Platform Services Controller 管理

Update 1
2018 年 10 月 16 日
VMware vSphere 6.7
VMware ESXi 6.7
vCenter Server 6.7

vmware®

您可以从 VMware 网站下载最新的技术文档：
https://docs.vmware.com/cn/。
VMware 网站还提供了最近的产品更新。
如果您对本文档有任何意见或建议，请将反馈信息发送至：
docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

目录

关于《Platform Services Controller 管理》 5

1 Platform Services Controller 入门 7

vCenter Server 和 Platform Services Controller 部署类型 7

具有外部 Platform Services Controller 实例和高可用性的部署拓扑 10

了解 vSphere 域、域名和站点 12

Platform Services Controller 功能 13

管理 Platform Services Controller 服务 14

管理 Platform Services Controller 设备 17

2 使用 vCenter Single Sign-On 进行 vSphere 身份验证 20

了解 vCenter Single Sign-On 20

配置 vCenter Single Sign-On 标识源 27

了解 vCenter Server 双因素身份验证 33

将 vCenter Single Sign-On 用作其他服务提供程序的身份提供程序 46

安全令牌服务 (STS) 47

管理 vCenter Single Sign-On 策略 53

管理 vCenter Single Sign-On 用户和组 57

vCenter Single Sign-On 安全性最佳做法 63

3 vSphere 安全证书 65

不同解决方案途径的证书要求 66

证书管理概览 69

使用 vSphere Client 管理证书 79

从 vSphere Web Client 管理证书 85

使用 vSphere 证书管理器实用程序管理证书 86

手动证书替换 99

4 使用 CLI 命令管理服务和证书 130

运行 CLI 所需的特权 131

更改 certool 配置选项 132

certool 初始化命令参考 133

certool 管理命令参考 135

vecs-cli 命令参考 138

dir-cli 命令参考 142

5 对 Platform Services Controller 进行故障排除 149

确定 Lookup Service 错误的原因 149

无法使用 Active Directory 域身份验证进行登录 150
由于用户帐户被锁定，vCenter Server 登录失败 152
VMware 目录服务复制需要较长时间 152
导出 Platform Services Controller 支持包 153
Platform Services Controller 服务日志引用 153

关于《Platform Services Controller 管理》

《Platform Services Controller 管理》文档介绍如何将 VMware® Platform Services Controller™ 部署到您的 vSphere 环境并帮助执行证书管理和 vCenter Single Sign-On 配置等常见任务。

《Platform Services Controller 管理》介绍如何设置 vCenter Single Sign-On 身份验证，以及如何管理 vCenter Server 和相关服务的证书。

表 1. 《《Platform Services Controller 管理》》内容要点

主题	内容要点
Platform Services Controller 入门指南	■ vCenter Server 部署模型和 Platform Services Controller 部署模型。注意：此信息因产品版本而异。 ■ Linux 和 Windows 上的 Platform Services Controller 服务。 ■ 管理 Platform Services Controller 服务。 ■ 使用 VAMI 管理 Platform Services Controller 设备。
使用 vCenter Single Sign-On 进行 vSphere 身份验证	■ 身份验证过程的架构。 ■ 如何添加标识源，以便域中的用户可以进行身份验证。 ■ 双因素身份验证。 ■ 管理用户、组和策略。
vSphere 安全证书	■ 证书模型和用于替换证书的选项。 ■ 从 UI 替换证书（简单情况）。 ■ 使用 Certificate Manager 实用程序替换证书。 ■ 使用 CLI 替换证书（复杂情况）。 ■ 证书管理 CLI 参考。

相关文档

相关文档《vSphere 安全性》介绍可用安全功能以及为保护您的环境免受攻击可采取的措施。该文档还说明了如何设置权限，并包括对特权的引用。

除上述文档外，VMware 还针对每个 vSphere 版本发布了《vSphere 安全性配置指南》（以前称为强化指南），网址为：http://www.vmware.com/security/hardening-guides.html。《vSphere 安全性配置指南》中包含有关以下安全设置的准则：客户可以或应设置的安全设置，以及 VMware 提供且应由客户审核以确保仍设置为默认值的安全设置。

目标读者

此信息面向需要配置 Platform Services Controller 及关联服务的管理员。本信息的目标读者为熟悉虚拟机技术和数据中心操作且具有丰富经验的 Windows 或 Linux 系统管理员。

vSphere Client 和 vSphere Web Client

本指南中的说明反映 vSphere Client（基于 HTML5 的 GUI）。您也可以使用这些说明通过 vSphere Web Client（基于 Flex 的 GUI）执行任务。

vSphere Client 和 vSphere Web Client 之间工作流明显不同的任务具有重复过程，其根据相应客户端界面提供步骤。与 vSphere Web Client 有关的过程在标题中包含 vSphere Web Client。

注 在 vSphere 6.7 Update 1 中，几乎所有 vSphere Web Client 功能在 vSphere Client 中得以实现。有关其他不受支持的功能的最新列表，请参见《vSphere Client 功能更新说明》。

Platform Services Controller 入门 1

Platform Services Controller 可以为 vSphere 环境提供通用基础架构服务。服务包括许可、证书管理和进行 vCenter Single Sign-On 身份验证。

本章讨论了以下主题：

- vCenter Server 和 Platform Services Controller 部署类型
- 具有外部 Platform Services Controller 实例和高可用性的部署拓扑
- 了解 vSphere 域、域名和站点
- Platform Services Controller 功能
- 管理 Platform Services Controller 服务
- 管理 Platform Services Controller 设备

vCenter Server 和 Platform Services Controller 部署类型

您可以部署具有嵌入式或外部 Platform Services Controller 部署的 vCenter Server Appliance，或安装具有嵌入式或外部 Platform Services Controller 部署的适用于 Windows 的 vCenter Server。您也可以将 Platform Services Controller 作为设备部署，或者将其安装在 Windows 上。如有必要，可以使用混合操作系统环境。

部署 vCenter Server Appliance 或安装适用于 Windows 的 vCenter Server 之前，必须确定适合您环境的部署模型。对于每个部署或安装，必须选择以下三种部署类型之一。

表 1-1. vCenter Server 和 Platform Services Controller 部署类型

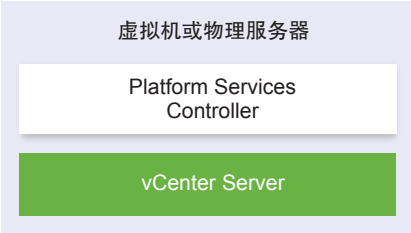
部署类型	描述
具有嵌入式 Platform Services Controller 部署的 vCenter Server	与 Platform Services Controller 捆绑在一起的所有服务与 vCenter Server 服务一起部署在同一虚拟机或物理服务器上。
Platform Services Controller	只有与 Platform Services Controller 捆绑在一起的服务会部署在虚拟机或物理服务器上。
具有外部 Platform Services Controller 的 vCenter Server（需要外部 Platform Services Controller）	只有 vCenter Server 服务会部署在虚拟机或物理服务器上。 必须向之前部署或安装的 Platform Services Controller 实例注册此类 vCenter Server 实例。

具有嵌入式 Platform Services Controller 部署的 vCenter Server

使用嵌入式 Platform Services Controller 会产生独立部署，它拥有自己的具有单一站点的 vCenter Single Sign-On 域。

从 vSphere 6.5 Update 2 开始，可以加入其他具有嵌入式 Platform Services Controller 的 vCenter Server 实例以启用增强型链接模式。

图 1-1. 具有嵌入式 Platform Services Controller 部署的 vCenter Server



安装具有嵌入式 Platform Services Controller 部署的 vCenter Server 具有以下优势：

- vCenter Server 与 Platform Services Controller 并非通过网络连接，且 vCenter Server 不容易出现因 vCenter Server 与 Platform Services Controller 之间的连接和名称解析问题导致的故障。
- 如果在 Windows 虚拟机或物理服务器上安装 vCenter Server，则需要较少的 Windows 许可证。
- 您管理较少的虚拟机或物理服务器。

可以在 vCenter High Availability 配置中配置具有嵌入式 Platform Services Controller 部署的 vCenter Server Appliance。有关信息，请参见《vSphere 可用性》。

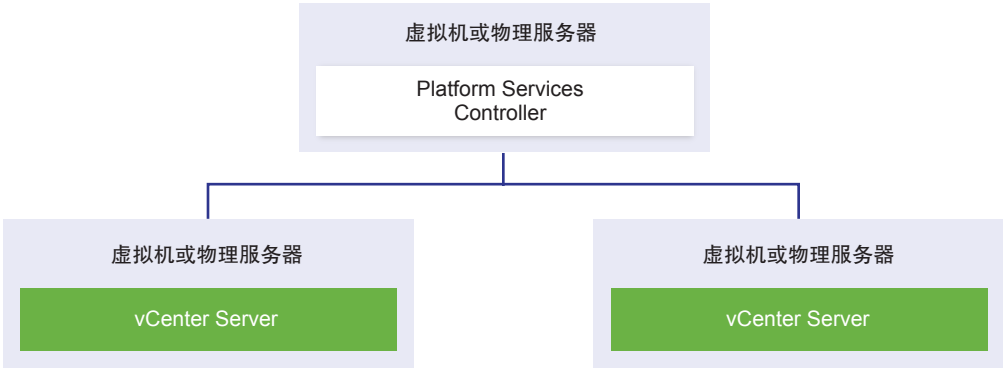
注 部署或安装具有嵌入式 Platform Services Controller 部署的 vCenter Server 后，您可以重新配置部署类型并切换到具有外部 Platform Services Controller 部署的 vCenter Server。

Platform Services Controller 与具有外部 Platform Services Controller 部署的 vCenter Server

部署或安装 Platform Services Controller 实例时，可以创建 vCenter Single Sign-On 域，或者加入现有的 vCenter Single Sign-On 域。加入的 Platform Services Controller 实例将复制其基础架构数据，如身份验证和许可信息，并且可以跨多个 vCenter Single Sign-On 站点。有关信息，请参见了解 vSphere 域、域名和站点。

可以向一个共同外部 Platform Services Controller 实例注册多个 vCenter Server 实例。vCenter Server 实例采用向其注册的 Platform Services Controller 实例的 vCenter Single Sign-On 站点。向一个共同或不同的已加入 Platform Services Controller 实例注册的所有 vCenter Server 实例都在增强型链接模式下进行连接。

图 1-2. 具有共同外部 Platform Services Controller 的两个 vCenter Server 示例



安装具有外部 Platform Services Controller 部署的 vCenter Server 具有以下缺点：

- vCenter Server 和 Platform Services Controller 之间的连接可能具有连接和名称解析问题。
- 如果在 Windows 虚拟机或物理服务器上安装 vCenter Server，则需要较多的 Microsoft Windows 许可证。
- 您需要管理较多虚拟机或物理服务器。

有关 Platform Services Controller 和 vCenter Server 最高配置的信息，请参见最高配置文档。

有关在 vCenter High Availability 配置中配置具有外部 Platform Services Controller 部署的 vCenter Server Appliance 的信息，请参见《《vSphere 可用性》》。

混合操作系统环境

安装在 Windows 上的 vCenter Server 实例可以注册到 Windows 上安装的 Platform Services Controller 中或 Platform Services Controller 设备中。vCenter Server Appliance 可以注册到 Windows 上安装的 Platform Services Controller 中或 Platform Services Controller 设备中。可以向同一 Platform Services Controller 注册 vCenter Server 和 vCenter Server Appliance。

图 1-3. 具有在 Windows 上运行的外部 Platform Services Controller 的混合操作系统环境的示例

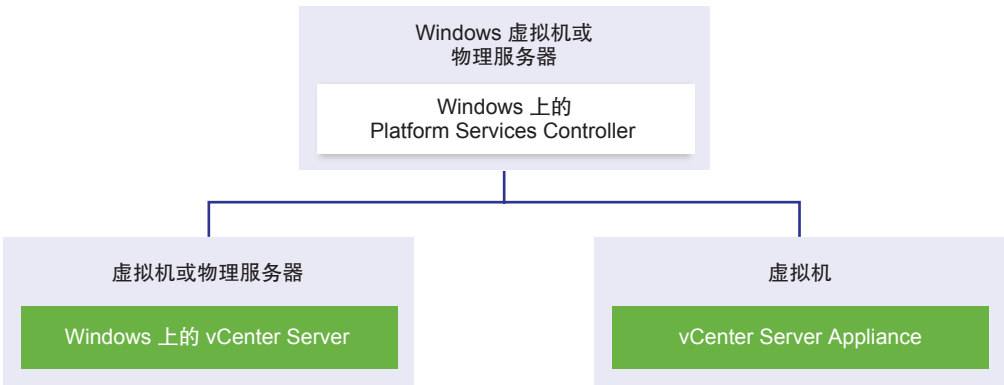
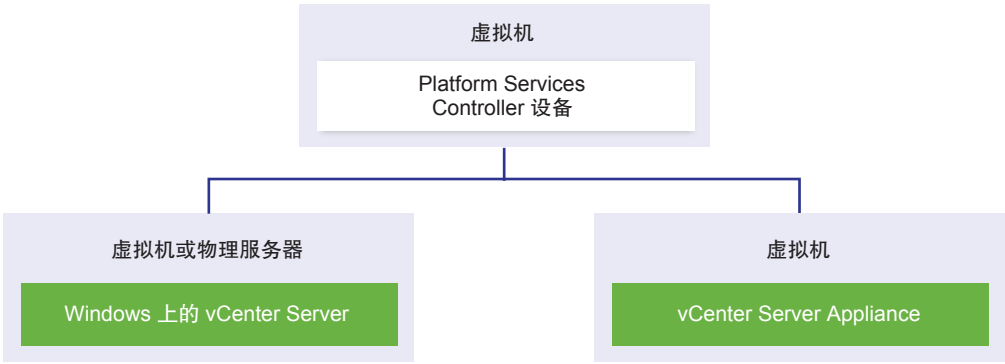


图 1-4. 具有外部 Platform Services Controller 设备的混合操作系统环境的示例



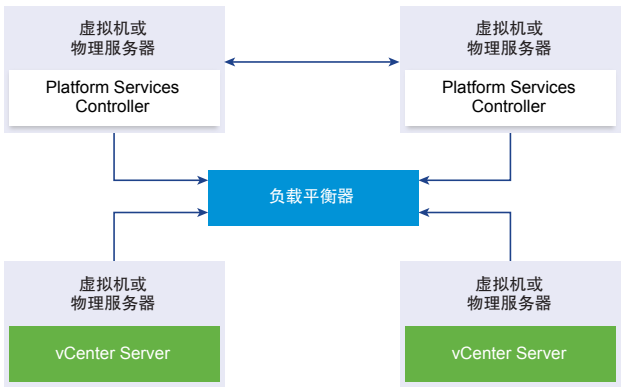
注 为确保易于管理和维护，请仅使用设备或者仅使用 vCenter Server 和 Platform Services Controller 的 Windows 安装。

具有外部 Platform Services Controller 实例和高可用性的部署拓扑

要确保外部部署中 Platform Services Controller 高可用性，您必须在 vCenter Single Sign-On 域中安装或部署至少两个已加入的 Platform Services Controller 实例。使用第三方负载平衡器时，您可以确保自动进行故障切换而不会出现停机。

具有负载平衡器的 Platform Services Controller

图 1-5. 实现了负载平衡的 Platform Services Controller 实例对的示例



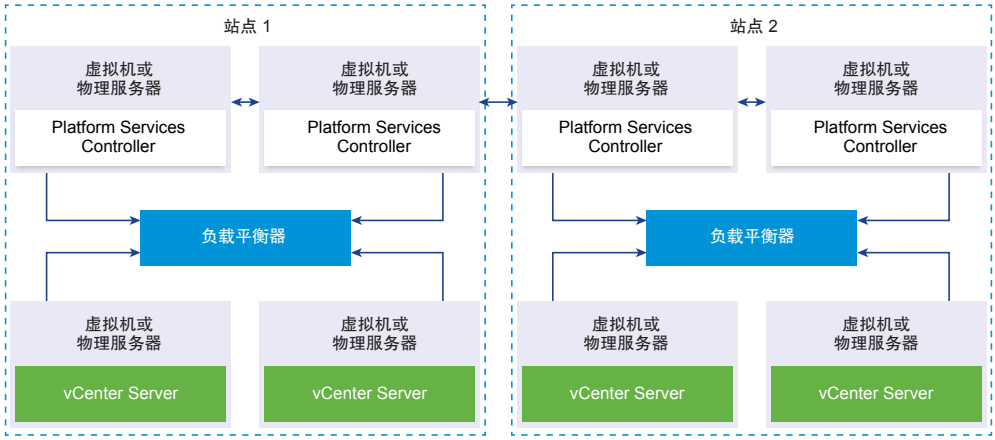
在您可以在每个站点中使用一个第三方负载平衡器来为此站点配置 Platform Services Controller 高可用性和自动故障切换。有关负载平衡器后的最大 Platform Services Controller 实例数的信息，请参见最高配置文档。

重要 要在负载平衡器后配置 Platform Services Controller 高可用性，Platform Services Controller 实例必须具有相同的操作系统类型。不支持在负载平衡器后运行混合操作系统 Platform Services Controller 实例。

vCenter Server 实例连接到负载平衡器。当一个 Platform Services Controller 实例停止响应时，负载平衡器自动在其他正常工作的 Platform Services Controller 实例之间分配负载，而不会出现停机。

跨 vCenter Single Sign-On 站点并具有负载平衡器的 Platform Services Controller

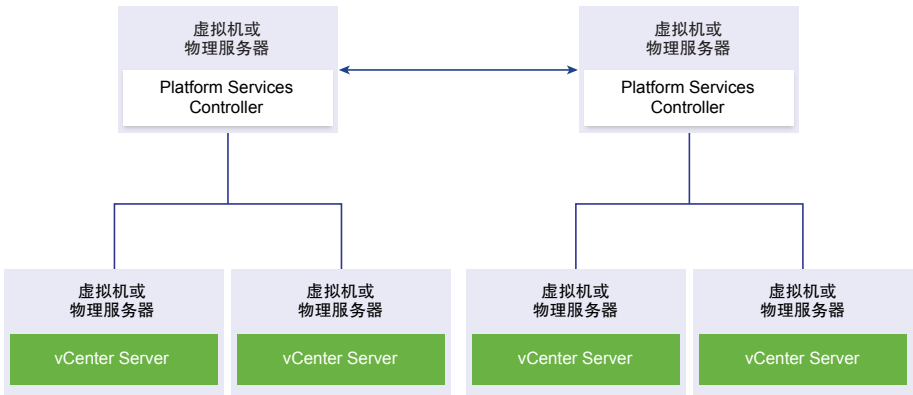
图 1-6. 跨两个站点并实现了负载平衡的两个 Platform Services Controller 实例对的示例



您的 vCenter Single Sign-on 域可能跨多个站点。要在整个域中实现 Platform Services Controller 高可用性和自动故障切换，您必须在每个站点中配置一个单独的负载平衡器。

无负载平衡器的 Platform Services Controller

图 1-7. 无负载平衡器的两个已加入 Platform Services Controller 实例的示例



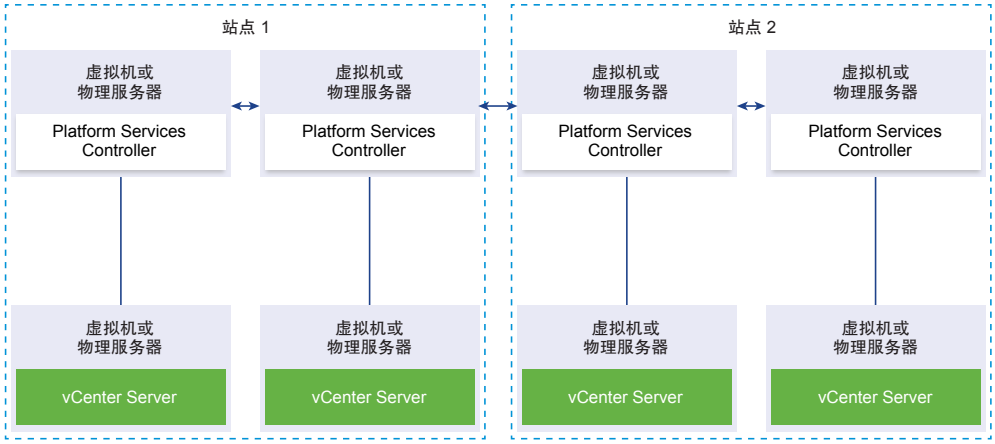
当您将两个或更多 Platform Services Controller 实例加入无负载平衡器的同一站点中时，您可以为此站点配置 Platform Services Controller 高可用性和手动故障切换。

当 Platform Services Controller 实例停止响应时，您必须手动故障切换在其中注册的 vCenter Server 实例。通过将实例重新指向同一站点内其他正常运行的 Platform Services Controller 实例来故障切换实例。有关如何使 vCenter Server 实例重新指向另一外部 Platform Services Controller 的信息，请参见《《vCenter Server 安装和设置》》。

注 如果您的 vCenter Single Sign-On 域包含三个或更多 Platform Services Controller 实例，您可以手动创建环形拓扑。其中一个实例发生故障时，环形拓扑可确保 Platform Services Controller 可靠性。要创建环形拓扑，请针对部署的第一个和最后一个 Platform Services Controller 实例运行 `/usr/lib/vmware-vmdir/bin/vdcrepadmin -f createagreement` 命令。

跨 vCenter Single Sign-On 站点并且不具有负载平衡器的 Platform Services Controller

图 1-8. 跨两个站点并且不具有负载平衡的两个已加入 Platform Services Controller 实例对的示例



您的 vCenter Single Sign-on 域可能跨多个站点。没有负载平衡器时，您可以手动将 vCenter Server 从出现故障的 Platform Services Controller 重新指向同一站点中正常工作的 Platform Services Controller。有关如何使 vCenter Server 实例重新指向另一外部 Platform Services Controller 的信息，请参见《《vCenter Server 安装和设置》》。

了解 vSphere 域、域名和站点

每个 Platform Services Controller 都与一个 vCenter Single Sign-On 域关联。域名默认为 vsphere.local，但可以在安装第一个 Platform Services Controller 时更改域名。域决定本地身份验证空间。您可以将一个域拆分为多个站点，并将每个 Platform Services Controller 和 vCenter Server 实例分配给一个站点。站点是逻辑构造，但通常对应于地理位置。

Platform Services Controller 域

安装 Platform Services Controller 时，系统会提示您创建 vCenter Single Sign-On 域或加入现有域。

域名由 VMware Directory Service (vmdir) 用于所有的轻量目录访问协议 (LDAP) 内部构造。

通过 vSphere 6.0 及更高版本，可以为 vSphere 域分配一个唯一名称。为防止身份验证冲突，请使用未被 OpenLDAP、Microsoft Active Directory 和其他目录服务使用的名称。

注 不能将域更改为某个 Platform Services Controller 或 vCenter Server 实例所属的域。

指定域名后，可以添加用户和组。通常，添加 Active Directory 或 LDAP 标识源并允许该标识源中的用户和组进行身份验证更有意义。也可以将 vCenter Server 或 Platform Services Controller 实例或其他 VMware 产品（例如，vRealize Operations）添加到该域。

Platform Services Controller 站点

可以将 Platform Services Controller 域组织为逻辑站点。VMware Directory Service 中的站点是逻辑容器，可用来对 vCenter Single Sign-On 域中的 Platform Services Controller 实例进行分组。

从 vSphere 6.5 开始，站点变得非常重要。在 Platform Services Controller 故障切换过程中，vCenter Server 实例被关联到相同站点中的其他 Platform Services Controller。为防止 vCenter Server 实例被关联到较远地理位置中的 Platform Services Controller，可以使用多个站点。

安装或升级 Platform Services Controller 时，系统会提示您输入站点名称。请参见《vCenter Server 安装和设置》文档。

Platform Services Controller 功能

Platform Services Controller 支持 vSphere 中的身份管理、证书管理和许可证管理等服务。

重要功能

Platform Services Controller 包括多项服务（如 Platform Services Controller 服务中所述），且具有以下重要功能。

- 通过 vCenter Single Sign-On 进行身份验证
- 默认使用 VMware Certificate Manager (VMCA) 证书置备 vCenter Server 组件和 ESXi 主机
- 使用自定义证书（存储在 VMware Endpoint Certificate Store (VECS) 中）

部署模型

可在 Windows 系统上安装 Platform Services Controller，或部署 Platform Services Controller 设备。

部署模型取决于正在使用的 Platform Services Controller 版本。请参见 vCenter Server 和 Platform Services Controller 部署类型。

从 vSphere 6.7 Update 1 开始，如果您部署或安装的 vCenter Server 实例采用外部 Platform Services Controller，您想将其转换为采用嵌入式 Platform Services Controller 的 vCenter Server 实例，您可以复制一个嵌入到现有 vCenter Server 实例中的新 Platform Services Controller。请参见《vCenter Server 安装和设置》文档。

从 vSphere 6.7 Update 1 开始，您可以将具有嵌入式 Platform Services Controller 部署的 vCenter Server 从一个 vSphere 域移至另一个 vSphere 域。诸如标记和许可等服务将保留并迁移到新的域。请参见《vCenter Server 安装和设置》文档。

管理 Platform Services Controller 服务

可以从 vSphere Client 或使用可用脚本和 CLI 之一来管理 Platform Services Controller 服务。

不同的 Platform Services Controller 服务支持不同的界面。

表 1-2. 用于管理 Platform Services Controller 服务的界面

接口	描述
vSphere Client	Web 界面（基于 HTML5 的客户端）。vSphere Client 用户界面术语、拓扑及工作流与 vSphere Web Client 用户界面的对应方面和元素高度一致。
vSphere Web Client	用于管理部分服务的 Web 界面。
证书管理实用程序	支持 CSR 生成和证书替换的命令行工具。请参见使用 vSphere 证书管理器实用程序管理证书。
用于管理 Platform Services Controller 服务的 CLI	用于管理证书、VMware Endpoint 证书存储 (VECS) 和 VMware Directory Service (vmdir) 的一组命令。请参见第 4 章，使用 CLI 命令管理服务和证书。

Platform Services Controller 服务

借助 Platform Services Controller，同一环境中的所有 VMware 产品均可共享身份验证域及其他服务。这些服务包括证书管理、身份验证及许可。

Platform Services Controller 包括以下核心基础架构服务。

表 1-3. Platform Services Controller 服务

服务	描述
`applmgmt` (VMware Appliance Management Service)	处理设备配置并为设备生命周期管理提供公用 API 端点。包含在 Platform Services Controller 设备上。
`vmware-cis-license` (VMware License Service)	每个 Platform Services Controller 都包含 VMware License Service，该服务可为环境中的 VMware 产品提供集中的许可证管理和报告功能。 License Service 清单将以 30 秒为间隔在域中的所有 Platform Services Controller 之间复制。
`vmware-cm` (VMware Component Manager)	Component Manager 可提供服务注册和查找功能。

表 1-3. Platform Services Controller 服务（续）

服务	描述
vmware-sts-idmd (VMware Identity Management Service) vmware-stsd (VMware Security Token Service)	vCenter Single Sign-On 功能支持的服务，这些服务可为 VMware 软件组件和用户提供安全的身份验证服务。 通过使用 vCenter Single Sign-On，VMware 组件可使用安全的 SAML 令牌交换机制进行通信。vCenter Single Sign-On 可构建一个内部安全域（默认为 vsphere.local），VMware 软件组件在安装或升级期间将在该域中进行注册。
vmware-rhttpproxy (VMware HTTP Reverse Proxy)	反向代理可在每个 Platform Services Controller 节点和每个 vCenter Server 系统上运行。它是节点的单一入口点，可使节点上运行的各项服务安全地进行通信。
vmware-sca (VMware Service Control Agent)	管理服务配置。可使用 service-control CLI 来管理各个服务配置。
vmware-statsmonitor （VMware 设备监控服务）	监控 vCenter Server Appliance 客户机操作系统资源消耗。
vmware-vapi-endpoint (VMware vAPI Endpoint)	vSphere Automation API 端点可提供对 vAPI 服务的单点访问。可以从 vSphere Client 更改 vAPI Endpoint 服务的属性。有关 vAPI 端点的详细信息，请参见《vSphere Automation SDK 编程指南》。
vmafdd VMware Authentication Framework	该服务可为 vmdir 身份验证提供客户端框架，并为 VMware Endpoint 证书存储 (VMware Endpoint Certificate Store, VECS) 提供服务。
vmcad VMware Certificate Service	可使用以 VMCA 作为根证书颁发机构的签名证书置备每个具有 vmafd 客户端库的 VMware 软件组件及每个 ESXi 主机。可以使用证书管理器实用程序更改默认证书。 VMware Certificate Service 使用 VMware Endpoint 证书存储 (VECS) 来充当每个 Platform Services Controller 实例上证书的本地存储库。尽管您可以决定不使用 VMCA 而改用自定义证书，但是必须将这些证书添加到 VECS。
vmdird VMware Directory Service	提供多租户、多重管理 LDAP 目录服务，该服务用于存储身份验证、证书、查找和许可证信息。不要使用 LDAP 浏览器更新 vmdird 中的数据。 如果您的域包含多个 Platform Services Controller 实例，则一个 vmdir 实例中的 vmdir 内容更新会传播到所有其他 vmdir 实例。
vmdnsd VMware 域名服务	未在 vSphere 6.x 中使用。
vmonapi VMware Lifecycle Manager API vmware-vmon VMware Service Lifecycle Manager	启动和停止 vCenter Server 服务以及监控服务 API 运行状况。vmware-vmon 服务是独立于平台的集中式服务，用于管理 Platform Services Controller 和 vCenter Server 的生命周期。向第三方应用程序公开 API 和 CLI。
lwsmd Likewise Service Manager	Likewise 有助于将主机加入 Active Directory 域以及后续的用户身份验证。

表 1-3. Platform Services Controller 服务 （续）

服务	描述
pschealth VMware Platform Services Controller 运行状况监控	监控所有核心 Platform Services Controller 基础架构服务的运行状况和状态。
vmware-analytics VMware Analytics Service	包括从各种 vSphere 组件收集并上载到 VMware 分析云中的遥测数据，以及管理客户体验提升计划 (CEIP) 的组件。

从 vSphere Client 管理 Platform Services Controller 服务

可以从 vSphere Client 管理 vCenter 访问控制、许可、解决方案、链接的域、证书和 Single Sign-On。

步骤

1 在本地 vCenter Single Sign-On 域（默认为 vsphere.local）中，以拥有管理员特权的用户身份登录到与 Platform Services Controller 关联的 vCenter Server。

2 选择**系统管理**，然后单击要管理的项。

从 vSphere Web Client 管理 Platform Services Controller 服务

您可以从 vSphere Web Client 管理 vCenter Single Sign-On 和许可服务。

使用 vSphere Client 或 CLI 而非 vSphere Web Client 管理以下服务。

- 证书
- VMware Endpoint Certificate Store (VECS)
- 双因素身份验证，例如通用访问卡身份验证
- 登录横幅

步骤

1 在本地 vCenter Single Sign-On 域（默认为 vsphere.local）中，以拥有管理员特权的用户身份登录到与 Platform Services Controller 关联的 vCenter Server。

2 选择**系统管理**，然后单击要管理的项。

选项	描述
Single Sign-On	配置 vCenter Single Sign-On。 ■ 设置策略。 ■ 管理标识源。 ■ 管理 STS 签名证书。 ■ 管理 SAML 服务提供商。 ■ 管理用户和组。
许可	配置许可。

使用脚本管理 Platform Services Controller 服务

Platform Services Controller 包括用于生成 CSR、管理证书和管理服务的脚本。

例如，在具有嵌入式 Platform Services Controller 部署和具有外部 Platform Services Controller 部署的情况下，均可使用 `certool` 实用程序生成 CSR 和替换证书。请参见使用 vSphere 证书管理器实用程序管理证书。

使用 CLI 执行 Web 界面不支持的管理任务，或者为环境创建自定义脚本。

表 1-4. 用于管理证书和关联服务的 CLI

CLI	描述	链接
`certool`	生成并管理证书和密钥。属于 VMCA。	certool 初始化命令参考
`vecs-cli`	管理 VMware 证书存储实例的内容。属于 VMAFD。	vecs-cli 命令参考
`dir-cli`	在 VMware Directory Service 中创建并更新证书。属于 VMAFD。	dir-cli 命令参考
`sso-config`	用于配置智能卡身份验证的实用程序。	了解 vCenter Server 双因素身份验证
`service-control`	用于启动、停止和列出服务的命令。	在运行其他 CLI 命令之前，运行此命令以停止服务。

步骤

1 登录 Platform Services Controller shell。

大多数情况下，您必须是 root 或管理员用户。有关详细信息，请参见运行 CLI 所需的特权。

2 在以下默认位置之一访问 CLI。

所需特权取决于要执行的任务。在某些情况下，为了保护敏感信息，系统会提示您输入密码两次。

Windows

```
C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe
C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli.exe
C:\Program Files\VMware\vCenter Server\vmcad\certool.exe
C:\Program Files\VMware\VCenter server\VMware Identity Services\sso-config
VCENTER_INSTALL_PATH\bin\service-control
```

Linux

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin
```

在 Linux 上，`service-control` 命令不要求您指定路径。

管理 Platform Services Controller 设备

您可以从虚拟设备管理界面或设备 shell 管理 Platform Services Controller 设备。

如果使用具有嵌入式 Platform Services Controller 部署的环境，则管理一个包含 Platform Services Controller 和 vCenter Server 的设备。请参见《vCenter Server Appliance 配置》。

表 1-5. 用于管理 Platform Services Controller 设备的界面

界面	描述
Platform Services Controller 虚拟设备管理界面 (VAMI)	使用该界面可以重新配置 Platform Services Controller 部署的系统设置。
Platform Services Controller 设备 shell	使用此命令行界面可以在 VMCA、VECS 和 VMDIR 上执行服务管理操作。请参见使用 vSphere 证书管理器实用程序管理证书和第 4 章，使用 CLI 命令管理服务和证书。

使用 Platform Services Controller 虚拟设备管理界面管理设备

在具有外部 Platform Services Controller 部署的环境中，可以使用 Platform Services Controller 虚拟设备管理界面 (VAMI) 配置设备系统设置。这些设置包括时间同步、网络设置以及 SSH 登录设置。您也可以更改 root 密码，将设备加入 Active Directory 域，以及退出 Active Directory 域。

在具有嵌入式 Platform Services Controller 部署的环境中，可以管理包括 Platform Services Controller 和 vCenter Server 在内的设备。

步骤

1 在 Web 浏览器中，转至 Web 界面，网址为 https://*platform_services_controller_ip*:5480。

2 如果显示有关 SSL 证书不可信的警告消息，请根据公司安全策略以及正在使用的 Web 浏览器解决此问题。

3 以 root 用户身份登录。

默认 root 密码是部署虚拟设备时设置的虚拟设备 root 密码。

登录后可以看到 Platform Services Controller 设备管理界面的“系统信息”页面。

从设备 Shell 管理设备

可以从设备 Shell 使用服务管理实用程序和 CLI。可以使用 TTY1 登录控制台，或者使用 SSH 连接到 Shell。

步骤

1 如果需要，请启用 SSH 登录。

a 登录到设备管理界面 (VAMI)，网址为 https://*platform_services_controller_ip*:5480。

b 在导航器中，选择**访问**，然后单击**编辑**。

c 切换到**启用 SSH 登录**，然后单击**确定**。

按照同样的步骤也可启用设备的 Bash Shell。

2 访问设备 shell。

- 如果可以直接访问设备控制台，请选择**登录**，然后按 Enter。
- 要远程连接，请使用 SSH 或其他远程控制台连接启动与设备的会话。

3 以 root 用户身份及最初部署设备时设置的密码登录。

如果已更改 root 密码，请使用新密码。

将 Platform Services Controller 设备添加到 Active Directory 域

如果要将 Active Directory 标识源添加到 Platform Services Controller，必须将 Platform Services Controller 设备加入 Active Directory 域。

如果使用的是安装在 Windows 上的 Platform Services Controller 实例，可以使用该计算机所属的域。

步骤

1 使用 vSphere Client 以本地 vCenter Single Sign-On 域（默认为 vsphere.local）中具有管理员特权的用户身份登录到与 Platform Services Controller 关联的 vCenter Server。

2 选择**管理**。

3 展开**单点登录**，然后单击**配置**。

4 单击 **Active Directory 域**。

5 单击**加入 AD**，指定域、可选的组织单位以及用户名和密码，然后单击**加入**。

后续步骤

要附加已加入的 Active Directory 域中的用户和组，请将已加入的域添加为 vCenter Single Sign-On 标识源。请参见添加或编辑 vCenter Single Sign-On 标识源。

使用 vCenter Single Sign-On 进行 vSphere 身份验证 2

vCenter Single Sign-On 是一个身份验证代理程序和安全令牌交换基础架构。当用户可以向 vCenter Single Sign-On 进行身份验证时，该用户将收到 SAML 令牌。从今往后，用户可以使用 SAML 令牌向 vCenter 服务进行身份验证。然后，该用户可以执行其权限范围内的操作。

由于所有通信的流量都会进行加密，且只有经过身份验证的用户才能执行其权限范围内的操作，因此您的环境是安全的。

从 vSphere 6.0 开始，vCenter Single Sign-On 是 Platform Services Controller 的一部分。Platform Services Controller 包含支持 vCenter Server 和 vCenter Server 组件的共享服务。这些服务包括 vCenter Single Sign-On、VMware Certificate Authority 和 License Service。有关 Platform Services Controller 的详细信息，请参见《《vCenter Server 安装和设置》》。

对于初始握手，用户使用用户名和密码进行身份验证，而解决方案用户使用证书进行身份验证。有关替换解决方案用户证书的信息，请参见 第 3 章，vSphere 安全证书。

下一步是授权能够进行身份验证的用户执行某些任务。在大多数情况下，通常可以通过将用户分配给具有角色的组来分配 vCenter Server 特权。vSphere 还包括其他权限模型，例如全局权限。请参见《vSphere 安全性》文档。

本章讨论了以下主题：

- 了解 vCenter Single Sign-On
- 配置 vCenter Single Sign-On 标识源
- 了解 vCenter Server 双因素身份验证
- 将 vCenter Single Sign-On 用作其他服务提供程序的身份提供程序
- 安全令牌服务 (STS)
- 管理 vCenter Single Sign-On 策略
- 管理 vCenter Single Sign-On 用户和组
- vCenter Single Sign-On 安全性最佳做法

了解 vCenter Single Sign-On

为有效管理 vCenter Single Sign-On，您需要了解基础架构以及该架构如何影响安装和升级。

vCenter Single Sign-On 6.0 域和站点
(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_sso_6_domains_sites)

如何使用 vCenter Single Sign-On 保护您的环境

vCenter Single Sign-On 允许 vSphere 组件通过安全的令牌机制相互通信。

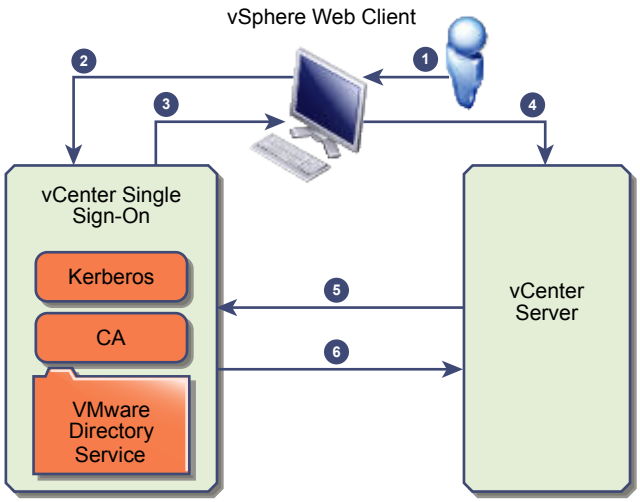
vCenter Single Sign-On 使用以下服务。

- STS (Security Token Service)。
- 用于确保安全流量的 SSL。
- 通过 Active Directory 或 OpenLDAP 对人工用户进行身份验证。
- 通过证书对解决方案用户进行身份验证。

人工用户的 vCenter Single Sign-On 握手

下图显示了人工用户的握手。

图 2-1. 人工用户的 vCenter Single Sign-On 握手



1 用户使用用户名和密码登录 vSphere Client 以访问 vCenter Server 系统或其他 vCenter 服务。

用户还可以不使用密码而选中**使用 Windows 会话身份验证**复选框进行登录。

2 vSphere Client 将登录信息传递到 vCenter Single Sign-On 服务，该服务将检查 vSphere Client 的 SAML 令牌。如果 vSphere Client 具有有效令牌，vCenter Single Sign-On 随后会检查用户是否位于已配置的标识源中（例如，Active Directory）。

- 如果仅使用用户名，则 vCenter Single Sign-On 将在默认域中执行检查。
- 如果域名随用户名一起提供（*DOMAIN*\user1 或 user1@*DOMAIN*），则 vCenter Single Sign-On 将检查该域。

3 如果用户可以对此标识源进行身份验证，则 vCenter Single Sign-On 会返回表示 vSphere Client 的用户的令牌。

4 vSphere Client 将令牌传递到 vCenter Server 系统。

5 vCenter Server 与 vCenter Single Sign-On 服务器确认令牌是否有效且未过期。

6 vCenter Single Sign-On 服务器将令牌返回到 vCenter Server 系统，从而使用 vCenter Server 授权框架以允许用户访问。

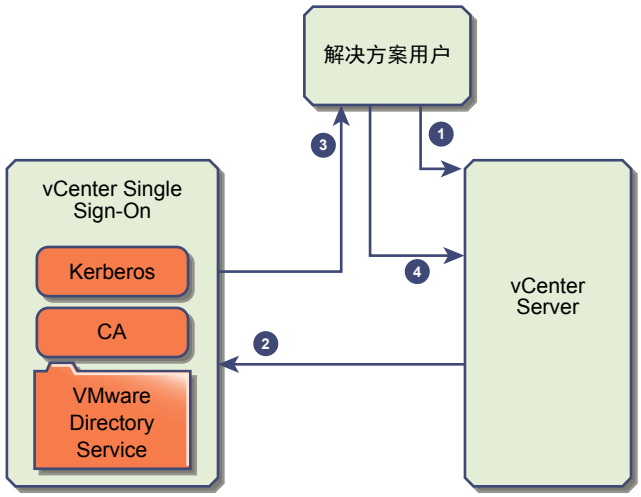
用户现在可以进行身份验证，并可以查看和修改用户角色具有特权的任何对象。

注 首先，每个用户都分配有“无权访问”角色。vCenter Server 管理员必须至少为用户分配“只读”角色，用户才能登录。请参见《vSphere 安全性》文档。

解决方案用户的 vCenter Single Sign-On 握手

解决方案用户是 vCenter Server 基础架构中使用的一组服务，例如 vCenter Server 或 vCenter Server 扩展。VMware 扩展及潜在的第三方扩展也可能对 vCenter Single Sign-On 进行身份验证。

图 2-2. 解决方案用户的 vCenter Single Sign-On 握手



对于解决方案用户，交互将以如下方式继续进行：

1 解决方案用户尝试连接到 vCenter 服务。

2 解决方案用户被重定向到 vCenter Single Sign-On。如果解决方案用户是 vCenter Single Sign-On 的新用户，则必须提供有效的证书。

3 如果证书有效，vCenter Single Sign-On 将向解决方案用户分配 SAML 令牌（持有者令牌）。令牌由 vCenter Single Sign-On 签名。

4 然后，解决方案用户被重定向到 vCenter Single Sign-On，并可以基于其权限执行任务。

5 下次解决方案用户必须进行身份验证时，可以使用 SAML 令牌登录到 vCenter Server。

默认情况下，此握手将自动执行，因为 VMCA 会在启动期间为解决方案用户置备证书。如果公司策略要求使用第三方 CA 签名证书，则可以将解决方案用户证书替换为第三方 CA 签名的证书。如果这些证书有效，vCenter Single Sign-On 将向解决方案用户分配 SAML 令牌。请参见在 vSphere 中使用自定义证书。

支持的加密

支持 AES 加密，即最高级别的加密。支持的加密会在 vCenter Single Sign-On 使用 Active Directory 作为标识源时影响安全性。

它还会在 ESXi 主机或 vCenter Server 加入 Active Directory 时影响安全性。

vCenter Single Sign-On 组件

vCenter Single Sign-On 包括安全令牌服务 (STS)、管理服务器和 vCenter Lookup Service 以及 VMware Directory Service (vmdir)。VMware Directory Service 还可用于证书管理。

在安装期间，组件将作为嵌入式部署的一部分或作为 Platform Services Controller 的一部分进行部署。

STS (Security Token Service)	STS 服务会发出安全断言标记语言 (SAML) 令牌。这些安全令牌表示 vCenter Single Sign-On 支持的标识源类型之一中的用户标识。SAML 令牌允许成功通过 vCenter Single Sign-On 身份验证的人工用户和解决方案用户使用 vCenter Single Sign-On 支持的所有 vCenter，而无需再次经过每个服务的身份验证。 vCenter Single Sign-On 服务会使用签名证书对所有令牌进行签名，并在磁盘上存储令牌签名证书。该服务本身的证书也会存储在磁盘上。
管理服务器	管理服务器允许用户具有 vCenter Single Sign-On 的管理员特权，以便配置 vCenter Single Sign-On 服务器并管理 vSphere Web Client 中的用户和组。最初，仅 administrator@*your_domain_name* 用户具有这些特权。在 vSphere 5.5 中，该用户为 administrator@vsphere.local。在 vSphere 6.0 中，使用新的 Platform Services Controller 安装 vCenter Server 或部署 vCenter Server Appliance 时，可以更改 vSphere 域。请勿使用 Microsoft Active Directory 或 OpenLDAP 域名命名该域名。
VMware Directory Service (vmdir)	VMware Directory Service (vmdir) 与安装期间您指定的域相关联，并且包含在每个嵌入式部署和每个 Platform Services Controller 中。该服务是在端口 389 上提供 LDAP 目录的多租户、多重管理目录服务。该服务仍使用端口 11711 实现与 vSphere 5.5 和更早版本系统的向后兼容性。 如果您的环境包含多个 Platform Services Controller 实例，则一个 vmdir 实例中的 vmdir 内容更新会传播到所有其他 vmdir 实例。 自 vSphere 6.0 起，VMware Directory Service 不仅会存储 vCenter Single Sign-On 信息，而且还会存储证书信息。
Identity Management Service	处理标识源和 STS 身份验证请求。

vCenter Single Sign-On 如何影响安装

从版本 5.1 开始，vSphere 包括作为 vCenter Server 管理基础架构一部分的 vCenter Single Sign-On 服务。此变更影响 vCenter Server 安装。

使用 vCenter Single Sign-On 进行身份验证会使 vSphere 更加安全，因为 vSphere 软件组件使用安全的令牌交换机制彼此进行通信，且所有其他用户也可以使用 vCenter Single Sign-On 进行身份验证。

从 vSphere 6.0 开始，vCenter Single Sign-On 包括在嵌入式部署中或是 Platform Services Controller 的一部分。Platform Services Controller 包含 vSphere 组件之间进行通信所需的全部服务，其中包括 vCenter Single Sign-On、VMware Certificate Authority、VMware Lookup Service 以及许可服务。

安装顺序非常重要。

首次安装	如果安装为分布式，则必须先安装 Platform Services Controller，然后再安装 vCenter Server 或部署 vCenter Server Appliance。对于嵌入式部署，将自动执行正确的安装顺序。
后续安装	如果最多大约四个 vCenter Server 实例，一个 Platform Services Controller 可以为整个 vSphere 环境提供服务。您可以将新的 vCenter Server 实例连接到同一个 Platform Services Controller。如果超过大约四个 vCenter Server 实例，您可以安装额外的 Platform Services Controller 以获得更佳的性能。每个 Platform Services Controller 上的 vCenter Single Sign-On 服务会与所有其他实例同步身份验证数据。准确数量取决于 vCenter Server 实例的使用程度以及其他因素。

有关部署模型、每种部署类型的优势和缺点的详细信息，请参见《vCenter Server 安装和设置》。

通过 vSphere 使用 vCenter Single Sign-On

当用户登录 vSphere 组件或 vCenter Server 解决方案用户访问另一个 vCenter Server 服务时，vCenter Single Sign-On 会执行身份验证。用户必须通过 vCenter Single Sign-On 进行身份验证，且应具有所需权限才能与 vSphere 对象进行交互。

vCenter Single Sign-On 会同时对解决方案用户和其他用户进行身份验证。

- 解决方案用户表示 vSphere 环境中的一组服务。在安装期间，默认情况下，VMCA 会向每个解决方案用户分配一个证书。解决方案用户使用该证书对 vCenter Single Sign-On 进行身份验证。vCenter Single Sign-On 会向解决方案用户提供一个 SAML 令牌，然后，该解决方案用户可以与环境中的其他服务进行交互。
- 其他用户登录到环境时（例如，从 vSphere Client 登录），vCenter Single Sign-On 会提示您输入用户名和密码。如果 vCenter Single Sign-On 在相应的标识源中找到具有这些凭据的用户，则会向该用户分配 SAML 令牌。现在，用户可以访问环境中的其他服务，而无需提示再次进行身份验证。

  用户可以查看哪些对象以及用户能够执行哪些操作通常由 vCenter Server 权限设置决定。vCenter Server 管理员可以从 vSphere Web Client 或 vSphere Client 中的权限界面分配这些权限，而不是通过 vCenter Single Sign-On 进行分配。请参见《vSphere 安全性》文档。

vCenter Single Sign-On 和 vCenter Server 用户

用户可通过在登录页面上输入凭据向 vCenter Single Sign-On 进行身份验证。连接到 vCenter Server 后，通过身份验证的用户可以查看所有 vCenter Server 实例或向其角色提供权限的其他 vSphere 对象。无需进一步进行身份验证。

安装后，vCenter Single Sign-On 域的管理员（默认为 administrator@vsphere.local）对 vCenter Single Sign-On 和 vCenter Server 具有管理员访问权限。然后，该用户可以添加标识源、设置默认标识源，以及管理 vCenter Single Sign-On 域中的用户和组。

可对 vCenter Single Sign-On 进行身份验证的所有用户均可重置其密码，即使这些密码已过期也是如此，只要用户知道密码。请参见更改 vCenter Single Sign-On 密码。只有 vCenter Single Sign-On 管理员可以为不再具有其密码的用户重置密码。

注　通过 vSphere Client 更改 SDDC 的密码时，新密码不会与“默认 vCenter 凭据”页面上显示的密码同步。该页面仅显示默认凭据。如果更改了凭据，您自己应负责记好新密码。请联系技术支持以请求更改密码。

vCenter Single Sign-On 管理员用户

可从 vSphere Client 或 vSphere Web Client 访问 vCenter Single Sign-On 管理界面。

要配置 vCenter Single Sign-On 并管理 vCenter Single Sign-On 用户和组，用户 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组中的用户必须登录到 vSphere Client。根据身份验证，该用户可以通过 vSphere Client 访问 vCenter Single Sign-On 管理界面，并管理标识源和默认域、指定密码策略以及执行其他管理任务。

注　如果在安装过程中指定了其他域，则不能重命名 vCenter Single Sign-On 管理员用户，它默认为 administrator@vsphere.local 或 administrator@*mydomain*。为提高安全性，请考虑在 vCenter Single Sign-On 域中创建其他命名的用户，并为其分配管理特权。然后，可以使用管理员帐户停止。

ESXi 用户

独立 ESXi 主机未与 vCenter Single Sign-On 或 Platform Services Controller 集成。请参见《vSphere 安全性》，了解有关将 ESXi 主机添加到 Active Directory 的信息。

如果使用 VMware Host Client、vCLI 或 PowerCLI 为受管 ESXi 主机创建本地 ESXi 用户，vCenter Server 不会识别这些用户。因此，创建本地用户会造成混淆，尤其是如果使用相同的用户名。如果可以对 vCenter Single Sign-On 进行身份验证的用户对 ESXi 主机对象拥有对应的权限，他们则可以查看和管理 ESXi 主机。

注　通过 vCenter Server 管理 ESXi 主机的权限（如果可能）。

如何登录到 vCenter Server 组件

可以通过连接到 vSphere Client 或 vSphere Web Client 登录。

用户从 vSphere Client 登录到 vCenter Server 系统时，登录行为取决于用户是否位于设置为默认标识源的域中。

- 默认域中的用户可使用其自身的用户名和密码进行登录。
- 如果用户位于已添加到 vCenter Single Sign-On 作为标识源的域而并非默认域中，则可以登录到 vCenter Server，但必须按照以下方式之一指定域。
  - 包含域名前缀，例如 MYDOMAIN\user1
  - 包含域，例如 user1@mydomain.com

- 如果用户位于不是 vCenter Single Sign-On 标识源的域中，则无法登录到 vCenter Server。如果添加到 vCenter Single Sign-On 的域是域层次结构的一部分，则 Active Directory 将确定层次结构中其他域的用户是否进行了身份验证。

如果环境中包括 Active Directory 层次结构，请参见 VMware 知识库文章 2064250 获取受支持和不支持的设置的详细信息。

注 从 vSphere 6.0 Update 2 开始，支持双因素身份验证。请参见了解 vCenter Server 双因素身份验证。

vCenter Single Sign-On 域中的组

vCenter Single Sign-On 域（默认为 vsphere.local）包含多个预定义组。如果将用户添加到其中一个组，则可以执行相应的操作。

请参见管理 vCenter Single Sign-On 用户和组。

对于 vCenter Server 层次结构中的所有对象，您可以通过将用户和角色与对象进行配对来分配权限。例如，您可以选择一个资源池，并通过向一组用户授予相应的角色，为这组用户分配对该资源池对象的读取特权。

对于某些并非由 vCenter Server 直接管理的服务，一个 vCenter Single Sign-On 组中的成员资格决定特权。例如，属于管理员组成员的用户可以管理 vCenter Single Sign-On。属于 CAAdmins 组成员的用户可以管理 VMware Certificate Authority，而属于 LicenseService.Administrators 组的用户可以管理许可证。

vsphere.local 中预定义了以下组。

注 其中许多组是 vsphere.local 的内部组或可向用户提供高级别管理特权。只有在仔细考虑相关风险后，才能将用户添加到以下任意组。

注 请勿删除 vsphere.local 域中的任何预定义组。否则，可能会导致身份验证错误或证书置备错误。

表 2-1. vsphere.local 域中的组

特权	描述
用户	vCenter Single Sign-On 域（默认为 vsphere.local）中的用户。
SolutionUsers	解决方案用户组 vCenter 服务。每个解决方案用户将使用证书单独向 vCenter Single Sign-On 进行身份验证。默认情况下，VMCA 将为解决方案用户置备证书。不要向该组明确添加成员。
CAAdmins	CAAdmins 组的成员拥有 VMCA 的管理员特权。不要向该组添加成员，除非您有充分的理由。
DCAdmins	DCAdmins 组的成员可以对 VMware Directory Service 执行域控制器管理员操作。 注 不要直接管理域控制器。请改用 `vmdir` CLI 或 vSphere Client 执行相应的任务。
SystemConfiguration.BashShellAdministrators	此组仅适用于 vCenter Server Appliance 部署。 此组中的用户可以启用和禁用对 BASH shell 的访问。默认情况下，使用 SSH 连接到 vCenter Server Appliance 的用户只能访问受限 shell 中的命令。此组中的用户可以访问 BASH shell。
ActAsUsers	Act-As Users 的成员可以从 vCenter Single Sign-On 获取 Act-As 令牌。
ExternalIPDUsers	vSphere 未使用此内部组。VMware vCloud Air 需要此组。

表 2-1. vsphere.local 域中的组 （续）

特权	描述
SystemConfiguration.Administrators	SystemConfiguration.Administrators 组的成员可以在 vSphere Client 中查看和管理系统配置。这些用户可以查看、启动和重新启动服务、对服务进行故障排除、查看可用节点以及管理这些节点。
DCClients	此组在内部使用，以便允许管理节点访问 VMware Directory Service 中的数据。 注 不要修改此组。任何更改都可能会影响证书基础架构。
ComponentManager.Administrators	ComponentManager.Administrators 组的成员可以调用组件管理器 API 以注册或取消注册服务，即修改服务。对服务进行读取访问不需要此组中的成员资格。
LicenseService.Administrators	LicenseService.Administrators 的成员对所有与许可相关的数据具有完全的写入访问权限，且可以为已在许可服务中注册的所有产品资产添加、移除、分配和取消分配序列密钥。
管理员	VMware Directory Service (vmdir) 的管理员。此组的成员可以执行 vCenter Single Sign-On 管理任务。不要向该组添加成员，除非您有充分的理由并了解后果。

配置 vCenter Single Sign-On 标识源

用户仅使用用户名登录时，vCenter Single Sign-On 会在默认标识源中检查该用户是否可以进行身份验证。当用户登录并在登录屏幕中提供域名时，vCenter Single Sign-On 会检查指定的域，确认该域是否已添加为标识源。可以添加标识源、移除标识源和更改默认值。

可从 vSphere Client 配置 vCenter Single Sign-On。要配置 vCenter Single Sign-On，您必须拥有 vCenter Single Sign-On 管理员特权。vCenter Single Sign-On 管理员特权不同于 vCenter Server 或 ESXi 上的管理员角色。在新安装中，仅 vCenter Single Sign-On 管理员（默认为 administrator@vsphere.local）可以对 vCenter Single Sign-On 进行身份验证。

- vCenter Server 和 vCenter Single Sign-On 的标识源

  可以使用标识源将一个或多个域附加到 vCenter Single Sign-On。域是用户和组的存储库，可以由 vCenter Single Sign-On 服务器用于用户身份验证。

- 设置 vCenter Single Sign-On 的默认域

  每个 vCenter Single Sign-On 标识源都与某个域相关联。vCenter Single Sign-On 使用默认域验证未使用域名登录的用户的身份。如果用户所属的域不是默认域，则用户在登录时必须包含域名。

- 添加或编辑 vCenter Single Sign-On 标识源

  仅当用户所在域已添加为 vCenter Single Sign-On 标识源时，用户才能登录到 vCenter Server。vCenter Single Sign-On 管理员用户可以添加标识源，或者更改已添加的标识源的设置。

- 将 vCenter Single Sign-On 与 Windows 会话身份验证结合使用

  您可以在 vCenter Single Sign-On 中使用 Windows 会话身份验证 (SSPI)。必须先将 Platform Services Controller 加入 Active Directory 域，然后才能使用 SSPI。

vCenter Server 和 vCenter Single Sign-On 的标识源

可以使用标识源将一个或多个域附加到 vCenter Single Sign-On。域是用户和组的存储库，可以由 vCenter Single Sign-On 服务器用于用户身份验证。

管理员可以添加标识源、设置默认标识源，以及在 vsphere.local 标识源中创建用户和组。

用户和组数据存储在 Active Directory 中、OpenLDAP 中或者存储到本地安装了 vCenter Single Sign-On 的计算机操作系统。在安装后，vCenter Single Sign-On 的每个实例都有标识源 *your_domain_name*，例如，vsphere.local。此标识源在 vCenter Single Sign-On 内部。

vCenter Server 5.1 版之前的版本支持将 Active Directory 和本地操作系统用户作为用户存储库。因此，本地操作系统用户始终能够对 vCenter Server 系统进行身份验证。vCenter Server 版本 5.1 和 5.5 使用 vCenter Single Sign-On 进行身份验证。有关 vCenter Single Sign-On 5.1 支持的标识源的列表，请参见 vSphere 5.1 文档。vCenter Single Sign-On 5.5 支持将以下类型的用户存储库用作标识源，但仅支持一个默认标识源。

- Active Directory 2003 版及更高版本。在 vSphere Client 中显示为 **Active Directory (集成 Windows 身份验证)**。vCenter Single Sign-On 允许您将单个 Active Directory 域指定为标识源。该域可包含子域或作为林的根域。VMware 知识库文章 2064250 讨论了 vCenter Single Sign-On 支持的 Microsoft Active Directory 信任。
- Active Directory over LDAP。vCenter Single Sign-On 支持多个 Active Directory over LDAP 标识源。包括此标识源类型是为了与 vSphere 5.1 附带的 vCenter Single Sign-On 服务兼容。在 vSphere Client 中显示为 **Active Directory 作为 LDAP 服务器**。
- OpenLDAP 版本 2.4 及更高版本。vCenter Single Sign-On 支持多个 OpenLDAP 标识源。在 vSphere Client 中显示为 **OpenLDAP**。
- 本地操作系统用户。本地操作系统用户是运行 vCenter Single Sign-On 服务器的操作系统的本地用户。本地操作系统标识源仅在基本 vCenter Single Sign-On 服务器部署中存在，并在具有多个 vCenter Single Sign-On 实例的部署中不可用。仅允许一个本地操作系统标识源。在 vSphere Client 中显示为 **localos**。

  注 如果 Platform Services Controller 与 vCenter Server 系统位于不同的计算机上，请勿使用本地操作系统用户。在嵌入式部署中也许可以使用本地操作系统用户，但并不建议这样做。

- vCenter Single Sign-On 系统用户。每次安装 vCenter Single Sign-On 时都会创建一个系统标识源。

注 无论何时都只存在一个默认域。来自非默认域的用户在登录时必须添加域名（*域\用户*）才能成功进行身份验证。

设置 vCenter Single Sign-On 的默认域

每个 vCenter Single Sign-On 标识源都与某个域相关联。vCenter Single Sign-On 使用默认域验证未使用域名登录的用户的身份。如果用户所属的域不是默认域，则用户在登录时必须包含域名。

用户从 vSphere Client 登录到 vCenter Server 系统时，登录行为取决于用户是否位于设置为默认标识源的域中。

- 默认域中的用户可使用其自身的用户名和密码进行登录。
- 如果用户位于已添加到 vCenter Single Sign-On 作为标识源的域而并非默认域中，则可以登录到 vCenter Server，但必须按照以下方式之一指定域。
  - 包含域名前缀，例如 MYDOMAIN\user1
  - 包含域，例如 user1@mydomain.com

- 如果用户位于不是 vCenter Single Sign-On 标识源的域中，则无法登录到 vCenter Server。如果添加到 vCenter Single Sign-On 的域是域层次结构的一部分，则 Active Directory 将确定层次结构中其他域的用户是否进行了身份验证。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在**单点登录**下，单击**配置**。

4 单击**标识源**，选择一个标识源，然后单击**设为默认设置**。

在域显示屏幕中，默认域显示在“域”列中（默认设置）。

添加或编辑 vCenter Single Sign-On 标识源

仅当用户所在域已添加为 vCenter Single Sign-On 标识源时，用户才能登录到 vCenter Server。vCenter Single Sign-On 管理员用户可以添加标识源，或者更改已添加的标识源的设置。

标识源可以是本机 Active Directory（集成 Windows 身份验证）域，也可以是 OpenLDAP 目录服务。为实现向后兼容性，也可以选择 Active Directory 作为 LDAP 服务器。请参见 vCenter Server 和 vCenter Single Sign-On 的标识源。

一旦完成安装，以下默认标识源和用户立即可用：

localos	所有本地操作系统用户。如果您要升级，则已进行身份验证的 `localos` 用户可以继续进行身份验证。在使用嵌入式 Platform Services Controller 的环境中使用 `localos` 标识源没有意义。
vsphere.local	包含 vCenter Single Sign-On 内部用户。

前提条件

如果您要添加 Active Directory 标识源，则 vCenter Server Appliance 或 vCenter Server 的 Windows 计算机必须位于 Active Directory 域中。请参见将 Platform Services Controller 设备添加到 Active Directory 域。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在**单点登录**下，单击**配置**。

4 单击**标识源**，然后单击**添加标识源**。

5 选择标识源，然后输入标识源设置。

选项	描述
Active Directory (集成 Windows 身份验证)	对于本机 Active Directory 实施，请使用此选项。如果要使用此选项，则运行 vCenter Single Sign-On 服务的计算机必须在 Active Directory 域中。 请参见 Active Directory 标识源设置。
基于 LDAP 的 Active Directory	此选项可用于向后兼容性。这需要您指定域控制器和其他信息。请参见 Active Directory LDAP Server 和 OpenLDAP Server 标识源设置。
OpenLDAP	对于 OpenLDAP 标识源，请使用此选项。请参见 Active Directory LDAP Server 和 OpenLDAP Server 标识源设置。
SSO 服务器的本地操作系统	对于 SSO 服务器的本地操作系统，请使用此选项。

注 如果用户帐户已锁定或禁用，Active Directory 域中的身份验证以及组和用户搜索将失败。用户帐户必须具有用户和组 OU 的只读访问权限，并且必须能够读取用户和组属性。默认情况下，Active Directory 可提供此访问权限。使用特殊服务用户以增强安全性。

6 单击**添加**。

后续步骤

添加标识源后，所有用户均可进行身份验证，但只有**无权访问**角色。具有 vCenter Server**Modify.permissions** 特权的用户可向用户或用户组分配特权。特权使用户或组能够登录到 vCenter Server 以及查看和管理对象。您可以配置权限，以便已加入的 Active Directory 域中的用户和组可以访问 vCenter Server 组件。请参见《vSphere 安全性》文档。

Active Directory 标识源设置

如果选择 **Active Directory (集成 Windows 身份验证)** 标识源类型，则可以使用本地计算机帐户作为 SPN（服务主体名称）或明确指定一个 SPN。只有在 vCenter Single Sign-On 服务器加入 Active Directory 域时，才能使用此选项。

使用 Active Directory 标识源的必备条件

仅当 Active Directory 标识源可用时，才能将 vCenter Single Sign-On 设置为使用该标识源。

- 对于 Windows 安装，请将 Windows 计算机加入 Active Directory 域。
- 对于 vCenter Server Appliance，请按照《vCenter Server Appliance 配置》文档中的说明操作。

注 Active Directory（集成 Windows 身份验证）始终使用 Active Directory 域林的根目录。要使用 Active Directory 林中的子域配置集成 Windows 身份验证标识源，请参见 VMware 知识库文章，网址为 http://kb.vmware.com/kb/2070433.）。

选择**使用计算机帐户**可加快配置速度。如果您希望重命名运行 vCenter Single Sign-On 的本地计算机，最好明确指定一个 SPN。

注 在 vSphere 5.5 中，即使指定 SPN，vCenter Single Sign-On 仍会使用计算机帐户。请参见 VMware 知识库文章，网址为 http://kb.vmware.com/kb/2087978。

表 2-2. 添加标识源设置

文本框	描述
域名	域名的 FQDN，例如，mydomain.com。请勿提供 IP 地址。该域名必须可由 vCenter Server 系统进行 DNS 解析。如果您使用的是 vCenter Server Appliance，请使用有关配置网络设置的信息来更新 DNS 服务器设置。
使用计算机帐户	选择此选项可将本地计算机帐户用作 SPN。选择此选项时，应仅指定域名。如果您希望重命名此计算机，请勿选择此选项。
使用服务主体名称 (SPN)	如果您希望重命名本地计算机，请选择此选项。必须指定 SPN、能够通过标识源进行身份验证的用户以及该用户的密码。
服务主体名称 (SPN)	有助于 Kerberos 识别 Active Directory 服务的 SPN。请在名称中包含域，例如 `STS/example.com`。 SPN 在域中必须唯一。运行 `setspn -S` 可检查是否未创建重复项。有关 `setspn` 的信息，请参见 Microsoft 文档。
用户主体名称 (UPN) **密码**	能够通过此标识源进行身份验证的用户的名称和密码。请使用电子邮件地址格式，例如 `jchin@mydomain.com`。可以通过 Active Directory 服务界面编辑器 (ADSI Edit) 验证用户主体名称。

Active Directory LDAP Server 和 OpenLDAP Server 标识源设置

作为 LDAP Server 标识源的 Active Directory 可用于向后兼容性。针对需要较少输入的设置，使用 Active Directory（已集成 Windows 身份验证）选项。OpenLDAP Server 标识源适用于使用 OpenLDAP 的环境。

配置 OpenLDAP 标识源时，请参见 VMware 知识库文章，网址为 http://kb.vmware.com/kb/2064977），以了解其他要求。

表 2-3. LDAP Server Active Directory 和 OpenLDAP 设置

选项	描述
名称	标识源的名称。
用户的基本 DN	用户的基本识别名。
组的基本 DN	组的基本识别名。
域名	域的 FQDN。
域别名	对于 Active Directory 标识源，该别名为域的 NetBIOS 名称。如果要使用 SSPI 身份验证，则将 Active Directory 域的 NetBIOS 名称添加为标识源的别名。 对于 OpenLDAP 标识源，如果不指定别名，则会添加大写字母域名。
用户名	域中用户的 ID，该用户对用户和组的基本 DN 只具有最小只读权限。

表 2-3. LDAP Server Active Directory 和 OpenLDAP 设置 （续）

选项	描述
密码	由**用户名**指定的用户的密码。
连接到	要连接到的域控制器。可以是域中的任何域控制器或特定控制器。
主服务器 URL	域的主域控制器 LDAP 服务器。 请使用 **ldap://hostname:port** 或 **ldaps://hostname:port** 格式。该端口通常为 389 用于 LDAP 连接，而 636 用于 LDAPS 连接。对于 Active Directory 多域控制器部署，该端口通常为 3268 用于 LDAP，而 3269 用于 LDAPS。 在主 LDAP URL 或辅助 LDAP URL 中使用 **ldaps://** 时，需要一个证书为 Active Directory 服务器的 LDAPS 端点建立信任。
辅助服务器 URL	用于故障切换的辅助域控制器 LDAP 服务器的地址。
SSL 证书	如果要将 LDAPS 与 Active Directory LDAP 服务器或 OpenLDAP 服务器标识源配合使用，请单击**浏览**选择证书。

将 vCenter Single Sign-On 与 Windows 会话身份验证结合使用

您可以在 vCenter Single Sign-On 中使用 Windows 会话身份验证 (SSPI)。必须先将 Platform Services Controller 加入 Active Directory 域，然后才能使用 SSPI。

使用 SSPI 可为当前已登录计算机的用户加快登录过程。

前提条件

- 将要运行 Platform Services Controller 的 Platform Services Controller 设备或 Windows 计算机加入 Active Directory 域。请参见将 Platform Services Controller 设备添加到 Active Directory 域。
- 确认域设置正确无误。请参见 VMware 知识库文章，网址为 http://kb.vmware.com/kb/2064250。
- 如果使用的是 vSphere 6.0 及更低版本，请确认安装了客户端集成插件。
- 如果使用的是 vSphere 6.5 及更高版本，请确认安装了增强型身份验证插件。请参见《vCenter Server 安装和设置》。

步骤

1. 导航至 vSphere Client 登录页面。
2. 选中**使用 Windows 会话身份验证**复选框。
3. 使用 Active Directory 用户名和密码登录。
   - 如果 Active Directory 域为默认标识源，则使用用户名登录，例如 jlee。
   - 否则，包含域名，例如 jlee@example.com。

了解 vCenter Server 双因素身份验证

通过 vCenter Single Sign-On，您可以作为 vCenter Single Sign-On 可识别的标识源中的用户进行身份验证，或者使用 Windows 会话身份验证。您还可以通过使用智能卡（基于 UPN 的通用访问卡或 CAC）或者通过使用 RSA SecurID 令牌来进行身份验证。

双因素身份验证方法

政府机构或大型企业通常需要双因素身份验证方法。

智能卡身份验证

智能卡身份验证仅允许在所登录计算机的 USB 驱动器上接入了物理卡的用户进行访问。例如，通用访问卡 (Common Access Card, CAC) 身份验证。

管理员可以部署 PKI，使智能卡证书成为由 CA 颁发的唯一客户端证书。对于此类部署，仅为用户提供智能卡证书。用户选择一个证书，然后系统会提示输入 PIN。只有同时具有物理卡以及与证书匹配的 PIN 的用户才能登录。

RSA SecurID 身份验证

对于 RSA SecurID 身份验证，您的环境必须包括正确配置的 RSA Authentication Manager。如果 Platform Services Controller 已配置为指向 RSA 服务器，并且如果已启用 RSA SecurID 身份验证，则用户可以通过其用户名和令牌进行登录。

有关详细信息，请参见两个有关 RSA SecurID 设置的 vSphere 博客帖子。

注 vCenter Single Sign-On 仅支持本机 SecurID。它不支持 RADIUS 身份验证。

指定非默认身份验证方法

管理员可以从 vSphere Client 或通过使用 `sso-config` 脚本设置非默认身份验证方法。

- 对于智能卡身份验证，可以从 vSphere Client 或通过使用 `sso-config` 执行 vCenter Single Sign-On 设置。设置包括启用智能卡身份验证以及配置证书吊销策略。
- 对于 RSA SecurID，使用 `sso-config` 脚本为域配置 RSA Authentication Manager，并启用 RSA 令牌身份验证。无法从 vSphere Client 配置 RSA SecurID 身份验证。但是，如果启用 RSA SecurID，该身份验证方法将显示在 vSphere Client 中。

结合使用各种身份验证方法

可以使用 `sso-config` 分别启用或禁用每种身份验证方法。在测试双因素身份验证方法时，先让用户名和密码身份验证处于启用状态；测试完成之后，仅启用一种身份验证方法。

智能卡身份验证登录

智能卡是具有嵌入式集成电路芯片的小型塑料卡。许多政府机构和大型企业使用诸如通用访问卡 (CAC) 之类的智能卡来提高其系统的安全性和遵循安全法规。在使用智能卡的环境中，每台计算机都应具有智能卡读取器。通常会预装用于管理智能卡的智能卡硬件驱动程序。

系统将提示登录到 vCenter Server 或 Platform Services Controller 系统的用户通过智能卡和 PIN 的组合进行身份验证，如下所述。

1 用户将智能卡插入智能卡读取器时，vCenter Single Sign-On 读取卡上的证书。

2 vCenter Single Sign-On 提示用户选择证书，然后提示用户输入该证书的 PIN。

3 vCenter Single Sign-On 检查智能卡上的证书是否已知以及 PIN 是否正确。如果打开了吊销检查，则 vCenter Single Sign-On 还会检查证书是否已被吊销。

4 如果是已知且未被吊销的证书，则用户通过身份验证并可以执行有权执行的任务。

注 通常情况下，在测试期间保持用户名和密码身份验证处于启用状态很有意义。测试完成后，禁用用户名和密码身份验证并启用智能卡身份验证。随后，vSphere Client 和 vSphere Web Client 仅允许智能卡登录。只有对计算机具有 root 特权或管理员特权的用户才可以通过直接登录到 Platform Services Controller 来重新启用用户名和密码身份验证。

配置和使用智能卡身份验证

可以将您的环境设置为在用户从 vSphere Client 或 vSphere Web Client 连接到 vCenter Server 或关联的 Platform Services Controller 时要求智能卡身份验证。

智能卡身份验证的设置方式取决于您所使用的 vSphere 版本。

vSphere 版本	过程	链接
6.0 Update 2 更高版本的 vSphere 6.0	1 设置 Tomcat 服务器。 2 启用和配置智能卡身份验证。	vSphere 6.0 文档中心。
6.5 及更高版本	1 设置反向代理。 2 启用和配置智能卡身份验证。	配置反向代理以请求客户端证书 使用命令行管理智能卡身份验证 管理智能卡身份验证

配置反向代理以请求客户端证书

在启用智能卡身份验证之前，您需要在 Platform Services Controller 系统上配置反向代理。如果您的环境使用嵌入式 Platform Services Controller，需在同时运行 vCenter Server 和 Platform Services Controller 的系统上执行此项任务。

vSphere 6.5 及更高版本需要配置反向代理。

前提条件

将 CA 证书复制到 Platform Services Controller 系统。

步骤

1 登录到 Platform Services Controller。

操作系统	描述
Appliance	以 root 用户身份登录设备 shell。
Windows	以管理员用户身份登录 Windows 命令提示符。

2 创建可信客户端 CA 存储。

该存储将包含可信发证 CA 的客户端证书。此处的客户端是在智能卡过程中用于提示最终用户提供信息的浏览器。

以下示例显示了如何在 Platform Services Controller 设备上创建证书存储。

对于单一证书：

```
cd /usr/lib/vmware-sso/
openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer > /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem
```

对于多个证书：

```
cd /usr/lib/vmware-sso/
openssl x509 -inform PEM -in xyzCompanySmartCardSigningCA.cer >> /usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem
```

注 在 Windows 上的 Platform Services Controller 上，使用 `C:\ProgramData\VMware\vCenterServer\runtime\VMwareSTSService\conf\` 并将命令更改为使用反斜杠。

3 备份包含反向代理定义的 `config.xml` 文件，然后在编辑器中打开 `config.xml`。

操作系统	描述
Appliance	`/etc/vmware-rhttpproxy/config.xml`
Windows	`C:\ProgramData\VMware\vCenterServer\cfg\vmware-rhttpproxy\config.xml`

4 按如下所示进行更改，然后保存文件。

```
<http>
<maxConnections> 2048 </maxConnections>
<requestClientCertificate>true</requestClientCertificate>
<clientCertificateMaxSize>4096</clientCertificateMaxSize>
<clientCAListFile>/usr/lib/vmware-sso/vmware-sts/conf/clienttrustCA.pem</clientCAListFile>
</http>
```

`config.xml` 文件包含其中一些元素。根据需要取消注释、更新或添加元素。

5 重新启动服务。

操作系统	描述
Appliance	`/usr/lib/vmware-vmon/vmon-cli --restart rhttpproxy`

Windows	重新启动操作系统，或通过执行以下步骤重新启动 VMware HTTP Reverse Proxy：
	a 打开权限提升的命令提示符。
	b 运行以下命令：
	`cd C:\Program Files\VMware\vCenter Server\bin`
	`service-control --stop vmware-rhttpproxy`
	`service-control --start vmware-rhttpproxy`

使用命令行管理智能卡身份验证

可以使用 `sso-config` 实用程序从命令行管理智能卡身份验证。该实用程序支持所有智能卡配置任务。

您可以在以下位置找到 `sso-config` 脚本：

Windows	`C:\Program Files\VMware\VCenter server\VMware Identity Services\sso-config.bat`
Linux	`/opt/vmware/bin/sso-config.sh`

支持的身份验证类型和吊销设置的配置存储在 VMware Directory Service 中，且在 vCenter Single Sign-On 域中的所有 Platform Services Controller 实例之间复制。

如果禁用用户名和密码身份验证，且智能卡身份验证出现问题，则用户无法登录。在这种情况下，root 或管理员用户可以从 Platform Services Controller 命令行打开用户名和密码身份验证。以下命令可启用用户名和密码身份验证。

操作系统	命令
Windows	`sso-config.bat -set_authn_policy -pwdAuthn true -t <tenant_name>` 如果您使用默认租户，请使用 vsphere.local 作为租户名称。
Linux	`sso-config.sh -set_authn_policy -pwdAuthn true -t <tenant_name>` 如果您使用默认租户，请使用 vsphere.local 作为租户名称。

如果您使用 OCSP 进行吊销检查，则可以依靠在智能卡证书 AIA 扩展中指定的默认 OCSP。您还可以替代默认设置并配置一个或多个替代 OCSP 响应者。例如，您可以设置 vCenter Single Sign-On 站点本地的 OCSP 响应者，用于处理吊销检查请求。

注 如果您的证书未定义 OCSP，请改为启用 CRL（证书吊销列表）。

前提条件

- 验证您的环境是否使用 Platform Services Controller 6.5 或更高版本，以及您是否使用 vCenter Server 版本 6.0 或更高版本。Platform Services Controller 版本 6.0 Update 2 支持智能卡身份验证，但设置过程有所不同。
- 验证在您的环境中是否设置了企业公钥基础架构 (PKI)，以及证书是否满足以下要求：
  - 用户主体名称 (UPN) 必须对应于主体备用名称 (SAN) 扩展名中的 Active Directory 帐户。
  - 必须在证书的“应用程序策略”或“增强型密钥使用”字段中指定“客户端身份验证”，否则浏览器将不显示证书。
- 验证 Platform Services Controller 证书是否受最终用户工作站信任。否则，浏览器不会尝试身份验证。
- 将 Active Directory 标识源添加到 vCenter Single Sign-On。
- 将 vCenter Server 管理员角色分配给 Active Directory 标识源中的一个或多个用户。然后，这些用户可执行管理任务，因为他们可以进行身份验证，并且具有 vCenter Server 管理员特权。

  注 默认情况下，vCenter Single Sign-On 域的管理员 administrator@vsphere.local 无法执行智能卡身份验证。

- 设置反向代理，然后重新启动物理机或虚拟机。

步骤

1 获取证书并将其复制到 `sso-config` 实用程序可以检测到的文件夹。

选项	描述
Windows	登录到 Platform Services Controller Windows 安装，并使用 WinSCP 或类似的实用程序复制文件。

Appliance	a 直接或者使用 SSH 登录到设备控制台。
	b 启用设备 shell，如下所示。
	`shell`
	`chsh -s "/bin/bash" root`
	c 使用 WinSCP 或类似的实用程序将证书复制到 Platform Services Controller 上的 `/usr/lib/vmware-sso/vmware-sts/conf`。
	d 选择性禁用设备 shell，如下所示。
	`chsh -s "/bin/appliancesh" root`

2 要为 VMware Directory Service (vmdir) 启用智能卡身份验证，请运行以下命令。

```
sso-config.[bat|sh] -set_authn_policy -certAuthn true -cacerts
first_trusted_cert.cer,second_trusted_cert.cer  -t tenant
```

例如：

```
sso-config.[bat|sh] -set_authn_policy -certAuthn true -cacerts MySmartCA1.cer,MySmartCA2.cer  -t
vsphere.local
```

使用逗号分隔多个证书，但不要在逗号后面加空格。

3 要禁用所有其他身份验证方法，请运行以下命令。

```
sso-config.[bat|sh] -set_authn_policy -pwdAuthn false -t vsphere.local
sso-config.sh -set_authn_policy -winAuthn false -t vsphere.local
sso-config.sh -set_authn_policy -securIDAuthn false -t vsphere.local
```

4 （可选）要设置证书策略白名单，请运行以下命令。

```
sso-config.[bat|sh] -set_authn_policy -certPolicies policies
```

要指定多个策略，请用逗号分隔它们，例如：

```
sso-config.bat -set_authn_policy -certPolicies 2.16.840.1.101.2.1.11.9,2.16.840.1.101.2.1.11.19
```

此白名单指定证书的证书策略扩展中允许的策略的对象 ID。X509 证书可具有证书策略扩展。

5 （可选）启用并配置使用 OCSP 进行吊销检查。

a 启用使用 OCSP 进行吊销检查。

```
sso-config.[bat|sh]  -set_authn_policy -t tenantName  -useOcsp true
```

b 如果证书的 AIA 扩展未提供 OCSP 响应者链接，请提供替代 OCSP 响应者 URL 和 OCSP 颁发机构证书。

为每个 vCenter Single Sign-On 站点配置了替代的 OCSP。您可以为 vCenter Single Sign-On 站点指定多个替代 OCSP 响应者，以便允许进行故障切换。

```
sso-config.[bat|sh] -t tenant -add_alt_ocsp  [-siteID yourPSCClusterID] -ocspUrl
http://ocsp.xyz.com/ -ocspSigningCert yourOcspSigningCA.cer
```

注 默认情况下，配置将应用于当前 vCenter Single Sign-On 站点。仅当为其他 vCenter Single Sign-On 站点配置替代 OCSP 时，才需要指定 `siteID` 参数。

请参见下面的示例：

```
 .sso-config.[bat|sh] -t vsphere.local -add_alt_ocsp -ocspUrl
http://failover.ocsp.nsn0.rcvs.nit.disa.mil/ -
ocspSigningCert ./DOD_JITC_EMAIL_CA-29__0x01A5__DOD_JITC_ROOT_CA_2.cer
 Adding alternative OCSP responder for tenant :vsphere.local
 OCSP responder is added successfully!
 [
 site::   78564172-2508-4b3a-b903-23de29a2c342
     [
     OCSP url::   http://ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
     [
     OCSP url::   http://failover.ocsp.nsn0.rcvs.nit.disa.mil/
     OCSP signing CA cert:   binary value]
     ]
 ]
```

c 要显示当前的替代 OCSP 响应者设置，请运行此命令。

```
sso-config.[bat|sh] -t tenantName -get_alt_ocsp]
```

d 要移除当前的替代 OCSP 响应者设置，请运行以下命令。

```
sso-config.[bat|sh] -t tenantName -delete_alt_ocsp [-allSite] [-siteID
pscSiteID_for_the_configuration]
```

6 （可选）要列出配置信息，请运行以下命令。

```
sso-config.[bat|sh] -get_authn_policy -t tenantName
```

管理智能卡身份验证

可以从 vSphere Client 启用和禁用智能卡身份验证、自定义登录横幅以及设置吊销策略。

如果已启用智能卡身份验证并禁用其他身份验证方法，则用户需要使用智能卡身份验证进行登录。

如果禁用用户名和密码身份验证，且智能卡身份验证出现问题，则用户无法登录。在这种情况下，root 或管理员用户可以从 Platform Services Controller 命令行打开用户名和密码身份验证。以下命令可启用用户名和密码身份验证。

操作系统	命令
Windows	`sso-config.bat -set_authn_policy -pwdAuthn true -t <tenant_name>` 如果您使用默认租户，请使用 vsphere.local 作为租户名称。
Linux	`sso-config.sh -set_authn_policy -pwdAuthn true -t <tenant_name>` 如果您使用默认租户，请使用 vsphere.local 作为租户名称。

前提条件

- 验证您的环境是否使用 Platform Services Controller 6.5 或更高版本，以及您是否使用 vCenter Server 版本 6.0 或更高版本。Platform Services Controller 版本 6.0 Update 2 支持智能卡身份验证，但设置过程有所不同。
- 验证在您的环境中是否设置了企业公钥基础架构 (PKI)，以及证书是否满足以下要求：
  - 用户主体名称 (UPN) 必须对应于主体备用名称 (SAN) 扩展名中的 Active Directory 帐户。
  - 必须在证书的“应用程序策略”或“增强型密钥使用”字段中指定“客户端身份验证”，否则浏览器将不显示证书。
- 验证 Platform Services Controller 证书是否受最终用户工作站信任。否则，浏览器不会尝试身份验证。
- 将 Active Directory 标识源添加到 vCenter Single Sign-On。
- 将 vCenter Server 管理员角色分配给 Active Directory 标识源中的一个或多个用户。然后，这些用户可执行管理任务，因为他们可以进行身份验证，并且具有 vCenter Server 管理员特权。

  注 默认情况下，vCenter Single Sign-On 域的管理员 administrator@vsphere.local 无法执行智能卡身份验证。

- 设置反向代理，然后重新启动物理机或虚拟机。

步骤

1 获取证书并将其复制到 `sso-config` 实用程序可以检测到的文件夹。

选项	描述
Windows	登录到 Platform Services Controller Windows 安装，并使用 WinSCP 或类似的实用程序复制文件。

Appliance	a 直接或者使用 SSH 登录到设备控制台。
	b 启用设备 shell，如下所示。
	`shell`
	`chsh -s "/bin/bash" root`
	`csh -s "bin/appliance/sh" root`
	c 使用 WinSCP 或类似的实用程序将证书复制到 Platform Services Controller 上的 `/usr/lib/vmware-sso/vmware-sts/conf`。
	d 选择性禁用设备 shell，如下所示。
	`chsh -s "/bin/appliancesh" root`

2 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

3 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

4 导航到配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在**单点登录**下，单击**配置**。

5 在**智能卡身份验证**下，单击**编辑**。

6 选择或取消选择身份验证方法，然后单击**保存**。

可以仅选择智能卡身份验证，也可以同时选择智能卡身份验证以及密码和 Windows 会话身份验证。

无法从此 Web 界面启用或禁用 RSA SecurID 身份验证。但是，如果已从命令行启用 RSA SecurID，状态将显示在该 Web 界面中。

此时将显示**受信任的 CA 证书**。

7 在**受信任的 CA 证书**选项卡下，单击**添加**，然后单击**浏览**。

8 从受信任的 CA 选择所有证书，然后单击**添加**。

后续步骤

您的环境可能需要增强的 OCSP 配置。

- 如果发出 OCSP 响应的 CA 不是智能卡的签名 CA，请提供 OCSP 签名 CA 证书。
- 您可以在多站点部署中为每个 Platform Services Controller 站点配置一个或多个本地 OCSP 响应者。您可以使用 CLI 配置这些替代 OCSP 响应者。请参见使用命令行管理智能卡身份验证。

设置智能卡身份验证的吊销策略

可以自定义证书吊销检查，并可以指定 vCenter Single Sign-On 查找有关已吊销证书的信息的位置。

通过使用 vSphere Client 或者通过使用 `sso-config` 脚本，可以自定义行为。所选设置部分取决于 CA 所支持的内容。

- 如果已禁用吊销检查，则 vCenter Single Sign-On 忽略任何 CRL 或 OCSP 设置。vCenter Single Sign-On 不对任何证书执行检查。
- 如果已启用吊销检查，则建议的设置取决于 PKI 设置。

  仅 OCSP：如果发证 CA 支持 OCSP 响应者，则启用 **OCSP** 并禁用 **CRL 作为 OCSP 的故障切换**。

  仅 CRL：如果发证 CA 不支持 OSCP，则启用 **CRL 检查**并禁用 **OSCP 检查**。

  OCSP 和 CRL：如果发证 CA 同时支持 OCSP 响应者和 CRL，则 vCenter Single Sign-On 首先检查 OCSP 响应者。如果响应者返回未知状态或者不可用，则 vCenter Single Sign-On 将检查 CRL。对于此情况，请同时启用 **OCSP 检查**和 **CRL 检查**，并启用 **CRL 作为 OCSP 的故障切换**。

- 如果已启用吊销检查，则高级用户可以指定以下其他设置。

  OCSP URL：默认情况下，vCenter Single Sign-On 检查在被验证的证书中定义的 OCSP 响应者的位置。如果该证书不存在 Authority Information Access 扩展名或如果想要替代该扩展名，则可以明确指定一个位置。

  使用证书中的 CRL：默认情况下，vCenter Single Sign-On 检查在被验证的证书中定义的 CRL 的位置。如果证书中缺少 CRL 分发点扩展或者您要替代默认值，请禁用此选项。

  CRL 位置：如果禁用**使用证书中的 CRL** 并且要指定 CRL 所在的位置（文件或 HTTP URL），则使用此属性。

可以通过添加证书策略来进一步限制 vCenter Single Sign-On 接受的证书。

前提条件

- 验证您的环境是否使用 Platform Services Controller6.5 或更高版本，以及您是否使用 vCenter Server 版本 6.0 或更高版本。Platform Services Controller 版本 6.0 Update 2 支持智能卡身份验证，但设置过程有所不同。
- 验证在您的环境中是否设置了企业公钥基础架构 (PKI)，以及证书是否满足以下要求：
  - 用户主体名称 (UPN) 必须对应于主体备用名称 (SAN) 扩展名中的 Active Directory 帐户。
  - 必须在证书的“应用程序策略”或“增强型密钥使用”字段中指定“客户端身份验证”，否则浏览器将不显示证书。
- 验证 Platform Services Controller 证书是否受最终用户工作站信任。否则，浏览器不会尝试身份验证。
- 将 Active Directory 标识源添加到 vCenter Single Sign-On。

- 将 vCenter Server 管理员角色分配给 Active Directory 标识源中的一个或多个用户。然后，这些用户可执行管理任务，因为他们可以进行身份验证，并且具有 vCenter Server 管理员特权。

  注 默认情况下，vCenter Single Sign-On 域的管理员 administrator@vsphere.local 无法执行智能卡身份验证。

步骤

1. 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。
2. 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

   如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。
3. 导航到配置 UI。
   a. 在**主页**菜单中，选择**系统管理**。
   b. 在**单点登录**下，单击**配置**。
4. 单击**智能卡身份验证**。
5. 单击**证书吊销**，然后单击**编辑**以启用或禁用吊销检查。
6. 如果证书策略在您的环境中是有效的，则可以在**证书策略**窗格中添加策略。

设置 RSA SecurID 身份验证

可以将您的环境设置为要求用户使用 RSA SecurID 令牌登录。仅支持从命令行进行 SecurID 设置。

有关详细信息，请参见两个有关 RSA SecurID 设置的 vSphere 博客帖子。

注 RSA Authentication Manager 要求用户 ID 为使用 1 到 255 个 ASCII 字符的唯一标识符。不允许使用以下字符：与号 (&)、百分号 (%)、大于号 (>)、小于号 (<) 和单引号 (`)。

前提条件

- 验证您的环境是否使用 Platform Services Controller6.5 或更高版本，以及您是否使用 vCenter Server 版本 6.0 或更高版本。Platform Services Controller 版本 6.0 Update 2 支持智能卡身份验证，但设置过程有所不同。
- 验证您的环境是否具有正确配置的 RSA Authentication Manager，以及用户是否具有 RSA 令牌。需要 RSA Authentication Manager 版本 8.0 或更高版本。
- 验证 RSA Manager 使用的标识源是否已添加到 vCenter Single Sign-On。请参见添加或编辑 vCenter Single Sign-On 标识源。
- 验证 RSA Authentication Manager 系统是否可以解析 Platform Services Controller 主机名，以及 Platform Services Controller 系统是否可以解析 RSA Authentication Manager 主机名。
- 通过选择**访问 > 身份验证代理 > 生成配置文件**，从 RSA Manager 导出 `sdconf.rec` 文件。解压缩生成的 `AM_Config.zip` 文件以查找 `sdconf.rec` 文件。
- 将 `sdconf.rec` 文件复制到 Platform Services Controller 节点。

步骤

1 更改到 `sso-config` 脚本所在的目录。

选项	描述
Windows	`C:\Program Files\VMware\VCenter server\VMware Identity Services`
Appliance	`/opt/vmware/bin`

2 要启用 RSA SecurID 身份验证，请运行以下命令。

```
sso-config.[sh|bat]  -t tenantName  -set_authn_policy  -securIDAuthn true
```

tenantName 是 vCenter Single Sign-On 域的名称，默认情况下为 vsphere.local。

3 （可选）要禁用其他身份验证方法，请运行以下命令。

```
sso-config.sh -set_authn_policy -pwdAuthn false -winAuthn false -certAuthn false -t vsphere.local
```

4 要配置环境以使当前站点的租户使用 RSA 站点，请运行以下命令。

```
sso-config.[sh|bat] -set_rsa_site [-t tenantName] [-siteID Location] [-agentName Name] [-sdConfFile
Path]
```

例如：

```
sso-config.sh -set_rsa_site -agentName SSO_RSA_AUTHSDK_AGENT -sdConfFile /tmp/sdconf.rec
```

可以指定以下选项。

选项	描述
siteID	可选 Platform Services Controller 站点 ID。Platform Services Controller 支持每个站点具有一个 RSA Authentication Manager 实例或群集。如果您未明确指定该选项，则 RSA 配置用于当前 Platform Services Controller 站点。仅当添加不同的站点时才使用此选项。
agentName	在 RSA Authentication Manager 中定义。
sdConfFile	从 RSA Manager 下载的 `sdconf.rec` 文件的副本，其中包括 RSA Manager 的 IP 地址等配置信息。

5 （可选）要将租户配置更改为非默认值，请运行以下命令。

```
sso-config.[sh|bat] -set_rsa_config [-t tenantName] [-logLevel Level] [-logFileSize Size] [-
maxLogFileCount Count] [-connTimeOut Seconds] [-readTimeOut Seconds] [-encAlgList Alg1,Alg2,...]
```

通常情况下，默认值是合适的，例如：

```
sso-config.sh -set_rsa_config -t vsphere.local -logLevel DEBUG
```

6 （可选）如果标识源未将用户主体名称用作用户 ID，则设置标识源的 userID 属性。

userID 属性确定哪个 LDAP 属性用作 RSA userID。

```
sso-config.[sh|bat] -set_rsa_userid_attr_map [-t tenantName] [-idsName Name] [-ldapAttr AttrName] [-siteID Location]
```

例如：

```
sso-config.sh -set_rsa_userid_attr_map -t vsphere.local -idsName ssolabs.com -ldapAttr userPrincipalName
```

7 要显示当前设置，请运行以下命令。

```
sso-config.sh -t tenantName -get_rsa_config
```

如果已禁用用户名和密码身份验证且已启用 RSA 身份验证，则用户必须使用其用户名和 RSA 令牌进行登录。无法再使用用户名和密码进行登录。

注 使用用户名格式 ***userID@domainName*** 或 ***userID@domain_upn_suffix***.

管理登录消息

可以在环境中包含登录消息。可以启用和禁用登录消息，并且可以要求用户单击用于表示明确同意的复选框。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在**单点登录**下，单击**配置**。

4 单击**登录消息**选项卡。

5 单击**编辑**并配置登录消息。

选项	描述
显示登录消息	打开**显示登录消息**以启用登录消息。除非打开此开关，否则无法对登录消息进行更改。
登录消息	消息的标题。默认情况下，当**“同意”复选框**打开时，登录消息文本为 `I agree to Terms and Conditions`。您必须将 `Terms and Conditions` 替换为自己的文本。如果关闭**同意**复选框，那么将显示 `Login message`，可在上面输入您的消息。

选项	描述
“同意”复选框	打开**“同意”复选框**以要求用户在登录之前单击复选框。也可以显示不带复选框的消息。
登录消息的详细信息	用户在单击登录消息时看到的消息，例如，条款和条件文本。您必须在此文本框中输入一些详细信息。

6 单击**保存**。

将 vCenter Single Sign-On 用作其他服务提供程序的身份提供程序

vSphere Client 将自动作为可信的 SAML 2.0 服务提供程序 (SP) 注册到 vCenter Single Sign-On。您可以将其他可信的服务提供程序添加到身份联合，其中 vCenter Single Sign-On 充当 SAML 身份提供程序 (IDP)。这些服务提供程序必须符合 SAML 2.0 协议。设置联合后，如果用户可以对 vCenter Single Sign-On 进行身份验证，服务提供程序将为用户授予访问权限。

注 vCenter Single Sign-On 可以是其他 SP 的 IDP。vCenter Single Sign-On 不能是使用其他 IDP 的 SP。

注册的 SAML 服务提供程序可以为已具有实时会话的用户（即，已登录到身份提供程序的用户）授予访问权限。例如，vRealize Automation 7.0 和更高版本支持 vCenter Single Sign-On 作为身份提供程序。可以从 vCenter Single Sign-On 和 vRealize Automation 设置联合。之后，vCenter Single Sign-On 可以在您登录到 vRealize Automation 时执行身份验证。

要将 SAML 服务提供程序加入到身份联合，必须通过在 SP 与 IDP 之间交换 SAML 元数据来建立彼此之间的信任。

必须同时对 vCenter Single Sign-On 和使用 vCenter Single Sign-On 的服务执行集成任务。

1 将 IDP 元数据导出到文件，然后将其导入到 SP。

2 导出 SP 元数据并将其导入到 IDP。

可以使用 vCenter Single Sign-On 的 vSphere Client 界面导出 IDP 元数据并从 SP 导入这些元数据。如果要使用 vRealize Automation 作为 SP，请参见 vRealize Automation 文档，了解有关导出 SP 元数据和导入 IDP 元数据的详细信息。

注 服务必须完全支持 SAML 2.0 标准，否则集成将不起作用。

将 SAML 服务提供程序加入到身份联合

可将 SAML 服务提供程序添加到 vCenter Single Sign-On，并将 vCenter Single Sign-On 作为身份提供程序添加到该服务。接下来，当用户登录到服务提供程序时，服务提供程序将通过 vCenter Single Sign-On 对用户进行身份验证。

前提条件

目标服务必须完全支持 SAML 2.0 标准，并且 SP 元数据必须具有 `SPSSODescriptor` 元素。

如果元数据未严格遵循 SAML 2.0 元数据架构，您可能必须先对元数据进行编辑才能将其导入。例如，如果使用的是 Active Directory 联合身份验证服务 (ADFS) SAML 服务提供程序，必须先对元数据进行编辑才能将其导入。移除以下非标准元素：

```
fed:ApplicationServiceType
fed:SecurityTokenServiceType
```

步骤

1. 将元数据从服务提供程序导出到文件。
2. 使用 vSphere Web Client 登录到已连接到 Platform Services Controller 的 vCenter Server。
3. 导航到配置 UI。
   a. 在**主页**菜单中，选择**系统管理**。
   b. 在**单点登录**下，单击**配置**。
4. 将 SP 元数据导入到 vCenter Single Sign-On 中。
   a. 选择 **SAML 服务提供程序**选项卡。
   b. 在 **SAML 服务提供程序中的元数据**对话框中，通过粘贴 XML 字符串或导入文件来导入元数据。
5. 导出 vCenter Single Sign-OnIDP 元数据。
   a. 在 **SAML 服务提供程序的元数据**文本框中，单击**下载**。
   b. 指定一个文件位置。
6. 登录到 SAML SP（例如 VMware vRealize Automation 7.0），并按照 SP 说明将 vCenter Single Sign-On 元数据添加到该服务提供程序。

   有关将元数据导入到该产品中的详细信息，请参见 vRealize Automation 文档。

安全令牌服务 (STS)

vCenter Single Sign-On 安全令牌服务 (STS) 是一项发布、验证和续订安全令牌的 Web 服务。

要获取 SAML 令牌，用户须向 STS 接口提供其主凭据。主凭据取决于用户类型。

用户	vCenter Single Sign-On 标识源中提供的用户名和密码。
应用程序用户	有效证书。

STS 将根据主凭据对用户进行身份验证，并构建包含用户属性的 SAML 令牌。STS 会使用其 STS 签名证书对 SAML 令牌进行签名，并将该令牌分配给用户。默认情况下，将由 VMCA 生成 STS 签名证书。可以从 vSphere Web Client 替换默认 STS 签名证书。除非贵公司的安全策略要求替换所有证书，否则不要替换 STS 签名证书。

用户具有 SAML 令牌后，该 SAML 令牌可作为该用户的 HTTP 请求的一部分进行发送（可能通过各种代理进行发送）。只有预期接收方（服务提供程序）可以使用 SAML 令牌中的信息。

刷新 Security Token Service 证书

vCenter Single Sign-On 服务器包含 Security Token Service (STS)。Security Token Service 是一项发布、验证和续订安全令牌的 Web 服务。现有 Security Token Service 证书过期或更改时，您可以从 vSphere Web Client 中手动对其进行刷新。

要获取 SAML 令牌，用户须向安全令牌服务器 (STS) 提供主凭据。主凭据取决于用户类型：

解决方案用户	有效证书
其他用户	vCenter Single Sign-On 标识源中提供的用户名和密码。

STS 将使用主凭据对用户进行身份验证，并构建包含用户属性的 SAML 令牌。STS 服务会使用其 STS 签名证书对 SAML 令牌进行签名，然后将该令牌分配给用户。默认情况下，将由 VMCA 生成 STS 签名证书。

用户具有 SAML 令牌后，该 SAML 令牌可作为该用户的 HTTP 请求的一部分进行发送（可能通过各种代理进行发送）。只有预期接收方（服务提供程序）可以使用 SAML 令牌中的信息。

如果公司策略需要该信息或如果您要更新过期的证书，则可以在 vSphere Web Client 中替换现有 STS 签名证书。

小心　请勿替换文件系统中的文件。如果替换该文件，则会导致意想不到且难以调试的错误。

注　替换证书后，必须重新启动节点，以便重新启动 vSphere Web Client 服务和 STS 服务。

前提条件

将刚刚添加到 java 密钥库的证书从 Platform Services Controller 复制到本地工作站。

Platform Services Controller 设备	*certificate_location*/keys/root-trust.jks 例如：/keys/root-trust.jks 例如： /root/newsts/keys/root-trust.jks
Windows 安装	*certificate_location*\root-trust.jks 例如： C:\Program Files\VMware\vCenter Server\jre\bin\root-trust.jks

步骤

1 以 administrator@vsphere.local 或拥有 vCenter Single Sign-On 管理员特权的其他用户的身份登录到 vSphere Web Client。

默认情况下，具有 vCenter Single Sign-On 管理员特权的用户位于本地 vCenter Single Sign-On 域 vsphere.local 中的管理员组。

2 导航到配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在**单点登录**下，单击**配置**。

3 依次选择**证书**选项卡和 **STS 签名**子选项卡，然后单击**添加 STS 签名证书**图标。

4 添加证书。

a 单击**浏览**浏览到包含新证书的密钥库 JKS 文件，然后单击**打开**。

b 出现提示时键入密码。

c 单击 STS 别名链的顶部，然后单击**确定**。

d 出现提示时再次键入密码。

5 单击**确定**。

6 重新启动 Platform Services Controller 节点，以启动 STS 服务和 vSphere Web Client。

重新启动之前，身份验证无法正常运行，因此必须重新启动。

在设备上生成新的 STS 签名证书

由于 vCenter Single Sign-On Security Token Service (STS) 签名证书是内部 VMware 证书，因此请勿替换它，除非贵公司要求替换内部证书。如果要替换默认的 STS 签名证书，必须生成一个新证书并将其添加到 Java 密钥库。此过程说明了在嵌入式部署设备或外部 Platform Services Controller 设备上执行该操作的步骤。

注 该证书的有效期为十年且不面向外部。除非贵公司的安全策略有相关规定，否则请勿替换此证书。

如果运行的是 Platform Services ControllerWindows 安装，请参见在 Windows 上安装 vCenter 时生成新的 STS 签名证书。

步骤

1 创建顶级目录以保存新证书并确人该目录的位置。

```
mkdir newsts
cd newsts
pwd
#resulting output: /root/newst
```

2 将 `certool.cfg` 文件复制到新目录中。

```
cp /usr/lib/vmware-vmca/share/config/certool.cfg /root/newsts
```

3 打开 `certool.cfg` 文件的副本并进行编辑，以便使用本地 Platform Services Controller 的 IP 地址和主机名。

国家/地区为必填字段且必须是两个字符，如以下示例所示。

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

4 生成密钥。

```
/usr/lib/vmware-vmca/bin/certool --server localhost --genkey --privkey=/root/newsts/sts.key --
pubkey=/root/newsts/sts.pub
```

5 生成证书

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=/root/newsts/newsts.cer --
privkey=/root/newsts/sts.key --config=/root/newsts/certool.cfg
```

6 将证书转换为 PK12 格式。

```
openssl pkcs12 -export -in /root/newsts/newsts.cer -inkey /root/newsts/sts.key -
certfile /etc/vmware-sso/keys/ssoserverRoot.crt -name "newstssigning" -passout pass:changeme -out
newsts.p12
```

7 将证书添加到 Java 密钥库 (JKS)。

```
/usr/java/jre-vmware/bin/keytool -v -importkeystore -srckeystore newsts.p12 -srcstoretype pkcs12 -
srcstorepass changeme -srcalias newstssigning -destkeystore root-trust.jks -deststoretype JKS -
deststorepass testpassword -destkeypass testpassword

/usr/java/jre-vmware/bin/keytool -v -importcert -keystore root-trust.jks -deststoretype JKS -
storepass testpassword -keypass testpassword -file /etc/vmware-sso/keys/ssoserverRoot.crt -alias
root-ca
```

8 出现提示时，键入 **Yes** 接受证书以将其添加到密钥库。

后续步骤

现在即可导入新证书。请参见刷新 Security Token Service 证书。

在 Windows 上安装 vCenter 时生成新的 STS 签名证书

由于 vCenter Single Sign-On Security Token Service (STS) 签名证书是内部 VMware 证书，因此请勿替换它，除非贵公司要求替换内部证书。如果要替换默认的 STS 签名证书，必须先生成一个新证书并将其添加到 Java 密钥库。以下过程说明了 Windows 中的安装步骤。

注 该证书的有效期为十年且不面向外部。除非贵公司的安全策略有相关规定，否则请勿替换此证书。

如果使用虚拟设备，请参见在设备上生成新的 STS 签名证书。

步骤

1 创建一个新目录以存放新证书。

```
cd C:\ProgramData\VMware\vCenterServer\cfg\sso\keys\
mkdir newsts
cd newsts
```

2 创建 `certool.cfg` 文件的副本并将其放入新目录中。

```
copy "C:\Program Files\VMware\vCenter Server\vmcad\certool.cfg" .
```

3 打开 `certool.cfg` 文件的副本并进行编辑，以便使用本地 Platform Services Controller 的 IP 地址和主机名。

国家/地区是必填项，且必须包含两个字符。以下示例说明了这一点。

```
#
# Template file for a CSR request
#

# Country is needed and has to be 2 characters
Country = US
Name = STS
Organization = ExampleInc
OrgUnit = ExampleInc Dev
State = Indiana
Locality = Indianapolis
IPAddress = 10.0.1.32
Email = chen@exampleinc.com
Hostname = homecenter.exampleinc.local
```

4 生成密钥。

```
"C:\Program Files\VMware\vCenter Server\vmcad\certool.exe" --server localhost --genkey --
privkey=sts.key --pubkey=sts.pub
```

5 生成证书

```
"C:\Program Files\VMware\vCenter Server\vmcad\certool.exe" --gencert --cert=newsts.cer --
privkey=sts.key --config=certool.cfg
```

6 将证书转换为 PK12 格式。

```
"C:\Program Files\VMware\vCenter Server\openSSL\openssl.exe" pkcs12 -export -in newsts.cer -inkey
sts.key -certfile ..\ssoserverRoot.crt -name "newstssigning" -passout pass:changeme -out newsts.p12
```

7 将证书添加到 Java 密钥库 (JKS)。

```
"C:\Program Files\VMware\vCenter Server\jre\bin\keytool.exe" -v -importkeystore -srckeystore
newsts.p12 -srcstoretype pkcs12 -srcstorepass changeme -srcalias newstssigning -destkeystore root-
trust.jks -deststoretype JKS -deststorepass testpassword -destkeypass testpassword
"C:\Program Files\VMware\vCenter Server\jre\bin\keytool.exe" -v -importcert -keystore root-
trust.jks -deststoretype JKS -storepass testpassword -keypass testpassword -
file ..\ssoserverRoot.crt -alias root-ca
```

后续步骤

现在即可导入新证书。请参见刷新 Security Token Service 证书。

确定 LDAPS SSL 证书的过期日期

如果选择 LDAP 标识源且决定使用 LDAPS，则可为 LDAP 流量上载 SSL 证书。SSL 证书在预定义的使用期限之后过期。知道证书何时过期使您能够在过期日期之前重新替换或更新证书。

只有使用 Active Directory LDAP 服务器或 OpenLDAP 服务器并为服务器指定 `ldaps://` URL 时，才可查看证书过期信息。其他类型的标识源或 `ldap://` 流量的“标识源**信任库**”选项卡仍然为空。

步骤

1 使用 vSphere Web Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在**单点登录**下，单击**配置**。

4 单击**证书**选项卡。

5 查看证书详细信息，并确认**有效期至**字段中的过期日期。

您可能会在选项卡的顶部看到一个警告，表示证书将要过期。

管理 vCenter Single Sign-On 策略

vCenter Single Sign-On 策略会在您的环境中执行安全规则。您可以查看和编辑默认 vCenter Single Sign-On 密码策略、锁定策略，以及令牌策略。

编辑 vCenter Single Sign-On 密码策略

vCenter Single Sign-On 密码策略确定了密码格式和密码过期时间。密码策略仅适用于 vCenter Single Sign-On 域（vsphere.local 或 vmc.local）中的用户。

默认情况下，vCenter Single Sign-On 密码在 90 天后过期。密码即将过期时，vSphere Client 将向您发出提醒。

注 密码策略仅适用于用户帐户，不适用于系统帐户（如 administrator@vsphere.local）。

请参见更改 vCenter Single Sign-On 密码。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在**单点登录**下，单击**配置**。

4 单击**策略**，选择**密码策略**，然后单击**编辑**。

5 编辑密码策略。

选项	描述
描述	密码策略描述。
最长生命周期	用户必须更改密码前密码保持有效的最大天数。可以输入的最大天数为 999999999。值为零 (0) 表示密码永不过期。
限制重用	不能重用的之前密码的个数。例如，如果输入 6，则用户不能重用最近六个密码中的任何一个。
最大长度	允许密码包含的最大字符数。
最小长度	密码必须包含的最少字符数。最小长度不得小于字母、数字和特殊字符要求的最小总和。

选项	描述
字符要求	密码必须包含的不同字符类型最小数目。您可以指定每种字符的数量，如下所示： ■ 特殊字符：& # % ■ 字母字符：A b c D ■ 大写字符：A B C ■ 小写字符：a b c ■ 数字字符：1 2 3 字母字符最小数目不得小于大写和小写字符的总和。 密码中支持非 ASCII 字符。在 vCenter Single Sign-On 的早期版本中，支持的字符存在限制。
相同的相邻字符数	密码中允许的连续相同字符的最大个数。例如，如果输入 1，则不允许使用以下密码：p@$$word. 该值必须大于 0。

6 单击**保存**。

编辑 vCenter Single Sign-On 锁定策略

如果用户尝试使用不正确的凭据进行登录，vCenter Single Sign-On 锁定策略会指定用户的 vCenter Single Sign-On 帐户被锁定的时间。管理员可以编辑锁定策略。

如果用户使用错误的密码多次登录 vsphere.local，则将锁定用户。通过锁定策略，管理员可以指定最多失败登录尝试次数，并设置两次失败之间的时间间隔。该策略还可指定在自动解锁帐户之前必须经过的时长。

注 锁定策略仅适用于用户帐户，而不适用于系统帐户（如 administrator@vsphere.local）。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在**单点登录**下，单击**配置**。

4 选择**锁定策略**，然后单击**编辑**。

5 编辑参数。

选项	描述
描述	锁定策略的可选描述。
最多失败登录尝试次数	在锁定帐户之前允许的最多失败登录尝试次数。
两次失败之间的时间间隔	必须发生失败登录尝试才能触发锁定的时间段。
解锁时间	帐户保持锁定状态的时间量。如果输入 0，则管理员必须明确地解锁帐户。

6 单击**保存**。

编辑 vCenter Single Sign-On 令牌策略

vCenter Single Sign-On 令牌策略可以指定令牌属性，如时钟容错和续订计数。您可以编辑令牌策略以确保令牌规范遵从贵公司的安全标准。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在**单点登录**下，单击**配置**。

4 选择**令牌策略**，然后单击**编辑**。

5 编辑令牌策略配置参数。

选项	描述
时钟容错	vCenter Single Sign-On 允许客户端时钟与域控制器时钟之间存在的时差（以毫秒为单位）。如果时差大于指定值，vCenter Single Sign-On 将声明令牌无效。
最大令牌续订计数	可以续订令牌的最大次数。超过最大续订尝试次数后，需要使用新安全令牌。
最大令牌委派计数	可以将密钥所有者令牌委派给 vSphere 环境中的服务。使用委派令牌的服务将代表提供该令牌的主体执行服务。令牌请求指定 DelegateTo 身份。DelegateTo 值可以是解决方案令牌或对解决方案令牌的引用。此值指定可以委派单个密钥所有者令牌的次数。
持有者令牌的最长生命周期	持有者令牌仅根据令牌的占有情况提供身份验证。持有者令牌只能在短期的单个操作中使用。持有者令牌不验证发送请求的用户或实体的身份。此值指定在重新发布持有者令牌之前该令牌的生命周期值。
密钥所有者令牌的最长生命周期	密钥所有者令牌根据令牌中嵌入的安全项目提供身份验证。密钥所有者令牌可用于委派。客户端可以获取密钥所有者令牌并将该令牌委托给其他实体。该令牌包含用于标识请求方和委派方的声明。在 vSphere 环境中，vCenter Server 系统代表用户获取委派的令牌并使用这些令牌执行操作。 此值决定在将密钥所有者令牌标记为无效之前该令牌的生命周期。

6 单击**保存**。

编辑 Active Directory 用户的密码过期通知

Active Directory 密码过期通知与 vCenter Server SSO 密码过期是分开的。Active Directory 用户的默认密码过期通知是 30 天，但实际密码过期取决于您的 Active Directory 系统。vSphere Client 和 vSphere Web Client 控制过期通知。您可以更改默认过期通知以满足您公司的安全标准。

步骤

1 以具有管理员特权的用户身份登录到 vCenter Server 系统。

具有超级管理员角色的默认用户是 root。

2 将目录更改为 `webclient.properties` 文件所在的位置。

操作系统	命令

Linux	■ vSphere Client：
	`cd /etc/vmware/vsphere-ui`
	■ vSphere Web Client：
	`cd /etc/vmware/vsphere-client`

Windows	■ vSphere Client：
	`cd %ALLUSERSPROFILE%\VMware\vCenterServer\cfg\vsphere-ui`
	■ vSphere Web Client：
	`cd %ALLUSERSPROFILE%\VMware\vCenterServer\cfg\vsphere-client`

3 使用文本编辑器打开 `webclient.properties` 文件。

4 编辑以下变量。

```
sso.pending.password.expiration.notification.days = 30
```

5 重新启动客户端。

操作系统	命令

Linux	■ vSphere Client：
	`service-control --stop vsphere-ui`
	`service-control --start vsphere-ui`
	■ vSphere Web Client：
	`service-control --stop vsphere-client`
	`service-control --start vsphere-client`

Windows	■ vSphere Client：
	`cd "C:\Program Files\VMware\vCenter Server\bin\"`
	`service-control --stop vsphere-ui`
	`service-control --start vsphere-ui`
	■ vSphere Web Client：
	`cd "C:\Program Files\VMware\vCenter Server\bin\"`
	`service-control --stop vspherewebclientsvc`
	`service-control --start vspherewebclientsvc`

管理 vCenter Single Sign-On 用户和组

vCenter Single Sign-On 管理员用户可以从 vSphere Client 管理 vsphere.local 域中的用户和组。

vCenter Single Sign-On 管理员用户可以执行以下任务。

- 添加 vCenter Single Sign-On 用户

  vSphere Client 的**用户**选项卡上列出的用户在 vCenter Single Sign-On 内部，属于 vsphere.local 域。您可从 vCenter Single Sign-On 管理界面将用户添加到该域。

- 禁用和启用 vCenter Single Sign-On 用户

  当禁用 vCenter Single Sign-On 用户帐户时，除非管理员启用该帐户，否则用户无法登录到 vCenter Single Sign-On 服务器。您可从一个 vCenter Single Sign-On 管理界面禁用和启用帐户。

- 删除 vCenter Single Sign-On 用户

  可以从 vCenter Single Sign-On 管理界面删除 vsphere.local 域中的用户。无法从 vCenter Single Sign-On 管理界面删除本地操作系统用户或其他域中的用户。

- 编辑 vCenter Single Sign-On 用户

  您可以从 vCenter Single Sign-On 管理界面更改 vCenter Single Sign-On 用户的密码或其他详细信息。无法在 vsphere.local 域中重命名用户。这意味着您无法重命名 administrator@vsphere.local。

- 添加 vCenter Single Sign-On 组

  默认情况下，vCenter Single Sign-On 的**组**选项卡显示本地域 vsphere.local 中的组。如果需要为组成员（主体）创建容器，则可以添加组。

- 向 vCenter Single Sign-On 组添加成员

  vCenter Single Sign-On 组的成员可以是来自一个或多个标识源的用户或其他组。您可以从 vSphere Client 中添加新成员。

- 从 vCenter Single Sign-On 组中移除成员

  可以通过使用 vSphere Client 从 vCenter Single Sign-On 组中移除成员。从组中移除某成员（用户或组）并不是将该成员从系统中删除。

- 删除 vCenter Single Sign-On 解决方案用户

  vCenter Single Sign-On 将显示解决方案用户。解决方案用户是服务集合。系统中已预定义多个 vCenter Server 解决方案用户，且这些解决方案用户通过作为安装的一部分的 vCenter Single Sign-On 进行身份验证。在进行故障排除时，如果没有完全完成卸载，则可以从 vSphere Web Client 删除单个解决方案用户。

- 更改 vCenter Single Sign-On 密码

  本地域（默认为 vsphere.local）中的用户可以从 Web 界面更改其 vCenter Single Sign-On 密码。其他域中的用户更改密码时应遵循对应域的规则。

添加 vCenter Single Sign-On 用户

vSphere Client 的**用户**选项卡上列出的用户在 vCenter Single Sign-On 内部，属于 vsphere.local 域。您可从 vCenter Single Sign-On 管理界面将用户添加到该域。

您可以选择其他域并查看这些域中用户的信息，但您无法从 vCenter Single Sign-On 管理界面将用户添加到其他域。

步骤

1. 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。
2. 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

   如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。
3. 导航到 vCenter Single Sign-On 用户配置 UI。
   a. 在**主页**菜单中，选择**系统管理**。
   b. 在 **Single Sign On** 下，单击**用户和组**。
4. 如果 vsphere.local 不是当前选择的域，请从下拉菜单中选择此域。

   您不能将用户添加到其他域。
5. 在**用户**选项卡上，单击**添加用户**。
6. 输入新用户的用户名和密码。

   创建用户后，将不能更改其用户名。密码必须符合系统的密码策略要求。
7. （可选）输入新用户的名字和姓氏。
8. （可选）输入此用户的电子邮件地址和描述。

9 单击**添加**。

添加某个用户时，该用户最初没有执行管理操作的特权。

后续步骤

将该用户添加到 vsphere.local 域中的一个组，例如可以管理 VMCA 的用户组 (CAAdmins) 或可以管理 vCenter Single Sign-On 的用户组（管理员）。请参见向 vCenter Single Sign-On 组添加成员。

禁用和启用 vCenter Single Sign-On 用户

当禁用 vCenter Single Sign-On 用户帐户时，除非管理员启用该帐户，否则用户无法登录到 vCenter Single Sign-On 服务器。您可从一个 vCenter Single Sign-On 管理界面禁用和启用帐户。

禁用的用户帐户在 vCenter Single Sign-On 系统中仍保持可用，但是用户无法在服务器上登录或执行操作。具有管理员特权的用户可以从 vCenter 的**用户和组**页面中禁用和启用帐户。

前提条件

您必须是 vCenter Single Sign-On 管理员组的成员才能禁用和启用 vCenter Single Sign-On 用户。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到 vCenter Single Sign-On 用户配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在 **Single Sign On** 下，单击**用户和组**。

4 选择一个用户名，单击垂直省略号图标，然后单击**禁用**。

5 单击**确定**。

6 要再次启用用户，请单击垂直省略号图标，单击**启用**，然后单击**确定**。

删除 vCenter Single Sign-On 用户

可以从 vCenter Single Sign-On 管理界面删除 vsphere.local 域中的用户。无法从 vCenter Single Sign-On 管理界面删除本地操作系统用户或其他域中的用户。

小心 如果您删除了 vsphere.local 域中的管理员用户，则将无法再登录 vCenter Single Sign-On。请重新安装 vCenter Server 及其组件。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到 vCenter Single Sign-On 用户配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在 **Single Sign On** 下，单击**用户和组**。

4 选择**用户**，然后从下拉菜单中选择 vsphere.local 域。

5 在用户列表中，选择要删除的用户，然后单击垂直省略号图标。

6 单击**删除**。

请谨慎执行后续操作。您无法撤消此操作。

编辑 vCenter Single Sign-On 用户

您可以从 vCenter Single Sign-On 管理界面更改 vCenter Single Sign-On 用户的密码或其他详细信息。无法在 vsphere.local 域中重命名用户。这意味着您无法重命名 administrator@vsphere.local。

可以使用与 administrator@vsphere.local 相同的特权创建其他用户。

vCenter Single Sign-On 用户存储在 vCenter Single Sign-On vsphere.local 域中。

可从 vCenter Single Sign-On 中查看 vSphere Client 密码策略。从**管理**菜单以 administrator@vsphere.local 身份登录，然后选择**配置 > 策略 > 密码策略**。

另请参见编辑 vCenter Single Sign-On 密码策略。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到 vCenter Single Sign-On 用户配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在 **Single Sign On** 下，单击**用户和组**。

4 单击**用户**。

5 单击垂直省略号图标，然后选择**编辑**。

6 编辑用户属性。

您不能更改用户的用户名。

密码必须符合系统的密码策略要求。

7 单击**确定**。

添加 vCenter Single Sign-On 组

默认情况下，vCenter Single Sign-On 的**组**选项卡显示本地域 vsphere.local 中的组。如果需要为组成员（主体）创建容器，则可以添加组。

您无法从 vCenter Single Sign-On 的**组**选项卡将组添加到其他域，如 Active Directory 域。

如果未将标识源添加到 vCenter Single Sign-On，则创建组和添加用户可以帮助您组织本地域。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到 vCenter Single Sign-On 用户配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在 **Single Sign On** 下，单击**用户和组**。

4 选择**组**，然后单击**添加组**。

5 输入组的名称和描述。

创建组后，将不能更改组名称。

6 单击**添加**。

后续步骤

- 向组添加成员。

向 vCenter Single Sign-On 组添加成员

vCenter Single Sign-On 组的成员可以是来自一个或多个标识源的用户或其他组。您可以从 vSphere Client 中添加新成员。

有关背景信息，请参见 VMware 知识库文章，网址为 http://kb.vmware.com/kb/2095342。

在 Web 界面的**组**选项卡上列出的组是 vsphere.local 域的一部分。请参见 vCenter Single Sign-On 域中的组。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到 vCenter Single Sign-On 用户配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在 **Single Sign On** 下，单击**用户和组**。

4 单击**组**，然后单击相关组（例如“管理员”）。

5 在“组成员”区域中，单击**添加成员**。

6 选择包含要添加到组中的成员的标识源。

7 （可选）输入搜索词，然后单击**搜索**。

8 选择成员。

您可添加多个成员。

9 单击**确定**。

从 vCenter Single Sign-On 组中移除成员

可以通过使用 vSphere Client 从 vCenter Single Sign-On 组中移除成员。从组中移除某成员（用户或组）并不是将该成员从系统中删除。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到 vCenter Single Sign-On 用户配置 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在 **Single Sign On** 下，单击**用户和组**。

4 选择**组**，然后单击一个组。

5 在组成员列表中，选择要移除的用户或组，然后单击垂直省略号图标。

6 单击**移除成员**。

7 单击**移除**。

用户将从组中移除，但在系统中仍然可用。

删除 vCenter Single Sign-On 解决方案用户

vCenter Single Sign-On 将显示解决方案用户。解决方案用户是服务集合。系统中已预定义多个 vCenter Server 解决方案用户，且这些解决方案用户通过作为安装的一部分的 vCenter Single Sign-On 进行身份验证。在进行故障排除时，如果没有完全完成卸载，则可以从 vSphere Web Client 删除单个解决方案用户。

如果从环境中移除与 vCenter Server 解决方案用户或第三方解决方案用户关联的服务集，则该解决方案用户将从 vSphere Web Client 显示中移除。如果您强制移除某个应用程序，或者如果当解决方案用户仍在系统中时系统变为不可恢复，则您可以从 vSphere Web Client 中明确移除该解决方案用户。

重要 如果删除解决方案用户，则相应的服务将无法再通过 vCenter Single Sign-On 进行身份验证。

步骤

1 使用 vSphere Web Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到 vCenter Single Sign-On 用户配置 UI。

   a 在**主页**菜单中，选择**系统管理**。

   b 在 **Single Sign-On** 下，单击**用户和组**。

4 单击**解决方案用户**选项卡，然后单击解决方案用户名。

5 单击**删除解决方案用户**图标。

6 单击**是**。

与该解决方案用户关联的服务将不再能够访问 vCenter Server，并且无法发挥 vCenter Server 服务的作用。

更改 vCenter Single Sign-On 密码

本地域（默认为 vsphere.local）中的用户可以从 Web 界面更改其 vCenter Single Sign-On 密码。其他域中的用户更改密码时应遵循对应域的规则。

vCenter Single Sign-On 锁定策略可以决定密码何时到期。默认情况下，vCenter Single Sign-On 用户密码在 90 天后过期，但管理员密码（如 administrator@vsphere.local 的密码）不会过期。密码即将到期时，vCenter Single Sign-On 管理界面将显示警告。

注 仅当密码未过期时才能更改密码。

如果密码已过期，本地域的管理员（默认为 administrator@vsphere.local）可以通过使用 `dir-cli password reset` 命令重置密码。只有 vCenter Single Sign-On 域的管理员组的成员才能重置密码。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

   如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 在上方的导航窗格中“帮助”菜单的右侧，单击您的用户名以弹出下拉菜单。

   除此之外，还可以选择 **Single Sign-On > 用户和组**，然后从垂直省略号菜单中选择**编辑用户**。

4 选择**更改密码**，然后键入您的新密码。

5 键入新密码并确认。

   该密码必须符合密码策略。

6 单击**确定**。

vCenter Single Sign-On 安全性最佳做法

遵循 vCenter Single Sign-On 安全性最佳做法以保护 vSphere 环境。

vSphere 身份验证基础架构可增强 vSphere 环境的安全性。要确保该基础架构不受危害，请遵循 vCenter Single Sign-On 最佳做法。

检查密码到期

vCenter Single Sign-On 默认密码策略的密码生命周期为 90 天。90 天之后，密码会过期，且您无法再登录。检查是否过期并及时刷新密码。

配置 NTP

确保所有系统使用相同的相对时间源（包括相关本地化偏移），且相对时间源可以与商定的时间标准（如协调世界时—UTC）相互关联。系统同步对于 vCenter Single Sign-On 证书有效性以及其他 vSphere 证书的有效性至关重要。

使用 NTP，还可以更轻松地跟踪日志文件中的入侵者。不正确的时间设置可能难以检查和关联日志文件以检测攻击，且可能使得审核不准确。

vSphere 安全证书

3

vSphere 通过使用证书来加密通信，对服务进行身份验证，以及对令牌进行签名来提供安全性。

vSphere 使用证书：

- 两个节点之间的加密通信，例如 vCenter Server 和 ESXi 主机之间。
- 对 vSphere 服务进行身份验证。
- 执行内部操作，如对令牌进行签名。

vSphere 的内部证书颁发机构 VMware Certificate Authority (VMCA) 提供 vCenter Server 和 ESXi 所需的所有证书。每一个 Platform Services Controller 上均安装了 VMCA，其可立即确保解决方案的安全，而不进行任何其他修改。保留此默认配置可为证书管理提供最低操作开销。vSphere 提供了一种机制，用于在这些证书过期时进行续订。

vSphere 还提供了一种机制，用于将某些证书替换为您自己的证书。但是，仅替换在节点之间提供加密的 SSL 证书，以保持较低的证书管理开销。

建议使用以下选项管理证书。

表 3-1. 建议用于管理证书的选项

模式	描述	优势
VMCA 默认证书	VMCA 为 vCenter Server 和 ESXi 主机提供所有证书。	最简单和最低开销。VMCA 可以管理 vCenter Server 和 ESXi 主机的证书生命周期。
使用外部 SSL 证书的 VMCA 默认证书（混合模式）	替换 Platform Services Controller 和 vCenter Server Appliance 的 SSL 证书，并允许 VMCA 管理解决方案用户和 ESXi 主机的证书。（可选）对于安全性很重要的部署，还可以替换 ESXi 主机的 SSL 证书。	简单且安全。VMCA 会管理内部证书，但您可以获得使用企业批准的 SSL 证书，并让浏览器信任这些证书的好处。

VMware 建议，既不要替换解决方案用户证书或 STS 证书，也不要使用辅助 CA 取代 VMCA。如果选择任意一种选项，您都可能会遇到很大复杂性和对安全产生负面影响的可能性，以及不必要地提高操作风险。有关管理 vSphere 环境内的证书的更多信息，请参见标题为 New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement 的博客帖子，网址为 http://vmware.com/go/hybridvmca。

可以使用以下选项替换现有证书：

表 3-2. 不同的证书替换方法

选项	请参见
使用 vSphere Client。从 vSphere 6.7 开始，将通过 vSphere Client 管理 Platform Services Controller。	使用 vSphere Client 管理证书
从命令行使用 vSphere 证书管理器实用程序。	使用 vSphere 证书管理器实用程序管理证书
使用 CLI 命令执行手动证书替换。	第 4 章，使用 CLI 命令管理服务和证书

vSphere 证书管理 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere6_cert_infrastructure)

本章讨论了以下主题：

- 不同解决方案途径的证书要求
- 证书管理概览
- 使用 vSphere Client 管理证书
- 从 vSphere Web Client 管理证书
- 使用 vSphere 证书管理器实用程序管理证书
- 手动证书替换

不同解决方案途径的证书要求

证书要求取决于是使用 VMCA 作为中间 CA，还是使用自定义证书。对于计算机证书和解决方案用户证书，要求也有所不同。

在开始之前，请确保环境中所有节点的时间都已同步。

对所有已导入证书的要求

- 密钥大小：2048 位或更大（PEM 编码）
- PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。将密钥添加到 VECS 时，它们将转换为 PKCS8。
- x509 版本 3
- SubjectAltName 必须包含 DNS Name=*machine_FQDN*
- CRT 格式
- 包含以下密钥用法：数字签名、密钥加密。
- “增强型密钥用法”可以为空或包含服务器身份验证。

VMCA 不支持以下证书。

- 使用通配符的证书
- 不建议使用的算法包括 md2WithRSAEncryption 1.2.840.113549.1.1.2、md5WithRSAEncryption 1.2.840.113549.1.1.4 和 sha1WithRSAEncryption 1.2.840.113549.1.1.5。

- 不支持 OID 为 1.2.840.113549.1.1.10 的算法 RSASSA-PSS。

证书符合 RFC 2253 规范

证书必须符合 RFC 2253 规范。

如果不使用 Certificate Manager 生成 CSR，请确保 CSR 包括以下字段。

String	X.500 AttributeType
CN	commonName
L	localityName
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName
C	countryName
STREET	streetAddress
DC	domainComponent
UID	userid

如果使用 Certificate Manager 生成 CSR，系统会提示您输入以下信息，然后 Certificate Manager 将对应的字段添加到 CSR 文件。

- administrator@vsphere.local 用户的密码或者要连接到的 vCenter Single Sign-On 域的管理员的密码。
- 如果您要在具有外部 Platform Services Controller 的环境中生成 CSR，则系统会提示您输入 Platform Services Controller 的主机名或 IP 地址。
- Certificate Manager 存储在 `certool.cfg` 文件中的信息。对于大多数字段，可以接受默认值或提供特定于站点的值。计算机的 FQDN 为必需值。
  - administrator@vsphere.local 的密码。
  - 两个字母组成的国家/地区代码
  - 公司名称
  - 组织名称
  - 组织单位
  - 省/市/自治区
  - 地区
  - IP 地址（可选）
  - 电子邮件
  - 主机名，即要替换证书的计算机的完全限定域名。如果主机名与 FQDN 不匹配，则证书替换无法正确完成，且环境可能最终会处于不稳定状态。
  - Platform Services Controller 的 IP 地址（如果要在 vCenter Server（管理）节点上运行该命令）

使用 VMCA 作为中间 CA 时的要求

当您将 VMCA 用作中间 CA 时，证书必须满足以下要求。

证书类型	证书要求
根证书	■ 可以使用 vSphere Certificate Manager 创建 CSR。请参见使用 vSphere 证书管理器生成 CSR 并准备根证书（中间 CA）。 ■ 如果希望手动创建 CSR，则发送以进行签名的证书必须满足以下要求： ■ 密钥大小：2048 位或更大 ■ PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。密钥添加到 VECS 后，会转换为 PKCS8。 ■ x509 版本 3 ■ 如果您当前使用的是自定义证书，对于根证书，CA 扩展必须设置为 true，并且证书签名必须在要求列表中。 ■ 必须启用 CRL 签名。 ■ “增强型密钥用法”可以为空或包含服务器身份验证。 ■ 对证书链的长度没有明确限制。VMCA 使用 OpenSSL 默认设置，即 10 个证书。 ■ 不支持包含通配符或多个 DNS 名称的证书。 ■ 不能创建 VMCA 的附属 CA。 请参见 http://kb.vmware.com/kb/2112009 中的 VMware 知识库文章，《在 vSphere 6.0 中创建 Microsoft 证书颁发机构模板以创建 SSL 证书》以获取使用 Microsoft 证书颁发机构的示例。
计算机 SSL 证书	可以使用 vSphere Certificate Manager 创建 CSR，或者手动创建 CSR。 如果手动创建 CSR，它必须满足前面在对所有已导入证书的要求下列出的要求。您还必须为主机指定 FQDN。
解决方案用户证书	可以使用 vSphere Certificate Manager 创建 CSR，或者手动创建 CSR。 **注** 您必须为每个解决方案用户的名称使用不同的值。如果手动生成证书，可能会在**主体**下显示为 **CN**，具体取决于使用的工具。 如果使用 vSphere Certificate Manager，该工具将提示您输入每个解决方案用户的证书信息。vSphere Certificate Manager 将信息存储在 `certool.cfg` 中。请参见 Certificate Manager 提示输入的信息。

对自定义证书的要求

当您希望使用自定义证书时，这些证书必须满足以下要求。

证书类型	证书要求
计算机 SSL 证书	每个节点上的计算机 SSL 证书必须包含来自第三方或企业 CA 的单独证书。 ■ 您可以使用 vSphere Certificate Manager 生成 CSR，或手动创建 CSR。CSR 必须满足前面在对导入的所有证书的要求下列出的要求。 ■ 如果使用 vSphere Certificate Manager，该工具将提示您输入每个解决方案用户的证书信息。vSphere Certificate Manager 将信息存储在 `certool.cfg` 中。请参见 Certificate Manager 提示输入的信息。 ■ 对于大多数字段，可以接受默认值或提供特定于站点的值。计算机的 FQDN 为必需值。
解决方案用户证书	每个节点上的每个解决方案用户必须具有来自第三方或企业 CA 的单独证书。 ■ 您可以使用 vSphere Certificate Manager 生成 CSR，或自己准备 CSR。CSR 必须满足前面在对导入的所有证书的要求下列出的要求。 ■ 如果使用 vSphere Certificate Manager，该工具将提示您输入每个解决方案用户的证书信息。vSphere Certificate Manager 将信息存储在 `certool.cfg` 中。请参见 Certificate Manager 提示输入的信息。 注 您必须为每个解决方案用户的名称使用不同的值。手动生成的证书可能会在**主体**下显示为 **CN**，具体取决于使用的工具。 稍后将解决方案用户证书替换为自定义证书时，请提供第三方 CA 的完整签名证书链。

注 不要在任何自定义证书中使用 CRL 分发点、授权信息访问或证书模板信息。

证书管理概览

设置或更新证书基础架构所需的工作取决于您的环境中的要求。必须考虑执行全新安装还是升级，以及考虑使用 ESXi 还是 vCenter Server。

未替换 VMware 证书的管理员

VMCA 可以处理所有证书管理。VMCA 使用将 VMCA 用作根证书颁发机构的证书置备 vCenter Server 组件和 ESXi 主机。如果要从之前版本的 vSphere 升级到 vSphere 6，所有自签名证书都会替换为由 VMCA 签名的证书。

如果您当前未替换 VMware 证书，环境将开始使用 VMCA 签名的证书而非自签名证书。

将 VMware 证书替换为自定义证书的管理员

对于全新安装，如果公司策略需要第三方或企业 CA 签名的证书或需要自定义证书信息，则您有以下几种选择。

- 由第三方 CA 或企业 CA 签发 VMCA 根证书。将 VMCA 根证书替换为该签名证书。在这种情况下，VMCA 证书是中间证书。VMCA 使用包含完整证书链的证书置备 vCenter Server 组件和 ESXi 主机。
- 如果公司策略不允许证书链中出现中间证书，可以明确替换这些证书。可以使用 vSphere Client、vSphere Certificate Manager 实用程序，或使用证书管理 CLI 手动替换证书。

升级使用自定义证书的环境时，可以保留某些证书。

- ESXi 主机在升级过程中保留其自定义证书。确保 vCenter Server 升级过程将所有相关根证书添加到 vCenter Server 上的 VECS 中的 TRUSTED_ROOTS 存储。

  升级到 vSphere 6.0 或更高版本之后，可以将证书模式设置为**自定义**。如果证书模式是默认的 VMCA，且用户从 vSphere Client 执行证书刷新，VMCA 签名证书将替换自定义证书。

- 对于 vCenter Server 组件，具体取决于现有环境。
  - 如果将简单安装升级为嵌入式部署，vCenter Server 将保留自定义证书。升级后，环境的运行方式不变。
  - 如果升级多站点部署，vCenter Single Sign-On 可与其他 vCenter Server 组件位于不同计算机上。在这种情况下，升级过程会创建包含一个 Platform Services Controller 节点和一个或多个管理节点的多节点部署。

    此方案将保留现有 vCenter Server 和 vCenter Single Sign-On 证书。这些证书将用作计算机 SSL 证书。

    此外，VMCA 将 VMCA 签名证书分配给每个解决方案用户（vCenter 服务的集合）。解决方案用户仅使用此证书对 vCenter Single Sign-On 进行身份验证。公司策略通常不要求替换解决方案用户证书。

  不再使用适用于 vSphere 5.5 安装的 vSphere 5.5 证书替换工具。新架构导致不同服务分布和放置。新命令行实用程序 vSphere Certificate Manager 适用于大多数证书管理任务。

vSphere 证书界面

对于 vCenter Server，可以使用以下工具和界面查看和替换证书。

表 3-3. 用于管理 vCenter Server 证书的界面

接口	适用情况
vSphere Client	使用图形用户界面执行常见证书任务。
vSphere Certificate Manager 实用程序	从 vCenter Server 安装的命令行执行常见证书替换任务。
证书管理 CLI	使用 `dir-cli`、`certool` 和 `vecs-cli` 执行所有证书管理任务。
vSphere Web Client	查看证书，包括过期信息。

对于 ESXi，从 vSphere Client 执行证书管理。VMCA 会置备证书并将其存储在 ESXi 主机本地。VMCA 不将 ESXi 主机证书存储在 VMDIR 或 VECS 中。请参见《vSphere 安全性》文档。

受支持的 vCenter 证书

对于 vCenter Server、Platform Services Controller 及相关的计算机和服务，支持以下证书：

- 由 VMware Certificate Authority (VMCA) 生成和签名的证书。
- 自定义证书。
  - 从内部 PKI 生成的企业证书。
  - 由外部 PKI（如 Verisign、GoDaddy 等）生成的第三方 CA 签名证书。

使用不包含根 CA 的 OpenSSL 创建的自签名证书不受支持。

证书替换概述

可以根据公司策略和正配置的系统的要求来执行不同类型的证书替换。可以使用 vSphere 证书管理器实用程序从 Platform Services Controller 执行证书替换，也可以通过使用安装中包含的 CLI 手动执行证书替换。

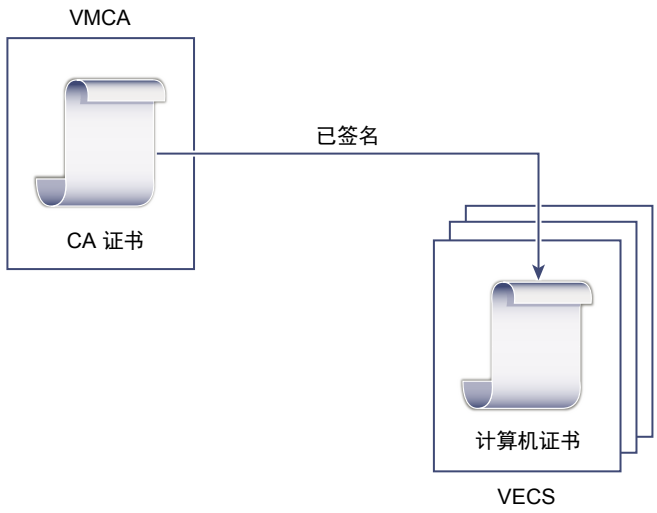
VMCA 包含在每个 Platform Services Controller 和每个嵌入式部署中。VMCA 可置备每个节点、每个 vCenter Server 解决方案用户，以及每个使用由 VMCA 签名的证书作为证书颁发机构的 ESXi 主机。vCenter Server 解决方案用户是 vCenter Server 服务组。

可以替换默认证书。对于 vCenter Server 组件，可以使用安装中包含的一组命令行工具。您具有多个选择。

替换为 VMCA 签名的证书

如果 VMCA 证书过期或由于其他原因要对其进行替换，可以使用证书管理 CLI 执行此过程。默认情况下，VMCA 根证书有效期为十年，且 VMCA 签名的所有证书都会在根证书过期时过期，即有效期最长为十年。

图 3-1. 由 VMCA 签名的证书存储在 VECS 中



您可以使用以下 vSphere 证书管理器选项：

- 将计算机 SSL 证书替换为 VMCA 证书

- 将解决方案用户证书替换为 VMCA 证书

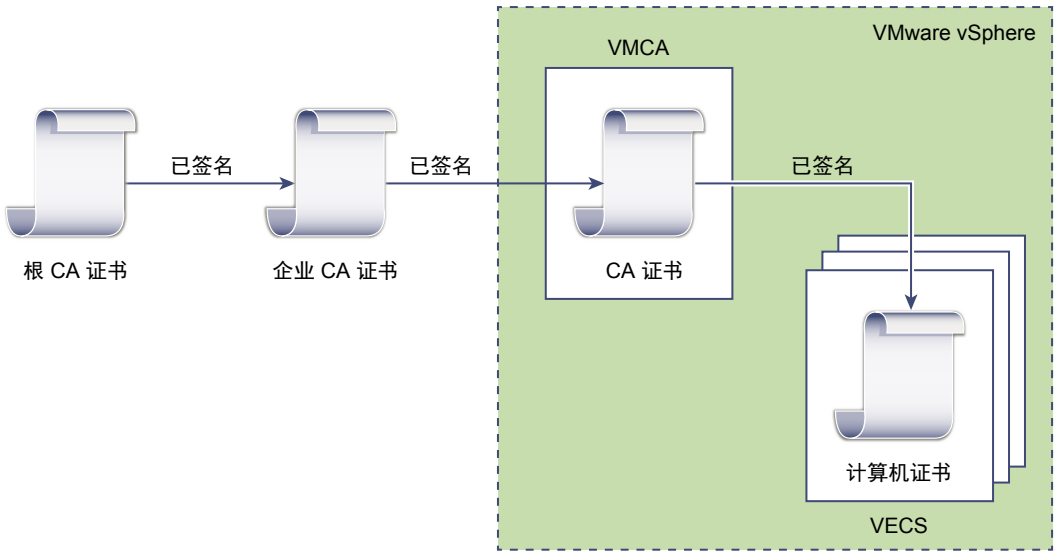
有关手动证书替换，请参见将现有 VMCA 签名证书替换为新的 VMCA 签名证书。

使 VMCA 成为中间 CA

您可以将 VMCA 根证书替换为由企业 CA 或第三方 CA 签名的证书。VMCA 在每次置备证书时都会签署自定义根证书，从而使 VMCA 成为中间 CA。

注 如果执行包含外部 Platform Services Controller 的全新安装，请首先安装 Platform Services Controller，并替换 VMCA 根证书。接下来，安装其他服务或将 ESXi 主机添加到环境中。如果执行包含嵌入式 Platform Services Controller 的全新安装，请在添加 ESXi 主机之前替换 VMCA 根证书。如果这样做，则 VMCA 会对整个链进行签名，且不必生成新证书。

图 3-2. 由第三方或企业 CA 签名的证书使用 VMCA 作为中间 CA



您可以使用以下 vSphere 证书管理器选项：

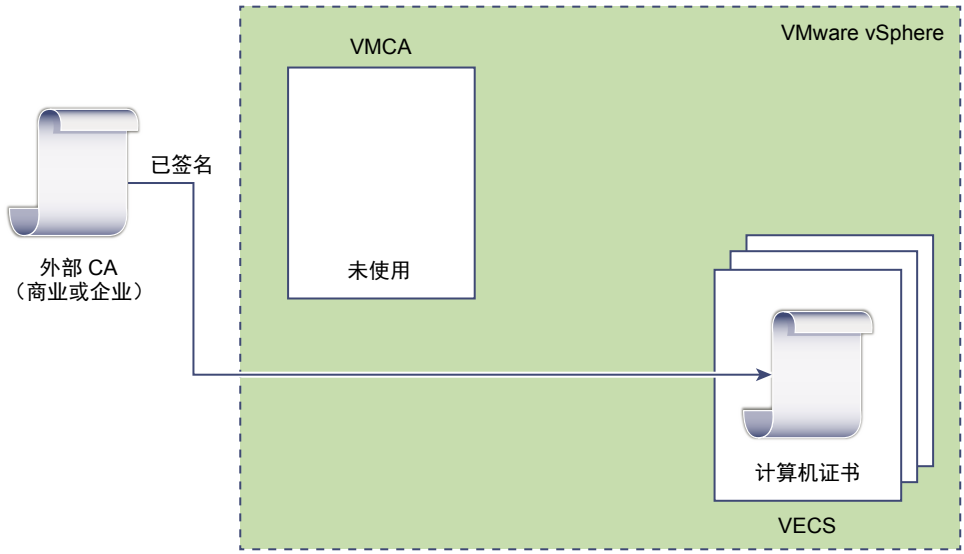
- 将 VMCA 根证书替换为自定义签名证书并替换所有证书
- 将计算机 SSL 证书替换为 VMCA 证书（多节点部署）
- 将解决方案用户证书替换为 VMCA 证书（多节点部署）

有关手动证书替换，请参见使用 VMCA 作为中间证书颁发结构。

不要使用 VMCA，使用自定证书进行置备

您可以将现有的 VMCA 签名证书替换为自定义证书。如果使用此方法，则您必须负责置备和监控所有证书。

图 3-3. 外部证书直接存储在 VECS 中



您可以使用以下 vSphere 证书管理器选项：

- 将计算机 SSL 证书替换为自定义证书
- 将解决方案用户证书替换为自定义证书

有关手动证书替换，请参见在 vSphere 中使用自定义证书。

混合部署

您可以让 VMCA 提供一些证书，但对基础架构的其他部分使用自定义证书。例如，由于解决方案用户证书仅用于对 vCenter Single Sign-On 进行身份验证，请考虑让 VMCA 置备这些证书。将计算机 SSL 证书替换为自定义证书以确保所有 SSL 流量的安全。

公司策略通常不允许使用中间 CA。在这些情况下，混合部署是一种有效的解决方案。它会最大程度地减少要替换的证书数量并确保所有流量的安全。混合部署只保留内部流量，即解决方案用户流量，以便使用默认的 VMCA 签名证书。

ESXi 证书替换

对于 ESXi 主机，您可以从 vSphere Client 更改证书置备行为。有关详细信息，请参见《vSphere 安全性》文档。

表 3-4. ESXi 证书替换选项

选项	描述
VMware Certificate Authority 模式（默认值）	从 vSphere Client 续订证书时，VMCA 将为主机颁发证书。如果已将 VMCA 根证书更改为包含证书链，则主机证书将包含完整链。
自定义证书颁发机构模式	允许您手动更新和使用未签名或由 VMCA 颁发的证书。
指纹模式	可用于在刷新期间保留 5.5 证书。仅在调试情况下临时使用此模式。

vSphere 用户证书的位置

在 vSphere 6.0 及更高版本中，VMware Certificate Authority (VMCA) 会使用证书置备您的环境。证书包括用于安全连接的计算机 SSL 证书，对 vCenter Single Sign-On 进行服务身份验证的解决方案用户证书，以及 ESXi 主机的证书。

以下证书正在使用中。

表 3-5. vSphere 6.0 及更高版本中的证书

证书	已置备	备注
ESXi 证书	VMCA（默认）	存储在 ESXi 主机本地
计算机 SSL 证书	VMCA（默认）	存储在 VECS 中
解决方案用户证书	VMCA（默认）	存储在 VECS 中
vCenter Single Sign-On SSL 签名证书	在安装期间置备。	在 vSphere Web Client 中管理此证书。 **注** 请勿在文件系统中更改此证书，否则可能导致不可预知的行为结果。
VMware Directory Service (VMDIR) SSL 证书	在安装期间置备。	从 vSphere 6.5 开始，计算机 SSL 证书将被用作 vmdir 证书。

ESXi

ESXi 证书存储在每个主机本地中的 `/etc/vmware/ssl` 目录下。默认情况下，ESXi 证书由 VMCA 置备，但也可以使用自定义证书。当首次将主机添加到 vCenter Server 时以及当主机重新连接时，会置备 ESXi 证书。

计算机 SSL 证书

每个节点的计算机 SSL 证书用于在服务器端上创建 SSL 套接字。SSL 客户端连接到 SSL 套接字。该证书用于服务器验证和安装通信，如 HTTPS 或 LDAPS。

每个节点都有自己的计算机 SSL 证书。节点包括 vCenter Server 实例、Platform Services Controller 实例或嵌入式部署实例。节点上正在运行的所有服务均使用该计算机 SSL 证书公开其 SSL 端点。

以下服务使用该计算机 SSL 证书。

- Platform Services Controller 节点上的反向代理服务。与各个 vCenter 服务的 SSL 连接始终会转到反向代理。流量不会转到服务自身。
- 管理节点和嵌入式节点上的 vCenter 服务 (vpxd)。
- 基础架构节点和嵌入式节点上的 VMware Directory Service (vmdir)。

VMware 产品使用标准 X.509 版本 3 (X.509v3) 证书来加密会话信息。会话信息通过组件之间的 SSL 发送。

解决方案用户证书

解决方案用户封装一个或多个 vCenter Server 服务。每个解决方案用户都必须对 vCenter Single Sign-On 进行身份验证。解决方案用户通过 SAML 令牌交换使用证书对 vCenter Single Sign-On 进行身份验证。

在首次必须进行身份验证时，在重新引导后以及在超时结束后，解决方案用户向 vCenter Single Sign-On 提供证书。可以在 vSphere Web Client 中设置超时（密钥所有者超时），默认值为 2592000 秒（30 天）。

例如，在连接到 vCenter Single Sign-On 时，vpxd 解决方案用户向 vCenter Single Sign-On 提供其证书。vpxd 解决方案用户从 vCenter Single Sign-On 收到一个 SAML 令牌，然后使用该令牌对其他解决方案用户和服务进行身份验证。

以下解决方案用户证书存储包括在每个管理节点和每个嵌入式部署的 VECS 中：

- `machine`：由组件管理器、许可证服务器和日志记录服务使用。

  注 Machine 解决方案用户证书与计算机 SSL 证书没有任何关系。计算机解决方案用户证书用于进行 SAML 令牌交换。计算机 SSL 证书用于计算机的安全 SSL 连接。

- `vpxd`：vCenter 服务守护程序 (vpxd) 存储位于管理节点和嵌入式部署上。vpxd 使用此存储中存储的解决方案用户证书对 vCenter Single Sign-On 进行身份验证。
- `vpxd-extension`：vCenter 扩展存储。包括 Auto Deploy 服务、Inventory Service 以及不属于其他解决方案用户的其他服务。
- `vsphere-webclient`：vSphere Web Client 存储。还包括其他一些服务，例如性能图表服务。

每个 Platform Services Controller 节点包含一个 `machine` 证书。

内部证书

vCenter Single Sign-On 证书未存储在 VECS 中，并且未使用证书管理工具进行管理。一般说来，无需进行更改，但在特殊情况下，可以替换这些证书。

vCenter Single Sign-On 签名证书

vCenter Single Sign-On 服务包括身份提供程序服务，该提供程序可发布用于在整个 vSphere 进行身份验证的 SAML 令牌。SAML 令牌表示用户的身份，还包含组成员资格信息。在 vCenter Single Sign-On 发布 SAML 令牌时，它将使用其签名证书对每个令牌进行签名，以便 vCenter Single Sign-On 的客户端可以验证 SAML 令牌是否来自可信源。

vCenter Single Sign-On 向解决方案用户发布密钥所有者 SAML 令牌并向其他用户发布持有者令牌，使用用户名和密码进行登录。

可以在 vSphere Web Client 中替换此证书。请参见刷新 Security Token Service 证书。

VMware Directory Service SSL 证书

从 vSphere 6.5 开始，计算机 SSL 证书将被用作 VMware 目录证书。对于 vSphere 的早期版本，请参见相应的文档。

vSphere 虚拟机加密证书

vSphere 虚拟机加密解决方案与外部密钥管理服务器 (KMS) 连接。根据该解决方案对 KMS 进行身份验证的方式，可能会生成证书并将其存储在 VECS 中。请参见《vSphere 安全性》文档。

VMCA 和 VMware 核心标识服务

核心标识服务是每个嵌入式部署和每个平台服务节点的一部分。VMCA 是每个 VMware 核心标识服务组的一部分。使用管理 CLI 和 vSphere Client 与这些服务进行交互。

VMware 核心标识服务包括多个组件。

表 3-6. 核心标识服务

服务	描述	包括在
VMware Directory Service (vmdir)	处理 SAML 证书管理以进行 vCenter Single Sign-On 身份验证。	Platform Services Controller 嵌入式部署
VMware Certificate Authority (VMCA)	颁发 VMware 解决方案用户的证书、正在运行服务的计算机的计算机证书以及 ESXi 主机证书。VMCA 可以立即使用或作为中间证书颁发机构。 VMCA 仅会对可以在同一域中对 vCenter Single Sign-On 进行身份验证的客户端颁发证书。	Platform Services Controller 嵌入式部署
VMware Authentication Framework 守护进程 (VMAFD)	包括 VMware Endpoint 证书存储 (VECS) 和其他一些身份验证服务。VMware 管理员与 VECS 进行交互。在内部使用其他服务。	Platform Services Controller vCenter Server 嵌入式部署

VMware Endpoint 证书存储概述

VMware Endpoint 证书存储 (VECS) 充当可以存储在密钥库中的证书、专用密钥以及其他证书信息的本地（客户端）存储库。可以选择不使用 VMCA 作为证书颁发机构和证书签名者，但必须使用 VECS 存储所有 vCenter 证书、密钥等。ESXi 证书存储在每个本地主机中，而不是 VECS 中。

VECS 作为 VMware Authentication Framework 守护进程 (VMAFD) 的一部分运行。VECS 在每个嵌入式部署、Platform Services Controller 节点以及管理节点上运行，并保留包含证书和密钥的密钥库。

VECS 会定期轮询 VMware Directory Service (vmdir)，以获取对受信任的根存储的更新。还可以使用 `vecs-cli` 命令显式管理 VECS 中的证书和密钥。请参见 vecs-cli 命令参考。

VECS 包括以下库。

表 3-7. VECS 中的库

库	描述
计算机 SSL 库 (MACHINE_SSL_CERT)	■ 由每个 vSphere 节点上的反向代理服务使用。 ■ 由 VMware Directory Service (vmdir) 在嵌入式部署和每个 Platform Services Controller 节点上使用。 vSphere 6.0 及更高版本中的所有服务通过使用计算机 SSL 证书的反向代理进行通信。为了实现向后兼容性，5.x 服务仍使用特定端口。因此，某些服务（如 vpxd）仍使其自身的端口处于打开状态。
受信任的根存储 (TRUSTED_ROOTS)	包含所有受信任的根证书。

表 3-7. VECS 中的库（续）

库	描述
解决方案用户库 ■ machine ■ vpxd ■ vpxd-extension ■ vsphere-webclient	VECS 为每个解决方案用户提供一个库。每个解决方案用户证书的主体必须是唯一的，例如 machine 证书不能具有与 vpxd 证书相同的主体。 解决方案用户证书用于对 vCenter Single Sign-On 进行身份验证。vCenter Single Sign-On 会检查证书是否有效，但不检查其他证书属性。在嵌入式部署中，所有解决方案用户证书都位于相同的系统中。 以下解决方案用户证书存储包括在每个管理节点和每个嵌入式部署的 VECS 中： ■ machine：由组件管理器、许可证服务器和日志记录服务使用。 注 Machine 解决方案用户证书与计算机 SSL 证书没有任何关系。计算机解决方案用户证书用于进行 SAML 令牌交换。计算机 SSL 证书用于计算机的安全 SSL 连接。 ■ vpxd：vCenter 服务守护程序 (vpxd) 存储位于管理节点和嵌入式部署上。vpxd 使用此存储中存储的解决方案用户证书对 vCenter Single Sign-On 进行身份验证。 ■ vpxd-extension：vCenter 扩展存储。包括 Auto Deploy 服务、Inventory Service 以及不属于其他解决方案用户的其他服务。 ■ vsphere-webclient：vSphere Web Client 存储。还包括其他一些服务，例如性能图表服务。 每个 Platform Services Controller 节点包含一个 machine 证书。
vSphere 证书管理器实用程序备份库 (BACKUP_STORE)	由 VMCA（VMware 证书管理器）用来支持证书恢复。仅将最近的状态存储为备份，无法返回多个步骤。
其他库	解决方案可能会添加其他库。例如，Virtual Volumes 解决方案会添加 SMS 库。请勿修改这些库中的证书，除非 VMware 文档或 VMware 知识库文章要求进行此类修改。 注 删除 TRUSTED_ROOTS_CRLS 存储可能会损坏证书基础架构。请勿删除或修改 TRUSTED_ROOTS_CRLS 存储。

vCenter Single Sign-On 服务会在磁盘上存储令牌签名证书及其 SSL 证书。可以从 vSphere Client 更改令牌签名证书。

某些证书在启动期间可以临时或永久存储在文件系统中。请勿更改文件系统上的证书。使用 vecs-cli 可在存储在 VECS 中的证书上执行操作。

注 请勿更改磁盘上的任何证书文件，除非 VMware 文档或知识库文章要求这样做。否则，可能会导致不可预知的行为。

管理证书吊销

如果怀疑您的其中一个证书已受到影响，请替换所有现有证书，包括 VMCA 根证书。

vSphere 6.0 支持替换证书，但不会强制吊销 ESXi 主机或 vCenter Server 系统的证书。

从所有节点中移除已吊销证书。如果未移除已吊销证书，则中间人攻击可能会通过模拟帐户凭据而感染系统。

大型部署中的证书替换

包括多个管理节点以及一个或多个 Platform Services Controller 节点的部署中的证书替换类似于嵌入式部署中的替换。在这两种情况下，均可使用 vSphere 证书管理实用程序或手动替换证书。某些最佳做法可指导该替换过程。

在包含负载平衡器的 High Availability 环境中替换证书

在少于 8 个 vCenter Server 系统的环境中，您通常可以部署单个 Platform Services Controller 实例和关联的 vCenter Single Sign-On 服务。在较大环境中，可考虑使用受网络负载平衡器保护的多个 Platform Services Controller 实例。VMware 网站上的白皮书《vCenter Server 6.0 部署指南》介绍了此设置。

具有多个管理节点的环境中的计算机 SSL 证书替换

如果您的环境中包括多个管理节点和一个 Platform Services Controller，可以使用 vSphere Certificate Manager 实用程序替换证书或使用 vSphere CLI 命令手动替换证书。

vSphere Certificate Manager

在每台计算机上运行 vSphere Certificate Manager。在管理节点上，按提示输入的 Platform Services Controller 的 IP 地址。根据您所执行的任务，也可能提示您输入证书信息。

手动证书替换

对于手动证书替换，可以在每台计算机上运行证书替换命令。在管理节点上，必须使用 `--server` 参数指定 Platform Services Controller。有关详细信息，请参见以下主题：

- 将计算机 SSL 证书替换为 VMCA 签名证书
- 替换计算机 SSL 证书（中间 CA）
- 将计算机 SSL 证书替换为自定义证书

具有多个管理节点的环境中的解决方案用户证书替换

如果您的环境中包括多个管理节点和一个 Platform Services Controller，请遵循以下步骤进行证书替换。

注 在大型部署中列出解决方案用户证书时，`dir-cli list` 的输出包括所有节点的所有解决方案用户。运行 `vmafd-cli get-machine-id --server-name localhost` 以查找每个主机的本地计算机 ID。每个解决方案用户名称均包括计算机 ID。

vSphere Certificate Manager

在每台计算机上运行 vSphere Certificate Manager。在管理节点上，按提示输入的 Platform Services Controller 的 IP 地址。根据您所执行的任务，也可能提示您输入证书信息。

手动证书替换

1 生成或请求证书。需要以下证书：

- Platform Services Controller 上计算机解决方案用户的证书。

- 每个管理节点上计算机解决方案用户的证书。
- 每个管理节点上以下每个解决方案用户的证书：
  - `vpxd solution` 用户
  - `vpxd-extension` 解决方案用户
  - `vsphere-webclient` 解决方案用户

2 在每个节点上替换证书。确切过程取决于您将执行的证书替换类型。请参见使用 vSphere 证书管理器实用程序管理证书。

有关详细信息，请参见以下主题：

- 将解决方案用户证书替换为新的 VMCA 签名证书
- 替换解决方案用户证书（中间 CA）
- 将解决方案用户证书替换为自定义证书

在包含外部解决方案的环境中替换证书

有些解决方案（如 VMware vCenter Site Recovery Manager 或 VMware vSphere Replication）始终与 vCenter Server 系统或 Platform Services Controller 安装在不同的计算机上。如果替换 vCenter Server 系统或 Platform Services Controller 上的默认计算机 SSL 证书，当解决方案尝试连接到 vCenter Server 系统时，会出现连接错误。

您可以通过运行 `ls_update_certs` 脚本解决此问题。有关详细信息，请参见 VMware 知识库文章，网址为 http://kb.vmware.com/kb/2109074。

使用 vSphere Client 管理证书

可以使用 vSphere Client 来查看和管理证书。也可以使用 vSphere 证书管理器实用程序执行许多证书管理任务。

使用 vSphere Client 可执行以下管理任务。

- 查看受信任的根证书和 SSL 证书。
- 续订现有证书或替换证书。

大多数证书替换工作流在 vSphere Client 中完全受支持。为了生成 CSR，可以使用 vSphere 证书管理器实用程序。

支持的工作流

安装 Platform Services Controller 后，默认情况下该节点上的 VMware Certificate Authority 为环境中的所有其他节点置备证书。有关管理证书的当前建议的建议，请参见第 3 章，vSphere 安全证书。

可以使用以下工作流之一续订或替换证书。

续订证书	可以让 VMCA 从 vSphere Client 续订环境中的 SSL 证书和解决方案用户证书。
使 VMCA 成为中间 CA	可以使用 vSphere 证书管理器实用程序生成 CSR。然后，可以编辑从 CSR 接收的证书以将 VMCA 添加到链中，然后向环境添加证书链和专用密钥。之后续订所有证书时，VMCA 将为所有计算机和解决方案用户置备已对整个链签名的证书。
将证书替换为自定义证书	如果不希望使用 VMCA，可以为要替换的证书生成 CSR。CA 将为每个 CSR 返回根证书和签名证书。可以从 Platform Services Controller 上载根证书和自定义证书。

注 如果使用 VMCA 作为中间 CA 或使用自定义证书，复杂性可能会显著提高，安全可能会受到负面影响，运营风险可能会不必要地提高。有关管理 vSphere 环境内的证书的更多信息，请参见标题为 New Product Walkthrough - Hybrid vSphere SSL Certificate Replacement 的博客帖子，网址为 http://vmware.com/go/hybridvmca。

在混合模式环境中，您可以使用 CLI 命令在替换其他证书后替换 vCenter Single Sign-On 证书。请参见在混合模式环境中替换 VMware Directory Service 证书。

从 vSphere Client 浏览证书存储

在每个 Platform Services Controller 节点和每个 vCenter Server 节点上都包括 VMware Endpoint 证书存储 (VECS) 实例。可以从 vSphere Client 浏览 VMware Endpoint 证书存储内部的不同存储。

有关 VECS 内部不同存储的详细信息，请参见 VMware Endpoint 证书存储概述。

前提条件

对于大多数管理任务，必须具有本地域帐户 administrator@vsphere.local 的管理员密码；或者如果在安装期间更改了此域，则必须具有其他域的管理员密码。

步骤

1. 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。
2. 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

   如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。
3. 导航到证书管理 UI。
   a. 在**主页**菜单中，选择**系统管理**。
   b. 在**证书**下，单击**证书管理**。
4. 输入您的 vCenter Server 凭据。
5. 浏览 VMware Endpoint 证书存储 (VECS) 内存储的证书。

   VMware Endpoint 证书存储概述介绍了各个存储中的具体内容。

6 要查看某证书的详细信息，请选择该证书，然后单击**查看详细信息**。

7 使用**操作**菜单续订或替换证书。

例如，如果替换现有证书，则稍后可以移除旧根证书。仅当确定证书不再使用时才将其移除。

为 vCenter 证书过期警告设置阈值

从 vSphere 6.0 开始，vCenter Server 会监控 VMware Endpoint 证书存储 (VECS) 中的所有证书，并在证书离过期还有 30 天或少于 30 天时发出警报。可以使用 `vpxd.cert.threshold` 高级选项更改向您发出警告的时间。

步骤

1 登录到 vSphere Client。

2 选择 vCenter Server 对象，然后单击**配置**。

3 单击**高级设置**。

4 单击**编辑设置**，然后针对**阈值**进行筛选。

5 将 `vpxd.cert.threshold` 的设置更改为所需值，然后单击**保存**。

从 vSphere Client 将证书替换为新的 VMCA 签名证书

可以将所有的 VMCA 签名证书替换为新的 VMCA 签名证书。此过程称为续订证书。可以从 vSphere Client 续订所选证书或环境中的所有证书。

前提条件

要管理证书，您必须提供本地域管理员（默认为 administrator@vsphere.local）的密码。如果要为 vCenter Server 系统续订证书，则您还必须为对 vCenter Server 系统具有管理员特权的用户提供 vCenter Single Sign-On 凭据。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到证书管理 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在**证书**下，单击**证书管理**。

4 输入您的 vCenter Server 凭据。

5 续订本地系统的计算机 SSL 证书。

a 选择**计算机 SSL 证书**。

b 单击**操作 > 续订**。

c 单击**续订**。

将显示一条续订证书的消息。

6 （可选）续订本地系统的解决方案用户证书。

a 在**解决方案证书**下，选择证书。

b 单击**操作 > 续订**以续订所选的各个证书，或者单击**全部续订**以续订所有的解决方案用户证书。

将显示一条续订证书的消息。

7 如果您的环境包括外部 Platform Services Controller，则可以续订每个 vCenter Server 系统的证书。

a 单击“证书管理”面板中的**注销**按钮。

b 出现提示时，指定 vCenter Server 系统的 IP 地址或 FQDN 以及可以向 vCenter Single Sign-On 进行身份验证的 vCenter Server 管理员的用户名和密码。

c 续订 vCenter Server 上的计算机 SSL 证书和（可选）每个解决方案用户证书。

d 如果您的环境中包含多个 vCenter Server 系统，则对每个系统重复该过程。

后续步骤

在 Platform Services Controller 上重新启动服务。可以重新启动 Platform Services Controller，或者从命令行运行以下命令：

Windows

在 Windows 上，`service-control` 命令位于 *VCENTER_INSTALL_PATH*\bin。

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

从 Platform Services Controller 将系统设置为使用自定义证书

可以使用 Platform Services Controller 将您的环境设置为使用自定义证书。

使用证书管理器实用程序，可以为每个计算机和每个解决方案用户生成证书签名请求 (CSR)。将 CSR 提交给内部或第三方 CA 时，CA 返回已签名证书和根证书。可以从 Platform Services Controller UI 同时上载根证书和已签名证书。

使用 vSphere 证书管理器生成证书签名请求（自定义证书）

您可以使用 vSphere 证书管理器生成证书签名请求 (CSR)，然后可以将其用于企业 CA 或发送给外部证书颁发机构。您可以通过受支持的不同证书替换流程使用证书。

可以按如下方式从命令行运行证书管理器工具：

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

前提条件

vSphere 证书管理器会提示您输入信息。提示信息取决于您的环境以及要替换的证书类型。

- 生成任何 CSR 时，系统会提示您输入 administrator@vsphere.local 用户的密码，或当前所连接的 vCenter Single Sign-On 域的管理员的密码。
- 如果您要在具有外部 Platform Services Controller 的环境中生成 CSR，则系统会提示您输入 Platform Services Controller 的主机名或 IP 地址。
- 要为计算机 SSL 证书生成 CSR，您需要按提示提供证书属性，这些属性存储在 `certool.cfg` 文件中。对于大多数字段，可以接受默认值或提供特定于站点的值。计算机的 FQDN 为必需值。

步骤

1. 在环境中的每个计算机上，启动 vSphere 证书管理器并选择选项 1。
2. 按照提示提供密码和 Platform Services Controller 的 IP 地址或主机名。
3. 选择选项 1 以生成 CSR，按提示提供信息，然后退出证书管理器。

   在此流程中，您还必须提供一个目录。证书管理器将证书和密钥文件放在此目录中。
4. 如果还希望替换所有解决方案用户证书，请重新启动证书管理器。
5. 选择选项 5。
6. 按照提示提供密码和 Platform Services Controller 的 IP 地址或主机名。
7. 选择选项 1 以生成 CSR，按提示提供信息，然后退出证书管理器。

   在此流程中，您还必须提供一个目录。证书管理器将证书和密钥文件放在此目录中。

   在每个 Platform Services Controller 节点上，证书管理器生成一个证书和密钥对。在每个 vCenter Server 节点上，证书管理器生成四个证书和密钥对。

后续步骤

执行证书替换。

将可信根证书添加到证书存储

如果要在您的环境中使用第三方证书，则必须将可信根证书添加到证书存储。

前提条件

从第三方或内部 CA 获取自定义根证书。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到证书管理 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在**证书**下，单击**证书管理**。

4 输入您的 vCenter Server 凭据。

5 在**可信根证书**下，单击**添加**。

6 单击**浏览**并选择证书链的位置。

可以使用 CER、PEM 或 CRT 类型的文件。

7 单击**添加**。

证书将添加到存储中。

后续步骤

将计算机 SSL 证书和（可选）解决方案用户证书替换为由此 CA 签名的证书。

从 Platform Services Controller 添加自定义证书

可以将自定义计算机 SSL 证书和自定义解决方案用户证书从 Platform Services Controller 添加到证书存储。

在大多数情况下，替换每个组件的计算机 SSL 证书就足够了。解决方案用户证书仍位于代理后面。

前提条件

为要替换的每个证书生成证书签名请求 (CSR)。可以使用 Certificate Manager 实用程序生成 CSR。在 Platform Services Controller 可以访问的位置中放置证书和专用密钥。

步骤

1 使用 vSphere Client 登录到已连接到 Platform Services Controller 的 vCenter Server。

2 为 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组的其他成员指定用户名和密码。

如果在安装时指定了不同的域，请以 administrator@*mydomain* 身份登录。

3 导航到证书管理 UI。

a 在**主页**菜单中，选择**系统管理**。

b 在**证书**下，单击**证书管理**。

4 输入您的 vCenter Server 凭据。

5 要替换计算机证书，请按照以下步骤操作：

a 在**计算机 SSL 证书**下，针对要更换的证书，单击**操作 > 替换**。

b 单击**浏览**以替换证书链，然后单击**浏览**以替换专用密钥。

c 单击**替换**。

6 要替换解决方案用户证书，请按照以下步骤操作：

a 在**解决方案证书**下，针对组件的第一个证书，例如**计算机**，单击**操作 > 替换**。

b 单击**浏览**以替换证书链，然后单击**浏览**以替换专用密钥。

c 单击**替换**。

d 针对同一组件的其他证书重复上述过程。

后续步骤

在 Platform Services Controller 上重新启动服务。可以重新启动 Platform Services Controller，或者从命令行运行以下命令：

Windows

在 Windows 上，`service-control` 命令位于 *VCENTER_INSTALL_PATH*\bin。

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

从 vSphere Web Client 管理证书

您可以从 vSphere Web Client 浏览证书。从 vSphere Client 执行所有其他管理任务。

请参见使用 vSphere Client 管理证书。

通过 vSphere Web Client 查看 vCenter 证书

可以查看 vCenter 证书颁发机构 (VMCA) 已知的证书以确定有效证书是否即将过期、检查过期证书以及查看根证书的状态。使用证书管理 CLI 执行所有证书管理任务。

查看与随嵌入式部署一起提供的 VMCA 实例或 Platform Services Controller 关联的证书。将在 VMware Directory Service (vmdir) 的实例之间复制证书信息。

尝试查看 vSphere Web Client 中的证书时，系统会提示您输入用户名和密码。为 VMware Certificate Authority 指定具有特权的用户的用户名和密码，即 vCenter Single Sign-On 组中的用户。

步骤

1 使用 vSphere Web Client 以 administrator@vsphere.local 或 CAAdmins vCenter Single Sign-On 组的另一个用户的身份登录到 vCenter Server。

2 在“主页”菜单中，选择**系统管理**。

3 单击**部署 > 系统配置**。

4 单击**节点**，然后在**节点**列表下选择一个主机。

5 依次单击**管理**选项卡和**证书颁发机构**。

6 单击要查看证书信息的证书类型。

选项	描述
有效证书	显示有效证书，包括其验证信息。证书即将过期时，绿色“有效期至”图标会发生更改。
已吊销证书	显示已吊销证书的列表。此版本中不支持。
已过期证书	列出已过期证书。
根证书	显示可用于此 vCenter 证书颁发机构的实例的根证书。

7 选择证书，然后单击**显示证书详细信息**按钮以查看证书详细信息。

详细信息包括主题名称、颁发者、有效性和算法。

使用 vSphere 证书管理器实用程序管理证书

vSphere 证书管理器实用程序可用于以交互方式从命令行执行大多数证书管理任务。vSphere 证书管理器会提示您输入要执行的任务、证书位置以及其他信息（根据需要），然后停止并启动服务，以及为您替换证书。

如果使用 vSphere 证书管理器，则无需替换 VECS（VMware Endpoint 证书存储）中的证书，且无需启动和停止服务。

在运行 vSphere 证书管理器之前，请确保熟悉替换过程并获取您要使用的证书。

小心 vSphere 证书管理器支持一个恢复级别。如果运行两次 vSphere 证书管理器并发现环境无意中遭到损坏，则该工具无法恢复前两次运行中的第一次运行。

证书管理器实用程序位置

可以按如下方式在命令行上运行该工具：

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

1 本文档中的证书管理器选项和工作流

您可以按顺序运行证书管理器选项以完成工作流。一些选项（例如生成 CSR）在不同的工作流中使用。

2 重新生成新的 VMCA 根证书并替换所有证书

可以重新生成 VMCA 根证书，并将本地计算机 SSL 证书和本地解决方案用户证书替换为 VMCA 签名证书。在多节点部署中，可以在 Platform Services Controller 上使用此选项运行 vSphere 证书管理器，然后在所有其他节点上重新运行该实用程序并选择 `Replace Machine SSL certificate with VMCA Certificate` 和 `Replace Solution user certificates with VMCA certificates`。

3 将 VMCA 设为中间证书颁发机构（证书管理器）

可以根据证书管理器实用程序的提示，将 VMCA 设为中间 CA。完成此过程后，VMCA 会对整个链中的所有证书进行签名。如果需要，可以使用证书管理器将所有现有证书替换为 VMCA 签名的新证书。

4 将所有证书替换为自定义证书（证书管理器）

可以使用 vSphere 证书管理器实用程序将所有证书替换为自定义证书。开始此过程之前，必须向您的 CA 发送 CSR。您可以使用证书管理器生成 CSR。

5 通过重新发布旧证书恢复上次执行的操作

通过使用 vSphere 证书管理器执行证书管理操作时，在替换证书之前，当前证书状态会先存储在 VECS 的 BACKUP_STORE 存储中。可以恢复上次执行的操作并返回到上一状态。

6 重置所有证书

如果要将所有现有 vCenter 证书替换为 VMCA 签名的证书，请使用重置所有证书选项。

本文档中的证书管理器选项和工作流

您可以按顺序运行证书管理器选项以完成工作流。一些选项（例如生成 CSR）在不同的工作流中使用。

将 VMCA 根证书替换为自定义签名证书并替换所有证书

此单选项工作流（选项 2）可以单独使用，也可以在中间证书工作流中使用。请参见重新生成新的 VMCA 根证书并替换所有证书。

将 VMCA 作为中间证书颁发机构

要将 VMCA 作为中间 CA，您必须多次运行证书管理器。该工作流提供了替换计算机 SSL 证书和解决方案用户证书的完整步骤。它说明了要在具有嵌入式 Platform Services Controller 或外部 Platform Services Controller 的环境中执行的操作。

1 要生成 CSR，请选择选项 2“将 VMCA 根证书替换为自定义签名证书并替换所有证书”。接下来，您可能必须提供有关证书的一些信息。再次提示选择一个选项时，选择选项 1。

将 CSR 提交到外部或企业 CA。您将从 CA 收到签名证书和根证书。

2 将 VMCA 根证书与 CA 根证书合并，然后保存文件。

3 选择选项 2“将 VMCA 根证书替换为自定义签名证书并替换所有证书”。此过程会替换本地计算机上的所有证书。

4 在多节点部署中，您必须替换每个节点上的证书。

a 首先将计算机 SSL 证书替换为（新）VMCA 证书（选项 3）。

b 然后将解决方案用户证书替换为（新）VMCA 证书（选项 6）

请参见将 VMCA 设为中间证书颁发机构（证书管理器）。

将所有证书替换为自定义证书

要将所有证书替换为自定义证书，您必须多次运行证书管理器。该工作流提供了替换计算机 SSL 证书和解决方案用户证书的完整步骤。它说明了要在具有嵌入式 Platform Services Controller 或外部 Platform Services Controller 的环境中执行的操作。

1 在每台计算机上分别为计算机 SSL 证书和解决方案用户证书生成证书签名请求。

a 要为计算机 SSL 证书生成 CSR，请选择选项 1。

b 如果公司策略要求您替换所有证书，则还要选择选项 5。

2 从 CA 收到签名证书和根证书后，使用选项 1 在每台计算机上替换计算机 SSL 证书。

3 如果您还想替换解决方案用户证书，请选择选项 5。

4 最后，在多节点部署中，您必须在每个节点上重复该过程。

请参见将所有证书替换为自定义证书（证书管理器）。

注 从 vSphere 6.5 开始，运行证书管理器实用程序时会显示以下提示：

```
Enter proper value for VMCA 'Name':
```

请输入运行证书配置的计算机的完全限定域名，以响应提示。

重新生成新的 VMCA 根证书并替换所有证书

可以重新生成 VMCA 根证书，并将本地计算机 SSL 证书和本地解决方案用户证书替换为 VMCA 签名证书。在多节点部署中，可以在 Platform Services Controller 上使用此选项运行 vSphere 证书管理器，然后在所有其他节点上重新运行该实用程序并选择 `Replace Machine SSL certificate with VMCA Certificate` 和 `Replace Solution user certificates with VMCA certificates`。

将现有计算机 SSL 证书替换为新的 VMCA 签名证书时，vSphere 证书管理器会提示您输入信息，并将除 Platform Services Controller 密码和 IP 地址以外的所有值输入到 `certool.cfg` 文件。

- administrator@vsphere.local 的密码。
- 两个字母组成的国家/地区代码
- 公司名称
- 组织名称
- 组织单位
- 省/市/自治区
- 地区
- IP 地址（可选）

- 电子邮件
- 主机名，即要替换证书的计算机的完全限定域名。如果主机名与 FQDN 不匹配，则证书替换无法正确完成，且环境可能最终会处于不稳定状态。
- Platform Services Controller 的 IP 地址（如果在管理节点上运行该命令）。
- VMCA 名称，即，运行证书配置的计算机的完全限定域名。

前提条件

在使用此选项运行 vSphere 证书管理器时，您必须了解以下信息。

- administrator@vsphere.local 的密码。
- 要为其生成新的 VMCA 签名证书的计算机的 FQDN。所有其他属性默认设置为预定义的值，但可以更改。

步骤

1 在嵌入式部署或者 Platform Services Controller 上启动 vSphere 证书管理器。

2 选择选项 4。

3 对提示做出响应。

证书管理器将基于您输入的内容生成新的 VMCA 根证书并替换运行证书管理器的系统上的所有证书。如果您使用嵌入式部署，则证书管理器重新启动服务后，替换过程便完成了。

4 如果您的环境包含外部 Platform Services Controller，您必须在每个 vCenter Server 系统上替换证书。

a 登录到 vCenter Server 系统。

b 停止所有服务，启动处理证书创建、传播和存储的服务。

服务名称在 Windows 和 vCenter Server Appliance 上有所不同。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

c 重新启动所有服务。

```
service-control --start --all
```

d 要替换计算机 SSL 证书，请使用选项 3
`Replace Machine SSL certificate with VMCA Certificate` 运行 vSphere 证书管理器。

e 要替换解决方案用户许可证，请使用选项 6
`Replace Solution user certificates with VMCA certificates` 运行证书管理器。

将 VMCA 设为中间证书颁发机构（证书管理器）

可以根据证书管理器实用程序的提示，将 VMCA 设为中间 CA。完成此过程后，VMCA 会对整个链中的所有证书进行签名。如果需要，可以使用证书管理器将所有现有证书替换为 VMCA 签名的新证书。

要将 VMCA 作为中间 CA，您必须多次运行证书管理器。该工作流提供了替换计算机 SSL 证书和解决方案用户证书的完整步骤。它说明了要在具有嵌入式 Platform Services Controller 或外部 Platform Services Controller 的环境中执行的操作。

1 要生成 CSR，请选择选项 1“将计算机 SSL 证书替换为自定义证书”，然后再次选择选项 1。

您将从 CA 收到签名证书和 root 证书。

2 将 VMCA root 证书与 CA root 证书合并，然后保存文件。

3 选择选项 2“将 VMCA root 证书替换为自定义签名证书并替换所有证书”。此过程会替换本地计算机上的所有证书。

4 在多节点部署中，您必须替换每个节点上的证书。

a 首先将计算机 SSL 证书替换为（新）VMCA 证书（选项 3）

b 然后将解决方案用户证书替换为（新）VMCA 证书（选项 6）

步骤

1 使用 vSphere 证书管理器生成 CSR 并准备根证书（中间 CA）

您可以使用 vSphere 证书管理器生成证书签名请求 (CSR)。将这些 CSR 提交到企业 CA 或外部证书颁发机构进行签名。您可以通过受支持的不同证书替换流程使用签名证书。

2 将 VMCA root 证书替换为自定义签名证书并替换所有证书

可以使用 vSphere 证书管理器生成 CSR 并将该 CSR 发送到企业或第三方 CA 进行签名。然后，可以将 VMCA root 证书替换为自定义签名证书，并将所有现有证书替换为自定义 CA 签名的证书。

3 将计算机 SSL 证书替换为 VMCA 证书（中间 CA）

在将 VMCA 用作中间 CA 的多节点部署中，必须明确替换计算机 SSL 证书。首先替换 Platform Services Controller 节点上的 VMCA 根证书，然后将 vCenter Server 节点上的证书替换为由整个链签名的证书。您也可以使用此选项替换已损坏或即将过期的计算机 SSL 证书。

4 将解决方案用户证书替换为 VMCA 证书（中间 CA）

在将 VMCA 用作中间 CA 的多节点环境中，可以明确替换解决方案用户证书。首先替换 Platform Services Controller 节点上的 VMCA 根证书，然后将 vCenter Server 节点上的证书替换为由整个链签名的证书。您也可以使用此选项替换已损坏或即将过期的解决方案用户证书。

使用 vSphere 证书管理器生成 CSR 并准备根证书（中间 CA）

您可以使用 vSphere 证书管理器生成证书签名请求 (CSR)。将这些 CSR 提交到企业 CA 或外部证书颁发机构进行签名。您可以通过受支持的不同证书替换流程使用签名证书。

- 可以使用 vSphere 证书管理器创建 CSR。
- 如果希望手动创建 CSR，则发送以进行签名的证书必须满足以下要求：
  - 密钥大小：2048 位或更大
  - PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。密钥添加到 VECS 后，会转换为 PKCS8。
  - x509 版本 3
  - 如果您当前使用的是自定义证书，对于根证书，CA 扩展必须设置为 true，并且证书签名必须在要求列表中。
  - 必须启用 CRL 签名。
  - “增强型密钥用法”可以为空或包含服务器身份验证。
  - 对证书链的长度没有明确限制。VMCA 使用 OpenSSL 默认设置，即 10 个证书。
  - 不支持包含通配符或多个 DNS 名称的证书。
  - 不能创建 VMCA 的附属 CA。

    请参见 http://kb.vmware.com/kb/2112009 中的 VMware 知识库文章，《在 vSphere 6.0 中创建 Microsoft 证书颁发机构模板以创建 SSL 证书》以获取使用 Microsoft 证书颁发机构的示例。

前提条件

vSphere 证书管理器会提示您输入信息。提示信息取决于您的环境以及要替换的证书类型。

生成任何 CSR 时，系统会提示您输入 administrator@vsphere.local 用户的密码，或当前所连接的 vCenter Single Sign-On 域的管理员的密码。

步骤

1 运行 vSphere 证书管理器。

操作系统	命令
Windows	`cd "C:\Program Files\VMware\vCenter Server\vmcad"` `certificate-manager`
Linux	`/usr/lib/vmware-vmca/bin/certificate-manager`

2 选择选项 2。

首先，使用此选项生成 CSR，而不是替换证书。

3 按照提示提供密码和 Platform Services Controller 的 IP 地址或主机名。

4 选择选项 1 以生成 CSR 并按提示提供信息。

在此流程中，您还必须提供一个目录。证书管理器会将要签名的证书（*.csr 文件）和相应密钥文件（*.key 文件）放入该目录中。

5 命名证书签名请求 (CSR) root_signing_cert.csr。

6 将 CSR 发送到您的企业或外部 CA 进行签名，并命名生成的签名证书 root_signing_cert.cer。

7 在文本编辑器中，按如下方式合并证书。

```
-----BEGIN CERTIFICATE-----
Signed VMCA root certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

8 将文件保存为 root_signing_chain.cer。

后续步骤

将现有根证书替换为链式根证书。请参见将 VMCA root 证书替换为自定义签名证书并替换所有证书。

将 VMCA root 证书替换为自定义签名证书并替换所有证书

可以使用 vSphere 证书管理器生成 CSR 并将该 CSR 发送到企业或第三方 CA 进行签名。然后，可以将 VMCA root 证书替换为自定义签名证书，并将所有现有证书替换为自定义 CA 签名的证书。

在嵌入式安装或外部 Platform Services Controller 中运行 vSphere 证书管理器以将 VMCA root 证书替换为自定义签名证书。

前提条件

- 生成证书链。
  - 可以使用 vSphere 证书管理器创建 CSR，或者手动创建 CSR。
  - 从第三方或者企业 CA 收到签名证书后，将它与初始 VMCA root 证书组合在一起以创建完整链。

    有关证书要求以及组合证书的过程，请参见使用 vSphere 证书管理器生成 CSR 并准备根证书（中间 CA）。
- 收集所需的信息。
  - administrator@vsphere.local 的密码。
  - Root 的有效自定义证书（.crt 文件）。
  - 有效的自定义 root 密钥（.key 文件）。

步骤

1 在嵌入式安装或外部 Platform Services Controller 上启动 vSphere 证书管理器，然后选择选项 2。

2 再次选择选项 2，开始证书替换并根据提示提供信息。

   a 出现提示后指定 root 证书的完整路径。

   b 如果是首次替换证书，则系统将提示您输入用于计算机 SSL 证书的信息。

   此信息包括计算机所需的 FQDN 并存储在 `certool.cfg` 文件中。

3 如果在多节点部署中替换 Platform Services Controller 上的 root 证书，则针对每个 vCenter Server 节点执行以下步骤。

   a 在 vCenter Server 节点上重新启动服务。

   b 通过使用选项 3 (`Replace Machine SSL certificate with VMCA Certificate`) 和选项 6 (`Replace Solution user certificates with VMCA certificates`) 在 vCenter Server 实例上重新生成所有证书。

   替换证书时，VMCA 会通过整个链进行签名。

后续步骤

如果从 vSphere 5.x 环境升级，可能必须替换 vmdir 中的 vCenter Single Sign-On 证书。请参见在混合模式环境中替换 VMware Directory Service 证书。

将计算机 SSL 证书替换为 VMCA 证书（中间 CA）

在将 VMCA 用作中间 CA 的多节点部署中，必须明确替换计算机 SSL 证书。首先替换 Platform Services Controller 节点上的 VMCA 根证书，然后将 vCenter Server 节点上的证书替换为由整个链签名的证书。您也可以使用此选项替换已损坏或即将过期的计算机 SSL 证书。

将现有计算机 SSL 证书替换为新的 VMCA 签名证书时，vSphere 证书管理器会提示您输入信息，并将除 Platform Services Controller 密码和 IP 地址以外的所有值输入到 `certool.cfg` 文件。

- administrator@vsphere.local 的密码。
- 两个字母组成的国家/地区代码
- 公司名称
- 组织名称
- 组织单位
- 省/市/自治区
- 地区
- IP 地址（可选）
- 电子邮件
- 主机名，即要替换证书的计算机的完全限定域名。如果主机名与 FQDN 不匹配，则证书替换无法正确完成，且环境可能最终会处于不稳定状态。

- Platform Services Controller 的 IP 地址（如果在管理节点上运行该命令）。
- VMCA 名称，即，运行证书配置的计算机的完全限定域名。

前提条件

- 如果替换了多节点部署中的 VMCA 根证书，请明确重新启动所有 vCenter Server 节点。
- 您必须了解以下信息才能使用此选项运行证书管理器。
  - administrator@vsphere.local 的密码。
  - 要为其生成新的 VMCA 签名证书的计算机的 FQDN。所有其他属性默认设置为预定义的值，但可以更改。
  - 如果运行的是具有外部 Platform Services Controller 的 vCenter Server 系统，则必须了解 Platform Services Controller 的主机名或 IP 地址。

步骤

1 启动 vSphere 证书管理器并选择选项 3。

2 对提示做出响应。

证书管理器将信息存储在 `certool.cfg` 文件中。

vSphere 证书管理器替换计算机 SSL 证书。

将解决方案用户证书替换为 VMCA 证书（中间 CA）

在将 VMCA 用作中间 CA 的多节点环境中，可以明确替换解决方案用户证书。首先替换 Platform Services Controller 节点上的 VMCA 根证书，然后将 vCenter Server 节点上的证书替换为由整个链签名的证书。您也可以使用此选项替换已损坏或即将过期的解决方案用户证书。

前提条件

- 如果替换了多节点部署中的 VMCA 根证书，请明确重新启动所有 vCenter Server 节点。
- 您必须了解以下信息才能使用此选项运行 Certificate Manager。
  - administrator@vsphere.local 的密码。
  - 如果运行的是具有外部 Platform Services Controller 的 vCenter Server 系统，则必须了解 Platform Services Controller 的主机名或 IP 地址。

步骤

1 启动 vSphere Certificate Manager 并选择选项 6。

2 对提示做出响应。

有关详细信息，请参见 VMware 知识库文章，网址为 http://kb.vmware.com/kb/2112281。

vSphere Certificate Manager 替换所有解决方案用户证书。

将所有证书替换为自定义证书（证书管理器）

可以使用 vSphere 证书管理器实用程序将所有证书替换为自定义证书。开始此过程之前，必须向您的 CA 发送 CSR。您可以使用证书管理器生成 CSR。

一种选择是仅使用 VMCA 置备的解决方案用户证书替换计算机 SSL 证书。解决方案用户证书仅用于 vSphere 组件之间的通信。

使用自定义证书时，将 VMCA 签名证书替换为自定义证书。可以使用 vSphere Client、vSphere 证书管理器实用程序或 CLI 进行手动证书替换。证书存储在 VECS 中。

要将所有证书替换为自定义证书，您必须多次运行证书管理器。该工作流提供了替换计算机 SSL 证书和解决方案用户证书的完整步骤。它说明了要在具有嵌入式 Platform Services Controller 或外部 Platform Services Controller 的环境中执行的操作。

1 在每台计算机上分别为计算机 SSL 证书和解决方案用户证书生成证书签名请求。

   a 要为计算机 SSL 证书生成 CSR，请选择选项 1。

   b 如果公司策略不允许混合部署，请选择选项 5。

2 从 CA 收到签名证书和根证书后，使用选项 1 在每台计算机上替换计算机 SSL 证书。

3 如果您还想替换解决方案用户证书，请选择选项 5。

4 最后，在多节点部署中，您必须在每个节点上重复该过程。

步骤

1 使用 vSphere 证书管理器生成证书签名请求（自定义证书）

   您可以使用 vSphere 证书管理器生成证书签名请求 (CSR)，然后可以将其用于企业 CA 或发送给外部证书颁发机构。您可以通过受支持的不同证书替换流程使用证书。

2 将计算机 SSL 证书替换为自定义证书

   计算机 SSL 证书由每个管理节点上的反向代理服务、Platform Services Controller 和嵌入式部署使用。每台计算机都必须拥有可用于与其他服务进行安全通信的计算机 SSL 证书。可以将每个节点上的证书替换为自定义证书。

3 将解决方案用户证书替换为自定义证书

   许多公司仅要求替换可从外部进行访问的服务的证书。但是，Certificate Manager 也支持替换解决方案用户证书。解决方案用户是服务的集合，例如，与 vSphere Client 关联的所有服务。在多节点部署中，替换 Platform Services Controller 上的计算机解决方案用户证书，以及每个管理节点上的整组解决方案用户。

使用 vSphere 证书管理器生成证书签名请求（自定义证书）

您可以使用 vSphere 证书管理器生成证书签名请求 (CSR)，然后可以将其用于企业 CA 或发送给外部证书颁发机构。您可以通过受支持的不同证书替换流程使用证书。

可以按如下方式从命令行运行证书管理器工具：

Windows

```
C:\Program Files\VMware\vCenter Server\vmcad\certificate-manager.bat
```

Linux

```
/usr/lib/vmware-vmca/bin/certificate-manager
```

前提条件

vSphere 证书管理器会提示您输入信息。提示信息取决于您的环境以及要替换的证书类型。

- 生成任何 CSR 时，系统会提示您输入 administrator@vsphere.local 用户的密码，或当前所连接的 vCenter Single Sign-On 域的管理员的密码。
- 如果您要在具有外部 Platform Services Controller 的环境中生成 CSR，则系统会提示您输入 Platform Services Controller 的主机名或 IP 地址。
- 要为计算机 SSL 证书生成 CSR，您需要按提示提供证书属性，这些属性存储在 `certool.cfg` 文件中。对于大多数字段，可以接受默认值或提供特定于站点的值。计算机的 FQDN 为必需值。

步骤

1. 在环境中的每个计算机上，启动 vSphere 证书管理器并选择选项 1。
2. 按照提示提供密码和 Platform Services Controller 的 IP 地址或主机名。
3. 选择选项 1 以生成 CSR，按提示提供信息，然后退出证书管理器。

   在此流程中，您还必须提供一个目录。证书管理器将证书和密钥文件放在此目录中。
4. 如果还希望替换所有解决方案用户证书，请重新启动证书管理器。
5. 选择选项 5。
6. 按照提示提供密码和 Platform Services Controller 的 IP 地址或主机名。
7. 选择选项 1 以生成 CSR，按提示提供信息，然后退出证书管理器。

   在此流程中，您还必须提供一个目录。证书管理器将证书和密钥文件放在此目录中。

   在每个 Platform Services Controller 节点上，证书管理器生成一个证书和密钥对。在每个 vCenter Server 节点上，证书管理器生成四个证书和密钥对。

后续步骤

执行证书替换。

将计算机 SSL 证书替换为自定义证书

计算机 SSL 证书由每个管理节点上的反向代理服务、Platform Services Controller 和嵌入式部署使用。每台计算机都必须拥有可用于与其他服务进行安全通信的计算机 SSL 证书。可以将每个节点上的证书替换为自定义证书。

前提条件

开始之前，您需要为环境中的每个计算机生成一个 CSR。您可以使用 vSphere Certificate Manager 生成 CSR 或明确生成 CSR。

1 要使用 vSphere Certificate Manager 生成 CSR，请参见使用 vSphere 证书管理器生成证书签名请求（自定义证书）。

2 要明确生成 CSR，请从第三方或企业 CA 为每个计算机请求一个证书。证书必须满足以下要求：

- 密钥大小：2048 位或更大（PEM 编码）
- CRT 格式
- x509 版本 3
- SubjectAltName 必须包含 DNS Name=<machine_FQDN>。
- 包含以下密钥使用：数字签名、不可否认性、密钥加密

注 不要在任何自定义证书中使用 CRL 分发点、授权信息访问或证书模板信息。

请参见位于 http://kb.vmware.com/kb/2112014 的 VMware 知识库文章，了解如何从 Microsoft 证书颁发机构获取 vSphere 证书。

步骤

1 启动 vSphere Certificate Manager 并选择选项 1。

2 选择选项 2 开始证书替换并根据提示提供信息。

vSphere Certificate Manager 提示您输入以下信息：

- administrator@vsphere.local 的密码。
- 有效的计算机 SSL 自定义证书（`.crt` 文件）。
- 有效的计算机 SSL 自定义密钥（`.key` 文件）。
- 有效的自定义计算机 SSL 证书的签名证书（`.crt` 文件）。
- 如果是在多节点部署中的管理节点中运行命令，则提示您输入 Platform Services Controller 的 IP 地址。

后续步骤

如果从 vSphere 5.x 环境升级，可能必须替换 `vmdir` 中的 vCenter Single Sign-On 证书。请参见在混合模式环境中替换 VMware Directory Service 证书。

将解决方案用户证书替换为自定义证书

许多公司仅要求替换可从外部进行访问的服务的证书。但是，Certificate Manager 也支持替换解决方案用户证书。解决方案用户是服务的集合，例如，与 vSphere Client 关联的所有服务。在多节点部署中，替换 Platform Services Controller 上的计算机解决方案用户证书，以及每个管理节点上的整组解决方案用户。

当提示您输入解决方案用户证书时，请提供第三方 CA 的完整签名证书链。

格式应类似于以下内容。

```
-----BEGIN CERTIFICATE-----
Signing certificate
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA intermediate certificates
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
Root certificate of enterprise or external CA
-----END CERTIFICATE-----
```

前提条件

开始之前，您需要为环境中的每个计算机生成一个 CSR。您可以使用 vSphere Certificate Manager 生成 CSR 或明确生成 CSR。

1 要使用 vSphere Certificate Manager 生成 CSR，请参见使用 vSphere 证书管理器生成证书签名请求（自定义证书）。

2 从第三方或企业 CA 为每个节点上的每个解决方案用户请求一个证书。您可以使用 vSphere Certificate Manager 生成 CSR 或自己准备 CSR。CSR 必须满足以下要求：

- 密钥大小：2048 位或更大（PEM 编码）
- CRT 格式
- x509 版本 3
- SubjectAltName 必须包含 DNS Name=<machine_FQDN>。
- 每个解决方案用户证书必须具有不同的 `Subject`。例如，考虑包含解决方案用户名（如 vpxd）或其他唯一标识符。
- 包含以下密钥使用：数字签名、不可否认性、密钥加密

请参见位于 http://kb.vmware.com/kb/2112014 的 VMware 知识库文章，了解如何从 Microsoft 证书颁发机构获取 vSphere 证书。

步骤

1 启动 vSphere Certificate Manager 并选择选项 5。

2 选择选项 2 开始证书替换并根据提示提供信息。

vSphere Certificate Manager 提示您输入以下信息：

- administrator@vsphere.local 的密码。
- 计算机解决方案用户的证书和密钥。
- 如果在 Platform Services Controller 节点上运行 vSphere Certificate Manager，则会提示您输入计算机解决方案用户的证书和密钥 (`vpxd.crt` 和 `vpxd.key`)。
- 如果在管理节点或嵌入式部署上运行 vSphere Certificate Manager，则会提示您输入所有解决方案用户的整组证书和密钥（`vpxd.crt` 和 `vpxd.key`）。

后续步骤

如果从 vSphere 5.x 环境升级，可能必须替换 vmdir 中的 vCenter Single Sign-On 证书。请参见在混合模式环境中替换 VMware Directory Service 证书。

通过重新发布旧证书恢复上次执行的操作

通过使用 vSphere 证书管理器执行证书管理操作时，在替换证书之前，当前证书状态会先存储在 VECS 的 BACKUP_STORE 存储中。可以恢复上次执行的操作并返回到上一状态。

注 恢复操作会还原当前在 BACKUP_STORE 中的内容。如果使用两个不同的选项运行 vSphere 证书管理器，然后尝试恢复，则仅会恢复上一个操作。

重置所有证书

如果要将所有现有 vCenter 证书替换为 VMCA 签名的证书，请使用重置所有证书选项。

使用此选项时，会覆盖当前在 VECS 中的所有自定义证书。

- 在 Platform Services Controller 节点上，vSphere 证书管理器可以重新生成根证书并替换计算机 SSL 证书和计算机解决方案用户证书。
- 在管理节点上，vSphere 证书管理器可以替换计算机 SSL 证书和所有解决方案用户证书。
- 在嵌入式部署中，vSphere 证书管理器可以替换所有证书。

替换的证书取决于您选择的选项。

手动证书替换

对于某些特殊情况，例如，如果要仅替换一种解决方案用户证书类型，则无法使用 vSphere 证书管理器实用程序。在这种情况下，可以使用随安装一起提供的 CLI 进行证书替换。

了解服务停止和启动

对于手动证书替换的某些部分，必须停止所有服务，然后仅启动管理证书基础架构的服务。如果仅在需要时停止服务，则可以最大程度地缩短停机时间。

在证书替换过程中，您必须停止和启动服务。

- 如果您的环境使用嵌入式 Platform Services Controller，请启动和停止所有服务，正如本文档所述。
- 如果您的环境使用外部 Platform Services Controller，那么不必停止和启动 vCenter Server 节点上的 VMware Directory Service (vmdird) 和 VMware Certificate Authority (vmcad)。这些服务运行于 Platform Services Controller 上。

请遵循以下经验规则。

- 请勿停止服务以生成新公用/专用密钥对或新证书。
- 如果您是唯一的管理员，则在添加新根证书时无需停止服务。旧根证书仍然可用，并且所有服务仍使用该证书进行身份验证。在添加根证书后停止并立即重新启动所有服务，以避免主机出现问题。

- 如果您的环境包括多个管理员，则在添加新根证书之前停止服务，并在添加新证书后重新启动服务。
- 请先停止服务，然后再执行以下任务：
  - 在 VECS 中删除计算机 SSL 证书或任何解决方案用户证书。
  - 替换 vmdir (VMware Directory Service) 中的解决方案用户证书。

将现有 VMCA 签名证书替换为新的 VMCA 签名证书

如果 VMCA 根证书在不久的将来会过期或者出于其他原因需要替换该证书，则可以生成新的根证书并将其添加到 VMware Directory Service。然后，可以使用新的根证书生成新的计算机 SSL 证书和解决方案用户证书。

大多数情况下，可以使用 vSphere 证书管理器实用程序替换证书。

如果需要进行精细控制，则此方案会为使用 CLI 命令替换一组完整的证书提供详细的分步说明。但是，也可以使用对应的任务中的步骤仅单独替换各个证书。

前提条件

仅有 administrator@vsphere.local 或 CAAdmins 组中的其他用户可以执行证书管理任务。请参见向 vCenter Single Sign-On 组添加成员。

步骤

1 生成新的 VMCA 签名根证书

使用 `certool` CLI 或 vSphere Certificate Manager 实用程序生成新的 VMCA 签名证书，并将证书发布到 vmdir。

2 将计算机 SSL 证书替换为 VMCA 签名证书

在生成新的 VMCA 签名根证书后，可以替换您环境中的所有计算机 SSL 证书。

3 将解决方案用户证书替换为新的 VMCA 签名证书

替换完计算机 SSL 证书后，可以替换所有解决方案用户证书。解决方案用户证书必须有效（即，不能过期），但证书中的其他所有信息可供证书基础架构使用。

4 在混合模式环境中替换 VMware Directory Service 证书

在升级过程中，您的环境可能暂时包括 vCenter Single Sign-On 版本 5.5 和 vCenter Single Sign-On 版本 6.x。在此情况下，如果替换正在运行 vCenter Single Sign-On 服务的节点的 SSL 证书，则必须执行其他步骤才能替换 VMware Directory Service SSL 证书。

生成新的 VMCA 签名根证书

使用 `certool` CLI 或 vSphere Certificate Manager 实用程序生成新的 VMCA 签名证书，并将证书发布到 vmdir。

在多节点部署中，在 Platform Services Controller 上运行根证书生成命令。

步骤

1 生成新的自签名证书和专用密钥。

```
certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config
<config_file>
```

2 将现有根证书替换为新证书。

```
certool --rootca --cert <cert_file_path> --privkey <key_file_path>
```

该命令会生成证书，将其添加到 vmdir，然后将其添加到 VECS。

3 停止所有服务，启动处理证书创建、传播和存储的服务。

服务名称在 Windows 和 vCenter Server Appliance 上有所不同。

注 如果您的环境使用外部 Platform Services Controller，则不必停止和启动 vCenter Server 节点上的 VMware Directory Service (vmdird) 和 VMware Certificate Authority (vmcad)。这些服务在 Platform Services Controller 上运行。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 （可选）将新的根证书发布到 vmdir。

```
dir-cli trustedcert publish --cert newRoot.crt
```

该命令会立即更新所有 vmdir 实例。如果不运行该命令，将新证书传播到所有节点可能需要一些时间。

5 重新启动所有服务。

```
service-control --start --all
```

示例：生成新的 VMCA 签名根证书

以下示例显示了验证当前根 CA 信息和重新生成根证书的所有步骤。

1 （可选）列出 VMCA 根证书以确保其位于证书存储中。

- 在 Platform Services Controller 节点或嵌入式安装中：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca
```

- 在管理节点（外部安装）中：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca --server=<psc-ip-or-fqdn>
```

输入类似于以下内容：

```
output:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
    ...
```

2 （可选）列出 VECS TRUSTED_ROOTS 库，并将证书序列号与步骤 1 中输出的序列号进行比较。

该命令可在 Platform Services Controller 节点和管理节点上运行，因为 VECS 会轮询 vmdir。

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry list --store TRUSTED_ROOTS  --text
```

在只有一个根证书的最简单情况下，输出类似于以下内容：

```
Number of entries in store :    1
Alias : 960d43f31eb95211ba3a2487ac840645a02894bd
Entry type :    Trusted Cert
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            cf:2d:ff:49:88:50:e5:af
```

3 生成新的 VMCA 根证书。该命令可将证书添加到 VECS 和 vmdir（VMware Directory Service）中的 TRUSTED_ROOTS 库。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --selfca --config="C:\Program
Files\VMware\vCenter Server\vmcad\certool.cfg"
```

在 Windows 中，可以选择 `--config`，因为该命令使用默认的 `certool.cfg` 文件。

将计算机 SSL 证书替换为 VMCA 签名证书

在生成新的 VMCA 签名根证书后，可以替换您环境中的所有计算机 SSL 证书。

每台计算机都必须拥有可用于与其他服务进行安全通信的计算机 SSL 证书。在多节点部署中，必须在每个节点上运行计算机 SSL 证书生成命令。使用 `--server` 参数从具有外部 Platform Services Controller 的 vCenter Server 指向 Platform Services Controller。

前提条件

准备好停止所有服务，启动处理证书传播和存储的服务。

步骤

1 为需要新证书的每台计算机复制一份 `certool.cfg`。

可以在以下位置找到 `certool.cfg`：

操作系统	路径
Windows	`C:\Program Files\VMware\vCenter Server\vmcad`
Linux	`/usr/lib/vmware-vmca/share/config/`

2 编辑每台计算机的自定义配置文件以包括该计算机的 FQDN。

对计算机的 IP 地址运行 `NSLookup`，以查看名称的 DNS 列表，并在文件的“主机名”字段中使用该名称。

3 为每个文件生成公用/专用密钥文件对和证书，通过刚刚自定义的配置文件进行传递。

例如：

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine1.crt --Name=Machine1_Cert --config
machine1.cfg
```

4 停止所有服务，启动处理证书创建、传播和存储的服务。

服务名称在 Windows 和 vCenter Server Appliance 上有所不同。

注 如果您的环境使用外部 Platform Services Controller，则不必停止和启动 vCenter Server 节点上的 VMware Directory Service (vmdird) 和 VMware Certificate Authority (vmcad)。这些服务在 Platform Services Controller 上运行。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 将新证书添加到 VECS。

所有计算机都需要本地证书存储中的新证书来通过 SSL 进行通信。首先删除现有条目，然后添加新条目。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

6 重新启动所有服务。

```
service-control --start --all
```

示例：将计算机证书替换为 VMCA 签名证书

1 为 SSL 证书创建配置文件，并在当前目录中将其保存为 `ssl-config.cfg`。

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = <my_company>
OrgUnit = <my_company Engineering>
State = <my_state>
Locality = <mytown>
Hostname = <FQDN>
```

2 为计算机 SSL 证书生成密钥对。在每个管理节点和 Platform Services Controller 节点上运行此命令；不需要 `--server` 选项。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv --
pubkey=ssl-key.pub
```

将在当前目录中创建 `ssl-key.priv` 和 `ssl-key.pub` 文件。

3 生成新的计算机 SSL 证书。此证书为 VMCA 签名证书。如果将 VMCA root 证书替换为自定义证书，则 VMCA 会对整个链中的所有证书进行签名。

- 在 Platform Services Controller 节点或嵌入式安装中：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --
privkey=ssl-key.priv --config=ssl-config.cfg
```

- 在 vCenter Server 中（外部安装）：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --
privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

将在当前目录中创建 `new-vmca-ssl.crt` 文件。

4 （可选）列出 VECS 的内容。

```
"C:\Program Files\VMware\vCenter Server\vmafdd\" vecs-cli store list
```

- Platform Services Controller 中的输出示例：

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- vCenter Server 中的输出示例：

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

5 将 VECS 中的计算机 SSL 证书替换为新的计算机 SSL 证书。`--store` 和 `--alias` 值必须与默认名称完全匹配。

- 在 Platform Services Controller 中，请运行以下命令以更新 MACHINE_SSL_CERT 存储中的计算机 SSL 证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- 在每个管理节点或嵌入式部署中，请运行以下命令以更新 MACHINE_SSL_CERT 存储中的计算机 SSL 证书。由于每个计算机具有不同的 FQDN，因此必须单独更新每个计算机的证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

后续步骤

您还可以替换 ESXi 主机的证书。请参见《vSphere 安全性》出版物。

在多节点部署中替换根证书后，必须在所有具有外部 Platform Services Controller 的 vCenter Server 节点上重新启动服务。

将解决方案用户证书替换为新的 VMCA 签名证书

替换完计算机 SSL 证书后，可以替换所有解决方案用户证书。解决方案用户证书必须有效（即，不能过期），但证书中的其他所有信息可供证书基础架构使用。

许多 VMware 客户未替换解决方案用户证书。他们仅将计算机 SSL 证书替换为自定义证书。这种混合方法符合其安全团队的要求。

- 证书位于代理后面或是自定义证书。
- 未使用中间 CA。

替换每个管理节点和每个 Platform Services Controller 节点上的计算机解决方案用户证书。只能替换每个管理节点上的其他解决方案用户证书。在具有外部 `--server` 的管理节点上运行命令时，请使用 Platform Services Controller 参数指向 Platform Services Controller。

注 在大型部署中列出解决方案用户证书时，`dir-cli list` 的输出包括所有节点的所有解决方案用户。运行 `vmafd-cli get-machine-id --server-name localhost` 以查找每个主机的本地计算机 ID。每个解决方案用户名称均包括计算机 ID。

前提条件

准备好停止所有服务，启动处理证书传播和存储的服务。

步骤

1 复制一份 `certool.cfg`，移除名称、IP 地址、DNS 名称和电子邮件字段，并重命名文件，例如，重命名为 `sol_usr.cfg`。

您可以通过命令行在生成过程中命名证书。解决方案用户不需要其他信息。如果保留默认信息，生成的证书可能会造成混淆。

2 传递刚自定义的配置文件为每个解决方案用户生成公用/专用密钥文件对和证书。

例如：

```
certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

3 查找每个解决方案用户的名称。

```
dir-cli service list
```

可以使用替换证书时返回的唯一 ID。输入和输出可能显示如下。

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

在多节点部署中列出解决方案用户证书时，`dir-cli` 列表输出将包含所有节点的所有解决方案用户。运行 `vmafd-cli get-machine-id --server-name localhost` 以查找每个主机的本地计算机 ID。每个解决方案用户名称均包括计算机 ID。

4 停止所有服务，启动处理证书创建、传播和存储的服务。

服务名称在 Windows 和 vCenter Server Appliance 上有所不同。

注 如果您的环境使用外部 Platform Services Controller，则不必停止和启动 vCenter Server 节点上的 VMware Directory Service (vmdird) 和 VMware Certificate Authority (vmcad)。这些服务在 Platform Services Controller 上运行。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 对于每个解决方案用户，请先替换 vmdir 中的现有证书，然后替换 VECS 中的证书。

以下示例显示了如何替换 vpxd 服务的证书。

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

注 如果不替换 vmdir 中的证书，则解决方案用户无法对 vCenter Single Sign-On 进行身份验证。

6 重新启动所有服务。

```
service-control --start --all
```

示例：使用 VMCA 签名解决方案用户证书

1 为每个解决方案用户生成公用/专用密钥对。其中包括每个 Platform Services Controller 和每个管理节点上的计算机解决方案用户的密钥对和每个管理节点上的每个其他解决方案用户（vpxd、vpxd-extension、vsphere-webclient）的密钥对。

a 为嵌入式部署的计算机解决方案用户或 Platform Services Controller 的计算机解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv
--pubkey=machine-key.pub
```

b （可选）对于使用外部 Platform Services Controller 的部署，请为每个管理节点上的计算机解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv
--pubkey=machine-key.pub
```

c 为每个管理节点上的 vpxd 解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --
pubkey=vpxd-key.pub
```

d 为每个管理节点上的 vpxd-extension 解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-
key.priv --pubkey=vpxd-extension-key.pub
```

e 为每个管理节点上的 vsphere-webclient 解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-
key.priv --pubkey=vsphere-webclient-key.pub
```

2 为每个 Platform Services Controller 和每个管理节点上的计算机解决方案用户以及每个管理节点上的每个其他解决方案用户（vpxd、vpxd-extension、vsphere-webclient）生成由新的 VMCA root 证书签名的解决方案用户证书。

注 `--Name` 参数必须唯一。包括解决方案用户存储的名称，可便于查看证书与解决方案用户之间的映射关系。在任何一种情况下，该示例都包括此名称，例如 `vpxd` 或 `vpxd-extension`。

a 在 Platform Services Controller 节点上运行以下命令可为该节点上的计算机解决方案用户生成解决方案用户证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --
privkey=machine-key.priv --Name=machine
```

b 为每个管理节点上的计算机解决方案用户生成证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --
privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

c 为每个管理节点上的 vpxd 解决方案用户生成证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --
privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

d 为每个管理节点上的 vpxd-extensions 解决方案用户生成证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-
extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

e 通过运行以下命令为每个管理节点上的 vsphere-webclient 解决方案用户生成证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>
```

3 将 VECS 中的解决方案用户证书替换为新的解决方案用户证书。

注 `--store` 和 `--alias` 参数必须与服务的默认名称完全匹配。

a 在 Platform Services Controller 节点上，请运行以下命令以替换计算机解决方案用户证书：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

b 替换每个管理节点上的计算机解决方案用户证书：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

c 替换每个管理节点上的 vpxd 解决方案用户证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd --alias vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

d 替换每个管理节点上的 vpxd-extension 解决方案用户证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

e 替换每个管理节点上的 vsphere-webclient 解决方案用户证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

4 使用新的解决方案用户证书更新 VMware Directory Service (vmdir)。系统将提示您输入 vCenter Single Sign-On 管理员密码。

a 运行 `dir-cli service list` 可获取每个解决方案用户的唯一服务 ID 后缀。可以在 Platform Services Controller 或 vCenter Server 系统上运行此命令。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

注 在大型部署中列出解决方案用户证书时，`dir-cli list` 的输出包括所有节点的所有解决方案用户。运行 `vmafd-cli get-machine-id --server-name localhost` 以查找每个主机的本地计算机 ID。每个解决方案用户名称均包括计算机 ID。

b 在 Platform Services Controller 上替换 vmdir 中的计算机证书。例如，如果 machine-29a45d00-60a7-11e4-96ff-00505689639a 为 Platform Services Controller 中的计算机解决方案用户，请运行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

c 替换每个管理节点上的 vmdir 中的计算机证书。例如，如果 machine-6fd7f140-60a9-11e4-9e28-005056895a69 为 vCenter Server 中的计算机解决方案用户，请运行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

d 替换每个管理节点上的 vmdir 中的 vpxd 解决方案用户证书。例如，如果 vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 为 vpxd 解决方案用户 ID，请运行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

e 替换每个管理节点上的 vmdir 中的 vpxd-extension 解决方案用户证书。例如，如果 vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 为 vpxd-extension 解决方案用户 ID，请运行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

f 替换每个管理节点上的 vsphere-webclient 解决方案用户证书。例如，如果 vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 为 vsphere-webclient 解决方案用户 ID，请运行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

后续步骤

重新启动每个 Platform Services Controller 节点和每个管理节点上的所有服务。

在混合模式环境中替换 VMware Directory Service 证书

在升级过程中，您的环境可能暂时包括 vCenter Single Sign-On 版本 5.5 和 vCenter Single Sign-On 版本 6.x。在此情况下，如果替换正在运行 vCenter Single Sign-On 服务的节点的 SSL 证书，则必须执行其他步骤才能替换 VMware Directory Service SSL 证书。

vmdir 使用 VMware Directory Service SSL 证书可在执行 vCenter Single Sign-On 复制的 Platform Services Controller 节点之间执行握手操作。

同时包括 vSphere 6.0 和 vSphere 6.5 节点的混合模式环境不需要执行这些步骤。仅在以下情况下需要执行这些步骤：

- 环境中同时包括 vCenter Single Sign-On 5.5 和 vCenter Single Sign-On 6.x 服务。
- vCenter Single Sign-On 服务设置为复制 vmdir 数据。
- 对于运行 vCenter Single Sign-On 6.x 服务的节点，计划将默认 VMCA 签名证书替换为自定义证书。

注 最佳做法是在重新启动服务之前先升级整个环境。通常不建议替换 VMware Directory Service 证书。

步骤

1 在运行 vCenter Single Sign-On 5.5 服务的节点上，请先设置环境以便熟悉 vCenter Single Sign-On 6.x 服务。

   a 备份所有文件 `C:\ProgramData\VMware\CIS\cfg\vmdird`。

   b 在 6.x 节点上创建 `vmdircert.pem` 文件的副本，并将其重命名为 `<sso_node2.domain.com>.pem`，其中 `<sso_node2.domain.com>` 是 6.x 节点的 FQDN。

   c 将重命名的证书复制到 `C:\ProgramData\VMware\CIS\cfg\vmdird` 以替换现有的复制证书。

2 在已替换证书的所有计算机上重新启动 VMware Directory Service。

   可以从 vSphere Client 中重新启动服务或使用 `service-control` 命令。

使用 VMCA 作为中间证书颁发结构

可以将 VMCA root 证书替换为证书链中包括 VMCA 的第三方 CA 签名证书。从今往后，VMCA 生成的所有证书都将包括完整链。可以将现有证书替换为新生成的证书。

步骤

1 替换根证书（中间 CA）

将 VMCA 证书替换为自定义证书的第一步是生成 CSR，发送要签名的 CSR。然后，将签名证书作为根证书添加到 VMCA。

2 替换计算机 SSL 证书（中间 CA）

当您收到 CA 的签名证书并使其成为 VMCA root 证书后，您可以替换所有计算机 SSL 证书。

3 替换解决方案用户证书（中间 CA）

在替换计算机 SSL 证书后，可以替换解决方案用户证书。

4 在混合模式环境中替换 VMware Directory Service 证书

在升级过程中，您的环境可能暂时包括 vCenter Single Sign-On 版本 5.5 和 vCenter Single Sign-On 版本 6.x。在此情况下，如果替换正在运行 vCenter Single Sign-On 服务的节点的 SSL 证书，则必须执行其他步骤才能替换 VMware Directory Service SSL 证书。

替换根证书（中间 CA）

将 VMCA 证书替换为自定义证书的第一步是生成 CSR，发送要签名的 CSR。然后，将签名证书作为根证书添加到 VMCA。

可以使用证书管理器实用程序或其他工具生成 CSR。CSR 必须满足以下要求：

- 密钥大小：2048 位或更大
- PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。密钥添加到 VECS 后，会转换为 PKCS8。
- x509 版本 3
- 如果您当前使用的是自定义证书，对于根证书，CA 扩展必须设置为 true，并且证书签名必须在要求列表中。
- 必须启用 CRL 签名。
- “增强型密钥用法”可以为空或包含服务器身份验证。
- 对证书链的长度没有明确限制。VMCA 使用 OpenSSL 默认设置，即 10 个证书。
- 不支持包含通配符或多个 DNS 名称的证书。
- 不能创建 VMCA 的附属 CA。

  请参见 http://kb.vmware.com/kb/2112009 中的 VMware 知识库文章，《在 vSphere 6.0 中创建 Microsoft 证书颁发机构模板以创建 SSL 证书》以获取使用 Microsoft 证书颁发机构的示例。

替换根证书时，VMCA 会验证以下证书属性：

- 密钥大小：2048 位或更多
- 密钥使用：证书签名
- 基本限制：主体类型 CA

步骤

1 生成 CSR 并将其发送给您的 CA。

按照 CA 的说明进行操作。

2 准备包括签名的 VMCA 证书以及第三方 CA 或企业 CA 的完整 CA 链的证书文件。保存该文件，例如，另存为 `rootca1.crt`。

可以通过将 PEM 格式的所有 CA 证书复制到单个文件来完成此步骤。以 VMCA 根证书开头，并以根 CA PEM 证书结尾。例如：

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

3 停止所有服务，启动处理证书创建、传播和存储的服务。

服务名称在 Windows 和 vCenter Server Appliance 上有所不同。

注 如果您的环境使用外部 Platform Services Controller，则不必停止和启动 vCenter Server 节点上的 VMware Directory Service (vmdird) 和 VMware Certificate Authority (vmcad)。这些服务在 Platform Services Controller 上运行。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 替换现有 VMCA 根 CA。

```
certool --rootca --cert=rootca1.crt --privkey=root1.key
```

运行此命令时，会执行以下操作：

- 将新的自定义根证书添加到文件系统中的证书位置。
- 将自定义根证书附加到 VECS 中的 TRUSTED_ROOTS 存储中（延迟后）。
- 将自定义根证书附加到 vmdir（延迟后）。

5 （可选）要将更改传播到 vmdir（VMware Directory Service）的所有实例，请将新根证书发布到 vmdir，并提供每个文件的完整文件路径。

例如：

```
dir-cli trustedcert publish --cert rootca1.crt
```

每 30 秒进行一次 vmdir 节点之间的复制。无需将根证书显式添加到 VECS，因为 VECS 会每 5 分钟轮询 vmdir 中的新根证书文件。

6 （可选）如有必要，可以强制刷新 VECS。

```
vecs-cli force-refresh
```

7 重新启动所有服务。

```
service-control --start --all
```

示例：替换根证书

使用 certool 命令和 `--rootca` 选项将 VMCA 根证书替换为自定义 CA 根证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\certool" --rootca --cert=C:\custom-certs\root.pem --
privkey=C:\custom-certs\root.key
```

运行此命令时，会执行以下操作：

- 将新的自定义根证书添加到文件系统中的证书位置。
- 将自定义根证书附加到 VECS 中的 TRUSTED_ROOTS 存储中。
- 将自定义根证书添加到 vmdir。

后续步骤

如果公司策略需要，可以从证书存储中移除原始的 VMCA 根证书。如果执行此操作，则必须替换 vCenter Single Sign-On 签名证书。请参见刷新 Security Token Service 证书。

替换计算机 SSL 证书（中间 CA）

当您收到 CA 的签名证书并使其成为 VMCA root 证书后，您可以替换所有计算机 SSL 证书。

这些步骤实际上与替换为使用 VMCA 作为证书颁发机构的证书的步骤相同。但是，在这种情况下，VMCA 会对整个链中的所有证书进行签名。

每台计算机都必须拥有可用于与其他服务进行安全通信的计算机 SSL 证书。在多节点部署中，必须在每个节点上运行计算机 SSL 证书生成命令。使用 `--server` 参数从具有外部 Platform Services Controller 的 vCenter Server 指向 Platform Services Controller。

前提条件

对于每个计算机 SSL 证书，`SubjectAltName` 必须包含 `DNS Name=<Machine FQDN>`。

步骤

1 为需要新证书的每台计算机复制一份 `certool.cfg`。

可以在以下位置找到 `certool.cfg`：

Windows	`C:\Program Files\VMware\vCenter Server\vmcad`
Linux	`/usr/lib/vmware-vmca/share/config/`

2 编辑每台计算机的自定义配置文件以包括该计算机的 FQDN。

对计算机的 IP 地址运行 `NSLookup`，以查看名称的 DNS 列表，并在文件的“主机名”字段中使用该名称。

3 传递刚自定义的配置文件为每个计算机生成公用/专用密钥文件对。

例如：

```
certool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certool --gencert --privkey=machine1.priv --cert machine42.crt --Name=Machine42_Cert --config
machine1.cfg
```

4 停止所有服务，启动处理证书创建、传播和存储的服务。

服务名称在 Windows 和 vCenter Server Appliance 上有所不同。

注 如果您的环境使用外部 Platform Services Controller，则不必停止和启动 vCenter Server 节点上的 VMware Directory Service (vmdird) 和 VMware Certificate Authority (vmcad)。这些服务在 Platform Services Controller 上运行。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 将新证书添加到 VECS。

所有计算机都需要本地证书存储中的新证书来通过 SSL 进行通信。首先删除现有条目，然后添加新条目。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

6 重新启动所有服务。

```
service-control --start --all
```

示例：替换计算机 SSL 证书（VMCA 为中间 CA）

1 为 SSL 证书创建配置文件，并在当前目录中将其保存为 `ssl-config.cfg`。

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = VMware
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

2 为计算机 SSL 证书生成密钥对。在每个管理节点和 Platform Services Controller 节点上运行此命令；不需要 `--server` 选项。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv --
pubkey=ssl-key.pub
```

将在当前目录中创建 `ssl-key.priv` 和 `ssl-key.pub` 文件。

3 生成新的计算机 SSL 证书。此证书为 VMCA 签名证书。如果将 VMCA root 证书替换为自定义证书，则 VMCA 会对整个链中的所有证书进行签名。

- 在 Platform Services Controller 节点或嵌入式安装中：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --
privkey=ssl-key.priv --config=ssl-config.cfg
```

- 在 vCenter Server 中（外部安装）：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --
privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

将在当前目录中创建 `new-vmca-ssl.crt` 文件。

4 （可选）列出 VECS 的内容。

```
"C:\Program Files\VMware\vCenter Server\vmafdd\" vecs-cli store list
```

- Platform Services Controller 中的输出示例：

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- vCenter Server 中的输出示例：

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
```

```
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

5 将 VECS 中的计算机 SSL 证书替换为新的计算机 SSL 证书。`--store` 和 `--alias` 值必须与默认名称完全匹配。

- 在 Platform Services Controller 中，请运行以下命令以更新 MACHINE_SSL_CERT 存储中的计算机 SSL 证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- 在每个管理节点或嵌入式部署中，请运行以下命令以更新 MACHINE_SSL_CERT 存储中的计算机 SSL 证书。由于每个计算机具有不同的 FQDN，因此必须单独更新每个计算机的证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

替换解决方案用户证书（中间 CA）

在替换计算机 SSL 证书后，可以替换解决方案用户证书。

许多 VMware 客户未替换解决方案用户证书。他们仅将计算机 SSL 证书替换为自定义证书。这种混合方法符合其安全团队的要求。

- 证书位于代理后面或是自定义证书。
- 未使用中间 CA。

替换每个管理节点和每个 Platform Services Controller 节点上的计算机解决方案用户证书。只能替换每个管理节点上的其他解决方案用户证书。在具有外部 `--server` 的管理节点上运行命令时，请使用 Platform Services Controller 参数指向 Platform Services Controller。

注 在大型部署中列出解决方案用户证书时，`dir-cli list` 的输出包括所有节点的所有解决方案用户。运行 `vmafd-cli get-machine-id --server-name localhost` 以查找每个主机的本地计算机 ID。每个解决方案用户名称均包括计算机 ID。

前提条件

每个解决方案用户证书必须具有不同的 `Subject`。例如，考虑包含解决方案用户名（如 vpxd）或其他唯一标识符。

步骤

1 复制一份 `certool.cfg`，移除名称、IP 地址、DNS 名称和电子邮件字段，并重命名文件，例如，重命名为 `sol_usr.cfg`。

您可以通过命令行在生成过程中命名证书。解决方案用户不需要其他信息。如果保留默认信息，生成的证书可能会造成混淆。

2 传递刚自定义的配置文件为每个解决方案用户生成公用/专用密钥文件对和证书。

例如：

```
certool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certool --gencert --privkey=vpxd.priv --cert vpxd.crt --Name=VPXD_1 --config sol_usr.cfg
```

3 查找每个解决方案用户的名称。

```
dir-cli service list
```

可以使用替换证书时返回的唯一 ID。输入和输出可能显示如下。

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

在多节点部署中列出解决方案用户证书时，`dir-cli` 列表输出将包含所有节点的所有解决方案用户。运行 `vmafd-cli get-machine-id --server-name localhost` 以查找每个主机的本地计算机 ID。每个解决方案用户名称均包括计算机 ID。

4 停止所有服务，启动处理证书创建、传播和存储的服务。

服务名称在 Windows 和 vCenter Server Appliance 上有所不同。

注 如果您的环境使用外部 Platform Services Controller，则不必停止和启动 vCenter Server 节点上的 VMware Directory Service (vmdird) 和 VMware Certificate Authority (vmcad)。这些服务在 Platform Services Controller 上运行。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

5 依次替换 vmdir 和 VECS 中的现有证书。

对于解决方案用户，必须以该顺序添加证书。例如：

```
dir-cli service update --name <vpxd-xxxx-xxx-7c7b769cd9f4> --cert ./vpxd.crt
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
```

注 如果不替换 vmdir 中的证书，则解决方案用户无法登录到 vCenter Single Sign-On。

6 重新启动所有服务。

```
service-control --start --all
```

示例：替换解决方案用户证书（中间 CA）

1 为每个解决方案用户生成公用/专用密钥对。其中包括每个 Platform Services Controller 和每个管理节点上的计算机解决方案用户的密钥对和每个管理节点上的每个其他解决方案用户（vpxd、vpxd-extension、vsphere-webclient）的密钥对。

a 为嵌入式部署的计算机解决方案用户或 Platform Services Controller 的计算机解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv
--pubkey=machine-key.pub
```

b （可选）对于使用外部 Platform Services Controller 的部署，请为每个管理节点上的计算机解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=machine-key.priv
--pubkey=machine-key.pub
```

c 为每个管理节点上的 vpxd 解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-key.priv --
pubkey=vpxd-key.pub
```

d 为每个管理节点上的 vpxd-extension 解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vpxd-extension-
key.priv --pubkey=vpxd-extension-key.pub
```

e 为每个管理节点上的 vsphere-webclient 解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=vsphere-webclient-
key.priv --pubkey=vsphere-webclient-key.pub
```

2 为每个 Platform Services Controller 和每个管理节点上的计算机解决方案用户以及每个管理节点上的每个其他解决方案用户（vpxd、vpxd-extension、vsphere-webclient）生成由新的 VMCA root 证书签名的解决方案用户证书。

注 `--Name` 参数必须唯一。包括解决方案用户存储的名称，可便于查看证书与解决方案用户之间的映射关系。在任何一种情况下，该示例都包括此名称，例如 `vpxd` 或 `vpxd-extension`。

a 在 Platform Services Controller 节点上运行以下命令可为该节点上的计算机解决方案用户生成解决方案用户证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --
privkey=machine-key.priv --Name=machine
```

b 为每个管理节点上的计算机解决方案用户生成证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-machine.crt --
privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>
```

c 为每个管理节点上的 vpxd 解决方案用户生成证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd.crt --
privkey=vpxd-key.priv --Name=vpxd --server=<psc-ip-or-fqdn>
```

d 为每个管理节点上的 vpxd-extensions 解决方案用户生成证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vpxd-
extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension --server=<psc-ip-or-fqdn>
```

e 通过运行以下命令为每个管理节点上的 vsphere-webclient 解决方案用户生成证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vsphere-
webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-
fqdn>
```

3 将 VECS 中的解决方案用户证书替换为新的解决方案用户证书。

注 `--store` 和 `--alias` 参数必须与服务的默认名称完全匹配。

a 在 Platform Services Controller 节点上，请运行以下命令以替换计算机解决方案用户证书：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --
alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --
alias machine --cert new-machine.crt --key machine-key.priv
```

b 替换每个管理节点上的计算机解决方案用户证书：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --
alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --
alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

c 替换每个管理节点上的 vpxd 解决方案用户证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd --alias
vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd --alias
vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

d 替换每个管理节点上的 vpxd-extension 解决方案用户证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-
extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-
extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

e 替换每个管理节点上的 vsphere-webclient 解决方案用户证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vsphere-
webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vsphere-
webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-
key.priv
```

4 使用新的解决方案用户证书更新 VMware Directory Service (vmdir)。系统将提示您输入 vCenter Single Sign-On 管理员密码。

a 运行 `dir-cli service list` 可获取每个解决方案用户的唯一服务 ID 后缀。可以在 Platform Services Controller 或 vCenter Server 系统上运行此命令。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69
```

注 在大型部署中列出解决方案用户证书时，`dir-cli list` 的输出包括所有节点的所有解决方案用户。运行 `vmafd-cli get-machine-id --server-name localhost` 以查找每个主机的本地计算机 ID。每个解决方案用户名称均包括计算机 ID。

b 在 Platform Services Controller 上替换 vmdir 中的计算机证书。例如，如果 machine-29a45d00-60a7-11e4-96ff-00505689639a 为 Platform Services Controller 中的计算机解决方案用户，请运行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

c 替换每个管理节点上的 vmdir 中的计算机证书。例如，如果 machine-6fd7f140-60a9-11e4-9e28-005056895a69 为 vCenter Server 中的计算机解决方案用户，请运行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

d 替换每个管理节点上的 vmdir 中的 vpxd 解决方案用户证书。例如，如果 vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 为 vpxd 解决方案用户 ID，请运行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

e 替换每个管理节点上的 vmdir 中的 vpxd-extension 解决方案用户证书。例如，如果 vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 为 vpxd-extension 解决方案用户 ID，请运行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

f 替换每个管理节点上的 vsphere-webclient 解决方案用户证书。例如，如果 vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 为 vsphere-webclient 解决方案用户 ID，请运行此命令：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

在混合模式环境中替换 VMware Directory Service 证书

在升级过程中，您的环境可能暂时包括 vCenter Single Sign-On 版本 5.5 和 vCenter Single Sign-On 版本 6.x。在此情况下，如果替换正在运行 vCenter Single Sign-On 服务的节点的 SSL 证书，则必须执行其他步骤才能替换 VMware Directory Service SSL 证书。

vmdir 使用 VMware Directory Service SSL 证书可在执行 vCenter Single Sign-On 复制的 Platform Services Controller 节点之间执行握手操作。

同时包括 vSphere 6.0 和 vSphere 6.5 节点的混合模式环境不需要执行这些步骤。仅在以下情况下需要执行这些步骤：

- 环境中同时包括 vCenter Single Sign-On 5.5 和 vCenter Single Sign-On 6.x 服务。
- vCenter Single Sign-On 服务设置为复制 vmdir 数据。

- 对于运行 vCenter Single Sign-On 6.x 服务的节点，计划将默认 VMCA 签名证书替换为自定义证书。

注 最佳做法是在重新启动服务之前先升级整个环境。通常不建议替换 VMware Directory Service 证书。

步骤

1 在运行 vCenter Single Sign-On 5.5 服务的节点上，请先设置环境以便熟悉 vCenter Single Sign-On 6.x 服务。

   a 备份所有文件 `C:\ProgramData\VMware\CIS\cfg\vmdird`。

   b 在 6.x 节点上创建 `vmdircert.pem` 文件的副本，并将其重命名为 `<sso_node2.domain.com>.pem`，其中 `<sso_node2.domain.com>` 是 6.x 节点的 FQDN。

   c 将重命名的证书复制到 `C:\ProgramData\VMware\CIS\cfg\vmdird` 以替换现有的复制证书。

2 在已替换证书的所有计算机上重新启动 VMware Directory Service。

   可以从 vSphere Client 中重新启动服务或使用 `service-control` 命令。

在 vSphere 中使用自定义证书

如果公司策略有相关要求，则可以将在 vSphere 中使用的某些或所有证书替换为第三方或企业 CA 签名的证书。如果执行了此操作，则 VMCA 将不在证书链中。您需要将所有 vCenter 证书存储在 VECS 中。

可以替换所有证书或使用混合解决方案。例如，可以考虑替换用于网络通信的所有证书，但保留 VMCA 签名的解决方案用户证书。解决方案用户证书仅适用于对 vCenter Single Sign-On 进行身份验证。

注 如果不需要使用 VMCA，则您必须负责亲自替换所有证书、使用证书置备新的组件以及跟踪证书过期情况。

即使您决定使用自定义证书，也仍可使用 VMware Certificate Manager 实用程序进行证书替换。请参见将所有证书替换为自定义证书（证书管理器）。

如果在替换证书后 vSphere Auto Deploy 遇到问题，请参见网址为 http://kb.vmware.com/kb/2000988 的 VMware 知识库文章 2000888。

步骤

1 请求证书并导入自定义根证书

   可以使用企业或第三方 CA 的自定义证书。第一步是向 CA 请求证书并将根证书导入 VECS。

2 将计算机 SSL 证书替换为自定义证书

   收到自定义证书后，可以替换每个计算机证书。

3 将解决方案用户证书替换为自定义证书

   在替换计算机 SSL 证书后，可以将 VMCA 签名解决方案用户证书替换为第三方或企业证书。

4 在混合模式环境中替换 VMware Directory Service 证书

   在升级过程中，您的环境可能暂时包括 vCenter Single Sign-On 版本 5.5 和 vCenter Single Sign-On 版本 6.x。在此情况下，如果替换正在运行 vCenter Single Sign-On 服务的节点的 SSL 证书，则必须执行其他步骤才能替换 VMware Directory Service SSL 证书。

请求证书并导入自定义根证书

可以使用企业或第三方 CA 的自定义证书。第一步是向 CA 请求证书并将根证书导入 VECS。

前提条件

证书必须满足以下要求：

- 密钥大小：2048 位或更大（PEM 编码）
- PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。密钥添加到 VECS 后，会转换为 PKCS8。
- x509 版本 3
- 对于根证书，CA 扩展必须设置为 true，并且 cert 签名必须在要求列表中。
- SubjectAltName 必须包含 DNS Name=<machine_FQDN>。
- CRT 格式
- 包含以下密钥使用：数字签名、不可否认性、密钥加密
- 比当前时间早一天的开始时间。
- CN（和 SubjectAltName）设置为 vCenter Server 清单中的 ESXi 主机的主机名（或 IP 地址）。

步骤

1 向企业或第三方证书提供商发送以下证书的 CSR。

   - 每个计算机具有一个计算机 SSL 证书。对于计算机 SSL 证书，SubjectAltName 字段必须包含完全限定域名 (DNS NAME=*machine_FQDN*)
   - （可选）每个嵌入式系统或管理节点具有四个解决方案用户证书。解决方案用户证书不应包括 IP 地址、主机名或电子邮件地址。每个证书必须具有不同的证书主体。
   - （可选）用于外部 Platform Services Controller 实例的计算机解决方案用户证书。该证书不同于 Platform Services Controller 的计算机 SSL 证书。

   通常，结果为信任链的 PEM 文件以及每个 Platform Services Controller 或管理节点的签名 SSL 证书。

2 列出 TRUSTED_ROOTS 存储和计算机 SSL 存储。

```
vecs-cli store list
```

   a 确保当前根证书和所有计算机 SSL 证书均为 VMCA 签名证书。

   b 请记下“序列号”、“颁发者”和“主体 CN”字段。

   c （可选）使用 Web 浏览器，打开与将替换证书的节点的 HTTPS 连接，检查证书信息，并确保该信息与计算机 SSL 证书相匹配。

3 停止所有服务，启动处理证书创建、传播和存储的服务。

服务名称在 Windows 和 vCenter Server Appliance 上有所不同。

注 如果您的环境使用外部 Platform Services Controller，则不必停止和启动 vCenter Server 节点上的 VMware Directory Service (vmdird) 和 VMware Certificate Authority (vmcad)。这些服务在 Platform Services Controller 上运行。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

4 发布自定义 root 证书。

```
dir-cli trustedcert publish --cert <my_custom_root>
```

如果在命令行上不指定用户名和密码，系统会提示您。

5 重新启动所有服务。

```
service-control --start --all
```

后续步骤

如果公司策略需要，可以从证书存储中移除原始的 VMCA 根证书。如果执行此操作，则必须刷新 vCenter Single Sign-On 证书。请参见刷新 Security Token Service 证书。

将计算机 SSL 证书替换为自定义证书

收到自定义证书后，可以替换每个计算机证书。

每台计算机都必须拥有可用于与其他服务进行安全通信的计算机 SSL 证书。在多节点部署中，必须在每个节点上运行计算机 SSL 证书生成命令。使用 `--server` 参数从具有外部 Platform Services Controller 的 vCenter Server 指向 Platform Services Controller。

必须具有以下信息才能开始替换证书：

- administrator@vsphere.local 的密码。
- 有效的计算机 SSL 自定义证书（`.crt` 文件）。
- 有效的计算机 SSL 自定义密钥（`.key` 文件）。
- Root 的有效自定义证书（`.crt` 文件）。

- 如果您在多节点部署中具有外部 Platform Services Controller 的 vCenter Server 上运行命令，则需要 Platform Services Controller 的 IP 地址。

前提条件

必须已从第三方或企业 CA 收到每个计算机的证书。

- 密钥大小：2048 位或更大（PEM 编码）
- CRT 格式
- x509 版本 3
- SubjectAltName 必须包含 DNS Name=<machine_FQDN>。
- 包含以下密钥使用：数字签名、不可否认性、密钥加密

步骤

1 停止所有服务，启动处理证书创建、传播和存储的服务。

服务名称在 Windows 和 vCenter Server Appliance 上有所不同。

注 如果您的环境使用外部 Platform Services Controller，则不必停止和启动 vCenter Server 节点上的 VMware Directory Service (vmdird) 和 VMware Certificate Authority (vmcad)。这些服务在 Platform Services Controller 上运行。

Windows

```
service-control --stop --all
service-control --start VMWareAfdService
service-control --start VMWareDirectoryService
service-control --start VMWareCertificateService
```

vCenter Server Appliance

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmcad
```

2 登录到每个节点，然后将您从 CA 接收到的新的计算机证书添加到 VECS。

所有计算机都需要本地证书存储中的新证书来通过 SSL 进行通信。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert <cert-file-path>
--key <key-file-path>
```

3 重新启动所有服务。

```
service-control --start --all
```

示例：将计算机 SSL 证书替换为自定义证书

以下示例展示了如何将 Windows 安装上的计算机 SSL 证书替换为自定义证书。可以以同样方法替换每个节点上的计算机 SSL 证书。

1 首先，删除 VECS 中的现有证书。

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store MACHINE_SSL_CERT --
alias __MACHINE_CERT
```

2 接下来，添加替换证书。

```
"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store MACHINE_SSL_CERT --
alias __MACHINE_CERT --cert E:\custom-certs\ms-ca\signed-ssl\custom-w1-vim-cat-
dhcp-094.eng.vmware.com.crt --key E:\custom-certs\ms-ca\signed-ssl\custom-x3-vim-cat-
dhcp-1128.vmware.com.priv
```

将解决方案用户证书替换为自定义证书

在替换计算机 SSL 证书后，可以将 VMCA 签名解决方案用户证书替换为第三方或企业证书。

许多 VMware 客户未替换解决方案用户证书。他们仅将计算机 SSL 证书替换为自定义证书。这种混合方法符合其安全团队的要求。

- 证书位于代理后面或是自定义证书。
- 未使用中间 CA。

解决方案用户仅使用证书对 vCenter Single Sign-On 进行身份验证。如果证书有效，vCenter Single Sign-On 将向解决方案用户分配 SAML 令牌，并且解决方案用户将使用该 SAML 令牌对其他 vCenter 组件进行身份验证。

替换每个管理节点和每个 Platform Services Controller 节点上的计算机解决方案用户证书。只能替换每个管理节点上的其他解决方案用户证书。在具有外部 `--server` 的管理节点上运行命令时，请使用 Platform Services Controller 参数指向 Platform Services Controller。

注 在大型部署中列出解决方案用户证书时，`dir-cli list` 的输出包括所有节点的所有解决方案用户。运行 `vmafd-cli get-machine-id --server-name localhost` 以查找每个主机的本地计算机 ID。每个解决方案用户名称均包括计算机 ID。

前提条件

- 密钥大小：2048 位或更大（PEM 编码）
- CRT 格式
- x509 版本 3
- SubjectAltName 必须包含 DNS Name=<machine_FQDN>。
- 每个解决方案用户证书必须具有不同的 `Subject`。例如，考虑包含解决方案用户名（如 vpxd）或其他唯一标识符。

- 包含以下密钥使用：数字签名、不可否认性、密钥加密

步骤

1 停止所有服务，启动处理证书创建、传播和存储的服务。

```
service-control --stop --all
service-control --start vmafdd
service-control --start vmdird
service-control --start vmca
```

2 查找每个解决方案用户的名称。

```
dir-cli service list
```

可以使用替换证书时返回的唯一 ID。输入和输出可能显示如下。

```
C:\Program Files\VMware\vCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

在多节点部署中列出解决方案用户证书时，`dir-cli` 列表输出将包含所有节点的所有解决方案用户。运行 `vmafd-cli get-machine-id --server-name localhost` 以查找每个主机的本地计算机 ID。每个解决方案用户名称均包括计算机 ID。

3 对于每个解决方案用户，请依次替换 VECS 和 vmdir 中的现有证书。

必须以该顺序添加证书。

```
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
dir-cli service update --name <vpxd-xxxx-xxx-xxxxxx> --cert vpxd.crt
```

注 如果不替换 vmdir 中的证书，则解决方案用户无法对 vCenter Single Sign-On 进行身份验证。

4 重新启动所有服务。

```
service-control --start --all
```

在混合模式环境中替换 VMware Directory Service 证书

在升级过程中，您的环境可能暂时包括 vCenter Single Sign-On 版本 5.5 和 vCenter Single Sign-On 版本 6.x。在此情况下，如果替换正在运行 vCenter Single Sign-On 服务的节点的 SSL 证书，则必须执行其他步骤才能替换 VMware Directory Service SSL 证书。

vmdir 使用 VMware Directory Service SSL 证书可在执行 vCenter Single Sign-On 复制的 Platform Services Controller 节点之间执行握手操作。

同时包括 vSphere 6.0 和 vSphere 6.5 节点的混合模式环境不需要执行这些步骤。仅在以下情况下需要执行这些步骤：

- 环境中同时包括 vCenter Single Sign-On 5.5 和 vCenter Single Sign-On 6.x 服务。
- vCenter Single Sign-On 服务设置为复制 vmdir 数据。
- 对于运行 vCenter Single Sign-On 6.x 服务的节点，计划将默认 VMCA 签名证书替换为自定义证书。

注 最佳做法是在重新启动服务之前先升级整个环境。通常不建议替换 VMware Directory Service 证书。

步骤

1 在运行 vCenter Single Sign-On 5.5 服务的节点上，请先设置环境以便熟悉 vCenter Single Sign-On 6.x 服务。

   a 备份所有文件 `C:\ProgramData\VMware\CIS\cfg\vmdird`。

   b 在 6.x 节点上创建 `vmdircert.pem` 文件的副本，并将其重命名为 `<sso_node2.domain.com>.pem`，其中 `<sso_node2.domain.com>` 是 6.x 节点的 FQDN。

   c 将重命名的证书复制到 `C:\ProgramData\VMware\CIS\cfg\vmdird` 以替换现有的复制证书。

2 在已替换证书的所有计算机上重新启动 VMware Directory Service。

   可以从 vSphere Client 中重新启动服务或使用 `service-control` 命令。

使用 CLI 命令管理服务和证书

4

一组 CLI 可用于管理 VMCA（VMware Certificate Authority）、VECS（VMware Endpoint Certificate Store）以及 VMware Directory Service (vmdir)。vSphere Certificate Manager 实用程序也支持许多相关任务，但手动证书管理和管理其他服务需要使用 CLI。

您通常使用 SSH 连接到设备 shell，访问 CLI 工具以管理证书和关联服务。有关详细信息，请参见 VMware 知识库文章，网址为 http://kb.vmware.com/kb/2100508。

手动证书替换提供了关于使用 CLI 命令替换证书的示例。

表 4-1. 用于管理证书和关联服务的 CLI 工具

CLI	描述	请参见
`certool`	生成并管理证书和密钥。属于 VMCAD（VMware 证书管理服务）的一部分。	certool 初始化命令参考
`vecs-cli`	管理 VMware 证书存储实例的内容。属于 VMAFD。	vecs-cli 命令参考
`dir-cli`	在 VMware Directory Service 中创建并更新证书。属于 VMAFD。	dir-cli 命令参考
`sso-config`	某些 vCenter Single Sign-On 配置。在大多数情况下，使用 vSphere Web Client 或 vSphere Client。使用该命令进行双因素身份验证设置。	命令行帮助。 了解 vCenter Server 双因素身份验证
`service-control`	启动或停止服务，例如，在证书替换工作流中。	在运行其他 CLI 命令之前，运行此命令以停止服务。

CLI 位置

默认情况下，可以在每个节点的以下位置查找 CLI。

Windows

```
C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe
C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli.exe
C:\Program Files\VMware\vCenter Server\vmcad\certool.exe
C:\Program Files\VMware\VCenter server\VMware Identity Services\sso-config
```

	VCENTER_INSTALL_PATH\bin\service-control
Linux	/usr/lib/vmware-vmafd/bin/vecs-cli /usr/lib/vmware-vmafd/bin/dir-cli /usr/lib/vmware-vmca/bin/certool /opt/vmware/bin 在 Linux 上，service-control 命令不要求您指定路径。

如果从具有外部 Platform Services Controller 部署的 vCenter Server 系统运行命令，则可以使用 --server 参数指定 Platform Services Controller。

本章讨论了以下主题：

- 运行 CLI 所需的特权
- 更改 certool 配置选项
- certool 初始化命令参考
- certool 管理命令参考
- vecs-cli 命令参考
- dir-cli 命令参考

运行 CLI 所需的特权

所需的特权取决于您使用的 CLI 以及要运行的命令。例如，对于大多数证书管理操作，您必须是本地 vCenter Single Sign-On 域（默认为 vsphere.local）的管理员。有些命令可供所有用户使用。

dir-cli	必须是本地域（默认为 vsphere.local）的管理员组成员才能运行 dir-cli 命令。如果不指定用户名和密码，系统将提示您输入本地 vCenter Single Sign-On 域的管理员（默认为 administrator@vsphere.local）的密码。
vecs-cli	最初，只有存储所有者和拥有完整访问特权的用户才能访问存储。Windows 上的管理员组中的用户和 Linux 上的 root 用户拥有完整访问特权。 MACHINE_SSL_CERT 和 TRUSTED_ROOTS 存储属于特殊存储。仅有 root 用户或管理员用户（取决于安装的类型）拥有完整的访问权限。
certool	大多数 certool 命令需要该用户是管理员组的成员。所有用户可以运行以下命令。 ■ genselfcacert ■ initscr ■ getdc ■ waitVMDIR ■ waitVMCA

- genkey
- viewcert

更改 certool 配置选项

运行 certool --gencert 或某些其他证书初始化或管理命令时，命令会读取配置文件中的所有值。可以在命令行中编辑现有文件，使用 --config=<file name> 选项替代默认配置文件，或者替代值。

默认情况下，配置文件 certool.cfg 位于以下位置。

操作系统	位置
Linux	/usr/lib/vmware-vmca/config
Windows	C:\Program Files\VMware\vCenter Server\vmcad\

文件包含具有以下默认值的多个字段：

```
Country = US
Name= Acme
Organization = AcmeOrg
OrgUnit = AcmeOrg Engineering
State = California
Locality = Palo Alto
IPAddress = 127.0.0.1
Email = email@acme.com
Hostname = server.acme.com
```

如下所示，通过在命令行中指定已修改的文件，或者通过在命令行中替代单个值，可以更改这些值。

- 创建配置文件的副本，然后编辑该文件。使用 --config 命令行选项指定该文件。指定完整路径，避免路径名称问题。
- ```
  certool --gencert --config C:\Temp\myconfig.cfg
  ```
- 在命令行中替代单个值。例如，要替代局部性，请运行以下命令：

  ```
  certool --gencert --privkey=private.key --Locality="Mountain View"
  ```

指定 --Name 以替换证书的主体名称的 CN 字段。

- 对于解决方案用户证书，按照约定，该名称为 <sol_user name>@<domain>，但如果在环境中使用其他约定，则可以更改该名称。
- 对于计算机 SSL 证书，使用计算机的 FQDN。

  VMCA 仅允许使用一个 DNSName（在 Hostname 字段中），但不允许使用其他任何别名选项。如果 IP 地址由用户指定，则也会存储在 SubAltName 中。

使用 --Hostname 参数指定证书的 SubAltName 的 DNSName。
  ```

certool 初始化命令参考

certool 初始化命令可以生成证书签名请求、查看和生成 VMCA 签名的证书和密钥、导入根证书以及执行其他证书管理操作。

在许多情况下，您可以将配置文件传递到 certool 命令中。请参见更改 certool 配置选项。有关一些用法示例，请参见将现有 VMCA 签名证书替换为新的 VMCA 签名证书。命令行帮助提供了有关选项的详细信息。

certool --initcsr

生成证书签名请求 (CSR)。此命令可生成 PKCS10 文件和专用密钥。

选项	描述
--initcsr	生成 CSR 时为必需项。
--privkey <key_file>	专用密钥文件的名称。
--pubkey <key_file>	公用密钥文件的名称。
--csrfile <csr_file>	发送到 CA 提供程序的 CSR 文件的文件名。
--config <config_file>	配置文件的可选名称。默认为 certool.cfg。

例如：

```
certool --initcsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

certool --selfca

创建自签名证书并使用自签名的根 CA 置备 VMCA 服务器。使用此选项是置备 VMCA 服务器最简单的方法之一。您也可以改用第三方根证书置备 VMCA 服务器，从而使 VMCA 成为中间 CA。请参见使用 VMCA 作为中间证书颁发结构。

此命令将生成日期早三天的证书以避免出现时区冲突。

选项	描述
--selfca	生成自签名证书时为必需项。
--predate <number_of_minutes>	允许您将根证书的“有效起始日期”字段设置为当前时间之前的指定分钟数。此选项有助于解决潜在的时区问题。最大值为三天。
--config <config_file>	配置文件的可选名称。默认为 certool.cfg。
--server <server>	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。

例如：

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280  --selfca --server= 192.0.2.24 --srp-upn=administrator@vsphere.local
```

certool --rootca

导入根证书。将指定的证书和专用密钥添加到 VMCA。VMCA 始终使用最新根证书进行签名，但其他根证书仍然受信任，直到您手动将它们删除为止。这意味着，您可以一步一步地更新基础架构，最后删除不再使用的证书。

选项	描述
`--rootca`	导入根 CA 时为必需项。
`--cert <certfile>`	证书文件的名称。
`--privkey <key_file>`	专用密钥文件的名称。该文件必须是 PEM 编码的格式。
`--server <server>`	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。

例如：

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

certool --getdc

返回 vmdir 使用的默认域名。

选项	描述
`--server <server>`	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。
`--port <port_num>`	可选的端口号。默认为端口 389。

例如：

```
certool --getdc
```

certool --waitVMDIR

等待 VMware Directory Service 运行或等待 `--wait` 指定的超时结束。将此选项与其他选项配合使用可调度特定任务，例如返回默认域名。

选项	描述
`--wait`	可选的等待分钟数。默认值为“3”。
`--server <server>`	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。
`--port <port_num>`	可选的端口号。默认为端口 389。

例如：

```
certool --waitVMDIR --wait 5
```

certool --waitVMCA

等待 VMCA 服务运行或等待指定的超时结束。将此选项与其他选项配合使用可调度特定任务，例如生成证书。

选项	描述
`--wait`	可选的等待分钟数。默认值为“3”。
`--server <server>`	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。
`--port <port_num>`	可选的端口号。默认为端口 389。

例如：

```
certool --waitVMCA --selfca
```

certool --publish-roots

强制更新根证书。此命令需要管理特权。

选项	描述
`--server <server>`	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。

例如：

```
certool --publish-roots
```

certool 管理命令参考

使用 `certool` 管理命令，您可以查看、生成和吊销证书以及查看有关证书的信息。

certool --genkey

生成专用和公用密钥对。这些文件随后可用于生成 VMCA 签名的证书。

选项	描述
`--genkey`	生成专用和公用密钥时为必需项。
`--privkey <keyfile>`	专用密钥文件的名称。
`--pubkey <keyfile>`	公用密钥文件的名称。
`--server <server>`	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。

例如：

```
certool --genkey --privkey=<filename> --pubkey=<filename>
```

certool --gencert

从 VMCA 服务器中生成证书。此命令使用 `certool.cfg` 或指定配置文件中的信息。您可以使用该证书置备计算机证书或解决方案用户证书。

选项	描述
`--gencert`	生成证书时为必需项。
`--cert <certfile>`	证书文件的名称。该文件必须是 PEM 编码的格式。
`--privkey <keyfile>`	专用密钥文件的名称。该文件必须是 PEM 编码的格式。
`--config <config_file>`	配置文件的可选名称。默认为 `certool.cfg`。
`--server <server>`	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。

例如：

```
certool --gencert --privkey=<filename> --cert=<filename>
```

certool --getrootca

以人工可读形式打印当前根 CA 证书。如果要在管理节点中运行此命令，请使用 Platform Services Controller 节点的计算机名称来检索根 CA。此输出无法用作证书，它将更改为人工可读。

选项	描述
`--getrootca`	打印根证书时为必需项。
`--server <server>`	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。

例如：

```
certool --getrootca --server=remoteserver
```

certool --viewcert

以人工可读形式打印证书中的所有字段。

选项	描述
`--viewcert`	查看证书时为必需项。
`--cert <certfile>`	配置文件的可选名称。默认为 `certool.cfg`。

例如：

```
certool --viewcert --cert=<filename>
```

certool --enumcert

列出 VMCA 服务器了解的所有证书。通过所需的 `filter` 选项，可以列出所有证书或仅列出已吊销、活动或过期的证书。

选项	描述
`--enumcert`	列出所有证书时为必需项。
`--filter [all | active]`	所需的筛选器。指定所有或活动。当前不支持已吊销和过期选项。

例如：

```
certool --enumcert --filter=active
```

certool --status

向 VMCA 服务器发送指定的证书以检查该证书是否已吊销。如果证书已吊销，则输出 `Certificate: REVOKED`，否则输出 `Certificate: ACTIVE`。

选项	描述
`--status`	检查证书状态时为必需项。
`--cert <certfile>`	配置文件的可选名称。默认为 `certool.cfg`。
`--server <server>`	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。

例如：

```
certool --status --cert=<filename>
```

certool --genselfcacert

根据配置文件中的值生成一个自签名证书。此命令将生成日期早三天的证书以避免出现时区冲突。

选项	描述
`--genselfcacert`	生成自签名证书时为必需项。
`--outcert <cert_file>`	证书文件的名称。该文件必须是 PEM 编码的格式。
`--outprivkey <key_file>`	专用密钥文件的名称。该文件必须是 PEM 编码的格式。
`--config <config_file>`	配置文件的可选名称。默认为 `certool.cfg`。

例如：

```
certool --genselfcert --privkey=<filename> --cert=<filename>
```

vecs-cli 命令参考

vecs-cli 命令集可用于管理 VMware Certificate Store (VECS) 实例。将这些命令与 dir-cli 和 certool 配合使用可管理证书基础架构和其他 Platform Services Controller 服务。

vecs-cli store create

创建证书存储。

选项	描述
--name <name>	证书存储的名称。
--server <server-name>	如果您连接到远程 VECS 实例，则用于指定服务器名称。
--upn <user-name>	用于登录到--server <server-name> 指定的服务器实例的用户主体名称。创建库时，会在当前用户环境中创建。因此，该库的所有者是当前用户环境，而不总是 root 用户。

例如：

```
vecs-cli store create --name <store>
```

vecs-cli store delete

删除证书存储。无法删除 MACHINE_SSL_CERT、TRUSTED_ROOTS 和 TRUSTED_ROOT_CRLS 系统存储。具有必需特权的用户可以删除解决方案用户存储。

选项	描述
--name <name>	要删除的证书存储的名称。
--server <server-name>	如果您连接到远程 VECS 实例，则用于指定服务器名称。
--upn <user-name>	用于登录到--server <server-name> 指定的服务器实例的用户主体名称。创建库时，会在当前用户环境中创建。因此，该库的所有者是当前用户环境，而不总是 root 用户。

例如：

```
vecs-cli store delete --name <store>
```

vecs-cli store list

列出证书存储。

选项	描述
`--server <server-name>`	如果您连接到远程 VECS 实例，则用于指定服务器名称。
`--upn <user-name>`	用于登录到`--server <server-name>` 指定的服务器实例的用户主体名称。创建库时，会在当前用户环境中创建。因此，该库的所有者是当前用户环境，而不总是 root 用户。

VECS 包括以下库。

表 4-2. VECS 中的库

库	描述
计算机 SSL 库 (MACHINE_SSL_CERT)	■ 由每个 vSphere 节点上的反向代理服务使用。 ■ 由 VMware Directory Service (vmdir) 在嵌入式部署和每个 Platform Services Controller 节点上使用。 vSphere 6.0 及更高版本中的所有服务通过使用计算机 SSL 证书的反向代理进行通信。为了实现向后兼容性，5.x 服务仍使用特定端口。因此，某些服务（如 vpxd）仍使其自身的端口处于打开状态。
受信任的根存储 (TRUSTED_ROOTS)	包含所有受信任的根证书。
解决方案用户库 ■ `machine` ■ `vpxd` ■ `vpxd-extension` ■ `vsphere-webclient`	VECS 为每个解决方案用户提供一个库。每个解决方案用户证书的主体必须是唯一的，例如 machine 证书不能具有与 vpxd 证书相同的主体。 解决方案用户证书用于对 vCenter Single Sign-On 进行身份验证。vCenter Single Sign-On 会检查证书是否有效，但不检查其他证书属性。在嵌入式部署中，所有解决方案用户证书都位于相同的系统中。 以下解决方案用户证书存储包括在每个管理节点和每个嵌入式部署的 VECS 中： ■ `machine`：由组件管理器、许可证服务器和日志记录服务使用。 注 Machine 解决方案用户证书与计算机 SSL 证书没有任何关系。计算机解决方案用户证书用于进行 SAML 令牌交换。计算机 SSL 证书用于计算机的安全 SSL 连接。 ■ `vpxd`：vCenter 服务守护程序 (vpxd) 存储位于管理节点和嵌入式部署上。vpxd 使用此存储中存储的解决方案用户证书对 vCenter Single Sign-On 进行身份验证。 ■ `vpxd-extension`：vCenter 扩展存储。包括 Auto Deploy 服务、Inventory Service 以及不属于其他解决方案用户的其他服务。 ■ `vsphere-webclient`：vSphere Web Client 存储。还包括其他一些服务，例如性能图表服务。 每个 Platform Services Controller 节点包含一个 `machine` 证书。

表 4-2. VECS 中的库（续）

库	描述
vSphere 证书管理器实用程序备份库 (BACKUP_STORE)	由 VMCA（VMware 证书管理器）用来支持证书恢复。仅将最近的状态存储为备份，无法返回多个步骤。
其他库	解决方案可能会添加其他库。例如，Virtual Volumes 解决方案会添加 SMS 库。请勿修改这些库中的证书，除非 VMware 文档或 VMware 知识库文章要求进行此类修改。 **注** 删除 TRUSTED_ROOTS_CRLS 存储可能会损坏证书基础架构。请勿删除或修改 TRUSTED_ROOTS_CRLS 存储。

例如：

```
vecs-cli store list
```

vecs-cli store permissions

授予或撤销对存储的权限。使用 `--grant` 或 `--revoke` 选项。

存储所有者可以执行所有操作，包括授予和撤销权限。本地 vCenter Single Sign-On 域的管理员（默认为 administrator@vsphere.local）对所有存储具有所有特权，包括授予和撤销权限。

您可以使用 `vecs-cli get-permissions --name <store-name>` 检索存储的当前设置。

选项	描述
`--name <name>`	证书存储的名称。
`--user <username>`	被授予权限的用户的唯一名称。
`--grant [read|write]`	授予读取或写入权限。
`--revoke [read|write]`	撤销读取或写入权限。当前不受支持。

vecs-cli store get-permissions

检索存储的当前权限设置。

选项	描述
`--name <name>`	证书存储的名称。
`--server <server-name>`	如果您连接到远程 VECS 实例，则用于指定服务器名称。
`--upn <user-name>`	用于登录到`--server <server-name>` 指定的服务器实例的用户主体名称。创建库时，会在当前用户环境中创建。因此，该库的所有者是当前用户环境，而不总是 root 用户。

vecs-cli entry create

在 VECS 中创建一个条目。使用此命令向存储中添加一个专用密钥或证书。

选项	描述
--store <NameOfStore>	证书存储的名称。
--alias <Alias>	证书的可选别名。对于受信任的 root 库，将忽略此选项。
--cert <certificate_file_path>	证书文件的完整路径。
--key <key-file-path>	与证书对应的密钥的完整路径。 可选。
--password <password>	加密专用密钥的可选密码。
--server <server-name>	如果您连接到远程 VECS 实例，则用于指定服务器名称。
--upn <user-name>	用于登录到--server <server-name> 指定的服务器实例的用户主体名称。创建库时，会在当前用户环境中创建。因此，该库的所有者是当前用户环境，而不总是 root 用户。

vecs-cli entry list

列出指定存储中的所有条目。

选项	描述
--store <NameOfStore>	证书存储的名称。

vecs-cli entry getcert

从 VECS 中检索证书。可以将证书发送到输出文件或将其显示为人工可读的文本。

选项	描述
--store <NameOfStore>	证书存储的名称。
--alias <Alias>	证书的别名。
--output <output_file_path>	要向其写入证书的文件。
--text	显示证书的人工可读版本。
--server <server-name>	如果您连接到远程 VECS 实例，则用于指定服务器名称。
--upn <user-name>	用于登录到--server <server-name> 指定的服务器实例的用户主体名称。创建库时，会在当前用户环境中创建。因此，该库的所有者是当前用户环境，而不总是 root 用户。

vecs-cli entry getkey

检索存储在 VECS 中的密钥。可以将密钥发送到输出文件或将其显示为人工可读的文本。

选项	描述
--store <NameOfStore>	证书存储的名称。
--alias <Alias>	密钥的别名。
--output <output_file_path>	要向其写入密钥的输出文件。

选项	描述
`--text`	显示密钥的人工可读版本。
`--server <server-name>`	如果您连接到远程 VECS 实例，则用于指定服务器名称。
`--upn <user-name>`	用于登录到`--server <server-name>` 指定的服务器实例的用户主体名称。创建库时，会在当前用户环境中创建。因此，该库的所有者是当前用户环境，而不总是 root 用户。

vecs-cli entry delete

删除证书存储中的条目。如果删除 VECS 中的条目，则会将其从 VECS 中永久移除。唯一的例外是当前根证书。VECS 轮询根证书的 vmdir。

选项	描述
`--store <NameOfStore>`	证书存储的名称。
`--alias <Alias>`	要删除的条目的别名。
`--server <server-name>`	如果您连接到远程 VECS 实例，则用于指定服务器名称。
`--upn <user-name>`	用于登录到`--server <server-name>` 指定的服务器实例的用户主体名称。创建库时，会在当前用户环境中创建。因此，该库的所有者是当前用户环境，而不总是 root 用户。
`-y`	取消确认提示。仅适用于高级用户。

vecs-cli force-refresh

强制刷新 VECS。默认情况下，VECS 会每 5 分钟轮询 vmdir 中的新根证书文件。使用此命令即时更新 vmdir 中的 VECS。

选项	描述
`--server <server-name>`	如果您连接到远程 VECS 实例，则用于指定服务器名称。
`--upn <user-name>`	用于登录到`--server <server-name>` 指定的服务器实例的用户主体名称。创建库时，会在当前用户环境中创建。因此，该库的所有者是当前用户环境，而不总是 root 用户。

dir-cli 命令参考

`dir-cli` 实用程序支持在 VMware Directory Service (vmdir) 中创建和更新解决方案用户、管理帐户以及管理证书和密码。您也可以使用 `dir-cli` 管理和查询 Platform Services Controller 实例的域功能级别。

dir-cli nodes list

列出指定的 Platform Services Controller 实例的所有 vCenter Server 系统。

选项	描述
--login <admin_user_id>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。
--server <psc_ip_or_fqdn>	如果您不需要将关联的 Platform Services Controller 作为目标，则使用此选项。指定 Platform Services Controller 的 IP 地址或 FQDN。

dir-cli computer password-reset

使您能够重置域中计算机帐户的密码。如果需要还原 Platform Services Controller 实例，此选项非常有用。

选项	描述
--login <admin_user_id>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。
--live-dc-hostname <server name>	Platform Services Controller 实例的当前名称。

dir-cli service create

创建解决方案用户。主要供第三方解决方案使用。

选项	描述
--name <name>	要创建的解决方案用户的名称
--cert <cert file>	证书文件的路径。这可以是 VMCA 签名的证书或第三方证书。
--ssogroups <comma-separated-groupnames>	将解决方案用户设置为指定组的成员。
--wstrustrole <ActAsUser>	将解决方案用户设置为内置管理员或用户组的成员。换句话说，确定解决方案用户是否具有管理特权。
--ssoadminrole <Administrator/User>	将解决方案用户设置为 ActAsUser 组的成员。ActAsUser 角色让用户可以代表其他用户执行操作。
--login <admin_user_id>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli service list

列出 dir-cli 了解的解决方案用户。

选项	描述
--login <admin_user_id>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli service delete

删除 vmdir 中的解决方案用户。删除该解决方案用户后，所有关联的服务将对使用此 vmdir 实例的所有管理节点不可用。

选项	描述
`--name`	要删除的解决方案用户的名称。
`--login <admin_user_id>`	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
`--password <admin_password>`	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli service update

更新指定的解决方案用户的证书，即服务集合。运行此命令后，VECS 将在 5 分钟后实现此更改，或可以使用 `vecs-cli force-refresh` 强制刷新。

选项	描述
`--name <name>`	要更新的解决方案用户的名称。
`--cert <cert_file>`	要分配给服务的证书名称。
`--login <admin_user_id>`	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
`--password <admin_password>`	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli user create

创建 vmdir 中的常规用户。此命令可用于使用用户名和密码对 vCenter Single Sign-On 进行身份验证的人工用户。只能在原型构建期间使用此命令。

选项	描述
`--account <name>`	要创建的 vCenter Single Sign-On 用户的名称。
`--user-password <password>`	用户的初始密码。
`--first-name <name>`	用户的名字。
`--last-name <name>`	用户的姓氏。
`--login <admin_user_id>`	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
`--password <admin_password>`	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli user modify

删除 vmdir 中的指定用户。

选项	描述
`--account <name>`	要删除的 vCenter Single Sign-On 用户的名称。
`--password-never-expires`	如果要为必须向 Platform Services Controller 进行身份验证的自动任务创建用户帐户，并且要确保这些任务不会因密码过期而停止运行，请将该选项设为 true。 谨慎使用该选项。
`--password-expires`	如果要恢复 `--password-never-expires` 选项，请将该选项设为 true。
`--login <admin_user_id>`	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
`--password <admin_password>`	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli user delete

删除 vmdir 中的指定用户。

选项	描述
`--account <name>`	要删除的 vCenter Single Sign-On 用户的名称。
`--login <admin_user_id>`	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
`--password <admin_password>`	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli user find-by-name

按名称在 vmdir 中查找用户。此命令返回的信息取决于您在 `--level` 选项中指定的设置。

选项	描述
`--account <name>`	要删除的 vCenter Single Sign-On 用户的名称。
`--level <info level 0|1|2>`	返回下列信息： ■ 级别 0 - 帐户和 UPN ■ 级别 1 - 级别 0 信息 + 名和姓 ■ 级别 2：级别 0 + 帐户禁用标记、帐户锁定标记、密码永不过期标记、密码已过期标记和密码过期标记。 默认级别为 0。
`--login <admin_user_id>`	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
`--password <admin_password>`	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli group modify

将用户或组添加到已存在的组。

选项	描述
--name <name>	vmdir 中组的名称。
--add <user_or_group_name>	要添加的用户或组的名称。
--login <admin_user_id>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli group list

列出指定的 vmdir 组。

选项	描述
--name <name>	vmdir 中组的可选名称。此选项可用于检查特定组是否存在。
--login <admin_user_id>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli ssogroup create

在本地域（默认为 vsphere.local）中创建组。

如果要创建组以管理 vCenter Single Sign-On 域中的用户权限，请使用此命令。例如，如果创建一个组，然后将其添加到 vCenter Single Sign-On 域的管理员组中，那么添加到该组的所有用户都将对该域拥有管理员权限。

也可以将 vCenter 清单对象权限分配给 vCenter Single Sign-On 域中的组。请参见《vSphere 安全性》文档。

选项	描述
--name <name>	vmdir 中组的名称。最大长度为 487 个字符。
--description <description>	组的可选描述。
--login <admin_user_id>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli trustedcert publish

将受信任的根证书发布到 vmdir。

选项	描述
--cert <file>	证书文件的路径。
--crl <file>	VMCA 不支持此选项。
--login <admin_user_id>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。

选项	描述
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。
--chain	如果发布的是链式证书，请指定此选项。不需要选项值。

dir-cli trustedcert publish

将受信任的根证书发布到 vmdir。

选项	描述
--cert <file>	证书文件的路径。
--crl <file>	VMCA 不支持此选项。
--login <admin_user_id>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。
--chain	如果发布的是链式证书，请指定此选项。不需要选项值。

dir-cli trustedcert unpublish

取消发布当前 vmdir 中的受信任根证书。例如，如果已将其他根证书添加到 vmdir 且该证书现在是您的环境中所有其他证书的根证书，则请使用此命令。取消发布不再使用的证书是强化环境的一部分。

选项	描述
--cert-file <file>	要取消发布的证书文件的路径。
--login <admin_user_id>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli trustedcert list

列出所有受信任的根证书及其对应的 ID。您需要证书 ID 才能使用 `dir-cli trustedcert get` 检索证书。

选项	描述
--login <admin_user_id>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli trustedcert get

从 vmdir 中检索受信任的根证书并将其写入到指定的文件。

选项	描述
--id <cert_ID>	要检索的证书的 ID。 dir-cli trustedcert list 命令显示 ID。
--outcert <path>	要将证书文件写入到的路径。
--outcrl <path>	要将 CRL 文件写入到的路径。当前未使用。
--login <admin_user_id>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli password create

创建符合密码要求的随机密码。此命令可供第三方解决方案用户使用。

选项	描述
--login <admin_user_id>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli password reset

可让管理员重置用户的密码。如果您是要重置密码的非管理员用户，则可使用 dir-cli password change。

选项	描述
--account	要向其分配新密码的帐户名称。
--new	指定用户的新密码。
--login <admin_user_id>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 administrator@vsphere.local。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli password change

可让用户更改其密码。您必须是拥有帐户的用户，才能执行此更改。管理员可以使用 dir-cli password reset 重置任何密码。

选项	描述
--account	帐户名称。
--current	拥有帐户的用户的当前密码。
--new	拥有帐户的用户的新密码。

对 Platform Services Controller 进行故障排除

5

以下主题提供对 Platform Services Controller 进行故障排除的起始步骤。有关其他说明，请搜索此文档中心和 VMware 知识库系统。

本章讨论了以下主题：

- 确定 Lookup Service 错误的原因
- 无法使用 Active Directory 域身份验证进行登录
- 由于用户帐户被锁定，vCenter Server 登录失败
- VMware 目录服务复制需要较长时间
- 导出 Platform Services Controller 支持包
- Platform Services Controller 服务日志引用

确定 Lookup Service 错误的原因

vCenter Single Sign-On 安装显示有关 vCenter Server、vSphere Client 或 vSphere Web Client 的错误。

问题

vCenter Server 和 Web Client 安装程序显示错误 `Could not contact Lookup Service. Please check VM_ssoreg.log...`。

原因

导致该问题的原因有多种，包括主机上的时钟未同步、防火墙阻止以及必须启动的服务未启动等。

解决方案

1. 验证运行 vCenter Single Sign-On、vCenter Server 和 Web Client 的主机上的时钟是否同步。
2. 查看错误消息中指明的特定日志文件。

   在该消息中，系统临时文件夹指的是 `%TEMP%`。

3 在日志文件中，搜索以下消息。

该日志文件包含所有安装尝试的输出内容。找到最后一条消息，其中显示 `Initializing registration provider...`

消息	原因和解决方案
`java.net.ConnectException: Connection timed out: connect`	IP 地址不正确、防火墙阻止了对 vCenter Single Sign-On 的访问，或者 vCenter Single Sign-On 过载。 确保防火墙未阻止 vCenter Single Sign-On 端口（默认为 7444）。还要确保安装 vCenter Single Sign-On 的计算机具有足够的可用 CPU、I/O 和 RAM 容量。
`java.net.ConnectException: Connection refused: connect`	IP 地址或 FQDN 不正确，并且 vCenter Single Sign-On 服务未启动或曾经启动过，但当前已停止运行。 通过检查 vCenter Single Sign-On 服务 (Windows) 和 vmware-sso 守护进程 (Linux) 的状态，确认 vCenter Single Sign-On 运行正常。 重新启动服务。如果重新启动不解决问题，请参见《vSphere 故障排除》指南中的“恢复”部分。
`Unexpected status code: 404. SSO Server failed during initialization`	重新启动 vCenter Single Sign-On。如果重新启动不解决问题，请参见《vSphere 故障排除》指南中的“恢复”部分。
UI 中显示的错误以 `Could not connect to vCenter Single Sign-On` 开头	您还会看到返回码 `SslHandshakeFailed`。此错误表明所提供的解析为 vCenter Single Sign-On 主机的 IP 地址或 FQDN 不是安装 vCenter Single Sign-On 时所使用的地址。 在 `%TEMP%\VM_ssoreg.log` 中，找到包含以下消息的行。 `host name in certificate did not match: <install-configured FQDN or IP> != <A> or <B> or <C>`，其中 A 表示您在 vCenter Single Sign-On 安装期间输入的 FQDN，B 和 C 表示系统生成的允许替代值。 将配置更正为使用该日志文件中的 `!=` 符号右侧的 FQDN。大多数情况下，使用在 vCenter Single Sign-On 安装期间指定的 FQDN。 如果这些替代值均不适用于您的网络配置，则请恢复您的 vCenter Single Sign-On SSL 配置。

无法使用 Active Directory 域身份验证进行登录

从 vSphere Client 或 vSphere Web Client 登录 vCenter Server 组件。使用您的 Active Directory 用户名和密码。身份验证失败。

问题

可将 Active Directory 标识源添加到 vCenter Single Sign-On，但用户无法登录 vCenter Server。

原因

用户使用他们的用户名和密码登录到默认域。对于所有其他域，用户必须包含域名（user@domain 或 DOMAIN\user）。

如果使用的是 vCenter Server Appliance，则可能存在其他问题。

解决方案

对于所有 vCenter Single Sign-On 部署，您可以更改默认标识源。执行此更改后，用户只能使用用户名和密码来登录默认标识源。

要使用 Active Directory 林中的子域配置集成 Windows 身份验证标识源，请参见 VMware 知识库文章，网址为 http://kb.vmware.com/kb/2070433. ）。默认情况下，集成的 Windows 身份验证使用 Active Directory 林的根域。

如果使用的是 vCenter Server Appliance，且更改默认标识源并未解决此问题，则请执行以下额外的故障排除步骤。

1 同步 vCenter Server Appliance 和 Active Directory 域控制器之间的时钟。

2 验证每个域控制器在 Active Directory 域 DNS 服务中是否均有指针记录 (PTR)。

验证域控制器的 PTR 记录信息与控制器的 DNS 名称是否匹配。使用 vCenter Server Appliance 时，运行以下命令来执行此任务：

a 要列出域控制器，请运行以下命令：

```
# dig SRV _ldap._tcp.my-ad.com
```

相关地址位于回答部分，如以下示例中所示：

```
;; ANSWER SECTION:
_ldap._tcp.my-ad.com. (...) my-controller.my-ad.com
...
```

b 对于每个域控制器，请运行以下命令验证正向和反向解析：

```
# dig my-controller.my-ad.com
```

相关地址位于回答部分，如以下示例中所示：

```
;; ANSWER SECTION:
my-controller.my-ad.com (...) IN A 控制器 IP 地址
...
```

```
# dig -x <controller IP address>
```

相关地址位于回答部分，如以下示例中所示：

```
;; ANSWER SECTION:
IP-in-reverse.in-addr.arpa. (...) IN PTR my-controller.my-ad.com
...
```

3 如果执行上述步骤未能解决问题，请从 Active Directory 域中移除 vCenter Server Appliance，然后重新加入域。请参见《vCenter Server Appliance 配置》文档。

4 关闭连接到 vCenter Server Appliance 的所有浏览器会话，然后重新启动所有服务。

```
/bin/service-control --restart --all
```

由于用户帐户被锁定，vCenter Server 登录失败

从 vSphere Client 或 vSphere Web Client 登录页面登录 vCenter Server 时，出现错误指示帐户被锁定。

问题

多次尝试均失败后，将无法使用 vCenter Single Sign-On 登录到 vSphere Client 或 vSphere Web Client。您会看到消息指明您的帐户被锁定。

原因

您已超出失败登录尝试次数上限。

解决方案

- 如果作为系统域（默认为 vsphere.local）中的用户进行登录，请要求您的 vCenter Single Sign-On 管理员解锁您的帐户。如果锁定在锁定策略中设为过期，则可以等待您的帐户解锁。vCenter Single Sign-On 管理员可以使用 CLI 命令解锁帐户。
- 如果以 Active Directory 或 LDAP 域中的用户身份登录，请要求您的 Active Directory 或 LDAP 管理员解锁您的帐户。

VMware 目录服务复制需要较长时间

如果环境中包括多个 Platform Services Controller 实例，其中一个 Platform Services Controller 实例不可用时，环境会继续工作。Platform Services Controller 再次可用时，通常会在 60 秒内复制用户数据和其他信息。但是，在某些特殊情况下，复制可能需要较长时间。

问题

在某些情况下，例如，如果环境中包括多个位于不同位置的 Platform Services Controller 实例，并在某个 Platform Services Controller 实例不可用时进行重大更改，则无法立即查看 VMware 目录服务实例之间的复制。例如，在复制完成之前，无法在其他实例中查看添加到可用 Platform Services Controller 实例的新用户。

原因

在正常操作期间，在一个 Platform Services Controller 实例（节点）上对 VMware 目录服务 (vmdir) 实例所做的更改大约会在 60 秒内显示在其直接复制合伙伙伴中。根据复制拓扑，一个节点中的更改可能需要通过中间节点传播才能到达每个节点上的每个 vmdir 实例。复制的信息包括使用 VMware vMotion 创建、克隆或迁移的虚拟机的用户信息、证书信息、许可证信息等详细信息。

如果复制链接已损坏（例如，由于网络中断或节点不可用），联合中的更改将无法聚合。不可用的节点恢复之后，每个节点均会尝试获取所有更改。最终，所有 vmdir 实例均会聚合为一致状态，但如果在一个节点不可用时出现大量更改，则可能需要一段时间才能达到一致状态。

解决方案

进行复制时，环境正常运行。请勿尝试解决问题，除非该问题已持续一个多小时之久。

导出 Platform Services Controller 支持包

可以导出包含 Platform Services Controller 服务的日志文件的支持包。导出后，可以在本地查看日志，或者将包发送给 VMware 技术支持。

前提条件

确认 Platform Services Controller 虚拟设备已成功部署和运行。

步骤

1. 从 Web 浏览器中，连接至 Platform Services Controller 管理界面，网址为 https://*platform_services_controller_ip*:5480
2. 以虚拟设备的 root 用户身份登录。
3. 从**操作**菜单中，选择**创建支持包**。
4. 除非浏览器设置阻止立即下载，否则支持包将保存到本地计算机。

Platform Services Controller 服务日志引用

Platform Services Controller 服务使用 syslog 进行日志记录。您可以查看日志文件，确定故障原因。

表 5-1. 服务日志

服务	描述
VMware Directory Service	默认情况下，vmdir 日志记录在 `/var/log/messages` 或 `/var/log/vmware/vmdird/` 中。 对于部署时的问题，`/var/log/vmware/vmdir/vmafdvmdirclient.log` 可能也包含有用的故障排除数据。
VMware Single Sign-On	vCenter Single Sign-On 日志记录在 `/var/log/vmware/sso/` 中。
VMware Certificate Authority (VMCA)	VMCA 服务日志位于 `/var/log/vmware/vmcad/vmcad-syslog.log`。
VMware Endpoint Certificate Store (VECS)	VECS 服务日志位于 `/var/log/vmware/vmafdd/vmafdd-syslog.log`。
VMware Lookup Service	查找服务日志位于 `/var/log/vmware/sso/lookupServer.log`。