

Secure Firewall 7.6 FTD HA 업그레이드 실패 감소

목차

[소개](#)

[배경 정보](#)

[문제](#)

[새로운 기능\(솔루션\)](#)

[사전 요구 사항](#)

[지원되는 플랫폼](#)

[기능 개요](#)

[FTD HA에 대한 새 업그레이드 워크플로](#)

[스탠바이 유닛은 첫 번째 업그레이드](#)

[첫 번째 유닛 업그레이드\(스탠바이 유닛\)](#)

[두 번째 유닛 업그레이드\(액티브 유닛\)](#)

[HA 고급 문제 해결](#)

[HA 고급 문제 해결 보고서](#)

[HA 검증 실패의 예](#)

[성공적인 HA 검증의 예](#)

[HA 고급 문제 해결 콘텐츠](#)

[HA 고급 문제 해결 파일의 위치](#)

[HA 고급 문제 해결 팁](#)

[HA Advance Troubleshoot의 Return Status and Action](#)

[오류 코드 및 분류](#)

[사용자 개입 메시지](#)

[TAC 개입 메시지](#)

[Firewall Management Center UI 변경](#)

[소프트웨어 아키텍처](#)

[FAQ](#)

소개

이 문서에서는 특히 HA(고가용성) 구축에서 버전 7.0에서 7.2로의 FTD 업그레이드 실패를 해결하기 위한 트러블슈팅에 대해 설명합니다.

배경 정보

이러한 장애의 절반 이상은 200_enable_maintenance_mode 단계의 문제에서 비롯되며, 기존 HA 검증은 주로 기본 활성/대기 상태 점검을 수행하는데, 이는 포괄적 HA 전환에는 충분하지 않습니다.

Secure Firewall 7.6 업데이트를 통해 이러한 문제를 해결하기 위해 향상된 HA 검증이 도입되었습니다. 이러한 개선 사항에는 HA 상태 전환에 대한 철저한 검사, 동기화 프로세스에 대한 시간 초과 연장, 향상된 오류 보고 등이 포함됩니다. 이번 업데이트는 업그레이드 후 HA 문제 및 전반적인 업그레이드 실패를 크게 줄여 HA 구축을 위한 더욱 원활하고 안정적인 업그레이드 프로세스를 보장하는 데 목적이 있습니다.

마이그레이션 원본: <https://confluence-eng-rtp2.cisco.com/conf/display/IFT/FTD+HA+Upgrade+Failure+Reduction>

문제

- HA 구축의 경우 7.0, 7.1, 7.2 릴리스에서 고객이 보고한 FTD 업그레이드 실패가 상당히 많습니다.
- 장애의 50% 이상은 FTD HA 구축에서 발생합니다. 200_enable_maintenance_mode에서 장애가 발생하면 HA 장애가 발생합니다.
- 기존 HA 상태 검증은 액티브/스탠바이 상태 확인과 같은 기본 검증이며 HA 전환을 완전히 검증하지는 않습니다.

새로운 기능(솔루션)

FTD 업그레이드를 위한 향상된 HA 검증:

- HA 상태 전환에 대한 검증
- 구성 동기화(7200초), 앱 동기화(1200초), 대량 동기화(7200초)와 같은 HA 전환 상태에 대한 FTD HA 업그레이드 시간 초과 개선
- FTD 업그레이드 시작 또는 실패 시점에 대해 FMC에 더 많은 제어 권한 부여
- FTD HA 업그레이드를 위한 향상된 오류 보고 및 복구 메시지

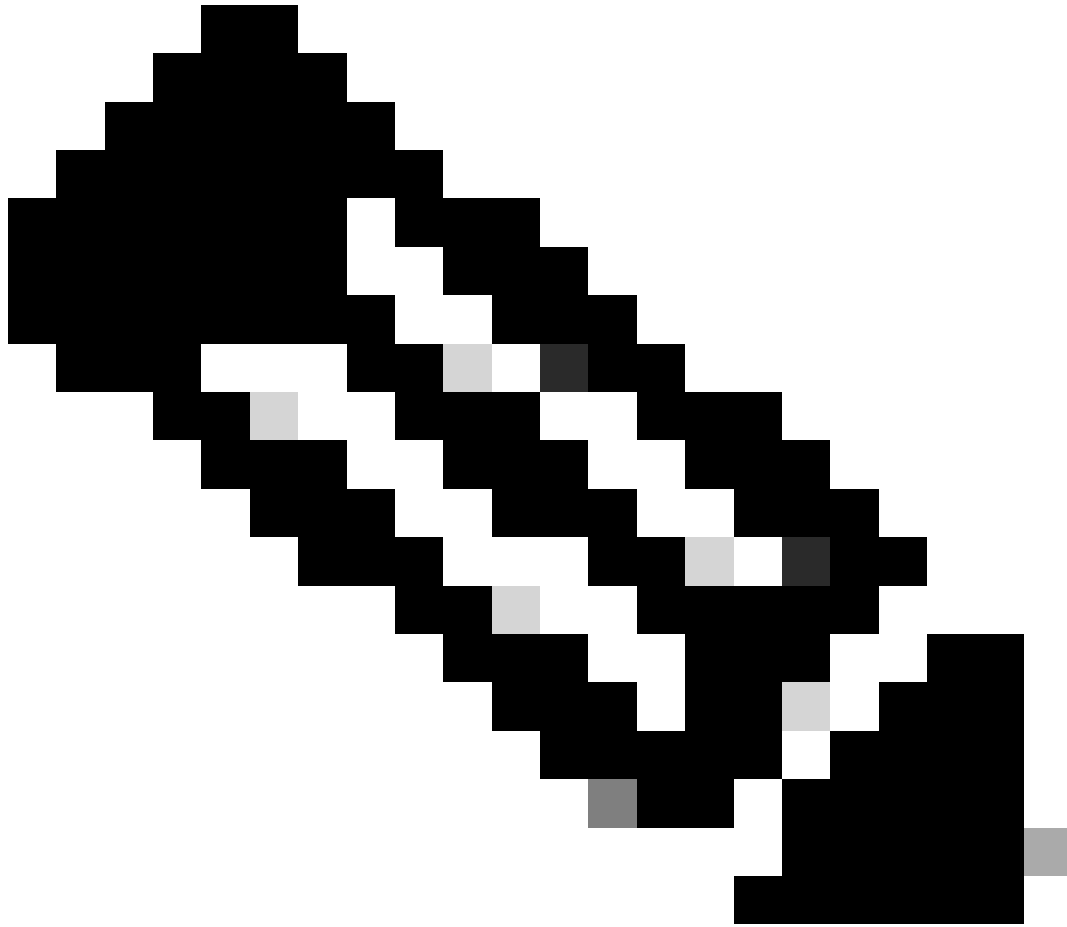
이전 릴리스와 비교하여 다음과 같은 특징이 있습니다.

- 향상된 HA 검증으로 HA 구축에서 업그레이드 후 HA 생성 문제 감소
- 향상된 검증 기능을 통해 FTD 업그레이드 실패 감소

사전 요구 사항

지원되는 플랫폼

- 관리자 및 버전: FMC 7.6.0
- 애플리케이션(ASA/FTD) 및 최소 애플리케이션 버전: FTD 7.6.0; FMC 관리 7.6.0 FTD HA
- 지원되는 플랫폼: FTD HA를 실행하는 모든 플랫폼

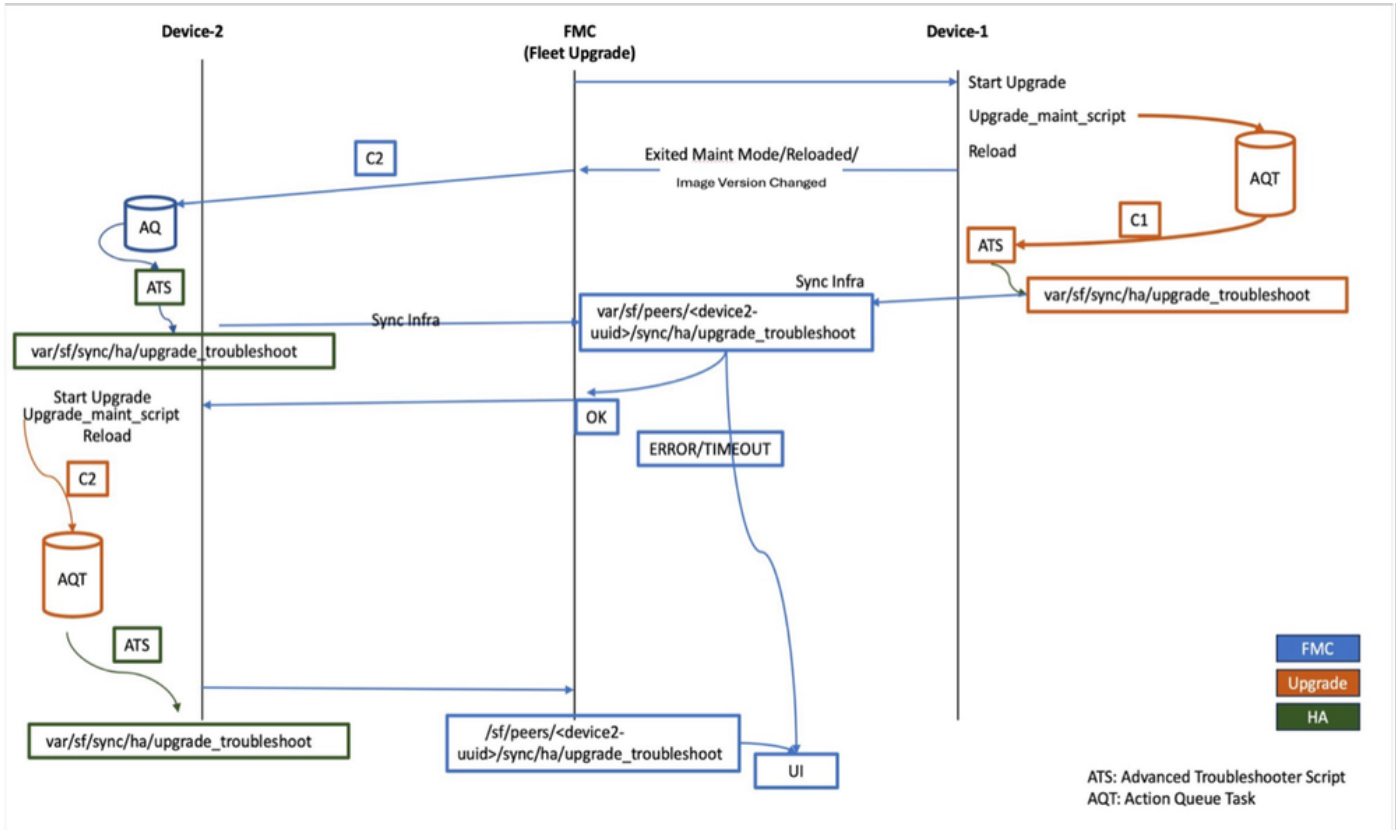


참고: 이 기능은 FMC 관리 FTD HA 구축에만 적용됩니다. 이 기능은 FDM 관리 FTD HA 또는 클러스터링된 디바이스에는 적용되지 않습니다.

기능 개요

- 이 기능은 업그레이드 프로세스의 재부팅 부분 이후 FMC에서 업그레이드된 유닛의 HA 상태를 확인하여 HA 구축에서 FTD 업그레이드 실패를 줄이는 데 도움이 됩니다.
- 업그레이드 재부팅 후 FMC는 액티브/스탠바이 상태 및 HA 동기화 실패를 확인합니다.
- FTD는 새 HA 고급 문제 해결 형식으로 두 번째 노드에서 업그레이드를 언제 시작할지 또는 실패할지를 FMC에 알립니다.
- HA 업그레이드 후 재부팅 참여에 장애가 발생하면 FMC UI에 적절한 메시지가 표시됩니다.

FTD HA에 대한 새 업그레이드 워크플로



스탠바이 유닛은 첫 번째 업그레이드

첫 번째 유닛 업그레이드(스탠바이 유닛)

- 첫 번째 유닛 업그레이드 과정에서 업그레이드 스크립트는 `action_queue` 작업을 시작하여 `999_finish` 단계에서 HA 고급 문제 해결 데이터를 수집합니다.
- 삽입된 작업 실행은 업그레이드 후 재부팅 후에만 시작되며 JSON 파일 형식의 문제 해결 정보를 수집합니다.
- 동일한 JSON 파일이 FMC에 동기화됩니다.
- 첫 번째 노드가 유지 관리 모드에서 종료되면 FMC는 HA 고급 문제 해결을 수집하기 위해 활성 유닛에서 `remote action_queue` 작업을 트리거합니다(활성 유닛은 7.6 이상이어야 함). 액티브 유닛이 7.6 미만이면 액티브 유닛에서 트러블슈팅이 수집되지 않으며 FMC는 스탠바이 유닛에서 수집된 트러블슈팅만 기반으로 결정을 내립니다.

두 유닛에서 HA 고급 문제 해결이 수집되면 FMC는 업그레이드를 시작하거나 두 번째 노드(액티브 유닛)에서 업그레이드를 차단하도록 결정합니다.

두 번째 유닛 업그레이드(액티브 유닛)

- 스탠바이 유닛과 마찬가지로 업그레이드 스크립트는 `999_finish` 단계에서 HA 고급 문제 해결을 수집하기 위해 `action_queue` 작업을 시작합니다.
- 삽입된 작업 실행은 업그레이드 후 재부팅만 시작하고 문제 해결 정보를 JSON 파일 형식으로 생성합니다.
- 동일한 파일이 FMC에 동기화됩니다.
- 유닛 중 하나에서 HA 장애를 보고하면 HA 장애 데이터가 업그레이드 탭의 FMC UI에 표시됨

니다.

- HA 사후 업그레이드 재부팅 참여에 실패한 경우 업그레이드가 완료된 것으로 표시되고 동일한 업그레이드 탭에서 HA 검증 실패가 보고됩니다.

HA 고급 문제 해결

- HA 고급 문제 해결은 HA 정보가 포함된 이 기능의 일부로 도입된 새로운 단일 JSON 파일입니다. 업그레이드 후 재부팅 후에 생성되고 FTD에서 FMC로 전송됩니다.
- 파일 이름 및 경로: /ngfw/var/sf/sync/ha/upgrade_troubleshoot
- FMC는 첫 번째(대기) 유닛에서 HA 고급 문제 해결을 수집하는 즉시 원격 작업을 트리거하여 활성 유닛에서 동일한 정보를 수집합니다.
 - 이 원격 데이터 수집은 디바이스가 7.6 이상을 실행 중인 경우에만 지원됩니다.
 - 7.6 미만의 버전을 실행 중인 디바이스가 발견되면 원격 데이터 수집을 건너뛵니다. 따라서 이 경우 FMC는 스탠바이 유닛에서 데이터를 수집하고 추가 작업을 결정합니다.
- HA 고급 문제 해결 생성이 빠릅니다. Lina가 다운되어 보고서를 생성하지 못하면 즉시 종료됩니다.
 - 디바이스 재부팅 시간은 플랫폼마다 다르며 재부팅 시간은 각 플랫폼에 대해 설명한 것과 동일합니다.

HA 고급 문제 해결 보고서

각 HA 유닛에서는 JSON 파일 업그레이드 후 재부팅 형식으로 HA 고급 문제 해결 데이터를 생성하고 FMC와 공유합니다. 다음은 실패와 성공이 있을 때의 검증 예입니다.

HA 검증 실패의 예

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

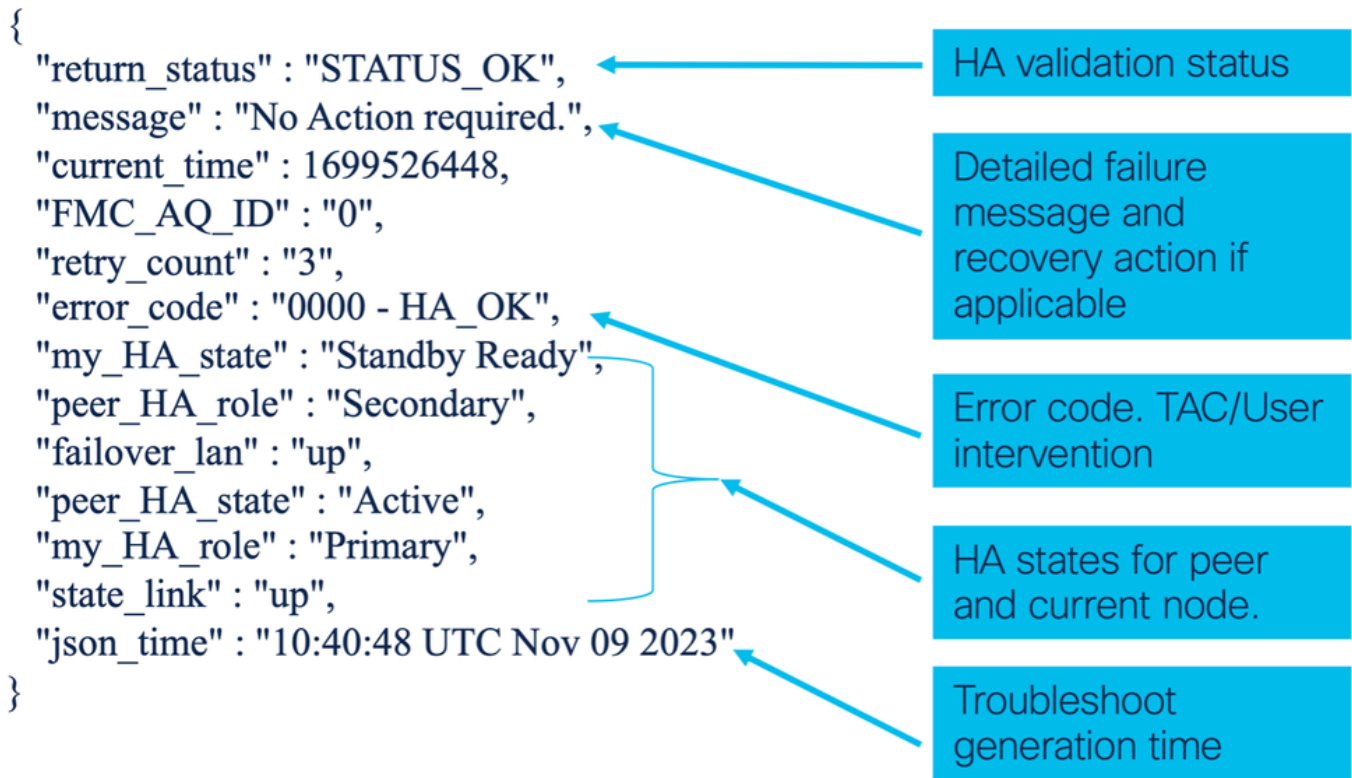
```
{
  "failover_lan" : "NA",
  "error_code" : "1046 -
STARTUP_FAILOVER_CONFIG_NOT_PRESENT",
  "current_time" : 1701369637,
  "peer_HA_state" : "Not Detected",
  "FMC_AQ_ID" : "0",
  "state_link" : "NA",
  "json_time" : "18:40:37 UTC Nov 30 2023",
  "my_HA_state" : "Disabled",
  "my_HA_role" : "Secondary",
  "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"
}
```

성공적인 HA 검증의 예

파일: /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 고급 문제 해결 콘텐츠



HA 고급 문제 해결 파일의 위치

HA 고급 JSON 파일 위치 문제 해결:

On FTD: /ngfw/var/sf/sync/ha/upgrade_troubleshoot

On FMC: /var/sf/peers/

/sync/ha/upgrade_troubleshoot

- HA 트러블슈팅은 lina 명령을 사용합니다.
 - /ngfw/var/sf/sync/ha/upgrade_troubleshoot에서 트러블슈팅을 생성하지 못하면 /ngfw/var/log/ha_upgrade_troubleshoot.log에서 로그를 참조할 수 있습니다.
- /ngfw/var/sf/sync/ha/upgrade_troubleshoot 및 /ngfw/var/log/ha_upgrade_troubleshoot.log 파일은 FTD 문제 해결 파일의 일부입니다.

HA 고급 문제 해결 팁

때로는 시스템 상태 및 이로 인한 이유로 인해 HA 고급 문제 해결이 생성되지 않고 lina가 중단되거나 작업 대기열 프로세스가 업그레이드 후 다운된 것일 수 있습니다. lina 또는 작업 대기열이 다운된 경우 문제가 됩니다.

이러한 경우 expert 모드에서 다음 명령을 사용하여 lina 및 ActionQueue 프로세스가 실행 중인지 확인합니다.

<#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 Advance Troubleshoot의 Return Status and Action

- 상태 초기화: 이는 HA 트러블슈팅이 트리거되었음을 나타냅니다.
- 상태 확인(_O): 디바이스가 안정적인 상태입니다. 추가 작업은 필요하지 않습니다.
- 상태 오류: 이는 HA가 형성되지 않은 오류가 발생했음을 확인합니다. 사용자는 표시된 메시지

에 따라 조치를 취하거나 TAC에 문의해야 합니다.

- 상태 다시 시도(_R): 디바이스는 중간 상태 중 하나일 수 있습니다. HA 트러블슈팅은 STATUS_ERROR 또는 STATUS_OK가 나타날 때까지 상태를 기준으로 고정 간격이 지난 후에도 계속 재시도합니다.
 - STATUS_ERROR에서 발생한 장애를 기반으로 HA 장애는 2가지 경우로 분류됩니다.
 - 사용자 개입 - 이러한 HA 오류는 사용자가 해결할 수 있으며, 사용자는 업그레이드를 다시 시작할 수 있습니다. 이 경우 TAC 개입이 필요하지 않습니다.
 - TAC 개입 - 이러한 HA 장애에 대해서는 사용자가 직접 해결할 수 없습니다. TAC 개입이 필요합니다.

오류 코드 및 분류

오류 코드에 따라 오류가 다음과 같이 분류됩니다.

반환 상태	오류 코드	설명	재시도 또는 복구 메커니즘
상태 확인(_O)	"0000 - HA_OK"(예약된 값은 0001 - 1023)	이는 성공 시나리오를 위한 것입니다. (여기서 HA 상태는 Active 및 Standby Ready)	(해당 없음)
상태_오류	"1024:2047 - ERROR_REASON"	오류 시나리오를 위한 것입니다(사용자 개입).	사용자 및 업그레이드 프레임워크에 표시할 실행 가능한 메시지는 향후 재시도 또는 복구 메커니즘(있는 경우)을 추가할 수 있습니다.
상태_오류	"2048:3071 - ERROR_REASON"	이는 오류 시나리오 (TAC 개입)를 위한 것입니다.	복구를 위해서는 TAC 개입이 필요합니다.

사용자 개입 메시지

오류	오류 메시지	오류 코드
'FAILOVER_CONFIG_NOT_PRESENT'	"장애 조치 컨피그레이션이"	"1024"

	디바이스에 없습니다."	
'FAILOVER_IS_NOT_ENABLED'	"디바이스에서 장애 조치가 활성화되지 않았습니다. 장애 조치를 활성화하십시오."	"1025"
'FAILOVER_LAN_DOWN'	"장애 조치(failover) LAN이 디바이스에서 다운되었습니다."	"1026"
'STATE_LINK_DOWN'	"디바이스의 상태 링크가 다운되었습니다."	"1027"
'FAILOVER_BLOCK_DEPLETION'	"디바이스의 다음 블록에 대한 고갈 차단:\n"	"1028"
'APP_SYNC_TIMEOUT'	"디바이스에서 앱 동기화 시간 초과"	"1029"
'CD_APP_SYNC_ERROR'	"디바이스에서 CD 앱 동기화 오류가 검색되었습니다."	"1030"
'CONFIG_SYNC_TIMEOUT'	"디바이스에서 컨피그레이션 동기화 시간 초과"	"1031"
'FAILED_TO_APPLY_CONFIG'	"디바이스에 컨피그레이션을 적용하지 못했습니다."	"1032"
'BULK_SYNC_TIMEOUT'	"디바이스에서 대량 동기화 시간 초과"	"1033"
'BULK_SYNC_CLIENT_ISSUE'	"디바이스에서 다음 클라이언트를 확인하십시오.\n"	"1034"
'IFC_CHECK_FAILED'	"디바이스의 다음 인터페이스에서 장애 조치 인터페이스를 확인하지 못했습니다"	"1035"

	.\n"	
'IFC_FAILED_CHECK_VLAN_SPANTREE'	"인터페이스가 가동 중이므로 스위치 측에서 VLAN이 허용되는지 아니면 스페닝 트리 문제가 있는지 확인하십시오."	"1036"
'VERSION_MISMATCH'	"다른 디바이스의 다른 소프트웨어 버전"	"1037"
'MODE_MISMATCH'	"다른 디바이스의 다른 작동 모드"	"1038"
'LIC_MISMATCH'	"다른 디바이스의 다른 라이선스"	"1039"
'CHASSIS_MISMATCH'	"다른 디바이스의 다른 새시 컨피그레이션"	"1040"
'CARD_MISMATCH'	"다른 디바이스의 다른 카드 컨피그레이션"	"1041"
'PEER_NOT_OK'	"이 디바이스는 정상 상태입니다. 피어 디바이스 확인"	"1042"

TAC 개입 메시지

오류	오류 메시지	오류 코드
'RUN_CMD_FAILED'	"명령을 실행하지 못했습니다."	"2048"
'LINA_NOT_STARTED'	"리나는 장치에서 시작하지 않았습니다. 잠시 후에 다시 시도하십시오."	"2049"
'HWIDB_MISMATCH'	"HWIDB 인덱스가 디바이스에서"	"2050"

	다릅니다."	
'BACKPLANE_FAILURE'	"디바이스의 백플레인 오류입니다. 백플레인 확인"	"2051"
'HA_PROGR_FAILURE'	"디바이스의 HA 진행 실패"	"2052"
'SVM_FAILURE'	"디바이스에서 서비스 모듈 실패"	"2053"
'SVM_MIO_HB_FAILURE'	"디바이스의 MIO와 App-agent 간의 하트비트 오류"	"2054"
'SVM_MIO_CRUZ_FAILED'	"디바이스의 MIO-blade 네트워크 어댑터 오류"	"2055"
'SVM_MIO_HB_CRUZ_FAILED'	"디바이스의 MIO-blade Heartbeat 및 네트워크 어댑터 오류"	"2056"
'SSM_CARD_FAILURE'	"디바이스의 서비스 카드 오류"	"2057"
'MY_COMM_FAILURE'	"디바이스의 통신 실패"	"2058"
'CRITICAL_PROCESS_DEAD'	"중요한 프로세스가 장치에서 중단되었습니다."	"2059"
'SNORT_FAILURE'	"디바이스에서 Snort 실패"	"2060"
'PEER_SVM_FAILURE'	"NGFW 서비스 모듈이 다른 디바이스에서 실패했습니다."	"2061"
'FAULT_MON_BLOCK_DEP'	"결합 모니터링에서 디바이스의 블록 고갈을 보고했습니다."	"2062"
'DISK_FAILURE'	"디바이스에서 디스크 실패"	"2063"

'SNORT_DiSK_FAILURE'	"디바이스에서 Snort 및 디스크 실패	"2064"
'INACTIVE_MATE_FOUND"	"부팅 중에 비활성 짝이 검색되었습니다.	"2065"
'SCRIPT_TIMEOUT'	"재시도 제한이 초과되었습니다. 스크립트 종료"	"2066"
'오류_알 수 없음'	"오류를 식별하지 못했습니다."	"2067"

Firewall Management Center UI 변경

▲ Upgrade Completed with Validation Errors

auto_hdaguba_ftd3

10.10.1.106

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

Versions: 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

7.6.0-1310

→

7.6.0.8123-1311

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

▼ Log Details

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.

Close

소프트웨어 아키텍처

이 기능은 기존 작업 대기열 프레임워크에 크게 종속됩니다. 이 기능은 기본 lina CLI를 사용하여 HA 고급 문제 해결 데이터를 생성합니다.

FAQ

- Q: FTD 업그레이드 되돌리기 기능에 적용할 수 있는 기능입니까?

A : 아니요. FTD 되돌리기가 1:1이 아니라 병렬로 작동하므로 이 기능은 되돌리기 기능에 적용할 수 없습니다.
- Q: 200_enable_maintenance_mode.pl에서 업그레이드가 실패할 경우 고급 문제 해결 데이터가 생성됩니까?

A : 아니요. HA 고급 트러블슈팅은 업그레이드 실패 시점이 아니라 업그레이드 후 재부팅 후에만 생성됩니다

Q: 두 번째 유닛의 HA 검증으로 인해 업그레이드가 차단된 경우, 사용자가 두 번째 유닛에서만 업그레이드를 트리거할 수 있습니까?

A : 예. 사용자는 업그레이드를 위해 HA 쌍을 다시 선택해야 하며 FMC는 업그레이드되지 않은 유닛에서만 업그레이드를 트리거합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.