Réduction des échecs de mise à niveau FTD HA de Secure Firewall 7.6

Table des matières

Introduction

Ce document décrit le dépannage pour résoudre les échecs de mise à niveau FTD des versions 7.0 à 7.2, en particulier dans les déploiements haute disponibilité (HA).

Informations générales

Plus de la moitié de ces défaillances proviennent de problèmes survenus pendant la phase 200_enable_maintenance_mode, les validations de haute disponibilité existantes effectuant principalement des vérifications de base de l'état actif/veille, ce qui est insuffisant pour des transitions de haute disponibilité complètes.

Avec la mise à jour Secure Firewall 7.6, des validations de haute disponibilité améliorées ont été introduites pour résoudre ces problèmes. Ces améliorations incluent des vérifications approfondies des transitions d'état de haute disponibilité, des délais d'attente étendus pour les processus de synchronisation et des rapports d'erreurs améliorés. Cette mise à jour vise à réduire de manière significative les problèmes de haute disponibilité après la mise à niveau et les échecs de mise à niveau globaux, garantissant un processus de mise à niveau plus fluide et plus fiable pour les déploiements haute disponibilité.

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

Problème

- Les clients signalent un nombre important d'échecs de mise à niveau FTD dans les versions 7.0, 7.1 et 7.2 pour les déploiements haute disponibilité.
- Plus de 50 % des pannes proviennent de déploiements FTD HA. Les défaillances en mode 200_enable_maintenance_mode contribuent aux défaillances de haute disponibilité.
- Les validations d’état de haute disponibilité existantes sont des validations de base, telles que les vérifications d’état actif/veille, qui ne valident pas complètement les transitions de haute disponibilité.

Nouveautés (solution)

Validations HA améliorées pour la mise à niveau FTD :

- Validation de la transition d'état haute disponibilité
- Délais de mise à niveau FTD HA améliorés pour l'état de transition HA comme la synchronisation de configuration (7 200 secondes), la synchronisation d'application (1 200 secondes) et la synchronisation en bloc (7 200 secondes)
- Davantage de contrôle sur le démarrage ou l'échec de la mise à niveau FTD par FMC
- Amélioration des rapports d'erreurs et des messages de récupération pour les mises à niveau FTD HA

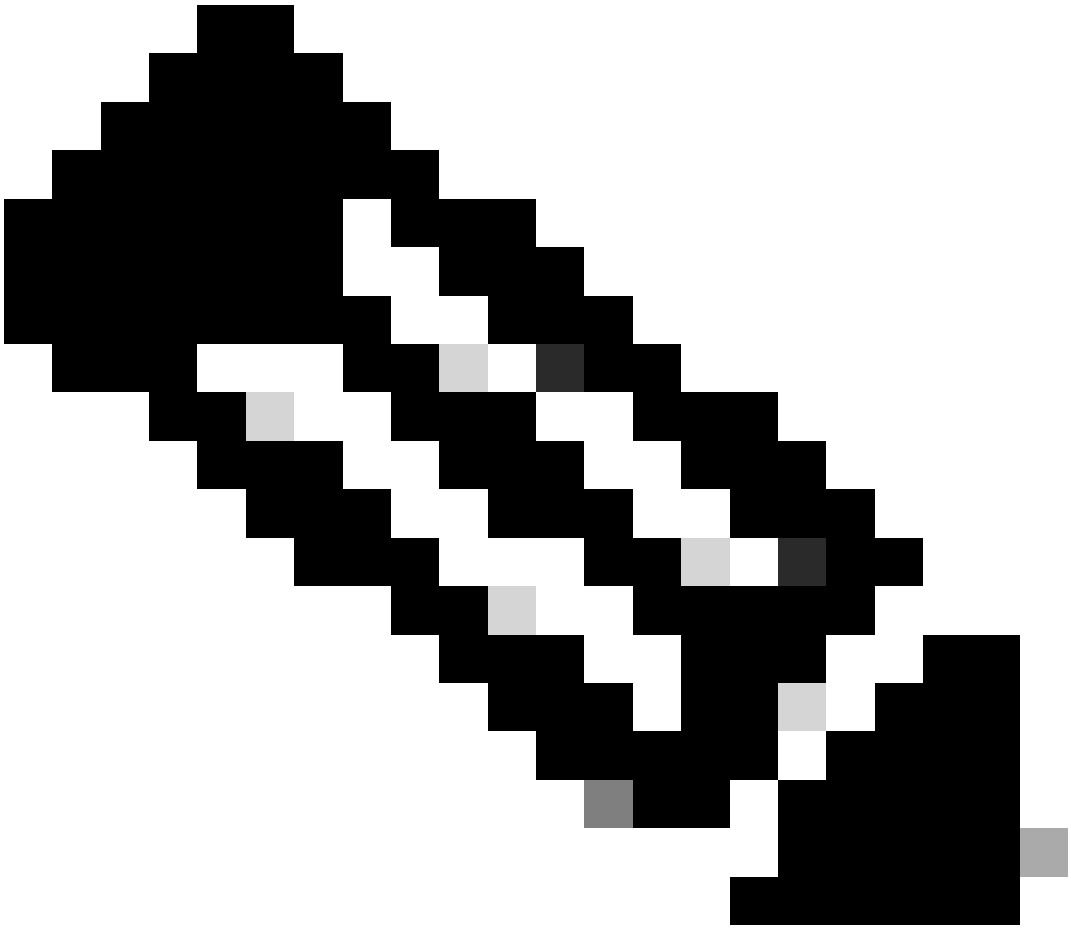
Par rapport aux versions précédentes, il a :

- Des validations de haute disponibilité améliorées permettent de réduire les problèmes de création de haute disponibilité post-mise à niveau dans les déploiements haute disponibilité
- Des validations améliorées permettent de réduire les échecs de mise à niveau FTD

Conditions préalables

Plates-formes prises en charge

- Responsable(s) et Version(s) : FMC 7.6.0
- Application (ASA/FTD) et version minimale de l'application : DFT 7.6.0 ; FMC gestion 7.6.0 FTD HA
- Plates-formes prises en charge: Toutes les plates-formes exécutant FTD HA

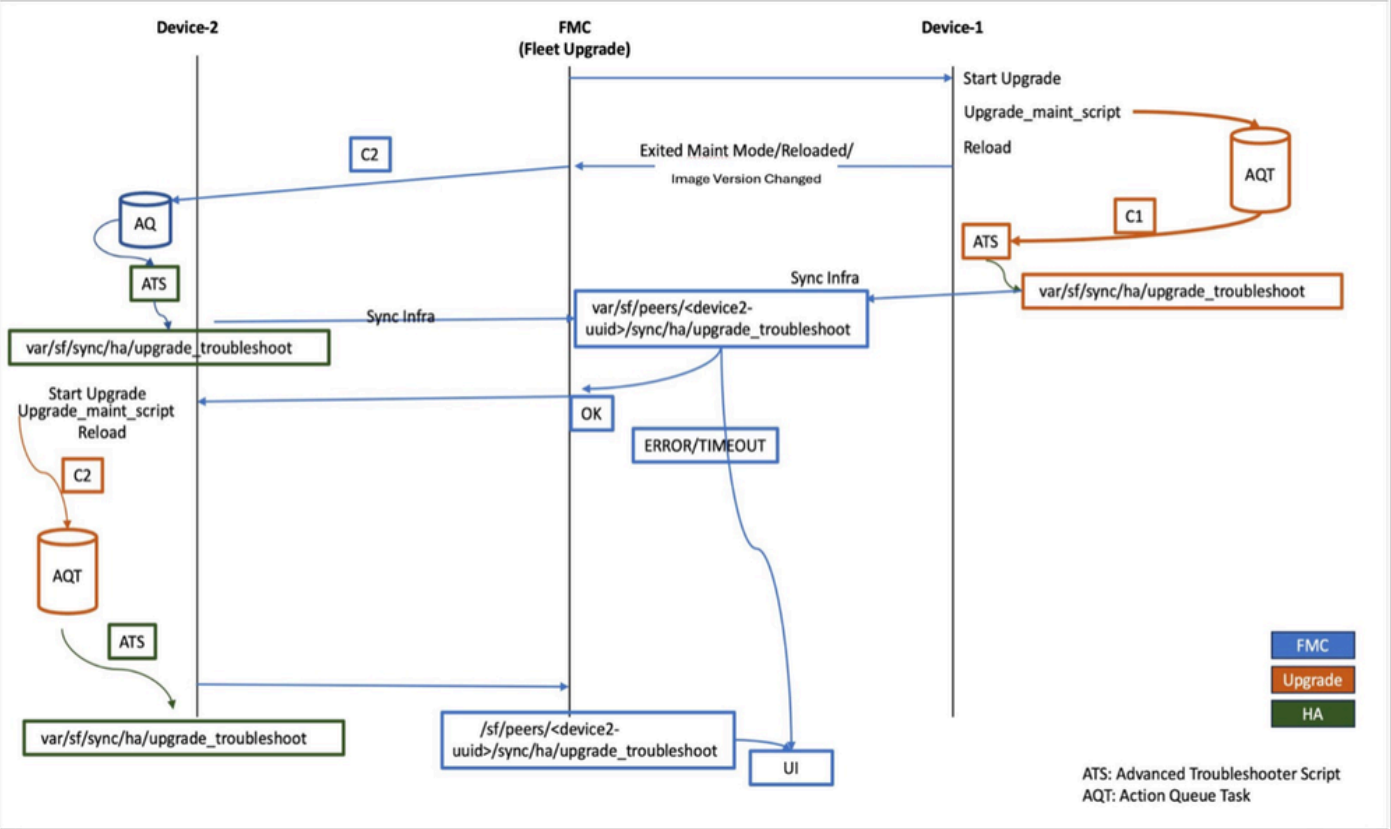


Remarque : Cette fonctionnalité s'applique uniquement aux déploiements FTD HA gérés par FMC. Cette fonctionnalité ne s'applique pas à la haute disponibilité FTD gérée par FDM ou aux périphériques en cluster.

Présentation des fonctionnalités

- Cette fonctionnalité permet de réduire les échecs de mise à niveau FTD dans le déploiement haute disponibilité en vérifiant les états haute disponibilité des unités mises à niveau par FMC après la partie de redémarrage du processus de mise à niveau.
- Après le redémarrage de la mise à niveau, FMC vérifie l'état actif/veille et les éventuelles défaillances de la synchronisation haute disponibilité.
- FTD avertit FMC du moment où démarrer ou échouer la mise à niveau sur le deuxième noeud sous la forme d'un nouveau dépannage avancé haute disponibilité.
- En cas d'échec lors du redémarrage de HA après la mise à niveau, un message approprié s'affiche sur l'interface utilisateur FMC.

Nouveau workflow de mise à niveau pour FTD HA



L'unité en veille est la première à être mise à niveau

Mise à niveau de la première unité (unité en veille)

- Lors de la première mise à niveau d'unité, le script de mise à niveau lance la tâche action_queue pour collecter les données de dépannage avancé haute disponibilité à l'étape 999_finish.
- L'exécution de la tâche insérée démarre uniquement après le redémarrage post-mise à niveau et collecte les informations de dépannage sous la forme d'un fichier JSON.
- Le même fichier JSON est synchronisé avec FMC.
- Une fois que le premier noeud quitte le mode maintenance, FMC déclenche une tâche action_queue distante sur l'unité active afin de collecter le dépannage avancé de haute disponibilité (l'unité active doit être 7.6 ou supérieure). Si l'unité active est trouvée inférieure

à 7,6, aucun dépannage n'est collecté à partir de l'unité active et FMC prend une décision basée uniquement sur le dépannage collecté à partir de l'unité en veille.

Une fois que le dépannage avancé haute disponibilité est collecté auprès des deux unités, FMC décide de démarrer la mise à niveau ou de bloquer la mise à niveau sur le deuxième noeud (unité active).

Mise à niveau de la deuxième unité (unité active)

- À l'instar de l'unité en veille, le script de mise à niveau lance la tâche action_queue pour collecter les informations de dépannage avancé haute disponibilité à l'étape 999_finish.
- L'exécution de la tâche insérée démarre uniquement après le redémarrage de la mise à niveau et génère des informations de dépannage sous la forme d'un fichier JSON.
- Le même fichier est synchronisé avec FMC.
- Si l'une des unités signale une défaillance HA, les données de défaillance HA sont affichées sur l'interface utilisateur FMC dans l'onglet de mise à niveau.
- En cas d'échec lors du redémarrage de la haute disponibilité après la mise à niveau, la mise à niveau est marquée comme terminée et, dans le même onglet de mise à niveau, les échecs de validation de la haute disponibilité sont signalés.

Dépannage avancé de HA

- Le dépannage avancé haute disponibilité est un nouveau fichier JSON unique introduit dans le cadre de cette fonctionnalité qui contient des informations haute disponibilité. Il est généré après le redémarrage après une mise à niveau et envoyé du FTD au FMC.
- Nom et chemin du fichier : /ngfw/var/sf/sync/ha/upgrade_troubleshoot
- Dès que FMC collecte le dépannage avancé haute disponibilité de la première unité (en veille), FMC déclenche une tâche à distance pour collecter les mêmes informations de l’unité active.
    - Cette collecte de données à distance est uniquement prise en charge lorsque les périphériques exécutent la version 7.6 ou ultérieure.
    - Si des périphériques exécutant une version antérieure à 7.6 sont détectés, la collecte de données à distance est ignorée. Ainsi, dans ce cas, FMC ne recueillerait que les données de l'unité en attente et déciderait des mesures à prendre.

- La génération de dépannage avancé haute disponibilité est rapide. Si Lina est en panne et ne parvient pas à générer le rapport, il se ferme immédiatement.
    - Le temps de redémarrage du périphérique dépend de la plate-forme et le temps de redémarrage est le même que celui que nous avons décrit pour chaque plate-forme.

Rapport de dépannage avancé HA

Chaque unité haute disponibilité génère des données de dépannage avancé haute disponibilité sous la forme d'un fichier JSON après le redémarrage de la mise à niveau et les partage avec FMC. Voici des exemples de validation en cas d'échec et de réussite.

Exemple d'échec de validation HA

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

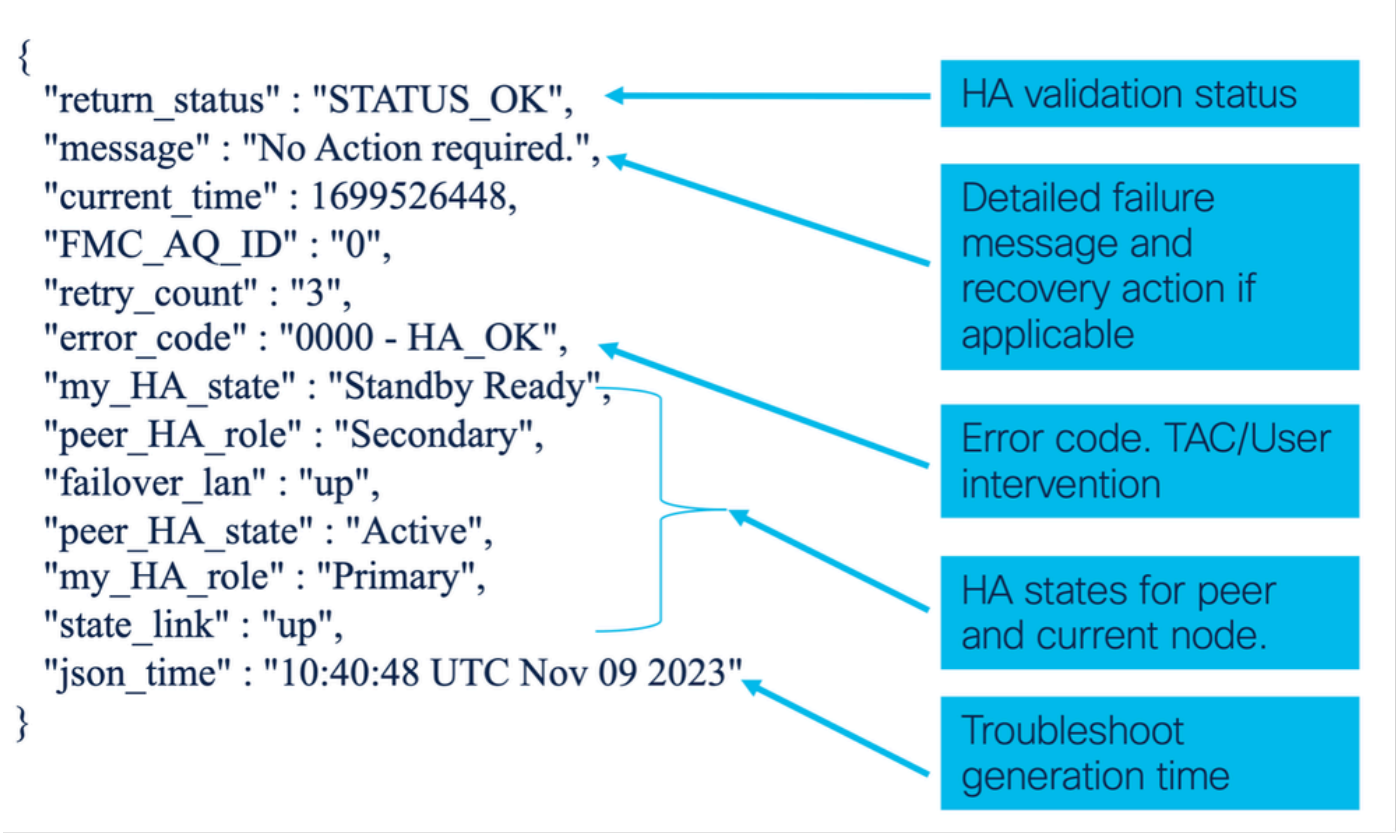

```
{
"failover_lan" : "NA",
"error_code" : "1046 -
STARTUP_FAILOVER_CONFIG_NOT_PRESENT",
"current_time" : 1701369637,
"peer_HA_state" : "Not Detected",
"FMC_AQ_ID" : "0",
"state_link" : "NA",
"json_time" : "18:40:37 UTC Nov 30 2023",
"my_HA_state" : "Disabled",
"my_HA_role" : "Secondary",
"return_status" : "STATUS_ERROR",
"message" : "Failover config is not present on the startup
config. Device is in standalone state. Please configure failover.",
"peer_HA_role" : "Primary"
}
```


Exemple de validation HA réussie

Fichier: /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
}
```


Contenu du dépannage avancé HA



Emplacement du fichier de dépannage avancé de HA

Emplacement du fichier JSON de dépannage avancé haute disponibilité :

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


        /sync/ha/upgrade_troubleshoot
```

- Le dépannage de la haute disponibilité repose sur la commande lina.
  - Si la génération du dépannage échoue dans /ngfw/var/sf/sync/ha/upgrade_troubleshoot, l'utilisateur peut consulter les journaux à l'adresse : /ngfw/var/log/ha_upgrade_troubleshoot.log
- Les fichiers /ngfw/var/sf/sync/ha/upgrade_troubleshoot et /ngfw/var/log/ha_upgrade_troubleshoot.log font partie du fichier FTD Troubleshoot.

Conseils pour les problèmes de génération de dépannage avancés HA

Parfois, le dépannage avancé haute disponibilité n'est pas généré en raison de l'état du système et la raison peut être lina down ou le processus de file d'attente d'action est down après le redémarrage de la mise à niveau. Si lina ou la file d'attente d'action est en panne, cela pose problème.

Dans de tels cas, vérifiez si les processus Lina et ActionQueue sont en cours d'exécution en utilisant cette commande en mode expert :

<#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
```

Statut et action de retour dans le dépannage avancé haute disponibilité

- INIT_ÉTAT : Cela indique que le dépannage de haute disponibilité a été déclenché.
- STATUS_OK : Le dispositif est dans un état stable. Aucune action n'est requise.
- ERREUR D'ÉTAT : Cela détermine qu'une erreur s'est produite en raison de laquelle la haute disponibilité n'est pas formée. L'utilisateur doit effectuer une action en fonction du message affiché ou il doit contacter le centre d'assistance technique.
- STATUS_RETRY : Le dispositif peut être dans l'un des états intermédiaires. Le dépannage de haute disponibilité continue à réessayer après un intervalle fixe basé sur l'état jusqu'à ce que STATUS_ERROR ou STATUS_OK soit rencontré.
    - En fonction des défaillances rencontrées dans STATUS ERROR, les défaillances de haute disponibilité sont classées en 2 cas :
        - Intervention de l'utilisateur : ces défaillances de haute disponibilité peuvent être corrigées par l'utilisateur et celui-ci peut reprendre la mise à niveau lorsque l'intervention du centre d'assistance technique n'est pas requise.
        - Intervention du CAT : pour ces défaillances de haute disponibilité, l'utilisateur ne peut pas y remédier seul ; Une intervention du TAC est requise.

Code d'erreur et classification

En fonction des codes d'erreur, les erreurs sont classées comme suit :

statut_retour	code_erreur	Description	Mécanisme de relance

			ou de récupération
ÉTAT_OK	«0000 - HA_OK»(Les valeurs réservées sont comprises entre 0001 et 1023)	C'est pour le scénario de réussite. (lorsque les états HA sont Actif et En veille)	(Sans objet)
ERREUR_ÉTAT	« 1024:2047 - ERROR_REASON »	Ceci est pour le scénario d'erreur (intervention de l'utilisateur)	Des messages exploitables à afficher à l'utilisateur et à la structure de mise à niveau peuvent ajouter le mécanisme de nouvelle tentative ou de récupération à l'avenir (le cas échéant).
ERREUR_ÉTAT	« 2048:3071 - ERROR_REASON »	Ceci est pour le scénario d'erreur (intervention du TAC)	Une intervention du TAC est nécessaire pour le rétablissement.

Messages d'intervention utilisateur

Erreur	Message d'erreur	« Error Code
'FAILOVER_CONFIG_NOT_PRESENT'	"La configuration du basculement n'est pas présente sur le périphérique"	"1024"
'FAILOVER_IS_NOT_ENABLED'	"Le basculement n'est pas activé sur le périphérique. Activez le basculement.	"1025"
'BASCULEMENT_LAN_DOWN'	"Le LAN de basculement est hors service sur le	"1026"

	périphérique"	
'LIEN_ÉTAT_INACTIF'	"La liaison d'état est désactivée sur le périphérique"	"1027"
'ÉPUISEMENT_BLOC_BASCULEMENT'	"Épuisement des blocs sur les blocs suivants du périphérique : \n"	"1028"
'APP_SYNC_TIMEOUT'	"Délai de synchronisation de l'application sur l'appareil"	"1029"
'CD_APP_SYNC_ERROR'	"Erreur de synchronisation de l'application CD détectée sur l'appareil"	"1030"
'CONFIG_SYNC_TIMEOUT'	"Délai de synchronisation de la configuration sur le périphérique"	"1031"
'FAILED_TO_APPLY_CONFIG'	"Échec de l'application de la configuration sur le périphérique"	"1032"
'DÉLAI_SYNCHRONISATION_EN BLOC'	"Délai de synchronisation en bloc sur le périphérique"	"1033"
'PROBLÈME_CLIENT_SYNCHRONISATION_EN BLOC'	"Vérifiez les clients suivants sur le périphérique : \n"	"1034"
'ÉCHEC_VÉRIFICATION_IFC'	"La vérification de l'interface de basculement a échoué	"1035"

	sur les interfaces suivantes du périphérique : \n"	
'IFC_FAILED_CHECK_VLAN_SPANTREE'	"Puisque les interfaces sont actives. Vérifiez si les VLAN sont autorisés côté commutateur ou s'il y a un problème de Spanning Tree.	"1036"
'VERSION_MISMATCH'	"Version logicielle différente sur l'autre périphérique"	"1037"
'MODE_MISMATCH'	"Mode de fonctionnement différent sur l'autre périphérique"	"1038"
'LIC_MISMATCH'	"Licence différente sur l'autre périphérique"	"1039"
'INCOMPATIBILITÉ_CHÂSSIS'	"Configuration de châssis différente sur l'autre périphérique"	"1040"
'DISCORDANCE_CARTE'	"Configuration de carte différente sur l'autre périphérique"	"1041"
'PEER_NOT_OK'	« Cet appareil est à l'état OK. Vérifier le périphérique homologue"	"1042"

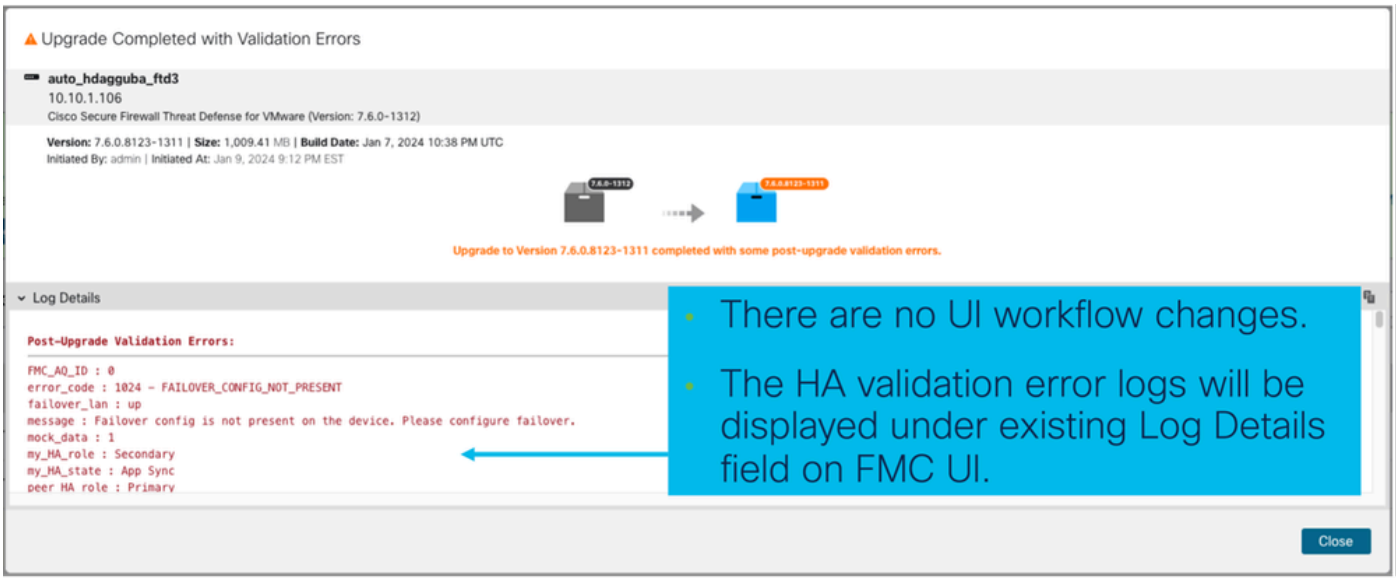
Messages d'intervention TAC

Erreur	Message d'erreur	« Error Code

'ÉCHEC_RUN_CMD'	"Echec de l'exécution de la commande"	"2048"
'LINA_NOT_STARTED'	"Lina n'a pas démarré sur l'appareil. Réessayez après un certain temps"	"2049"'
'HWIDB_MISMATCH'	"L'index HWIDB est différent sur le périphérique"	"2050"
'ÉCHEC_FOND_DE PANIER'	"Panne du fond de panier sur le périphérique. Vérifiez le fond de panier.	"2051"
'HA_PROGR_FAILURE'	"Échec de progression HA sur le périphérique"	"2052"
'ÉCHEC_SVM'	"Échec du module de service sur le périphérique"	"2053"
'SVM_MIO_HB_FAILURE'	"Échec de pulsation entre MIO et App-agent sur le périphérique"	"2054"
'ÉCHEC_SVM_MIO_CRUZ'	"Panne de la carte réseau de la carte MIO sur le périphérique"	"2055"
'SVM_MIO_HB_CRUZ_FAILED'	"Pulsation de la carte MIO et défaillance de la carte réseau sur le périphérique"	"2056"
'ÉCHEC_CARTE_SSM'	"Défaillance de la carte de service sur le périphérique"	"2057"

'ÉCHEC_COMM_MY'	"Échec de la communication sur le périphérique"	"2058"
'PROCESSUS_CRITIQUE_DÉCÉDÉ'	"Le processus critique est mort sur le périphérique"	"2059"
'ÉCHEC_SNORT'	"Echec de la commande Snort sur le périphérique"	"2060"
'PEER_SVM_FAILURE'	"Le module de service NGFW est tombé en panne sur l'autre périphérique"	"2061"
'PROFONDEUR_BLOC_MON_DÉFAILLANCE'	"La surveillance des pannes a signalé un épuisement des blocs sur le périphérique"	"2062"
'ÉCHEC_DISQUE'	"Le disque a échoué sur le périphérique"	"2063"
'ÉCHEC_SNORT_DiSK'	"Echec de la commande Snort and Disk sur le périphérique	"2064"
'INACTIVE_MATE_FOUND"	"Détection d'un partenaire inactif au démarrage	"2065"
'SCRIPT_TIMEOUT'	"Limite de tentatives dépassée. Sortie du script"	"2066"
'ERREUR_INCONNUE'	"Impossible d'identifier l'erreur"	"2067"

Modifications de l'interface utilisateur Firewall Management Center



Architecture logicielle

Cette fonctionnalité dépend fortement du cadre de file d'attente d'actions existant. La fonctionnalité utilise l'interface CLI de Lina sous-jacente pour générer les données de dépannage avancé de la haute disponibilité.

FAQ

Q : La fonctionnalité est-elle applicable à la fonctionnalité de retour de mise à niveau FTD ?
A : Non. Cette fonctionnalité n'est pas applicable à la fonctionnalité de retour car le retour FTD fonctionne en parallèle, et non 1 par 1.

Q : Si la mise à niveau échoue sur 200_enable_maintenance_mode.pl, génère-t-elle les données de dépannage avancées ?
A : Non. Le dépannage avancé de la haute disponibilité est généré uniquement après le redémarrage post-mise à niveau et non lors d'un échec de mise à niveau

Q : Si la mise à niveau est bloquée en raison des validations de haute disponibilité sur la seconde unité, un utilisateur peut-il déclencher la mise à niveau sur la seconde unité uniquement ?
A : Oui. L'utilisateur doit sélectionner à nouveau la paire haute disponibilité pour la mise à niveau et FMC déclenche la mise à niveau uniquement sur l'unité non mise à niveau.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.