Riduzione degli errori di aggiornamento di Secure Firewall 7.6 FTD HA

Sommario

Introduzione

Questo documento descrive la risoluzione dei problemi per risolvere gli errori di aggiornamento FTD dalle versioni 7.0 alla 7.2, in particolare nelle distribuzioni ad alta disponibilità (HA).

Premesse

Oltre la metà di questi errori deriva da problemi durante la fase 200_enable_maintenance_mode, con convalide HA esistenti che eseguono principalmente controlli di base dello stato attivo/standby, insufficienti per transizioni HA complete.

Con l'aggiornamento Secure Firewall 7.6, sono state introdotte convalide HA migliorate per affrontare questi problemi. Tali miglioramenti includono controlli approfonditi delle transizioni di stato HA, timeout estesi per i processi di sincronizzazione e funzionalità avanzate di segnalazione degli errori. Questo aggiornamento mira a ridurre in modo significativo i problemi di elevata disponibilità post-aggiornamento e i problemi di aggiornamento complessivi, garantendo un processo di aggiornamento più fluido e affidabile per le installazioni di elevata disponibilità.

Migrazione eseguita da: https://confluence-eng-rtp2.cisco.com/conf/display/IFT/FTD+HA+Upgrade+Failure+Reduction

Problema

- Nelle release 7.0, 7.1 e 7.2, i clienti segnalano un numero significativo di errori di aggiornamento FTD per le implementazioni HA.
- Oltre il 50% dei guasti deriva da implementazioni FTD HA. Gli errori in 200_enable_maintenance_mode contribuiscono agli errori HA.
- Le convalide dello stato HA esistenti sono convalide di base, come i controlli dello stato attivo/standby, e non convalidano completamente le transizioni HA.

Novità (soluzione)

Convalide HA migliorate per l'aggiornamento FTD:

- Convalida per la transizione dello stato HA
- Timeout di aggiornamento FTD HA migliorati per lo stato di transizione HA, ad esempio sincronizzazione della configurazione (7200 secondi), sincronizzazione dell'applicazione (1200 secondi) e sincronizzazione bulk (7200 secondi)
- Maggior controllo del FMC su quando avviare o non eseguire l'aggiornamento FTD
- Miglioramento della segnalazione degli errori e del messaggio di ripristino per gli aggiornamenti FTD HA

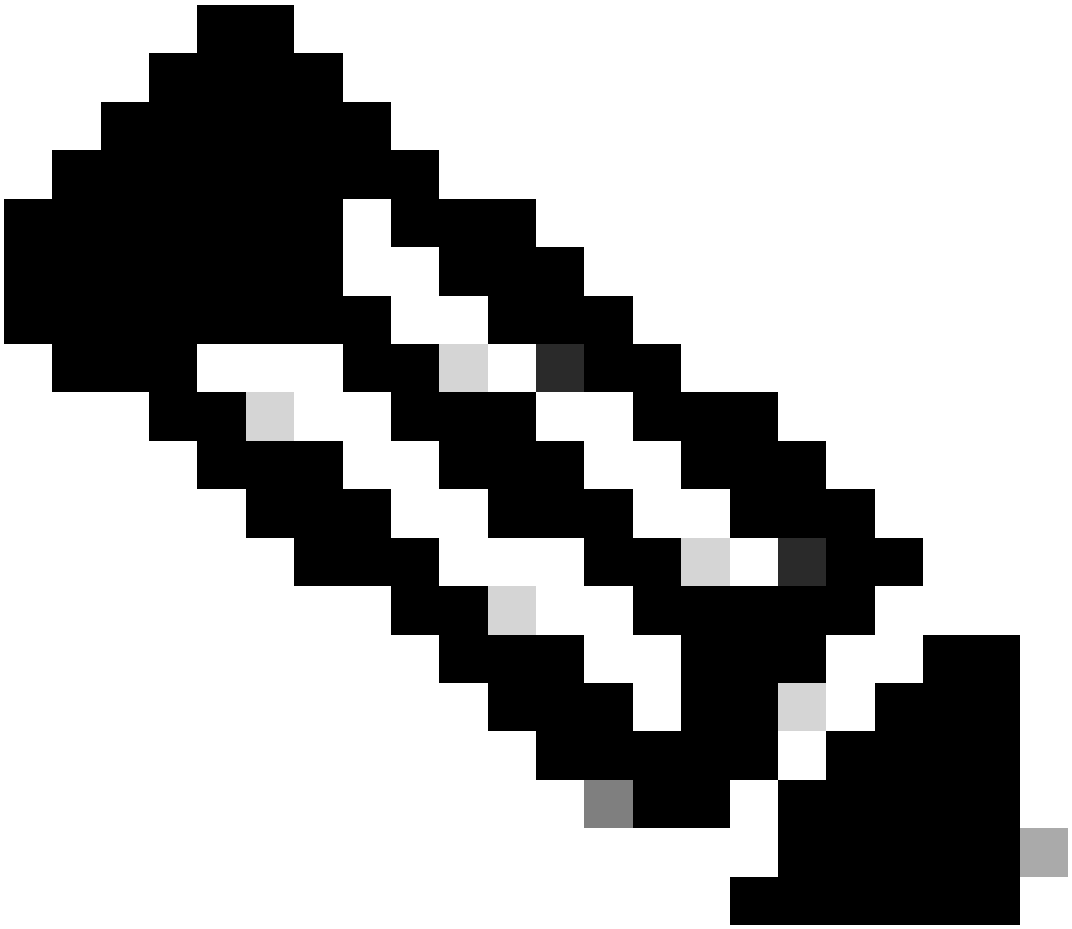
Rispetto alle versioni precedenti, offre:

- Le convalide HA migliorate consentono di ridurre i problemi di creazione di HA post-aggiornamento nelle installazioni HA
- Le convalide migliorate consentono di ridurre gli errori di aggiornamento FTD

Prerequisiti

Piattaforme supportate

- Responsabili e versioni: FMC 7.6.0
- Applicazione (ASA/FTD) e versione minima dell'applicazione: FTD 7.6.0; FMC che gestisce 7.6.0 FTD HA
- Piattaforme supportate: Tutte le piattaforme con FTD HA



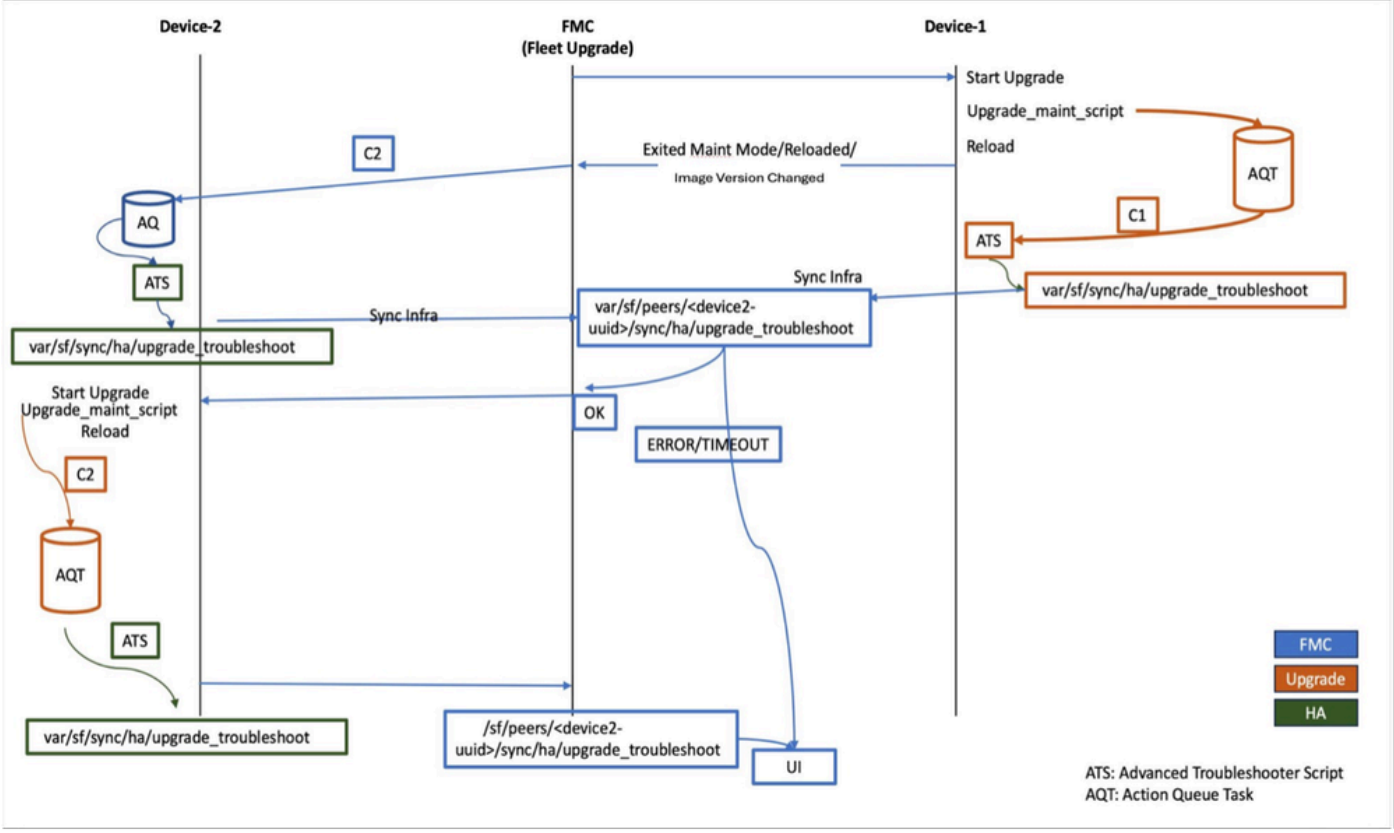
Nota: Questa funzionalità si applica solo alle distribuzioni HA FTD gestite da FMC. Questa funzionalità non è applicabile a FTD HA gestito da FDM o a dispositivi in cluster.

Panoramica delle funzionalità

- Questa funzionalità consente di ridurre gli errori di aggiornamento FTD nella distribuzione HA verificando gli stati HA delle unità aggiornate da FMC dopo la parte di riavvio del processo di aggiornamento.

- Dopo il riavvio dell'aggiornamento, FMC verifica lo stato attivo/standby e gli eventuali errori nella sincronizzazione HA.
- L'FTD notifica al FMC quando avviare o interrompere l'aggiornamento sul secondo nodo sotto forma di una nuova risoluzione avanzata dei problemi di HA.
- In caso di errori durante il riavvio successivo all'aggiornamento di HA, viene visualizzato un messaggio appropriato nell'interfaccia utente del CCP.

Nuovo flusso di lavoro di aggiornamento per FTD HA



L'unità di standby è la prima ad essere aggiornata

Aggiornamento della prima unità (unità di standby)

- Durante il primo aggiornamento dell'unità, lo script di aggiornamento avvia l'operazione action_queue per raccogliere i dati di risoluzione avanzata dei problemi HA nella fase 999_finish.
- L'esecuzione dell'attività inserita inizia solo dopo il riavvio successivo all'aggiornamento e raccoglie le informazioni sulla risoluzione dei problemi sotto forma di file JSON.
- Lo stesso file JSON viene sincronizzato con FMC.
- Una volta che il primo nodo esce dalla modalità di manutenzione, FMC attiva un'operazione action_queue remota sull'unità attiva per raccogliere la risoluzione avanzata dei problemi HA (l'unità attiva deve essere 7.6 o superiore). Se l'unità attiva risulta inferiore alla 7.6, non viene raccolta alcuna risoluzione dei problemi dall'unità attiva e il CCP prende una decisione solo in base alla risoluzione dei problemi raccolta dall'unità di standby.

Una volta raccolta la risoluzione avanzata dei problemi di HA da entrambe le unità, FMC decide di avviare l'aggiornamento o di bloccarlo sul secondo nodo (unità attiva).

Aggiornamento seconda unità (unità attiva)

- Analogamente all'unità in standby, lo script di aggiornamento avvia l'operazione action_queue per raccogliere l'avanzamento HA nella fase 999_finish.
- L'esecuzione dell'attività inserita avvia solo il riavvio successivo all'aggiornamento e genera informazioni per la risoluzione dei problemi sotto forma di file JSON.
- Lo stesso file viene sincronizzato con FMC.
- Se una delle unità segnala un errore HA, i dati relativi all'errore HA vengono visualizzati nell'interfaccia utente di FMC nella scheda di aggiornamento.
- In caso di errori durante l'unione al riavvio successivo all'aggiornamento di HA, l'aggiornamento viene contrassegnato come completato e nella stessa scheda di aggiornamento vengono segnalati errori di convalida HA.

Risoluzione avanzata dei problemi HA

- La risoluzione avanzata dei problemi HA è un nuovo singolo file JSON introdotto come parte di questa funzione che contiene informazioni HA. Viene generato dopo il riavvio dopo un aggiornamento e inviato dall'FTD al CCP.
- Nome e percorso file: /ngfw/var/sf/sync/ha/upgrade_troubleshoot
- Non appena FMC raccoglie la risoluzione avanzata dei problemi HA dalla prima unità (standby), attiva un'operazione remota per raccogliere le stesse informazioni dall'unità attiva.
    - La raccolta remota dei dati è supportata solo quando i dispositivi eseguono la versione 7.6 o successive.
    - Se vengono rilevati dispositivi con una versione inferiore a 7.6, la raccolta dei dati in remoto viene ignorata. Pertanto, in questo caso, il CCP raccoglierebbe i dati solo dall'unità di attesa e deciderebbe di adottare ulteriori misure.

- La generazione avanzata di risoluzione dei problemi HA è rapida. Se Lina è inattiva e non riesce a generare il report, esce immediatamente.
    - Il tempo di riavvio del dispositivo dipende dalla piattaforma in uso e il tempo di riavvio è lo stesso documentato per ciascuna piattaforma.

Rapporto di risoluzione avanzata dei problemi HA

Ogni unità HA genera un file HA avanzato per la risoluzione dei problemi sotto forma di file JSON dopo il riavvio dell'aggiornamento e lo condivide con FMC. Di seguito sono riportati alcuni esempi di convalida in caso di esito negativo o positivo.

Esempio di errore di convalida HA

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

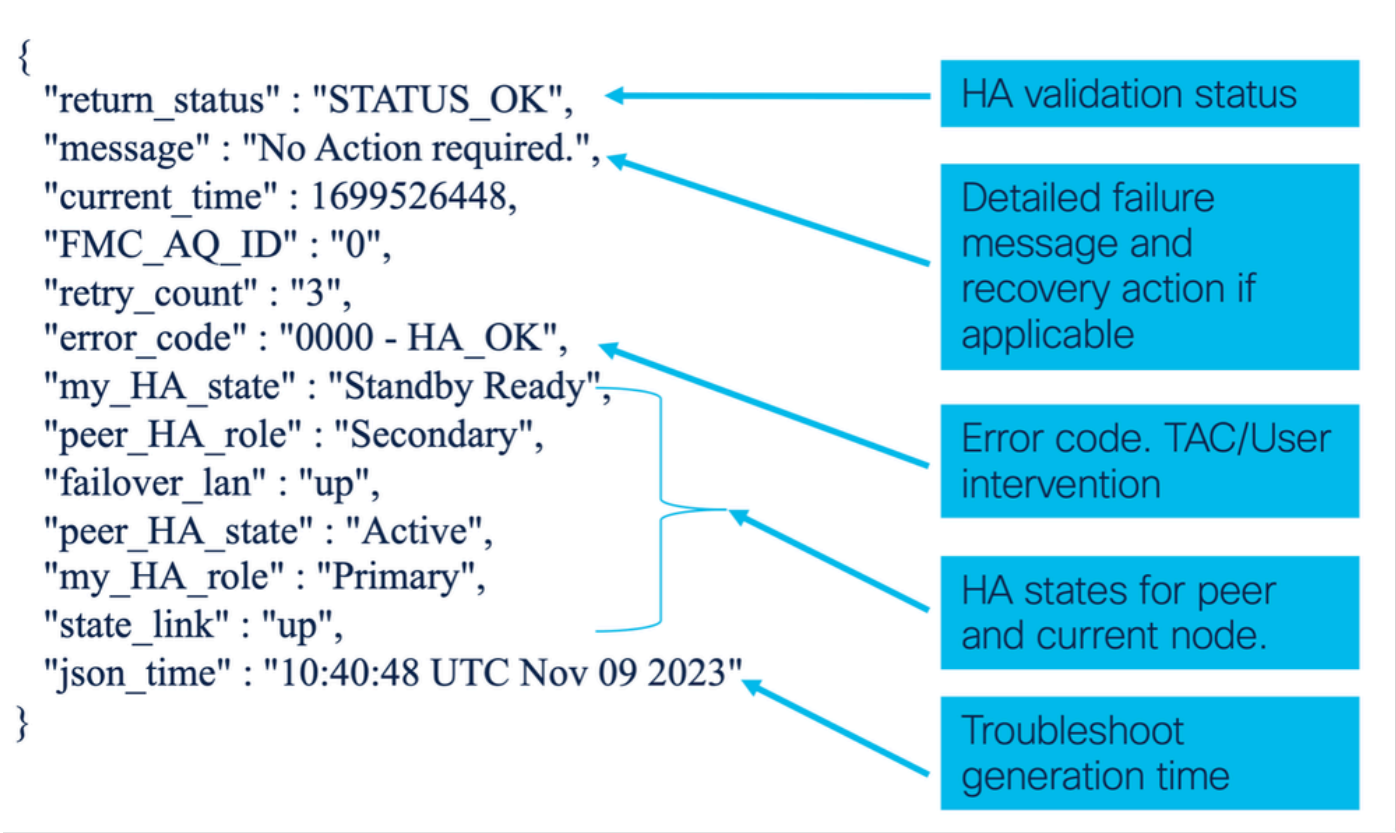
```
{
"failover_lan" : "NA",
"error_code" : "1046 -
STARTUP_FAILOVER_CONFIG_NOT_PRESENT",
"current_time" : 1701369637,
"peer_HA_state" : "Not Detected",
"FMC_AQ_ID" : "0",
"state_link" : "NA",
"json_time" : "18:40:37 UTC Nov 30 2023",
"my_HA_state" : "Disabled",
"my_HA_role" : "Secondary",
"return_status"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


Esempio di convalida HA riuscita

File: /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
}
```


Risoluzione avanzata dei problemi relativi al contenuto HA



Percorso del file di risoluzione dei problemi avanzata HA

Percorso file JSON per risoluzione avanzata problemi HA:

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


        /sync/ha/upgrade_troubleshoot
```

- La risoluzione dei problemi HA si basa sul comando lina.
  - Se la risoluzione dei problemi non viene generata in /ngfw/var/sf/sync/ha/upgrade_troubleshoot, l'utente può fare riferimento ai log in: /ngfw/var/log/ha_upgrade_troubleshoot.log
- I file /ngfw/var/sf/sync/ha/upgrade_troubleshoot e /ngfw/var/log/ha_upgrade_troubleshoot.log fanno parte del file FTD Troubleshoot.

Suggerimenti per la risoluzione avanzata dei problemi di generazione di HA

A volte la risoluzione avanzata dei problemi HA non viene generata a causa dello stato del sistema e il motivo potrebbe essere un'interruzione di connessione o il processo della coda delle azioni è inattivo dopo il riavvio dell'aggiornamento. Se lina o la coda di azioni è inattiva, si tratta di un problema.

In questi casi, verificare se i processi lina e ActionQueue sono in esecuzione utilizzando questo comando in modalità 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
```

Restituisci stato e azione in HA Advanced Risoluzione dei problemi

- STATUS_INIT: Ciò indica che la risoluzione dei problemi HA è stata attivata.
- STATUS_OK: Il dispositivo è in uno stato stabile. Non sono necessarie ulteriori azioni.
- ERRORE DI STATO: Questo comando determina che si è verificato un errore a causa del quale non è stato creato HA. L'utente deve eseguire un'azione in base al messaggio visualizzato o deve contattare TAC.
- STATO_RIPROVA: Il dispositivo può trovarsi in uno degli stati intermedi. La risoluzione dei problemi HA prosegue dopo un intervallo fisso basato sullo stato fino a quando non viene rilevato STATUS_ERROR o STATUS_OK.
    - In base agli errori rilevati in STATUS ERROR, gli errori HA sono classificati in 2 casi:
        - Intervento utente: questi errori HA possono essere risolti dall'utente, che può riprendere l'aggiornamento se l'intervento TAC non è necessario.
        - Intervento TAC - Per questi guasti HA, l'utente non può correggerlo da solo; È necessario l'intervento del TAC.

Codice errore e classificazione

In base ai codici di errore, gli errori vengono classificati come indicato di seguito:

stato_ritorno	codice_errore	Descrizione	Meccanismo di nuovo tentativo o recupero

STATO_OK	"0000 - HA_OK"(I valori riservati sono compresi tra 0001 e 1023)	Questo è per lo scenario di successo. (in cui gli stati HA sono Attivo e Pronto per standby)	(Non applicabile)
ERRORE_STATO	"1024:2047 - ERROR_REASON"	Questo vale per lo scenario di errore (intervento dell'utente)	Messaggi attivabili da visualizzare per l'utente e il framework di aggiornamento possono aggiungere il meccanismo di ripetizione dei tentativi o di ripristino in futuro (se presente).
ERRORE_STATO	"2048:3071 - ERROR_REASON"	Questo è lo scenario di errore (intervento TAC)	Per la ricostituzione è necessario l'intervento del TAC.

Messaggi di intervento utente

Errore	Messaggio di errore	Codice di errore
'FAILOVER_CONFIG_NOT_PRESENCE'	"Configurazione di failover non presente nel dispositivo"	"1024"
'FAILOVER_IS_NOT_ENABLED'	"Failover non abilitato sul dispositivo. Abilitare il failover"	"1025"
'FAILOVER_LAN_DOWN'	"La LAN di failover non è attiva sul dispositivo"	"1026"
'COLLEGAMENTO_STATO_INATTIVO'	"State Link is down on the device" (Collegamento stato non attivo sul	"1027"

	dispositivo)	
'FAILOVER_BLOCK_DEPLETION'	"Blocca l'esaurimento dei seguenti blocchi nel dispositivo:\n"	"1028"
'APP_SYNC_TIMEOUT'	"Timeout sincronizzazione app nel dispositivo"	"1029"
'ERRORE_SINCRONIZZAZIONE_APP_CD'	"Errore di sincronizzazione dell'app CD rilevato nel dispositivo"	"1030"
'CONFIG_SYNC_TIMEOUT'	"Timeout sincronizzazione configurazione sul dispositivo"	"1031"
'FAILED_TO_APPLY_CONFIG'	"Impossibile applicare la configurazione nel dispositivo"	"1032"
'BULK_SYNC_TIMEOUT'	"Timeout sincronizzazione in blocco sul dispositivo"	"1033"
'BULK_SYNC_CLIENT_ISSUE'	"Controllare i seguenti client nel dispositivo:\n"	"1034"
'IFC_CHECK_FAILED'	"Controllo interfaccia di failover non riuscito sulle seguenti interfacce nel dispositivo:\n"	"1035"
'IFC_FAILED_CHECK_VLAN_SPANTREE'	"Poiché le interfacce sono attive. Verificare che le VLAN siano consentite sul lato dello switch o che si sia verificato un problema nello spanning tree"	"1036"

'VERSIONE_NON CORRISPONDENTE'	"Versione software diversa sull'altro dispositivo"	"1037"
'MODE_MISMATCH'	"Modalità operativa diversa sull'altro dispositivo"	"1038"
'LIC_MISMATCH'	"Licenza diversa sull'altro dispositivo"	"1039"
'MANCATA CORRISPONDENZA DI CHASSIS'	"Configurazione diversa dello chassis sull'altro dispositivo"	"1040"
'CARD_MISMATCH'	"Configurazione scheda diversa sull'altro dispositivo"	"1041"
'PEER_NOT_OK'	"Lo stato del dispositivo è OK. Controlla il dispositivo peer"	"1042"

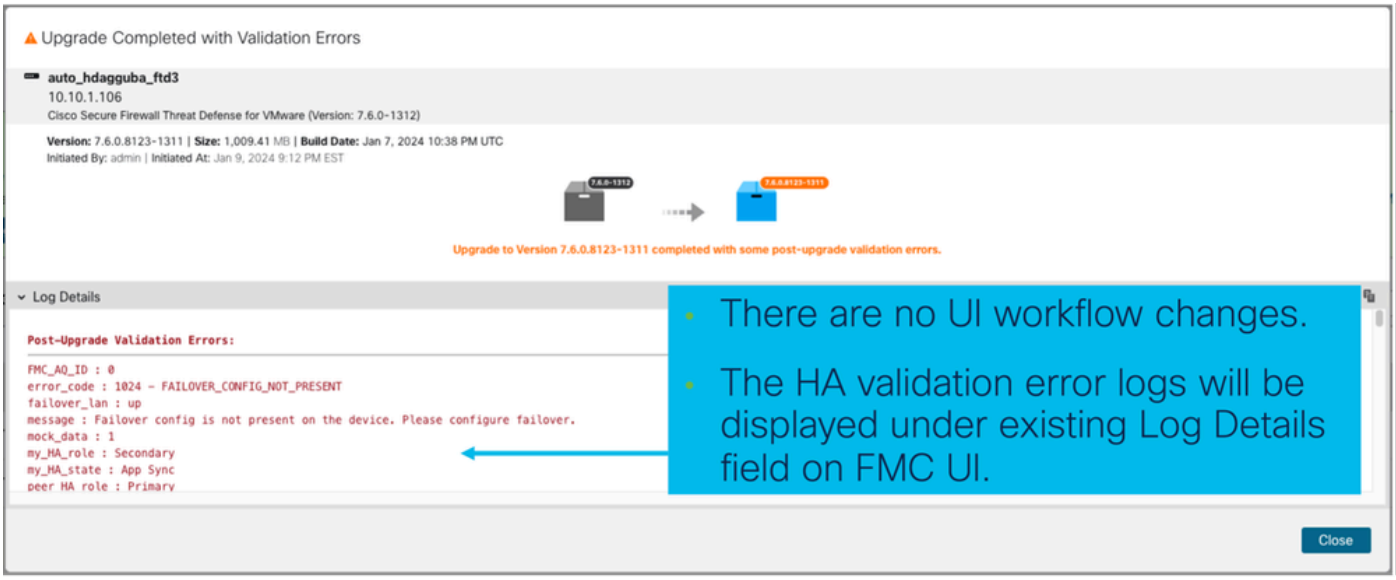
Messaggi di intervento TAC

Errore	Messaggio di errore	Codice di errore
'RUN_CMD_FAILED'	"Impossibile eseguire il comando"	"2048"
'LINA_NOT_STARTED'	"Lina non è stata avviata sul dispositivo. Riprova in seguito"	"2049"'
'HWIDB_MISMATCH'	"L'indice HWIDB sul dispositivo è diverso"	"2050"
'BACKPLANE_FAILURE'	"Errore del backplane sul	"2051"

	dispositivo. Controlla il backplane"	
'HA_PROGR_FAILURE'	"Avanzamento HA non riuscito sul dispositivo"	"2052"
'ERRORE_SVM'	"Modulo del servizio non riuscito sul dispositivo"	"2053"
'SVM_MIO_HB_FAILURE'	"Errore heartbeat tra MIO e App-agent sul dispositivo"	"2054"
'SVM_MIO_CRUZ_FAILED'	"Errore della scheda di rete MIO-blade sul dispositivo"	"2055"
'SVM_MIO_HB_CRUZ_FAILED'	"Errore dell'heartbeat MIO-blade e della scheda di rete sul dispositivo"	"2056"
'ERRORE_SCHEDA_SSM'	"Errore della scheda di servizio nel dispositivo"	"2057"
'ERRORE_COMUNICAZIONE_PERSONALE'	Errore di comunicazione sul dispositivo	"2058"
'CRITICO_PROCESSO_MORTO'	"Il processo critico è morto sul dispositivo"	"2059"
'ERRORE_SNORT'	"Snort non riuscito sul dispositivo"	"2060"
'PEER_SVM_FAILURE'	"Errore del modulo di servizio NGFW sull'altro dispositivo"	"2061"
'FAULT_MON_BLOCK_DEP'	"Il monitoraggio degli	"2062"

	errori ha segnalato l'esaurimento del blocco sul dispositivo"	
'ERRORE_DISCO'	"Errore del disco sul dispositivo"	"2063"
'SNORT_DiSK_FAILURE'	"Errore durante lo snort e il disco sul dispositivo	"2064"
'INACTIVE_MATE_FOUND"	"Rilevato un partner inattivo durante l'avvio	"2065"
'TIMEOUT_SCRIPT'	"Limite tentativi superato. Chiusura script in corso"	"2066"
'ERRORE_SCONOSCIUTO'	"Impossibile identificare l'errore"	"2067"

Modifiche all'interfaccia utente di Centro gestione firewall



Architettura software

Questa funzionalità dipende fortemente dal framework della coda di azioni esistente. La funzionalità utilizza la CLI di Lina sottostante per generare i dati di risoluzione avanzata dei problemi HA.

Wireless LAN Controller serie 9800

Q: La funzione è applicabile per la funzionalità di ripristino dell'aggiornamento FTD?
A: No. Questa funzione non è applicabile per la funzionalità di ripristino in quanto il ripristino FTD funziona in parallelo, non 1 per 1.

Q: Se l'aggiornamento non riesce in corrispondenza di 200_enable_maintenance_mode.pl, vengono generati i dati per la risoluzione avanzata dei problemi?
A: No. La risoluzione avanzata dei problemi HA viene generata solo dopo il riavvio successivo all'aggiornamento e non durante un errore di aggiornamento

Q: Se l'aggiornamento è bloccato a causa di convalide HA sulla seconda unità, un utente può attivare l'aggiornamento solo sulla seconda unità?
A: Sì. L'utente deve selezionare di nuovo la coppia HA per l'aggiornamento e FMC avvia l'aggiornamento solo su unità non aggiornate.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).