Reduce Secure Firewall 7.6 FTD HA Upgrade Failure

Contents

Introduction

This document describes troubleshooting to address FTD upgrade failures from versions 7.0 to 7.2, particularly in High Availability (HA) deployments.

Background Information

Over half of these failures stem from issues during the 200_enable_maintenance_mode phase, with existing HA validations mainly performing basic active/standby state checks, which are insufficient for comprehensive HA transitions.

With the Secure Firewall 7.6 update, improved HA validations have been introduced to tackle these problems. These enhancements include thorough checks for HA state transitions, extended timeouts for synchronization processes, and enhanced error reporting. This update aims to significantly reduce post-upgrade HA issues and overall upgrade failures, ensuring a smoother and more reliable upgrade process for HA deployments.

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

Problem

- There are a significant number of FTD upgrade failures reported by customers across 7.0, 7.1, and 7.2 releases for HA deployments.
- More than 50% of failures come from FTD HA deployments. Failures in 200_enable_maintenance_mode contribute to HA failures.
- Existing HA state validations are basic validations like active/standby state checks and do not validate the HA transitions completely.

What's New (Solution)

Improved HA validations for FTD upgrade:

- Validation for HA state transition
- Improved FTD HA upgrade timeouts for HA transition state like config sync(7200 seconds), app sync(1200 seconds), and bulk sync(7200 seconds)
- Giving more control to FMC on when to start or fail the FTD upgrade
- Improved error reporting and recovery message for FTD HA upgrades

As compared to previous releases, it has:

- Improved HA validations helps reduce the post-upgrade HA creation issues in HA deployments
- Improved validations helps to reduce FTD upgrade failures

Prerequisites

Supported Platforms

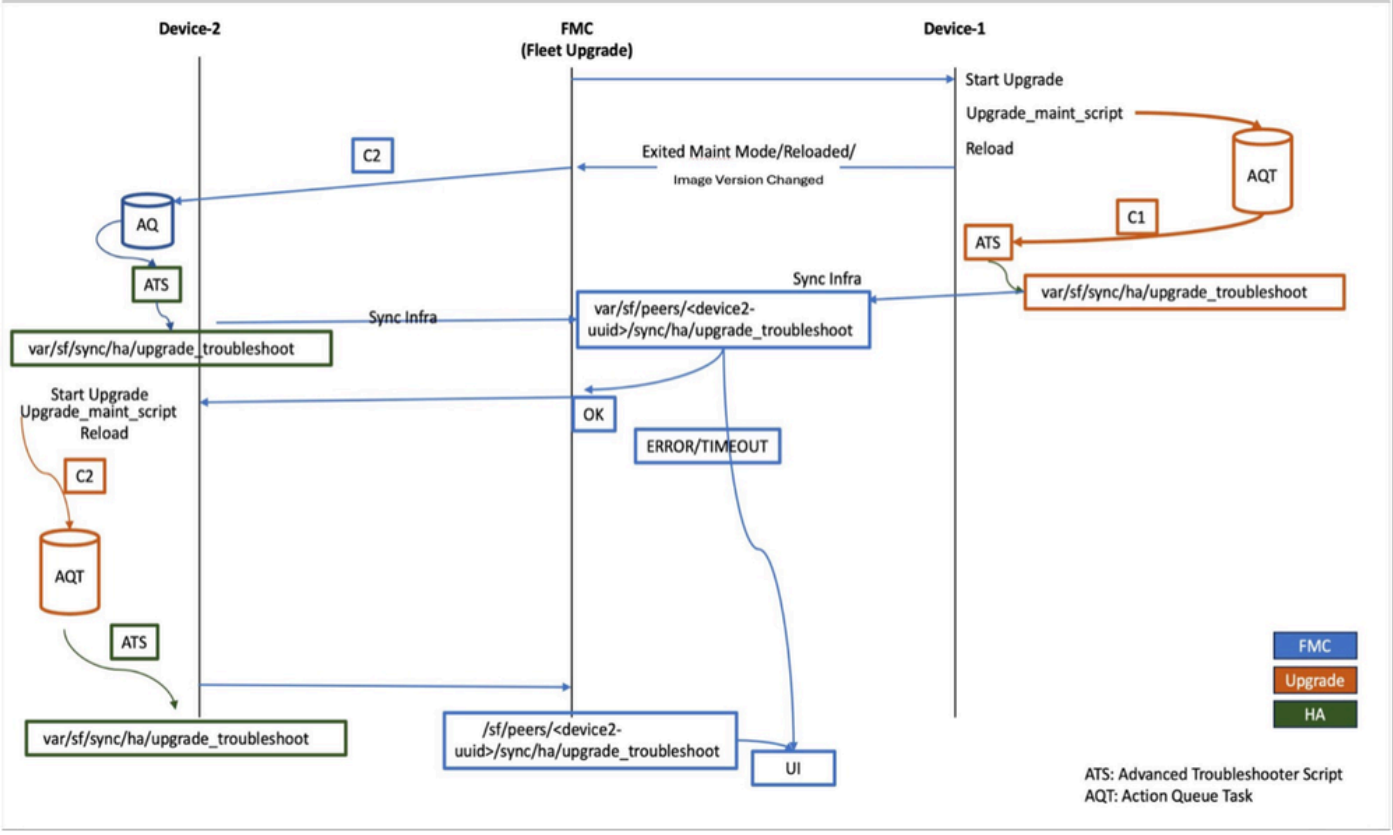
- Manager(s) and Version (s) : FMC 7.6.0
- Application (ASA/FTD) and Minimum Version of Application: FTD 7.6.0; FMC managing 7.6.0 FTD HA
- Supported Platforms: All platforms running FTD HA

Note: This feature applies to only FMC-managed FTD HA deployments. This feature does not apply to FDM-managed FTD HA or clustered devices.

Feature Overview

- This feature helps in reducing FTD upgrade failures in HA deployment by checking the HA states of upgraded units by FMC after the reboot part of the upgrade process.
- After the upgrade reboot, FMC checks for active/standby state and any failures in HA synchronization.
- FTD notifies FMC on when to start or fail the upgrade on the second node in the form of a new HA advance troubleshoot.
- If there is any failure in joining the HA post-upgrade reboot, an appropriate message is displayed on the FMC UI.

New Upgrade Workflow for FTD HA


Device-2
FMC
(Fleet Upgrade)
Device-1
Start Upgrade
Upgrade_maint_script
Reload
AQT
C1
ATS
Exited Maint Mode/Reloaded/
Image Version Changed
C2
AQ
ATS
Sync Infra
var/sf/sync/ha/upgrade_troubleshoot
var/sf/peers/<device2-uuid>/sync/ha/upgrade_troubleshoot
Sync Infra
var/sf/sync/ha/upgrade_troubleshoot
Start Upgrade
Upgrade_maint_script
Reload
OK
ERROR/TIMEOUT
C2
AQT
ATS
var/sf/sync/ha/upgrade_troubleshoot
/sf/peers/<device2-uuid>/sync/ha/upgrade_troubleshoot
UI
FMC
Upgrade
HA
ATS: Advanced Troubleshooter Script
AQT: Action Queue Task

Standby Unit is the First to Upgrade

First unit upgrade (Standby Unit)

- During the first unit upgrade, the upgrade script initiates action_queue task to collect HA advance troubleshoot data at 999_finish stage.
- Inserted task execution starts only after post-upgrade reboot and collects troubleshoot information in the form of JSON file.
- The same JSON file is synced to FMC.
- Once the first node exits from maintenance mode, FMC triggers a remote action_queue task on the active unit in order to collect the HA advance troubleshoot (Active unit needs to be 7.6 or above). If the active unit is found lower than 7.6, no troubleshoot is collected from the active unit and FMC takes decision based only on troubleshoot collected from the standby unit.

Once HA advance troubleshoot is collected from both units, FMC decides to start the upgrade or block the upgrade on the second node (active unit).

Second Unit Upgrade (Active Unit)

- Similar to the standby unit, the upgrade script initiates the action_queue task to collect HA advance troubleshoot at 999_finish stage.
- Inserted task execution start only post-upgrade reboot and generates troubleshoot information in the form of a JSON file.
- The same file is synced to FMC.
- If either of the units reports HA failure, HA failure data is shown on the FMC UI on the upgrade tab.
- In case of any failure in joining HA post-upgrade reboot, the upgrade is marked completed and on the same upgrade tab HA validation failures are reported.

HA Advance Troubleshoot

- HA advance troubleshoot is a new single JSON file introduced as part of this feature which contains HA information. It is generated after the reboot after an upgrade and sent from the FTD to the FMC.
- File name and path: /ngfw/var/sf/sync/ha/upgrade_troubleshoot
- As soon as FMC collects the HA advance troubleshoot from the first (standby) unit, FMC triggers a remote task to collect the same information from the active unit.
    - This remote data collection is only supported when the devices are running 7.6 or higher.
    - If devices are found running a version less than 7.6, then remote data collection is skipped. So, in this case, FMC would only collect data from the standby unit and decide for further action.

- HA advance troubleshoot generation is quick. If Lina is down and fails to generate the report, it immediately exits.
    - Device reboot time depends on platform to platform and reboot time is the same as we have documented for each platform.

HA Advance Troubleshoot Report

Each HA unit generates an HA advance troubleshoot data in form of JSON file post-upgrade reboot and shares it with FMC. Here are validation examples when there is a failure and success.

Example of HA Validation Failure

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

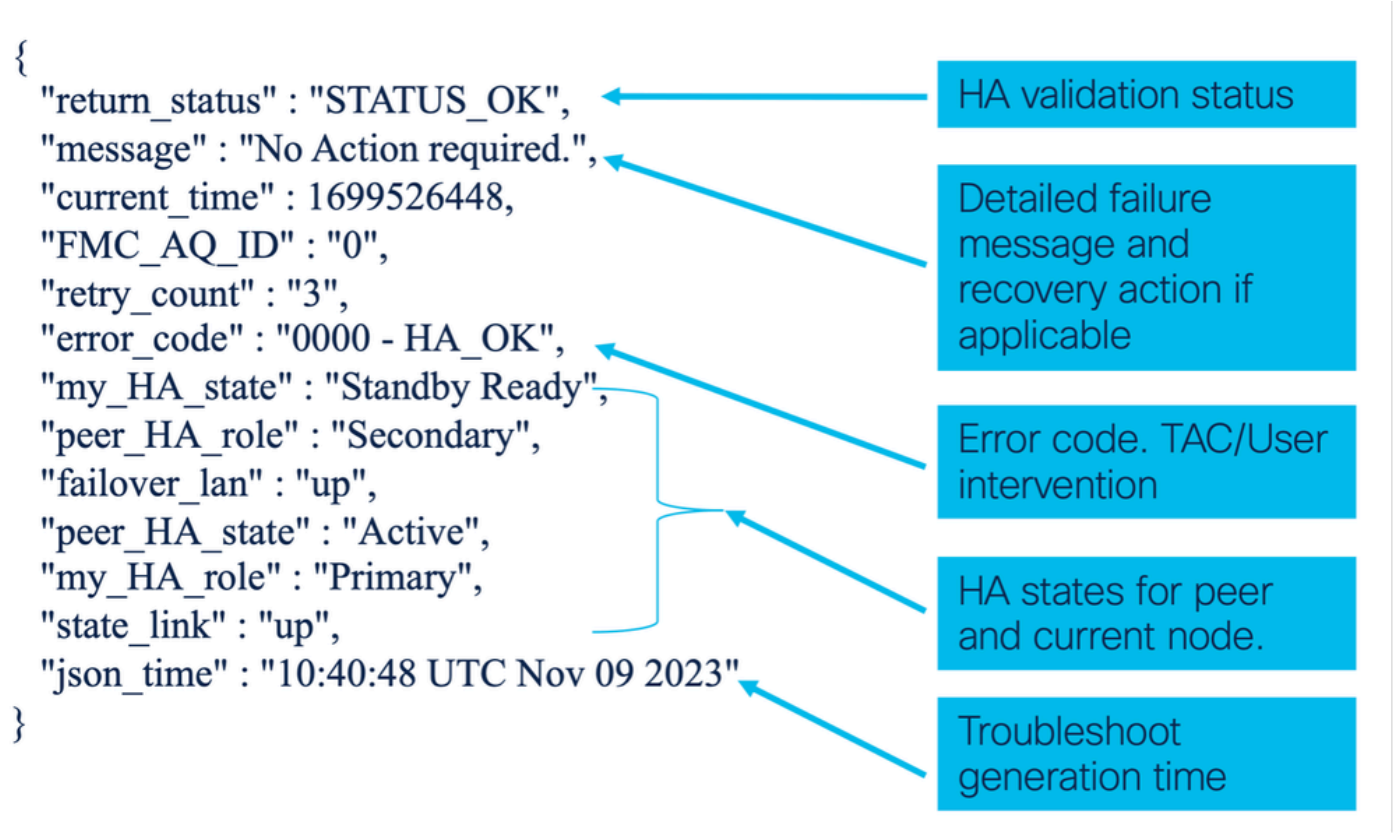
```
{
"failover_lan" : "NA",
"error_code" : "1046 -
STARTUP_FAILOVER_CONFIG_NOT_PRESENT",
"current_time" : 1701369637,
"peer_HA_state" : "Not Detected",
"FMC_AQ_ID" : "0",
"state_link" : "NA",
"json_time" : "18:40:37 UTC Nov 30 2023",
"my_HA_state" : "Disabled",
"my_HA_role" : "Secondary",
"return_status"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

Example of Successful HA Validation

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
}
```

HA Advance Troubleshoot Contents



```
{
  "return_status" : "STATUS_OK",
  "message" : "No Action required.",
  "current_time" : 1699526448,
  "FMC_AQ_ID" : "0",
  "retry_count" : "3",
  "error_code" : "0000 - HA_OK",
  "my_HA_state" : "Standby Ready",
  "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 2023"
}
```

HA validation status
Detailed failure message and recovery action if applicable
Error code. TAC/User intervention
HA states for peer and current node.
Troubleshoot generation time

Location of HA Advance Troubleshoot File

HA advance troubleshoot JSON file location:

```
On FTD: /ngfw/var/sf/sync/ha/upgrade_troubleshoot
On FMC: /var/sf/peers/<peer-uuid>/sync/ha/upgrade_troubleshoot
```

- The HA troubleshoot relies on the lina command.
  - If troubleshoot fails to generate at /ngfw/var/sf/sync/ha/upgrade_troubleshoot, user can refer to

    logs at: /ngfw/var/log/ha_upgrade_troubleshoot.log

- /ngfw/var/sf/sync/ha/upgrade_troubleshoot and /ngfw/var/log/ha_upgrade_troubleshoot.log files are part of FTD Troubleshoot file.

Tips for HA Advance Troubleshoot Generation Issues

Sometimes HA advance troubleshoot is not be generated due to system state and reason for this could be lina down or action queue process is down post upgrade reboot. If lina or action queue is down, this is a problem.

In such cases, check to see if lina and ActionQueue processes are running by using this command in expert mode:

```
<#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
```

Return Status and Action in HA Advance Troubleshoot

- STATUS_INIT: This indicates the HA troubleshoot has been triggered.
- STATUS_OK: The device is in a stable state. No action is required.
- STATUS ERROR: This determines an error has occurred due to which HA is not formed. The user needs to take an action based on the message displayed or the user needs to contact TAC.
- STATUS_RETRY: The device can be in one of the intermediate states. The HA troubleshoot keeps retrying after a fixed interval based on the state until STATUS_ERROR or STATUS_OK is encountered.
    - Based on failures encountered STATUS ERROR, the HA failures are categorized into 2 cases:
        - User Intervention – These HA failures can be fixed by the user, and the user can resume the upgrade, where the TAC intervention is not required.
        - TAC intervention – For these HA failures, the user cannot fix it by themselves; TAC intervention is required.

Error Code and Classification

Based on error codes, Errors are classified as shown here:

return_status	**error_code**	**Description**	**Retry or Recovery Mechanism**

STATUS_OK	“0000 – HA_OK”(Reserved values are from 0001 – 1023)	This is for the success scenario. (Where the HA states are Active and Standby Ready)	(Not Applicable)
STATUS_ERROR	“1024:2047 – ERROR_REASON”	This is for the error scenario (user intervention)	Actionable messages to be displayed to the user and upgrade framework can add the retry or recovery mechanism in the future (if any).
STATUS_ERROR	“2048:3071 – ERROR_REASON”	This is for the error scenario (TAC intervention)	TAC intervention is required for recovery.

User Intervention Messages

Error	Error Message	Error code
'FAILOVER_CONFIG_NOT_PRSENT'	"Failover config is not present on the device"	"1024"
'FAILOVER_IS_NOT_ENABLED'	"Failover is not enabled on the device. Please enable failover"	"1025"
'FAILOVER_LAN_DOWN'	"Failover LAN is down on the device"	"1026"
'STATE_LINK_DOWN'	"State Link is down on the device"	"1027"
'FAILOVER_BLOCK_DEPLETION'	"Block depletion on the following blocks in the device:\n"	"1028"
'APP_SYNC_TIMEOUT'	"App sync timeout on the device"	"1029"
'CD_APP_SYNC_ERROR'	"CD app sync error detected	"1030"

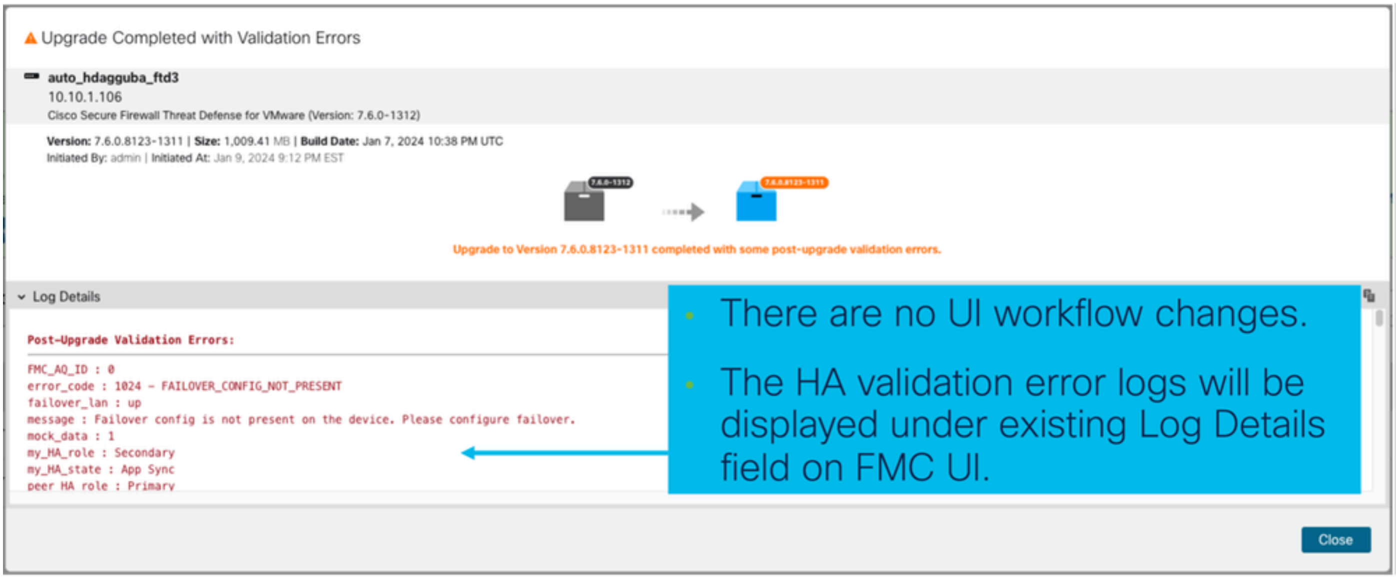
	on the device"	
'CONFIG_SYNC_TIMEOUT'	"Config sync timeout on the device"	"1031"
'FAILED_TO_APPLY_CONFIG'	"Failed to apply configuration on the device"	"1032"
'BULK_SYNC_TIMEOUT'	"Bulk sync timeout on the device"	"1033"
'BULK_SYNC_CLIENT_ISSUE'	"Check the following clients on the device:\n"	"1034"
'IFC_CHECK_FAILED'	"Failover interface check failed on following interfaces in the device:\n"	"1035"
'IFC_FAILED_CHECK_VLAN_SPANTREE'	"Since the interfaces are up. Please check if the VLANs are allowed on the switch side or there is a spanning tree issue"	"1036"
'VERSION_MISMATCH'	"Different software version on the other device"	"1037"
'MODE_MISMATCH'	"Different operating mode on the other device"	"1038"
'LIC_MISMATCH'	"Different license on the other device"	"1039"
'CHASSIS_MISMATCH'	"Different chassis configuration on the other device"	"1040"
'CARD_MISMATCH'	"Different card configuration on the other device"	"1041"
'PEER_NOT_OK'	"This device is in Okay state. Check the peer device"	"1042"

TAC Intervention Messages

Error	Error Message	Error code
'RUN_CMD_FAILED'	"Failed to run command"	"2048"
'LINA_NOT_STARTED'	"Lina not started on the device. Try again after some time"	"2049"'
'HWIDB_MISMATCH'	"HWIDB index is different on the device"	"2050"
'BACKPLANE_FAILURE'	"Backplane failure on the device. Check the backplane"	"2051"
'HA_PROGR_FAILURE'	"HA progression failure on the device"	"2052"
'SVM_FAILURE'	"Service Module failed on the device"	"2053"
'SVM_MIO_HB_FAILURE'	"Heartbeat failure between MIO and App-agent on the device"	"2054"
'SVM_MIO_CRUZ_FAILED'	"MIO-blade network adapter failure on the device"	"2055"
'SVM_MIO_HB_CRUZ_FAILED'	"MIO-blade Heartbeat and network adapter failure on the device"	"2056"
'SSM_CARD_FAILURE'	"Service card failure on the device"	"2057"
'MY_COMM_FAILURE'	"Communication failure on the device"	"2058"
'CRITICAL_PROCESS_DIED'	"Critical process died on the device"	"2059"
'SNORT_FAILURE'	"Snort failed on the device"	"2060"

'PEER_SVM_FAILURE'	"NGFW Service Module has failed on the other device"	"2061"
'FAULT_MON_BLOCK_DEP'	"Fault monitoring reported block depletion on the device"	"2062"
'DISK_FAILURE'	"Disk failed on the device"	"2063"
'SNORT_DiSK_FAILURE'	"Snort and Disk failed on the device	"2064"
'INACTIVE_MATE_FOUND"	"Detected an inactive mate during bootup	"2065"
'SCRIPT_TIMEOUT'	"Retry limit exceeded. Exiting script"	"2066"
'ERROR_UNKNOWN'	"Failed to identify error"	"2067"

Firewall Management Center UI Changes



Upgrade Completed with Validation Errors

auto_hdagguba_ftd3
10.10.1.106
Cisco Secure Firewall Threat Defense for VMware (Version: 7.6.0-1312)

Version: 7.6.0.8123-1311 | **Size:** 1,009.41 MB | **Build Date:** Jan 7, 2024 10:38 PM UTC
Initiated By: admin | Initiated At: Jan 9, 2024 9:12 PM EST

Upgrade to Version 7.6.0.8123-1311 completed with some post-upgrade validation errors.

```
Post-Upgrade Validation Errors:

FMC_AQ_ID : 0
error_code : 1024 - FAILOVER_CONFIG_NOT_PRESENT
failover_lan : up
message : Failover config is not present on the device. Please configure failover.
mock_data : 1
my_HA_role : Secondary
my_HA_state : App Sync
peer HA role : Primary
```

- There are no UI workflow changes.
- The HA validation error logs will be displayed under existing Log Details field on FMC UI.

Software Architecture

This feature is highly dependent on existing action queue framework. The feature uses underlying lina CLI to generate the HA advance troubleshoot data.

FAQs

Q: Is the feature applicable for FTD upgrade revert functionality?

A: No. This feature is not applicable for revert functionality as FTD revert works in parallel, not 1-by-1.

Q: If upgrade fails at 200_enable_maintenance_mode.pl, does it generate the advance troubleshoot data?
A: No. HA advance troubleshoot is generated only after post-upgrade reboot and not during upgrade failure

Q: If upgrade is blocked due to HA validations on second unit, can a user trigger upgrade on second unit alone?
A: Yes. User has to select the HA pair again for upgrade and FMC triggers the upgrade only on non-upgraded unit.