

借助安全云控制将本地FMC迁移到云(cdFMC)

目录

[问题](#)

[环境](#)

[分辨率](#)

[原因](#)

[相关内容](#)

- [问题](#)
 - [环境](#)
 - [分辨率](#)
 - [原因](#)
 - [相关内容](#)
-

问题

用户需要帮助，才能将其生产防火墙管理中心(FMCv300)虚拟设备迁移到安全云控制(SCC)租户中的云交付FMC(cdFMC)。具体关注点包括：

- 了解迁移过程的哪些部分可能会导致停机，以及如何最大限度地减少对生产的影响。
- 获取迁移工作流程的分步指南。
- 确定在迁移完成后如何处理FMCv300。
- 为高可用性(HA)配置中的多个防火墙威胁防御(FTD)设备规划分阶段迁移方法。
- 在触发迁移向导之前，说明是否必须手动将本地FMC配置导入cdFMC。

环境

- 源FMC:FMCv300虚拟设备，版本7.6.5。还可以部署其他硬件(HW)和软件(SW)平台。
- 目标：已调配cdFMC租户。

- 受管设备是来自不同硬件和软件版本的FTD，例如：
 - 2个Secure Firewall 3130,FTD 7.6.4，以高可用性对配置。
 - 2个Firepower 2130,FTD 7.4.4，在高可用性对中配置。
 - 1个FTDv在Azure 7.6.4中，独立配置。

分辨率

迁移前提条件和版本验证

环境版本满足迁移到cdFMC的必备条件：

- FMC 7.6.5符合迁移工作流的书面最低要求。
- FTD版本7.6.4和7.4.4满足已记录的最低迁移要求。
- cdFMC支持环境中的FTD版本系列。

迁移前验证步骤

在启动迁移之前，请验证以下前提条件：

- FMCv300上没有挂起部署。
- 两个HA对正常且已同步。
- FMCv300备份已完成。
- 足够的FMC可用磁盘空间（至少10%的可用空间）。
- 从FTD管理路径执行DNS解析。
- 允许通过所需的云管理端口（TCP 443和TCP 8305）从FTD管理接口到cdFMC的出站连接。
- FMCv300具有对SCC的出站HTTPS访问。

配置导入过程

在运行迁移向导之前，无需手动将本地FMCv300配置导入cdFMC。“将FTD迁移到cdFMC”工作流程在迁移作业中处理配置导入：

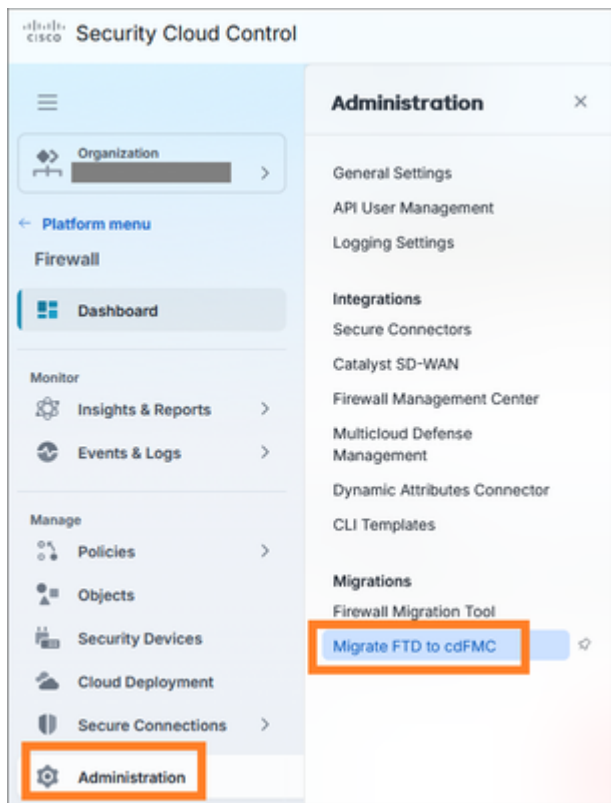
1. SCC连接到内部FMCv300。
2. 它从内部FMC导出相关配置。
3. 它将共享策略/对象导入到cdFMC中。
4. 导入特定于设备的配置，例如接口和路由。
5. 它将选定的FTD设备注册到cdFMC。
6. 14天的评估期在迁移完成后开始。

如果在迁移之前在cdFMC中手动创建与FMCv300上的项同名的策略或对象，迁移工作流程可以使用现有cdFMC项而不是导入内部版本，这会导致意外结果。

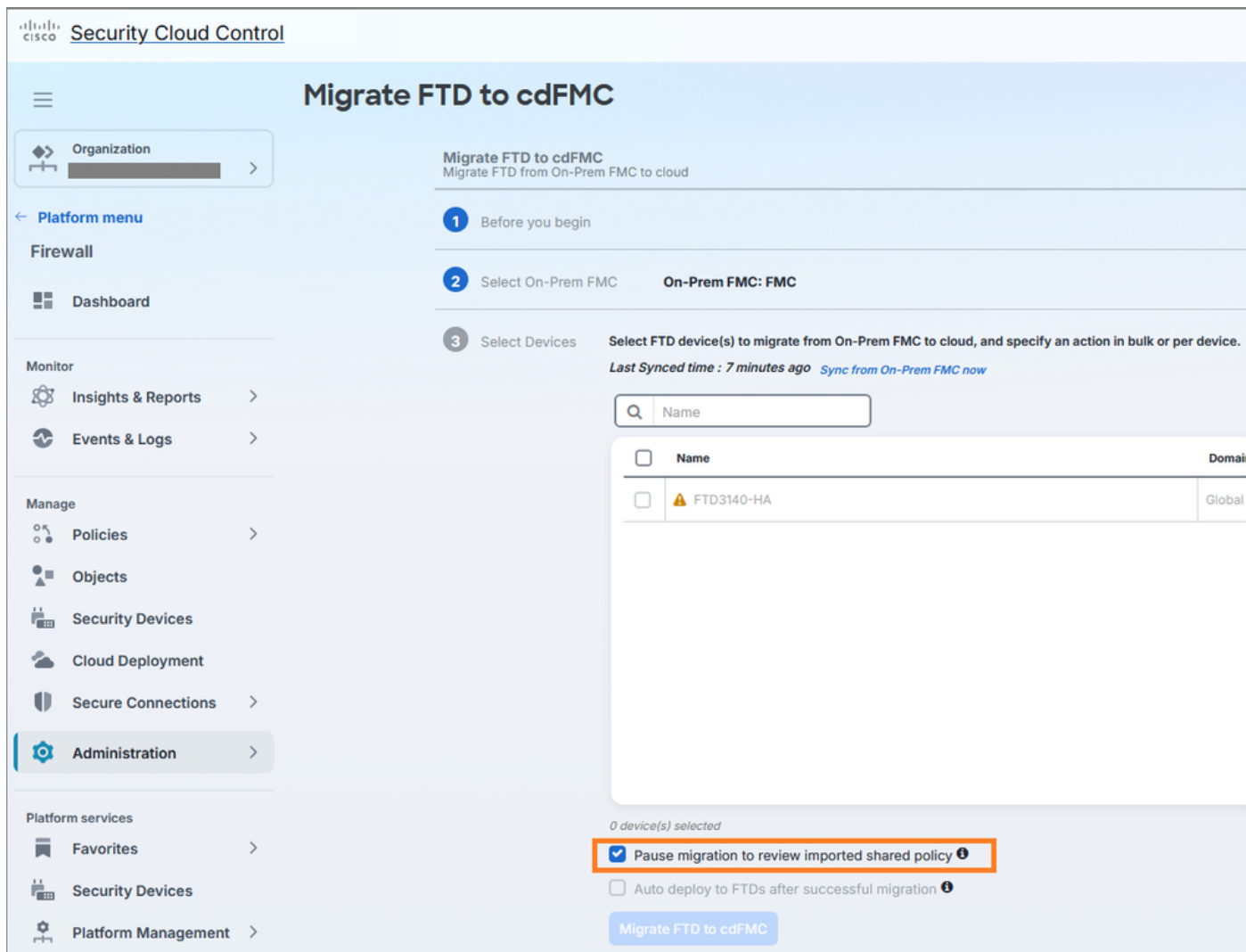
推荐的迁移顺序

第 1 阶段：迁移前设置

1. 在您的SCC租户中部署cdFMC。
2. 将当前FMCv300连接到SCC。
3. 确认cdFMC的智能许可。
4. 从Firewall > Administration > Migrations > Migrate FTD to cdFMC启动迁移工作流程：



5. 使用选项在共享策略导入后暂停以供审阅：



第 2 阶段：迁移执行

在维护期间，使用分阶段的方法迁移设备：

1. 从独立FTD开始（影响最小）。
2. 迁移第一对高可用性。
3. 验证设备运行状况和功能。
4. 迁移第二对高可用性。

第 3 阶段:迁移后验证

迁移每个设备或HA对后：

1. 在cdFMC中确认设备运行状况。
2. 确认适用的HA状态。
3. 查看部署预览/警告。
4. 从cdFMC部署。
5. 验证流量和事件可视性。

包含配置冻结的三阶段迁移计划

建议的方法包括分三个阶段执行FTD迁移，每个阶段分别执行三个不同的日期，每个阶段最少进行三天的割接后监控。此方法降低了风险，并提供了验证以下内容的时间：

- 从cdFMC进行策略部署。
- 设备运行状况。
- 两个HA对的高可用性状态。
- 云中的事件/分析可视性。
- 在进入下一阶段之前遇到任何操作问题。

配置冻结实施

在迁移/评估期间，使用以下方法实施配置冻结：

- 最佳选择：冻结FMCv300和cdFMC中所有与FTD相关的配置更改，直到验证并提交每个阶段。
- 最小值选项：冻结要迁移的设备以及已迁移和未迁移的设备使用的任何共享策略/对象。
- 避免在分阶段迁移期间在FMCv300和cdFMC中编辑相同的共享策略/对象。
- 避免在评估期间发生重大变化。

紧急变更流程

对于迁移期间的紧急更改：

- 仅将更改应用于该设备的当前授权管理器：
 - 尚未迁移的设备：FMCv300。
 - 已迁移的设备：cdFMC。
- 记录更改、受影响的策略/对象、时间戳和设备范围。
- 在阶段完成之后协调更改，尤其是当更改影响共享对象或共享策略时。

评估期管理

14天评估窗口的重要注意事项：

- 跟踪每个迁移阶段/作业的14天评估窗口。
- 不要让任何阶段无意中达到自动提交。
- 如果三天监控成功，请手动提交此阶段，而不是等待整整14天。

FMCv300停用进程

请勿在设备迁移后立即关闭或删除FMCv300。保持FMCv300可用，直到：

- 所有FTD设备均已成功迁移。
- cdFMC部署成功。
- 云分析/事件已确认。
- 迁移已提交。
- 满足任何日志/事件保留要求。
- 根据组织策略保留最终FMCv300备份。

满足这些条件后，FMCv300可根据标准虚拟机停用流程从活动使用和停用。

原因

这是从本地FMC到cdFMC的计划迁移。迁移的驱动因素是需要利用基于云的管理功能并停用现有的FMCv300虚拟设备。

相关内容

- [将FTD迁移至cdFMC — 思科文档](#)
- [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）。