

Solucionar problemas de implantações da política do Firepower Threat Defense

Contents

[Introduction](#)

[Informações de Apoio](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Visão geral da implantação da política](#)

[Visão geral do exemplo](#)

[Troubleshooting](#)

[Interface gráfica do usuário \(GUI\) do FMC](#)

[Utilizar As Transcrições De Implantação](#)

[Solucionar problemas com registros do FMC](#)

[/var/opt/CSCOpX/MDC/log/operation/usmsharedsvcs.log](#)

[/var/log/sf/policy_deployment.log](#)

[Solução de problemas de dispositivo gerenciado](#)

[/ngfw/var/log/ngfwManager.log](#)

[/ngfw/var/log/sf/policy_deployment.log](#)

[Exemplo](#)

[Mensagens de falha comuns](#)

[Entre em contato com o TAC para obter assistência](#)

Introduction

Este documento descreve uma visão geral de alto nível do processo de implantação de política no FTD e também técnicas básicas de solução de problemas.

Informações de Apoio

Com Cisco Firepower Threat Defense (FTD), recursos de firewall com informações de estado tradicionais oferecidos pela Adaptive Security Appliances (ASA) e Next-Gen recursos de firewall (com tecnologia Snort) são agora combinados em um produto.

Devido a essa alteração, Policy Deployment Infrastructure no FTD agora lida com alterações de configuração para o código ASA (também conhecido como LINA) e Snort em um pacote.

Prerequisites

A Cisco recomenda o conhecimento destes produtos:

- Firepower Management Center (FMC)
- Firepower Threat Defense (FTD)

Componentes Utilizados

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Visão geral da implantação da política

O Cisco FTD utiliza **Policy Deployments** gerenciar e distribuir configurações para dispositivos registrados no **Firepower Management Center (CVP)**.

Dentro da implantação, há uma série de etapas divididas em "Fases".

As fases do CVP podem ser resumidas na presente lista.

Fase 0	Inicialização da implantação
Fase 1	Coleção de Objetos de Banco de Dados
Fase 2	Política e Coleção de Objetos
Fase 3	Geração de configuração de linha de comando de NGFW
Fase 4	Geração de Pacote de Implantação de Dispositivo
Fase 5	Enviar e Receber o Pacote de Implantação
Fase 6	Implantação pendente, ações de implantação e mensagens de êxito da implantação

O conhecimento das fases e do local das falhas no processo pode ajudar a solucionar as falhas que um **Firepower** faces de sistema.

Em algumas situações, pode ser um conflito devido a configurações anteriores ou causado por um **Advanced Flex Configuration** que não possui uma palavra-chave que possa causar falhas que o relatório do dispositivo não aborda.

Visão geral do exemplo

Etapa 1. Clique em **Deployment**, que especifica o dispositivo a ser selecionado.

Etapa 2. Quando a implantação de um dispositivo é confirmada, o FMC começa a coletar todas as configurações relevantes para o dispositivo.

Etapa 3. Quando as configurações são coletadas, o FMC cria o pacote e o envia ao sensor pelo mecanismo de comunicação chamado **SFTunnel**.

Etapa 4. O FMC notifica o sensor para iniciar o processo de implantação com a política fornecida enquanto ouve as respostas individuais.

Etapa 5. O dispositivo gerenciado descompacta o arquivo e começa a aplicar as configurações e os pacotes individuais.

A. A primeira metade da implantação é a **snort** configuração em que o **snort** a configuração é testada localmente para garantir sua validade.

Quando comprovada como válida, a nova configuração é movida para o diretório de produção para **snort**. Se a validação falhar, a implantação da política falhará nesta etapa.

B. A segunda metade da carga do pacote de implantação é para a configuração LINA, onde é aplicada diretamente ao processo LINA pelo processo **ngfwManager**.

Se ocorrer uma falha, as alterações serão revertidas e ocorrerá uma falha na implantação da política.

Etapa 6. Se ambos **snort** e os pacotes LINA são bem-sucedidos, os sinais de dispositivos gerenciados **snort** para reiniciar ou recarregar para carregar a nova configuração e salvar todas as configurações atuais.

Etapa 7. Se todas as mensagens forem bem-sucedidas, o sensor enviará uma mensagem de êxito e esperará que ela seja confirmada pelo Centro de Gerenciamento.

Etapa 8. Uma vez recebido, o FMC marca a tarefa como um sucesso e permite que o pacote de políticas seja concluído.

Troubleshooting

Problemas encontrados durante **Policy Deployment** pode ser devido a, mas não limitado a:

1. Configuração incorreta
2. Comunicação entre o CVP e o DTF
3. Integridade do banco de dados e do sistema
4. Avisos e defeitos de software
5. Outras situações únicas

Alguns desses problemas podem ser facilmente corrigidos, enquanto outros podem precisar de assistência da **Cisco Technical Assistance Center (TAC)**.

O objetivo desta seção é fornecer técnicas para isolar o problema ou determinar a causa raiz.

Interface gráfica do usuário (GUI) do FMC

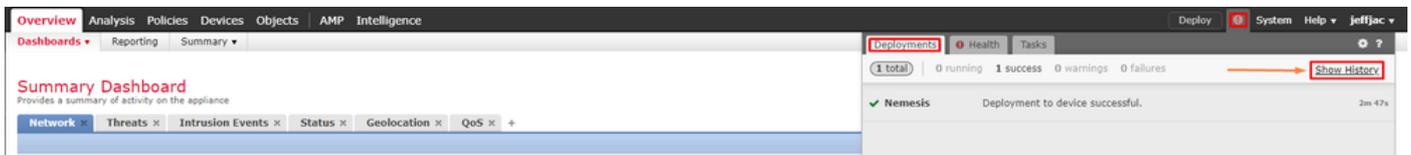
A Cisco recomenda que cada sessão de solução de problemas para falhas de implantação seja iniciada no dispositivo FMC.

Na janela de notificação de falha, em todas as versões além de 6.2.3, há ferramentas adicionais que podem ajudar com outras possíveis falhas.

Utilizar As Transcrições De Implantação

Etapa 1. Puxe o **Deployments** na **interface do usuário da Web do FMC**.

Etapa 2. Embora a **Deployments** estiver selecionada, clique em **Show History**.



Etapa 3. Dentro do **Deployment History** você pode ver todas as implantações anteriores do FMC. Selecione a implantação na qual você deseja ver mais dados.

Etapa 4. Depois que um elemento de implantação for selecionado, o **Deployment Details** exibe uma lista de todos os dispositivos dentro do **Transaction**. Estas entradas são divididas nestas colunas: **Device Number**, **Device Name**, **Status**, e **Transcript**.

Device	Status	Transcript
1 Nemesis	✓ Success	

Etapa 5. Selecione o dispositivo em questão e clique na opção de transcrição para ver a transcrição de implantação individual que pode informá-lo sobre falhas, bem como configurações que são colocadas nos dispositivos gerenciados.

Solucionar problemas com registros do FMC

Embora seja apropriado envolver o TAC da Cisco para analisar os logs, uma pesquisa nos logs pode ajudar no isolamento inicial do problema e acelerar a resolução. Há vários arquivos de log no FMC que revelam os detalhes sobre o processo de implantação da política.

Os dois registros mais comumente consultados são `policy_deployment.log` e `usmshredsvcs.log`.

Todos os arquivos mencionados neste documento podem ser visualizados com vários comandos Linux, como `more`, `less` e `vi`. No entanto, é muito importante garantir que apenas `read` são executadas. Todos os arquivos requerem acesso raiz para serem visualizados.

`/var/opt/CSCOpX/MDC/log/operation/usmshredsvcs.log`

Esse registro marca claramente o início da tarefa de implantação da política no FMC e a conclusão de cada fase, o que ajuda a determinar a fase em que a implantação ocorreu uma falha, juntamente com o código de falha.

O `transactionID` o valor incluído na parte JSON do log pode ser usado para localizar entradas de log relacionadas a uma tentativa de disponibilização específica.

```
22-Nov-2019 01:28:52.844, [INFO], (DefenseCenterServiceImpl.java:1372)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-4
** REST Request [ CSM ]
** ID : e1c84364-0966-42eb-9356-d2914be2b4a3
** URL: Broadcast message.send.deployment
{
  "body" : {
    "property" : "deployment:deployment_initiated_for_the_device",
    "argumentList" : [ {
      "key" : "PHASE",
      "value" : "Phase-0"
    } ]
  },
  "user" : "68d03c42-d9bd-11dc-89f2-b7961d42c462",
  "type" : "deployment",
  "status" : "running",
  "progress" : 5,
  "silent" : true,
  "restart" : true,
  "transactionId" : 12884916552,
  "devices" : [ "93a2089a-fa82-11e9-8219-e1abeec81dc9" ]
}
```

`/var/log/sf/policy_deployment.log`

Embora esse arquivo de log tenha existido em todas as versões 6.x, que começam na 6.4, sua cobertura foi expandida.

Agora, ele descreve as etapas detalhadas executadas no FMC para criar os pacotes de implantação, portanto, é melhor usado para analisar falhas das Fases 1 a 4.

O início de cada fase é marcado por uma linha com `"INFO start.. "`:

```
Jul 18 17:20:03 firepower ActionQueueScrape.pl[17287]: INFO starting populateGlobalSnapshot -
sqlite = /var/cisco/umpd/8589938337/DC_policy_deployment.db, transaction = 8589938337, time =
1563470402, running as (memory = 56.35 MB) (Framework 3950<196 <- CSMTasks 223<10 <-
SF::ActionQueue 2457)
Jul 18 17:20:03 firepower ActionQueueScrape.pl[17287]: INFO deployment threading: disabled
(Framework 198 <- CSMTasks 223<10 <- SF::ActionQueue 2457)
Jul 18 17:20:03 firepower ActionQueueScrape.pl[17287]: INFO -> calling
SF::UMPD::Plugins::Correlation::Manager::getPluginDependencies (Plugin 298<90 <- Framework
3579<3566<216 <- CSMTasks 223)
...
```

Solução de problemas de dispositivo gerenciado

Há fases e seções adicionais que dependem do pacote do dispositivo, da configuração de alta disponibilidade e do resultado das fases anteriores para cada dispositivo gerenciado.

Se um problema de implantação for isolado a uma falha no dispositivo gerenciado, uma solução de problemas adicional poderá ser executada no dispositivo com dois logs no dispositivo: **policy_deployment.log** e **ngfwManager.log**.

/ngfw/var/log/ngfwManager.log

Esse arquivo de log fornece etapas detalhadas executadas pelo **Config Communication Manager** e **Config Dispatcher** para se comunicar com o FMC, trabalhar com o pacote de implantação e orquestrar a validação e a aplicação das configurações **Snort** e **LINA**.

Estes são alguns exemplos de **ngfwManager.log** que representam o início das fases principais:

FTD receives FMC's request for running configuration:

```
May 30 16:37:10 ccm[4293] Thread-10: INFO com.cisco.ccm.ConfigCommunicationManager- Passing CD-
Message-Request to Config Dispatcher...
May 30 16:37:10 ccm[4293] Thread-10: DEBUG com.cisco.ccm.ConfigCommunicationManager- <?xml
version="1.0" encoding="UTF-
8"??><cdMessagesList><timeStamp>1559234230012</timeStamp><cdMessage><name>LinaShowCommand</name><
messageId>-
753133537443151390</messageId><contentType>XML</contentType><msgContent><![CDATA[<?xml
version="1.0" encoding="UTF-8"??><message><name>LinaShowCommand</name>...
```

FTD receives FMC's request to download the deployment package:

```
May 30 16:37:18 ccm[4293] Thread-9: INFO com.cisco.ccm.ConfigCommunicationManager- Downloading
database (transaction 8589938211, version 1559234236)
May 30 16:37:18 ccm[4293] Thread-9: DEBUG com.cisco.ccm.DownloadManager- handle record:
8589938211, status = PENDING
May 30 16:37:18 ccm[4293] Thread-9: DEBUG com.cisco.ccm.DownloadManager- begin downloading
database
```

FTD begins the deployment of policy changes:

```
May 30 16:37:21 ccm[4293] Thread-9: INFO com.cisco.ccm.ConfigCommunicationManager- Starting
deployment
May 30 16:37:21 ccm[4293] Thread-11: INFO com.cisco.ccm.ConfigCommunicationManager- Sending
```

message: DEPLOYMENT_STATUS_CCM to Manager

FTD begins LINA deployment:

```
May 30 16:37:42 ccm[4293] Thread-19: DEBUG
com.cisco.ngfw.configdispatcher.communicators.LinaCommunicatorImpl- Trying to send Start-Config-
Sequencerequest to lina
```

FTD begins finalizing the deployment:

```
May 30 16:38:48 ccm[4293] Thread-19: DEBUG
com.cisco.ngfw.configdispatcher.communicators.LinaCommunicatorImpl- Clustering Message sent out
of ConfigDispatcher:
Name:Cluster-App-Conf-Finalize-Request
```

/ngfw/var/log/sf/policy_deployment.log

Esse log contém os detalhes da política aplicada ao **Snort**. Embora o conteúdo do registro seja principalmente avançado e exija análise pelo TAC, ainda é possível rastrear o processo com algumas entradas importantes:

Config Dispatcher begins extracting the packaged policies for validation:

```
Jul 18 17:20:57 firepower policy_apply.pl[25122]: INFO -> calling
SF::UMPD::Plugins::NGFWPolicy::Device::exportDeviceSnapshotToSandbox (Plugin 230 <- Framework
611 <- Transaction 1085)
Jul 18 17:20:57 firepower policy_apply.pl[25122]: INFO found NGFWPolicy => (NGFWPolicy::Util
32 <- NGFWPolicy::Device 43 <- Plugin 235)
...
Jul 18 17:20:57 firepower policy_apply.pl[25122]: INFO export FTD platform settings...
(PlatformSettings::FTD::Device 29 <- Plugin 235<339 <- PlatformSettings::Device 13)
```

Config validation begins:

```
Jul 18 17:21:37 firepower policy_apply.pl[25122]: INFO starting validateExportedFiles - sqlite
= /var/cisco/deploy/sandbox/policy_deployment.db, sandbox = /var/cisco/deploy/sandbox/exported-
files (memory = 229.99 MB) (Framework 3950<687 <- Transaction 1101 <- main 194)
```

Validation has completed successfully:

```
Jul 18 17:21:49 firepower policy_apply.pl[25122]: INFO validateExportedFiles - sqlite =
/var/cisco/deploy/sandbox/policy_deployment.db, sandbox = /var/cisco/deploy/sandbox/exported-
files took 12 (memory = 238.50 MB, change = 8.51 MB) (Framework 3976<724 <- Transaction 1101 <-
main 194)
```

Config Dispatcher begins moving the validated configuration to the Snort directories in production:

```
Jul 18 17:21:54 firepower policy_apply.pl[26571]: INFO -> calling
SF::UMPD::Plugins::NGFWPolicy::Device::publishExportedFiles (Plugin 230 <- Framework 822 <-
```

Transaction 1662)

Snort processes will reload to apply the new configurations:

```
Jul 18 17:22:02 firepower policy_apply.pl[26571]: INFO Reconfiguring DE a3bcd340-992f-11e9-  
a1f1-ac829f31a4f9... (Snort::SnortNotifications 292<154 <- Snort::Device 343 <- Plugin 235)  
Jul 18 17:22:02 firepower policy_apply.pl[26571]: INFO sending SnortReload to a3bcd340-992f-  
11e9-a1f1-ac829f31a4f9 (Snort::SnortNotifications 298<154 <- Snort::Device 343 <- Plugin 235)
```

Snort reload has completed successfully:

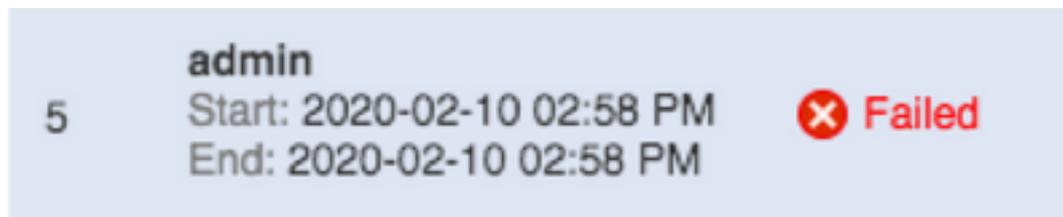
```
Jul 18 17:22:14 firepower policy_apply.pl[26571]: INFO notifyProcesses - sandbox =  
/var/cisco/deploy/sandbox/exported-files took 16 (memory = 169.52 MB, change = 16.95 MB)  
(Framework 3976<964 <- Transaction 1680 <- main 200)
```

After LINA config apply finishes, Snort deployment is finalized:

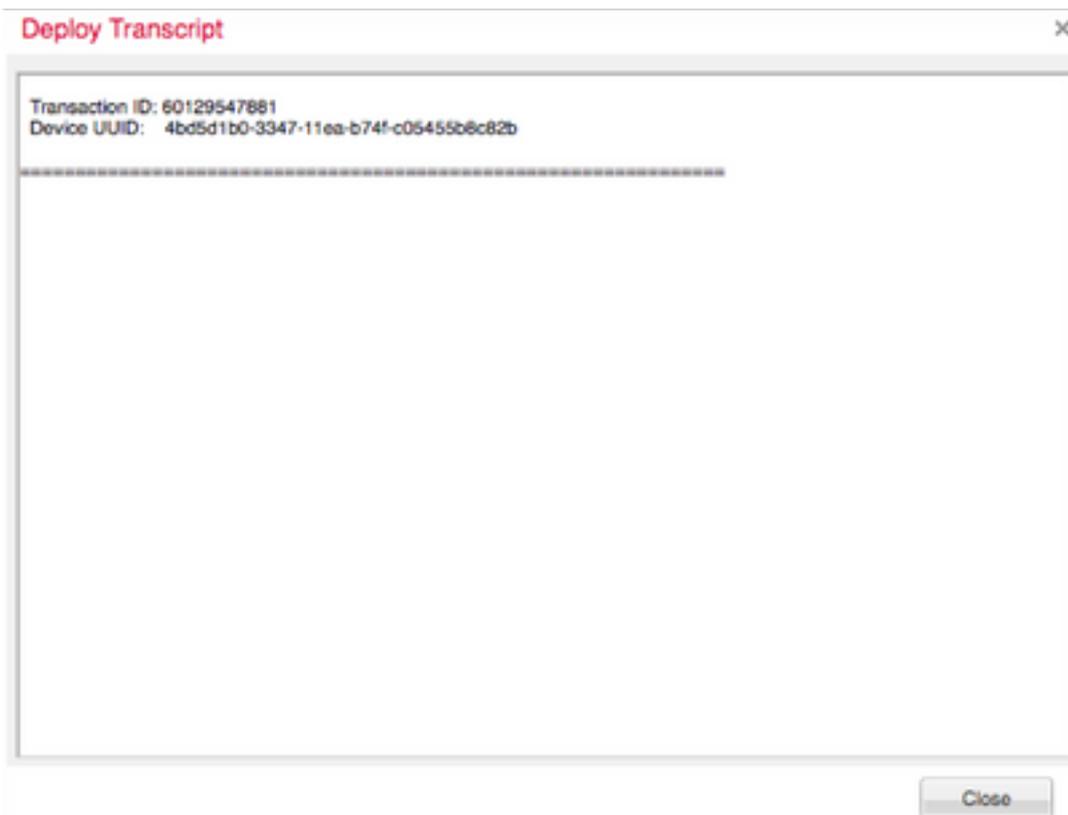
```
Jul 18 17:23:32 firepower policy_apply.pl[26913]: INFO starting finalizeDeviceDeployment -  
sandbox = /var/cisco/deploy/sandbox (memory = 101.14 MB) (Framework 3950<980 <- Transaction  
1740 <- main 206)
```

Exemplo

Etapa 1. Uma implantação falha



Etapa 2. Obter o Deploy Transcript e Transaction ID.



Etapa 3. SSH no seu **Management Center** e utilizar o utilitário Linux `less` para ler o arquivo conforme mostrado no FMC:

Exemplo: "`sudo less /var/opt/CSCOpX/MDC/log/operation/usmshredsvcs.log`" (A senha sudo é sua senha de usuário para ssh)

```
admin@firepower:~$ sudo less /var/opt/CSCOpX/MDC/log/operation/usmshredsvcs.log
Password: _
```

Etapa 4. Quando você estiver em `less` use a barra e digite o ID da mensagem para procurar os logs relacionados ao deployment **transactionID**.

Exemplo: `/60129547881` (Enquanto estiver em `less`, use `n` para navegar até o próximo resultado)

Exemplo de mensagem em execução:

```
10-Feb-2020 19:58:35.810, [INFO], (DefenseCenterServiceImpl.java:1394)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, Thread-526
** REST Request [ CSM ]
** ID : b1b660d2-6c1e-40a0-bbc4-feac62673cc8
** URL: Broadcast message.send.deployment
{
  "body" : {
    "property" : "deployment:domain_snapshot_success",
    "argumentList" : [ {
      "key" : "PHASE",
      "value" : "Phase-2"
    } ]
  },
  "user" : "68d03c42-d9bd-11dc-89f2-b7961d42c462",
  "type" : "deployment",
  "status" : "running",
  "progress" : 20,
  "silent" : true,
  "restart" : false,
  "transactionId" : 60129547881,
  "devices" : [ "4bd5d1b0-3347-11ea-b74f-c05455b8c82b" ]
}
```

Exemplo de mensagem de falha:

```
10-Feb-2020 19:58:36.516, [INFO], (DefenseCenterServiceImpl.java:1394)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, Thread-526
** REST Request [ CSM ]
** ID : 3df80a13-2da8-4eb1-a599-c123bf48ac9f
** URL: Broadcast message.send.deployment
{
  "body" : {
    "property" : "deployment:failed_to_retrieve_running_configuration",
    "argumentList" : [ {
      "key" : "PHASE",
      "value" : "Phase-3"
    } ]
  },
  "user" : "68d03c42-d9bd-11dc-89f2-b7961d42c462",
  "type" : "deployment",
  "status" : "failure",
  "progress" : 100,
  "silent" : false,
  "restart" : false,
  "transactionId" : 60129547881,
  "devices" : [ "4bd5d1b0-3347-11ea-b74f-c05455b8c82b" ]
}
```

5) Compare a falha apropriada com a tabela anexada de Mensagens de falha comuns.

Ou seja, failed_to_recover_running_configuration ocorre durante falhas de comunicação entre os

dois dispositivos.

Mensagens de falha comuns

Essas são mensagens de falha comuns que podem ser vistas no front-end da **Management Center Task** assim como o código de erro que pode ser visto no back-end.

Essas mensagens podem ser analisadas e comparadas com as razões comuns para possíveis resoluções.

Caso eles não sejam vistos ou não resolvam sua situação, entre em contato com o TAC para obter assistência.

Código de erro	Mensagens de erro	Razão
<code>device_has_changed_domain</code>	Falha na implantação - O dispositivo alterou o domínio de {SRCDOMAIN} para {DESTINATIONDOMAIN}. Try again later.	Esse erro geralmente ocorre quando um dispositivo é movido ou retirado de um segundo domínio. Uma reimplantação geralmente corrige esse problema.
<code>device_currently_under_deployment</code>	Falha na implantação devido a outra implantação em andamento para este dispositivo. Try again later.	Isso geralmente é relatado quando a implantação é acionada em um dispositivo implantado. Em algumas versões, isso é evitado sem uma notificação de falha; no entanto, essa fase ainda exige assistência na solução de problemas.
<code>device_not_member_of_container</code>	A implantação não pode ser executada em um dispositivo individual que seja membro de um cluster. Tente implantar o cluster novamente mais tarde.	Essa mensagem é aplicada para FTD em dispositivos gerenciador de chassi do Firepower eXtensible Operating System (FXOS). Se o cluster não foi criado em FXOS, mas não é um FMC, esta mensagem será mostrada. Crie o cluster no equipamento do Management Center antes de tentar implantar.

policy_altered_after_timestamp_for_other_devices_in_job_error

As políticas para um ou mais dispositivos foram alteradas desde {TIMESTAMP}. Tentar implantação novamente.

Este erro é mostrado se qualquer política/objeto for alterado para qualquer dispositivo no trabalho de implantação depois que o usuário acionar a implantação antes que os elementos CSM instantâneos de domínio sejam criados. Uma reimplantação corrige esse problema. Isso pode ocorrer quando muitos usuários usam o Management Center para editar e salvar o trabalho durante a implantação.

policy_altered_after_timestamp_error

A política {Policy Name} foi alterada desde {Timestamp}. Tentar implantação novamente.

Este erro é mostrado se qualquer política/objeto for alterado para o dispositivo em questão no trabalho de implantação, depois que o usuário acionar a implantação antes que os instantâneos de domínio e CSM sejam criados. Uma reimplantação corrige esse problema.

csm_snapshot_error

Falha na implantação devido à falha da coleção de políticas e objetos. Se o problema persistir após uma tentativa repetida, entre em contato com o TAC da Cisco.

Se uma Importação de políticas recente for fornecida, aguarde uma hora e tente outra implantação. Se isso não permitir que a importação prossiga para, entre em contato com o TAC, pois é uma mensagem relacionada ao banco de dados.

domain_snapshot_timeout

Falha na implantação devido ao tempo limite esgotado para coletar políticas e objetos. Se o problema persistir após outra tentativa, entre em contato com o TAC da Cisco.

O instantâneo de domínio tem um tempo limite de 5 minutos por padrão. Se o sistema estiver sob carga alta ou o hipervisor apresentar mau funcionamento, isso pode causar atrasos naturais na chamada. Isso pode ocorrer se o Management Center ou o dispositivo não receber a quantidade adequada de recursos de memória também. Se isso ocorrer sem carregamento não continuar mais tarde, entre em contato com o TAC.

domain_snapshot_errors

Falha na implantação da política e da coleção de objetos. Se o problema persistir após outra tentativa, entre em contato com o TAC da Cisco.

Entre em contato com o TAC da Cisco para uma solução avançada de problemas se a solução padrão não é necessária.

failed_to_retrieve_running_configuration

Falha na implantação devido a uma falha ao recuperar informações de configuração de execução do dispositivo. Tentar implantação novamente.

Esta mensagem pode ocorrer quando a conectividade entre um sensor final e um FMC não funciona como esperado. Verifique a integridade do túnel entre as unidades e monitore a conectividade entre os dois dispositivos.

device_is_busy

Falha na implantação porque o dispositivo pode estar executando uma implantação anterior ou uma reinicialização. Se o problema persistir após outra tentativa, entre em contato com o TAC da Cisco.

Se o túnel funcionar como esperado e os dispositivos puderem se comunicar, entre em contato com o TAC.

Esta mensagem é mostrada quando o FMC tenta uma implantação, enquanto uma implantação anterior está em andamento no FTD. Geralmente acontece quando uma implantação anterior não é concluída no FTD e o FTD é reinicializado ou o processo ngfwManager no FTD é reiniciado. Uma nova tentativa após 20 minutos para permitir que os processos formalmente expirem deve resolver esse problema.

Se após um atraso ou se o atraso não for aceitável, entre em contato com o TAC.

no_response_for_show_cmd

Falha na implantação devido a problemas de conectividade com o dispositivo ou o dispositivo não responde. Se o problema persistir após outra tentativa, entre em contato com o TAC da Cisco.

O FMC emite determinados comandos "show" da LINA para buscar a configuração atual para a geração da configuração. Isso pode acontecer quando há problemas de conectividade com problemas com o processo ngfwManager no sensor físico. Caso você não esteja enfrentando problemas de conectividade entre suas unidades, entre em contato com o TAC.

network_latency_or_device_not_reachable

Falha na implantação devido a uma falha de comunicação com o dispositivo. Se o problema persistir após outra tentativa, entre em contato com o TAC da Cisco.

Geralmente ocorre com alta latência de rede entre os dispositivos para causar um timeout de política. Verifique a latência de rede entre os dispositivos para verificar se corresponde aos mínimos da versão mencionada no guia do usuário.

slave_app_sync

Falha na implantação porque a sincronização da configuração do cluster está em andamento. Tentar implantação novamente.

Aplicável somente para configurações de cluster de FTD. Se uma implantação tentada em um cluster FTD enquanto a sincronização de aplicativo (sincronização de configuração) estiver em andamento, o mesmo será rejeitado pelo FTD. Uma tentativa após a sincronização da configuração deve resolver esse problema.

O status atual do cluster pode ser rastreado com este comando no CLISH do dispositivo gerenciado:

```
>show cluster info
```

Depois de revisar os registros

USMS mencionados

anteriormente, você poderá

qual configuração está

causando o erro. Esses são

geralmente erros nos quais

registros podem ser navegados

através da ferramenta de busca

da Cisco ou entre em contato

com o TAC da Cisco para

solucionar outros problemas.

asa_configuration_generation_errors

A implantação não pôde gerar a configuração do dispositivo. Se o problema persistir após outra tentativa, entre em contato com o TAC da Cisco.

Isso ocorre nos modelos 4

ou 9300 se a interface não

estiver associada ao dispositivo

durante ou imediatamente

de uma implantação.

Verifique se a interface está

totalmente associada ou não

antes de tentar a implantação.

interface_out_of_date

Falha na implantação porque as interfaces no dispositivo estão desatualizadas. Salve a configuração na página de interfaces e tente novamente.

device_package_error

Falha da implantação ao gerar configuração para o dispositivo. Se o problema persistir após outra tentativa, entre em contato com o

Esse erro indica falha ao gerar

configuração do dispositivo.

Entre em contato com o TAC da

TAC da Cisco.

device_package_timeout

Falha na implantação devido ao tempo limite durante a geração da configuração. Se o problema persistir após outra tentativa, entre em contato com o TAC da Cisco.

Isso pode acontecer se houver latência entre os dispositivos além dos intervalos normais. Entre em contato com o TAC depois que a latência estiver normalizada, esse problema ainda ocorrer.

device_communication_errors

Falha na implantação devido a uma falha na comunicação do dispositivo. Verifique a conectividade de rede e repita a implantação.

Essa mensagem é o fallback para qualquer problema de comunicação entre os dispositivos. Devido à sua natureza vaga, é escrito como fallback para declarar que ocorreu um erro de conectividade desconhecido.

unable_to_initiate_deployment_dc

Falha na implantação da política. Tentar implantação novamente.

Outra tentativa deve resolver esse problema. Isso pode ocorrer quando o FMC não pode iniciar a implantação devido a um bloqueio temporário no banco de dados.

device_failure_timeout

Falha na implantação para o dispositivo devido ao tempo limite. Tentar implantação novamente.

Isso está relacionado à implantação do FTD. Os processos no FTD aguardam minutos para que o dispositivo conclua a implantação. Caso contrário, o tempo expira. Se isso ocorrer, verifique a conectividade entre dispositivos e se a conectividade for como esperado, entre em contato com o TAC.

device_failure_download_timeout

Falha na implantação devido ao tempo limite de download da configuração para o dispositivo. Se o problema persistir após outra tentativa, entre em contato com o TAC da Cisco.

Isso está relacionado à implantação do FTD. O FTD pode baixar todos os arquivos de configuração do dispositivo durante a implantação devido a problemas de conectividade. Tente novamente depois que a conectividade de rede tiver sido verificada. Se isso tiver sido verificado, entre em contato com o TAC.

<p>device_failure_configuration</p>	<p>Falha na implantação devido a um erro de configuração. Se o problema persistir após outra tentativa, entre em contato com o TAC da Cisco.</p>	<p>Quaisquer erros na configuração gerada pelo F para o dispositivo devem resultar nesse erro após a aplicação. Isso precisa ser analisado logs do USMS para verificar quais problemas são vistos e tentar revertê-los. Uma vez reparado, isso geralmente requer intervenção do TAC e criação de bug se os logs não puderem ser correspondidos com um de conhecido na Cisco Bug Search Tool.</p>
<p>deployment_timeout_no_response_from_device</p>	<p>Falha na implantação devido ao tempo limite de comunicação com o dispositivo. Se o problema persistir após outra tentativa, entre em contato com o TAC da Cisco.</p>	<p>Esse tempo limite será atingido se o FMC não tiver recebido informações de um dispositivo após 45 minutos ou apenas este. Este é um erro de comunicação. Verifique a comunicação e verificado, entre em contato com o TAC.</p>
<p>device_failure_change_master</p>	<p>Falha na implantação do cluster, pois a unidade primária foi alterada. Tentar implantação novamente.</p>	<p>Para uma implantação de configuração de cluster FT o nó primário alternar quando a implantação estiver em andamento no dispositivo (notificação), esse erro será indicado. Tente novamente quando o primário estiver estável.</p>

device_failure_unknown_master	Falha na implantação para o cluster devido a uma falha na identificação da unidade primária. Tentar implantação novamente.	O status atual do membro cluster pode ser rastreado com este comando no CLISH do dispositivo gerenciado: >show cluster info
cd_deploy_app_sync	Falha na implantação porque a sincronização da configuração do cluster está em andamento. Tentar implantação novamente.	O FMC não pôde determinar o nó primário atual durante a implantação. Isso pode ser devido a algumas possibilidades: Problemas de conectividade ou primário não adicionado ao cluster FMC. Ele deve ser resolvido depois que a conectividade for restabelecida ou depois da adição do primário atual ao cluster FMC e uma nova tentativa for feita. O status atual do cluster pode ser rastreado com este comando no CLISH do dispositivo gerenciado: >show cluster info Isso pode ocorrer se o dispositivo estiver na Sincronização de Aplicativos depois que a Sincronização de Aplicativos for concluída, reimplantação mais uma vez.
cd_existing_deployment	Falha na implantação devido a conflito com a implantação anterior simultânea. Se o problema persistir após outra tentativa, entre em contato com o TAC da Cisco.	Isso pode ocorrer se uma implantação for simultânea em um lado, mas não no outro. Geralmente, isso é causado por problemas de comunicação entre os dispositivos. Entre em contato com o TAC após o tempo limite, você não conseguir fazer a implantação.

Entre em contato com o TAC para obter assistência

Caso as informações anteriores não permitam que uma implantação de política prossiga, ou caso o problema pareça não estar relacionado a um comportamento documentado preexistente, use as

etapas fornecidas no próximo link para gerar um arquivo de Solução de problemas e entre em contato com o TAC para análise e criação de bugs.

<https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html>

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.