更改 **Unified Manager** 虚拟设备主机名

Active IQ Unified Manager 9.13

NetApp
October 16, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/active-iq-unified-manager-913/config/task_generate_an_https_security_certificate_ocf.html on October 16, 2025. Always check docs.netapp.com for the latest.

目录

更改 Unified Manager 虚拟设备主机名 1
生成 HTTPS 安全证书 1
重新启动 Unified Manager 虚拟机 3

更改 Unified Manager 虚拟设备主机名

首次部署 Unified Manager 虚拟设备时，系统会为网络主机分配一个名称。您可以在部署后更改主机名。如果更改主机名，则还必须重新生成 HTTPS 证书。

- 您需要的内容 *

要执行这些任务，您必须以维护用户身份登录到 Unified Manager 或分配有应用程序管理员角色。

您可以使用主机名（或主机 IP 地址）访问 Unified Manager Web UI 。如果您在部署期间为网络配置了静态 IP 地址，则应指定网络主机的名称。如果使用 DHCP 配置网络，则应从 DNS 中获取主机名。如果 DHCP 或 DNS 配置不正确，系统会自动分配主机名 "`Unified Manager` " 并将其与安全证书关联。

无论主机名的分配方式如何，如果更改主机名并打算使用新主机名访问 Unified Manager Web UI ，则必须生成新的安全证书。

如果您使用服务器的 IP 地址而不是主机名访问 Web UI ，则在更改主机名后不必生成新证书。但是，最好更新证书，使证书中的主机名与实际主机名匹配。

如果在 Unified Manager 中更改主机名，则必须在 OnCommand Workflow Automation （ WFA ）中手动更新主机名。主机名不会在 WFA 中自动更新。

新证书在 Unified Manager 虚拟机重新启动后才会生效。

步骤

1. 生成 HTTPS 安全证书

   如果要使用新主机名访问 Unified Manager Web UI ，则必须重新生成 HTTPS 证书才能将其与新主机名关联。

2. 重新启动 Unified Manager 虚拟机

   重新生成 HTTPS 证书后，必须重新启动 Unified Manager 虚拟机。

生成 HTTPS 安全证书

首次安装 Active IQ Unified Manager 时，将安装默认 HTTPS 证书。您可以生成一个新的 HTTPS 安全证书来替换现有证书。

- 您需要的内容 *

您必须具有应用程序管理员角色。

重新生成证书的原因可能有多种，例如您希望为可分辨名称（ Distinguished Name ， DN ）设置更好的值，或者您希望增加密钥大小或延长到期期限，或者当前证书已过期。

如果您无法访问 Unified Manager Web UI ，则可以使用维护控制台使用相同的值重新生成 HTTPS 证书。在重新生成证书时，您可以定义密钥大小和密钥的有效期。如果您使用 `Reset Server Certificate` 选项、则会创建一个新的HTTPS证书、此证书的有效期为397天。此证书的 RSA 密钥大小为 2048 位。

步骤

1. 在左侧导航窗格中，单击 * 常规 * > * HTTPS 证书 * 。
2. 单击 * 重新生成 HTTPS 证书 * 。

   此时将显示重新生成 HTTPS 证书对话框。

3. 根据要生成证书的方式，选择以下选项之一：

如果您要 ...	执行此操作 ...
使用当前值重新生成证书	单击 * 使用当前证书属性重新生成 * 选项。
使用不同的值生成证书	单击 * 更新当前证书属性 * 选项。 如果不输入新值， " 公用名 " 和 " 备用名称 " 字段将使用现有证书中的值。应将 "`Common Name` " 设置为主机的 FQDN 。其他字段不需要值，但您可以输入电子邮件，公司，部门， 城市，省 / 自治区 / 直辖市和国家 / 地区，以便在证书中填充这些值。您也可以从可用密钥大小（密钥算法为 "`RSA` " ）和有效期中进行选择。 • 允许的密钥大小值为 2048，3072 和 4096。 • 有效期至少为 1 天，最多为 36500 天。 即使允许使用 36500 天的有效期，建议您使用的有效期不超过 397 天或 13 个月。由于如果您选择的有效期超过 397 天，并计划导出此证书的 CSR 并使其由知名 CA 签名，则此 CA 返回给您的签名证书的有效期将缩短为 397 天。 • 如果要从证书的 " 备用名称 " 字段中删除本地标识信息，可以选中 " 排除本地标识信息（例如本地主机） " 复选框。选中此复选框后，备用名称字段将仅使用您在字段中输入的内容。如果留空，则生成的证书将根本没有备用名称字段。

4. 单击 * 是 * 重新生成证书。
5. 重新启动 Unified Manager 服务器，以使新证书生效。
6. 通过查看 HTTPS 证书来验证新证书信息。

重新启动 **Unified Manager** 虚拟机

您可以从 Unified Manager 的维护控制台重新启动虚拟机。生成新的安全证书或虚拟机出现问题时，必须重新启动。

- 您需要的内容 *

虚拟设备已启动。

您以维护用户身份登录到维护控制台。

您也可以使用 * 重新启动来宾 * 选项从 vSphere 重新启动虚拟机。有关详细信息，请参见 VMware 文档。

步骤

1. 访问维护控制台
2. 选择 * 系统配置 * > * 重新启动虚拟机 * 。

版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。