Reduza a falha de atualização do Secure Firewall 7.6 FTD HA

Contents

Introdução

Este documento descreve a solução de problemas para resolver falhas de atualização de FTD das versões 7.0 a 7.2, particularmente em implantações de alta disponibilidade (HA).

Informações de Apoio

Mais da metade dessas falhas provém de problemas durante a fase 200_enable_maintenance_mode, com validações de HA existentes executando principalmente verificações básicas de estado ativo/standby, que são insuficientes para transições de HA abrangentes.

Com a atualização do Secure Firewall 7.6, foram introduzidas validações de HA aprimoradas para resolver esses problemas. Esses aprimoramentos incluem verificações completas para transições de estado de HA, timeouts estendidos para processos de sincronização e relatórios de erros aprimorados. Esta atualização tem como objetivo reduzir significativamente os problemas de HA pós-atualização e as falhas gerais de atualização, garantindo um processo de atualização mais tranquilo e confiável para implantações de HA.

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

Problema

- Há um número significativo de falhas de atualização de FTD relatadas pelos clientes nas versões 7.0, 7.1 e 7.2 para implantações de HA.
- Mais de 50% das falhas vêm de implantações HA do FTD. Falhas em 200_enable_maintenance_mode contribuem para falhas de HA.
- As validações de estado HA existentes são validações básicas, como verificações de estado ativo/standby, e não validam completamente as transições de HA.

O que há de novo (solução)

Validações de HA aprimoradas para atualização de FTD:

- Validação para transição de estado de HA
- Tempos limite de atualização de HA de FTD aprimorados para estado de transição de HA, como sincronização de configuração (7200 segundos), sincronização de aplicativo (1200 segundos) e sincronização em massa (7200 segundos)
- Dar mais controle ao FMC sobre quando iniciar ou falhar a atualização do FTD
- Relatórios de erros e mensagens de recuperação aprimorados para atualizações de FTD HA

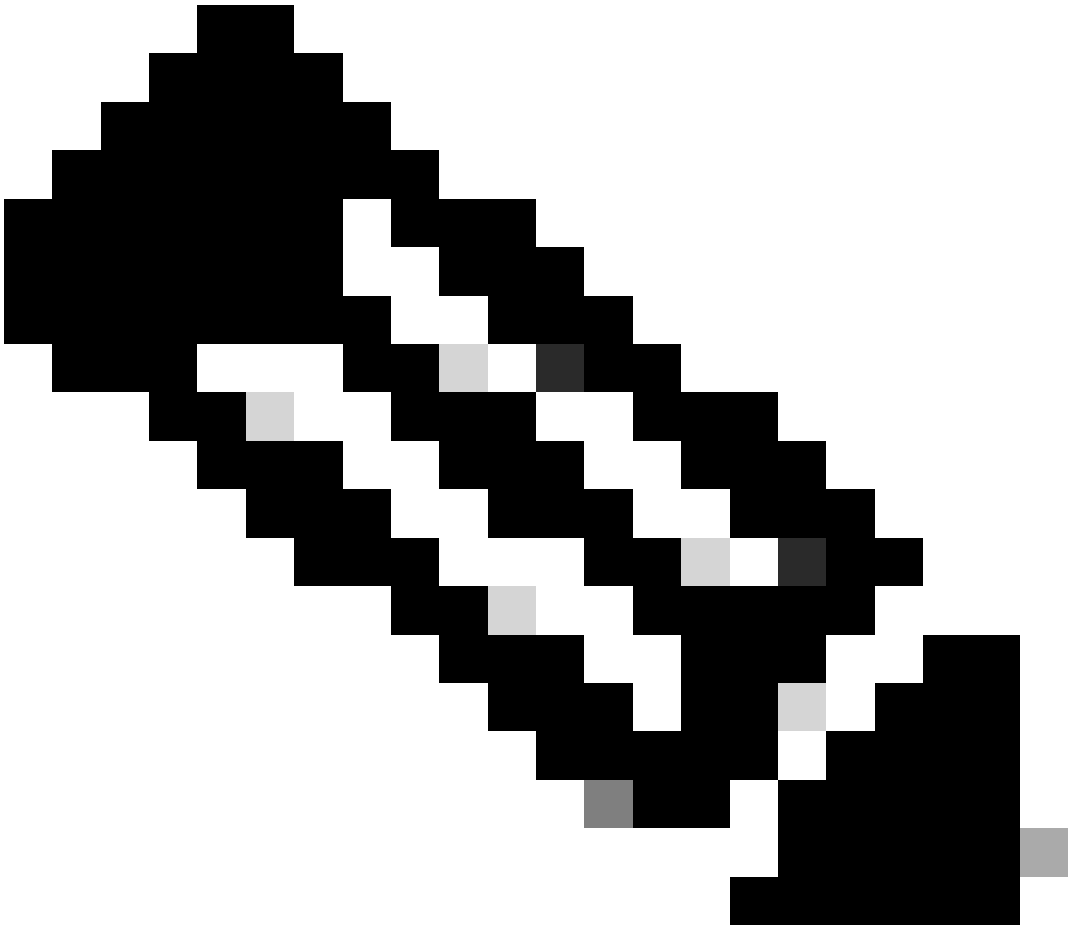
Em comparação com as versões anteriores, ele tem:

- Validações de HA aprimoradas ajudam a reduzir os problemas de criação de HA pós-atualização em implantações de HA
- Validações aprimoradas ajudam a reduzir as falhas de atualização do FTD

Pré-requisitos

Plataformas suportadas

- Gerente(s) e Versão(ões): FMC 7.6.0
- Aplicação (ASA/FTD) e versão mínima da aplicação: FTD 7.6.0; FMC que gere o 7.6.0 FTD HA
- Plataformas suportadas: Todas as plataformas que executam o FTD HA



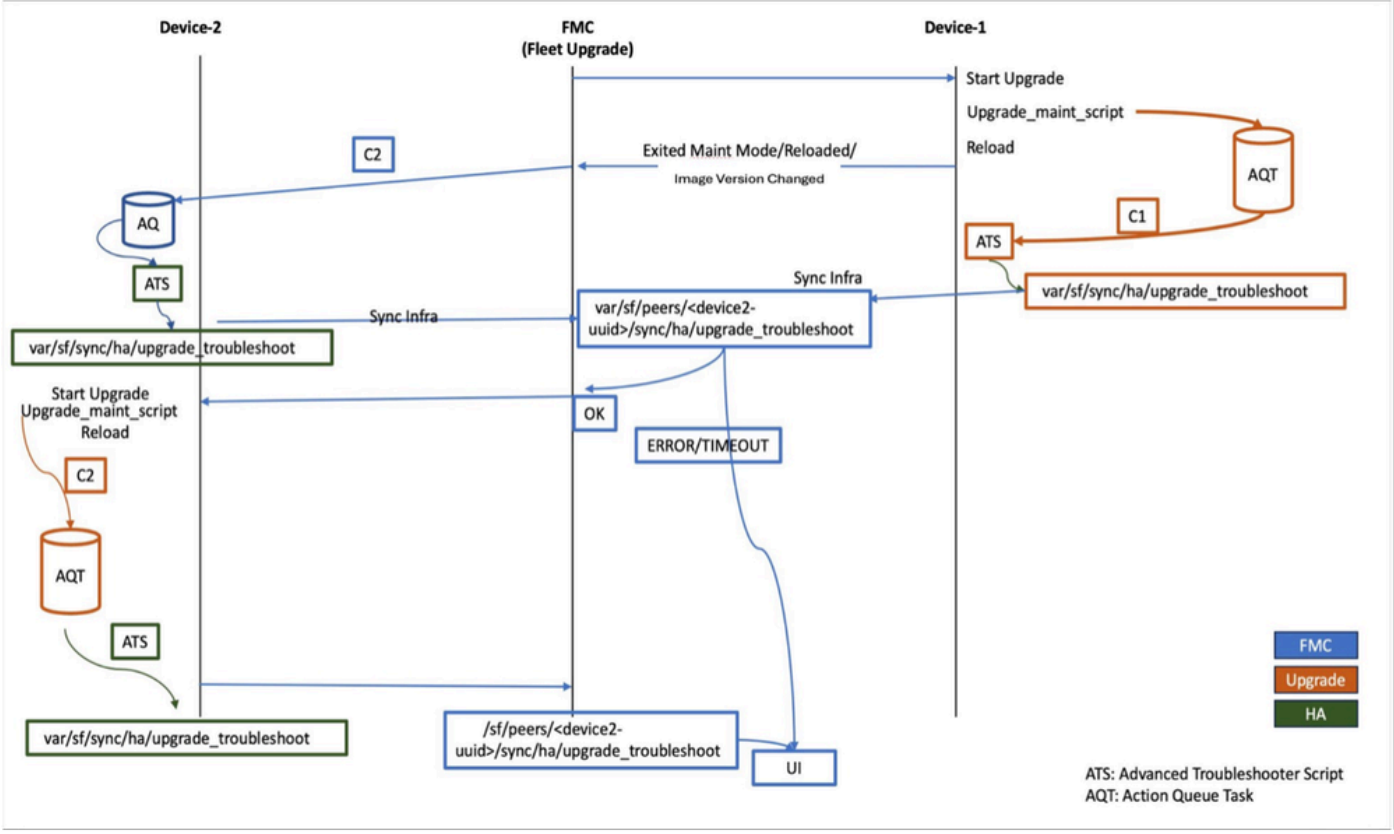
Note: Este recurso se aplica somente a implantações de HA de FTD gerenciadas pelo FMC. Este recurso não se aplica a dispositivos FTD HA ou em cluster gerenciados pelo FDM.

Visão geral do recurso

- Este recurso ajuda a reduzir falhas de atualização de FTD na implantação de HA, verificando os estados de HA das unidades atualizadas pelo FMC após a parte de

reinicialização do processo de atualização.
- Após a reinicialização da atualização, o FMC verifica o estado ativo/standby e quaisquer falhas na sincronização de HA.
- O FTD notifica o FMC sobre quando iniciar ou falhar a atualização no segundo nó na forma de uma nova solução de problemas avançada de HA.
- Se houver qualquer falha ao ingressar na reinicialização de HA pós-atualização, uma mensagem apropriada será exibida na interface do usuário do FMC.

Novo fluxo de trabalho de atualização para FTD HA



A unidade em standby é a primeira a ser atualizada

Atualização da primeira unidade (unidade em standby)

- Durante a atualização da primeira unidade, o script de atualização inicia a tarefa action_queue para coletar dados de identificação e solução de problemas avançados de HA no estágio 999_finish.
- A execução da tarefa inserida começa somente após a reinicialização pós-atualização e coleta informações de solução de problemas na forma de arquivo JSON.
- O mesmo arquivo JSON é sincronizado com o FMC.
- Quando o primeiro nó sai do modo de manutenção, o FMC aciona uma tarefa action_queue remota na unidade ativa para coletar a solução avançada de problemas de HA (a unidade ativa precisa ser 7.6 ou superior). Se a unidade ativa for inferior a 7.6, não é efetuada nenhuma resolução de problemas na unidade ativa e o FMC toma uma decisão apenas com base na resolução de problemas recolhida na unidade de reserva.

Depois que a solução avançada de problemas de HA é coletada de ambas as unidades, o FMC decide iniciar a atualização ou bloqueá-la no segundo nó (unidade ativa).

Atualização da Segunda Unidade (Unidade Ativa)

- Semelhante à unidade em standby, o script de atualização inicia a tarefa action_queue para coletar a solução avançada de problemas de HA no estágio 999_finish.
- A execução da tarefa inserida inicia apenas a reinicialização pós-atualização e gera informações de solução de problemas na forma de um arquivo JSON.
- O mesmo arquivo é sincronizado com o FMC.
- Se uma das unidades relatar falha de HA, os dados de falha de HA serão mostrados na interface do usuário do FMC na guia de atualização.
- No caso de qualquer falha em ingressar na reinicialização de HA pós-atualização, a atualização é marcada como concluída e na mesma guia de atualização as falhas de validação de HA são relatadas.

Solução avançada de problemas de HA

- A solução avançada de problemas de HA é um novo arquivo JSON único introduzido como parte deste recurso que contém informações de HA. Ele é gerado após a reinicialização após uma atualização e enviado do FTD para o FMC.
- Nome e caminho do arquivo: /ngfw/var/sf/sync/ha/upgrade_troubleshoot
- Assim que o FMC recolhe a solução avançada de problemas de alta disponibilidade da primeira unidade (em espera), o FMC aciona uma tarefa remota para recolher as mesmas informações da unidade ativa.
    - Essa coleta de dados remota só é suportada quando os dispositivos estão executando a versão 7.6 ou posterior.
    - Se forem encontrados dispositivos executando uma versão anterior à 7.6, a coleta de dados remotos será ignorada. Assim, neste caso, o FMC só recolheria dados da unidade de reserva e decidiria tomar medidas adicionais.

- A geração de solução de problemas avançada de alta disponibilidade é rápida. Se Lina estiver inoperante e não conseguir gerar o relatório, ele será fechado imediatamente.
    - O tempo de reinicialização do dispositivo depende de plataforma para plataforma e o tempo de reinicialização é o mesmo que documentamos para cada plataforma.

Relatório de Troubleshooting Avançado de HA

Cada unidade de HA gera dados de solução avançada de problemas de HA na forma de reinicialização pós-atualização do arquivo JSON e os compartilha com o FMC. Aqui estão exemplos de validação quando há falha e sucesso.

Exemplo de falha de validação de HA

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

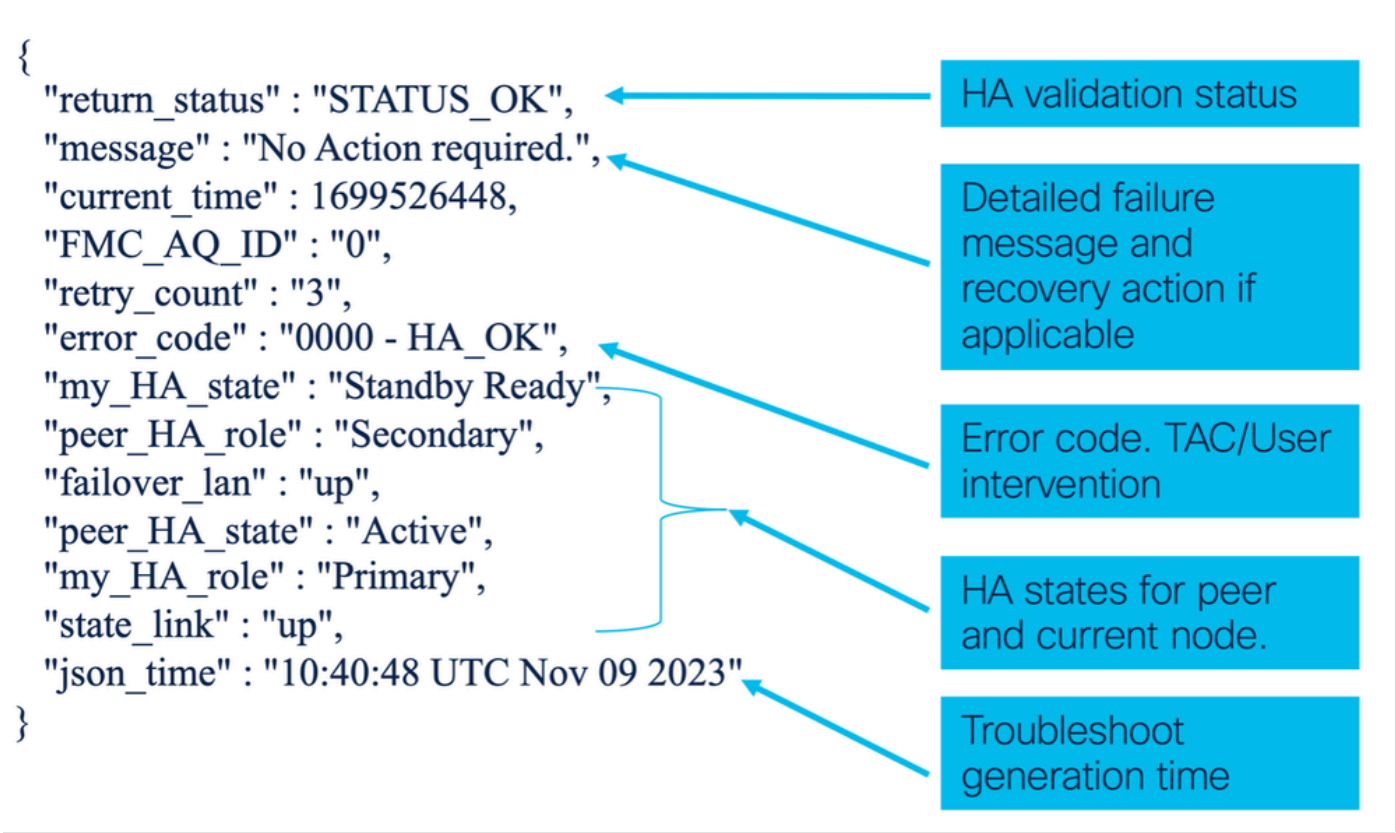
```
{
"failover_lan" : "NA",
"error_code" : "1046 -
STARTUP_FAILOVER_CONFIG_NOT_PRESENT",
"current_time" : 1701369637,
"peer_HA_state" : "Not Detected",
"FMC_AQ_ID" : "0",
"state_link" : "NA",
"json_time" : "18:40:37 UTC Nov 30 2023",
"my_HA_state" : "Disabled",
"my_HA_role" : "Secondary",
"return_status"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


Exemplo de validação de HA bem-sucedida

Arquivo: /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
}
```


Conteúdo da solução avançada de problemas de alta disponibilidade



Local do arquivo de solução avançada de problemas de HA

Solução avançada de problemas de HA no local do arquivo JSON:

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


        /sync/ha/upgrade_troubleshoot
```

- A solução de problemas de HA se baseia no comando lina.
  - Se a solução de problemas falhar ao gerar em /ngfw/var/sf/sync/ha/upgrade_troubleshoot, o usuário poderá consultar os registros em: /ngfw/var/log/ha_upgrade_troubleshoot.log
- Os arquivos /ngfw/var/sf/sync/ha/upgrade_troubleshoot e /ngfw/var/log/ha_upgrade_troubleshoot.log fazem parte do arquivo de Solução de Problemas do FTD.

Dicas para solução avançada de problemas de geração de problemas de HA

Às vezes, a solução avançada de problemas de alta disponibilidade não é gerada devido ao estado do sistema e o motivo disso pode ser uma linha inativa ou o processo da fila de ações está inativo após a reinicialização da atualização. Se a linha ou a fila de ações estiver inativa, isso é um problema.

Nesses casos, verifique se os processos de linha e ActionQueue estão em execução usando esse comando no modo especialista:

<#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
```

Status de retorno e ação na solução avançada de problemas de alta disponibilidade

- STATUS_INIT: Indica que a solução de problemas de HA foi acionada.
- STATUS_OK: O dispositivo está em um estado estável. Nenhuma ação é exigida.
- ERRO DE STATUS: Isso determina que ocorreu um erro devido ao qual o HA não está formado. O usuário precisa executar uma ação com base na mensagem exibida ou precisa entrar em contato com o TAC.
- STATUS_RETRY: O dispositivo pode estar em um dos estados intermediários. A solução de problemas de HA continua tentando após um intervalo fixo com base no estado até que STATUS_ERROR ou STATUS_OK seja encontrado.
    - Com base nas falhas encontradas STATUS ERROR, as falhas de HA são categorizadas em 2 casos:
        - Intervenção do usuário - Essas falhas de HA podem ser corrigidas pelo usuário, que pode retomar a atualização, onde a intervenção do TAC não é necessária.
        - Intervenção do TAC - Para essas falhas de HA, o usuário não pode corrigi-las sozinho; A intervenção do TAC é necessária.

Código de erro e classificação

Com base nos códigos de erro, os erros são classificados como mostrado aqui:

return_status	error_code	Descrição	Mecanismo de Repetição ou

			Recuperação
STATUS_OK	"0000 - HA_OK"(Os valores reservados são de 0001 a 1023)	Isso é para o cenário de sucesso. (Onde os estados de HA são Ativo e Pronto para espera)	(Não aplicável)
STATUS_ERROR	"1024:2047 - ERROR_REASON"	Isso é para o cenário de erro (intervenção do usuário)	Mensagens acionáveis a serem exibidas para o usuário e a estrutura de atualização podem adicionar o mecanismo de repetição ou recuperação no futuro (se houver).
STATUS_ERROR	"2048:3071 - ERROR_REASON"	Isso é para o cenário de erro (intervenção do TAC)	A intervenção do TAC é necessária para a recuperação.

Mensagens de intervenção do usuário

Erro	Mensagem de erro	Código de erro
'FAILOVER_CONFIG_NOT_PRESSENT'	"A configuração de failover não está presente no dispositivo"	"1024"
'FAILOVER_IS_NOT_ENABLED'	"O failover não está habilitado no dispositivo. Habilite o failover"	"1025"
'FAILOVER_LAN_DOWN'	"A LAN de failover está inativa no dispositivo"	"1026"
'ESTADO_LINK_DOWN'	"O link de estado está	"1027"

	inoperante no dispositivo"	
'FAILOVER_BLOCK_DEPLETION'	"Bloquear redução nos seguintes blocos do dispositivo:\n"	"1028"
'APP_SYNC_TIMEOUT'	"Tempo limite de sincronização do aplicativo no dispositivo"	"1029"
'CD_APP_SYNC_ERROR'	"Erro de sincronização de aplicativo de CD detectado no dispositivo"	"1030"
'CONFIG_SYNC_TIMEOUT'	"Tempo limite de sincronização de configuração no dispositivo"	"1031"
'FAILED_TO_APPLY_CONFIG'	"Falha ao aplicar a configuração no dispositivo"	"1032"
'BULK_SYNC_TIMEOUT'	"Tempo limite de sincronização em massa no dispositivo"	"1033"
'BULK_SYNC_CLIENT_ISSUE'	"Verifique os seguintes clientes no dispositivo:\n"	"1034"
'IFC_CHECK_FAILED'	"Falha na verificação de interface de failover nas seguintes interfaces do dispositivo:\n"	"1035"
'IFC_FAILED_CHECK_VLAN_SPANTREE'	"Já que as interfaces estão ativas. Verifique se as VLANs são permitidas no lado do switch ou se há um problema com o	"1036"

	spanning tree"	
'VERSION_MISMATCH'	"Versão de software diferente no outro dispositivo"	"1037"
'MODE_MISMATCH'	"Modo de operação diferente no outro dispositivo"	"1038"
'LIC_MISMATCH'	"Licença diferente no outro dispositivo"	"1039"
'CHASSIS_MISMATCH'	"Configuração de chassi diferente no outro dispositivo"	"1040"
'CARD_MISMATCH'	"Configuração de placa diferente no outro dispositivo"	"1041"
'PEER_NOT_OK'	"Este dispositivo está no estado OK. Verificar o dispositivo par"	"1042"

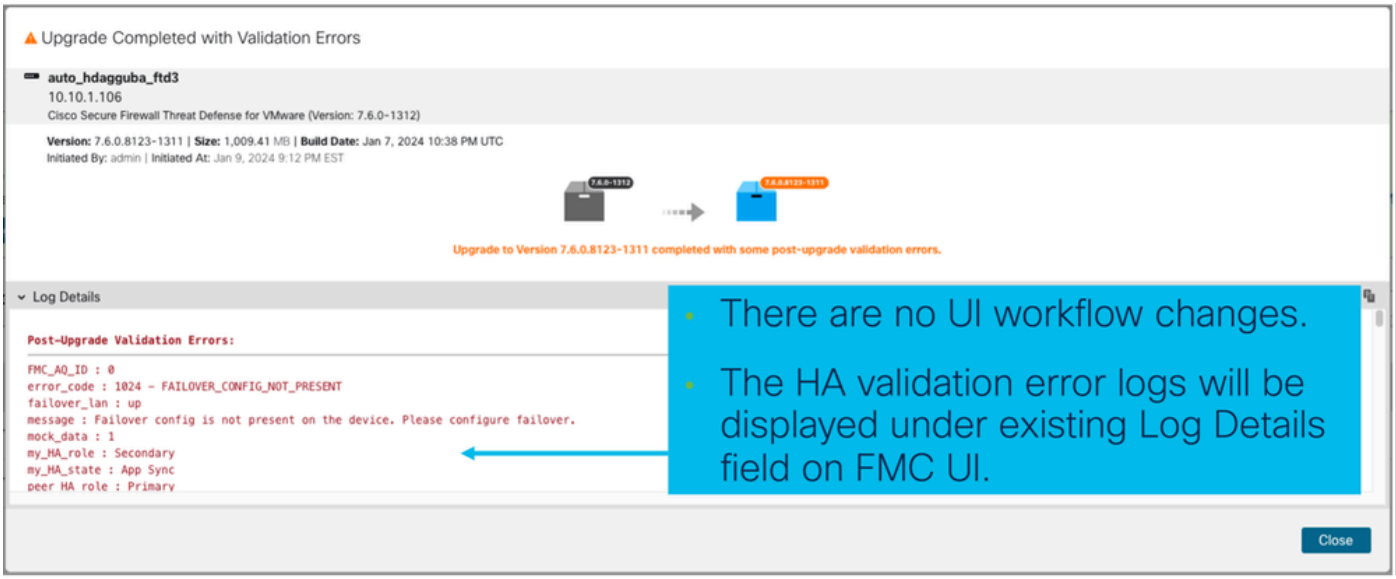
Mensagens de intervenção do TAC

Erro	Mensagem de erro	Código de erro
'RUN_CMD_FAILED'	"Falha ao executar o comando"	"2048"
'LINA_NOT_STARTED'	"Lina não iniciou no dispositivo. Tente novamente mais tarde"	"2049"
'HWIDB_MISMATCH'	"O índice HWIDB é diferente no dispositivo"	"2050"
'BACKPLANE_FAILURE'	"Falha do backplane no	"2051"

	dispositivo. Verifique o backplane"	
'HA_PROGR_FAILURE'	"Falha de progressão de HA no dispositivo"	"2052"
'SVM_FAILURE'	"Falha do módulo de serviço no dispositivo"	"2053"
'SVM_MIO_HB_FAILURE'	"Falha de pulsação entre MIO e agente de aplicativo no dispositivo"	"2054"
'SVM_MIO_CRUZ_FAILED'	"Falha do adaptador de rede MIO-blade no dispositivo"	"2055"
'SVM_MIO_HB_CRUZ_FAILED'	"Falha de pulsação de MIO-blade e adaptador de rede no dispositivo"	"2056"
'SSM_CARD_FAILURE'	"Falha da placa de serviço no dispositivo"	"2057"
'MY_COMM_FAILURE'	"Falha de comunicação no dispositivo"	"2058"
'CRITICAL_PROCESS_DIED'	"Processo crítico inoperante no dispositivo"	"2059"
'SNORT_FAILURE'	"Snort failed on the device" (Falha de Snort no dispositivo)	"2060"
'PEER_SVM_FAILURE'	"Falha do módulo de serviço NGFW no outro dispositivo"	"2061"
'FAULT_MON_BLOCK_DEP'	"O monitoramento de falhas relatou a redução de blocos no dispositivo"	"2062"

'DISK_FAILURE'	"Falha de disco no dispositivo"	"2063"
'SNORT_DiSK_FAILURE'	"Snort and Disk failed on the device (Falha de Snort e Disco no dispositivo)	"2064"
'INATIVE_MATE_FOUND"	"Detectado um parceiro inativo durante a inicialização	"2065"
'SCRIPT_TIMEOUT'	"Limite de novas tentativas excedido. Saindo do script"	"2066"
'ERROR_UNKNOWN'	"Falha ao identificar erro"	"2067"

Alterações na IU do Centro de Gerenciamento de Firewall



Arquitetura de software

Este recurso é altamente dependente da estrutura da fila de ações existente. O recurso usa a linha CLI subjacente para gerar os dados de solução avançada de problemas de HA.

Perguntas freqüentes

P: O recurso se aplica à funcionalidade de reversão de atualização do FTD?
R: Não. Este recurso não se aplica à funcionalidade de reversão, pois a reversão de FTD funciona em paralelo, e não 1 por 1.

P: Se a atualização falhar em 200_enable_maintenance_mode.pl, ela gerará os dados avançados de solução de problemas?
R: Não. A solução avançada de problemas de HA é gerada somente após a reinicialização pós-atualização e não durante a falha de atualização

P: Se a atualização for bloqueada devido a validações de HA na segunda unidade, um usuário pode disparar a atualização somente na segunda unidade?
R: Yes. O usuário precisa selecionar o par HA novamente para atualização e o FMC dispara a atualização somente em uma unidade não atualizada.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.