在FTD注册期间排除FMC自动配置部署故障

目录

问题

在将防火墙威胁防御(FTD)设备迁移到新的防火墙管理中心(FMC)环境期间，FMC会在FTD注册后立即自动部署配置。此自动部署发生在手动VPN策略重新连接和证书配置完成之前，这会导致安全客户端/AnyConnect用户的VPN连接丢失，并导致计划外服务中断。

环境

- 安全防火墙管理中心(FMC)。
- 为安全客户端/AnyConnect VPN服务配置的FTD。
- 从现有FMC到新FMC环境的迁移方案。

分辨率

用户通过以下后续步骤解决了即时连接问题：

- 步骤1.重新配置设备配置：用户重新配置了自动部署期间覆盖的原始设备配置和工作VPN设置。
- 步骤2.重新附加策略：已手动重新连接正确的策略，以确保为新的FMC环境恢复并正确配置VPN功能。

原因

FTD注册到新FMC期间的自动部署行为是预期功能，而不是缺陷。用户对手动部署控制的期望基于文档解释，但系统的默认行为是在设备注册时自动部署配置，以确保整个FMC托管环境的策略一致性。


提示：考虑使用设备模板在FTD注册时应用第2天配置更改。FMC版本7.6.0中引入了设备模板。

相关内容

- 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）。