

由于接口导致cdFMC的FTD部署失败

目录

问题

云交付的Firepower管理中心(cdFMC)无法将配置更改部署到设备。部署始终以约10%的进度失败，并显示以下错误消息：“由于生成设备配置失败，部署失败。如果重试后问题仍然存在，请与思科TAC联系。”

尝试配置虚拟隧道接口(VTI)站点到站点VPN时，最初触发了此问题。但是，回滚VPN配置无法解决部署故障，只有特定设备受到影响，而其他受管设备继续成功部署。

环境

- 运行FTD版本7.4.2的思科安全防火墙1140(FPR1140)设备，由cdFMC 10.0.93管理
- 独立的cdFMC和FTD配置
- 触发问题的VTI站点到站点VPN配置和删除尝试

分辨率

通过对cdFMC和受影响的FTD设备之间的管理接口状态进行虚拟编辑，解决了部署故障。此过程涉及从cdFMC用户界面取消合并并重新合并FTD管理接口。

执行的故障排除步骤

1:分析部署历史记录、预览和部署脚本，以确认配置生成阶段出现的失败进度约为10%。

```
=====FMC DEPLOY=====
DEVICE SNAPSHOT ERROR: "Deployment halted due to interface data inconsistency in Firewall Management Ce
SF::UMPD::Plugins::NGFWPolicy::Manager::populateDeviceSnapshot(<SF::UMPD::Snapshot>, <SF::UMPD::CSMDData
SF::UMPD::Plugin::execute("SF::UMPD::Plugins::NGFWPolicy::Manager", "populateDeviceSnapshot", <SF::UMPD
SF::UMPD::Framework::populateDeviceSnapshot("/var/cisco/umpd/51539718357/DC_policy_deployment.db", "/va
=====TRANSACTION INFO=====
Transaction ID: 51539718357
Device UUID:    UUID
Transaction ID: 51539718357
Selected policy group list: Prefilter Policy, Access Control Policy, NGFW Interface, NGFW Automatic App
```

2:从cdFMC和受影响的FTD设备收集故障排除和跟踪文件，以确定部署故障的根本原因。

```
Mar 25 17:26:14 CDFMC  mojo_server.pl[20297]: DEVICE SNAPSHOT ERROR: "Deployment halted due to interfac
Mar 25 17:26:14 CDFMC  mojo_server.pl[20297]: Deployment halted due to interface data inconsistency in
Mar 25 17:26:14 CDFMC  mojo_server.pl[20297]:          SF::UMPD::Plugins::NGFWPolicy::Manager::populateDev
Mar 25 17:26:14 CDFMC  mojo_server.pl[20297]:          SF::UMPD::Plugin::execute("SF::UMPD::Plugins::NGFWP
Mar 25 17:26:14 CDFMC  mojo_server.pl[20297]:          SF::UMPD::Framework::populateDeviceSnapshot("/var/c
```

3:内部分析根据缺陷Cisco Bug ID CSCwt46144 (软件从7.2.4升级到7.4.2后发生) 识别出与FTD管理接口状态相关的异常。

解决步骤

1:如果管理接口出现问题，请从FTD CLI或cdFMC UI确认FTD是否具有融合接口。如果是，则管理接口需要取消合并，并且由于虚拟编辑在融合接口上不可行，因此重新合并管理接口。



注意：对于可能导致此缺陷的任何其他接口，解决方法是为指定接口部署“虚拟编辑”。

```
> show management-interface convergence
management-interface convergence
>
```

2:访问cdFMC UI Devices > Device Management，然后点击Firewall Threat Defense的Edit (编辑图标)，并取消合并受影响的FTD设备管理接口以重置设备管理状态。对于管理接口，点击取消合并管理接口 (取消合并管理接口)。

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	OUTSIDE	Physical	OUTSIDE-ZONE			Disabled	Global
GigabitEthernet0/1	INSIDE	Physical	INSIDE-ZONE			Disabled	Global

接口恢复为Diagnostic0/0。

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Diagnostic0/0	diagnostic	Physical			192.168.40.74/255.255.255.0(Stat...	Disabled	Global
GigabitEthernet0/0		Physical				Disabled	
GigabitEthernet0/1		Physical				Disabled	

2:从cdFMC用户界面重新合并FTD管理接口，以将设备管理状态与cdFMC重新同步。

Firewall Management Center

Overview Analysis Policies Devices Objects Integration

Deploy admin

Tac_test

Cisco Firepower Threat Defense for VMware

Device Interfaces Inline Sets Routing DHCP

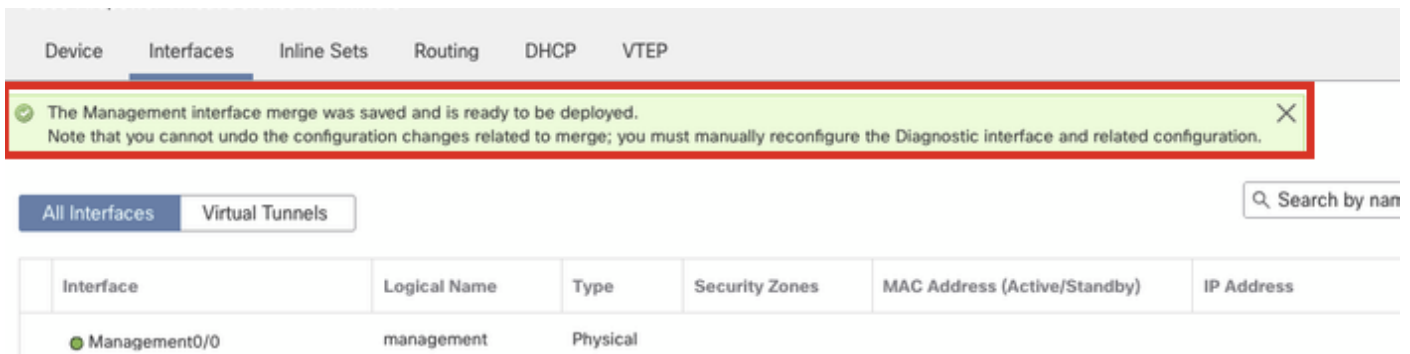
Management Interface Merge

- The management interface merge will be synced to the standby/data unit. The IP addresses shown in the "Review Uses" section shows the active unit's active address.
- After you click Proceed, IP address changes will be saved, and you cannot revert the management interface merge, even if you discard the deployment.
- Diagnostic interface static routing is no longer supported; you must delete the route before you can proceed.
- HA monitoring for diagnostic interface is not supported.

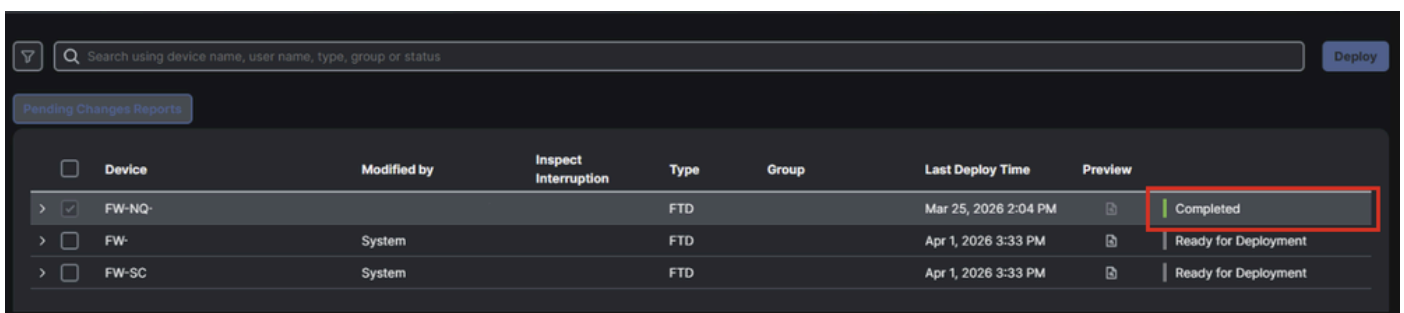
In this release, you can merge the Management and Diagnostic interfaces to use the single IP instead of two IP addresses. The merged interface will be called Management and use the current management IP address. You will need to update all external services that communicate with Diagnostic IP address.

Proceed Cancel

3:重新合并操作完成后，执行所有挂起配置更改的完整部署。



4:确认部署成功完成且没有错误，并且所有配置更改已正确应用到FTD设备。



原因

此问题由Cisco bug ID CSCwt46144引起。从版本7.2.4升级到7.4.2后，受影响的FTD设备上引入了陈旧和不一致的管理接口状态。这种不一致使cdFMC无法成功构建和推送设备特定的配置，导致配置生成阶段早期部署失败。管理接口状态异常会特别影响cdFMC和FTD设备之间的通信和同步，导致部署过程失败，然后任何配置更改都可以应用到目标设备。

该缺陷特定于cdFMC设备，并打算在下一版10.0.94的cdFMC中解决。

相关内容

- Cisco Bug ID [CSCwt46144](#) — 策略部署失败，错误为10% — 由于防火墙管理中心中的接口数据不一致，部署暂停
- [在FMC中配置管理和诊断接口的合并](#)
- [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）。