Reducción del fallo de actualización de Secure Firewall 7.6 FTD HA

Contenido

- Introducción
- Antecedentes
- Problema
- Novedades (solución)
- Prerequisites
  - Plataformas Soportadas
- Descripción general de características
- Nuevo flujo de trabajo de actualización para FTD HA
- La unidad en espera es la primera en actualizarse
  - Actualización de la primera unidad (unidad en espera)
  - Actualización de segunda unidad (unidad activa)
- Solución de problemas avanzados de HA
- Informe de solución de problemas avanzada de HA
  - Ejemplo de fallo de validación de HA
  - Ejemplo de validación de HA satisfactoria
- Contenido de solución de problemas avanzados de HA
- Ubicación del archivo de resolución de problemas avanzada de HA
- Consejos para problemas de generación de problemas avanzados de HA
  - Estado y acción de devolución en la resolución de problemas avanzada de HA
- Código de error y clasificación
  - Mensajes de intervención del usuario
  - Mensajes de intervención del TAC
- Cambios en la IU de Firewall Management Center
  - Arquitectura del software
- Preguntas más Frecuentes

Introducción

Este documento describe la solución de problemas para solucionar los errores de actualización de FTD de las versiones 7.0 a 7.2, especialmente en implementaciones de alta disponibilidad (HA).

Antecedentes

Más de la mitad de estos fallos se deben a problemas durante la fase 200_enable_maintenance_mode, en la que las validaciones de HA existentes realizan principalmente comprobaciones básicas del estado activo/en espera, que son insuficientes para transiciones de HA completas.

Con la actualización de Secure Firewall 7.6, se han introducido validaciones de HA mejoradas para abordar estos problemas. Estas mejoras incluyen comprobaciones exhaustivas de las transiciones de estado de HA, tiempos de espera extendidos para los procesos de sincronización y mejores informes de errores. Esta actualización tiene como objetivo reducir significativamente los problemas de HA posteriores a la actualización y los fallos de actualización generales, garantizando un proceso de actualización más fluido y fiable para las implementaciones de HA.

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

Problema

- Hay un número significativo de fallos de actualización de FTD notificados por los clientes en las versiones 7.0, 7.1 y 7.2 para implementaciones de HA.
- Más del 50% de los fallos provienen de implementaciones de HA de FTD. Las fallas en 200_enable_maintenance_mode contribuyen a las fallas de HA.
- Las validaciones de estado de HA existentes son validaciones básicas, como las comprobaciones de estado activo/en espera, y no validan por completo las transiciones de HA.

Novedades (solución)

Validaciones de HA mejoradas para la actualización de FTD:

- Validación para transición de estado de HA
- Tiempos de espera de actualización de FTD HA mejorados para el estado de transición de HA, como config sync (7200 segundos), app sync (1200 segundos) y bulk sync (7200 segundos)
- Proporciona más control al FMC sobre cuándo iniciar o no la actualización del FTD.
- Notificación de errores y mensaje de recuperación mejorados para actualizaciones de FTD HA

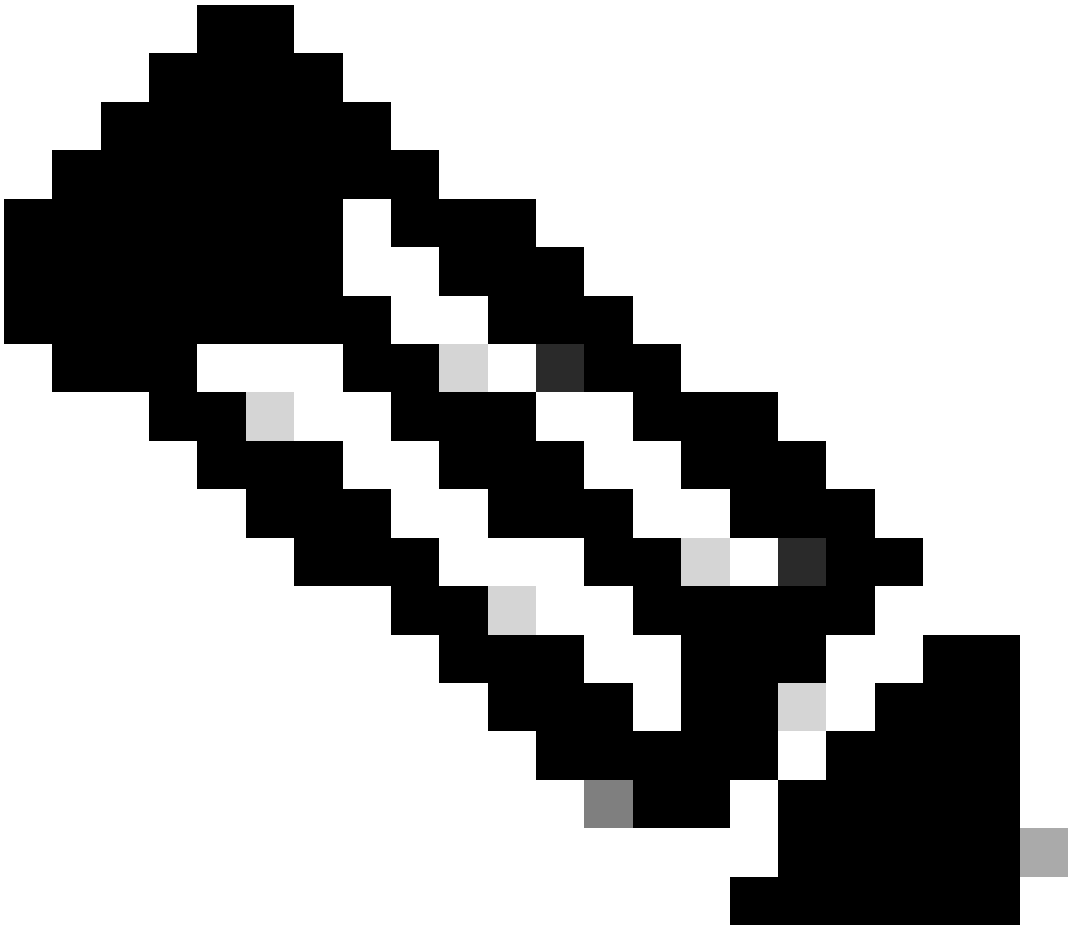
En comparación con las versiones anteriores, cuenta con:

- Las validaciones de HA mejoradas ayudan a reducir los problemas de creación de HA posteriores a la actualización en implementaciones de HA
- Las validaciones mejoradas ayudan a reducir los fallos de actualización de FTD

Prerequisites

Plataformas Soportadas

- Administrador(es) y versión(es): FMC 7.6.0
- Aplicación (ASA/FTD) y versión mínima de la aplicación: FTD 7.6.0; CSP que gestionan 7.6.0 FTD HA
- Plataformas Soportadas: Todas las plataformas que ejecutan FTD HA

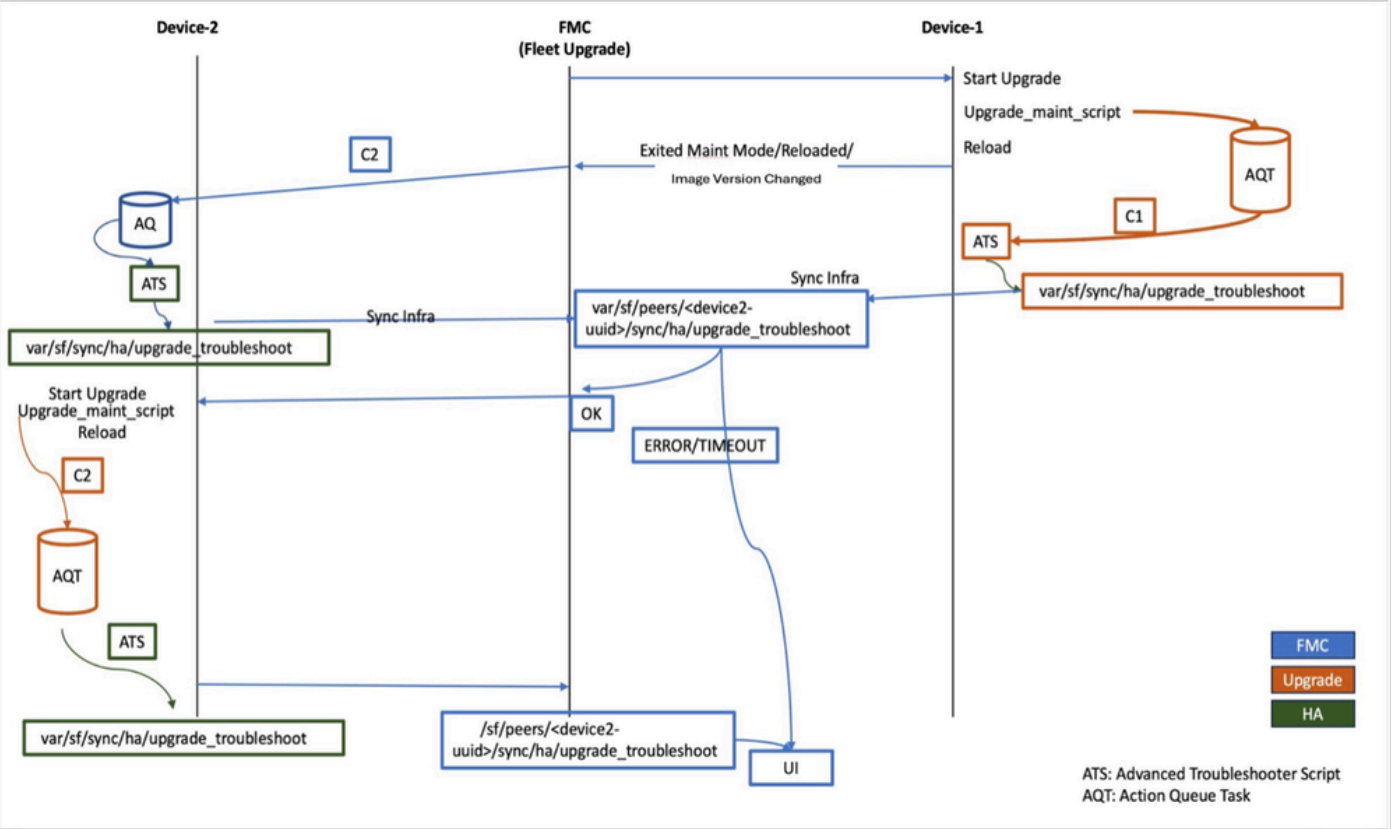


Nota: Esta función solo se aplica a las implementaciones de FTD HA gestionadas por FMC. Esta función no se aplica a FTD HA administrado por FDM ni a los dispositivos agrupados.

Descripción general de características

- Esta función ayuda a reducir los fallos de actualización de FTD en la implementación de HA mediante la comprobación de los estados de HA de las unidades actualizadas por FMC después de la parte de reinicio del proceso de actualización.
- Después del reinicio de la actualización, FMC verifica el estado activo/en espera y cualquier falla en la sincronización de HA.
- El FTD notifica al FMC cuándo iniciar o fallar la actualización en el segundo nodo en forma de una nueva solución de problemas de avance de HA.
- Si se produce algún error al incorporarse al reinicio posterior a la actualización de HA, se muestra un mensaje adecuado en la interfaz de usuario de FMC.

Nuevo flujo de trabajo de actualización para FTD HA



La unidad en espera es la primera en actualizarse

Actualización de la primera unidad (unidad en espera)

- Durante la actualización de la primera unidad, el script de actualización inicia la tarea action_queue para recopilar los datos de solución de problemas avanzados de HA en la etapa 999_finish.
- La ejecución de la tarea insertada se inicia solamente después del reinicio posterior a la actualización y recopila la información de solución de problemas en forma de archivo JSON.
- El mismo archivo JSON se sincroniza con FMC.
- Una vez que el primer nodo sale del modo de mantenimiento, FMC acciona una tarea action_queue remota en la unidad activa para recopilar la resolución de problemas avanzada de HA (la unidad activa debe ser 7.6 o superior). Si la unidad activa se encuentra

por debajo de 7.6, no se recopila ninguna resolución de problemas de la unidad activa y el FMC toma la decisión basándose únicamente en la resolución de problemas recopilada de la unidad en espera.

Una vez que se recopila la resolución de problemas de avance de HA de ambas unidades, FMC decide iniciar la actualización o bloquear la actualización en el segundo nodo (unidad activa).

Actualización de segunda unidad (unidad activa)

- De forma similar a la unidad en espera, el script de actualización inicia la tarea action_queue para recopilar los problemas de avance de HA en la etapa 999_finish.
- La ejecución de tareas insertadas sólo se inicia tras el reinicio de la actualización y genera información de solución de problemas en forma de archivo JSON.
- El mismo archivo se sincroniza con FMC.
- Si alguna de las unidades informa de un fallo de HA, los datos de fallo de HA se muestran en la interfaz de usuario de FMC en la ficha de actualización.
- En caso de que se produzca algún error al incorporarse al reinicio posterior a la actualización de HA, la actualización se marca como completada y, en la misma ficha de actualización, se notifican los errores de validación de HA.

Solución de problemas avanzados de HA

- La solución de problemas avanzada de HA es un nuevo archivo JSON único introducido como parte de esta función que contiene información de HA. Se genera después del reinicio después de una actualización y se envía desde el FTD al FMC.
- Nombre de archivo y ruta: /ngfw/var/sf/sync/ha/upgrade_troubleshoot
- Tan pronto como el FMC recopila la resolución de problemas avanzada de HA de la primera unidad (en espera), el FMC activa una tarea remota para recopilar la misma información de la unidad activa.
    - Esta recopilación de datos remota solo se admite cuando los dispositivos ejecutan la versión 7.6 o superior.
    - Si se encuentra que los dispositivos ejecutan una versión inferior a 7.6, se omite la recopilación de datos remotos. Por lo tanto, en este caso, el CSP solo recopilaría datos de la unidad en espera y decidiría qué medidas tomar.

- La generación de resolución de problemas avanzada de HA es rápida. Si Lina está inactiva y no puede generar el informe, se cerrará inmediatamente.
    - El tiempo de reinicio del dispositivo depende de la plataforma y el tiempo de reinicio es el mismo que hemos documentado para cada plataforma.

Informe de solución de problemas avanzada de HA

Cada unidad de HA genera un avance de HA para solucionar problemas de datos en forma de reinicio posterior a la actualización del archivo JSON y lo comparte con FMC. A continuación se muestran ejemplos de validación en los que se ha producido un error y un éxito.

Ejemplo de fallo de validación de HA

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

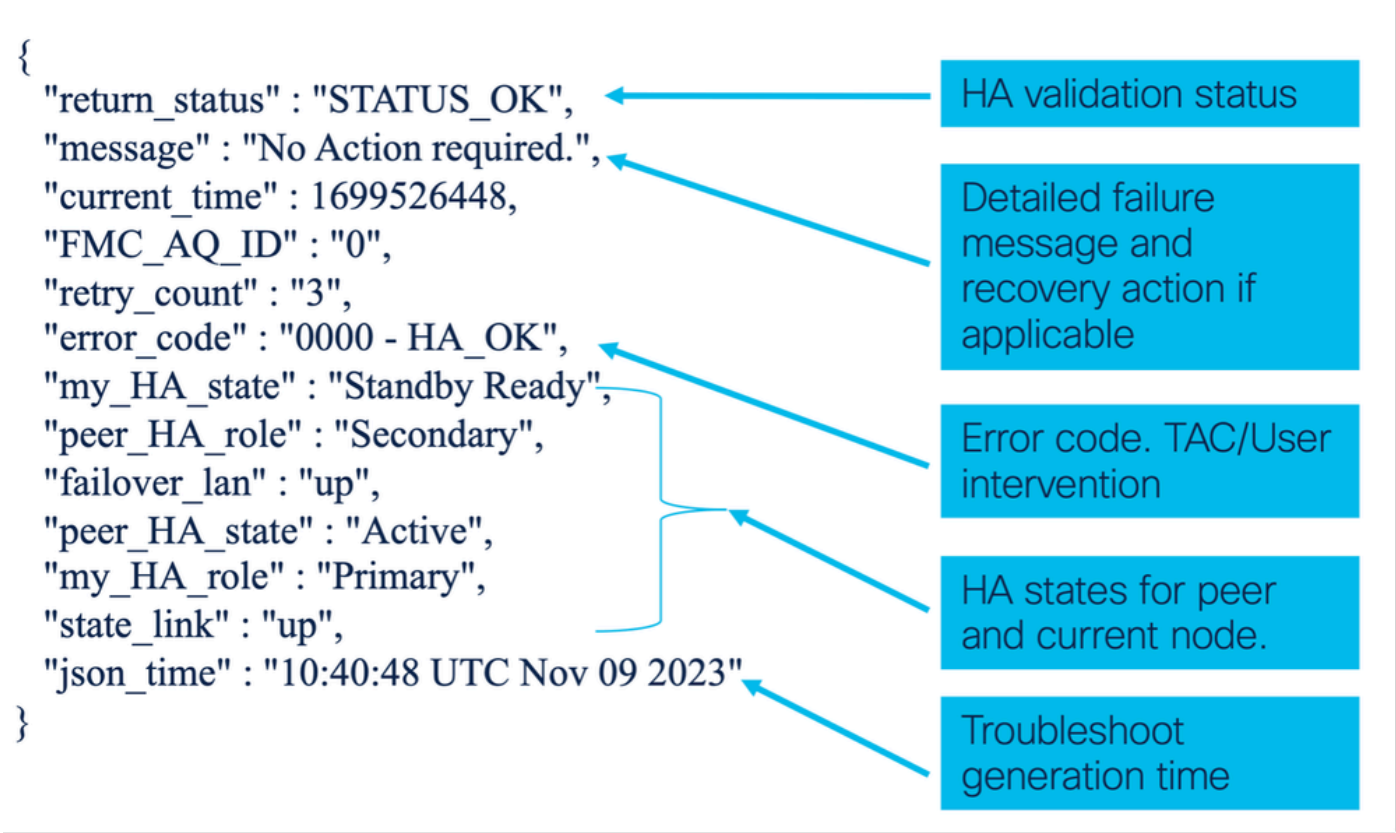

```
{
"failover_lan" : "NA",
"error_code" : "1046 -
STARTUP_FAILOVER_CONFIG_NOT_PRESENT",
"current_time" : 1701369637,
"peer_HA_state" : "Not Detected",
"FMC_AQ_ID" : "0",
"state_link" : "NA",
"json_time" : "18:40:37 UTC Nov 30 2023",
"my_HA_state" : "Disabled",
"my_HA_role" : "Secondary",
"return_status"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


Ejemplo de validación de HA satisfactoria

Archivo: /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
}
```


Contenido de solución de problemas avanzados de HA



Ubicación del archivo de resolución de problemas avanzada de HA

HA advanced Troubleshoot JSON file location:

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

        /sync/ha/upgrade_troubleshoot
```

- La resolución de problemas de HA se basa en el comando lina.
  - Si el troubleshooting no se genera en /ngfw/var/sf/sync/ha/upgrade_Troubleshoot, el usuario puede consultar los registros en: /ngfw/var/log/ha_upgrade_troubleshoot.log
- Los archivos /ngfw/var/sf/sync/ha/upgrade_Troubleshoot y /ngfw/var/log/ha_upgrade_troubleshoot.log forman parte del archivo de solución de problemas de FTD.

Consejos para problemas de generación de problemas avanzados de HA

A veces, la resolución de problemas avanzada de HA no se genera debido al estado del sistema y la razón de esto podría ser que el proceso de cola de acciones está inactivo después del reinicio de la actualización. Si la línea o la cola de acciones están inactivas, esto es un problema.

En estos casos, verifique si los procesos Line y ActionQueue se están ejecutando mediante este comando en el modo experto:

<#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
```

Estado y acción de devolución en la resolución de problemas avanzada de HA

- STATUS_INIT: Esto indica que se ha activado la resolución de problemas de HA.
- STATUS_OK: El dispositivo se encuentra en un estado estable. No se requiere ninguna acción.
- ERROR DE ESTADO: Esto determina que se ha producido un error debido al cual no se ha formado HA. El usuario debe realizar una acción basada en el mensaje mostrado o debe ponerse en contacto con el TAC.
- STATUS_RETRY: El dispositivo puede estar en uno de los estados intermedios. La solución de problemas de HA se reintenta después de un intervalo fijo basado en el estado hasta que se encuentra STATUS_ERROR o STATUS_OK.
    - Según los fallos encontrados en STATUS ERROR, los fallos de HA se clasifican en 2 casos:
        - Intervención del usuario: el usuario puede corregir estos fallos de HA y el usuario puede reanudar la actualización cuando no se requiera la intervención del TAC.
        - Intervención del TAC: para estos fallos de HA, el usuario no puede corregirlos por sí mismo. Se requiere la intervención del TAC.

Código de error y clasificación

Según los códigos de error, los errores se clasifican como se muestra a continuación:

return_status	error_code	Descripción	Mecanismo de reintento o recuperación

STATUS_OK	"0000 - HA_OK"(Los valores reservados son de 0001 - 1023)	Esto es para el escenario de éxito. (donde los estados de HA son Activo y Preparado para Standby)	(No aplicable)
STATUS_ERROR	"1024:2047 - ERROR_REASON"	Esto es para el escenario de error (intervención del usuario)	Los mensajes procesables que se mostrarán al usuario y al marco de actualización pueden agregar el mecanismo de reintento o recuperación en el futuro (si lo hubiera).
STATUS_ERROR	"2048:3071 - ERROR_REASON"	Esto es para el escenario de error (intervención del TAC)	La recuperación requiere la intervención del TAC.

Mensajes de intervención del usuario

Error	Mensaje de error	Código de error
'FAILOVER_CONFIG_NOT_PRESENT'	"La configuración de conmutación por error no está presente en el dispositivo"	"1024"
'FAILOVER_IS_NOT_ENABLED'	"La conmutación por fallo no está habilitada en el dispositivo. Habilite la conmutación por error"	"1025"
'FAILOVER_LAN_DOWN'	"La LAN de conmutación por error no funciona en el dispositivo"	"1026"

'STATE_LINK_DOWN'	"El enlace de estado no funciona en el dispositivo"	"1027"
'FAILOVER_BLOCK_DEPLETION'	"Agotamiento de bloques en los siguientes bloques del dispositivo:\n"	"1028"
'APP_SYNC_TIMEOUT'	"Tiempo de espera de sincronización de aplicaciones en el dispositivo"	"1029"
'CD_APP_SYNC_ERROR'	"Error de sincronización de la aplicación de CD detectado en el dispositivo"	"1030"
'CONFIG_SYNC_TIMEOUT'	"Tiempo de espera de sincronización de configuración en el dispositivo"	"1031"
'FAILED_TO_APPLY_CONFIG'	"Error al aplicar la configuración en el dispositivo"	"1032"
'BULK_SYNC_TIMEOUT'	"Tiempo de espera de sincronización masiva en el dispositivo"	"1033"
'BULK_SYNC_CLIENT_ISSUE'	"Compruebe los siguientes clientes en el dispositivo:\n"	"1034"
'IFC_CHECK_FAILED'	"Error en la comprobación de la interfaz de conmutación por error en las siguientes interfaces del dispositivo:\n"	"1035"

'IFC_FAILED_CHECK_VLAN_SPANTREE'	"Ya que las interfaces están activas. Verifique si las VLAN están permitidas en el lado del switch o si hay un problema de árbol de expansión"	"1036"
'VERSION_MISMATCH'	"Versión de software diferente en el otro dispositivo"	"1037"
'MODE_MISMATCH'	"Modo de funcionamiento diferente en el otro dispositivo"	"1038"
'LIC_MISMATCH'	"Licencia diferente en el otro dispositivo"	"1039"
'CHASSIS_MISMATCH'	"Configuración de chasis diferente en el otro dispositivo"	"1040"
'CARD_MISMATCH'	"Configuración de tarjeta diferente en el otro dispositivo"	"1041"
'PEER_NOT_OK'	"Este dispositivo se encuentra en el estado Correcto. Comprobar el dispositivo par"	"1042"

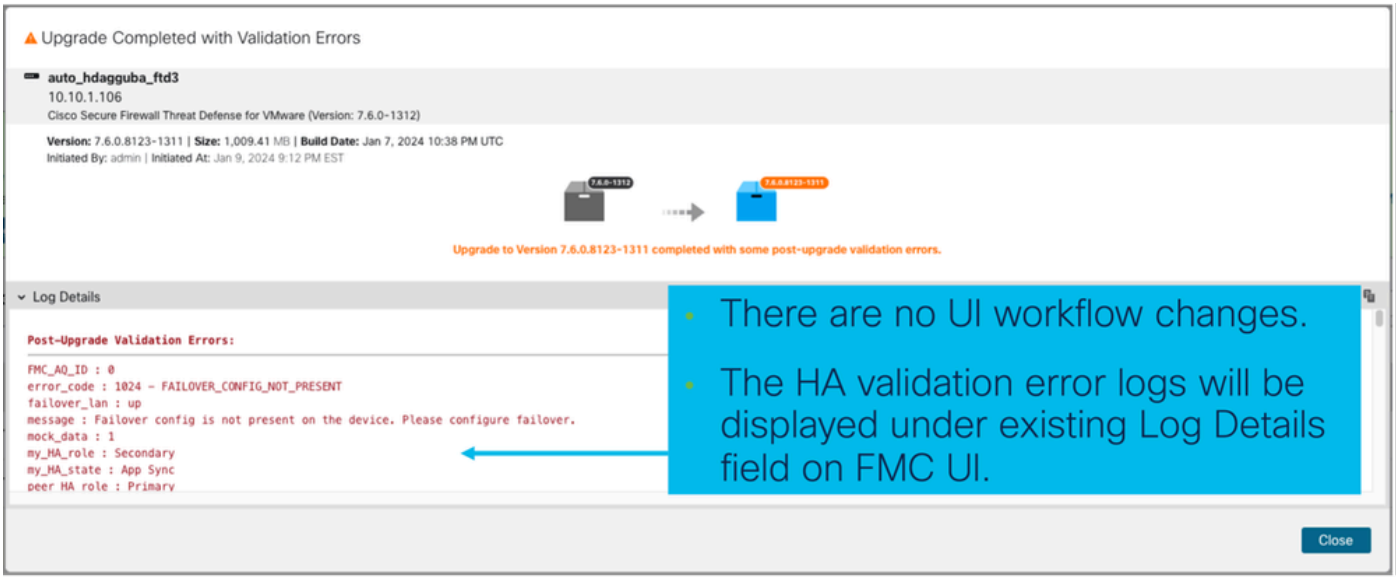
Mensajes de intervención del TAC

Error	Mensaje de error	Código de error
'RUN_CMD_FAILED'	"Error al ejecutar el comando"	"2048"
'LINA_NOT_STARTED'	"Lina no se inició en el dispositivo. Inténtelo de nuevo	"2049"'

	más tarde"	
'HWIDB_MISMATCH'	"El índice HWIDB es diferente en el dispositivo"	"2050"
'BACKPLANE_FAILURE'	"Fallo de placa base en el dispositivo. Compruebe el backplane"	"2051"
'HA_PROGR_FAILURE'	"Fallo de progresión de HA en el dispositivo"	"2052"
'SVM_FAILURE'	"Error del módulo de servicio en el dispositivo"	"2053"
'SVM_MIO_HB_FAILURE'	"Error de latido entre MIO y el agente de aplicaciones en el dispositivo"	"2054"
'SVM_MIO_CRUZ_FAILED'	"Fallo del adaptador de red MIO-blade en el dispositivo"	"2055"
'SVM_MIO_HB_CRUZ_FAILED'	"Latido del blade MIO y fallo del adaptador de red en el dispositivo"	"2056"
'SSM_CARD_FAILURE'	"Fallo de la tarjeta de servicio en el dispositivo"	"2057"
'MY_COMM_FAILURE'	"Fallo de comunicación en el dispositivo"	"2058"
'CRITICAL_PROCESS_DIED'	"El proceso crítico ha muerto en el dispositivo"	"2059"
'SNORT_FAILURE'	"Error de Snort en el dispositivo"	"2060"

'PEER_SVM_FAILURE'	"El módulo de servicio de NGFW ha fallado en el otro dispositivo"	"2061"
'FAULT_MON_BLOCK_DEP'	"Supervisión de fallos informó de agotamiento de bloques en el dispositivo"	"2062"
'DISK_FAILURE'	"Error de disco en el dispositivo"	"2063"
'SNORT_DiSK_FAILURE'	"Snort y disco fallaron en el dispositivo	"2064"
'INACTIVE_MATE_FOUND"	"Se detectó un mate inactivo durante el arranque	"2065"
'SCRIPT_TIMEOUT'	"Se ha superado el límite de reintentos. Saliendo del script"	"2066"
'ERROR_UNKNOWN'	"Error al identificar el error"	"2067"

Cambios en la IU de Firewall Management Center



Arquitectura del software

Esta característica depende en gran medida del marco de cola de acciones existente. La función

utiliza la línea subyacente CLI para generar los datos de resolución de problemas avanzados de HA.

Preguntas más Frecuentes

A: ¿La función es aplicable a la función de reversión de actualización de FTD?
R: No. Esta función no se aplica a la función de reversión, ya que la reversión de FTD funciona en paralelo, no de 1 por 1.

A: Si la actualización falla en 200_enable_maintenance_mode.pl, ¿genera los datos de resolución de problemas avanzada?
R: No. La resolución de problemas avanzada de HA se genera solamente después del reinicio posterior a la actualización y no durante el fallo de la actualización

A: Si la actualización se bloquea debido a las validaciones de HA en la segunda unidad, ¿puede un usuario accionar la actualización en la segunda unidad solamente?
R: Yes. El usuario tiene que seleccionar el par HA nuevamente para la actualización y FMC acciona la actualización solamente en la unidad no actualizada.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).