減少安全防火牆7.6 FTD HA升級失敗

目錄

簡介

本檔案介紹疑難排解，以解決從7.0版到7.2版的FTD升級失敗，特別是高可用性(HA)部署中的問題。

背景資訊

一半以上的故障源於200_enable_maintenance_mode階段的問題，現有HA驗證主要執行基本主用/備用狀態檢查，這些檢查不足以進行全面的HA轉換。

通過Secure Firewall 7.6更新，引入了改進的HA驗證來解決這些問題。這些增強功能包括徹底檢查HA狀態轉換、延長同步進程超時時間，以及增強錯誤報告。此更新旨在顯著減少升級後HA問題和整體升級失敗，確保更順利和更可靠的HA部署升級過程。

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

問題

- 在7.0、7.1和7.2版本的HA部署中，客戶報告的有大量FTD升級失敗。
- 超過50%的故障來自FTD HA部署。200_enable_maintenance_mode中的故障會導致HA故障。
- 現有的HA狀態驗證是基本驗證（如活動/備用狀態檢查），不會完全驗證HA轉換。

快訊（解決方案）

FTD升級的改進HA驗證：

- 驗證HA狀態轉換
- 針對配置同步（7200秒）、應用同步（1200秒）和批次同步（7200秒）等HA轉換狀態改進的FTD HA升級超時
- 在何時啟動或失敗FTD升級時向FMC提供更多控制權
- 改進了FTD HA升級的錯誤報告和恢復消息

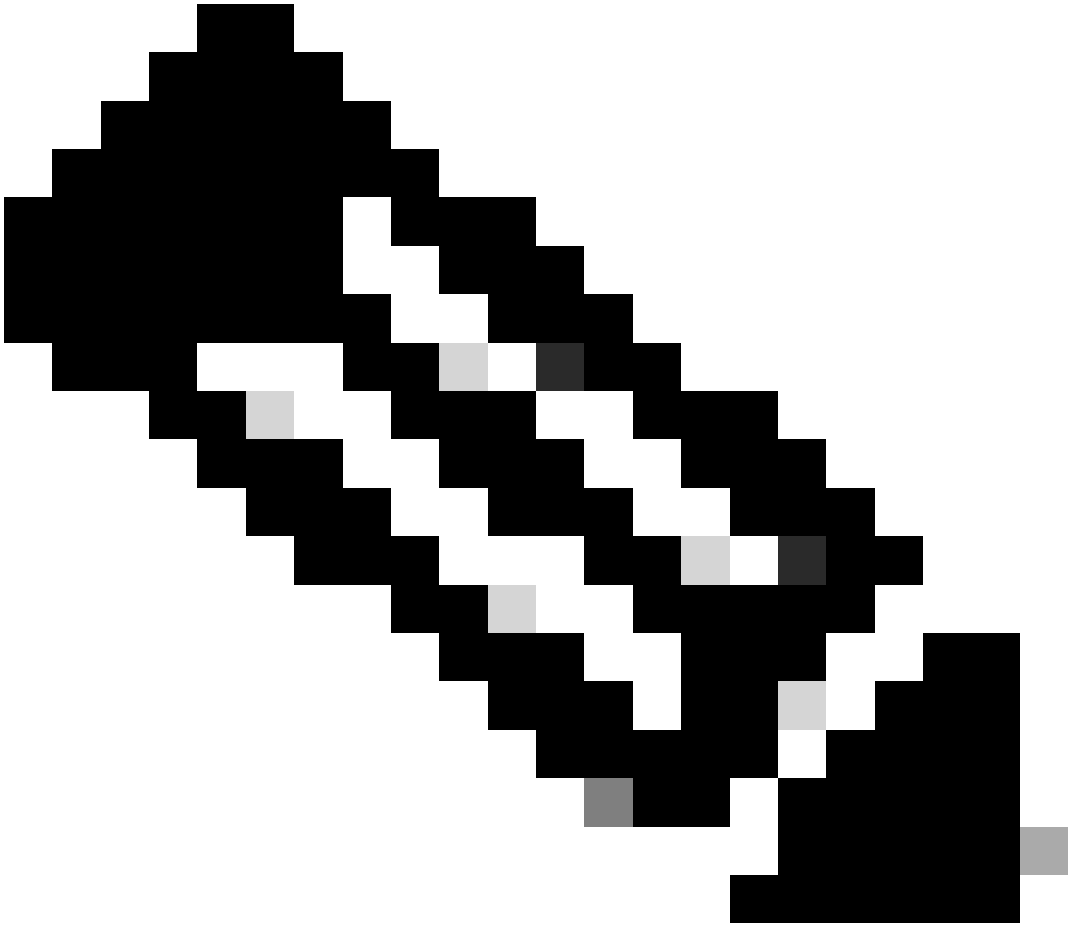
與先前版本相比，它具有：

- 改進的HA驗證有助於減少HA部署中的升級後HA建立問題
- 改進的驗證有助於減少FTD升級失敗

必要條件

支援的平台

- 管理器和版本：FMC 7.6.0
- 應用程式(ASA/FTD)和應用程式的最低版本：FTD 7.6.0;FMC管理7.6.0 FTD高可用性
- 支援的平台：所有執行FTD HA的平台

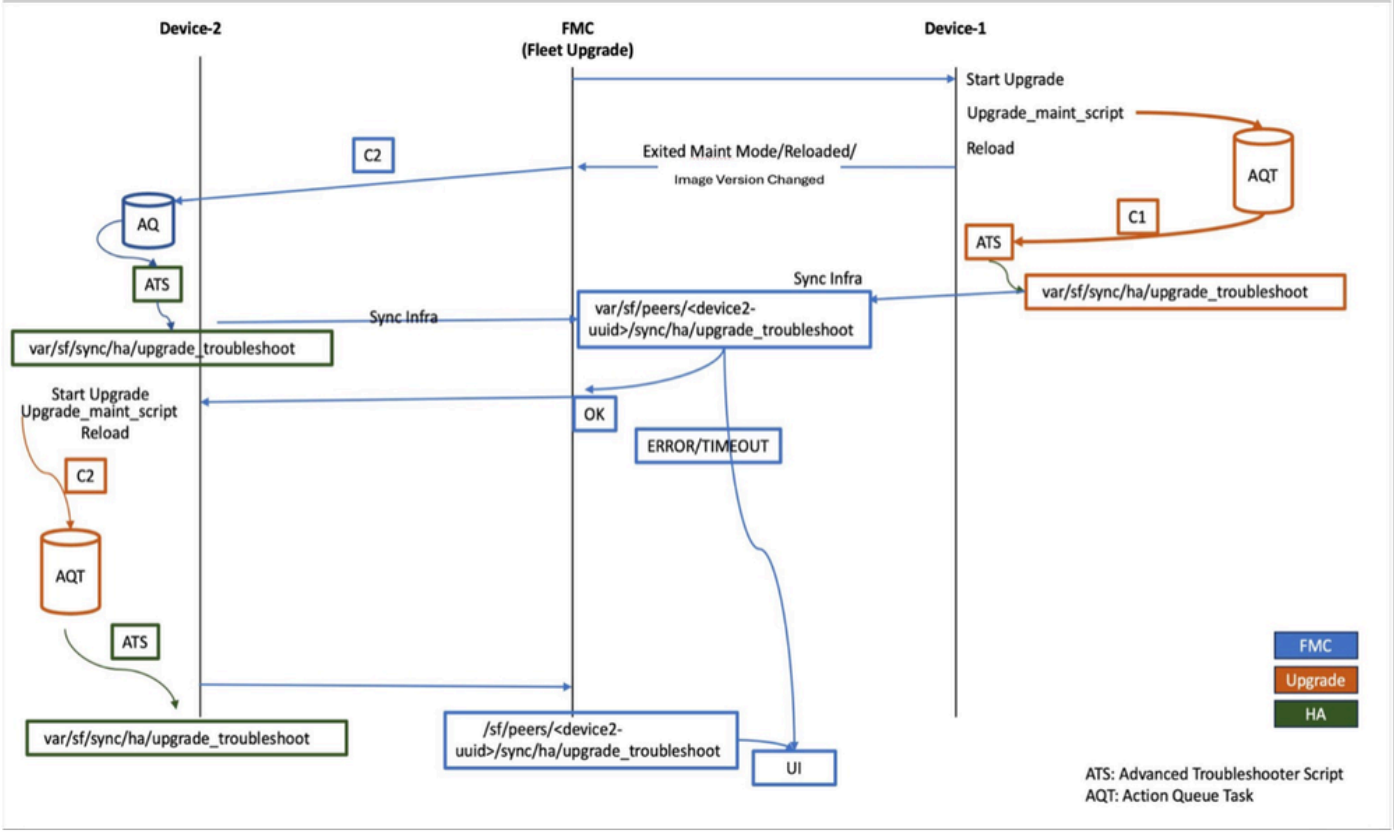


附註：此功能僅適用於FMC管理的FTD HA部署。此功能不適用於FDM管理的FTD HA或集群裝置。

功能概述

- 此功能可協助在升級程式的重新啟動後，FMC檢查已升級裝置的HA狀態，以減少HA部署中的FTD升級失敗。
- 升級重新啟動後，FMC會檢查主用/備用狀態以及HA同步中的任何故障。
- FTD會以新的HA預先疑難排解的方式，通知第二個節點上的升級何時開始或失敗。
- 如果在加入HA升級後重新引導時出現任何故障，FMC UI上會顯示適當的消息。

FTD HA的新升級工作流程



備用裝置是第一個升級的裝置

首次裝置升級（備用裝置）

- 在第一次裝置升級期間，升級指令碼啟動action_queue任務以收集999_finish階段的HA高級故障排除資料。
- 插入的任務執行僅在升級後重新啟動後開始，並以JSON檔案的形式收集故障排除資訊。
- 同一個JSON檔案同步到FMC。
- 一旦第一個節點退出維護模式，FMC將在主用裝置上觸發遠端action_queue任務，以收集HA高級故障排除（主用裝置需要為7.6或更高）。 如果發現主用裝置低於7.6，則不從主用裝置收集故障排除，FMC僅根據從備用裝置收集的故障排除做出決策。

從兩台裝置收集HA高級故障排除後，FMC決定在第二個節點（活動裝置）上開始升級或阻止升級。

第二次裝置升級（活動裝置）

- 與備用裝置類似，升級指令碼在999_finish階段啟動action_queue任務以收集HA高級故障排除。
- 插入的任務執行僅在升級後重新啟動時開始，並以JSON檔案的形式生成故障排除資訊。
- 相同檔案同步到FMC。
- 如果任一裝置報告高可用性故障，高可用性故障資料將顯示在升級頁籤的FMC UI上。
- 如果在加入HA升級後重新引導時出現任何故障，則升級會標籤為已完成，並在同一個升級頁籤上報告HA驗證故障。

HA高級故障排除

- HA高級故障排除是一個新的單個JSON檔案，作為此功能的一部分引入，它包含HA資訊。升級後重新開機後產生，並從FTD傳送到FMC。
- 檔名和路徑：/ngfw/var/sf/sync/ha/upgrade_troubleshoot
- FMC從第一個（備用）單元收集HA高級故障排除後，FMC會觸發遠端任務，以從主用單元收集相同的資訊。
    - 僅當裝置運行7.6或更高版本時，才支援此遠端資料收集。
    - 如果找到的裝置運行版本低於7.6，則會跳過遠端資料收集。因此，在這種情況下，FMC將只從備用單元收集資料並決定進一步操作。

- HA高級故障排除生成非常快速。如果Lina關閉且無法產生報告，便會立即退出。
    - 裝置重新啟動時間取決於平台到平台的時間以及重新啟動時間與我們記錄的每個平台的時間相同。

HA高級故障排除報告

每個HA單元以JSON檔案形式在升級後重新啟動時生成一個HA高級故障排除資料，並與FMC共用。以下是發生失敗和成功時的驗證示例。

HA驗證失敗示例

檔案：/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"
}
```

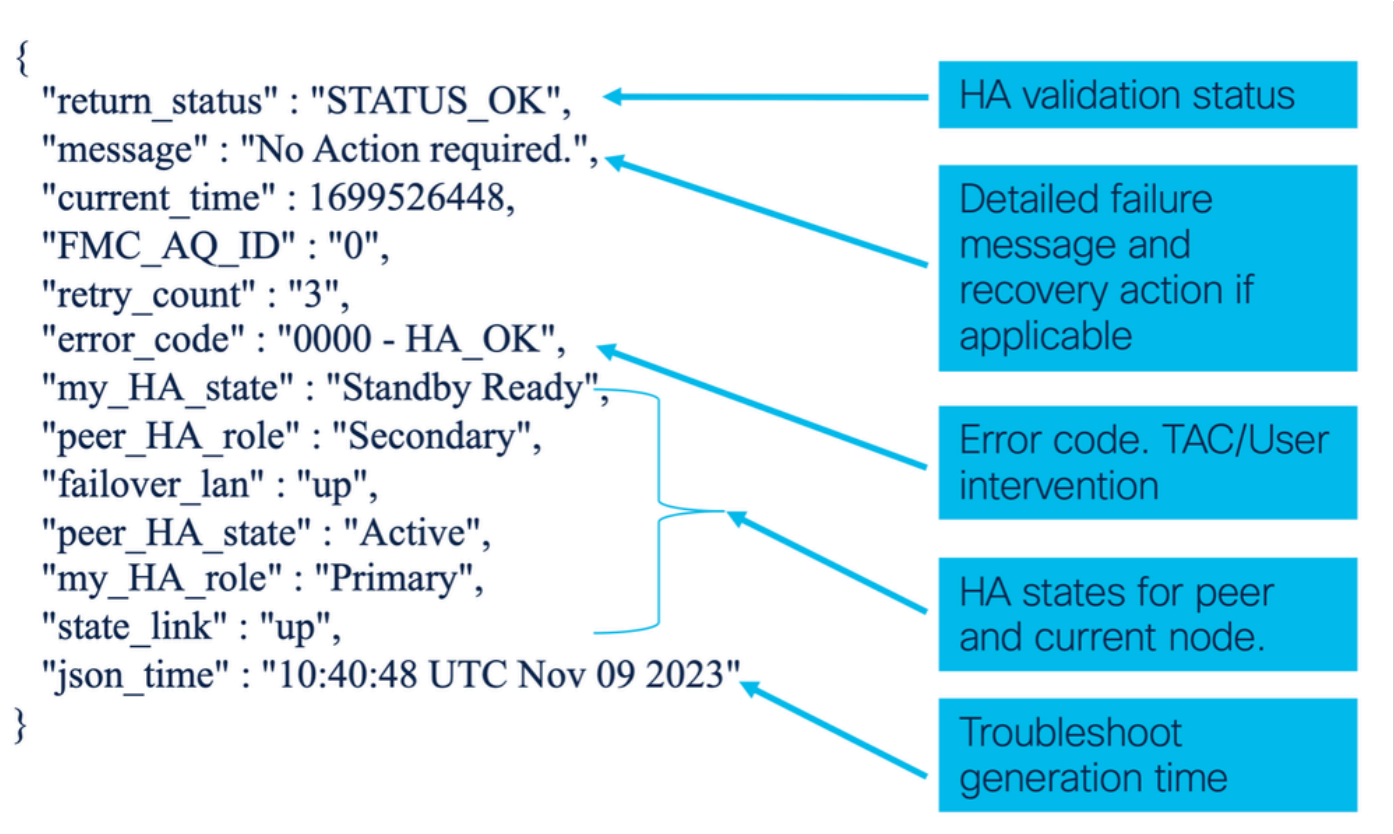

成功的HA驗證示例

檔案：/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高級故障排除內容



HA高級故障排除檔案的位置

HA高級故障排除JSON檔案位置：

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

```
        /sync/ha/upgrade_troubleshoot
```

- HA疑難排解取決於lina指令。
  - 如果在/ngfw/var/sf/sync/ha/upgrade_troubleshoot中無法生成故障排除，則使用者可以參考以下位置的日誌：/ngfw/var/log/ha_upgrade_troubleshoot.log
- /ngfw/var/sf/sync/ha/upgrade_troubleshoot和/ngfw/var/log/ha_upgrade_troubleshoot.log檔案是FTD故障排除檔案的一部分。

HA高級故障排除生成問題提示

有時，由於系統狀態而無法生成HA高級故障排除，原因可能是升級重新啟動後發生故障或操作隊列進程中斷。如果lina或動作佇列關閉，則會發生問題。

在這種情況下，請在專家模式下使用以下命令檢查lina和ActionQueue進程是否正在運行：

<#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
```

HA高級故障排除中的返回狀態和操作

- STATUS_INIT:這表示已觸發HA故障排除。
- STATUS_OK:裝置處於穩定狀態。無需執行任何動作。
- 狀態錯誤：這確定由於未形成HA而發生的錯誤。使用者需要根據顯示的消息採取行動，或者使用者需要聯絡TAC。
- STATUS_RETRY:裝置可以處於中間狀態之一。HA疑難排解會在固定時間間隔後根據狀態不斷重試，直到遇到STATUS_ERROR或STATUS_OK。
  - 根據遇到的STATUS ERROR故障，HA故障被分類為2種情況：
    - 使用者干預 — 使用者可以修正這些HA失敗，且使用者可以在不需要TAC干預的情況下繼續升級。
    - TAC干預 — 對於這些HA故障，使用者無法自行修正；需要TAC干預。

錯誤代碼和分類

根據錯誤代碼，錯誤分類如下：

return_status	錯誤代碼	說明	重試或恢復機制
STATUS_OK	"0000 - HA_OK"（保留值是從0001到1023）	這是成功的案例。（其中HA狀態為「活動」和「備用就緒」）	（不適用）
STATUS_ERROR	"1024:2047 - ERROR_REASON"	此錯誤用於錯誤情況(用戶干預)	要向使用者和升級框架顯示的可操作消息可以在將來（如果有）新增重試或恢復機制。
STATUS_ERROR	"2048:3071 - ERROR_REASON"	適用於錯誤案例（TAC干預）	恢復需要TAC干預。

使用者干預消息

錯誤	錯誤消息	錯誤代碼
'FAILOVER_CONFIG_NOT_PRSENT'	"裝置上不存在故障轉移配置"	"1024"
'FAILOVER_IS_NOT_ENABLED'	「裝置上未啟用故障轉移。請啟用故障轉移"	"1025"
'FAILOVER_LAN_DOWN'	"裝置上的故障切換LAN已關閉"	"1026"
'STATE_LINK_DOWN'	"裝置上的狀態鏈路已關閉"	"1027"
'FAILOVER_BLOCK_DEPLETION'	"裝置中的以下塊上的塊耗盡：\n"	"1028"
'APP_SYNC_TIMEOUT'	"裝置上的應用同步超時"	"1029"

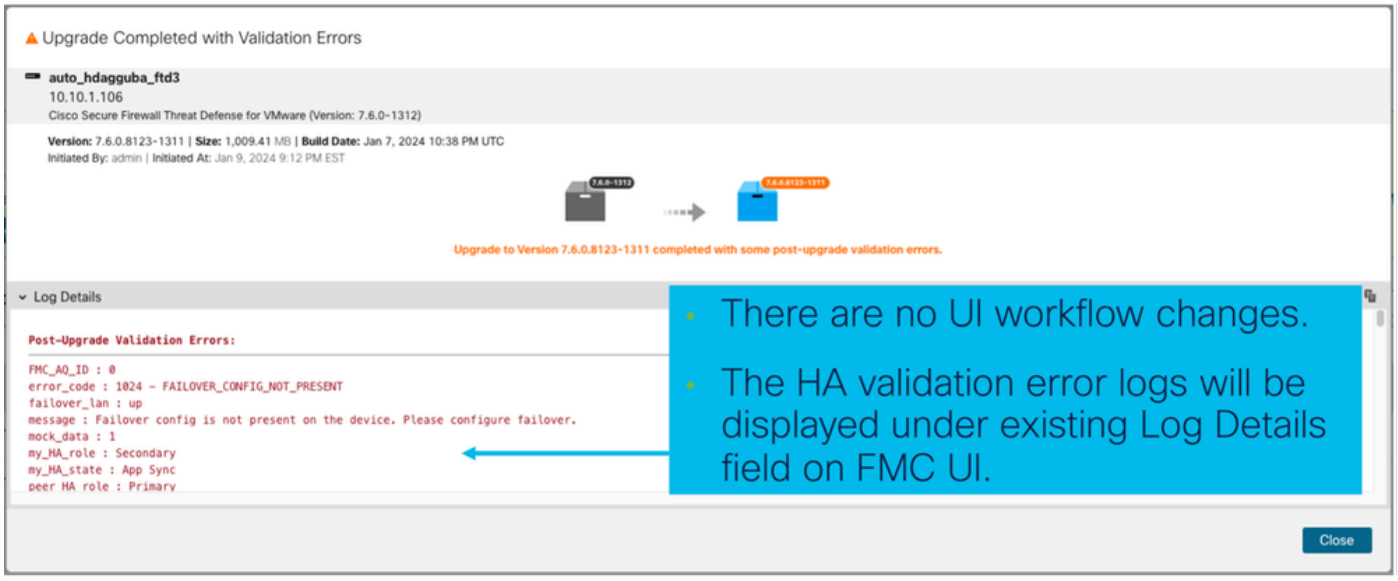
'CD_APP_SYNC_ERROR'	"在裝置上檢測到CD應用同步錯誤"	"1030"
'CONFIG_SYNC_TIMEOUT'	"裝置上的配置同步超時"	"1031"
'FAILED_TO_APPLY_CONFIG'	"無法在裝置上應用配置"	"1032"
'BULK_SYNC_TIMEOUT'	"裝置上的批次同步超時"	"1033"
'BULK_SYNC_CLIENT_ISSUE'	"檢查裝置上的以下客戶端：\n"	"1034"
'IFC_CHECK_FAILED'	"裝置中的以下介面上的故障轉移介面檢查失敗：\n"	"1035"
'IFC_FAILED_CHECK_VLAN_SPANTREE'	「因為介面已開啟。請檢查交換機側是否允許VLAN或者是否存在生成樹問題」	"1036"
'版本不匹配'	"其他裝置上的軟體版本不同"	"1037"
'模式不匹配'	"其他裝置上的不同操作模式"	"1038"
'LIC_MISMATCH'	"其他裝置上的不同許可證"	"1039"
'CHASSIS_MISMATCH'	"其他裝置上的不同機箱配置"	"1040"
'CARD_MISMATCH'	"其他裝置上的不同卡配置"	"1041"
'PEER_NOT_OK'	「此裝置處於正常狀態。檢查對等裝置」	"1042"

TAC干預消息

錯誤	錯誤消息	錯誤代碼
'RUN_CMD_FAILED'	"無法運行命令"	"2048"
'LINA_NOT_STARTED'	"Lina未在裝置上啟動。過一段時間後再試」	《2049年》
'HWIDB_MISMATCH'	"裝置上的HWIDB索引不同"	"2050"
'BACKPLANE_FAILURE'	「裝置上的底板故障。檢查底板」	"2051"
'HA_PROGR_FAILURE'	"裝置上的HA進程失敗"	"2052"
'SVM_FAILURE'	"裝置上的服務模組出現故障"	"2053"
'SVM_MIO_HB_FAILURE'	"裝置上的MIO和App-agent之間的心跳故障"	"2054"
'SVM_MIO_CRUZ_FAILED'	"裝置上的MIO-blade網路介面卡故障"	"2055"
'SVM_MIO_HB_CRUZ_FAILED'	"裝置上的MIO-blade心跳和網路介面卡故障"	"2056"
'SSM_CARD_FAILURE'	"裝置上的服務卡故障"	"2057"
'MY_COM_FAILURE'	"裝置上的通訊故障"	"2058"
'CRITICAL_PROCESS_DEAD'	"關鍵進程死在裝置上"	"2059"
'SNORT_FAILURE'	"裝置上的Snort失敗"	"2060"
'PEER_SVM_FAILURE'	"另一台裝置上的NGFW服務模組出現故障"	"2061"

'FAULT_MON_BLOCK_DEP'	"故障監控報告裝置上的塊耗盡"	"2062"
'DISK_FAILURE'	"磁碟在裝置上發生故障"	"2063"
'SNORT_DiSK_FAILURE'	"Snort和磁碟在裝置上失敗	"2064"
'INACTIVE_MATE_FOUND"	「在啟動期間檢測到非活動夥伴	"2065"
'SCRIPT_TIMEOUT'	"已超出重試限制。正在退出指令碼」	"2066"
'錯誤_未知'	"未能識別錯誤"	"2067"

Firewall Management Center UI更改



軟體體系結構

此功能高度依賴於現有的操作隊列框架。此功能使用底層lina CLI產生HA進階疑難排解資料。

常見問題

Q:此功能是否適用於FTD升級還原功能？
A:不能。此功能不適用於還原功能，因為FTD還原並行工作，而不是1乘1。

Q:如果在200_enable_maintenance_mode.pl升級失敗，是否會生成高級故障排除資料？
A:不能。只有在升級後重新啟動後才會生成HA高級故障排除，而不是在升級失敗期間生成

Q:如果由於第二台裝置的HA驗證而阻止升級，使用者是否可以單獨觸發第二台裝置的升級？
A:會。使用者必須再次選擇HA對進行升級，FMC僅在未升級的裝置上觸發升級。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。