减少Secure Firewall 7.6 FTD高可用性升级故障

目录

简介

本文档介绍如何排除故障，以解决从版本7.0到7.2的FTD升级故障，尤其是在高可用性(HA)部署中。

背景信息

一半以上的故障源于200_enable_maintenance_mode阶段的问题，现有HA验证主要执行基本主用/备用状态检查，这些检查不足以进行全面的HA转换。

通过Secure Firewall 7.6更新，引入改进的HA验证来解决这些问题。这些增强功能包括全面检查高可用性状态转换、延长同步进程超时时间，以及增强错误报告。此更新旨在显着减少升级后的HA问题和整体升级失败，确保更顺利和更可靠的HA部署升级流程。

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

问题

- 在7.0、7.1和7.2版本中，客户报告的适用于HA部署的FTD升级失败次数相当多。
- 超过50%的故障来自FTD HA部署。200_enable_maintenance_mode中的故障导致HA故障。
- 现有HA状态验证是基本验证（如主用/备用状态检查），不会完全验证HA转换。

新增内容（解决方案）

改进了FTD升级的高可用性验证：

- 验证HA状态转换
- 改善了HA过渡状态(如配置同步（7200秒）、应用同步（1200秒）和批量同步（7200秒）)的FTD高可用性升级超时
- 在启动或失败FTD升级时为FMC提供更多控制权
- 改进了FTD HA升级的错误报告和恢复消息

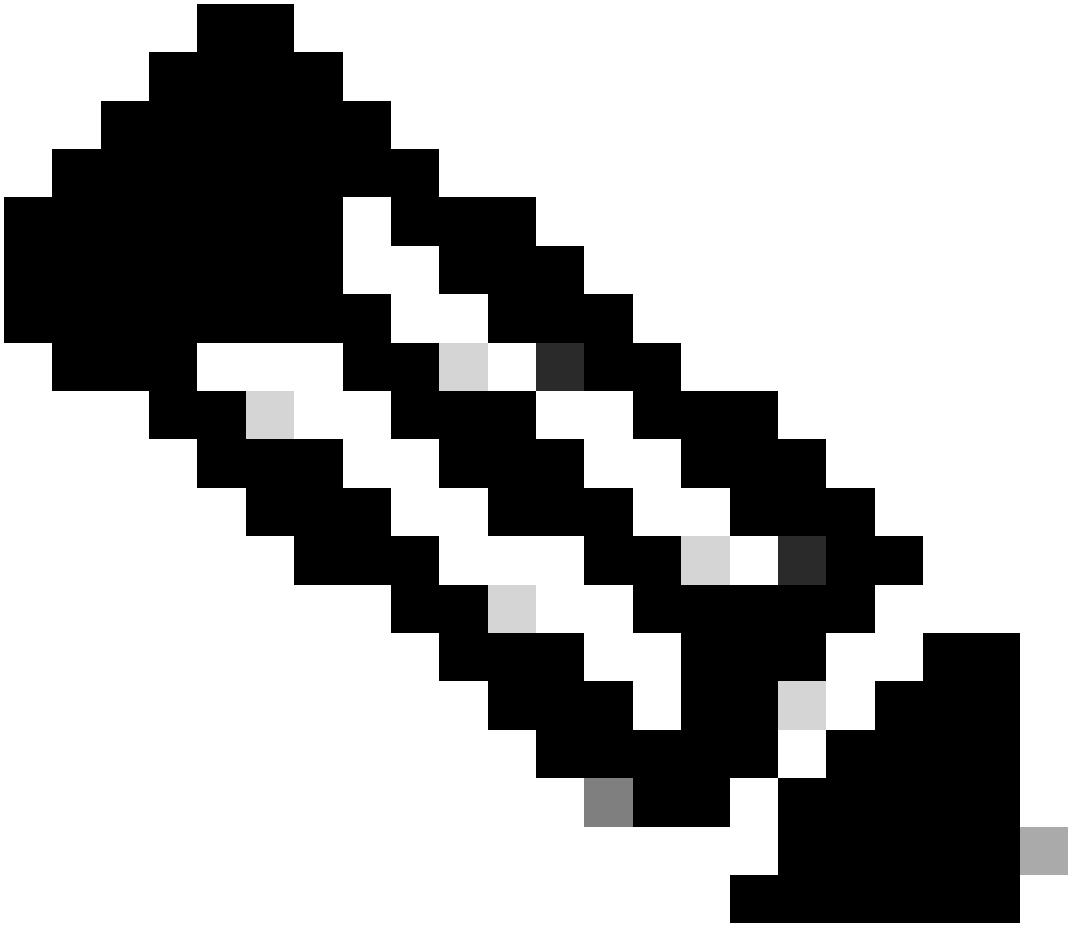
与之前的版本相比，它具有：

- 改进的高可用性验证有助于减少高可用性部署中的升级后高可用性创建问题
- 改进的验证有助于减少FTD升级失败

先决条件

支持的平台

- 管理器和版本：FMC 7.6.0
- 应用(ASA/FTD)和应用的最低版本：FTD 7.6.0;FMC管理7.6.0 FTD高可用性
- 支持的平台:所有运行FTD HA的平台

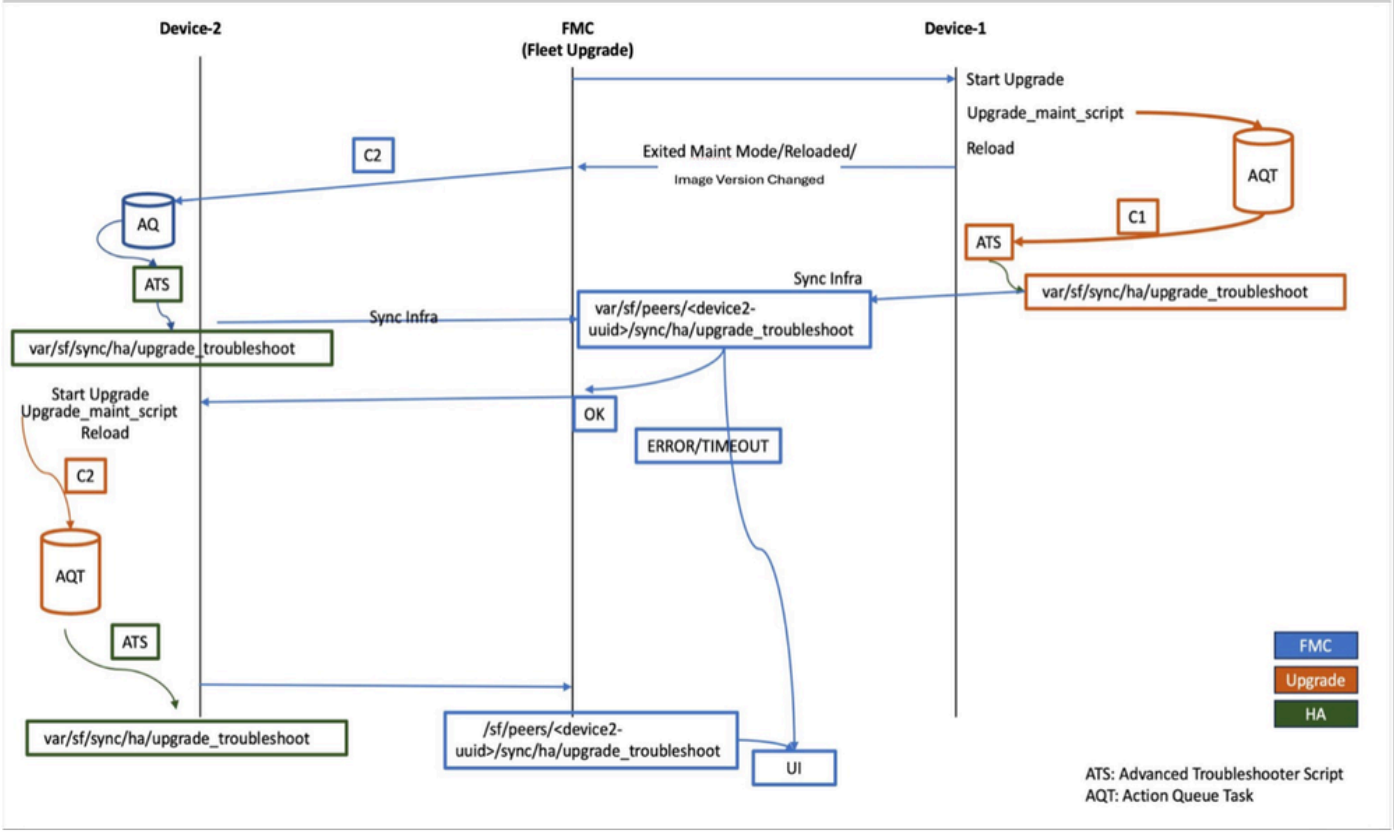


注意：此功能仅适用于FMC管理的FTD HA部署。此功能不适用于FDM管理的FTD HA或集群设备。

功能概述

- 此功能通过在升级过程重新启动部分后由FMC检查已升级设备的HA状态，帮助减少HA部署中的FTD升级故障。
- 升级重新启动后，FMC将检查主用/备用状态和HA同步中的所有故障。
- FTD会通知FMC何时在第二个节点上以新的HA高级故障排除形式启动或失败升级。
- 如果在加入高可用性升级后重新启动时出现任何故障，FMC UI上会显示相应的消息。

FTD HA的新升级工作流程



备用设备是第一个升级的设备

首次设备升级（备用设备）

- 在第一次设备升级期间，升级脚本启动action_queue任务以收集999_finish阶段的HA高级故障排除数据。
- 插入的任务执行仅在升级后重新启动后开始，并以JSON文件的形式收集故障排除信息。
- 同一个JSON文件同步到FMC。
- 一旦第一个节点退出维护模式，FMC会在主用设备上触发远程action_queue任务，以收集HA高级故障排除（主用设备需要是7.6或更高版本）。 如果发现主用设备低于7.6，则不会从主用设备收集故障排除，FMC仅根据从备用设备收集的故障排除做出决策。

从两台设备收集HA高级故障排除后，FMC决定在第二个节点（主用设备）上开始升级或阻止升级。

第二次单元升级（主用单元）

- 与备用设备类似，升级脚本在999_finish阶段启动action_queue任务以收集HA高级故障排除。
- 插入的任务执行仅在升级后重新启动时启动，并以JSON文件的形式生成故障排除信息。
- 同一文件同步到FMC。
- 如果任一设备报告高可用性故障，高可用性故障数据将显示在升级选项卡的FMC UI上。
- 如果在加入高可用性升级后重新引导时出现任何故障，升级会标记为已完成，并在同一升级选项卡上报告HA验证故障。

HA高级故障排除

- HA高级故障排除是作为此功能的一部分引入的一个新的单个JSON文件，它包含HA信息。它会在升级后重新启动后生成，并从FTD发送到FMC。
- 文件名和路径：/ngfw/var/sf/sync/ha/upgrade_troubleshoot
- FMC从第一个（备用）单元收集HA高级故障排除后，FMC立即触发远程任务，从主用单元收集相同的信息。
    - 仅当设备运行7.6或更高版本时，才支持此远程数据收集。
    - 如果找到运行低于7.6版本的设备，则会跳过远程数据收集。因此，在这种情况下，FMC将只从备用设备收集数据并决定采取进一步的操作。

- HA高级故障排除生成非常快速。如果Lina关闭且无法生成报告，它会立即退出。
    - 设备重启时间取决于平台到平台，并且重启时间与我们在每个平台中记录的相同。

HA高级故障排除报告

每个HA单元以JSON文件形式在升级后重新引导生成一个HA高级故障排除数据，并与FMC共享。以下是失败和成功时的验证示例。

HA验证失败示例

文件:/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"
}
```

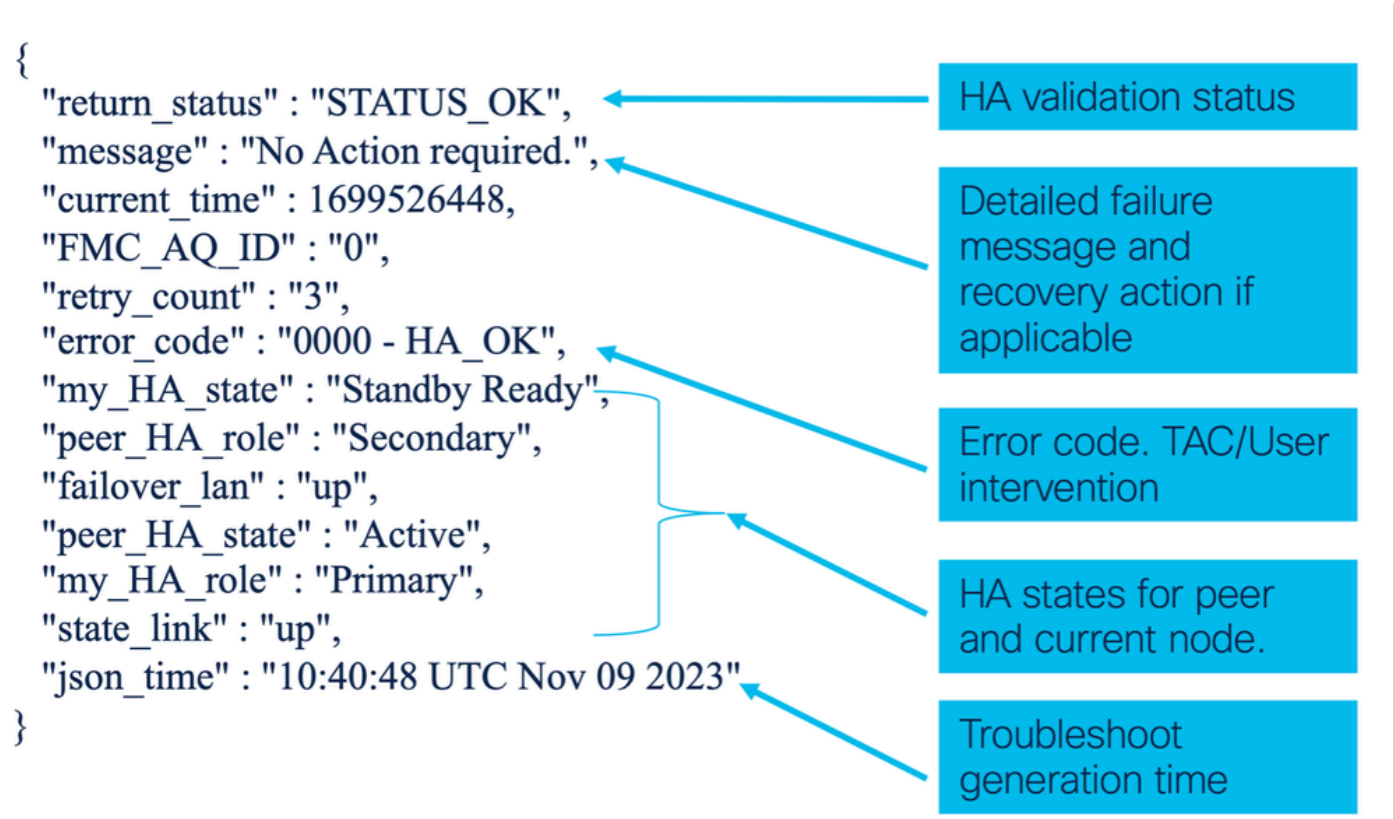

成功的HA验证示例

文件:/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高级故障排除内容



HA高级故障排除文件的位置

HA高级故障排除JSON文件位置：

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

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

- HA故障排除依赖于lina命令。
  - 如果在/ngfw/var/sf/sync/ha/upgrade_troubleshoot处无法生成故障排除，则用户可以参考以下位置的日志：/ngfw/var/log/ha_upgrade_troubleshoot.log
- /ngfw/var/sf/sync/ha/upgrade_troubleshoot和/ngfw/var/log/ha_upgrade_troubleshoot.log文件是FTD故障排除文件的一部分。

HA高级故障排除生成问题提示

有时，由于系统状态而无法生成HA高级故障排除，原因可能是升级重新启动后中断或操作队列进程中断。如果lina或操作队列关闭，则存在此问题。

在这种情况下，请在专家模式下使用此命令检查lina和ActionQueue进程是否正在运行：

<#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高级故障排除中的返回状态和操作

- STATUS_INIT:这表示已触发HA故障排除。
- STATUS_OK:设备处于稳定状态。不需要采取任何操作。
- 状态错误：这确定由于未形成HA而发生的错误。用户需要根据显示的消息采取行动，或者用户需要联系TAC。
- STATUS_RETRY:设备可以处于中间状态之一。HA故障排除在固定时间间隔后根据状态不断重试，直到遇到STATUS_ERROR或STATUS_OK。
  - 根据failures encountered STATUS ERROR，HA故障分为两种情况：
    - 用户干预 — 用户可修复这些HA故障，并且用户可以恢复升级，而无需进行TAC干预。
    - TAC干预 — 对于这些HA故障，用户无法自行修复；需要TAC干预。

错误代码和分类

根据错误代码，错误分类如下：

return_status	error_code	描述	重试或恢复机制
STATUS_OK	"0000 - HA_OK"（保留值为从0001到1023）	这是成功场景。（其中HA状态为“活动”和“备用就绪”）	(不适用)
STATUS_ERROR	"1024:2047 - ERROR_REASON"	这是用于错误场景(用户干预)	要向用户和升级框架显示的可操作消息可以在将来添加重试或恢复机制（如果有）。
STATUS_ERROR	"2048:3071 - ERROR_REASON"	这是用于错误场景（TAC干预）	恢复需要TAC干预。

用户干预消息

错误	错误消息	错误代码
'FAILOVER_CONFIG_NOT_PRSENT'	"故障切换配置不存在于设备上"	“1024”
'FAILOVER_IS_NOT_ENABLED'	“设备上未启用故障转移。请启用故障转移”	“1025”
'FAILOVER_LAN_DOWN'	"设备上的故障切换LAN已关闭"	“1026”
'STATE_LINK_DOWN'	"设备上的状态链路已关闭"	“1027”
'FAILOVER_BLOCK_DELETION'	"设备中的以下块上的块耗尽：\n"	“1028”
'APP_SYNC_超时'	"设备上的应用同步超时"	“1029”
'CD_APP_SYNC_ERROR'	"在设备上检测到CD应用同	“1030”

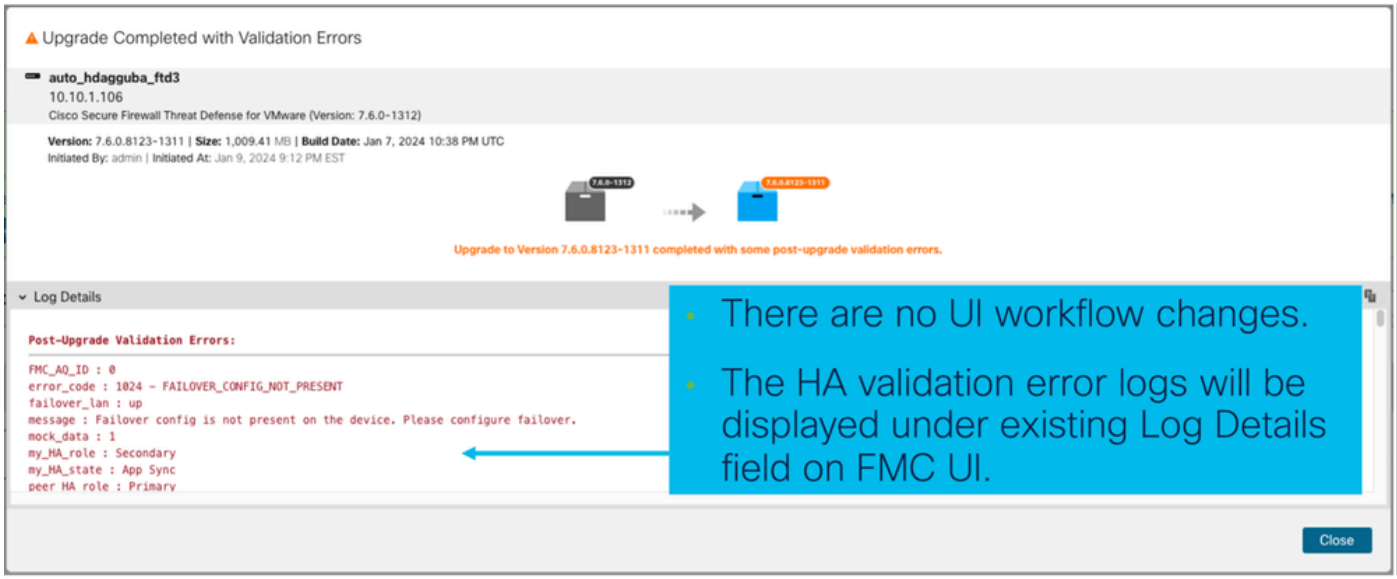
	步错误"	
'配置同步超时'	"设备上的配置同步超时"	“1031”
'FAILED_TO_APPLY_CONFIG'	"无法在设备上应用配置"	“1032”
'批量同步超时'	"设备上的批量同步超时"	“1033”
'BULK_SYNC_CLIENT_ISSUE'	"检查设备上的以下客户端：\n"	“1034”
'IFC_CHECK_FAILED'	"设备中的以下接口上的故障转移接口检查失败：\n"	“1035”
'IFC_FAILED_CHECK_VLAN_SPANTREE'	“因为接口是打开的。请检查交换机端是否允许VLAN或者是否存在生成树问题”	“1036”
'版本不匹配'	"其他设备上的不同软件版本"	“1037”
'模式不匹配'	"其他设备上的不同操作模式"	“1038”
'LIC_MISMATCH'	"其他设备上的不同许可证"	“1039”
'机箱不匹配'	"其他设备上的不同机箱配置"	“1040”
'CARD_MISMATCH'	"其他设备上的不同卡配置"	“1041”
'PEER_NOT_OK'	“此设备处于正常状态。检查对等设备”	“1042”

TAC干预消息

错误	错误消息	错误代码
'RUN_CMD_FAILED'	"无法运行命令"	“2048”
'LINA_NOT_STARTED'	“设备上未启动Lina。请稍后重试”	《2049年》
'HWIDB_MISMATCH'	"设备上的HWIDB索引不同"	“2050”
'BACKPLANE_FAILURE'	“设备上的背板故障。检查底板”	“2051”
'HA_PROGR_FAILURE'	"设备上的HA进程失败"	“2052”
'SVM_FAILURE'	"服务模块在设备上发生故障"	“2053”
'SVM_MIO_HB_FAILURE'	"设备上MIO和App-agent之间的心跳故障"	“2054”
'SVM_MIO_CRUZ_FAILED'	"设备上的MIO刀片网络适配器故障"	“2055”
'SVM_MIO_HB_CRUZ_FAILED'	"设备上的MIO-blade心跳和网络适配器故障"	“2056”
'SSM_CARD_FAILURE'	"设备上的服务卡故障"	“2057”
'MY_COM_FAILURE'	"设备上的通信故障"	“2058”
'CRITICAL_PROCESS_DEAD'	"关键进程死在设备上"	“2059”
'SNORT_FAILURE'	"设备上的Snort失败"	“2060”
'PEER_SVM_FAILURE'	"另一设备上的NGFW服务模块发生故障"	“2061”
'FAULT_MON_BLOCK_DEP'	"故障监控报告设备上的块耗尽"	“2062”

'DISK_FAILURE'	"设备上的磁盘发生故障"	“2063”
'SNORT_DiSK_FAILURE'	“Snort和磁盘在设备上发生故障	“2064”
'INACTIVE_MATE_FOUND"	“在启动期间检测到非活动伙伴	“2065”
'脚本超时'	"Retry limit exceeded.正在退出脚本”	“2066”
'错误_未知'	"识别错误失败"	“2067”

防火墙管理中心UI更改



软件架构

此功能高度依赖于现有的操作队列框架。该功能使用底层lina CLI生成HA高级故障排除数据。

常见问题解答

问:此功能是否适用于FTD升级还原功能？
A：否。此功能不适用于还原功能，因为FTD还原并行工作，而不是1乘1。

问:如果在200_enable_maintenance_mode.pl升级失败，是否会生成高级故障排除数据？
A：不需要。只有在升级后重新启动后才会生成HA高级故障排除，而在升级失败时不会生成

问:如果由于第二台设备上的HA验证而阻止升级，用户能否单独触发第二台设备的升级？
A：Yes.用户必须再次选择HA对进行升级，FMC仅在未升级的设备上触发升级。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。