升级FMCv并从VMware ESXi 7.0迁移到ESXi 8.0:分阶段方法和最佳实践

目录

问题

在VMware ESXi 7.0上运行防火墙管理中心虚拟(FMCv)版本7.3.1的管理员计划将FMC升级到受支持的更高版本，然后将FMCv虚拟机迁移到新的VMware ESXi 8.0群集。在规划过程中提出了以下问题：

- 先将FMCv从7.3.1升级到7.4.2，然后将VM迁移到ESXi 8.0群集是否安全，然后再执行任何进一步的升级。
- 将运行版本7.3.1或7.4.2的FMCv迁移到VMware ESXi 8.0环境时，是否存在已知的兼容性问题或限制。
- 是否可以使用VMware vMotion来执行FMCv虚拟机到新群集的无缝、同一IP迁移，而无需创建新的VM实例。
- 在升级或迁移失败时，VMware快照是否可以用作备份和回滚机制。
- 最高可支持的FMC版本适用于现有受管设备环境，包括从7.2.8版到7.4.2版的防火墙威胁防御(FTD)设备。
- 如何避免在切换到新群集上的新FMCv实例时发生IP地址冲突，同时保持相同的管理IP地址和主机名。
- 正确的操作顺序是分阶段升级和迁移计划，以最大限度地降低风险和停机时间。

环境

- 产品:FMCv
- 当前FMC软件版本：7.3.1
- 当前虚拟机监控程序平台：VMware ESXi 7.0

- 目标虚拟机监控程序平台：VMware ESXi 8.0.3（新群集）
- FMC部署类型：独立（不是高可用性对的一部分）
- 受管设备:从7.2.8版到7.4.2版的多个FTD设备

分辨率

针对此环境的推荐方法是分阶段、分阶段升级和迁移计划。此计划将FMC软件升级、虚拟机监控程序平台迁移和任何后续FMC版本升级分为不同的维护事件。此方法可降低每个阶段的风险并提供明确的回滚点。使用VMware vMotion、快照、克隆或直接的VM级迁移显然不是在群集或版本之间迁移FMCv的支持方法。

重要信息：FMCv迁移不支持VMware快照、vMotion和克隆

在继续本计划的任何阶段之前，必须了解以下有关VMware本地迁移方法的限制条件：

- VMware快照不是FMCv升级或迁移支持的备份、还原或回滚方法。将FMCv恢复为VMware快照可能会导致数据库损坏、版本和内容更新不匹配或系统状态不受支持。
- VMware vMotion、克隆和集群之间的直接虚拟机迁移不受支持将FMCv迁移到新的虚拟机监控程序平台的方法。这些方法绕过FMC的内部数据完整性机制。
- 将FMCv迁移到新群集或主机的唯一受支持方法是FMC本地备份和还原工作流，以及结合在目标平台上部署新的FMCv实例。

如果转换后验证失败，正确的回滚策略是关闭新的FMCv实例并将原始FMCv恢复为服务。不要依赖快照还原来实现此目的。

第 1 阶段：升级前兼容性检查

在启动任何FMC软件升级之前，请确认环境中所有托管FTD设备的确切软件版本。

- FMC 7.4.2支持对运行版本7.0及更高版本的FTD设备进行管理。

- FMC 7.6.6支持对运行版本7.1及更高版本的FTD设备进行管理。
- 如果环境中的任何FTD设备运行的版本低于7.0，则在FMC保留在7.3.1版本时，必须将该设备升级到至少版本7.0，然后升级FMC本身。
- 对于已编档的环境(FTD范围：7.2.8到7.4.2)，所有受管设备都在FMC 7.4.2和FMC 7.6.6的兼容性范围内。在这种情况下，不需要FTD预升级。

在继续操作之前，请确认以下内容：

- FMC是独立的，不是高可用性(HA)对的一部分。
- 新群集上精确的VMware ESXi 8.0版本（在此环境中已确认为ESXi 8.0.3）。
- FMCv资源配置文件（vCPU、内存、磁盘）满足目标FMC版本的要求。必须根据当前部署指南检查当前的4个vCPU、32 GB RAM和250 GB磁盘规格，尤其是在升级到FMC 7.6.6之前。
- 迁移后FMC管理IP地址和主机名是否保持不变（强烈建议避免在所有托管FTD设备上要求管理员地址更新）。

第 2 阶段：将当前ESXi 7.0群集上的现有FMCv从7.3.1升级到7.4.2

此阶段将FMCv软件升级到版本7.4.2，同时将其保留在现有的ESXi 7.0基础架构上。FMCv 7.4.2添加了对VMware ESXi 8.0的明确支持，这是在第3阶段平台迁移之前所必需的。

步骤 1：在开始升级之前，请确认FMC上当前未运行任何挂起策略部署、活动备份作业或后台任务。

步骤 2：使用FMC内置备份实用程序执行完全本机FMC备份。将备份存储在FMCv虚拟机之外的安全远程位置。在继续操作之前，请验证备份是否成功完成。

步骤 3：按照FMC 7.4升级规划指南中的说明完成所有升级准备情况检查。在启动升级之前解决所有标记的问题。

步骤 4：将现有FMCv从版本7.3.1升级到版本7.4.2。这将使用支持的升级过渡路径：7.3 → 7.4。

步骤 5：升级完成后，执行升级后验证：

- 检验所有托管FTD设备是否已重新连接到FMC。

- 确认事件接收处于活动状态，且事件显示在FMC中。
- 确认许可状态正确。
- 对受管设备执行测试策略部署并确认其成功。

在升级后的FMCv 7.4.2上成功通过所有升级后验证步骤之前，请勿继续执行阶段3。

第 3 阶段:使用本地备份和还原将FMCv迁移到VMware ESXi 8.0.3群集

此阶段将FMCv从现有ESXi 7.0群集迁移到新的ESXi 8.0.3群集。通过在目标群集上部署新的FMCv实例并将本地FMC备份还原到该实例上，可以实现此目的。保留相同的管理IP地址和主机名，以避免要求所有托管FTD设备上的管理器地址发生更改。

步骤 1：在7.4.2版本中确认FMCv稳定后，生成新的本地FMC备份。将其存储在安全的远程位置。在继续操作之前，请验证备份是否完整有效。

步骤 2：在ESXi 8.0.3群集中部署新的FMCv实例。此新实例的软件版本和内部版本必须与从中进行备份的FMCv(FMCv 7.4.2)的版本（包括补丁程序和修补程序）完全匹配。 确保新实例配置了等效或更大量的资源（vCPU、内存、磁盘），并且网络配置是暂存的，但此时尚未将生产管理IP地址分配给新实例。

步骤 3：将本地FMC备份还原到ESXi 8.0.3上的新FMCv实例上。

步骤 4：在将新的FMCv与生产管理IP地址和主机名联机之前，请完全关闭原始FMCv或将其断开网络。这是防止重复IP条件和避免两个FMC实例同时尝试与同一受管FTD设备通信的强制步骤。

在原始FMCv断电和新的FMCv联机之前，托管FTD设备预期会发生以下行为：

- 流量转发：FTD设备独立于FMC运行数据平面，并继续无缝转发流量并执行上次成功部署的访问控制策略，此处提及的情形除外。
- 管理和可视性变更：策略部署、配置调整、FMC运行状况警报和设备管理可视性完全不可用。
- 事件缓冲和潜在损失：FMC的实时事件可视性暂停。当FTD尝试在其临时统一文件中本地记录安全和连接事件时，这些文件具有严格的存储限制，并以循环覆盖的方式运行。在扩展迁移期间，可能会覆盖或丢失大量连接日志。在新的FMC联机后，本地缓冲区中剩余的事件将流

式传输到新的FMC。

- 恶意软件(AMP)规则：未缓存文件的实时云查找请求暂时不可用，因为FMC将这些信誉查询代理到AMP云。FTD继续对已存储在其本地机上处置缓存中的文件执行阻止或仅允许规则。未缓存的文件绕过云分析并使用策略的故障保护设置（通常无法打开以防止流量中断）。 将沙盒提交到Threat Grid和追溯性警报暂停，直到新的FMC运行正常。
- 基于身份的规则：已登录并映射到IP地址的用户不会遇到中断，因为FTD在其本地内存中保留活动映射。但是，由于FMC充当身份源（例如，思科ISE或Active Directory代理）的代理，因此FTD无法获知此窗口期间的新用户登录或IP更改。这些未知会话将回退到策略的默认或访客规则。
- URL 过滤:完全未知网站的实时云查找暂时不可用，因为FMC将未知URL请求代理到思科Talos云。FTD继续完全过滤和执行策略，只对已在其推送的本地数据集或其活动本地内存缓存中找到的网站执行策略。命中未缓存的未知URL的网络流量会绕过云分类，并匹配未分类流量的策略回退设置（通常允许）。URL数据库包更新暂停，直到新的FMC联机。

步骤 5：将生产管理IP地址和主机名分配给ESXi 8.0.3上恢复的FMCv并使其联机。由于使用相同的IP地址和主机名，受管FTD设备可以自动重新连接到FMC，而无需在单个FTD设备上更改管理器地址。

步骤 6：执行迁移后验证：

- 检验所有托管FTD设备是否已重新连接到新的FMCv实例。
- 检查许可状态并确认所有许可证已正确应用。
- 确认事件流和任何外部集成均正常运行。
- 对受管设备执行受控策略部署并确认其成功。

如果在此阶段的任何时候验证失败，请关闭新FMCv实例的电源，将ESXi 7.0上的原始FMCv恢复为服务，并在重新尝试迁移之前进行故障排除。请勿将VMware快照恢复用作回滚机制。

第 4 阶段：将FMCv从7.4.2升级到7.6.6（确认迁移稳定后）

一旦FMCv迁移到ESXi 8.0.3经过完全验证并确认稳定，可以考虑进一步升级到FMC 7.6.6。强烈建议不要将虚拟机监控程序平台迁移（第3阶段）和此附加FMC版本升级合并到单个维护事件中。完成迁移之前，先提供一个干净、低风险的检查点，然后再继续操作。

开始升级到7.6.6之前，请确认以下前提条件：

- 环境中的每个托管FTD设备都运行版本7.1或更高版本。FMC 7.6.6不支持管理FTD设备（版本7.1）。在文档环境(FTD范围：7.2.8到7.4.2)，所有设备均符合此要求。
- FMCv资源配置文件（4个vCPU、32 GB RAM和250 GB磁盘）已根据FMC 7.6.6部署指南对此环境中的受管设备总数和事件保留要求进行了验证。
- 已确认支持的升级过渡路径：7.4 → 7.6。
- FMC被确认为独立（不是高可用性对的一部分）。

步骤 1：从ESXi 8.0.3上稳定的FMCv 7.4.2实例创建并验证新的本地FMC备份。将其存储在安全的远程位置。

步骤 2：将FMCv从版本7.4.2升级到版本7.6.6。

步骤 3：执行最终的升级后验证：

- 检验所有托管FTD设备是否已重新连接到FMC。
- 确认事件处理和事件接收功能正常。
- 确认许可状态正确。
- 执行受控策略部署以确认策略应用成功。

升级路径和过渡顺序总结

该表汇总了完整的阶段计划、支持的升级过渡以及每个阶段的关键操作：

阶段	操作	FMC版本	虚拟机监控程序	支持的过渡
第 1 阶段	升级前兼容性检查；确认FTD版本、FMC HA状态和资源配置文件	7.3.1（当前）	ESXi 7.0	不适用 — 仅准备
第 2 阶段	升级FMCv软件；执行本地备份；验证受管设备和策略部署	7.3.1 → 7.4.2	ESXi 7.0	7.3 → 7.4（支持）
第 3 阶段	在ESXi 8.0.3上部署新的FMCv;恢复本机备份；使用同一IP/主机名进行切换；验证	7.4.2（无版本更改）	ESXi 7.0 → ESXi 8.0.3	本地备份/恢复 — 支持的方法

第 4 阶段	迁移稳定后：升级FMCv;验证设备连接、许可、事件、策略	7.4.2 → 7.6.6	ESXi 8.0.3	7.4 → 7.6（支持）

主要考虑因素

- 升级路径合规性：完整的升级序列(7.3.1 → 7.4.2 → 7.6.6)使用支持的FMC升级过渡路径（7.3 → 7.4和7.4 → 7.6）。 不建议跳过中间版本或将阶段组合为一个事件。
- FMC-FTD兼容性：FMC 7.6.6与运行版本7.2.8至7.4.2的FTD设备保持完全的管理兼容性。FMC 7.6要求所有托管FTD设备都处于版本7.1或更高版本。
- 相同的IP地址转换：在替换FMCv与生产管理IP地址一起联机之前，必须完全关闭原始FMCv的电源或与网络断开连接。这可防止出现重复IP情况，并避免两个管理中心同时尝试与同一FTD设备通信。当恢复的FMCv使用相同的IP地址和主机名返回时，托管的FTD设备可以重新连接，而无需更改管理器地址。
- 7.6.6之前的资源验证：在升级到FMC 7.6.6之前，必须根据当前部署指南审查FMCv资源配置文件（4个vCPU、32 GB RAM、250 GB磁盘），同时考虑环境的受管设备总数和事件保留要求。
- 本地备份验证：在执行本地FMC备份的每个阶段，必须先验证备份是否完整有效，然后才能继续。备份必须存储在FMCv虚拟机之外的安全远程位置。
- 不要将迁移和升级结合使用：平台迁移（第3阶段）和随后的FMC版本升级到7.6.6（第4阶段）必须作为单独的维护事件执行。这可以确保ESXi 8.0.3上的FMCv 7.4.2存在干净的检查点，然后进行进一步更改。

原因

这不是由软件缺陷或配置错误引起的中断修复问题。需要此指南的根本原因是版本兼容性要求与特定于VMware上的Cisco FMCv的平台迁移限制的组合：

- FMC版本与FTD 7.4.2的兼容性：如果环境中存在运行版本7.4.2的托管FTD设备，则需要FMC升级到版本7.4.2的最低版本，因为早期的FMC版本无法管理版本高于FMC本身的FTD设备。
- VMware ESXi 8.0的FMCv支持：FMCv 7.3.1不支持VMware ESXi 8.0作为虚拟机监控程序平台。FMCv必须升级到版本7.4.2（或更高版本）才能在ESXi 8.0.x上部署或操作。尝试将FMCv 7.3.1 VM直接迁移到ESXi 8.0而不首先升级FMC软件会导致兼容性风险。

- 不受支持的VM迁移方法：VMware vMotion、快照、克隆和直接虚拟机迁移不支持在集群或虚拟机监控程序版本之间迁移FMCv的方法。这些方法可能会导致数据库损坏、版本不匹配或系统状态不受支持。唯一支持的迁移路径是FMC本地备份和恢复工作流程与在目标平台上的全新FMCv部署相结合。

相关内容

- Cisco Secure Firewall Management Center升级指南，版本7.4 — 升级规划和支持的路径
- Cisco Secure Firewall Management Center升级指南，版本7.6 — 升级规划和支持的路径
- 思科安全防火墙管理中心兼容性指南（FMC和FTD兼容性矩阵）
- Cisco Secure Firewall Management Center新功能（按版本） — 7.4.2版
- Cisco Firepower管理中心升级指南 — 升级规划
- 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）。