validierung](#)

[HA - Erweiterte Fehlerbehebung - Inhalt](#)

[Speicherort der HA Advanced-Problembehebungsdatei](#)

[Tipps zur erweiterten Fehlerbehebung bei Problemen mit der HA-Funktion](#)

[Rückgabestatus und Aktion bei HA Advanced-Fehlerbehebung](#)

[Fehlercode und Klassifizierung](#)

[Interventionsmeldungen für Benutzer](#)

[TAC-Interventionsmeldungen](#)

[Änderungen der Benutzeroberfläche des Firewall Management Centers](#)

[Software-Architektur](#)

[Häufig gestellte Fragen](#)

Einleitung

Dieses Dokument beschreibt die Fehlerbehebung bei FTD-Upgrade-Fehlern von Version 7.0 auf 7.2, insbesondere bei Hochverfügbarkeits-Bereitstellungen (HA).

Hintergrundinformationen

Mehr als die Hälfte dieser Fehler sind auf Probleme in der 200_enable_maintenance_mode-Phase zurückzuführen, in der die vorhandenen HA-Validierungen hauptsächlich grundlegende Prüfungen des aktiven/Standby-Zustands durchführen, die für umfassende HA-Übergänge nicht ausreichen.

Mit Secure Firewall 7.6 wurden verbesserte HA-Validierungen eingeführt, um diese Probleme zu beheben. Zu diesen Verbesserungen gehören gründliche Prüfungen auf HA-Zustandsübergänge, erweiterte Zeitüberschreitungen für Synchronisierungsprozesse und eine verbesserte Fehlerberichterstattung. Dieses Update soll HA-Probleme nach dem Upgrade und allgemeine Upgrade-Fehler deutlich reduzieren und einen reibungsloseren und zuverlässigeren Upgrade-Prozess für HA-Bereitstellungen gewährleisten.

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

Problem

- Kunden berichten von zahlreichen FTD-Upgrade-Fehlern in den Versionen 7.0, 7.1 und 7.2 für HA-Bereitstellungen.
- Mehr als 50 % der Ausfälle werden durch FTD HA-Bereitstellungen verursacht. Fehler in 200_enable_maintenance_mode tragen zu HA-Fehlern bei.
- Bestehende HA-Statusüberprüfungen sind grundlegende Validierungen wie Prüfungen des aktiven/Standby-Status und validieren die HA-Übergänge nicht vollständig.

Neuerungen (Lösung)

Verbesserte HA-Validierung für FTD-Upgrade:

- Validierung für HA-Zustandsübergang
- Verbesserte Zeitüberschreitungen bei FTD-HA-Upgrades für HA-Übergangstatus wie Config Sync (7.200 Sekunden), App Sync (1.200 Sekunden) und Bulk Sync (7.200 Sekunden)
- Mehr Kontrolle für FMC beim Start oder Ausfall des FTD-Upgrades
- Verbesserte Fehlerberichte und Wiederherstellungsmeldungen für FTD HA-Upgrades

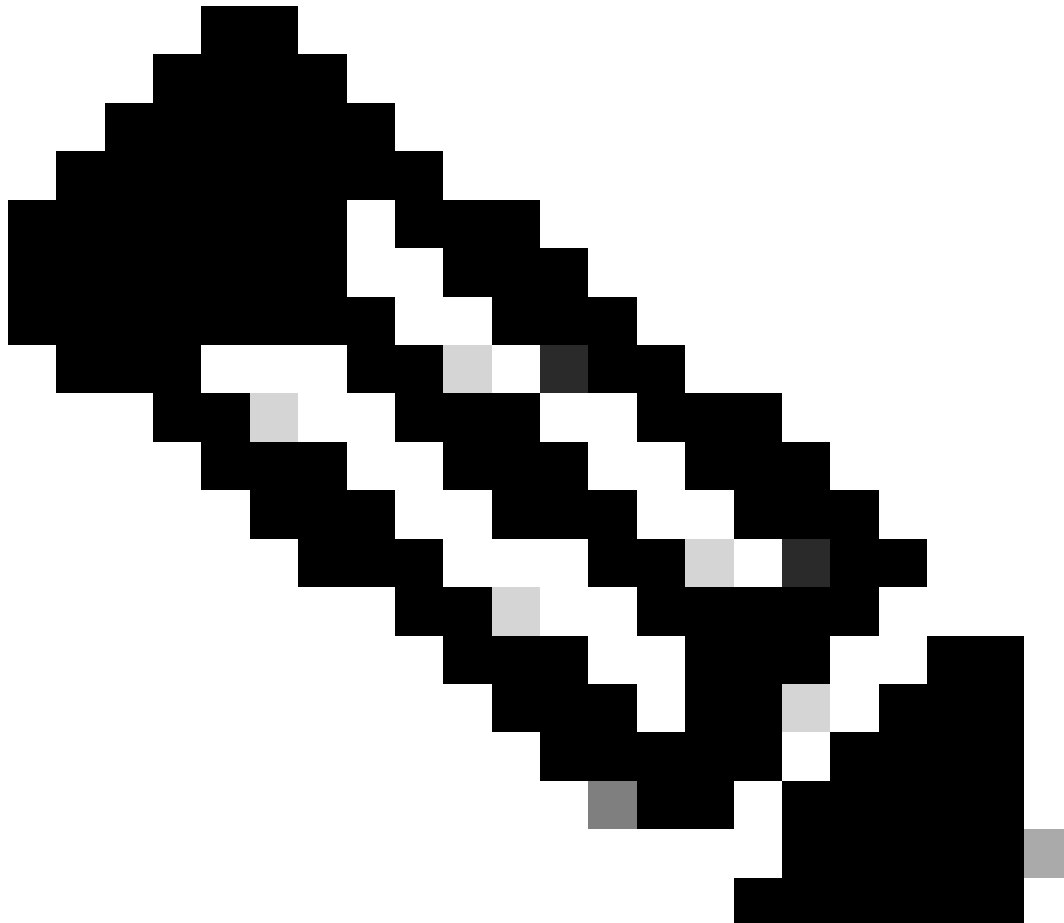
Im Vergleich zu früheren Versionen bietet es folgende Vorteile:

- Verbesserte HA-Validierungen tragen zur Reduzierung von HA-Problemen bei HA-Bereitstellungen nach dem Upgrade bei
- Verbesserte Validierungen tragen zur Reduzierung von FTD-Upgrade-Fehlern bei

Voraussetzungen

Unterstützte Plattformen

- Manager und Version: FMC 7.6.0
 - Anwendung (ASA/FTD) und Mindestversion der Anwendung: FTD 7.6.0 FMC verwaltet 7.6.0 FTD HA
 - Unterstützte Plattformen: Alle Plattformen mit FTD HA
-



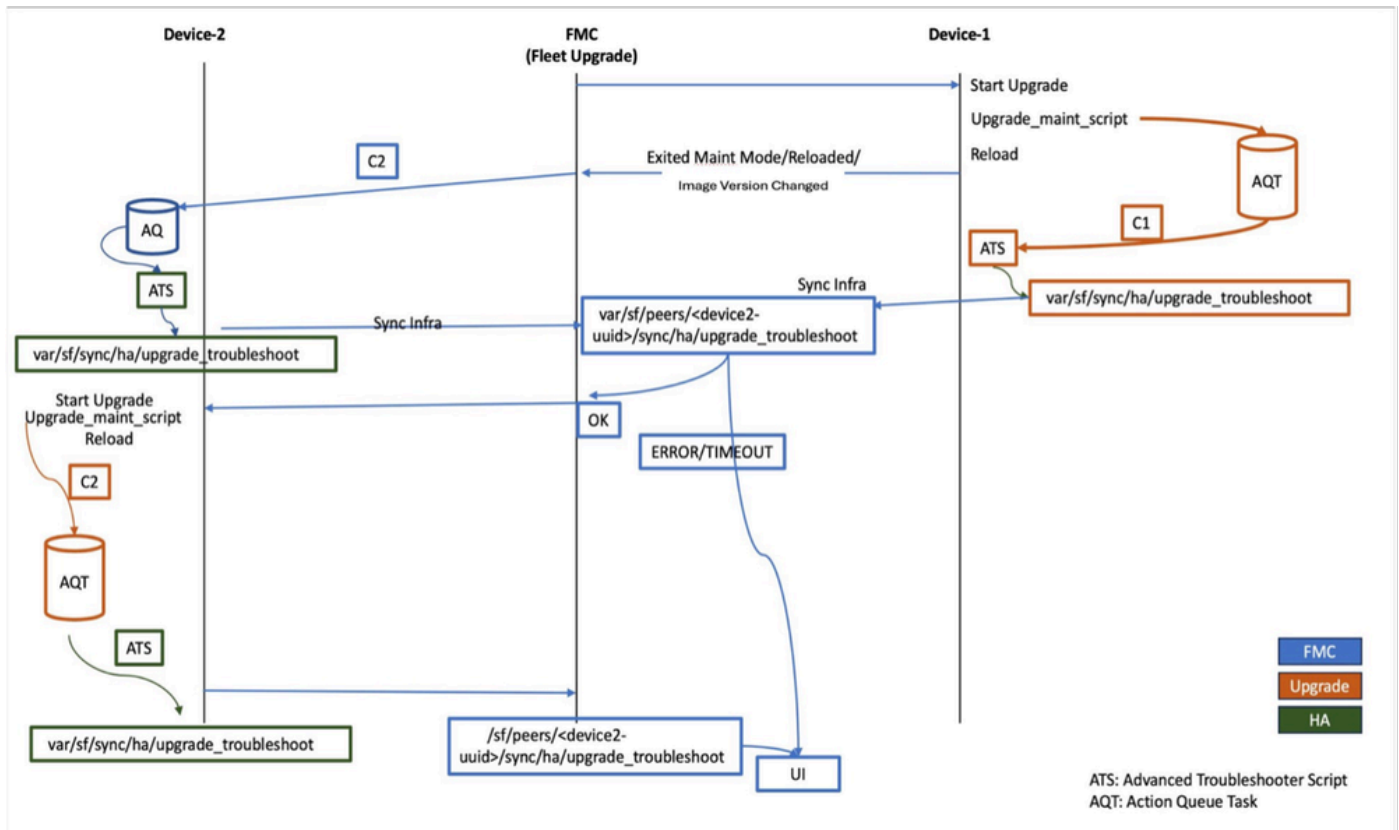
Anmerkung: Diese Funktion gilt nur für von FMC verwaltete FTD HA-Bereitstellungen.
Diese Funktion gilt nicht für vom FDM verwaltete FTD HA- oder Cluster-Geräte.

Funktionsüberblick

- Diese Funktion trägt zur Reduzierung von FTD-Upgrade-Fehlern bei der HA-Bereitstellung bei, indem der HA-Status der aktualisierten Einheiten nach dem Neustart während des Upgrade-Vorgangs vom FMC überprüft wird.
- Nach dem Neustart des Upgrades überprüft FMC den Aktiv-/Standby-Status und alle Fehler bei der HA-Synchronisierung.

- FTD benachrichtigt FMC in Form einer neuen erweiterten Fehlerbehebung für HA, wenn das Upgrade auf dem zweiten Knoten gestartet werden soll oder wenn es fehlschlägt.
- Wenn bei der Einbindung in den HA-Neustart nach dem Upgrade ein Fehler auftritt, wird eine entsprechende Meldung auf der FMC-Benutzeroberfläche angezeigt.

Neuer Upgrade-Workflow für FTD HA



Standby-Gerät ist die erste Upgrade-Einheit

Upgrade der ersten Einheit (Standby-Einheit)

- Während der ersten Aktualisierung der Einheit initiiert das Upgrade-Skript die Aufgabe "action_queue", um die Daten zur erweiterten Fehlerbehebung in der 999_finish-Phase zu erfassen.
- Die eingefügte Aufgabenausführung startet erst nach dem Neustart nach dem Upgrade und sammelt Informationen zur Fehlerbehebung in Form einer JSON-Datei.
- Dieselbe JSON-Datei wird mit FMC synchronisiert.
- Wenn der erste Knoten den Wartungsmodus verlässt, löst FMC eine Remote-action_queue-Aufgabe auf dem aktiven Gerät aus, um die HA-Vorabfehlerbehebung zu erfassen (das aktive Gerät muss 7,6 oder höher sein). Wenn das aktive Gerät älter als 7,6 ist, wird keine Fehlerbehebung vom aktiven Gerät durchgeführt, und das FMC trifft seine Entscheidung nur auf Grundlage der Fehlerbehebung, die vom Standby-Gerät durchgeführt wurde.

Sobald die HA-Fehlerbehebung von beiden Einheiten erfasst wurde, beschließt das FMC, das Upgrade zu starten oder das Upgrade auf dem zweiten Knoten (aktive Einheit) zu blockieren.

Upgrade der zweiten Einheit (aktive Einheit)

- Ähnlich wie bei der Standby-Einheit initiiert das Upgrade-Skript die action_queue-Aufgabe, um die HA-Vorabfehlerbehebung in der 999_finish-Phase zu erfassen.
- Die eingefügte Aufgabenausführung startet erst nach dem Neustart des Upgrades und generiert Informationen zur Fehlerbehebung in Form einer JSON-Datei.
- Dieselbe Datei wird mit FMC synchronisiert.
- Wenn eines der Geräte einen HA-Ausfall meldet, werden Daten zu HA-Ausfällen auf der FMC-Benutzeroberfläche auf der Registerkarte "Upgrade" angezeigt.
- Bei Fehlern beim Beitritt zu HA nach dem Neustart des Upgrades wird das Upgrade als abgeschlossen markiert, und auf derselben Registerkarte für das Upgrade werden Fehler bei der HA-Validierung gemeldet.

HA Vorzeitige Fehlerbehebung

- HA-Fehlerbehebung ist eine neue einzelne JSON-Datei, die als Teil dieser Funktion eingeführt wurde und HA-Informationen enthält. Sie wird nach dem Neustart nach einem Upgrade generiert und vom FTD an das FMC gesendet.
- Dateiname und Pfad: /ngfw/var/sf/sync/ha/upgrade_troubleshoot
- Sobald das FMC die HA-Vorabfehlerbehebung vom ersten (Standby-) Gerät erfasst, löst das FMC eine Remote-Aufgabe aus, um dieselben Informationen vom aktiven Gerät zu erfassen.
 - Diese Remote-Datensammlung wird nur unterstützt, wenn die Geräte mit Version 7.6 oder höher ausgeführt werden.
 - Wenn Geräte mit einer Version kleiner als 7.6 gefunden werden, wird die Remote-Datensammlung übersprungen. In diesem Fall würde FMC also nur Daten von der Standby-Einheit sammeln und weitere Maßnahmen beschließen.
- Die Fehlerbehebung erfolgt schnell. Wenn Lina nicht verfügbar ist und den Bericht nicht generiert, wird er sofort beendet.
 - Die Zeit für den Neustart des Geräts hängt von der Plattform für die andere ab, und die Zeit für den Neustart ist dieselbe wie für die einzelnen Plattformen angegeben.

HA-Bericht zur erweiterten Fehlerbehebung

Jede HA-Einheit generiert eine HA-Advanced-Fehlerbehebung für Daten in Form eines JSON-Datei-Neustarts nach dem Upgrade und teilt diese mit dem FMC. Im Folgenden finden Sie Beispiele für erfolgreiche Validierungen.

Beispiel für HA-Validierungsfehler

Datei: /ngfw/var/sf/sync/ha/upgrade_troubleshoot

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

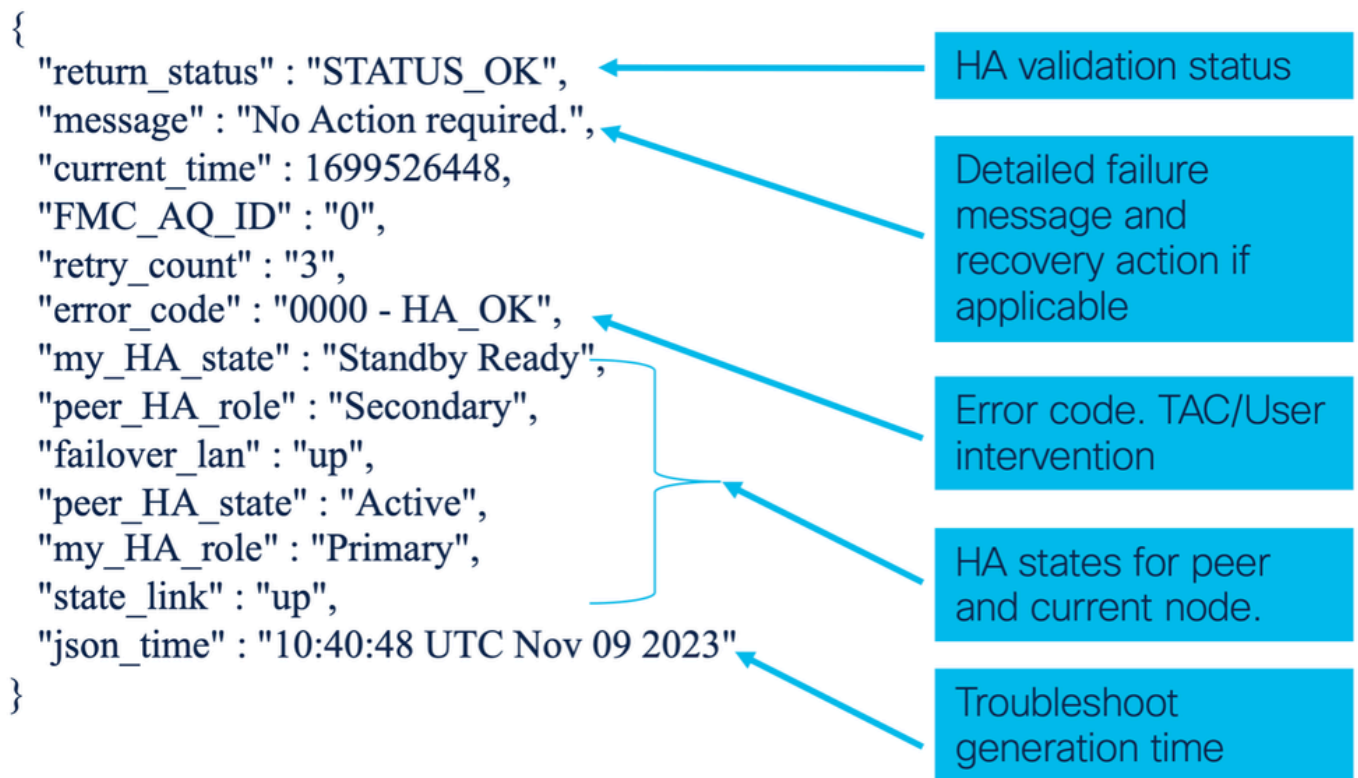
```
STARTUP_FAILOVER_CONFIG_NOT_PRESENT",
"current_time" : 1701369637,
"peer_HA_state" : "Not Detected",
"FMC_AQ_ID" : "0",
"state_link" : "NA",
"json_time" : "18:40:37 UTC Nov 30 2023",
"my_HA_state" : "Disabled",
"my_HA_role" : "Secondary",
"return_status" : "STATUS_ERROR",
"message" : "Failover config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

Beispiel für erfolgreiche HA-Validierung

Datei: /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 - Erweiterte Fehlerbehebung - Inhalt



Speicherort der HA Advanced-Problembhebungsdatei

HA-Advanced-Fehlerbehebung für den Speicherort der JSON-Datei:

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

`/sync/ha/upgrade_troubleshoot`

- Die HA-Fehlerbehebung beruht auf dem Befehl `lina`.
 - Wenn die Fehlerbehebung unter `/ngfw/var/sf/sync/ha/upgrade_troubleshoot` nicht generiert werden kann, kann der Benutzer die Protokolle unter folgender Adresse anzeigen: `/ngfw/var/log/ha_upgrade_troubleshoot.log`
- `/ngfw/var/sf/sync/ha/upgrade_troubleshoot` und `/ngfw/var/log/ha_upgrade_troubleshoot.log` Dateien sind Teil der FTD Troubleshoot Datei.

Tipps zur erweiterten Fehlerbehebung bei Problemen mit der HA-Funktion

Manchmal wird aufgrund des Systemzustands keine HA-Vorabdiagnose generiert, und der Grund dafür könnte "lina down" sein, oder der Prozess der Aktionswarteschlange ist nach dem Neustart des Upgrades "down". Wenn Lina oder die Aktionswarteschlange nicht verfügbar ist, ist dies ein Problem.

Überprüfen Sie in diesem Fall mithilfe des folgenden Befehls im Expertenmodus, ob lina- und ActionQueue-Prozesse ausgeführt werden:

```
<#root>
```

```
pmtool status | grep lina
```

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

```
pmtool status | grep ActionQueueScape
```

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

Rückgabestatus und Aktion bei HA Advanced-Fehlerbehebung

- STATUS_INIT: Dies zeigt an, dass die HA-Fehlerbehebung ausgelöst wurde.
- STATUS_OK: Das Gerät befindet sich in einem stabilen Zustand. Es sind keine Maßnahmen erforderlich.
- STATUSFEHLER: Dadurch wird festgestellt, dass ein Fehler aufgetreten ist, aufgrund dessen keine hohe Verfügbarkeit gebildet wird. Der Benutzer muss eine Aktion basierend auf der angezeigten Meldung durchführen, oder der Benutzer muss sich an das TAC wenden.
- STATUS_WIEDERHOLEN: Die Vorrichtung kann sich in einem der Zwischenzustände befinden. Die HA-Fehlerbehebung wird nach einem festen Intervall auf Basis des Status so lange wiederholt, bis STATUS_ERROR oder STATUS_OK erkannt wird.
 - Basierend auf den aufgetretenen Fehlern STATUS_ERROR werden die HA-Fehler in 2 Fälle eingeteilt:
 - Benutzereingriff - Diese HA-Fehler können vom Benutzer behoben werden, und der Benutzer kann das Upgrade fortsetzen, wenn kein TAC-Eingriff erforderlich ist.
 - TAC-Intervention: Bei HA-Ausfällen kann der Benutzer die Störung nicht selbst beheben. TAC-Intervention ist erforderlich.

Fehlercode und Klassifizierung

Auf der Grundlage von Fehlercodes werden Fehler wie folgt klassifiziert:

Rückgabestatus	Fehlercode	Beschreibung	Wiederholungs- oder Wiederherstellungsmechanismus
STATUS_OK	"0000 - HA_OK"(Reservierte Werte liegen zwischen 0001 und 1023)	Dies gilt für das Erfolgsszenario. (HA-Status: Aktiv und Standby-fähig)	(Nicht zutreffend)
STATUS_FEHLER	"1024:2047 - ERROR_REASON"	Dies gilt für das Fehlerszenario (Benutzereingriff)	Aussagekräftige Meldungen, die dem Benutzer und dem Upgrade-Framework angezeigt werden, können den Wiederholungs- oder Wiederherstellungsmechanismus zu einem späteren Zeitpunkt hinzufügen (falls vorhanden).
STATUS_FEHLER	"2048:3071 - ERROR_REASON"	Dies gilt für das Fehlerszenario (TAC-Intervention)	Für die Bestandserholung sind TAC-Interventionen erforderlich.

Interventionsmeldungen für Benutzer

Fehler	Fehlermeldung	Fehlercode
'FAILOVER_CONFIG_NOT_PRESENT'	"Failover-Konfiguration auf Gerät nicht vorhanden"	"1024"
FAILOVER_IS_NOT_ENABLED	"Failover ist auf dem Gerät nicht aktiviert. Aktivieren Sie Failover."	"1025"
FAILOVER_LAN_DOWN	"Failover LAN ist auf dem Gerät inaktiv."	"1026"
STATE_LINK_DOWN	"Die Statusverbindung auf dem	"1027"

	Gerät ist ausgefallen."	
'FAILOVER_BLOCK_DEPLETION'	"Blockerschöpfung bei folgenden Blöcken im Gerät:\n"	"1028"
'APP_SYNC_TIMEOUT'	"Zeitüberschreitung bei App-Synchronisierung auf dem Gerät"	"1029"
'CD_APP_SYNC_ERROR'	"CD-App-Synchronisierungsfehler auf dem Gerät erkannt"	"1030"
'CONFIG_SYNC_TIMEOUT'	"Zeitüberschreitung bei der Konfigurationssynchronisierung auf dem Gerät"	"1031"
FAILED_TO_APPLY_CONFIG	"Fehler beim Anwenden der Konfiguration auf das Gerät."	"1032"
'BULK_SYNC_TIMEOUT'	"Zeitüberschreitung bei Massensynchronisierung auf dem Gerät"	"1033"
'BULK_SYNC_CLIENT_ISSUE'	"Überprüfen Sie die folgenden Clients auf dem Gerät:\n"	"1034"
'IFC_CHECK_FAILED'	"Fehler bei der Failover-Schnittstellenüberprüfung für die folgenden Schnittstellen im Gerät:\n"	"1035"
IFC_FAILED_CHECK_VLAN_SPANTREE	"Da die Schnittstellen aktiv sind. Überprüfen Sie, ob die VLANs auf der Switch-Seite zulässig sind oder ein Spanning-Tree-Problem vorliegt."	"1036"

VERSION_MISMATCH	"Andere Softwareversion auf dem anderen Gerät"	"1037"
MODE_MISMATCH	"Anderer Betriebsmodus am anderen Gerät"	"1038"
LIC_MISMATCH	"Anderes Gerät verfügt über eine andere Lizenz."	"1039"
CHASSIS_MISMATCH	"Unterschiedliche Chassis-Konfiguration auf dem anderen Gerät"	"1040"
'KARTE NICHT ÜBEREINSTIMMEND'	"Unterschiedliche Kartenkonfiguration auf dem anderen Gerät"	"1041"
PEER_NOT_OK	"Dieses Gerät ist in OK. Überprüfen Sie das Peer-Gerät."	"1042"

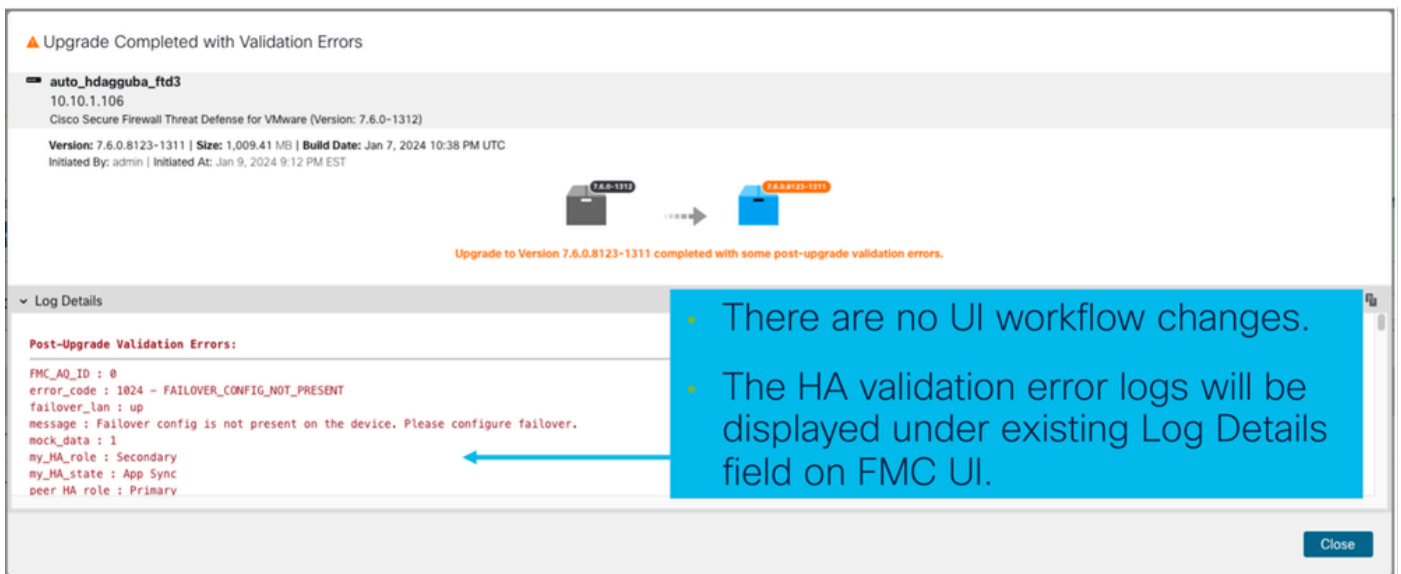
TAC-Interventionsmeldungen

Fehler	Fehlermeldung	Fehlercode
'RUN_CMD_FAILED'	"Befehl konnte nicht ausgeführt werden"	"2048"
LINA_NOT_STARTED	"Lina wurde auf dem Gerät nicht gestartet. Versuchen Sie es später erneut."	„2049“
HWIDB_MISMATCH	"Der HWIDB-Index auf dem Gerät ist anders."	"2050"
'BACKPLANE_FAILURE'	"Backplane Failure on the device. Backplane prüfen"	"2051"

HA_PROGR_FAILURE	"HA-Progressionsfehler auf dem Gerät"	"2052"
SVM_FAILURE	"Servicemodul auf Gerät fehlgeschlagen"	"2053"
SVM_MIO_HB_FAILURE	"Heartbeat Failure zwischen MIO und App-Agent auf dem Gerät"	"2054"
'SVM_MIO_CRUZ_FAILED'	"Ausfall des MIO-Blade-Netzwerkadapters auf dem Gerät"	"2055"
'SVM_MIO_HB_CRUZ_FAILED'	"MIO-Blade-Heartbeat- und Netzwerkadapterfehler auf dem Gerät"	"2056"
'SSM_CARD_FAILURE'	"Servicekartenfehler auf dem Gerät"	"2057"
'MY_COMM_FAILURE'	"Kommunikationsfehler auf dem Gerät"	"2058"
CRITICAL_PROCESS_DIED	"Kritischer Prozess starb auf dem Gerät"	"2059"
SNORT_FAILURE	"Snort auf dem Gerät fehlgeschlagen"	"2060"
PEER_SVM_FAILURE	"Das NGFW-Servicemodul auf dem anderen Gerät ist ausgefallen."	"2061"
'FAULT_MON_BLOCK_DEP'	"Fehlerüberwachung meldet Blockerschöpfung auf dem Gerät"	"2062"
'DISK_FAILURE'	"Festplatte auf dem Gerät"	"2063"

	ausgefallen"	
SNORT_DiSK_FAILURE	"Snort and Disk failed on the device	"2064"
'INACTIVE_MATE_FOUND"	"Inaktiver Partner beim Hochfahren erkannt	"2065"
SCRIPT_TIMEOUT	"Grenzwert für Wiederholungen überschritten. Skript beenden"	"2066"
'FEHLER_UNBEKANNT'	"Fehler beim Identifizieren des Fehlers"	"2067"

Änderungen der Benutzeroberfläche des Firewall Management Centers



▲ Upgrade Completed with Validation Errors

auto_hdagguba_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

Software-Architektur

Diese Funktion ist stark vom vorhandenen Aktionswarteschlangen-Framework abhängig. Die Funktion verwendet die zugrunde liegende Kommandozeile, um die erweiterten HA-Fehlerbehebungsdaten zu generieren.

Häufig gestellte Fragen

F: Gilt die Funktion für die FTD-Upgrade-Rückgängig-Funktion?

A : Nein. Diese Funktion gilt nicht für die Rückgängig-Funktion, da die FTD-Rückwärts-Funktion

parallel und nicht 1-by-1 arbeitet.

F: Wenn das Upgrade bei 200_enable_maintenance_mode.pl fehlschlägt, werden dann die erweiterten Fehlerbehebungsdaten generiert?

A : Nein. Die HA-Fehlerbehebung wird nur nach dem Neustart des Upgrades und nicht während des fehlgeschlagenen Upgrades durchgeführt.

F: Wenn das Upgrade aufgrund von HA-Validierungen auf der zweiten Einheit blockiert wird, kann ein Benutzer das Upgrade auf der zweiten Einheit allein auslösen?

A : Ja. Der Benutzer muss das HA-Paar erneut für das Upgrade auswählen, und das FMC löst das Upgrade nur für nicht aktualisierte Geräte aus.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.