排除Firepower威胁防御策略部署故障

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

策略部署概述

示例概述

故障排除

- FMC图形用户界面(GUI)
- 使用FMC日志进行故障排除
- 受管设备故障排除
- 示例

常见故障消息

相关信息

简介

本文档简要介绍FTD上的策略部署流程以及基本的故障排除技术。

先决条件

要求

Cisco 建议您了解以下主题：

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

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

使用Cisco Firepower Threat Defense (FTD),Adaptive Security Appliances Next-Gen(ASA)提供的传统状态防火墙功能和（由Snort ASA支持的）防火墙功能现在组合到一个产品中。由于此更改，Policy Deployment Infrastructure FTD现在处理两个ASA代码（也称为LINA）和一个捆绑包中的配置更改Snort。

策略部署概述

思科FTDPolicy Deployments用于管理和推送注册到(FMC)本身的设Firewall Management Center备的配置。

在部署中，有一系列步骤分为多个阶段。

FMC阶段可总结在此列表中。

第 0 阶段	部署初始化
第 1 阶段	数据库对象集合
第 2 阶段	策略和对象集合
第 3 阶段	NGFW命令行配置生成
第 4 阶段	设备部署包生成
第 5 阶段	发送和接收部署包
第 6 阶段	待处理的部署、部署操作和部署成功消息

了解流程中的阶段和故障位置有助于对系统面临的故障进行Firepower故障排除。

在某些情况下，由于先前的配置或缺少关键字导致设备报告无法解决的故障，它可能是冲突Advanced Flex Configuration。

示例概述

步骤1.点**Deployment**击，指定要选择的设备。

步骤2.提交设备部署后，FMC开始收集与设备相关的所有配置。

步骤3.收集配置后，FMC会创建数据包并通过其称为SFTunnel的通信机制将其发送到传感器。

步骤4. FMC通知传感器使用提供的策略开始部署过程，同时侦听单个响应。

步骤5.受管设备解压缩归档文件，并开始应用各个配置和软件包。

A.部署的前半部分是在本地测Snort试配置Snort以确保其有效性的配置。

当证明有效时，新配置将移至生产目录，以便在Snort.验证失败时，策略部署在此步骤中失败。

B.部署包负载的第二半部分用于LINA配置，在该配置中由ngfwManager进程直接应用到LINA进程。

如果发生故障，更改将回滚并发生策略部署故障。

步骤6.如果和SnortLINA包都成功，受管设备会发出重新启动或重新加载信号的信Snort号，以便加载新配置并保存所有当前配置。

步骤7.如果所有消息均成功，传感器将发送成功消息，并等待管理中心确认该消息。

步骤8.收到任务后，FMC将任务标记为成功并允许完成策略捆绑包。

故障排除

期间遇到Policy Deployment的问题可能是由于（但不限于）：

1. 配置错误
2. FMC和FTD之间的通信
3. 数据库和系统运行状况
4. 软件缺陷和警告
5. 其他特殊情况

其中一些问题可以轻松解决，而另一些问题则需要思科的帮Technical Assistance Center (TAC)助。

本部分的目的是提供隔离问题或确定根本原因的技术。

FMC图形用户界面(GUI)

思科建议在FMC设备上启动针对部署故障的每个故障排除会话。

在故障通知窗口中，在6.2.3以上的所有版本上，都有其他工具可以协助处理其他可能的故障。

利用部署记录

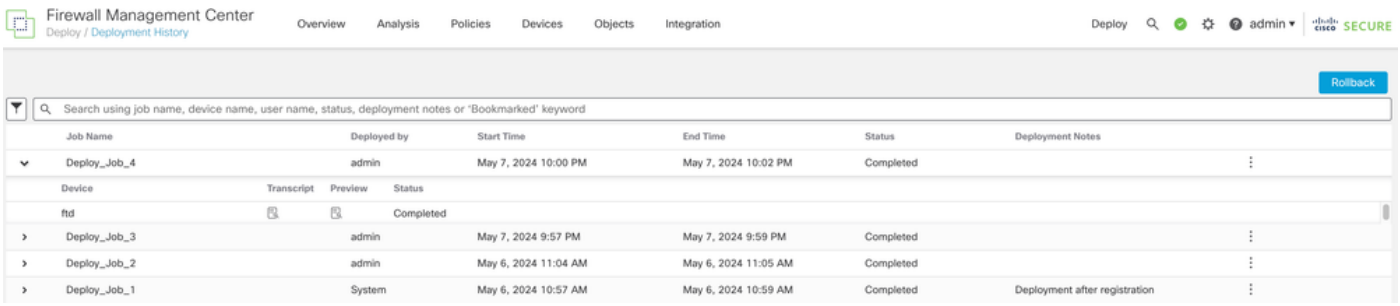
步骤1.上拉**Deployments**FMC Web UI上的列表。

步骤2.选中**Deployments**选项卡时，单**Show History**击。

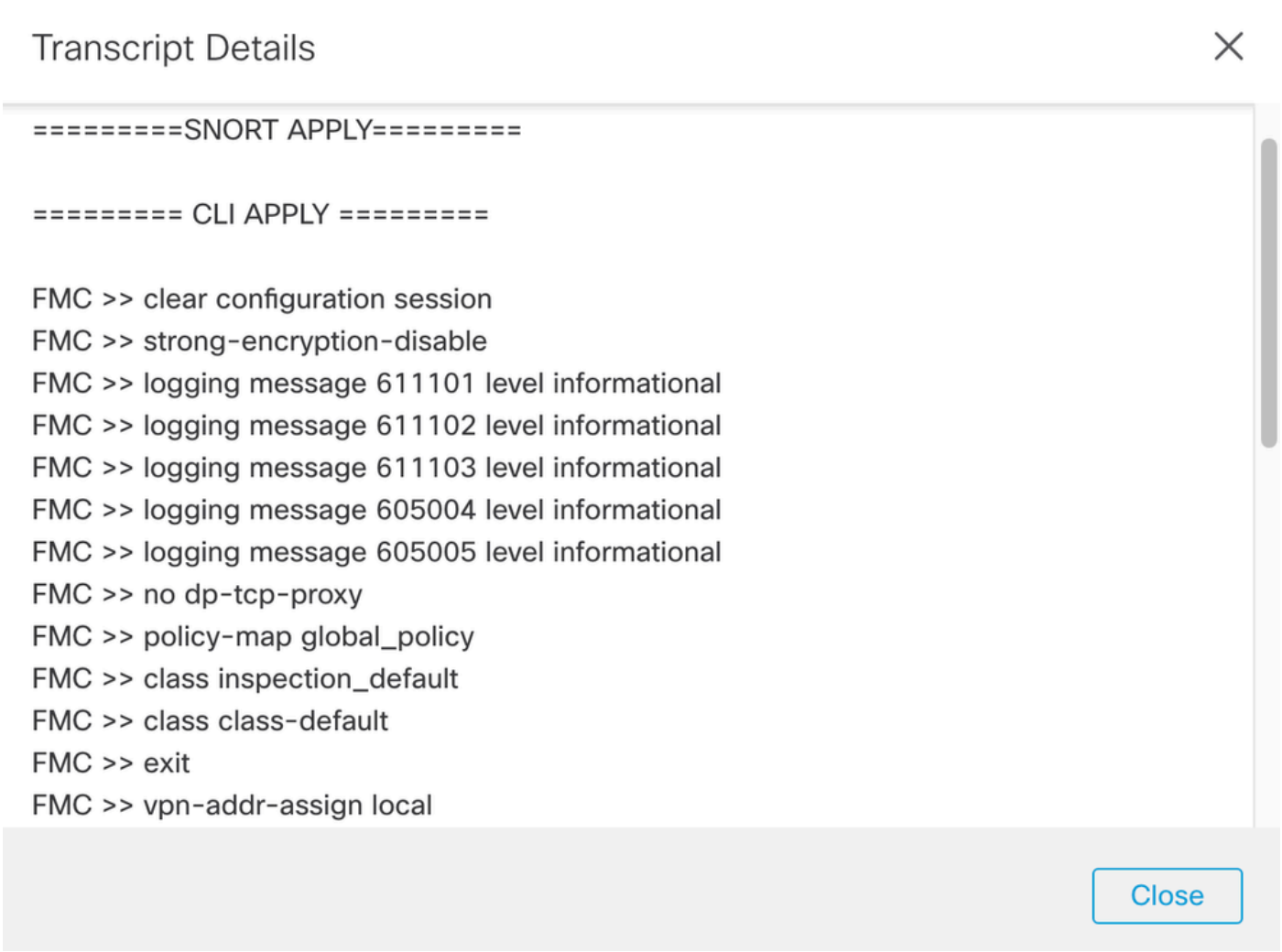


步骤3.在框内Deployment History部，您可以从FMC查看所有以前的部署。选择要查看更多数据的部署。

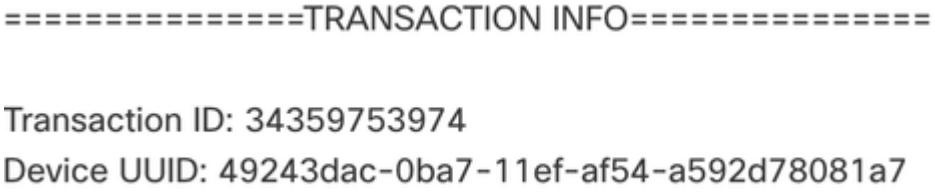
步骤4.选择部署元素后，该选Deployment Details择将显示内部所有设备的列Transaction表。这些条目按以下列划分：Device Number, Device Name, Status,和 Transcript.



第5步：选择所讨论的设备，然后单击transcript选项以查看单个部署脚本，该脚本可以通知您托管设备上的故障和配置。



步骤6.该脚本可以指定某些故障条件，并为下一步指明一个非常重要的编号：Transaction ID.



步骤7.在中Firepower Deployment是可Transaction ID用于跟踪策略部署的每个单独部分的内容。这样，在设备的命令行中，您可以获取此数据的更深入版本，用于补救和分析。

提示：如果您无法找到事务ID，或者您使用的版本在此版本打印之前，此日志仍可用于查找单个故障消息。

使用FMC日志进行故障排除

尽管与Cisco TAC一起分析日志是合适的，但搜索日志有助于初步隔离问题并加快解决速度。FMC上有多个日志文件，显示有关策略部署过程的详细信息。

两个最常引用的日志是policy_deployment.log和usmsharedsvcs.log的。

本文档中提及的所有文件都可使用多个Linux命令查看，**more**例如**less**和**vi**。但是，确保仅对其执行操作**read**非常重要。所有文件都需要root访问权限才能查看它们。

/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

此日志清楚地标示FMC上的策略部署任务的开始和每个阶段的完成，这有助于确定部署发生故障的阶段以及故障代码。

日志transactionID的JSON部分中包括的值可用于查找与特定部署尝试相关的日志条目。

```
10-May-2024 18:05:31.249,[INFO],(JsonRESTServerResource.java:111)
com.cisco.nm.vms.api.rest.DeploymentServerResource, ajp-nio-127.0.0.1-9009-exec-3
** REST Request [ DC ]
** ID : e45c6abd-0fff-4341-bdad-ddd5fee10034
** URL: POST https://localhost6/csm/api/deploy/GetTranscript
{
"data": {},
"deviceUUID": "49243dac-0ba7-11ef-af54-a592d78081a7",
"jobID": 34359753974,
"offset": {
"size": 20,
"start": 0
},
"requestID": "e3be908a0ef711ef9d519da21f9032fa",
"version": "7.2.5"
}
```

/var/log/sf/policy_deployment.log

虽然此日志文件在从6.4开始的6.x版本中一直存在，但其覆盖范围已扩展。

现在它描述了FMC上构建部署软件包的详细步骤，因此最好将其用于分析第1-4阶段的故障。

每个阶段的开始都标有一条线，上面写着 INFO start.

```
May 8 02:00:58 RTP-vFMC-Pod-09 ActionQueueScrape.pl[10413]: > SF::UMPD::CSMData::getPolicyRollbackInfo
May 8 02:00:58 RTP-vFMC-Pod-09 ActionQueueScrape.pl[10413]: < SF::UMPD::CSMData::getPolicyRollbackInfo
...
```

受管设备故障排除

还有一些阶段和部分取决于设备软件包、高可用性配置以及每个受管设备的先前阶段的结果。

如果部署问题被隔离为受管设备上的故障，则可以在设备上执行进一步的故障排除，并在设备上执行两次日志：policy_deployment.log和ngfwManager.log。

/ngfw/var/log/ngfwManager.log

此日志文件提供了由FMC采取的和与FMC进行通信、处理部署包以及协调Snort和LINA配置的验证和应用的详细步骤Config Dispatcher。

下面是ngfwManager.log的一些示例，它们代表主要阶段的开始：

```
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
May 30 16:37:10 ccm[4293] Thread-10: DEBUG com.cisco.ccm.ConfigCommunicationManager- <?xml version="1.0
```

```
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 databas
May 30 16:37:18 ccm[4293] Thread-9: DEBUG com.cisco.ccm.DownloadManager- handle record: 8589938211, sta
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: D
```

FTD begins LINA deployment:

```
May 30 16:37:42 ccm[4293] Thread-19: DEBUG com.cisco.ngfw.configdispatcher.communicators.LinaCommunicat
```

FTD begins finalizing the deployment:

```
May 30 16:38:48 ccm[4293] Thread-19: DEBUG com.cisco.ngfw.configdispatcher.communicators.LinaCommunicat
Name:Cluster-App-Conf-Finalize-Request
```

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

此日志包含应用于的策略的详细信息。尽管日志的内容大多是高级的，并且需要TAC进行分析，但仍可以使用几个关键条目跟踪该过程Snort.:

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::Devic
Jul 18 17:20:57 firepower policy_apply.pl[25122]: INFO  found NGFWPolicy =>   (NGFWPolicy::Util 32 <- N
...
Jul 18 17:20:57 firepower policy_apply.pl[25122]: INFO export FTD platform settings... (PlatformSetting
```

Config validation begins:

```
Jul 18 17:21:37 firepower policy_apply.pl[25122]: INFO  starting validateExportedFiles - sqlite = /var/
```

Validation has completed successfully:

```
Jul 18 17:21:49 firepower policy_apply.pl[25122]: INFO validateExportedFiles - sqlite = /var/cisco/depl
```

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::Devic
```

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-ac829f
Jul 18 17:22:02 firepower policy_apply.pl[26571]: INFO  sending SnortReload to a3bcd340-992f-11e9-a1f1-
```

Snort reload has completed successfully:

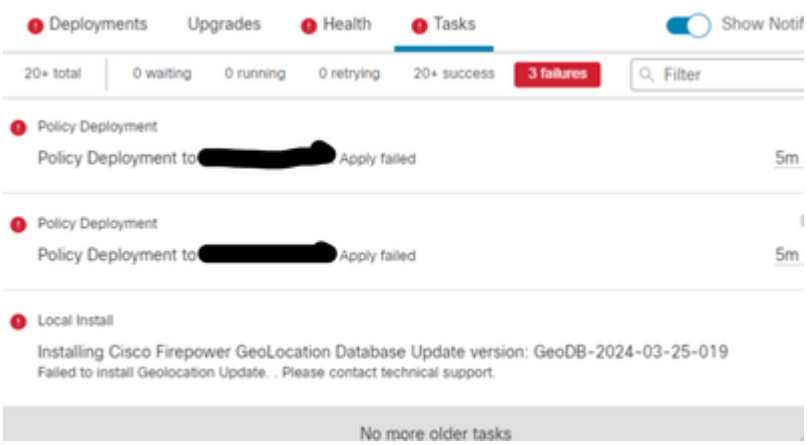
```
Jul 18 17:22:14 firepower policy_apply.pl[26571]: INFO notifyProcesses - sandbox = /var/cisco/deploy/sa
```

```
After LINA config apply finishes, Snort deployment is finalized:

Jul 18 17:23:32 firepower policy_apply.pl[26913]: INFO  starting finalizeDeviceDeployment - sandbox = /
```

示例

步骤1.部署失败。



步骤2.获取和**Deploy Transcript**URL **Transaction ID**.

```
===============TRANSACTION INFO===============

Transaction ID: 34359753974
Device UUID: 49243dac-0ba7-11ef-af54-a592d78081a7
```

步骤3.通过SSH连**Management Center**接到并使用Linux实**less**用程序读取文件，如FMC中所示：

示例：sudo less /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log（sudo password是您的ssh用户密码。）

```
admin@firepower:~$ sudo less /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log
Password:
```

步骤4.当您使用forward 斜杠并输入消息ID搜索与部署事务ID相关的日志时。

示例：/60129547881（使用时less,n可导航至下一个结果。）

运行消息示例

```
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" ]
}
```

失败消息示例

```
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)将正确的故障与附加的常见故障消息表进行比较。

即，failed_to_retrieve_running_configuration发生在两台设备之间的通信故障期间。

常见故障消息

这些是可在前端看到的常见故障消息以及可在后端看到的错误代Management Center Task码。

您可以对这些消息进行分析，并与可能解决方案的常见原因进行比较。如果看不到这些消息，或无法解决您的问题，请联系TAC寻求帮助。

错误代码	错误消息	原因
device_has_changed_domain	部署失败 — 设备已更改域。从{SRCDOMAIN}到{DESTINATIONDOMAIN}。请稍后再试。	当设备已移动或从第二个域获取时，通常会发生此错误。在没有跨域信息的情况下重新部署通常

		可以解决此问题。
device_currently_under_deployment	由于此设备正在进行另一个部署，部署失败。请稍后再试。	这通常在部署中的设备上触发部署时报告。在某些版本中，可在不发出故障通知的情况下防止发生故障；但是，此阶段仍用于故障排除帮助。
device_not_member_of_container	无法在作为集群成员的单个设备上执行部署。请稍后再次尝试部署集群。	此消息适用于具有Firepower可扩展操作系统(FXOS)机箱管理器的设备上的FTD。如果集群构建在FXOS上，但不构建在FMC上，则会显示此消息。尝试部署之前，请在管理中心设备上创建集群。
policy_altered_after_timestamp_for_other_devices_in_job_error	自{TIMESTAMP}以来，已更改一个或多个设备的策略。重试部署。	如果用户触发部署后、创建CSM元素和域快照前，部署作业中任何设备的任何策略/对象

		发生更改，则会显示此错误。重新部署可解决此问题。 当许多用户在部署时使用同一FMC编辑和保存对象时，可能会出现这种情况。
policy_altered_after_timestamp_error	自{Timestamp}以来，策略{Policy Name}已更改。重试部署。	如果部署作业中相关设备的任何策略/对象被更改，在用户触发部署之后，创建CSM和域快照之前，将显示此错误。 重新部署可解决此问题。
csm_snapshot_error	由于未能收集策略和对象，部署失败。如果反复尝试后问题仍然存在，请联系思科TAC。	如果提供了最近的Policy Import，请等待一个小时左右，然后尝试进行其他部署。 如果此操作不允许继续执行，请联系TAC，因为它是与数据库相关的消息。
domain_snapshot_timeout	部署失败，因为收集策略和对象超时。如果再次尝试后问题仍然存在，请联系思科TAC。	默认情况下，域快照的超时时间为5分钟。如果系统负载过重或虚拟机监控程序发生故障，则可

		能导致调用中出现非自然延迟。 如果管理中心或设备未获得适当的内存资源量，则可能会出现这种情况。 如果此操作在没有加载的情况下发生，或者稍后无法继续，请联系TAC。
domain_snapshot_errors	策略和对象集合中的部署失败。如果再次尝试后问题仍然存在，请联系思科TAC。	联系 TAC.需要高级故障排除。
failed_to_retrieve_running_configuration	部署失败，因为无法从设备检索运行配置信息。重试部署。	当终端传感器和FMC之间的连接未按预期运行时，可能会出现此消息。检验设备之间的隧道运行状况并监控两台设备之间的连接。 如果隧道按预期运行，并且设备可以通信，请联系TAC。
device_is_busy	部署失败，因为设备可以运行以前的部署或重新启动。	当FMC尝试部署时，当FTD上

	如果再次尝试后问题仍然存在，请联系思科TAC。	正在进行先前的部署时，会显示此消息。通常，在FTD上未完成之前的部署，并且FTD重新启动，或者FTD上的ngfwManager进程重新启动时，会发生这种情况。20分钟后重试以允许进程正式超时必须解决此问题。 如果延迟过后或者延迟不可接受，请联系TAC。
no_response_for_show_cmd	由于设备存在连接问题，部署失败，或者设备未响应。如果再次尝试后问题仍然存在，请联系思科TAC。	FMC发出某些LINA show命令来获取用于生成配置的运行配置。 当终端传感器上的ngfwManager进程出现连接问题或问题时，可能会发生这种情况。 如果您的设备之间没有出现连接问题，请联系TAC。
network_latency_or_device_not_reachable	由于与设备的通信失败，部	通常发生设备之

	署失败。如果再次尝试后问题仍然存在，请联系思科TAC。	间的高网络延迟，导致策略超时。验证设备之间的网络延迟，以验证它是否与用户指南中提到的版本的最小值匹配。
slave_app_sync	部署失败，因为正在进行群集配置同步。重试部署。	这仅适用于FTD集群设置。如果在进行应用同步（配置同步）时尝试在FTD集群上进行部署，则FTD会拒绝相同的部署。配置同步后重试必须解决此问题。 在受管设备CLISH中，可以使用此命令跟踪当前集群状态： > show cluster info
asa_configuration_generation_erations	部署无法生成设备配置。如果再次尝试后问题仍然存在，请联系思科TAC。	查看前面提到的USMS日志后，您可以查看导致错误的配置。这些漏洞通常是可以通过思科Bug工具浏览日志或联系思科TAC进行进一步故障排除的漏洞。

interface_out_of_date	部署失败，因为设备上的接口已过期。请保存接口页面上的配置并重试。	如果接口在部署期间或部署之前与设备取消关联，则会在4100或9300型号上发生这种情况。 在尝试部署之前，验证接口是否已完全关联或取消关联。
device_package_error	部署无法为设备生成配置。如果再次尝试后问题仍然存在，请联系思科TAC。	此错误表示无法生成设备的设备配置。联系TAC.
device_package_timeout	由于配置生成期间超时，部署失败。如果再次尝试后问题仍然存在，请联系思科TAC。	如果设备之间的延迟超过正常范围，则可能会出现这种情况。如果在延迟规范化后，仍然出现此问题，请联系TAC。
device_communication_errors	由于设备通信失败，部署失败。检查网络连接并重试部署。	此消息是设备之间所有通信问题的回退。由于其模糊性质，它被写为回退，表明发生了未知连接错误。

unable_to_initiate_deployment_dc	策略部署失败。重试部署。	必须再次尝试解决此问题。 当FMC由于临时锁定数据库而无法启动部署时，可能会发生这种情况。
device_failure_timeout	由于超时，部署到设备失败。重试部署。	这与FTD部署相关。FTD上的进程等待30分钟，以便调度完成部署。如果不成功，则会超时。 如果发生这种情况，请验证设备间的连接，如果连接符合预期，请联系TAC。
device_failure_download_timeout	由于设备配置下载超时，部署失败。如果再次尝试后问题仍然存在，请联系思科TAC。	这与FTD部署相关。由于连接问题，FTD无法在部署过程中下载所有设备配置文件。 请在验证网络连接后重试。 如果已经过验证，请联系TAC。
device_failure_configuration	由于配置错误，部署失败。如果再次尝试后问题仍然存在，请联系思科TAC。	FMC为设备生成的配置中的任何错误都必须在

		应用后导致此错误。 需要在USMS日志中分析此问题，以验证发现的问题并尝试回滚它们。 修复后，如果日志无法与Cisco Bug Search Tool中的已知缺陷匹配，则通常需要TAC干预和漏洞创建。
deployment_timeout_no_response_from_device	由于与设备的通信超时，部署失败。如果再次尝试后问题仍然存在，请联系思科TAC。	如果FMC在45分钟后仍未收到设备的回音，则会出≤此超时。 这是通信错误。 验证通信，如果验证，请联系TAC。
device_failure_change_master	部署到集群失败，因为主设备已更改。重试部署。	对于FTD集群设置部署，如果主节点在设备上进行部署时进行切换（后通知），则指示此错误。 在主节点稳定后重试。

		在受管设备CLISH中，可以使用此命令跟踪当前集群成员状态： > show cluster info
device_failure_unknown_master	由于主设备识别失败，部署到集群失败。重试部署。	FMC在部署期间无法确定当前的主节点。 通常，这归因于以下可能性：连接问题或当前主节点未添加到FMC上的集群中。 必须在重新建立连接后或在将当前主节点添加到FMC集群后对其进行解析，然后进行重试。 在受管设备CLISH中，可以使用此命令跟踪当前集群状态： > show cluster info
cd_deploy_app_sync	部署失败，因为正在进行群	如果设备处于应

	集配置同步。 重试部署。	用同步，则可能会发生这种情况。应用同步完成后，请再次重试部署。
cd_existing_deployment	由于与并行先前部署冲突，部署失败。如果再次尝试后问题仍然存在，请联系思科TAC。	如果部署在一端是并发的，而在另一端不是并发的，则可能会发生这种情况。 这些故障通常是由设备之间的通信问题引起的。 如果在超时后仍无法部署，请联系TAC。

相关信息

- 排除Firepower文件生成过程故障
- 思科技术支持和下载

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）。