排除Firepower威胁防御策略部署故障

目录

简介

本文档简要概述了FTD中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

借助 **Cisco Firepower Threat Defense** (FTD)， **Adaptive Security Appliances** (ASA)提供的传统状态防火墙功能和 **Next-Gen** 防火墙功能(由 **Snort** 支持)现在可组合为一个产品。

由于此更改，FTD上 **Policy Deployment Infrastructure** 现在处理ASA代码（也称为LINA）和 **Snort** 一个捆绑包的配置更改。

策略部署概述

思科FTD利用 **Policy Deployments** 管理和推出注册到 **Firewall Management Center** (FMC)自身的设备的配置。

在部署中，有一系列步骤被划分为“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	待定部署、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排除 **Firepower** 系统面临的故障。

在某些情况下，冲突可能是由于先前的配置或由于缺少 **Advanced Flex Configuration** 关键字而导致设备报告无法解决的故障。

示例概述

步骤1:点击 **Deployment**，指定要选择的设备。

第二步：提交设备部署后，FMC开始收集与设备相关的所有配置。

第三步：收集配置时，FMC创建数据包并通过其名为**SFTunnel**的通信机制将其发送到传感器。

第四步：FMC在侦听单个响应时通知传感器使用提供的策略启动部署过程。

第五步：受管设备解压缩存档文件并开始应用单个配置和包。

A.部署的前半部分是 **Snort** 配置，该配 **Snort** 置在本地进行测试以确保其有效性。

在证明有效后，新配置将移到 **Snort**的生产目录中。如果验证失败，则策略部署在此步骤失败。

B.部署包负载的第二半部分用于LINA配置，其中它由**ngfwManager**进程直接应用到LINA进程。

如果发生故障，更改将回滚并且策略部署发生故障。

第六步：如果 **Snort** 和LINA数据包均成功，受管设备会发出信号 **Snort** 以重新启动或重新加载，从而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消息。

步骤 8收到任务后，FMC会将任务标记为成功并允许策略捆绑完成。

故障排除

期间遇到的问题 **Policy Deployment** 可能是由于（但不限于）：

- 配置错误
- FMC和FTD之间的通信
- 数据库和系统运行状况
- 软件缺陷和警告
- 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 **Technical Assistance Center (TAC)**的帮助。

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设备上启动部署失败的每个故障排除会话。

在“故障通知”窗口中，在6.2.3以上的所有版本中，都有其他工具可以帮助处理其他可能的故障。

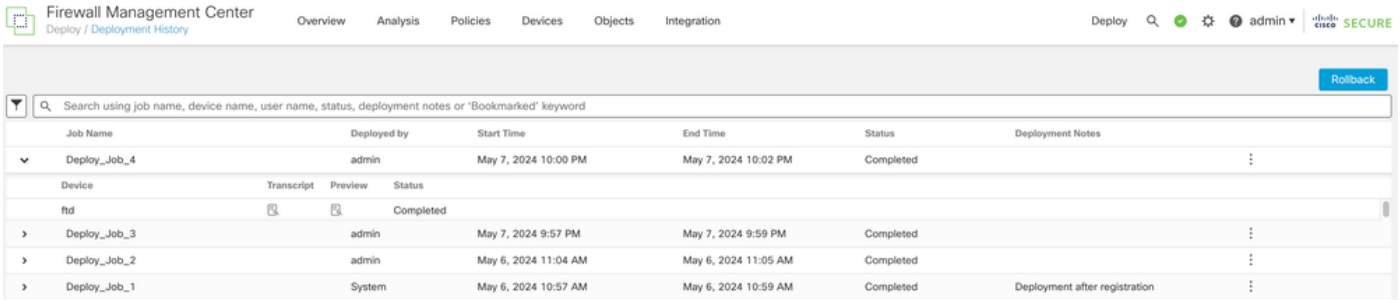
利用部署记录

步骤1:上拉**FMC Web UI**上的列 **Deployments** 表。

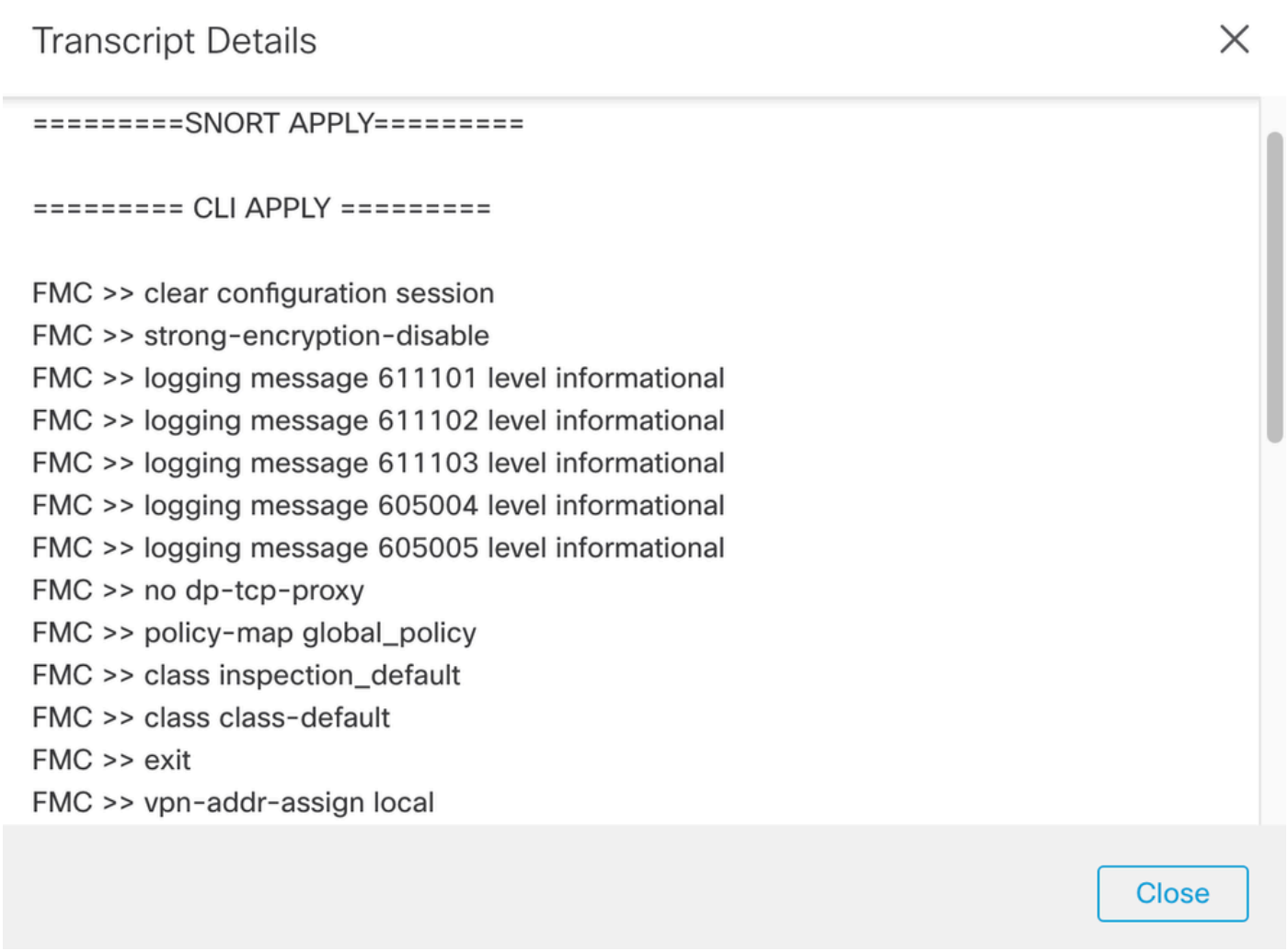
第二步：当 **Deployments** 选项卡处于选中状态时，请点击 **Show History**。

第三步：在 **Deployment History** 框内，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。

第四步：选择部署元素后，选 **Deployment Details** 择内容将显示 **Transaction**内部所有设备的列表。这些条目细分为以下列： **Device Number, Device Name, Status,**和 **Transcript**。



第五步：选择所讨论的设备，并点击transcript选项以查看单个部署脚本，该脚本可以通知您受管设备上的故障和配置。



第六步：该记录可以指定某些故障条件，并为下一步骤显示一个非常重要的编号： **Transaction ID**。

==========TRANSACTION INFO==========

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

步骤 7.在 **Firepower Deployment**中， **Transaction ID** 是可用于跟踪策略部署的每个独立部分的内容。这样，在设备的**命令行**上，您可以获取此数据的更深入版本，以进行补救和分析。

提示：如果找不到事务ID，或者您使用的版本在此版本打印之前，则此日志仍可用于查找单个失败消息。

使用FMC日志进行故障排除

尽管让Cisco TAC参与分析日志是合适的，但搜索日志可以帮助初步隔离问题并加快解决速度。FMC上有多个显示策略部署过程详细信息的日志文件。

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

本文档中所有提及的文件均可使用多个Linux命令查看，例如 **more**、 **less** 和 **vi**。但是，确保仅对其执行操 **read** 作非常重要。所有文件都需要root访问权限才能查看。

/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。

日志的JSON部分中包含的 **transactionID** 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

虽然此日志文件存在于6.x版本（从6.4开始）的所有版本中，但其覆盖范围已扩展。

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

每个阶段的开始都标有一行，其上带有 **INFO start** .

May 8 02:00:58 RTP-vFMC-Pod-09 ActionQueueScrape.pl[10413]: > SF::UMPD::CSMData::getPolicyRollbackInfo start (161.32M)
May 8 02:00:58 RTP-vFMC-Pod-09 ActionQueueScrape.pl[10413]: < SF::UMPD::CSMData::getPolicyRollbackInfo end (161.32M, 0.012(sec))
...

受管设备故障排除

还存在一些额外的阶段和部分，具体取决于设备软件包、高可用性配置以及每个受管设备的先前阶段的结果。

如果部署问题隔离到受管设备上的故障，则可以在设备上执行进一步故障排除，并在设备上执行两个日志：**policy_deployment.log**和**ngfwManager.log**。

/ngfw/var/log/ngfwManager.log

此日志文件提供 **Config Communication Manager** 和 **Config Dispatcher** 与FMC进行通信、处理部署软件包以及协调**Snort**和LINA配置的验证和应用的详细步骤。

下面是**ngfwManager.log**的几个示例，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- Pas

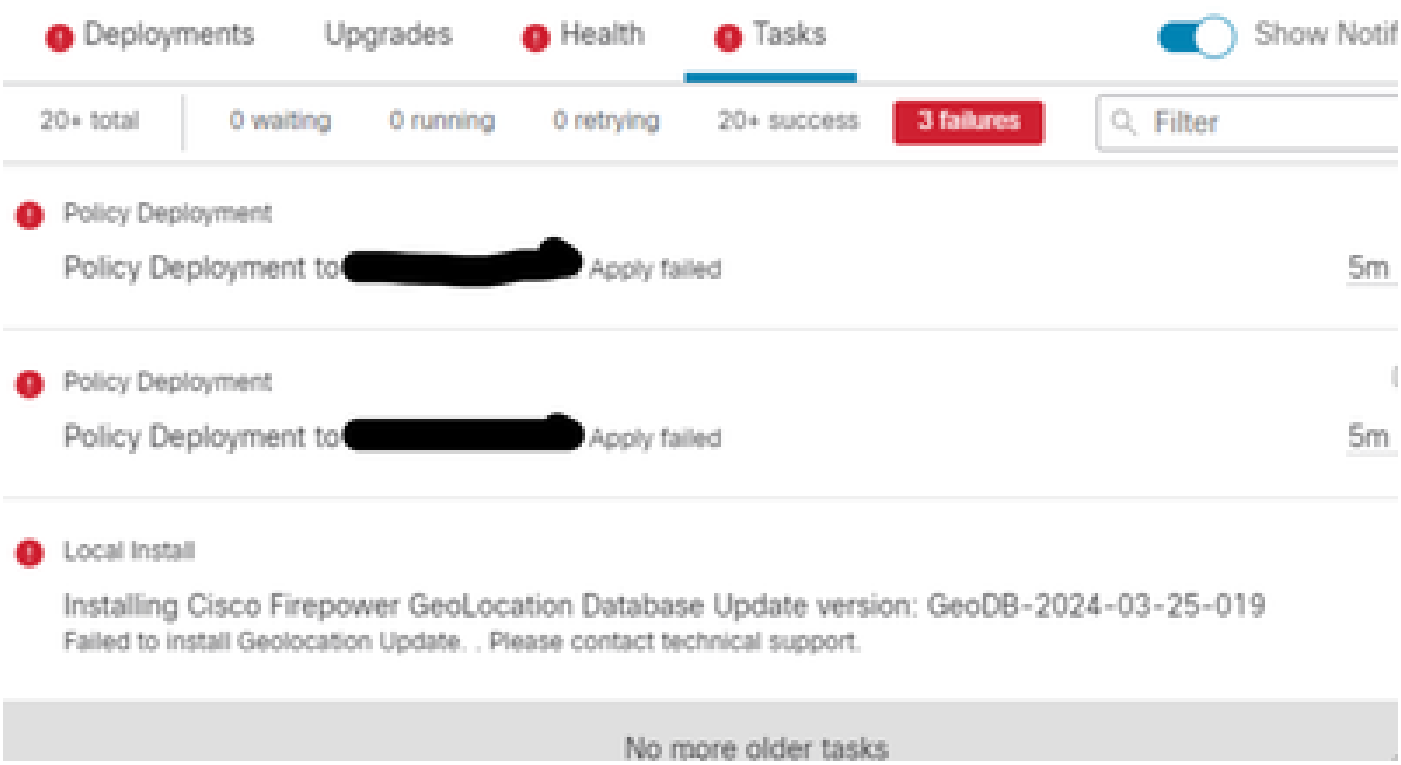
/ngfw/var/log/sf/policy_deployment.log

此日志包含应用于 **Snort**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，但仍可以通过几个关键条目跟踪该过程：

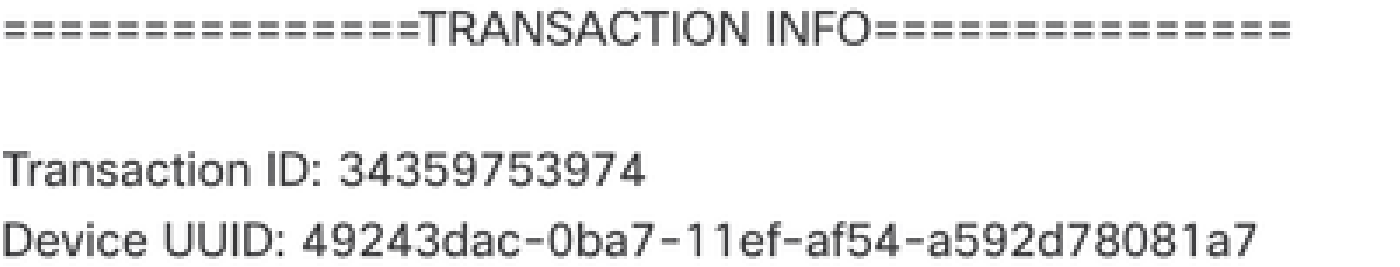
Config Dispatcher begins extracting the packaged policies for validation: Jul 18 17:20:57 firepower policy_apply.pl[25122]: INFO -> calling SF::UMPD::I

示例

步骤1:部署失败



第二步：获取 **Deploy Transcript** 和 **Transaction ID**。



第三步：通过SSH登录 **Management Center** 并使用Linux实用程序 **less** 来读取文件，如您的FMC所示：

示例：**sudo less /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log**（sudo密码是ssh的用户密码。）

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

第四步：当您在 **less**中时，使用正斜杠并在消息ID中输入以搜索与部署事务**ID**相关的日志。

示例： **/60129547881** (在**less**，使用**n**导航到下一个结果。)

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**发生在两个设备之间的通信故障期间。

常见故障消息

这些是常见故障消息，可在 **Management Center Task** 的前端看到，错误代码可在后端看到。

可以分析这些消息，并将其与可能解决问题的常见原因进行比较。

如果未看到这些内容，或者无法解决您的问题，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-设备已将域从 **{SRCDOMAIN}**更改为 **{DESTINATIONDOMAIN}**。请稍后再试。	当设备移动或从第二个域中取走时，通常会发生此错误。在没有发生跨域信息的情况下进行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。	在部署中的设备上触发部署时，通常会报告此问题。在某些版

		本中，此过程会在不发出故障通知的情况下被阻止；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。如果集群基于FXOS而非FMC构建，则显示此消息。在尝试部署之前，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，一个或多个设备的策略已更改。重试部署。	如果在用户触发部署后，以及在创建CSM元素和域快照之前，为部署作业中的任何设备更改任何策略/对象，将显示此错误。 重新部署可以解决此问题。 当许多用户在部署时使用同一FMC编辑和保存对象时，可能会发生这种情况。

policy_altered_after_timestamp_error	自{Timestamp}以来，策略{Policy Name}已更改。重试部署。	此错误显示为：如果在部署作业中、用户触发部署后、CSM和域快照创建前，为相关设备更改了任何策略/对象。 重新部署可以解决此问题。
csm_snapshot_error	由于策略和对象收集失败，部署失败。如果重复尝试后问题仍然存在，请与Cisco TAC联系。	如果提供了最近的策略导入，请等待一小时左右，然后尝试进行其他部署。 如果这不允许继续执行，请联系TAC，因为它是与数据库相关的消息。
domain_snapshot_timeout	由于收集策略和对象超时，部署失败。如果再次尝试后问题仍然存在，请与Cisco TAC联系。	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，则可能导致呼叫中出现不自然的延迟。 如果管理中心或设备未获得适当数量的内存资源，则可能出现这种情况。 如果在不加载的情况下发生此情

		况，或稍后未继续操作，请与TAC联系。
domain_snapshot_errors	在策略和对象集合中部署失败。如果再次尝试后问题仍然存在，请与Cisco TAC联系。	联系 TAC.需要进行高级故障排除。
failed_to_retrieve_running_configuration	由于无法从设备检索运行配置信息，部署失败。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。验证设备之间的隧道运行状况并监控两个设备之间的连接。 如果隧道如预期那样运作并且设备可以通信，请与TAC联系。
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。如果再次尝试后问题仍然存在，请与Cisco TAC联系。	当FMC尝试部署时，当FTD上正在进行先前的部署时，会显示此消息。通常，在FTD上未完成先前的部署，并且FTD已重新启动，或者FTD上的**ngfwManager**进程已重新启动时发生。20分钟后重试以允许进程正式超时必须

		解决此问题。 如果延迟后或者延迟不可接受，请与TAC联系。
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，请与Cisco TAC联系。	FMC发出某些LINA **show**命令来获取用于生成配置的运行配置。 当终端传感器上存在连接问题或**ngfwManager**进程问题时，可能出现这种情况。 如果您的设备之间没有出现连接问题，请与TAC联系。
network_latency_or_device_not_reachable	由于与设备的通信失败，部署失败。如果再次尝试后问题仍然存在，请与Cisco TAC联系。	通常在设备之间的高网络延迟下发生，从而导致策略超时。验证设备之间的网络延迟，以验证它是否与用户指南中提及的最低版本匹配。

slave_app_sync	由于正在进行群集配置同步，部署失败。重试部署。	这仅适用于FTD集群设置。如果在应用程序同步（配置同步）进行中时尝试在FTD集群上进行部署，FTD将拒绝相同操作。配置同步后重试必须解决此问题。 可通过受管设备CLISH中的以下命令跟踪当前集群状态： > **show cluster** info
asa_configuration_generation_error	部署无法生成设备配置。如果再次尝试后问题仍然存在，请与Cisco TAC联系。	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漏洞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interfaces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，则在4100或9300型号上会发生这种情况。

		在尝试部署之前，验证接口已完全关联或未关联。
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，请与Cisco TAC联系。	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，请与Cisco TAC联系。	如果设备之间的延迟超过正常范围，则可能会发生这种情况。如果延迟规范化后，仍然出现此问题，请与TAC联系。
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。	此消息是设备之间的所有通信问题的回退。由于其模糊性，它被写为回退以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，等待调度完成部署。否则，它会超时。 如果出现这种情况，请验证设备间的连接，如果连接正常，请与TAC联系。
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，请与Cisco TAC联系。	这与FTD部署相关。由于连接问题，FTD无法在部署期间下载所有设备配置文件。 请在验证网络连接后重试。 如果验证成功，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，请与Cisco TAC联系。	FMC为设备生成的配置中的任何错误都必须导致此**error post apply**。 需要在USMS日志中对此进行分析，以验证发现的问题并尝试将其回滚。 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，请与Cisco TAC联系。	如果FMC在≤45分钟后仍未收到来自设备的消息，则会出现此超时。 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。 主节点稳定后重试。 可通过受管设备CLISH中的以下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在部署过程中无法确定当前的主节点。 通常，这归因于以下可能性：连接问题或当前主设备未添加到FMC上的集群。 必须在重新建立连接后或者将当前主节点添加到FMC集群后解决它，并完成重试。 可通过受管设备CLISH中的以下命令跟踪当前集群状态： **> show cluster** info
cd_deploy_app_sync	由于正在进行群集配置同步，部署失败。 重试部署。	如果设备处于应用同步状态，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	部署失败，因为与并行以前的部署冲突。如果再次尝试后问题仍然存在，请与Cisco TAC联系。	如果部署在一端并行执行，而在另一端并行执行，则可能发生这种情况。

		这些故障通常由设备之间的通信问题引起。 如果在超时后仍然无法部署，请与TAC联系。

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）。