

Fout bij upgrade naar Secure Firewall 7.6 FTD HA verminderen

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Probleem](#)

[Wat is nieuw \(oplossing\)](#)

[Voorwaarden](#)

[Ondersteunde platforms](#)

[Overzicht van functies](#)

[Nieuwe Upgrade Workflow voor FTD HA](#)

[Standby Unit is de eerste die een upgrade uitvoert](#)

[Eerste upgrade van de eenheid \(stand-byeenheid\)](#)

[Tweede upgrade-eenheid \(actieve eenheid\)](#)

[HA Advance-probleemoplossing](#)

[Voorafgaand probleemoplossingsrapport van HA](#)

[Voorbeeld van HA-validatiefout](#)

[Voorbeeld van succesvolle HA-validatie](#)

[Inhoud van HA Advance Troubleshoot](#)

[Locatie van HA Advance Troubleshoot File](#)

[Tips voor HA Advance Troubleshoot Generation-problemen](#)

[Status en actie retourneren in probleemoplossing van HA Advance](#)

[Foutcode en classificatie](#)

[Berichten voor gebruikersinterventie](#)

[TAC-interventieberichten](#)

[UI-wijzigingen in Firewall Management Center](#)

[Softwarearchitectuur](#)

[Veelgestelde vragen](#)

Inleiding

In dit document wordt beschreven hoe problemen kunnen worden opgelost bij FTD-upgradefouten van versie 7.0 tot 7.2, met name bij High Availability (HA)-implementaties.

Achtergrondinformatie

Meer dan de helft van deze fouten is het gevolg van problemen tijdens de fase 200_enable_maintenance_mode, waarbij bestaande HA-validaties voornamelijk basiscontroles van de actieve/stand-bystatus uitvoeren, die ontoereikend zijn voor uitgebreide HA-overgangen.

Met de Secure Firewall 7.6-update zijn verbeterde HA-validaties geïntroduceerd om deze problemen aan te pakken. Deze verbeteringen omvatten grondige controles voor HA-toestandsovergangen, verlengde time-outs voor synchronisatieprocessen en verbeterde foutenrapportage. Deze update heeft tot doel de problemen met HA na de upgrade en de algehele upgradefouten aanzienlijk te verminderen, waardoor een soepeler en betrouwbaarder upgradeproces voor HA-implementaties wordt gegarandeerd.

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

Probleem

- Er zijn een aanzienlijk aantal FTD-upgradefouten gemeld door klanten in 7.0-, 7.1- en 7.2-releases voor HA-implementaties.
- Meer dan 50% van de storingen komt van FTD HA-implementaties. Fouten in 200_enable_maintenance_mode dragen bij aan HA-fouten.
- Bestaande HA-toestandsvalidaties zijn basisvalidaties zoals actieve/standby-toestandscontroles en valideren de HA-overgangen niet volledig.

Wat is nieuw (oplossing)

Verbeterde HA-validaties voor FTD-upgrade:

- Validering voor overgang van HA-toestand
- Verbeterde FTD HA-upgradetime-outs voor HA-overgangstoestand zoals config-synchronisatie (7200 seconden), app-synchronisatie (1200 seconden) en bulksynchronisatie (7200 seconden)
- FMC meer controle geven over wanneer de FTD-upgrade moet worden gestart of mislukt
- Verbeterde foutmelding en herstelbericht voor FTD HA-upgrades

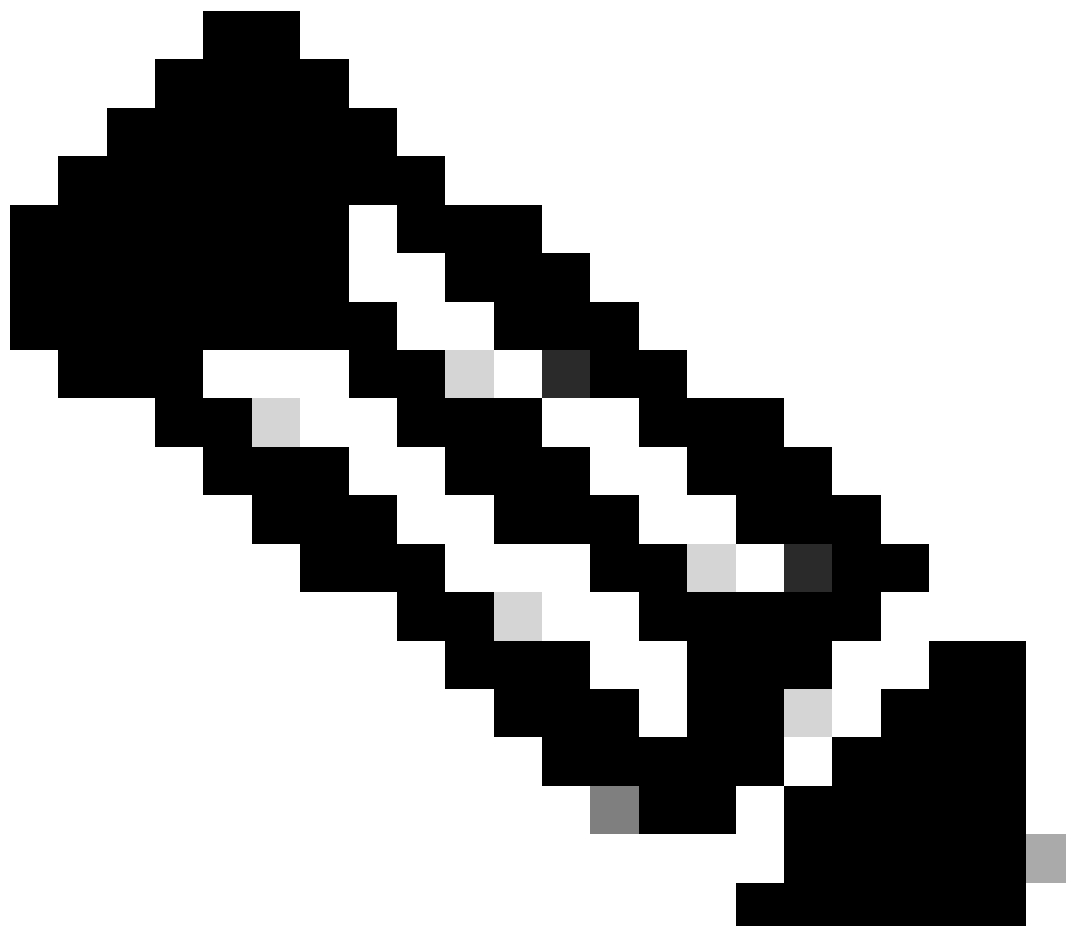
In vergelijking met eerdere releases heeft het:

- Verbeterde HA-validaties helpen de problemen met het maken van HA na de upgrade bij HA-implementaties te verminderen
- Verbeterde validaties helpen FTD-upgradefouten te verminderen

Voorwaarden

Ondersteunde platforms

- Manager(s) en Versie(s): FMC 7.6.0
 - Toepassing (ASA/FTD) en minimale versie van toepassing: FTD 7.6.0; FMC beheert 7.6.0 FTD HA
 - Ondersteunde platforms: Alle platforms waarop FTD HA wordt uitgevoerd
-



Opmerking: deze functie is alleen van toepassing op FTD HA-implementaties die door de FMC worden beheerd. Deze functie is niet van toepassing op door FDM beheerde FTD HA of geclusterde apparaten.

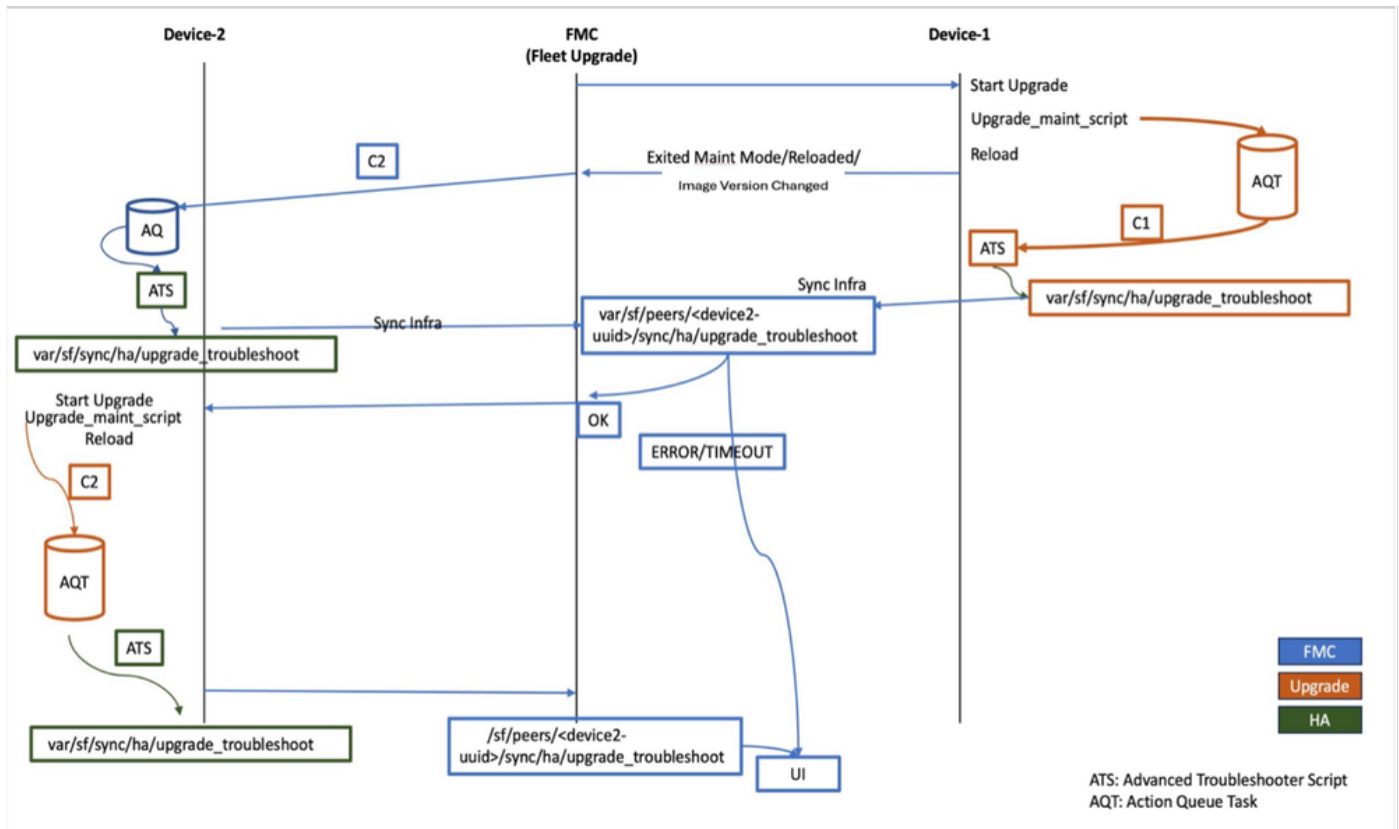
Overzicht van functies

- Deze functie helpt FTD-upgradefouten bij HA-implementatie te verminderen door de HA-status van de geüpgradede eenheden door FMC te controleren na het reboot-gedeelte van het upgradeproces.
- Nadat de upgrade opnieuw is opgestart, controleert de FMC of de status actief/stand-by is

en of er fouten zijn opgetreden in de synchronisatie van de HA.

- FTD geeft FMC een melding wanneer de upgrade op het tweede knooppunt moet worden gestart of mislukt in de vorm van een nieuwe probleemoplossing vooraf van HA.
- Als het na het opnieuw opstarten van de upgrade niet lukt om deel te nemen aan de HA, wordt een passend bericht weergegeven op de FMC UI.

Nieuwe Upgrade Workflow voor FTD HA



Standby Unit is de eerste die een upgrade uitvoert

Eerste upgrade van de eenheid (stand-byeenheid)

- Tijdens de eerste upgrade van de eenheid initieert het upgradescrypt de `action_queue`-taak om vooraf HA-probleemoplossingsgegevens te verzamelen in de `999_finish`-fase.
- De uitvoering van de ingevoegde taak begint pas na het opnieuw opstarten van de upgrade en verzamelt informatie over probleemoplossing in de vorm van een JSON-bestand.
- Hetzelfde JSON-bestand wordt gesynchroniseerd met FMC.
- Zodra de eerste node de onderhoudsmodus verlaat, activeert FMC een taak op afstand `action_queue` op de actieve eenheid om de probleemoplossing voor HA vooraf te verzamelen (actieve eenheid moet 7,6 of hoger zijn). Als de actieve eenheid lager dan 7,6 wordt gevonden, wordt er geen probleemoplossing verzameld van de actieve eenheid en neemt de FMC een beslissing op basis van de probleemoplossing die is verzameld van de stand-byeenheid.

Zodra de probleemoplossing voor HA vooraf bij beide eenheden is verzameld, besluit de FMC de

upgrade te starten of de upgrade op het tweede knooppunt (actieve eenheid) te blokkeren.

Tweede upgrade-eenheid (actieve eenheid)

- Net als bij de stand-by-eenheid, initieert het upgradedescript de action_queue-taak om vooraf HA-problemen op te lossen in de 999_finish-fase.
- Ingevoegde taakuitvoering start alleen na het opnieuw opstarten van de upgrade en genereert probleemoplossingsinformatie in de vorm van een JSON-bestand.
- Hetzelfde bestand wordt gesynchroniseerd met FMC.
- Als een van de units HA-fout meldt, worden de HA-foutgegevens weergegeven op de FMC UI op het tabblad Upgrade.
- In het geval van een fout in het deelnemen aan HA na het opnieuw opstarten van de upgrade, wordt de upgrade gemarkeerd als voltooid en op hetzelfde upgradetabblad worden HA-validatiefouten gemeld.

HA Advance-probleemoplossing

- HA advance troubleshoot is een nieuw JSON-bestand dat als onderdeel van deze functie is geïntroduceerd en HA-informatie bevat. Het wordt gegenereerd na de reboot na een upgrade en verzonden van de FTD naar de FMC.
- Bestandsnaam en pad: /ngfw/var/sf/sync/ha/upgrade_troubleshoot
- Zodra FMC de HA-probleemoplossing van de eerste (stand-by) eenheid verzamelt, activeert FMC een externe taak om dezelfde informatie van de actieve eenheid te verzamelen.
 - Deze gegevensverzameling op afstand wordt alleen ondersteund wanneer de apparaten 7.6 of hoger uitvoeren.
 - Als apparaten worden gevonden met een versie van minder dan 7.6, wordt het verzamelen van gegevens op afstand overgeslagen. In dit geval zou de FMC dus alleen gegevens van de stand-by-eenheid verzamelen en besluiten tot verdere actie.
- HA geavanceerde probleemoplossingsgeneratie is snel. Als Lina down is en er niet in slaagt om het rapport te genereren, wordt het onmiddellijk afgesloten.
 - De reboot-tijd van het apparaat is afhankelijk van platform tot platform en de reboot-tijd is hetzelfde als we voor elk platform hebben gedocumenteerd.

Voorafgaand probleemoplossingsrapport van HA

Elke HA-eenheid genereert vooraf een HA-probleemoplossingsgegevens in de vorm van een JSON-bestand na het opnieuw opstarten van de upgrade en deelt deze met FMC. Hier zijn validatievoorbeelden wanneer er sprake is van een mislukking en succes.

Voorbeeld van HA-validatiefout

Bestand: /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"
}

```

Voorbeeld van succesvolle HA-validatie

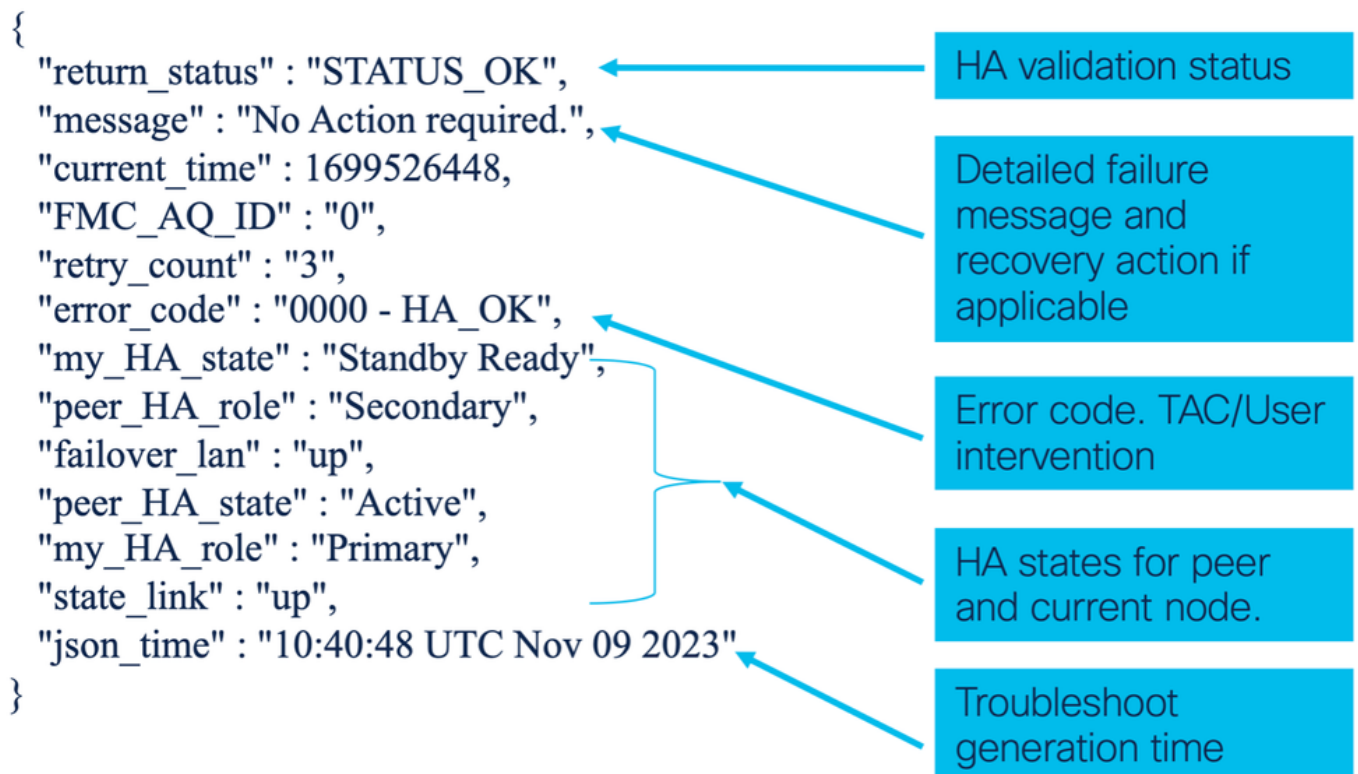
Bestand: /ngfw/var/sf/sync/ha/upgrade_troubleshoot

```

{
"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
}

```

Inhoud van HA Advance Troubleshoot



Locatie van HA Advance Troubleshoot File

HA advance troubleshoot JSON bestandslocatie:

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

`/sync/ha/upgrade_troubleshoot`

- De HA-probleemoplossing is gebaseerd op het `lina-commando`.
 - Als de probleemoplossing niet kan worden gegenereerd op `/ngfw/var/sf/sync/ha/upgrade_troubleshoot`, kan de gebruiker de logbestanden raadplegen op: `/ngfw/var/log/ha_upgrade_troubleshoot.log`
- `/ngfw/var/sf/sync/ha/upgrade_troubleshoot` en `/ngfw/var/log/ha_upgrade_troubleshoot.log` maken deel uit van het FTD Troubleshoot-bestand.

Tips voor HA Advance Troubleshoot Generation-problemen

Soms wordt HA advance troubleshoot niet gegenereerd vanwege de systeemstatus en de reden hiervoor kan lineair zijn of het proces van de actiewachtrij is down na het opnieuw opstarten van

de upgrade. Als lina of action queue niet beschikbaar is, is dit een probleem.

Controleer in dergelijke gevallen of lina- en ActionQueue-processen worden uitgevoerd met behulp van deze opdracht in de expertmodus:

```
<#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
```

Status en actie retourneren in probleemoplossing van HA Advance

- STATUS_INIT: Dit geeft aan dat de HA-probleemoplossing is geactiveerd.
- STATUS_OK: Het apparaat bevindt zich in een stabiele toestand. Er is geen actie vereist.
- STATUS_FOUT: Hiermee wordt bepaald dat er een fout is opgetreden als gevolg waarvan geen HA is gevormd. De gebruiker moet een actie ondernemen op basis van het weergegeven bericht of de gebruiker moet contact opnemen met TAC.
- STATUS_RETRY: Het apparaat kan zich in een van de tussenliggende toestanden bevinden. De HA-probleemoplossing blijft opnieuw proberen na een vast interval op basis van de status totdat STATUS_ERROR of STATUS_OK wordt aangetroffen.
 - Op basis van de aangetroffen fouten STATUS_ERROR, worden de HA-fouten onderverdeeld in 2 gevallen:
 - Interventie van de gebruiker – Deze HA-fouten kunnen door de gebruiker worden opgelost en de gebruiker kan de upgrade hervatten, waarbij de TAC-interventie niet vereist is.
 - TAC-interventie – Voor deze HA-fouten kan de gebruiker het niet zelf oplossen; TAC-interventie is vereist.

Foutcode en classificatie

Op basis van foutcodes worden Fouten geclassificeerd zoals hieronder weergegeven:

return_status	error_code	Beschrijving	mechanisme voor hervatting of herstel
STATUS_OK	"0000 –	Dit is voor het	(niet van toepassing)

	HA_OK"(Gereserveerde waarden zijn van 0001 – 1023)	successscenario. (Wanneer de HA-staten actief en klaar voor stand-by zijn)	
STATUS_FOUT	"1024:2047 – FOUT_REDEN"	Dit is voor het fouts scenario (interventie van de gebruiker)	Actionable berichten die aan de gebruiker en het upgradekader moeten worden weergegeven, kunnen in de toekomst (indien van toepassing) het herstel- of herhalingsmechanisme toevoegen.
STATUS_FOUT	"2048:3071 – FOUT_REDEN"	Dit is voor het foutenscenario (TAC-interventie)	TAC-interventie is vereist voor herstel.

Berichten voor gebruikersinterventie

Fout	Fout	Foutcode
'FAILOVER_CONFIG_NOT_PRESENT'	"Failover-configuratie is niet aanwezig op het apparaat"	"1024"
'FAILOVER_IS_NOT_ENABLED'	"Failover is niet ingeschakeld op het apparaat. Schakel failover in."	"1025"
'FAILOVER_LAN_DOWN'	"Failover LAN is down op het apparaat"	"1026"

'STATE_LINK_DOWN'	"State Link is down op het apparaat"	"1027"
'FAILOVER_BLOCK_DEPLETION'	"Blokuitputting op de volgende blokken in het apparaat:\n"	"1028"
'APP_SYNC_TIMEOUT'	"Time-out voor synchronisatie van app op het apparaat"	"1029"
'CD_APP_SYNC_ERROR'	"Fout bij synchronisatie van cd-app gedetecteerd op apparaat"	"1030"
'CONFIG_SYNC_TIMEOUT'	"Config synchronisatie time-out op het apparaat"	"1031"
'FAILED_TO_APPLY_CONFIG'	"Kan configuratie niet toepassen op het apparaat"	"1032"
'BULK_SYNC_TIMEOUT'	"Time-out voor bulksgewijs synchroniseren op het apparaat"	"1033"
'BULK_SYNC_CLIENT_ISSUE'	Controleer de volgende clients op het apparaat:\n	"1034"
'IFC_CHECK_FAILED'	"Failover-interfacecontrole mislukt op volgende	"1035"

	interfaces in het apparaat:\n"	
'IFC_FAILED_CHECK_VLAN_SPANTREE'	"Omdat de interfaces zijn opgeheven. Controleer of de VLAN's zijn toegestaan aan de kant van de switch of er een spanning tree probleem is."	"1036"
'VERSION_MISMATCH'	"Andere softwareversie op het andere apparaat"	"1037"
'MODE_MISMATCH'	"Andere bedrijfsmodus op het andere apparaat"	"1038"
'LIC_MISMATCH'	"Andere licentie op het andere apparaat"	"1039"
'CHASSIS_MISMATCH'	"Verschillende chassisconfiguratie op het andere apparaat"	"1040"
'CARD_MISMATCH'	"Verschillende kaartconfiguratie op het andere apparaat"	"1041"
'PEER_NOT_OK'	"Dit apparaat is in de goede staat. Controleer het peer-apparaat."	"1042"

TAC-interventieberichten

Fout	Fout	Foutcode
'RUN_CMD_FAILED'	"Kan opdracht niet uitvoeren"	"2048"
'LINA_NOT_STARTED'	"Lina is niet gestart op het apparaat. Probeer het na een tijdje nog eens."	"2049"
'HWIDB_MISMATCH'	"HWIDB-index is anders op het apparaat"	"2050"
'BACKPLANE_FAILURE'	"Backplane-fout op het apparaat. Controleer de backplane"	"2051"
'HA_PROGR_FAILURE'	"HA progressie falen op het apparaat"	"2052"
'SVM_FAILURE'	"Servicemodule is mislukt op het apparaat"	"2053"
'SVM_MIO_HB_FAILURE'	"Hartslagfalen tussen MIO en App-agent op het apparaat"	"2054"
'SVM_MIO_CRUZ_FAILED'	"Mislukte MIO-blade-netwerkadapter op het apparaat"	"2055"
'SVM_MIO_HB_CRUZ_FAILED'	"Mislukte hartslag van MIO-blade en netwerkadapter op het apparaat"	"2056"
'SSM_CARD_FAILURE'	"Service card failure op het apparaat"	"2057"
'MY_COMM_FAILURE'	"Communicatiefout op het	"2058"

	apparaat"	
'CRITICAL_PROCESS_DIED'	"Kritiek proces stierf op het apparaat"	"2059"
'SNORT_FAILURE'	"Snijden mislukt op het apparaat"	"2060"
'PEER_SVM_FAILURE'	"NGFW-servicemodule is mislukt op het andere apparaat"	"2061"
'FAULT_MON_BLOCK_DEP'	"Foutbewaking meldde blokdepletie op het apparaat"	"2062"
'DISK_FAILURE'	"Schijf mislukt op het apparaat"	"2063"
'SNORT_DISK_FAILURE'	"Snijden en schijf is mislukt op het apparaat"	"2064"
'INACTIVE_MATE_FOUND'	"Een inactieve partner gedetecteerd tijdens opstarten"	"2065"
'SCRIPT_TIMEOUT'	"Limiet voor nieuwe poging overschreden. Script afsluiten"	"2066"
'ERROR_UNKNOWN'	"Fout niet geïdentificeerd"	"2067"

UI-wijzigingen in Firewall Management Center

▲ 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

7.6.0-1312

→

7.6.0.8123-1311

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

Softwarearchitectuur

Deze functie is sterk afhankelijk van het bestaande actiewachtrijkader. De functie maakt gebruik van de onderliggende lina CLI om de HA vooraf probleemoplossingsgegevens te genereren.

Veelgestelde vragen

V: Is de functie van toepassing op de FTD-upgradeterugkeerfunctionaliteit?

A: Nee. Deze functie is niet van toepassing op de terugkeerfunctionaliteit, omdat FTD-terugkeerfuncties parallel werken en niet 1 bij 1.

V: Als de upgrade mislukt op 200_enable_maintenance_mode.pl, genereert deze dan de gegevens voor het vooraf oplossen van problemen?

A: Nee. Problemen met HA vooraf worden alleen na het opnieuw opstarten van de upgrade gegenereerd en niet tijdens het mislukken van de upgrade

V: Als de upgrade is geblokkeerd vanwege HA-validaties op de tweede eenheid, kan een gebruiker dan alleen de upgrade op de tweede eenheid activeren?

A: Ja. De gebruiker moet het HA-paar opnieuw selecteren voor een upgrade en FMC activeert de upgrade alleen op een niet-geüpgraded apparaat.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.