

vSphere 身份验证

VMware vSphere 8.0

VMware ESXi 8.0

vCenter Server 8.0

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

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

**威睿信息技术（中国）有
限公司**
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

版权所有 © 2019-2022 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

目录

关于《vSphere 身份验证》 7

1 vSphere 证书管理和身份验证入门 9

- 管理 vCenter Server 证书 10
 - 使用 vSphere Client 管理 vCenter Server 证书 11
 - 使用 CLI 管理 vCenter Server 证书 11
- 管理 vCenter Server 身份验证服务 12
 - 使用 vSphere Client 管理 vCenter Server 身份验证服务 12
 - 使用脚本管理 vCenter Server 身份验证服务 13
- 管理 vCenter Server 13
 - 使用管理界面管理 vCenter Server 14
 - 使用 vCenter Server Shell 管理 vCenter Server 14
 - 将 vCenter Server 添加到 Active Directory 域 15

2 vSphere 安全证书 16

- 不同解决方案途径的 vSphere 证书要求 17
- vSphere 证书管理概览 21
 - 替换 vSphere 证书 23
 - vSphere 使用证书的情况 25
 - VMware Certificate Authority 和 VMware 核心标识服务 27
 - VMware Endpoint 证书存储概述 28
 - 管理 vSphere 证书吊销 30
 - 替换大型部署中的 vSphere 证书 30
- 使用 vSphere Client 管理证书 31
 - 使用 vSphere Client 浏览证书存储 32
 - 使用 vSphere Client 为 vCenter 证书过期警告设置阈值 32
 - 通过 vSphere Client 使用新的 VMCA 签名证书续订 VMCA 证书 33
 - 使用 vSphere Client 将证书替换为自定义证书 33
 - 使用 vSphere Client 为计算机 SSL 证书生成证书签名请求（自定义证书） 34
 - 使用 vSphere Client 将可信根证书添加到证书存储 35
 - 使用 vSphere Client 添加自定义证书 35
- 使用 vSphere Certificate Manager 实用程序管理证书 36
 - 使用 Certificate Manager 重新生成新的 VMCA 根证书并替换所有证书 38
 - 使用 Certificate Manager 将 VMCA 设为中间证书颁发机构 39
 - 使用 Certificate Manager 生成 CSR，并准备根证书（中间 CA） 40
 - 使用 Certificate Manager 将 VMCA 根证书替换为自定义签名证书并替换所有证书 41
 - 使用 Certificate Manager 将计算机 SSL 证书替换为 VMCA 证书（中间 CA） 42

使用 Certificate Manager 将解决方案用户证书替换为 VMCA 证书（中间 CA）	43
使用 Certificate Manager 将所有证书替换为自定义证书	44
使用 Certificate Manager 生成证书签名请求（自定义证书）	44
使用 Certificate Manager 将计算机 SSL 证书替换为自定义证书	45
使用 Certificate Manager 将解决方案用户证书替换为自定义证书	46
使用 Certificate Manager 重新发布旧证书以恢复上次执行的操作	47
使用 Certificate Manager 重置所有证书	48
手动替换 vSphere 证书	48
vCenter Server 服务停止和启动指南	48
使用 CLI 将现有 VMCA 签名证书替换为新的 VMCA 签名证书	49
使用 CLI 生成新的 VMCA 签名根证书	49
使用 CLI 将计算机 SSL 证书替换为 VMCA 签名证书	50
使用 CLI 将解决方案用户证书替换为新的 VMCA 签名证书	53
使用 CLI 将 VMCA 设为中间证书颁发机构	57
使用 CLI 替换根证书（中间 CA）	57
使用 CLI 替换计算机 SSL 证书（中间 CA）	60
使用 CLI 替换解决方案用户证书（中间 CA）	62
使用 CLI 将证书替换为自定义证书	67
使用 CLI 请求证书并导入自定义根证书	67
使用 CLI 将计算机 SSL 证书替换为自定义证书	68

3 vSphere 证书和服务 CLI 命令参考 70

certool 初始化命令参考	72
certool 管理命令参考	75
vecs-cli 命令参考	78
dir-cli 命令参考	83

4 使用 vCenter Single Sign-On 进行 vSphere 身份验证 90

如何使用 vCenter Single Sign-On 保护您的环境	91
了解 vCenter Server 身份提供程序联合	94
vCenter Server 身份提供程序联合的工作原理	94
vCenter Server 身份提供程序联合和增强型链接模式	95
vCenter Server 身份提供程序局限性和互操作性	97
vCenter Server 身份提供程序联合生命周期	98
配置 vCenter Server 身份提供程序联合	99
vCenter Server 身份提供程序联合配置过程流	99
使用可信根证书存储，而不使用 JRE 信任库	100
为 AD FS 配置 vCenter Server 身份提供程序联合	101
了解 vCenter Single Sign-On	104
vCenter Single Sign-On 组件	104
通过 vSphere 使用 vCenter Single Sign-On	105

vCenter Single Sign-On 域中的组	107
配置 vCenter Single Sign-On 标识源	109
vCenter Server 和 vCenter Single Sign-On 的标识源	109
设置 vCenter Single Sign-On 的默认域	110
添加或编辑 vCenter Single Sign-On 标识源	110
基于 LDAP 的 Active Directory 和 OpenLDAP 服务器标识源设置	112
Active Directory 标识源设置	113
使用 CLI 添加或移除标识源	114
vCenter Single Sign-On 使用 Windows 会话身份验证	115
管理 vCenter Server Security Token Service	115
使用 vSphere Client 刷新 vCenter Server STS 证书	116
使用 vSphere Client 导入并替换 vCenter Server STS 证书	118
使用命令行替换 vCenter Server STS 证书	118
使用 vSphere Client 查看活动的 vCenter Server STS 签名证书链	120
使用命令行确定 LDAPS SSL 证书的过期日期	120
管理 vCenter Single Sign-On 策略	121
编辑 vCenter Single Sign-On 密码策略	121
编辑 vCenter Single Sign-On 锁定策略	122
编辑 vCenter Single Sign-On 令牌策略	123
编辑 Active Directory（集成 Windows 身份验证）用户的密码过期通知	124
管理 vCenter Single Sign-On 用户和组	124
添加 vCenter Single Sign-On 用户	125
停用和激活 vCenter Single Sign-On 用户	125
删除 vCenter Single Sign-On 用户	126
编辑 vCenter Single Sign-On 用户	127
添加 vCenter Single Sign-On 组	127
向 vCenter Single Sign-On 组添加成员	128
从 vCenter Single Sign-On 组中移除成员	129
更改 vCenter Single Sign-On 密码	129
了解其他 vSphere 身份验证选项	130
智能卡身份验证登录	131
配置和使用智能卡身份验证	132
配置反向代理以请求客户端证书	132
使用命令行管理智能卡身份验证	133
使用 vSphere Client 管理智能卡身份验证	136
设置智能卡身份验证的吊销策略	137
设置 RSA SecurID 身份验证	139
管理 vSphere Client 登录页面的登录消息	141
管理 vSphere Client 登录页面的登录消息	141
vCenter Single Sign-On 安全性最佳做法	141

5	对 vCenter Server 身份验证进行故障排除	143
	确定 Lookup Service 错误的原因	143
	无法使用 Active Directory 域身份验证进行登录	144
	由于用户帐户被锁定，vCenter Server 登录失败	146
	VMware Directory Service 复制需要较长时间	146
	导出 vCenter Server 支持包	147
	vCenter Server 身份验证服务日志参考	147

关于《vSphere 身份验证》

《vSphere 身份验证》文档提供的信息可帮助您执行诸如证书管理和 vCenter Single Sign-On 配置等常见任务。

VMware 非常重视包容性。为了在客户、合作伙伴和内部社区中促进这一原则，我们采用包容性语言创建内容。

《vSphere 身份验证》介绍了如何管理 vCenter Server 和相关服务的证书，以及如何使用 vCenter Single Sign-On 设置身份验证。

表 1-1. 《vSphere 身份验证》内容要点

主题	内容要点
身份验证入门	<ul style="list-style-type: none">■ 管理身份验证服务。■ 使用 vCenter Server 管理界面管理 vCenter Server。
vSphere 安全证书	<ul style="list-style-type: none">■ 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。
使用 vCenter Single Sign-On 进行 vSphere 身份验证	<ul style="list-style-type: none">■ 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。■ vCenter Server 身份提供程序联合

Platform Services Controller 发生了什么情况

从 vSphere 7.0 开始，部署新的 vCenter Server 或升级到 vCenter Server 7.0 需要使用 vCenter Server Appliance，它是针对运行 vCenter Server 而优化的预配置虚拟机。新的 vCenter Server 包含所有 Platform Services Controller 服务，同时保留功能和工作流，包括身份验证、证书管理、标记和许可。不再需要也无法部署和使用外部 Platform Services Controller。所有 Platform Services Controller 服务都已整合到 vCenter Server 中，并且简化了部署和管理。

由于这些服务现在是 vCenter Server 的一部分，因此不再将其描述为 Platform Services Controller 的一部分。在 vSphere 7.0 中，《vSphere 身份验证》出版物替换了《Platform Services Controller 管理》出版物。新出版物包含有关身份验证和证书管理的完整信息。有关从使用现有外部 Platform Services Controller 的 vSphere 6.5 和 6.7 部署迁移到使用 vCenter Server Appliance 的 vSphere 7.0 的信息，请参见《vSphere 升级》文档。

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：<https://core.vmware.com/security>。《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

本信息面向需要配置 vCenter Server 身份验证以及管理证书的管理员。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 Linux 系统管理员。

vSphere 证书管理和身份验证入门

1

vSphere 提供了通用基础架构服务来管理 vCenter Server 和 ESXi 组件的证书，以及管理向 vCenter Single Sign-On 的身份验证。

如何管理 vSphere 证书

默认情况下，vSphere 支持使用 VMware Certificate Authority (VMCA) 证书置备 vCenter Server 组件和 ESXi 主机。也可以使用自定义证书，这些证书存储在 VMware 端点证书存储 (VECS) 中。有关详细信息，请参见[可通过哪些选项管理 vSphere 证书](#)。

什么是 vCenter Single Sign-On

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 使用一些必须了解的特定术语和定义。

表 1-1. vCenter Single Sign-On 术语表

术语	定义
主体	可以对其进行身份验证的实体，例如用户。
身份提供程序	管理标识源和对主体进行身份验证的服务。示例：Microsoft Active Directory 联合身份验证服务 (AD FS) 和 vCenter Single Sign-On。
标识源（目录服务）	存储和管理主体。主体包含有关用户或服务帐户的属性集合，例如名称、地址、电子邮件地址和组成员资格。示例：Microsoft Active Directory 和 VMware Directory Service (vmdir)。
身份验证	确定某人或某物实际上是否是其自身声明为的人或物的方法。例如，用户在提供凭据（如智能卡、用户名和正确密码等）时对其进行身份验证。
授权	验证主体有权访问哪些对象的过程。
令牌	包含给定主体标识信息的签名数据集合。令牌可能不仅包括有关主体的基本信息（如电子邮件地址和全名），还包括主体的组和角色，具体取决于令牌类型。

表 1-1. vCenter Single Sign-On 术语表（续）

术语	定义
vmdir	VMware Directory Service。vCenter Server 中的内部（本地）LDAP 存储库，包含用户身份、组和配置数据。
OpenID Connect (OIDC)	基于 OAuth2 的身份验证协议。在与 Active Directory 联合身份验证服务 (AD FS) 交互时，vCenter Server 使用 OIDC 功能。

有哪些 vCenter Single Sign-On 身份验证类型

vCenter Single Sign-On 使用不同类型的身份验证，具体取决于是否涉及内置 vCenter Server 身份提供程序还是外部身份提供程序。

表 1-2. vCenter Single Sign-On 身份验证类型

身份验证类型	作为身份提供程序的服务	vCenter Server 是否处理密码？	描述
基于令牌的身份验证	外部身份提供程序。例如，AD FS。	否	vCenter Server 通过特定协议访问外部身份提供程序，并获取表示特定用户身份的令牌。
简单身份验证	vCenter Server	是	用户名和密码直接传递到 vCenter Server，以便通过其标识源验证凭据。

本章讨论了以下主题：

- [管理 vCenter Server 证书](#)
- [管理 vCenter Server 身份验证服务](#)
- [管理 vCenter Server](#)

管理 vCenter Server 证书

可以从 vSphere Client 管理 vCenter Server 证书，也可以使用 API、脚本或 CLI 管理这些证书。

下表介绍了可用于管理 vCenter Server 证书的界面。

表 1-3. 用于管理 vSphere 证书的界面

接口	描述
vSphere Client	Web 界面（基于 HTML5 的客户端）。请参见 使用 vSphere Client 管理证书 。
vSphere Automation API	请参见《VMware vSphere Automation SDK 编程指南》，网址为： https://developer.vmware.com/docs/11699/vmware-vsphere-automation-sdks-programming-guide 。

表 1-3. 用于管理 vSphere 证书的界面（续）

接口	描述
证书管理实用程序	支持证书签名请求 (CSR) 生成和证书替换的命令行工具。请参见使用 vSphere Certificate Manager 实用程序管理证书。
用于管理证书和目录服务的 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 3 章 vSphere 证书和服务 CLI 命令参考 。

使用 vSphere Client 管理 vCenter Server 证书

您可以从 vSphere Client 管理 vCenter Server 证书。

步骤

- 1 在本地 vCenter Single Sign-On 域中，以拥有管理员特权的用户身份登录到 vCenter Server。
默认域为 vsphere.local。
- 2 选择**管理**。
- 3 在**证书**下，单击**证书管理**。
将显示不同类型证书的证书面板。
- 4 执行证书任务，例如查看证书详细信息、续订计算机 SSL 证书和添加可信根证书。
有关详细信息，请参见使用 [vSphere Client](#) 管理证书。

使用 CLI 管理 vCenter Server 证书

vCenter Server 包括用于生成证书签名请求 (CSR)、管理证书和管理服务的 CLI。

例如，您可以使用 certool 命令生成 CSR 并替换证书。

使用 CLI 执行 vSphere Client 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 vCenter Server 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。VMware Certificate Authority (VMCA) 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 VMware Authentication Framework 守护进程 (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	更新安全令牌服务 (STS) 证书。	使用命令行替换 vCenter Server STS 证书
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。

前提条件

启用 SSH，以通过 SSH 登录到 vCenter Server。您可以使用 vCenter Server 管理界面中的[访问设置](#)选项卡 (https://vcenter_server_ip:5480) 激活和停用 SSH 登录。

步骤

1 登录 vCenter Server shell。

通常情况下，您必须是 root 或管理员用户。有关详细信息，请参见《[运行 vSphere 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。有时，为了保护敏感信息，系统会提示您输入两次密码。

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certtool
/opt/vmware/bin/sso-config.sh
```

service-control 命令不要求输入路径。

有关详细信息，请参见[手动替换 vSphere 证书](#)。

管理 vCenter Server 身份验证服务

可以通过 vSphere Client 或使用 CLI 管理身份验证服务。还可以使用 API 管理 vCenter Server 身份提供程序联合配置过程。

可以使用不同的界面管理 vCenter Server 身份验证。

表 1-5. 用于管理 vCenter Server 身份验证服务的界面

接口	描述
vSphere Client	Web 界面（基于 HTML5 的客户端）。
API	管理 vCenter Server 身份提供程序联合配置过程。
sso-config	用于配置 vCenter Server 内置身份提供程序的命令行实用程序。

使用 vSphere Client 管理 vCenter Server 身份验证服务

可以从 vSphere Client 管理 vCenter Server 身份验证服务。

步骤

1 在本地 vCenter Single Sign-On 域中，以拥有管理员特权的用户身份登录到 vCenter Server。

默认域为 vsphere.local。

2 选择管理。

- 3 在 **Single Sign On** 下，单击**配置**以管理身份提供程序并配置密码和锁定策略。

有关详细信息，请参见第 4 章 [使用 vCenter Single Sign-On 进行 vSphere 身份验证](#)。

使用脚本管理 vCenter Server 身份验证服务

vCenter Server 包含一个用于管理身份验证服务的实用程序 `sso-config`。

可以使用 `sso-config` 实用程序执行 vSphere Client 不支持的管理任务，或者为环境创建自定义脚本。

表 1-6. 用于管理身份验证和关联服务的 CLI

CLI	描述	链接
<code>sso-config</code>	用于配置 vCenter Server 内置身份提供程序的命令行实用程序。	要参考 <code>sso-config</code> 帮助，请运行 <code>sso-config.sh -help</code> ，或者参见 VMware 知识库文章（网址为 https://kb.vmware.com/s/article/67304 ），获得用法示例。
<code>service-control</code>	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。 <code>service-control</code> 命令不要求您指定路径。

前提条件

启用 SSH，以通过 SSH 登录到 vCenter Server。您可以使用 vCenter Server 管理界面中的**访问设置**选项卡 (https://vcenter_server_ip:5480) 激活和停用 SSH 登录。

步骤

- 1 登录 vCenter Server shell。

通常情况下，您必须是 `root` 或管理员用户。有关详细信息，请参见《[运行 vSphere CLI 所需的特权](#)》。

- 2 在以下默认位置访问 `sso-config` 实用程序。

```
/opt/vmware/bin/sso-config.sh
```

所需特权取决于要执行的任务。有时，为了保护敏感信息，系统会提示您输入两次密码。

管理 vCenter Server

您可以从 vCenter Server 管理界面或 vCenter Server shell 管理 vCenter Server。

有关管理 vCenter Server 的详细信息，请参见《[vCenter Server 配置](#)》。

表 1-7. 用于管理 vCenter Server 的界面

接口	描述
vCenter Server 管理界面	使用此界面重新配置系统设置。请参见 使用管理界面管理 vCenter Server 。
vCenter Server 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 Certificate Manager 实用程序管理证书 和 第 3 章 vSphere 证书和服务 CLI 命令参考 。

使用管理界面管理 vCenter Server

您可以使用 vCenter Server 管理界面来配置系统设置。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。

步骤

- 1 在浏览器中，转至 Web 界面，网址为 `https://vcenter_server_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浏览器解决此问题。
- 3 以 root 用户身份登录。

默认 root 密码是您在部署 vCenter Server 时设置的 root 密码。

结果

您将看到 vCenter Server 管理界面的摘要页面。

使用 vCenter Server Shell 管理 vCenter Server

可以从 vCenter Server 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 vCenter Server 管理界面，网址为 `https://vcenter_server_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 vCenter Server 的 Bash Shell。
- 2 访问 Shell。
 - 如果可以直接访问 vCenter Server 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 vCenter Server 的会话。
- 3 以 root 用户身份及最初部署 vCenter Server 时设置的密码登录。

如果已更改 root 密码，请使用新密码。

将 vCenter Server 添加到 Active Directory 域

如果要将 Active Directory 标识源添加到 vCenter Server，必须将 vCenter Server 加入 Active Directory 域。

如果无法使用 vCenter Server 身份提供程序联合或基于 LDAPS 的 Active Directory，则 vCenter Server 支持集成 Windows 身份验证 (IWA)。要使用 IWA，必须将 vCenter Server 加入 Active Directory 域。

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使用 vSphere Client 登录到 vCenter Server。
- 2 选择**管理**。
- 3 展开**单点登录**，然后单击**配置**。
- 4 在**身份提供程序**选项卡下，单击 **Active Directory 域**。
- 5 单击**加入 AD**，输入域、可选的组织单位以及用户名和密码，然后单击**加入**。
- 6 重新启动 vCenter Server。

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](#)。

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 如何使用证书

vSphere 使用证书：

- 对两个节点（例如 vCenter Server 和 ESXi 主机）之间的通信进行加密。
- 对 vSphere 服务进行身份验证。
- 执行内部操作，如对令牌进行签名。

什么是 VMware Certificate Authority

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 vCenter Server 主机上均安装了 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。

可通过哪些选项管理 vSphere 证书

建议使用以下选项管理证书。

表 2-1. 管理 vSphere 证书的建议选项

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 vCenter Server 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](http://vmware.com/go/hybridvmca) 的博客帖子，网址为 <http://vmware.com/go/hybridvmca>。

哪些工具可用于替换 vSphere 证书

可以使用以下选项替换现有证书。

表 2-2. 替换 vSphere 证书的不同方法

选项	请参见
使用 vSphere Client。	使用 vSphere Client 管理证书
使用 vSphere Automation API 管理证书的生命周期。	《VMware vSphere Automation SDKs 编程指南》，网址 https://developer.vmware.com/docs/11699/vmware-vsphere-automation-sdks-programming-guide
从命令行使用 vSphere Certificate Manager 实用程序。	使用 vSphere Certificate Manager 实用程序管理证书
使用 CLI 命令执行手动证书替换。	第 3 章 vSphere 证书和服务 CLI 命令参考

本章讨论了以下主题：

- [不同解决方案途径的 vSphere 证书要求](#)
- [vSphere 证书管理概览](#)
- [使用 vSphere Client 管理证书](#)
- [使用 vSphere Certificate Manager 实用程序管理证书](#)
- [手动替换 vSphere 证书](#)

不同解决方案途径的 vSphere 证书要求

证书要求取决于是使用 VMware Certificate Authority (VMCA) 作为中间证书颁发机构，还是使用自定义证书。对于计算机证书，要求也有所不同。

在开始更改证书之前，请确保 vSphere 环境中所有节点的时间都已同步。

注 vSphere 仅部署用于服务器身份验证的 RSA 证书，不支持生成 ECDSA 证书。vSphere 验证其他服务器提供的 ECDSA 证书。例如，如果 vSphere 连接到 syslog 服务器，并且 syslog 服务器具有 ECDSA 证书，则 vSphere 支持验证该证书。

所有导入的 vSphere 证书的要求

- 密钥大小：2048 位（最小值）到 16384 位（最大值）（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。
- 除了 vpxd-extension 解决方案用户证书，扩展密钥用法可以为空或包含服务器身份验证。

vSphere 不支持以下证书。

- 使用通配符的证书。
- 不支持算法 md2WithRSAEncryption、md5WithRSAEncryption、RSASSA-PSS、dsaWithSHA1、ecdsa_with_SHA1 和 sha1WithRSAEncryption。

vSphere 证书符合 RFC 2253 规范

证书必须符合 RFC 2253 规范。

如果不使用 vSphere 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 vSphere Certificate Manager 生成 CSR，系统会提示您输入以下信息，然后 vSphere 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。
- vSphere Certificate Manager 存储在 certtool.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。
- 在其上运行 vSphere Certificate Manager 的 vCenter Server 节点的 IP 地址。

使用 VMCA 作为中间证书颁发结构时的证书要求

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	<ul style="list-style-type: none"> ■ 可以使用 vSphere Certificate Manager 创建 CSR。请参见使用 Certificate Manager 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： <ul style="list-style-type: none"> ■ 密钥大小：2048 位（最小值）到 16384 位（最大值）（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，并且证书签名必须在要求列表中。例如： <pre>basicConstraints = critical,CA:true keyUsage = critical,digitalSignature,keyCertSign</pre> ■ 必须启用 CRL 签名。 ■ 扩展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。 <p>有关使用 Microsoft 证书颁发机构的示例，请参见 VMware 知识库文章《在 vSphere 6.x 中创建 Microsoft 证书颁发机构模板以创建 SSL 证书》，网址为 http://kb.vmware.com/kb/2112009。</p>
计算机 SSL 证书	<p>可以使用 vSphere Certificate Manager 创建 CSR，或者手动创建 CSR。</p> <p>如果手动创建 CSR，该 CSR 必须满足前面“所有导入的 vSphere 证书的要求”中列出的要求。您还必须为主机指定 FQDN。</p>
解决方案用户证书	<p>可以使用 vSphere Certificate Manager 创建 CSR，或者手动创建 CSR。</p> <p>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。</p> <p>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 certtool.cfg 中。</p> <p>对于 vpxd-extension 解决方案用户，可以将“扩展密钥用法”留空或使用“TLS WWW 客户端身份验证”。</p>

使用自定义证书时的要求

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	<p>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。</p> <ul style="list-style-type: none"> ■ 可以使用 vSphere Client 或 vSphere Certificate Manager 生成 CSR，也可以手动创建 CSR。CSR 必须满足前面“所有导入的 vSphere 证书的要求”中列出的要求。 ■ 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	<p>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。</p> <ul style="list-style-type: none"> ■ 您可以使用 vSphere Certificate Manager 生成 CSR，或自己准备 CSR。CSR 必须满足前面“所有导入的 vSphere 证书的要求”中列出的要求。 ■ 如果使用 vSphere Certificate Manager，该实用程序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 certtool.cfg 中。 <p>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。</p> <p>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。</p> <p>对于 vpxd-extension 解决方案用户，可以将“扩展密钥用法”留空或使用“TLS WWW 客户端身份验证”。</p>

vSphere 证书管理概览

设置或更新 vSphere 证书基础架构所需的工作取决于您环境的要求。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。VMware Certificate Authority (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 6.0 或更高版本，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 VMware 端点证书存储 (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 VMCA（默认设置），则从 vSphere Client 执行证书刷新时，VMCA 签名证书将替换自定义证书。

- 如果将简单 vCenter Server 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。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。VMware 不建议替换解决方案用户证书。

vSphere 证书接口

对于 vCenter Server，可以使用以下工具和界面查看和替换证书。

表 2-3. 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 Automation API	请参见《VMware vSphere Automation SDK 编程指南》。
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。
vSphere 证书管理 CLI	使用 <code>dir-cli</code> 、 <code>certtool</code> 和 <code>vecs-cli</code> 执行所有证书管理任务。
sso-config 实用程序	从 vCenter Server 安装的命令行执行 STS 证书管理。
PowerCLI 12.4（需要使用 vSphere 7.0 或更高版本）	执行可信证书存储管理，管理 vCenter Server 计算机 SSL 证书以及管理 ESXi 计算机 SSL 证书。

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 以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。

替换 vSphere 证书

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 Certificate Manager 实用程序从 vSphere Client 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。

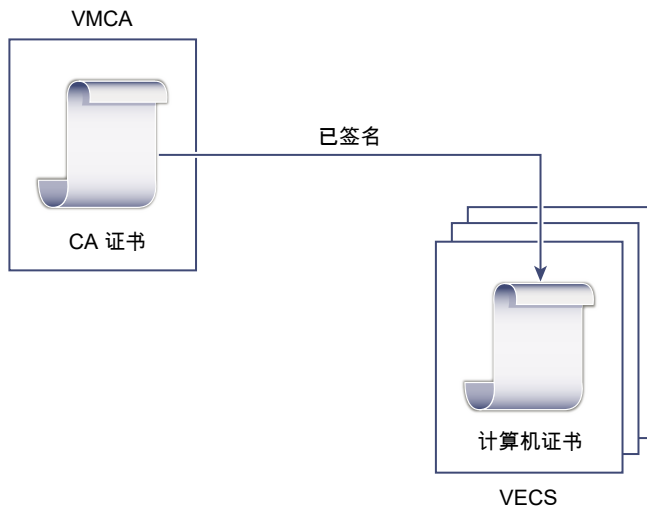
VMware Certificate Authority (VMCA) 包含在每个 vCenter Server 部署中。VMCA 使用由 VMCA 作为证书颁发机构签名的证书置备每个节点、每个 vCenter Server 解决方案用户和每个 ESXi 主机。

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。

将证书替换为 VMCA 签名证书

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 2-1. 由 VMCA 签名的证书存储在 VECS 中



您可以使用以下 vSphere Certificate Manager 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

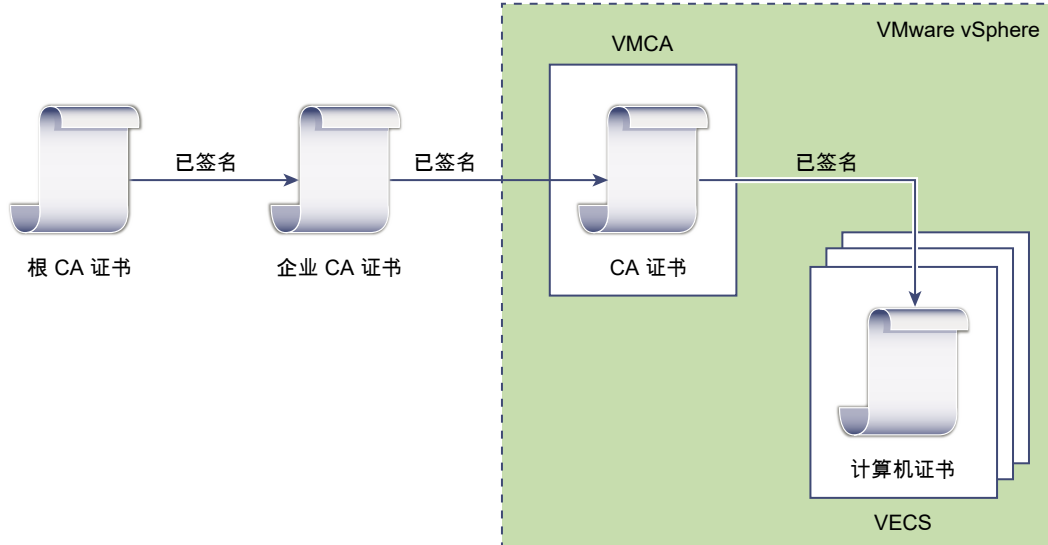
有关手动证书替换，请参见使用 [CLI](#) 将现有 [VMCA](#) 签名证书替换为新的 [VMCA](#) 签名证书。

使 VMCA 成为中间证书颁发机构

可以将 VMCA 根证书替换为企业证书颁发机构 (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 vCenter Server 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 2-2. 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 Certificate Manager 选项：

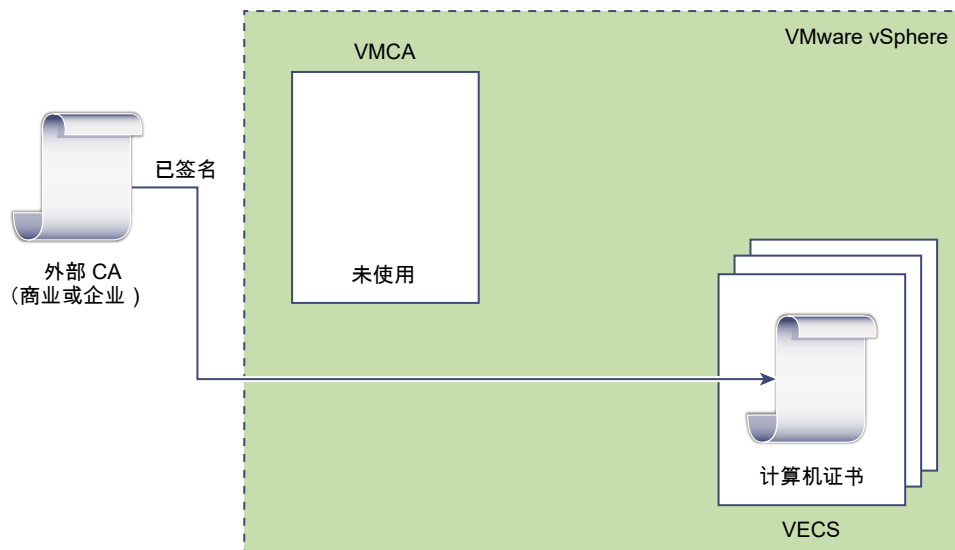
- 将 VMCA 根证书替换为自定义签名证书并替换所有证书
- 将计算机 SSL 证书替换为 VMCA 证书（多节点增强型链接模式部署）
- 将解决方案用户证书替换为 VMCA 证书（多节点增强型链接模式部署）

有关手动证书替换，请参见使用 [CLI](#) 将 VMCA 设为中间证书颁发机构。

将 VMCA 签名证书替换为自定义证书

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 2-3. 外部证书直接存储在 VECS 中



您可以使用以下 vSphere Certificate Manager 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，请参见使用 [CLI 将证书替换为自定义证书](#)。

您还可以使用 vSphere Client 为计算机 SSL 证书生成 CSR（自定义），并在 CA 返回 CSR 后替换证书。请参见使用 [vSphere Client 为计算机 SSL 证书生成证书签名请求（自定义证书）](#)。

使用混合方法部署证书

在混合方法中，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 2-4. 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 使用证书的情况

VMware Certificate Authority (VMCA) 会为您的环境置备证书。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 2-5. vSphere 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 VMware 端点证书存储 (VECS) 中。
解决方案用户证书	VMCA（默认）	存储在 VECS 中。

表 2-5. vSphere 中的证书（续）

证书	已置备	备注
vCenter Single Sign-On SSL 签名证书	在安装期间置备。	从命令行管理此证书。 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。	在 vSphere 6.5 及更高版本中，计算机 SSL 证书将被用作 vmdir 证书。
SMS 自签名证书	已在注册 IOFilter Provider 期间置备。	在 vSphere 7.0 及更高版本中，SMS 自签名证书存储在 /etc/vmware/ssl/iofiltervp_castore.pem 中。在 vSphere 7.0 之前，SMS 自签名证书存储在 /etc/vmware/ssl/castore.pem 中。此外，当 retainVasaProviderCertificate=True 时，SMS Store 还可以存储 VVOL VASA Provider（版本 4.0 及更低版本）的自签名证书。

ESXi 证书

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。有关详细信息，请参见《vSphere 安全性》文档。

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 vCenter Server 节点都有自己的计算机 SSL 证书。vCenter Server 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。

- 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。
- vCenter Server 服务 (vpxd)。
- 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 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。

VECS 中包含以下解决方案用户证书存储：

- **machine**：由 License Server 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 服务守护进程 (vpxd) 存储。vpxd 使用存储在此存储中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 Client 存储。还包括其他一些服务，例如性能图表服务。
- **wcp**：VMware vSphere® 和 VMware Tanzu™ 存储。

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。

可以从 CLI 替换此证书。请参见[使用命令行替换 vCenter Server STS 证书](#)。

VMware Directory Service SSL 证书

在 vSphere 6.5 及更高版本中，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密钥服务器连接。根据该解决方案对密钥服务器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。

VMware Certificate Authority 和 VMware 核心标识服务

核心标识服务是每个 vCenter Server 系统的一部分。VMware 证书颁发机构 (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 2-6. 核心标识服务

服务	描述
VMware Directory Service (vmdir)	处理 SAML 证书管理以进行 vCenter Single Sign-On 身份验证的标识源。
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。
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。

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 vCenter Server 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 2-7. VECS 中的库

库	描述
计算机 SSL 库 (MACHINE_SSL_CERT)	<ul style="list-style-type: none"> ■ 由每个 vSphere 节点上的反向代理服务使用。 ■ 由 VMware Directory Service (vmdir) 在每个 vCenter Server 节点上使用。 <p>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。</p>
解决方案用户库 <ul style="list-style-type: none"> ■ machine ■ vpxd ■ vpxd-extension ■ vsphere-webclient ■ wcp 	<p>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。</p> <p>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。</p> <p>VECS 中包含以下解决方案用户证书存储：</p> <ul style="list-style-type: none"> ■ machine：由 License Server 和日志记录服务使用。 <p>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。</p> <ul style="list-style-type: none"> ■ vpxd：vCenter 服务守护进程 (vpxd) 存储。vpxd 使用存储在此存储中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 Client 存储。还包括其他一些服务，例如性能图表服务。 ■ wcp：VMware vSphere® 和 VMware Tanzu™ 存储。 <p>每个 vCenter Server 节点包含一个 machine 证书。</p>
受信任的根存储 (TRUSTED_ROOTS)	包含所有受信任的根证书。
vSphere Certificate Manager 实用程序备份库 (BACKUP_STORE)	由 VMCA (VMware Certificate Manager) 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	<p>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。</p> <p>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。</p>

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 CLI 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。

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 vSphere 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 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。

替换大型部署中的 vSphere 证书

在具有大量 vCenter Server 主机的部署中替换证书时，可以使用 vSphere Certificate Manager 实用程序进行替换，也可以使用 CLI 手动替换证书。一些最佳做法可指导您选择的过程。

在具有多个 vCenter Server 节点的环境中替换计算机 SSL 证书

如果您的环境包含多个 vCenter Server 节点，则可以使用 vSphere Client 或 vSphere Certificate Manager 实用程序替换计算机 SSL 证书，也可以使用 CLI 命令手动替换证书。

vSphere Certificate Manager

在每台计算机上运行 vSphere Certificate Manager。根据您所执行的任务，也可能提示您输入证书信息。有关详细信息，请参见以下主题：

- 使用 [Certificate Manager](#) 将 VMCA 根证书替换为自定义签名证书并替换所有证书
- 使用 [Certificate Manager](#) 将计算机 SSL 证书替换为 VMCA 证书（中间 CA）
- 使用 [Certificate Manager](#) 将解决方案用户证书替换为 VMCA 证书（中间 CA）

手动证书替换

要手动替换证书，请在每台计算机上运行证书替换 CLI 命令。有关详细信息，请参见以下主题：

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

在具有多个处于增强型链接模式的 vCenter Server 系统的环境中替换解决方案用户证书

如果您的环境包含多个处于增强型链接模式的 vCenter Server 系统，请按照以下步骤替换解决方案用户证书。

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。根据您所执行的任务，也可能提示您输入证书信息。请参见[使用 vSphere Certificate Manager 实用程序管理证书](#)。

手动证书替换

- 1 生成或请求证书。需要以下证书：
 - 每个 vCenter Server 上计算机解决方案用户的证书。
 - 每个节点上以下每个解决方案用户的证书：
 - vpxd 解决方案用户
 - vpxd-extension 解决方案用户
 - vsphere-webclient 解决方案用户
 - wcp 解决方案用户
- 2 使用 CLI 命令替换每个节点上的证书。确切过程取决于您将执行的证书替换类型。
有关详细信息，请参见以下主题：
 - [使用 CLI 将解决方案用户证书替换为新的 VMCA 签名证书](#)
 - [使用 CLI 替换解决方案用户证书（中间 CA）](#)
 - [使用 Certificate Manager 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

某些解决方案（如 VMware vCenter Site Recovery Manager 或 VMware vSphere Replication）始终安装在不同于 vCenter Server 系统的计算机上。如果替换 vCenter Server 系统上的默认计算机 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。

使用 vSphere Client 可执行以下管理任务。

- 查看计算机 SSL 证书、VMware Certificate Authority (VMCA) 根证书、受信任根证书和 Security Token Service (STS) 证书。
- 添加新的受信任根证书，并续订或替换现有的计算机 SSL 和 STS 证书。
- 为计算机 SSL 证书生成自定义证书签名请求 (CSR) 并在证书颁发机构返回 CSR 时替换证书。

大多数证书替换工作流在 vSphere Client 中完全受支持。其他证书替换工作流受 vSphere Certificate Manager 实用程序支持。请参见[使用 vSphere Certificate Manager 实用程序管理证书](#)。

要了解有关用于替换默认证书的选项的详细信息，请参见[替换 vSphere 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，并且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](http://vmware.com/go/hybridvmca) 的博客帖子，网址为 <http://vmware.com/go/hybridvmca>。

使用 vSphere Client 浏览证书存储

每个 vCenter Server 节点上都包括一个 VMware 端点证书存储 (VECS) 实例。可以从 vSphere Client 浏览 VMware 端点证书存储中的不同存储，包括计算机 SSL 证书和可信根证书。

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 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 如果系统出现提示，请输入 vCenter Server 的凭据。
- 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。

使用 vSphere Client 为 vCenter 证书过期警告设置阈值

vCenter Server 可监控 VMware 端点证书存储 (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。您可以使用 vSphere Client 通过 `vpxd.cert.threshold` 高级选项更改项您发出警告的时间。

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**。

通过 vSphere Client 使用新的 VMCA 签名证书续订 VMCA 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 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 如果系统出现提示，请输入 vCenter Server 的凭据。
- 5 续订本地系统的 VMCA 签名计算机 SSL 证书。
 - a 从**计算机 SSL 证书**图标中，单击**操作 > 续订**。
 - b 指定证书的持续时间（以天为单位）。
 - c 单击**续订**。

vCenter Server 服务将自动重新启动。您必须重新登录，因为重新启动服务会结束 UI 会话。

使用 vSphere Client 将证书替换为自定义证书

您可以使用 vSphere Client 将默认证书替换为自定义证书。

您可以使用 vSphere Client 为每台计算机生成 CSR，并在收到来自内部或第三方证书颁发机构 (CA) 的证书时替换这些证书。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。您可以从 vSphere Client 同时上载根证书和已签名证书。

使用 vSphere Client 为计算机 SSL 证书生成证书签名请求（自定义证书）

计算机 SSL 证书由每个 vCenter Server 节点上的反向代理服务使用。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。可以使用 vSphere Client 为计算机 SSL 证书生成证书签名请求 (CSR)，并在准备就绪后替换该证书。

前提条件

证书必须满足以下要求：

- 密钥大小：2048 位（最小值）到 16384 位（最大值）（PEM 编码）
- CRT 格式
- x509 版本 3
- SubjectAltName 必须包含 DNS Name=<machine_FQDN>。
- 包含以下密钥用法：数字签名、密钥加密。

步骤

- 1 使用 vSphere Client 登录 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 生成 CSR。
 - a 在计算机 SSL 证书图标下，单击操作 > 生成证书签名请求 (CSR)。
 - b 输入证书信息，然后单击下一步。

从 vSphere 8.0 开始，3072 位是密钥大小的默认值。使用 vSphere Client 生成 CSR 时，不再支持 2048 位。vCenter Server 仍接受密钥长度为 2048 位的自定义证书。但是，从 vSphere 8.0 开始，只能使用 vSphere Client 生成最小密钥长度为 3072 位的 CSR。

注 使用 vCenter Server 生成密钥大小为 16384 位的 CSR 时，生成需要几分钟才能完成，因为该操作具有 CPU 密集型特性。

- c 复制或下载 CSR。
- d 单击完成。
- e 向证书颁发机构提供 CSR。

后续步骤

当证书颁发机构返回证书时，替换证书存储中的现有证书。请参见使用 [vSphere Client](#) 添加自定义证书。

使用 vSphere Client 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。可以使用 vSphere Client 完成此操作。

前提条件

从第三方或内部证书颁发机构 (CA) 获取自定义根证书。

vSphere 仅接受有效的 CA 证书进行导入。为确保 CA 证书有效，CA 证书必须分别在基本限制和密钥用法 X.509 v3 证书扩展中设置 CA 位和 keyCertSign 位。这意味着该证书是 CA 证书，其用途是证书签名。有关详细信息，请参见 <https://www.rfc-editor.org/rfc/rfc5280>。

步骤

- 1 使用 vSphere Client 登录 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 如果系统出现提示，请输入 vCenter Server 的凭据。
- 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。

使用 vSphere Client 添加自定义证书

可以使用 vSphere Client 将自定义计算机 SSL 证书添加到证书存储。

通常，替换每个组件的计算机 SSL 证书就已满足要求。

前提条件

为要替换的每个证书生成证书签名请求 (CSR)。请参见使用 [vSphere Client](#) 为计算机 SSL 证书生成证书签名请求（自定义证书）。在 vCenter Server 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 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 如果系统出现提示，请输入 vCenter Server 的凭据。
- 5 在**计算机 SSL 证书**图标下，单击**操作 > 导入并替换证书**。
- 6 单击适当的证书替换选项，然后单击**下一步**。

选项	描述
替换为 VMCA	创建 VMCA 生成的 CSR 以替换当前证书。
替换为从 vCenter Server 生成的证书	使用通过 vCenter Server 生成的 CSR 签名的证书替换当前证书。
替换为外部 CA 证书 (需要私钥)	使用外部 CA 签名的证书替换当前证书。

- 7 输入 CSR 信息，或上载相应的证书。
- 8 单击**替换**。

vCenter Server 服务将自动重新启动。

使用 vSphere Certificate Manager 实用程序管理证书

vSphere Certificate Manager 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 Certificate Manager 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。

要了解有关用于替换默认证书的选项的详细信息，请参见**替换 vSphere 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，并且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>。

如果使用 vSphere Certificate Manager，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。

按顺序运行 vSphere Certificate Manager 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。在运行 vSphere Certificate Manager 之前，请确保熟悉替换过程并获取您要使用的证书。

小心 vSphere Certificate Manager 支持一个恢复级别。如果运行两次 vSphere Certificate Manager 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。

vSphere Certificate Manager 实用程序位置

vSphere Certificate Manager 实用程序位于：

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

注 运行 vSphere Certificate Manager 时，某些选项会显示以下提示：

```
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，以响应此提示。

vSphere Certificate Manager 实用程序中的工作流概述

下表概述了可以使用 vSphere Certificate Manager 实用程序完成的证书替换工作流。

表 2-8. vSphere 证书管理实用程序中的工作流

工作流	描述	请参见
将 VMCA 根证书替换为自定义签名证书并替换所有证书	要生成 VMCA 根证书并替换所有证书，请使用选项 4 “重新生成新的 VMCA 根证书并替换所有证书”。	使用 Certificate Manager 重新生成新的 VMCA 根证书并替换所有证书
使 VMCA 成为中间证书颁发机构	要使 VMCA 成为中间 CA，必须多次运行 vSphere Certificate Manager 实用程序并使用多个选项。此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。	使用 Certificate Manager 将 VMCA 设为中间证书颁发机构
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，必须多次运行 vSphere Certificate Manager 实用程序并使用多个选项。此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。	使用 Certificate Manager 将所有证书替换为自定义证书
恢复上次执行的操作	要恢复上次执行的证书操作并恢复到先前状态，请使用选项 7 “通过重新发布旧证书来恢复上次执行的操作”。	使用 Certificate Manager 重新发布旧证书以恢复上次执行的操作
正在重置所有证书	要将所有现有 vCenter 证书替换为 VMCA 签名的证书，请使用选项 8 “重置所有证书”。	使用 Certificate Manager 重置所有证书

使用 Certificate Manager 重新生成新的 VMCA 根证书并替换所有证书

可以使用 vSphere Certificate Manager 实用程序重新生成 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。当多个 vCenter Server 实例以增强型链接模式配置进行连接时，必须替换每个 vCenter Server 上的证书。

将现有计算机 SSL 证书替换为新的 VMCA 签名证书时，vSphere Certificate Manager 会提示您输入信息，并将除 vCenter Server 密码和 IP 地址以外的所有值输入到 `certtool.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。
- vCenter Server 的 IP 地址
- 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 Certificate Manager 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 登录到 vCenter Server Shell，然后启动 vSphere Certificate Manager。

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

- 2 选择选项 4，重新生成新的 VMCA 根证书并替换所有证书。
- 3 输入管理员用户和密码。

4 对提示做出响应。

vSphere Certificate Manager 根据您的输入生成新的 VMCA 根证书，并替换运行 vSphere Certificate Manager 的系统上的所有证书。vSphere Certificate Manager 重新启动服务后，替换过程即完成。

5 要替换计算机 SSL 证书，请使用选项 3 “将计算机 SSL 证书替换为 VMCA 证书” 运行 vSphere Certificate Manager。

6 要替换解决方案用户证书，请使用选项 6 “将解决方案用户证书替换为 VMCA 证书” 运行 Certificate Manager。

使用 Certificate Manager 将 VMCA 设为中间证书颁发机构

可以使用 vSphere Certificate Manager 实用程序将 VMCA 设置为中间 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 vSphere Certificate Manager 将所有现有证书替换为新的 VMCA 签名证书。

VMware 不建议将 VMCA 作为辅助（或中间）证书颁发机构。如果选择此选项，您可能会面临极度复杂的情况并且可能对安全产生负面影响，以及增加不必要的操作风险。有关管理 vSphere 环境内的证书的详细信息，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>。

要使 VMCA 成为中间 CA，必须多次运行 vSphere Certificate Manager。替换计算机 SSL 证书和解决方案用户证书的简要步骤包括：

- 1 启动 vSphere Certificate Manager 实用程序。
- 2 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” 以生成 CSR。接下来，您可能必须提供有关证书的一些信息。再次提示选择选项时，选择选项 1 “为 VMCA 根签名证书生成证书签名请求和密钥”。
- 3 将 CSR 提交给外部 CA 或企业 CA。您将从 CA 收到签名证书和根证书。
- 4 将 VMCA 根证书与 CA 根证书组合并保存文件。
- 5 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”，然后按照提示替换证书。此过程会替换本地计算机上的所有证书。
- 6 （可选）在增强型链接模式配置中连接多个 vCenter Server 实例时，按照以下步骤替换每个节点上的证书：
 - a 首先将计算机 SSL 证书替换为新的 VMCA 证书（选项 3 “将计算机 SSL 证书替换为 VMCA 证书”）。
 - b 然后将解决方案用户证书替换为新的 VMCA 证书（选项 6 “将解决方案用户证书替换为 VMCA 证书”）。

使用 Certificate Manager 生成 CSR，并准备根证书（中间 CA）

您可以使用 vSphere Certificate Manager 实用程序生成证书签名请求 (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 Certificate Manager 创建 CSR。

注 从 vSphere 8.0 开始，如果使用 vCenter Server 生成 CSR，则默认情况下密钥大小将从 2048 位更改为 3072 位。

- 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（最小值）到 16384 位（最大值）（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，并且证书签名必须在要求列表中。例如：

```
basicConstraints      = critical,CA:true
keyUsage              = critical,digitalSignature,keyCertSign
```

- 必须启用 CRL 签名。
- 扩展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。

有关使用 Microsoft 证书颁发机构的示例，请参见 VMware 知识库文章《在 vSphere 6.x 中创建 Microsoft 证书颁发机构模板以创建 SSL 证书》，网址为 <http://kb.vmware.com/kb/2112009>。

前提条件

vSphere Certificate Manager 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 登录到 vCenter Server Shell，然后启动 vSphere Certificate Manager。

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

- 2 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”。

首先，使用此选项生成 CSR，而不是替换证书。

- 3 输入管理员用户和密码。

- 4 选择选项 1 “为 VMCA 根签名证书生成证书签名请求和密钥”，以生成 CSR 并响应提示。

在此流程中，您还必须提供一个目录。vSphere Certificate Manager 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[使用 Certificate Manager 将 VMCA 根证书替换为自定义签名证书并替换所有证书](#)。

使用 Certificate Manager 将 VMCA 根证书替换为自定义签名证书并替换所有证书

可以使用 vSphere Certificate Manager 实用程序生成 CSR 并将其发送到企业或第三方 CA 进行签名。然后，可以将 VMCA 根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 vCenter Server 上运行 vSphere Certificate Manager 以将 VMCA 根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 Certificate Manager 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 根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 Certificate Manager 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
 - 有效的自定义根证书 (.crt 文件)
 - 根的有效自定义密钥 (.key 文件)

步骤

- 1 登录到 vCenter Server Shell，然后启动 vSphere Certificate Manager。

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

- 2 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”。
- 3 输入管理员用户和密码。
- 4 选择选项 2，导入自定义证书和密钥，替换现有 VMCA 根签名证书，然后对提示做出响应。

- a 出现提示后指定根证书的完整路径。
- 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 certtool.cfg 文件中。

使用 Certificate Manager 将计算机 SSL 证书替换为 VMCA 证书（中间 CA）

将 VMCA 用作中间 CA 时，可以使用 vSphere Certificate Manager 实用程序明确替换计算机 SSL 证书。首先替换 vCenter Server 上的 VMCA 根证书，然后可以替换将由 VMCA 的新根签名的计算机 SSL 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 Certificate Manager 会提示您输入信息，并将除 vCenter Server 密码和 IP 地址以外的所有值输入到 certtool.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。
- vCenter Server 的 IP 地址
- 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

- 您必须了解以下信息才能使用此选项运行 vSphere Certificate Manager。
 - 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。
- vCenter Server 系统的主机名或 IP 地址。

步骤

- 1 登录到 vCenter Server Shell，然后启动 vSphere Certificate Manager。

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

- 2 选择选项 3 “将计算机 SSL 证书替换为 VMCA 证书”。
- 3 输入管理员用户和密码。
- 4 对提示做出响应。

vSphere Certificate Manager 将信息存储在 certtool.cfg 文件中。

结果

vSphere Certificate Manager 替换计算机 SSL 证书。

使用 Certificate Manager 将解决方案用户证书替换为 VMCA 证书（中间 CA）

将 VMCA 用作中间 CA 时，可以使用 vSphere Certificate Manager 实用程序明确替换解决方案用户证书。首先替换 vCenter Server 上的 VMCA 根证书，然后可以替换将由 VMCA 的新根签名的解决方案用户证书。您也可以使用此选项替换已损坏或即将过期的解决方案证书。

前提条件

- 如果在增强型链接模式配置中包含多个 vCenter Server 实例的部署中替换了 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 vSphere Certificate Manager。
 - administrator@vsphere.local 的密码
 - vCenter Server 系统的主机名或 IP 地址

步骤

- 1 登录到 vCenter Server Shell，然后启动 vSphere Certificate Manager。

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

- 2 选择选项 6 “将解决方案用户证书替换为 VMCA 证书”。
- 3 输入管理员用户和密码。
- 4 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>。

结果

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

使用 Certificate Manager 将所有证书替换为自定义证书

可以使用 vSphere Certificate Manager 实用程序将所有证书替换为自定义证书。开始此过程之前，必须向您的证书颁发机构 (CA) 发送 CSR。您可以使用 Certificate Manager 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 Certificate Manager 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，必须多次运行 vSphere Certificate Manager 实用程序。替换计算机 SSL 证书和解决方案用户证书的简要步骤包括：

- 1 启动 vSphere Certificate Manager 实用程序。
- 2 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 “将计算机 SSL 证书替换为自定义证书”。再次提示输入选项时，请选择选项 1 “为计算机 SSL 证书生成证书签名请求和密钥”。
 - b 如果公司策略不允许混合部署，请选择选项 5 “将解决方案用户证书替换为自定义证书”。
- 3 将 CSR 提交给外部 CA 或企业 CA。您将从 CA 收到签名证书和根证书。
- 4 从 CA 收到签名证书和根证书后，使用选项 1 “将计算机 SSL 证书替换为自定义证书”，替换每个计算机上的计算机 SSL 证书。
- 5 如果还希望替换解决方案用户证书，请选择选项 5 “将解决方案用户证书替换为自定义证书”。
- 6 最后，当多个 vCenter Server 实例以增强型链接模式配置进行连接时，请在每个节点上重复该过程。

使用 Certificate Manager 生成证书签名请求（自定义证书）

您可以使用 vSphere Certificate Manager 实用程序生成证书签名请求 (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。

前提条件

vSphere Certificate Manager 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。
- 系统将提示您输入 vCenter Server 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 certtool.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。

注 从 vSphere 8.0 开始，如果使用 vCenter Server 生成 CSR，则默认情况下密钥大小将从 2048 位更改为 3072 位。

步骤

- 1 登录到环境中的每个 vCenter Server (vCenter Server Shell)，然后启动 vSphere Certificate Manager。

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

- 2 选择选项 1 “将计算机 SSL 证书替换为自定义证书”。
- 3 输入管理员用户和密码。
- 4 选择选项 1 “为计算机 SSL 证书生成证书签名请求和密钥”，以生成 CSR，响应提示并退出 vSphere Certificate Manager。

在此流程中，您还必须提供一个目录。vSphere Certificate Manager 将证书和密钥文件放在目录中。

- 5 如果还要替换所有解决方案用户证书，请重新启动 vSphere Certificate Manager 并选择选项 5 “将解决方案用户证书替换为自定义证书”。
- 6 按照提示提供密码和 vCenter Server 的 IP 地址或主机名。
- 7 选择选项 1 “为解决方案用户证书生成证书签名请求和密钥”，以生成 CSR，响应提示并退出 vSphere Certificate Manager。

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

后续步骤

要执行证书替换，请参见[使用 Certificate Manager 将计算机 SSL 证书替换为自定义证书](#)。

使用 Certificate Manager 将计算机 SSL 证书替换为自定义证书

您可以使用 vSphere Certificate Manager 实用程序将每个节点上的计算机 SSL 证书替换为自定义证书。计算机 SSL 证书由每个 vCenter Server 节点上的反向代理服务使用。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。

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 Certificate Manager 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（最小值）到 16384 位（最大值）（PEM 编码）
 - CRT 格式
 - x509 版本 3
 - SubjectAltName 必须包含 DNS Name=<machine_FQDN>。
 - 包含以下密钥用法：数字签名、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 登录到 vCenter Server，然后启动 vSphere Certificate Manager。

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

- 2 选择选项 1 “将计算机 SSL 证书替换为自定义证书”。
- 3 输入管理员用户和密码。
- 4 选择选项 2 “导入自定义证书和密钥以替换现有计算机 SSL 证书”，启动证书替换并对提示做出响应。

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）
- 自定义计算机 SSL 证书的有效签名证书（.crt 文件）
- vCenter Server 的 IP 地址

使用 Certificate Manager 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，vSphere Certificate Manager 实用程序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。

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。

格式看起来与下面类似。

```
-----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 [Certificate Manager 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（最小值）到 16384 位（最大值）（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。
 - 包含以下密钥用法：数字签名、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 登录到 vCenter Server，然后启动 vSphere Certificate Manager。

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

- 2 选择选项 5 “将解决方案用户证书替换为自定义证书”。
- 3 输入 SSO 用户和密码。
- 4 选择选项 2 “导入自定义证书和密钥以替换现有解决方案用户证书”，然后对提示做出响应。

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
- 计算机解决方案用户的证书和密钥（vpxd.crt 和 vpxd.key）
- 所有解决方案用户的全套证书和密钥（vpxd.crt 和 vpxd.key）

使用 Certificate Manager 重新发布旧证书以恢复上次执行的操作

通过使用 vSphere Certificate Manager 实用程序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 Certificate Manager，然后尝试恢复，则仅会恢复上一个操作。

步骤

- 1 登录到 vCenter Server Shell，然后启动 vSphere Certificate Manager。

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

- 2 选择选项 7 “通过重新发布旧证书恢复上次执行的操作”。

- 3 输入管理员用户和密码。
- 4 要继续，请输入 **y**。

使用 Certificate Manager 重置所有证书

可以使用 vSphere Certificate Manager 实用程序将所有现有 vCenter 证书替换为 VMCA 签名的证书。

使用此选项时，会覆盖当前在 VMware 端点证书存储 (VECS) 中的所有自定义证书。

vSphere Certificate Manager 可以替换所有证书。替换的证书取决于您选择的选项。

步骤

- 1 登录到 vCenter Server shell，然后启动 vSphere Certificate Manager。

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

- 2 选择选项 8 “重置所有证书”。
- 3 输入管理员用户和密码。
- 4 出现提示时，输入您的证书信息。

后续步骤

替换证书并重新启动服务后，请验证您的证书信息。

手动替换 vSphere 证书

对于某些特殊的证书替换情况，无法使用 vSphere Certificate Manager 实用程序。可以改用随安装一起提供的 CLI 进行证书替换。

vCenter Server 服务停止和启动指南

对于手动证书替换的某些部分，必须停止所有 vCenter Server 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。您可以使用 `service-control` 命令启动和停止服务。可以启动和停止所有服务或单个服务。有关详细信息，请参见命令行帮助。

请遵循以下准则。

- 请勿停止服务以生成新公用/专用密钥对新证书。
- 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。
- 在 VMware Endpoint Certificate Store (VECS) 中删除计算机 SSL 证书之前立即停止服务。

使用 CLI 将现有 VMCA 签名证书替换为新的 VMCA 签名证书

如果 VMware 证书颁发机构 (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，则可以使用 CLI 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 Certificate Manager 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](#)。

使用 CLI 生成新的 VMCA 签名根证书

可以使用 certool CLI 生成新的 VMCA 签名证书，并将证书发布到 vmdir。

步骤

- 1 在 vCenter Server 上，生成新的自签名证书和私钥。

```
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。

```
service-control --stop --all
service-control --start vmafd
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）在 vCenter Server 上，列出 VMCA 根证书以确保其位于证书存储中。

```
/usr/lib/vmware-vmca/bin/certool --getrootca
```

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 存储，并将证书序列号与步骤 1 中输出的序列号进行比较。

```
/usr/lib/vmware-vmca/bin/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 存储。

```
/usr/lib/vmware-vmca/bin/certool --selfca --config=/usr/lib/vmware-vmca/share/config/certool.cfg
```

使用 CLI 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，可以使用 `vecs-cli` 命令替换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。当多个 vCenter Server 实例以增强型链接模式配置进行连接时，必须在每个节点上运行计算机 SSL 证书生成命令。

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 certtool.cfg。

您可以在 /usr/lib/vmware-vmca/share/config/ 目录中找到 certtool.cfg 文件。

- 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：

```
certtool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certtool --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。

```
service-control --stop --all
service-control --start vmafd
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.crt
--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-<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。在包含以增强型链接模式配置连接的多个 vCenter Server 实例的部署中，在每个 vCenter Server 节点上运行以下命令。

```
/usr/lib/vmware-vmca/bin/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 根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。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv  
--config=ssl-config.cfg
```

将在当前目录中创建 new-vmca-ssl.crt 文件。

- 4 (可选) 列出 VECS 的内容。

```
/usr/lib/vmware-vmafd/bin/vecs-cli store list
```

■ vCenter Server 中的输出示例：

```
output (on vCenter):  
MACHINE_SSL_CERT  
TRUSTED_ROOTS  
TRUSTED_ROOT_CRLS  
machine  
vsphere-webclient  
vpxd  
vpxd-extension  
hvc  
data-encipherment  
APPLMGMT_PASSWORD  
SMS  
wcp  
KMS_ENCRYPTION
```

- 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。

- 在每个 vCenter Server 上，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。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias  
__MACHINE_CERT  
/usr/lib/vmware-vmafd/bin/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。

使用 CLI 将解决方案用户证书替换为新的 VMCA 签名证书

替换计算机 SSL 证书后，可以使用 `dir-cli` 命令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 vCenter Server 系统上的计算机解决方案用户证书和解决方案用户证书。

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 `certtool.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：

```
certtool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certtool --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。

```
dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

在包含以增强型链接模式配置连接的多个 vCenter Server 实例的部署中，`dir-cli service 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。

- 4 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 vmafd
service-control --start vmdird
service-control --start vmcad
```

- 5 对于每个解决方案用户，请先替换 `vmdird` 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 `vpzd` 服务的证书。

```
dir-cli service update --name <vpzd-xxxx-xxx-7c7b769cd9f4> --cert ./vpzd.crt
vecs-cli entry delete --store vpzd --alias vpzd
vecs-cli entry create --store vpzd --alias vpzd --cert vpzd.crt --key vpzd.priv
```

注 如果不替换 `vmdird` 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 在增强型链接模式配置中的每个 vCenter Server 节点上，为每个解决方案用户生成一个公钥/私钥对，其中包括为计算机解决方案用户生成一个密钥对以及为每个其他解决方案用户（`vpzd`、`vpzd-extension`、`vsphere-webclient`、`wcp`）生成一个密钥对。

- a 为计算机解决方案用户生成密钥对。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- b 为每个节点上的 `vpzd` 解决方案用户生成密钥对。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpzd-key.priv --pubkey=vpzd-key.pub
```

- c 为每个节点上的 `vpzd-extension` 解决方案用户生成密钥对。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpzd-extension-key.priv --pubkey=vpzd-extension-key.pub
```

- d 为每个节点上的 `vsphere-webclient` 解决方案用户生成密钥对。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub
```

- e 为每个节点上的 wcp 解决方案用户生成密钥对。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

- 2 为每个 vCenter Server 节点上的计算机解决方案用户以及每个其他解决方案用户（vpxd、vpxd-extension、vsphere-webclient、wcp）生成由新的 VMCA 根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 运行以下命令，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。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

- b 为每个节点上的计算机解决方案用户生成证书。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine
```

- c 为每个节点上的 vpxd 解决方案用户生成证书。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd.crt --privkey=vpxd-key.priv --Name=vpxd
```

- d 为每个节点上的 vpxd-extension 解决方案用户生成证书。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpxd-extension.crt --privkey=vpxd-extension-key.priv --Name=vpxd-extension
```

- e 通过运行以下命令为每个节点上的 vsphere-webclient 解决方案用户生成证书。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient
```

- f 通过运行以下命令为每个节点上的 wcp 解决方案用户生成证书。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --Name=wcp
```

- 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 替换每个节点上的计算机解决方案用户证书：

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

- b 替换每个节点上的 **vpzd** 解决方案用户证书。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpzd --alias vpzd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpzd --alias vpzd --cert new-
vpzd.crt --key vpzd-key.priv
```

- c 替换每个节点上的 **vpzd-extension** 解决方案用户证书。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpzd-extension --alias vpzd-
extension
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpzd-extension --alias vpzd-
extension --cert new-vpzd-extension.crt --key vpzd-extension-key.priv
```

- d 替换每个节点上的 **vsphere-webclient** 解决方案用户证书。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias
vsphere-webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias
vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

- e 替换每个节点上的 **wcp** 解决方案用户证书。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-
wcp.crt --key wcp-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 vCenter Server 系统上运行以下命令。

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
output:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpzd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpzd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

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 替换每个 vCenter Server 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：

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```


- c 替换每个节点上的 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：

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

- d 替换每个节点上的 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：

```
/usr/lib/vmware-vmafd/bin/dir-cli update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

- e 替换每个节点上的 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：

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

- f 替换每个节点上的 wcp 解决方案用户证书。例如，如果 wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e 是 wcp 解决方案用户 ID，请运行以下命令：

```
/usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
b5e7-9460e2b8200e --cert new-wcp.crt
```

后续步骤

重新启动每个 vCenter Server 节点上的所有服务。

使用 CLI 将 VMCA 设为中间证书颁发机构

可以使用 CLI 将 VMCA 根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。

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 环境内的证书的详细信息，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>。

使用 CLI 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 并发送要签名的 CSR。然后，使用 CLI 将签名证书作为根证书添加到 VMCA。

可以使用 Certificate Manager 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（最小值）到 16384 位（最大值）（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，并且证书签名必须在要求列表中。例如：

```
basicConstraints      = critical,CA:true
keyUsage              = critical,digitalSignature,keyCertSign
```

- 必须启用 CRL 签名。
- 扩展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。

有关使用 Microsoft 证书颁发机构的示例，请参见 VMware 知识库文章《在 vSphere 6.x 中创建 Microsoft 证书颁发机构模板以创建 SSL 证书》，网址为 <http://kb.vmware.com/kb/2112009>。

替换根证书时，VMCA 会验证以下证书属性：

- 密钥大小：2048 位（最小值）到 16384 位（最大值）
- 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。

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

4 替换现有 VMCA 根 CA。

```
certool --rootca --cert=rootcal.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，如果证书链中只有一个证书：

```
dir-cli trustedcert publish --cert rootcal.crt
```

如果证书链中有多个证书：

```
dir-cli trustedcert publish --cert rootcal.crt --chain
```

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

使用带 --rootca 选项的 certool 命令将 VMCA 根证书替换为自定义 CA 根证书。

```
/usr/lib/vmware-vmca/bin/certool --rootca --cert=<path>/root.pem --privkey=<path>/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[使用命令行替换 vCenter Server STS 证书](#)。

使用 CLI 替换计算机 SSL 证书（中间 CA）

从 CA 收到签名证书后，您可以使用 CLI 将其设置为 VMCA 根证书并替换所有计算机 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。当多个 vCenter Server 实例以增强型链接模式配置进行连接时，必须在每个节点上运行计算机 SSL 证书生成命令。

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 certtool.cfg。

certtool.cfg 文件位于 /usr/lib/vmware-vmca/share/config/ 目录中。

- 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：

```
certtool --genkey --privkey=machine1.priv --pubkey=machine1.pub
certtool --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。

```
service-control --stop --all
service-control --start vmafd
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-<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。在包含以增强型链接模式配置连接的多个 vCenter Server 实例的部署中，在每个 vCenter Server 节点上运行以下命令。

```
/usr/lib/vmware-vmca/bin/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 根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。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv
--config=ssl-config.cfg
```

将在当前目录中创建 `new-vmca-ssl.crt` 文件。

- 4 （可选）列出 VECS 的内容。

```
/usr/lib/vmware-vmafd/bin/vecs-cli store list
```

■ vCenter Server 中的输出示例：

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vsphere-webclient
vpxd
vpxd-extension
hvc
data-encipherment
APPLMGMT_PASSWORD
SMS
wcp
KMS_ENCRYPTION
```

- 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。

- 在每个 vCenter Server 上，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。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store MACHINE_SSL_CERT --alias
__MACHINE_CERT
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store MACHINE_SSL_CERT --alias
__MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

使用 CLI 替换解决方案用户证书（中间 CA）

替换计算机 SSL 证书后，可以使用 CLI 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 vCenter Server 系统上的计算机解决方案用户证书和解决方案用户证书。

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 certtool.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：

```
certtool --genkey --privkey=vpxd.priv --pubkey=vpxd.pub
certtool --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。

```
dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e
```

在包含以增强型链接模式配置连接的多个 vCenter Server 实例的部署中，dir-cli service 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。

- 4 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 vmafd
service-control --start vmdird
service-control --start vmcad
```

- 5 依次替换 vmdird 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 vmdird 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 在增强型链接模式配置中的每个 vCenter Server 节点上，为每个解决方案用户生成一个公钥/私钥对，其中包括为计算机解决方案用户生成一个密钥对以及为每个其他解决方案用户（vpxd、vpxd-extension、vsphere-webclient、wcp）生成一个密钥对。

- a 为计算机解决方案用户生成密钥对。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- b 为每个节点上的 vpxd 解决方案用户生成密钥对。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpxd-key.priv --pubkey=vpxd-key.pub
```

- c 为每个节点上的 **vpzd-extension** 解决方案用户生成密钥对。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vpzd-extension-key.priv --
pubkey=vpzd-extension-key.pub
```

- d 为每个节点上的 **vsphere-webclient** 解决方案用户生成密钥对。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=vsphere-webclient-key.priv --
pubkey=vsphere-webclient-key.pub
```

- e 为每个节点上的 **wcp** 解决方案用户生成密钥对。

```
/usr/lib/vmware-vmca/bin/certool --genkey --privkey=wcp-key.priv --pubkey=wcp-key.pub
```

- 2 为每个 vCenter Server 节点上的计算机解决方案用户以及每个其他解决方案用户（**vpzd**、**vpzd-extension**、**vsphere-webclient**、**wcp**）生成由新的 **VMCA** 根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 **vpzd** 或 **vpzd-extension**。

- a 运行以下命令，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。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-
key.priv --Name=machine
```

- b 为每个节点上的计算机解决方案用户生成证书。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-machine.crt --privkey=machine-
key.priv --Name=machine
```

- c 为每个节点上的 **vpzd** 解决方案用户生成证书。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpzd.crt --privkey=vpzd-key.priv
--Name=vpzd
```

- d 为每个节点上的 **vpzd-extension** 解决方案用户生成证书。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vpzd-extension.crt --
privkey=vpzd-extension-key.priv --Name=vpzd-extension
```

- e 通过运行以下命令为每个节点上的 **vsphere-webclient** 解决方案用户生成证书。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-vsphere-webclient.crt --
privkey=vsphere-webclient-key.priv --Name=vsphere-webclient
```

- f 通过运行以下命令为每个节点上的 **wcp** 解决方案用户生成证书。

```
/usr/lib/vmware-vmca/bin/certool --gencert --cert=new-wcp.crt --privkey=wcp-key.priv --
Name=wcp
```


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 替换每个节点上的计算机解决方案用户证书：

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store machine --alias machine
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store machine --alias machine --cert
new-machine-vc.crt --key machine-vc-key.priv
```

b 替换每个节点上的 vpxd 解决方案用户证书。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd --alias vpxd
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd --alias vpxd --cert new-
vpxd.crt --key vpxd-key.priv
```

c 替换每个节点上的 vpxd-extension 解决方案用户证书。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vpxd-extension --alias vpxd-
extension
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vpxd-extension --alias vpxd-
extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

d 替换每个节点上的 vsphere-webclient 解决方案用户证书。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store vsphere-webclient --alias
vsphere-webclient
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store vsphere-webclient --alias
vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

e 替换每个节点上的 wcp 解决方案用户证书。

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry delete --store wcp --alias wcp
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store wcp --alias wcp --cert new-
wcp.crt --key wcp-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 vCenter Server 系统上运行以下命令。

```
/usr/lib/vmware-vmafd/bin/dir-cli service list
output:
1. machine-623bef28-0311-436e-b21f-6e0d39aa5179
2. vsphere-webclient-623bef28-0311-436e-b21f-6e0d39aa5179
```

```

3. vpxd-623bef28-0311-436e-b21f-6e0d39aa5179
4. vpxd-extension-623bef28-0311-436e-b21f-6e0d39aa5179
5. hvc-623bef28-0311-436e-b21f-6e0d39aa5179
6. wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e

```

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 替换每个 vCenter Server 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：

```

/usr/lib/vmware-vmafd/bin/dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt

```

- c 替换每个节点上的 `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：

```

/usr/lib/vmware-vmafd/bin/dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt

```

- d 替换每个节点上的 `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：

```

/usr/lib/vmware-vmafd/bin/dir-cli update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt

```

- e 替换每个节点上的 `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：

```

/usr/lib/vmware-vmafd/bin/dir-cli service update --name vsphere-
webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt

```

- f 替换每个节点上的 `wcp` 解决方案用户证书。例如，如果 `wcp-1cbe0a40-e4ce-4378-b5e7-9460e2b8200e` 是 `wcp` 解决方案用户 ID，请运行以下命令：

```

/usr/lib/vmware-vmafd/bin/dir-cli service update --name wcp-1cbe0a40-e4ce-4378-
b5e7-9460e2b8200e --cert new-wcp.crt

```

使用 CLI 将证书替换为自定义证书

如果公司策略有相关要求，则可以使用 CLI 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。vCenter Server 仅将解决方案用户证书用于内部通信。解决方案用户证书不用于外部通信。

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 [使用 Certificate Manager 将所有证书替换为自定义证书](#)。

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。

使用 CLI 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。第一步是使用 CLI 向证书颁发机构请求证书并将根证书导入 VMware 端点证书存储 (VECS)。

前提条件

证书必须满足以下要求：

- 密钥大小：2048 位（最小值）到 16384 位（最大值）（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
- 包含以下密钥用法：数字签名、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证书签名请求 (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）每个节点具有五个解决方案用户证书。解决方案用户证书不需包括 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。

通常，结果为信任链的 PEM 文件以及每个 vCenter Server 节点的签名 SSL 证书。

2 列出 TRUSTED_ROOTS 和计算机 SSL 存储。

```
vecs-cli store list
```

- 确保当前根证书和所有计算机 SSL 证书均为 VMCA 签名证书。
- 请记住“序列号”、“颁发者”和“主体 CN”字段。
- （可选）使用 Web 浏览器，打开与将替换证书的节点的 HTTPS 连接，查看证书信息，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。

```
service-control --stop --all
service-control --start vmafd
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[使用命令行替换 vCenter Server STS 证书](#)。

使用 CLI 将计算机 SSL 证书替换为自定义证书

收到自定义证书后，可以使用 CLI 替换每个计算机证书。

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）
- 有效的自定义根证书（.crt 文件）

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（最小值）到 16384 位（最大值）（PEM 编码）
- CRT 格式
- x509 版本 3
- SubjectAltName 必须包含 DNS Name=<machine_FQDN>。
- 包含以下密钥用法：数字签名、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 vmafd
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 更新 Lookup Service 注册端点。

```
/usr/lib/vmware-lookupsvc/tools/ls_update_certs.py --url https://<vCenterServer_FQDN>/lookupservice/sdk --certfile <cert-file-path> --user 'administrator@vsphere.local' --password '<password>' --fingerprint <SHA1_hash_of_the_old_certificate_to_replace>
```

- 4 重新启动所有服务。

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

vSphere 证书和服务 CLI 命令参考

3

您可以使用一组 CLI 管理 VMCA (VMware Certificate Authority)、VECS (VMware Endpoint 证书存储)、VMware Directory Service (vmdir) 和 Security Token Service (STS) 证书。vSphere Certificate Manager 实用程序也支持许多相关任务，但手动证书管理和与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>。

手动替换 vSphere 证书提供了关于使用 CLI 命令替换证书的示例。

表 3-1. 用于管理证书和关联服务的 vSphere 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 VMware Authentication Framework 守护进程 (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.sh	管理 STS 证书。	命令行帮助。输入不带任何选项的 sso-config.sh 将显示命令行帮助。
service-control	启动或停止服务，例如，在证书替换工作流程中。	在运行其他 CLI 命令之前，运行此命令以停止服务。

vSphere CLI 位置

默认情况下，在以下位置查找 CLI。

```
/usr/lib/vmware-vmafd/bin/vecs-cli
/usr/lib/vmware-vmafd/bin/dir-cli
/usr/lib/vmware-vmca/bin/certool
/opt/vmware/bin/sso-config.sh
```

注 service-control 命令不要求您指定路径。

运行 vSphere 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 (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。管理员组中的用户具有完整访问权限。

MACHINE_SSL_CERT 和 TRUSTED_ROOTS 存储属于特殊存储。只有 root 用户或管理员用户（取决于安装类型）才拥有完全访问权限。

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 /usr/lib/vmware-vmca/share/config/ 目录中。

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。

```
■ /usr/lib/vmware-vmca/bin/certool --gencert --config /tmp/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：

```
/usr/lib/vmware-vmca/bin/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`。

本章讨论了以下主题：

- [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](#)

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 VMware 证书颁发机构 (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[使用 CLI 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
--gencsr	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 --gencsr --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 CLI 将 VMCA 设为中间证书颁发机构](#)。

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。

选项	描述
<code>--privkey <key_file></code>	专用密钥文件的名称。该文件必须是 PEM 编码的格式。
<code>--server <server></code>	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
<code>--server <server></code>	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。
<code>--port <port_num></code>	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
<code>--wait</code>	可选的等待分钟数。默认值为“3”。
<code>--server <server></code>	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。
<code>--port <port_num></code>	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
<code>--wait</code>	可选的等待分钟数。默认值为“3”。
<code>--server <server></code>	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。
<code>--port <port_num></code>	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
<code>--server <server></code>	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
<code>--genkey</code>	生成专用和公用密钥时为必需项。
<code>--privkey <keyfile></code>	专用密钥文件的名称。
<code>--pubkey <keyfile></code>	公用密钥文件的名称。
<code>--server <server></code>	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
<code>--gencert</code>	生成证书时为必需项。
<code>--cert <certfile></code>	证书文件的名称。该文件必须是 PEM 编码的格式。
<code>--privkey <keyfile></code>	专用密钥文件的名称。该文件必须是 PEM 编码的格式。
<code>--config <config_file></code>	配置文件的可选名称。默认为 <code>certool.cfg</code> 。
<code>--server <server></code>	VMCA 服务器的可选名称。默认情况下，该命令使用 <code>localhost</code> 。

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。此输出无法用作证书，它将更改为人工可读。

选项	描述
<code>--getrootca</code>	打印根证书时为必需项。
<code>--server <server></code>	VMCA 服务器的可选名称。默认情况下，该命令使用 <code>localhost</code> 。

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
<code>--viewcert</code>	查看证书时为必需项。
<code>--cert <certfile></code>	配置文件的可选名称。默认为 <code>certool.cfg</code> 。

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
<code>--enumcert</code>	列出所有证书时为必需项。
<code>--filter [all active]</code>	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
<code>--status</code>	检查证书状态时为必需项。
<code>--cert <certfile></code>	配置文件的可选名称。默认为 <code>certool.cfg</code> 。
<code>--server <server></code>	VMCA 服务器的可选名称。默认情况下，该命令使用 <code>localhost</code> 。

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
<code>--genselfcacert</code>	生成自签名证书时为必需项。
<code>--outcert <cert_file></code>	证书文件的名称。该文件必须是 PEM 编码的格式。
<code>--outprivkey <key_file></code>	专用密钥文件的名称。该文件必须是 PEM 编码的格式。
<code>--config <config_file></code>	配置文件的可选名称。默认为 <code>certool.cfg</code> 。

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身份验证服务。

vecs-cli store create

创建证书存储。

选项	描述
<code>--name <name></code>	证书存储的名称。
<code>--server <server-name></code>	如果您连接到远程 VECS 实例，则用于指定服务器名称。
<code>--upn <user-name></code>	用于登录到 <code>--server <server-name></code> 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 <code>root</code> 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
<code>--name <name></code>	要删除的证书存储的名称。
<code>--server <server-name></code>	如果您连接到远程 VECS 实例，则用于指定服务器名称。
<code>--upn <user-name></code>	用于登录到 <code>--server <server-name></code> 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 <code>root</code> 用户。

例如：

```
vecs-cli store delete --name <store>
```

vecs-cli store list

列出证书存储。

选项	描述
<code>--server <server-name></code>	如果您连接到远程 VECS 实例，则用于指定服务器名称。
<code>--upn <user-name></code>	用于登录到 <code>--server <server-name></code> 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 3-2. VECS 中的库

库	描述
计算机 SSL 库 (MACHINE_SSL_CERT)	<ul style="list-style-type: none"> ■ 由每个 vSphere 节点上的反向代理服务使用。 ■ 由 VMware Directory Service (vmdir) 在每个 vCenter Server 节点上使用。 <p>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。</p>
解决方案用户库 <ul style="list-style-type: none"> ■ machine ■ vpxd ■ vpxd-extension ■ vsphere-webclient ■ wcp 	<p>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。</p> <p>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。</p> <p>VECS 中包含以下解决方案用户证书存储：</p> <ul style="list-style-type: none"> ■ machine：由 License Server 和日志记录服务使用。 <p>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。</p> <ul style="list-style-type: none"> ■ vpxd：vCenter 服务守护进程 (vpxd) 存储。vpxd 使用存储在此存储中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 Client 存储。还包括其他一些服务，例如性能图表服务。 ■ wcp：VMware vSphere® 和 VMware Tanzu™ 存储。 <p>每个 vCenter Server 节点包含一个 machine 证书。</p>
受信任的根存储 (TRUSTED_ROOTS)	包含所有受信任的根证书。

表 3-2. VECS 中的库（续）

库	描述
vSphere Certificate Manager 实用程序备份库 (BACKUP_STORE)	由 VMCA (VMware Certificate Manager) 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	<p>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。</p> <p>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。</p>

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
<code>--name <name></code>	证书存储的名称。
<code>--user <username></code>	被授予权限的用户的唯一名称。
<code>--grant [read write]</code>	授予读取或写入权限。
<code>--revoke [read write]</code>	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
<code>--name <name></code>	证书存储的名称。
<code>--server <server-name></code>	如果您连接到远程 VECS 实例，则用于指定服务器名称。
<code>--upn <user-name></code>	用于登录到 <code>--server <server-name></code> 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 <code>root</code> 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。

注 请勿使用此命令将根证书添加到 TRUSTED_ROOTS 存储，而是使用 `dir-cli` 命令发布根证书。

选项	描述
<code>--store <NameOfStore></code>	证书存储的名称。
<code>--alias <Alias></code>	证书的可选别名。对于受信任的根存储，将忽略此选项。
<code>--cert <certificate_file_path></code>	证书文件的完整路径。
<code>--key <key-file-path></code>	与证书对应的密钥的完整路径。 可选。
<code>--password <password></code>	加密专用密钥的可选密码。
<code>--server <server-name></code>	如果您连接到远程 VECS 实例，则用于指定服务器名称。
<code>--upn <user-name></code>	用于登录到 <code>--server <server-name></code> 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
<code>--store <NameOfStore></code>	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
<code>--store <NameOfStore></code>	证书存储的名称。
<code>--alias <Alias></code>	证书的别名。
<code>--output <output_file_path></code>	要向其写入证书的文件。
<code>--text</code>	显示证书的人工可读版本。
<code>--server <server-name></code>	如果您连接到远程 VECS 实例，则用于指定服务器名称。
<code>--upn <user-name></code>	用于登录到 <code>--server <server-name></code> 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
<code>--store <NameOfStore></code>	证书存储的名称。
<code>--alias <Alias></code>	密钥的别名。
<code>--output <output_file_path></code>	要向其写入密钥的输出文件。
<code>--text</code>	显示密钥的人工可读版本。
<code>--server <server-name></code>	如果您连接到远程 VECS 实例，则用于指定服务器名称。
<code>--upn <user-name></code>	用于登录到 <code>--server <server-name></code> 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
<code>--store <NameOfStore></code>	证书存储的名称。
<code>--alias <Alias></code>	要删除的条目的别名。
<code>--server <server-name></code>	如果您连接到远程 VECS 实例，则用于指定服务器名称。
<code>--upn <user-name></code>	用于登录到 <code>--server <server-name></code> 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。
<code>-y</code>	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
<code>--server <server-name></code>	如果您连接到远程 VECS 实例，则用于指定服务器名称。
<code>--upn <user-name></code>	用于登录到 <code>--server <server-name></code> 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。可以使用 dir-cli 管理和查询 vCenter Server 实例的域功能级别。

dir-cli nodes list

列出所有通过增强型链接模式连接的 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>	使用此选项可连接到其他 vCenter Server 以查看其复制合作伙伴。

dir-cli computer password-reset

使您能够重置域中计算机帐户的密码。

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>	vCenter Server 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。

选项	描述
<code>--last-name <name></code>	用户的姓氏。
<code>--login <admin_user_id></code>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 <code>administrator@vsphere.local</code> 。
<code>--password <admin_password></code>	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

修改 vmdir 中的指定用户。

选项	描述
<code>--account <name></code>	要修改的 vCenter Single Sign-On 用户的名称。
<code>--password-never-expires</code>	如果要修改必须向 vCenter Server 进行身份验证的自动任务的用户帐户，并且要确保这些任务不会因密码过期而停止运行，请将该选项设置为 <code>True</code> 。 谨慎使用该选项。
<code>--password-expires</code>	如果要恢复 <code>--password-never-expires</code> 选项，请将该选项设置为 <code>true</code> 。
<code>--login <admin_user_id></code>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 <code>administrator@vsphere.local</code> 。
<code>--password <admin_password></code>	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
<code>--account <name></code>	要删除的 vCenter Single Sign-On 用户的名称。
<code>--login <admin_user_id></code>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 <code>administrator@vsphere.local</code> 。
<code>--password <admin_password></code>	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
<code>--account <name></code>	要删除的 vCenter Single Sign-On 用户的名称。
<code>--level <info level 0 1 2></code>	返回下列信息： <ul style="list-style-type: none"> ■ 级别 0 - 帐户和 UPN ■ 级别 1 - 级别 0 信息 + 名和姓 ■ 级别 2: 级别 0 + 帐户停用标记、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。
<code>--login <admin_user_id></code>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 <code>administrator@vsphere.local</code> 。
<code>--password <admin_password></code>	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

将用户或组添加到现有组。

选项	描述
<code>--name <name></code>	vmdir 中组的名称。
<code>--add <user_or_group_name></code>	要添加的用户或组的名称。
<code>--login <admin_user_id></code>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 <code>administrator@vsphere.local</code> 。
<code>--password <admin_password></code>	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
<code>--name <name></code>	vmdir 中组的可选名称。此选项可用于检查特定组是否存在。
<code>--login <admin_user_id></code>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 <code>administrator@vsphere.local</code> 。
<code>--password <admin_password></code>	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。
--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
<code>--cert-file <file></code>	要取消发布的证书文件的路径。
<code>--login <admin_user_id></code>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 <code>administrator@vsphere.local</code> 。
<code>--password <admin_password></code>	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
<code>--login <admin_user_id></code>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 <code>administrator@vsphere.local</code> 。
<code>--password <admin_password></code>	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
<code>--id <cert_ID></code>	要检索的证书的 ID。 <code>dir-cli trustedcert list</code> 命令显示 ID。
<code>--outcert <path></code>	要将证书文件写入到的路径。
<code>--outcrl <path></code>	要将 CRL 文件写入到的路径。当前未使用。
<code>--login <admin_user_id></code>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 <code>administrator@vsphere.local</code> 。
<code>--password <admin_password></code>	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
<code>--login <admin_user_id></code>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 <code>administrator@vsphere.local</code> 。
<code>--password <admin_password></code>	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
<code>--account</code>	要向其分配新密码的帐户名称。
<code>--new</code>	指定用户的新密码。
<code>--login <admin_user_id></code>	默认情况下，为本地 vCenter Single Sign-On 域的管理员 <code>administrator@vsphere.local</code> 。
<code>--password <admin_password></code>	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
<code>--account</code>	帐户名称。
<code>--current</code>	拥有帐户的用户的当前密码。
<code>--new</code>	拥有帐户的用户的新密码。

使用 vCenter Single Sign-On 进行 vSphere 身份验证

4

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。vCenter Single Sign-On 在用户进行身份验证时发出令牌。用户可以使用该令牌向 vCenter Server 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。

用户和服务帐户使用令牌或者用户名和密码进行身份验证。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 2 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。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：

- 如何使用 vCenter Single Sign-On 保护您的环境
- 了解 vCenter Server 身份提供程序联合
- 配置 vCenter Server 身份提供程序联合
- 了解 vCenter Single Sign-On
- 配置 vCenter Single Sign-On 标识源
- 管理 vCenter Server Security Token Service
- 管理 vCenter Single Sign-On 策略
- 管理 vCenter Single Sign-On 用户和组
- 了解其他 vSphere 身份验证选项
- 管理 vSphere Client 登录页面的登录消息
- vCenter Single Sign-On 安全性最佳做法

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。

- 通过外部身份提供程序联合或 vCenter Server 内置身份提供程序对用户进行身份验证。内置身份提供程序支持本地帐户、Active Directory 或 OpenLDAP、集成 Windows 身份验证 (IWA) 和其他身份验证机制（智能卡、RSA SecurID 和 Windows 会话身份验证）。
- 通过证书对解决方案用户进行身份验证。
- Security Token Service (STS)。
- 用于确保安全流量的 SSL。

身份提供程序概述

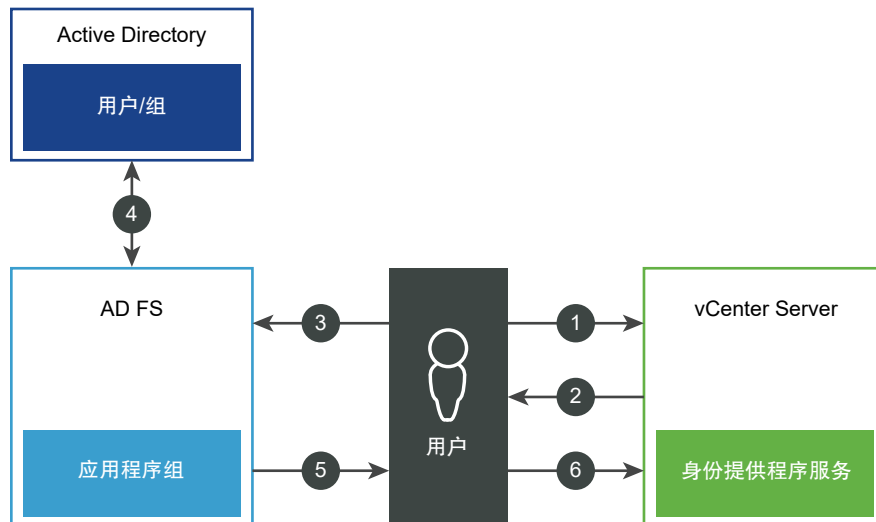
在 vSphere 7.0 之前，vCenter Server 包含一个内置身份提供程序。默认情况下，vCenter Server 使用 vsphere.local 域作为标识源（但可以在安装过程中进行更改）。可以使用 LDAP/S、OpenLDAP/S 和集成 Windows 身份验证 (IWA)，将 vCenter Server 内置身份提供程序配置为使用 Active Directory (AD) 作为其标识源。此类配置允许客户使用其 AD 帐户登录到 vCenter Server。

从 vSphere 7.0 开始，可以使用联合身份验证为 vCenter Server 配置外部身份提供程序。在此类配置中，将替换 vCenter Server 作为身份提供程序。目前，vSphere 支持将 Active Directory 联合身份验证服务 (AD FS) 作为外部身份提供程序。在此配置中，AD FS 代表 vCenter Server 与标识源进行交互。

用户使用 vCenter Server 身份提供程序联合身份验证登录

下图显示了 vCenter Server 身份提供程序联合的用户登录流程。

图 4-1. vCenter Server 身份提供程序联合用户登录



vCenter Server、AD FS 和 Active Directory 按以下方式进行交互:

- 1 用户首先在 vCenter Server 登录页输入用户名。
- 2 如果用户名用于联合域，vCenter Server 会将身份验证请求重定向到 AD FS。
- 3 （如果需要）AD FS 提示用户使用 Active Directory 凭据登录。
- 4 AD FS 使用 Active Directory 对用户进行身份验证。
- 5 AD FS 发出包含 Active Directory 中组信息的安全令牌。
- 6 vCenter Server 使用令牌登录用户。

现在对用户进行身份验证，然后用户可以查看和修改用户角色具有特权的任何对象。

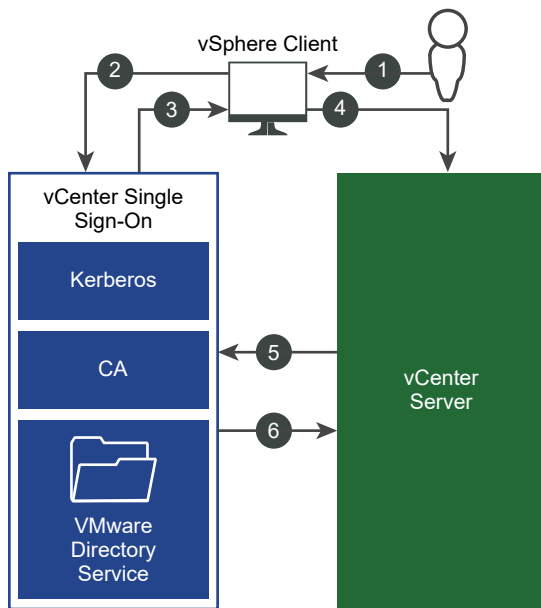
注 首先，每个用户都分配有“无权访问”角色。vCenter Server 管理员必须至少为用户分配“只读”角色，用户才能登录。请参见《vSphere 安全性》文档。

如果外部身份提供程序不可访问，登录过程将回退到 vCenter Server 登录页，并显示相应的信息消息。用户仍可以使用 `vsphere.local` 标识源中的本地帐户登录。

用户使用 vCenter Server 内置身份提供程序登录

下图显示了 vCenter Server 作为身份提供程序时的用户登录流程。

图 4-2. 用户使用 vCenter Server 内置身份提供程序登录



- 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。

配置了集成 Windows 身份验证 (IWA) 后，用户也可以通过选中**使用 Windows 会话身份验证**复选框来登录，而无需重新输入其 Windows 密码。

- 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。

现在对用户进行身份验证，然后用户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。

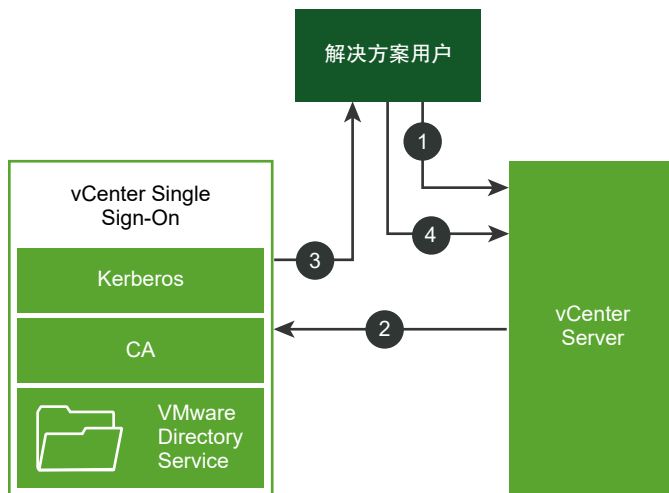
解决方案用户登录

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 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。

注 vCenter Server 仅将解决方案用户证书用于内部通信。解决方案用户证书不用于外部通信。

下图显示了解决方案用户的登录流程。

图 4-3. 解决方案用户登录



- 1 解决方案用户尝试连接到 vCenter Server 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。

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[使用 CLI 将证书替换为自定义证书](#)。

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。

了解 vCenter Server 身份提供程序联合

从 vSphere 7.0 开始，vCenter Server 支持登录到 vCenter Server 时执行联合身份验证。

要启用对 vCenter Server 进行联合身份验证，需要配置与外部身份提供程序的连接。配置的身份提供程序实例会替换 vCenter Server 作为身份提供程序。目前，vCenter Server 仅支持 Active Directory 联合身份验证服务 (AD FS) 作为外部身份提供程序。

注 随着 vSphere 转向基于令牌的身份验证，VMware 建议使用联合身份验证。vCenter Server 继续拥有本地帐户，用于管理访问和错误恢复。

vCenter Server 身份提供程序联合的工作原理

通过 vCenter Server 身份提供程序联合，可以配置外部身份提供程序，以实现联合身份验证。在此配置中，外部身份提供程序代表 vCenter Server 与标识源进行交互。

vCenter Server 身份提供程序联合基础知识

从 vSphere 7.0 开始，vCenter Server 支持联合身份验证。在这种情况下，当用户登录到 vCenter Server 时，vCenter Server 会将用户登录重定向到外部身份提供程序。不再直接向 vCenter Server 提供用户凭据。而是，用户向外部身份提供程序提供凭据。vCenter Server 信任外部身份提供程序以执行身份验证。在联合模型中，用户永远不会直接向任何服务或应用程序提供凭据，而是仅向身份提供程序提供凭据。因此，可以将您的应用程序和服务（如 vCenter Server）与您的身份提供程序进行“联合”。

vCenter Server 身份提供程序联合的优势

vCenter Server 身份提供程序联合提供以下优势。

- 可以将 Single Sign-On 与现有联合基础架构和应用程序配合使用。

- 可以提高数据中心的安全性，因为 vCenter Server 从不处理用户的凭据。
- 可以使用外部身份提供程序支持的身份验证机制，例如多因素身份验证。

vCenter Server 身份提供程序联合组件

以下组件包含使用 Microsoft Active Directory 联合身份验证服务 (AD FS) 的 vCenter Server 身份提供程序联合配置：

- vCenter Server
- 在 vCenter Server 上配置的身份提供程序服务
- AD FS 服务器和关联的 Microsoft Active Directory 域
- AD FS 应用程序组
- 映射到 vCenter Server 组和用户的 Active Directory 组 and 用户

注 目前，vCenter Server 仅支持 AD FS 作为外部身份提供程序。

vCenter Server 身份提供程序联合架构

在 vCenter Server 身份提供程序联合中，vCenter Server 使用 OpenID Connect (OIDC) 协议接收身份令牌，用于对 vCenter Server 用户进行身份验证。

要在 vCenter Server 和身份提供程序之间建立依赖方信任，必须在它们之间建立标识信息和共享密钥。为此，在 AD FS 中，需要创建称为“应用程序组”的 OIDC 配置，该配置由服务器应用程序和 Web API 组成。这两个组件指定 vCenter Server 用于信任 and 与 AD FS 服务器通信的信息。还需在 vCenter Server 中创建相应的身份提供程序。最后，在 vCenter Server 中配置组成员资格，以授权来自 AD FS 域中用户的登录。

AD FS 管理员必须提供以下信息才能创建 vCenter Server 身份提供程序配置：

- 客户端标识符：由 AD FS “应用程序组” 向导生成并标识应用程序组本身的 UUID 字符串。
- 共享密钥：由 AD FS “应用程序组” 向导生成并用于通过 AD FS 对 vCenter Server 进行身份验证的密钥。
- OpenID 地址：AD FS 服务器的 OpenID 提供程序发现端点 URL，指定通常作为与路径 “/.well-known/openid-configuration” 连接的颁发者端点的已知地址。例如：`https://webserver.example.com/adfs/.well-known/openid-configuration`。

vCenter Server 身份提供程序联合和增强型链接模式

在使用增强型链接模式的 vCenter Server 环境中启用身份提供程序联合时，身份验证和工作流的运行方式保持不变。

如果使用增强型链接模式配置，在使用联合身份验证登录到 vCenter Server 时，请注意以下几点。

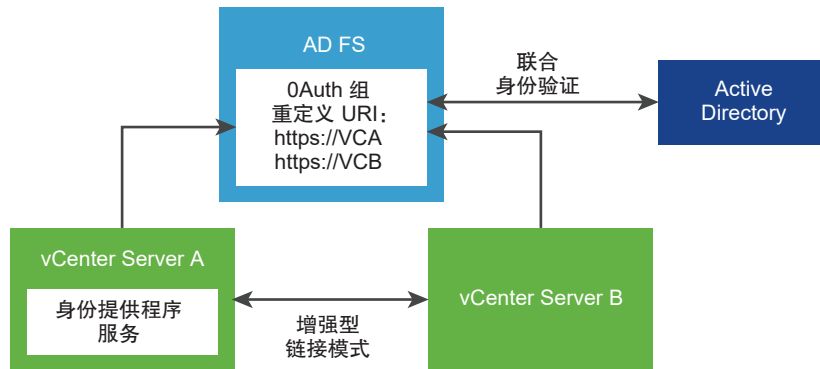
- 根据 vCenter Server 权限和角色模型，用户继续查看相同的清单，并执行相同的操作。

- 采用增强型链接模式的 vCenter Server 主机无需访问彼此的身份提供程序。例如，假设有两个 vCenter Server 系统 A 和 B，并使用增强型链接模式。在 vCenter Server A 授权用户之后，也会在 vCenter Server B 上授权该用户。

身份验证工作流程增强型链接模式和 vCenter Server 身份提供程序联合

下图显示了使用增强型链接模式和 vCenter Server 身份提供程序联合的身份验证工作流程。

图 4-4. 增强型链接模式和 vCenter Server 身份提供程序联合



- 1 以增强型链接模式配置部署两个 vCenter Server 节点。
- 2 已使用 vSphere Client 中的“更改身份提供程序”向导在 vCenter Server A 上配置 AD FS 设置。还为 AD FS 用户或组建立了组成员资格和权限。
- 3 vCenter Server A 将 AD FS 配置复制到 vCenter Server B。
- 4 两个 vCenter Server 节点的所有重定向 URI 都将添加到 AD FS 中的 OAuth 应用程序组。仅创建一个 OAuth 应用程序组。
- 5 当用户登录到 vCenter Server A 并获得授权时，该用户也获得了 vCenter Server B 的授权。如果用户先登录到 vCenter Server B，同样如此。

vCenter Server 增强型链接模式支持身份提供程序联合的以下配置方案。在此部分中，术语“AD FS 设置”和“AD FS 配置”指的是在 vSphere Client 中使用“更改身份提供程序”向导配置的设置，以及为 AD FS 用户或组建立的任何组成员资格或权限。

在现有增强型链接模式配置上启用 AD FS

简要步骤：

- 1 以增强型链接模式配置部署 N 个 vCenter Server 节点。
- 2 在其中一个链接的 vCenter Server 节点上配置 AD FS。
- 3 将 AD FS 配置复制到所有其他 (N-1) 个 vCenter Server 节点。
- 4 将所有 N 个 vCenter Server 节点的所有重定向 URI 添加到 AD FS 中的已配置 OAuth 应用程序组。

将新的 vCenter Server 链接到现有的增强型链接模式 AD FS 配置

简要步骤:

- 1 (必备条件) 在 vCenter Server N 节点增强型链接模式配置上设置 AD FS。
- 2 部署新的独立 vCenter Server 节点。
- 3 使用 N 个节点中的一个作为其复制合作伙伴, 将新 vCenter Server 重新指向 N 节点 AD FS 增强型链接模式域。
- 4 现有增强型链接模式配置中的所有 AD FS 设置都将复制到新 vCenter Server。
N 节点 AD FS 增强型链接模式域中的 AD FS 设置将覆盖新链接的 vCenter Server 上的任何现有 AD FS 设置。
- 5 将新 vCenter Server 的所有重定向 URI 添加到 AD FS 中的现有已配置 OAuth 应用程序组。

取消 vCenter Server 与增强型链接模式 AD FS 配置的链接

简要步骤:

- 1 (必备条件) 在 N 节点 vCenter Server 增强型链接模式配置上设置 AD FS。
- 2 取消注册 N 节点配置中的一个 vCenter Server 主机, 并将其重新指向新域, 以便取消其与 N 节点配置的链接。
- 3 域重新指向过程不保留 SSO 设置, 因此取消链接的 vCenter Server 节点上的所有 AD FS 设置都将恢复并丢失。要在此取消链接的 vCenter Server 节点上继续使用 AD FS, 必须从头开始重新配置 AD FS, 或者必须将 vCenter Server 重新链接到已设置 AD FS 的增强型链接模式配置。

vCenter Server 身份提供程序局限性和互操作性

vCenter Server 身份提供程序联合可以与许多其他 VMware 功能进行交互操作。

在计划 vCenter Server 身份提供程序联合策略时, 请考虑可能的互操作限制。

身份验证机制

在 vCenter Server 身份提供程序联合配置中, 外部身份提供程序处理身份验证机制 (密码、MFA、生物识别等)。

支持单一 Active Directory 域

在配置 vCenter Server 身份提供程序联合时, “配置主身份提供程序” 向导将提示您输入包含希望访问 vCenter Server 的用户和组的 AD 域的 LDAP 信息。vCenter Server 将从您在向导中指定的用户基本 DN 派生用于授权和权限的 AD 域。只能为此 AD 域中的用户和组添加 vSphere 对象的权限。vCenter Server 身份提供程序联合不支持 AD 子域中或 AD 林中其他域中的用户或组。

vCenter Server 策略

当 vCenter Server 作为身份提供程序时, 您可以控制 vsphere.local 域的 vCenter Server 密码、锁定和令牌策略。将联合身份验证与 vCenter Server 结合使用时, 外部身份提供程序可控制存储在标识源 (如 Active Directory) 中的帐户的密码、锁定和令牌策略。

审核和合规性

使用 vCenter Server 身份提供程序联合时，vCenter Server 会继续为成功用户登录创建日志条目。但是，外部身份提供程序负责跟踪和记录操作，如密码输入尝试失败和用户帐户锁定。vCenter Server 不会记录此类事件，因为这些事件对 vCenter Server 不再可见。例如，当 AD FS 是身份提供程序时，AD FS 跟踪并记录联合登录错误。当 vCenter Server 是用于本地登录的身份提供程序时，vCenter Server 跟踪并记录本地登录错误。在联合配置中，vCenter Server 会继续记录用户的登录后操作。

现有 VMware 产品集成

与 vCenter Server 集成的 VMware 产品（例如，VMware vRealize Operations、VMware vSAN™、VMware NSX® 等）可继续像以前一样正常工作。

集成登录后的产品

集成登录后的产品（即，不需要单独登录）可继续像以前一样正常工作。

用于 API、SDK 和 CLI 访问的简单身份验证

现有脚本、产品和其他依赖于使用简单身份验证（即，用户名和密码）的 API、SDK 或 CLI 命令的功能可继续像以前一样正常工作。在内部，身份验证是通过传递用户名和密码进行的。这种传递用户名和密码的方式会影响使用身份联合的一些优势，因为它会向 vCenter Server（和您的脚本）暴露密码。请考虑尽可能迁移到基于令牌的身份验证。

vCenter Server 管理界面

如果用户是管理员组的成员，则支持访问 vCenter Server 管理界面（以前称为 vCenter Server Appliance 管理界面或 VAMI）。

在 AD FS 登录页面上输入用户名文本

AD FS 登录页面不支持传递文本以预填充用户名文本框。因此，在使用 AD FS 进行联合登录期间，在 vCenter Server 登录页面上输入用户名并重定向到 AD FS 登录页面后，您必须在 AD FS 登录页面上重新输入您的用户名。需要使用您在 vCenter Server 登录页面上输入的用户名将登录重定向到相应的身份提供程序，并且需要 AD FS 登录页面上的用户名才能使用 AD FS 进行身份验证。无法将用户名传递给 AD FS 登录页面是 AD FS 的局限性。您无法直接从 vCenter Server 配置或更改此行为。

vCenter Server 身份提供程序联合生命周期

管理 vCenter Server 身份提供程序联合的生命周期时，需要考虑一些特定的注意事项。

您可以通过以下方式管理 vCenter Server 身份提供程序联合生命周期。

从使用 Active Directory 迁移到 AD FS

如果使用 Active Directory 作为 vCenter Server 的标识源，则可以直接迁移到使用 AD FS。如果您的 Active Directory 组和角色与您的 AD FS 组和角色相匹配，则无需执行任何其他操作。当组和角色不匹配时，您必须执行一些额外的工作。如果 vCenter Server 是域成员，请考虑将其从域中移除，因为身份联合不需要或使用它。

跨域重定向和迁移

vCenter Server 身份提供程序联合支持跨域重新指向，即在 vSphere SSO 域之间移动 vCenter Server。被重新指向的 vCenter Server 将从它被指向的一个或多个 vCenter Server 系统接收复制的 AD FS 配置。

通常，除非满足以下条件之一，否则无需为跨域重新指向执行任何其他 AD FS 重新配置。

- 1 被重新指向的 vCenter Server 的 AD FS 配置不同于它被指向的 vCenter Server 的 AD FS 配置。
- 2 这是被重新指向 vCenter Server 第一次接收 AD FS 配置。

在这些情况下，必须将 vCenter Server 系统的重定向 URI 添加到 AD FS 服务器上的相应应用程序组。例如，如果将具有 AD FS 应用程序组 A（或没有 AD FS 配置）的 vCenter Server 1 重新指向具有 AD FS 应用程序组 B 的 vCenter Server 2，则必须将 vCenter Server 1 的重定向 URI 添加到应用程序组 B。

配置 vCenter Server 身份提供程序联合

在最初部署 vCenter Server 后，您可以为联合身份验证配置外部身份提供程序。

您可以从 vSphere Client 或 API 配置 vCenter Server 身份提供程序联合。您还必须在外部身份提供程序上执行一些配置。要配置 vCenter Server 身份提供程序联合，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。

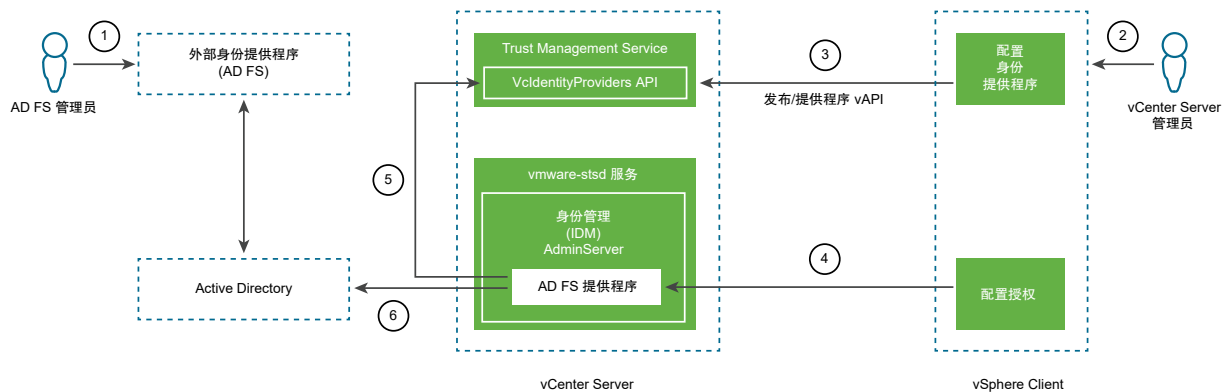
vCenter Server 身份提供程序联合配置过程流

要有效地配置 vCenter Server 身份提供程序联合，必须了解发生的通信流。

vCenter Server 身份提供程序联合配置过程流

下图显示了配置 vCenter Server 身份提供程序联合时执行的过程流。

图 4-5. vCenter Server 身份提供程序联合配置过程流



vCenter Server、AD FS 和 Active Directory 按以下方式进行交互。

- 1 AD FS 管理员为 vCenter Server 配置 AD FS OAuth 应用程序。

- 2 vCenter Server 管理员通过 vSphere Client 登录到 vCenter Server。
- 3 vCenter Server 管理员将 AD FS 身份提供程序添加到 vCenter Server，同时输入有关 Active Directory 域的信息。

vCenter Server 需要此信息才能与 AD FS 服务器的 Active Directory 域建立 LDAP 连接。使用此连接，vCenter Server 搜索用户和组，并在下一步中将其添加到 vCenter Server 本地组。有关详细信息，请参见下文标题为“搜索 Active Directory 域”的部分。

- 4 vCenter Server 管理员在 vCenter Server 中为 AD FS 用户配置授权权限。
- 5 AD FS 提供程序查询 VcIdentityProviders API 以获取 Active Directory 源的 LDAP 连接信息。
- 6 AD FS 提供程序在 Active Directory 中搜索查询的用户或组，以完成授权配置。

搜索 Active Directory 域

可以使用 vSphere Client 中的“配置主身份提供程序”向导在 vCenter Server 中将 AD FS 配置为外部身份提供程序。在配置过程中，必须输入有关 Active Directory 域的信息，包括用户和组的标识名信息。配置 AD FS 进行身份验证需要此 Active Directory 连接信息。需要此连接，才能搜索 Active Directory 用户名和组并将其映射到 vCenter Server 中的角色和权限，而 AD FS 用于对用户进行身份验证。“配置主身份提供程序”向导的这一步不创建基于 LDAP 的 Active Directory 标识源。而是，vCenter Server 使用此信息建立与 Active Directory 域的有效可搜索连接，以便在其中查找用户和组。

例如，假设使用以下标识名条目：

- 用户的基本标识名：cn=Users,dc=corp,dc=local
- 组的基本标识名：dc=corp,dc=local
- 用户名：cn=Administrator,cn=Users,dc=corp,dc=local

如果 AdfsUser@corp.local 用户是 ADGroup@corp.local 组的成员，则在向导中输入此信息可允许 vCenter Server 管理员搜索和查找 ADGroup@corp.local 组，并将其添加到 vCenter Server Administrators@vsphere.local 组。因此，AdfsUser@corp.local 用户登录时，会向其授予 vCenter Server 中的管理特权。

在为 Active Directory 用户和组配置全局权限时，vCenter Server 也使用此搜索过程。无论是配置全局权限，还是添加用户或组，在这两种情况下，均可从域下拉菜单中选择为 AD FS 身份提供程序输入的域以进行搜索，然后从 Active Directory 域中选择用户和组。

使用可信根证书存储，而不使用 JRE 信任库

如果已在 vSphere 7.0 中将您自己的内部证书颁发机构颁发的根 CA 证书导入到 JRE 信任库，则从 vSphere 7.0 Update 1 开始，可以将该证书注册到可信根证书存储。

要在 vSphere 7.0 中使用您自己的内部证书颁发机构颁发的根 CA 证书配置 vCenter Server 身份提供程序联合，必须将其导入到 JRE 信任库。从 vSphere 7.0 Update 1 开始，可以将证书注册到可信根证书存储。此更改意味着应该将您自己的内部证书颁发机构颁发的根 CA 证书添加到可信根证书存储（也称为 VMware 端点证书存储或 VECS）。JRE 信任库中的证书仍正常运行，但 vCenter Server 将实现使用可信根证书存储标准化。

步骤

- 1 使用 vSphere Client 登录 vCenter Server。
- 2 导航到**管理 > 证书 > 证书管理**。
- 3 在**可信根证书**旁边，单击**添加**。
- 4 浏览 AD FS 根证书，然后单击**添加**。

证书将添加到**可信根证书**下的面板中。

为 AD FS 配置 vCenter Server 身份提供程序联合

安装或升级到 vSphere 7.0 或更高版本后，可以配置 vCenter Server 身份提供程序联合。

vCenter Server 仅支持配置一个外部身份提供程序（一个源）和 vsphere.local 标识源。不能使用多个外部身份提供程序。用户登录到 vCenter Server 时，vCenter Server 身份提供程序联合使用 OpenID Connect (OIDC)。

此任务介绍如何将 AD FS 组添加到 vSphere 管理员组，以便控制权限。此外，您还可以通过 vCenter Server 中的全局或对象权限使用 AD FS 授权配置特权。有关添加权限的详细信息，请参见《vSphere 安全性》文档。

小心 如果使用之前添加到 vCenter Server 的 Active Directory 标识源作为 AD FS 标识源，请不要从 vCenter Server 中删除该现有标识源。如果删除，会导致之前分配的角色和组成员资格出现回归问题。具有全局权限的 AD FS 用户和添加到管理员组的用户将无法登录。

解决办法：如果您不需要之前分配的角色和组成员资格，并且希望移除以前的 Active Directory 标识源，请在创建 AD FS 提供程序并在 vCenter Server 中配置组成员资格之前移除标识源。

前提条件

Active Directory 联合身份验证服务要求：

- 必须已经部署适用于 Windows Server 2016 或更高版本的 AD FS。
- AD FS 必须已连接到 Active Directory。
- 在配置过程中，必须在 AD FS 中创建 vCenter Server 的应用程序组。请参见 VMware 知识库文章，网址为 <https://kb.vmware.com/s/article/78029>。
- 已将 AD FS 根 CA 证书添加到可信根证书存储（也称为 VMware 证书存储）。
- 您已在 AD FS 中创建了一个 vCenter Server 管理员组，其中包含您要向其授予 vCenter Server 管理员特权的用户。

有关配置 AD FS 的详细信息，请参见 Microsoft 文档。

vCenter Server 和其他要求：

- vSphere 7.0 或更高版本
- vCenter Server 必须能够连接到 AD FS 发现端点，以及在发现端点元数据中通告的授权、令牌、注销、JWKS 和任何其他端点。

- 您需要 **VcIdentityProviders.管理** 特权，才能创建、更新或删除联合身份验证所需的 vCenter Server 身份提供程序。要限制用户只能查看身份提供程序配置信息，请分配 **VcIdentityProviders.读取** 特权。

步骤

- 1 使用 vSphere Client 登录 vCenter Server。
- 2 将 AD FS 根 CA 证书添加到可信根证书存储。
 - a 导航到**管理 > 证书 > 证书管理**。
 - b 在**可信根存储**旁边单击**添加**。
 - c 浏览 AD FS 根证书，然后单击**添加**。
证书将添加到**可信根证书**下的面板中。
- 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**身份提供程序**选项卡，然后获取重定向 URI。
 - a 单击“更改身份提供程序”链接旁边的信息性“i”图标。
此时将在弹出横幅中显示两个重定向 URI。
 - b 将这两个 URI 复制到一个文件中，或者将其记下来，供稍后在后续步骤中配置 AD FS 服务器时使用。
 - c 关闭弹出横幅。
- 5 在 AD FS 中创建 OpenID Connect 配置，并对其进行配置以用于 vCenter Server。

要在 vCenter Server 和身份提供程序之间建立依赖方信任，必须在它们之间建立标识信息和共享密钥。为此，在 AD FS 中，需要创建称为“应用程序组”的 OpenID Connect 配置，该配置由服务器应用程序和 Web API 组成。这两个组件指定 vCenter Server 用于信任和与 AD FS 服务器通信的信息。要在 AD FS 中启用 OpenID Connect，请参见 VMware 知识库文章，网址为 <https://kb.vmware.com/s/article/78029>。

在创建 AD FS 应用程序组时，请注意以下事项。

- 需要从上一步中获取和保存的两个重定向 URI。
- 将以下信息复制到文件中，或将其记下来，以供在下一步中配置 vCenter Server 身份提供程序时使用。
 - 客户端标识符
 - 共享密钥
 - AD FS 服务器的 OpenID 地址

6 在 vCenter Server 上创建身份提供程序。

a 返回 vSphere Client 中的**身份提供程序**选项卡。

b 单击“更改身份提供程序”链接。

此时将打开“配置主身份提供程序”向导。

c 选择 **Microsoft ADFS**，然后单击**下一步**。

在以下文本框中输入您之前收集的信息：

- 客户端标识符
- 共享密钥
- AD FS 服务器的 OpenID 地址

d 单击**下一步**。

e 输入基于 LDAP 的 Active Directory 连接的用户和组信息，以搜索用户和组。

vCenter Server 从用户的基本标识名中派生用于授权和权限的 AD 域。只能为此 AD 域中的用户和组添加对 vSphere 对象的权限。vCenter Server 身份提供程序联合不支持 AD 子域中或 AD 林中其他域中的用户或组。

选项	描述
用户的基本标识名	用户的基本识别名。
组的基本标识名	组的基本识别名。
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。
密码	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。
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。

f 单击**下一步**，查看信息，然后单击**完成**。

7 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**。

8 为 AD FS 授权配置组成员资格 vCenter Server。

- a 单击**组**选项卡。
- b 单击**管理员组**，然后单击**添加成员**。
- c 从下拉菜单中选择域。
- d 在下拉菜单下方的文本框中，输入要添加的 AD FS 组的前几个字符，然后等待下拉选项显示。
可能需要几秒钟时间才能显示所选内容，因为 vCenter Server 需要建立与 Active Directory 的连接并进行搜索。
- e 选择 AD FS 组，然后将其添加到管理员组。
- f 单击**保存**。

9 确认以 Active Directory 用户身份登录到 vCenter Server。

了解 vCenter Single Sign-On

如果不使用外部身份提供程序，则必须了解内置身份提供程序 vCenter Single Sign-On 的底层基础架构以及它如何影响安装和升级。

vCenter Single Sign-On 组件

vCenter Single Sign-On 包括 Security Token Service (STS)（管理服务器）、vCenter Lookup Service 和 VMware Directory Service (vmdir)。VMware Directory Service 还可用于证书管理。

在安装过程中，以下组件会作为 vCenter Server 部署的一部分进行部署。

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 Server 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 身份验证的交互式用户、脚本式用户和服务用户使用 vCenter Single Sign-On 支持的任何 vCenter 服务，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 Client 中的用户和组。最初，仅 `administrator@your_domain_name` 用户具有这些特权。可以在安装 vCenter Server 时更改 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 vCenter Server 部署中。此服务是一个多租户、对等复制目录服务，可使 LDAP 目录在端口 389 上可用。此外，还会存储和管理由 SHA-512 哈希算法保护的 vCenter Single Sign-On 用户帐户和密码。

如果您的环境包含在链接模式下配置的多个 vCenter Server 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。

VMware Directory Service 不仅会存储 vCenter Single Sign-On 信息，还会存储证书信息。

Identity Management Service

处理标识源和 STS 身份验证请求。

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 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。

可以向 vCenter Single Sign-On 进行身份验证的所有用户都可以重置其密码。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。

vCenter Single Sign-On 管理员用户

可从 vSphere 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。

其他用户帐户

以下用户帐户将在 vsphere.local 域（或在安装时创建的默认域）中的 vCenter Server 内自动创建。这些用户帐户是 shell 帐户。vCenter Single Sign-On 密码策略不适用于这些帐户。

表 4-1. 其他 vSphere 用户帐户

帐户	描述
K/M	用于 Kerberos 密钥管理。
krbtgt/VSPHERE.LOCAL	用于集成 Windows 身份验证兼容性。
waiter-random_string	用于 Auto Deploy。

ESXi 用户

独立的 ESXi 主机未与 vCenter Single Sign-On 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、ESXCLI 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 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。

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。将用户添加到其中一个组，以允许他们执行相应的操作。

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。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。

小心 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 4-2. 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	vCenter 服务的解决方案用户组。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	此组中的用户可以激活和停用对 BASH shell 的访问。默认情况下，使用 SSH 连接到 vCenter Server 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。
ExternalIDPUsers	vSphere 未使用此内部组。VMware vCloud Air 需要此组。

表 4-2. 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。
TrustedAdmins	此组的成员可以执行 VMware® vSphere Trust Authority™ 配置和管理任务。默认情况下，此组不包含任何成员。必须将成员添加到此组，才能执行 vSphere Trust Authority 任务。
AutoUpdate	此组在内部用于 vCenter Cloud Gateway。
SyncUsers	此组在内部用于 vCenter Cloud Gateway。
vsphereClientSolutionUsers	此组在内部用于 vSphere Client。
ServiceProviderUsers	此组的成员可以管理 vSphere with Tanzu 和 VMware Cloud on AWS 基础架构。
NsxAdministrators	此组用于 VMware NSX。
WorkloadStorage	工作负载存储组。
RegistryAdministrators	此组的成员可以管理注册表。
NsxAuditors	此组用于 VMware NSX。
NsxViAdministrators	此组用于 VMware NSX。
SystemConfiguration.SupportUsers	SystemConfiguration.SupportUsers 组的成员可以访问支持包 API。
SystemConfiguration.ReadOnly	此组的成员可以访问 vCenter Server Appliance 只读操作。

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。

注 在 vSphere 7.0 Update 2 及更高版本中，可以在 vCenter Server 上启用 FIPS。请参见《vSphere 安全性》文档。启用 FIPS 后，不支持基于 LDAP 的 AD 和 IWA。请在 FIPS 模式下使用外部身份提供程序联合。请参见[配置 vCenter Server 身份提供程序联合](#)。

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。安装后，每个 vCenter Single Sign-On 实例都具有标识源 *your_domain_name*，例如 vsphere.local。此标识源是 vCenter Single Sign-On 的内部标识源。

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才能成功进行身份验证。域名格式为：

```
DOMAIN\user
```

以下标识源可用。

- Active Directory over LDAP。vCenter Single Sign-On 支持多个 Active Directory over LDAP 标识源。
- Active Directory（集成 Windows 身份验证）版本 2003 及更高版本。vCenter Single Sign-On 允许将单个 Active Directory 域指定为一个标识源。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。
- OpenLDAP 版本 2.4 及更高版本。vCenter Single Sign-On 支持多个 OpenLDAP 标识源。

注 未来对 Microsoft Windows 进行的更新将更改 Active Directory 的默认行为，以要求强身份验证和加密。此更改将影响 vCenter Server 对 Active Directory 进行身份验证的方式。如果使用 Active Directory 作为 vCenter Server 的标识源，则必须计划启用 LDAPS。有关此 Microsoft 安全更新的详细信息，请参见 <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023> 和 <https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html>。

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 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 在**身份提供程序**选项卡下，单击**标识源**，选择一个标识源，然后单击**设置为默认值**。
- 5 单击**确定**。

在域显示屏幕中，默认域显示在“类型”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。

标识源可以是基于 LDAP 的 Active Directory、本机 Active Directory（集成 Windows 身份验证）域，也可以是 OpenLDAP 目录服务。请参见 [vCenter Server](#) 和 [vCenter Single Sign-On](#) 的标识源。

在安装后，便能够立即使用 vsphere.local 域（或安装期间指定的域）与 vCenter Single Sign-On 内部用户。

注 如果已更新或替换 Active Directory SSL 证书，则必须在 vCenter Server 中移除并重新添加标识源。

前提条件

如果要添加 Active Directory（集成 Windows 身份验证）标识源，则 vCenter Server 必须位于 Active Directory 域中。请参见[将 vCenter Server 添加到 Active Directory 域](#)。

步骤

- 1 使用 vSphere Client 登录 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 在**身份提供程序**选项卡下，单击**标识源**，然后单击**添加**。
- 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	此选项需要您指定域控制器和其他信息。请参见 基于 LDAP 的 Active Directory 和 OpenLDAP 服务器标识源设置 。
OpenLDAP	对于 OpenLDAP 标识源，请使用此选项。请参见 基于 LDAP 的 Active Directory 和 OpenLDAP 服务器标识源设置 。

注 如果用户帐户已锁定或停用，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

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。

基于 LDAP 的 Active Directory 和 OpenLDAP 服务器标识源设置

基于 LDAP 的 Active Directory 标识源优先于 Active Directory（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。

注 未来对 Microsoft Windows 进行的更新将更改 Active Directory 的默认行为，以要求强身份验证和加密。此更改将影响 vCenter Server 对 Active Directory 进行身份验证的方式。如果使用 Active Directory 作为 vCenter Server 的标识源，则必须计划启用 LDAPS。有关此 Microsoft 安全更新的详细信息，请参见 <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023> 和 <https://blogs.vmware.com/vsphere/2020/01/microsoft-ldap-vsphere-channel-binding-signing-adv190023.html>。

表 4-3. 基于 LDAP 的 Active Directory 和 OpenLDAP 服务器设置

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。输入要从中开始用户搜索的 DN。例如，cn=Users,dc=myCorp,dc=com。
组的基本 DN	组的基本标识名。输入从中开始组搜索的 DN。例如，cn=Groups,dc=myCorp,dc=com。
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。ID 可以采用以下任何格式： <ul style="list-style-type: none"> ■ UPN (user@domain.com) ■ NetBIOS (DOMAIN\user) ■ DN (cn=user,cn=Users,dc=domain,dc=com) 用户名必须为完全限定的名称。“user”条目不起作用。
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。

表 4-3. 基于 LDAP 的 Active Directory 和 OpenLDAP 服务器设置（续）

选项	描述
主服务器 URL	域的主域控制器 LDAP 服务器。可以使用主机名或 IP 地址。 请使用 <code>ldap://hostname_or_IPaddress:port</code> 或 <code>ldaps://hostname_or_IPaddress:port</code> 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 <code>ldaps://</code> 时，需要油一个证书才能为 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。可以使用主机名或 IP 地址。
SSL 证书	如果要与 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。要从 Active Directory 中导出根 CA 证书，请参阅 Microsoft 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（集成 Windows 身份验证）标识源的必备条件

仅当 Active Directory（集成 Windows 身份验证）标识源可用时，才能将 vCenter Single Sign-On 设置为使用该标识源。请按照《vCenter Server 配置》文档中的说明执行操作。

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。

如果在 Active Directory 中启用诊断事件日志记录以确定可能需要强化的位置，则可能会在该目录服务器上看到事件 ID 为 2889 的日志事件。在使用集成 Windows 身份验证时，事件 ID 2889 作为异常（而不是安全风险）生成。有关事件 ID 2889 的详细信息，请参见 VMware 知识库文章，网址为 <https://kb.vmware.com/s/article/78644>。

表 4-4. 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。
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 命令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。

使用 CLI 添加或移除标识源

您可以使用 sso-config 实用程序添加或移除标识源。

标识源可以是本机 Active Directory（集成 Windows 身份验证）域、AD over LDAP、使用 LDAPS (LDAP over SSL) 的 AD over LDAP，也可以是 OpenLDAP。请参见 [vCenter Server](#) 和 [vCenter Single Sign-On](#) 的标识源。还可以使用 sso-config 实用程序设置智能卡和 RSA SecurID 身份验证。

前提条件

如果要添加 Active Directory 标识源，则 vCenter Server 必须位于 Active Directory 域中。请参见将 [vCenter Server](#) 添加到 [Active Directory](#) 域。

启用 SSH 登录。请参见使用 [vCenter Server Shell](#) 管理 [vCenter Server](#)。

步骤

- 1 在 vCenter Server 系统上，使用 SSH 或其他远程控制台连接启动会话。
- 2 以 root 用户身份登录。
- 3 更改到 sso-config 实用程序所在的目录。

```
cd /opt/vmware/bin
```

- 4 要参考 sso-config 帮助，请运行 sso-config.sh -help，或者参见 VMware 知识库文章（网址为 <https://kb.vmware.com/s/article/67304>），获得用法示例。

vCenter Single Sign-On 使用 Windows 会话身份验证

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

前提条件

- 将 vCenter Server 加入 Active Directory 域。请参见[将 vCenter Server 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>。
- 验证是否已安装增强身份验证插件。请参见《vCenter Server 安装和设置》。

注 将 vCenter Server 配置为对 Active Directory 联合身份验证服务使用联合身份验证时，增强型身份验证插件仅适用于配置，其中 vCenter Server 是身份提供程序（基于 LDAP 的 Active Directory、集成 Windows 身份验证和 OpenLDAP 配置）。

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。

管理 vCenter Server Security Token Service

vCenter Server Security Token Service (STS) 是一项发布、验证和续订安全令牌的 Web 服务。

作为令牌颁发者，Security Token Service (STS) 使用私钥对令牌进行签名，并发布公用证书供服务验证令牌签名。vCenter Server 管理 STS 签名证书并将其存储在 VMware Directory Service (vmdir) 中。令牌的生存期可能很长，长期以来可能已由多个密钥中的任何一个进行签名。

要获取令牌，用户须向 STS 接口提供其主凭据。主凭据取决于用户类型。

表 4-5. STS 用户和凭据

用户类型	主凭据
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。

默认情况下，VMware Certificate Authority (VMCA) 会生成 STS 签名证书。您可以使用新的 VMCA 证书刷新 STS 签名证书。您还可以导入默认 STS 签名证书并将其替换为自定义或第三方生成的 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。

您可以使用 vSphere Client 执行以下操作：

- 刷新 STS 证书
- 导入并替换自定义和第三方生成的 STS 证书
- 查看 STS 证书详细信息，例如过期日期

您还可以使用命令行替换自定义和第三方生成的 STS 证书。

STS 证书持续时间和过期

全新安装 vSphere 7.0 Update 1 和更高版本将创建持续时间为 10 年的 STS 签名证书。当 STS 签名证书即将过期时，将从 90 天开始发出警报向您警告，每周发送一次，然后还剩七天时每天发送一次。

注 在某些情况下，替换 STS 签名证书可能会更改证书的持续时间。执行证书替换时，请注意颁发日期和过期日期。

STS 证书自动续订

从 vSphere 8.0 开始，vCenter Single Sign-On 会自动续订 VMCA 生成的 STS 签名证书。自动续订发生在 STS 签名证书过期之前，以及触发 90 天过期警报之前。如果自动续订失败，vCenter Single Sign-On 会在日志文件中创建一条错误消息。如有必要，您可以手动刷新 STS 签名证书。

注 vCenter Single Sign-On 不会自动续订自定义生成的或第三方 STS 签名证书。

刷新和导入和替换 STS 证书

从 8.0 开始，刷新或导入和替换 STS 签名证书不需要重新启动 vCenter Server，因此可避免任何停机。此外，在链接配置中，刷新或导入和替换单个 vCenter Server 上的 STS 签名证书会更新所有链接的 vCenter Server 系统上的 STS 证书。

注 在某些情况下，刷新或导入和替换 STS 签名证书可能需要手动重新启动 vCenter Server 系统。

使用 vSphere Client 刷新 vCenter Server STS 证书

可以使用 vSphere Client 刷新 vCenter Server STS 签名证书。VMware Certificate Authority (VMCA) 颁发新证书并替换当前证书。

刷新 STS 签名证书时，VMware Certificate Authority (VMCA) 会颁发新证书，并替换 VMware Directory Service (vmdir) 中的当前证书。STS 开始使用新证书颁发新令牌。在增强型链接模式配置中，vmdir 会将新证书从颁发 vCenter Server 系统上载到链接的所有 vCenter Server 系统。刷新 STS 签名证书时，无需重新启动 vCenter Server 系统，也无需重新启动增强型链接模式配置中的任何其他 vCenter Server 系统。

如果使用自定义生成的 STS 签名证书或第三方 STS 签名证书，则刷新操作会使用 VMCA 颁发的证书覆盖该证书。要更新自定义生成的或第三方 STS 签名证书，请使用导入和替换选项。请参见[使用 vSphere Client 导入并替换 vCenter Server STS 证书](#)。

VMCA 颁发的 STS 签名证书的有效期为 10 年且不面向外部。除非贵公司的安全策略需要，否则请勿替换此证书。

前提条件

对于证书管理，您必须提供本地域管理员的密码（默认为 administrator@vsphere.local）。如果要续订证书，还必须为在 vCenter Server 系统上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 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 如果系统出现提示，请输入 vCenter Server 的凭据。
- 5 在 STS 签名证书下，单击操作 > 使用 vCenter 证书刷新。

如果使用自定义生成的 STS 签名证书或第三方 STS 签名证书，则刷新操作会使用 VMCA 生成的证书覆盖该证书。

注 如果出于合规性原因而使用第三方证书，刷新可能会导致您的 vCenter Server 系统不合规。此外，如果使用自定义生成的 STS 签名证书或第三方 STS 签名证书，则 Security Token Service 不再将该自定义证书或第三方证书用于令牌签名。

- 6 单击刷新。

此时 VMCA 会刷新此 vCenter Server 系统以及链接的任何 vCenter Server 系统上的 STS 签名证书。

- 7 （可选）如果显示强制刷新按钮，表明 vCenter Single Sign-On 检测到问题。单击强制刷新之前，请考虑以下潜在结果。
 - 如果所有受影响的 vCenter Server 系统均未至少运行 vSphere 7.0 Update 3，则不支持证书刷新。
 - 选择强制刷新要求重新启动所有 vCenter Server 系统，并且可能会致使这些系统在重新启动之前无法正常运行。
 - a 如果不确定影响，请单击取消并研究您的环境。
 - b 如果确定影响，请单击强制刷新继续刷新，然后手动重新启动 vCenter Server 系统。

使用 vSphere Client 导入并替换 vCenter Server STS 证书

可以使用 vSphere Client 导入并将 vCenter Server STS 证书替换为自定义生成的证书或第三方证书。

要导入并替换默认 STS 签名证书，必须先生成新证书。导入和替换 STS 签名证书时，VMware Directory Service (vmdir) 会将新证书从颁发 vCenter Server 系统上载到链接的所有 vCenter Server 系统。

STS 证书不面向外部。除非贵公司的安全策略需要，否则请勿替换此证书。

前提条件

对于证书管理，您必须提供本地域管理员的密码（默认为 `administrator@vsphere.local`）。还必须为在 vCenter Single Sign-On 系统上具有管理员特权的用户提供 vCenter Server 凭据。

步骤

- 1 使用 vSphere Client 登录 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 如果系统出现提示，请输入 vCenter Server 的凭据。
- 5 在 **STS 签名证书** 下，单击**操作 > 导入并替换**。
- 6 选择 PEM 文件。

PEM 文件包括签名证书链和私钥。
- 7 单击**替换**。

将在此 vCenter Server 系统和链接的任何 vCenter Server 系统上替换 STS 签名证书。除非另有说明，否则无需重新启动 vCenter Server 系统。

使用命令行替换 vCenter Server STS 证书

可以使用 CLI 将 vCenter Server STS 证书替换为自定义生成的证书或第三方证书。

要使用公司所需的证书或刷新即将过期的证书，可以替换现有 STS 签名证书。要替换默认 STS 签名证书，必须先生成新证书。

STS 证书不面向外部。除非贵公司的安全策略需要，否则请勿替换此证书。

小心 您必须使用此处所述的过程。请勿直接替换文件系统中的证书。

前提条件

启用 SSH，以通过 SSH 登录到 vCenter Server。请参见[使用 vCenter Server Shell 管理 vCenter Server](#)。

步骤

- 1 以 root 身份登录 vCenter Server Shell。
- 2 创建证书。
 - a 创建顶级目录以保存新证书并确认该目录的位置。

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

- b 将 certtool.cfg 文件复制到新目录中。

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

- c 使用诸如 Vim 等命令行编辑器，打开 certtool.cfg 文件的副本并进行编辑，以便使用本地 vCenter Server 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
```

- d 生成密钥。

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

- e 生成证书。

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

- f 创建带有证书链和私钥的 PEM 文件。

```
cat newsts.cer /var/lib/vmware/vmca/root.cer sts.key > newsts.pem
```

3 更新 STS 签名证书，例如：

```
/opt/vmware/bin/sso-config.sh -set_signing_cert -t vsphere.local /root/newsts/newsts.pem
```

此时 VMCA 会刷新此 vCenter Server 系统以及链接的任何 vCenter Server 系统上的 STS 签名证书。

使用 vSphere Client 查看活动的 vCenter Server STS 签名证书链

您可以使用 vSphere Client 查看活动的 vCenter Server STS 签名证书链。

您可以查看有关活动 STS 证书的以下信息。

- “有效期至”日期
- 表示证书有效的绿色对勾和表示证书过期的橙色对勾警告
- 用于显示活动证书链的[查看详细信息](#)链接

步骤

- 1 使用 vSphere Client 登录 vCenter Server。
- 2 输入至少具有读取特权的用户的用户名和密码。
- 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 如果系统出现提示，请输入 vCenter Server 的凭据。
- 5 要查看活动 STS 证书的详细信息，请单击[查看详细信息](#)。

使用命令行确定 LDAPS SSL 证书的过期日期

使用基于 LDAPS 的 Active Directory 时，可以上载适用于 LDAP 流量的 SSL 证书。SSL 证书在预定义的使用期限之后过期。可以使用 `sso-config.sh` 命令查看证书的过期日期，以便知悉要在证书过期之前将其替换或续订。

当活动 LDAP SSL 证书接近过期日期时，vCenter Server 系统会发出警示。

只有使用基于 LDAP 的 Active Directory 或 OpenLDAP 标识源并为服务器指定 `ldaps://` URL 时，才可查看证书过期信息。

前提条件

启用 SSH，以通过 SSH 登录到 vCenter Server。请参见[使用 vCenter Server Shell 管理 vCenter Server](#)。

步骤

- 1 以 root 身份登录到 vCenter Server。

2 运行下列命令。

```
/opt/vmware/bin/sso-config.sh -get_identity_sources
```

忽略 SLF4J 消息。

3 要确定过期日期，请查看 SSL 证书的详细信息并验证 NotAfter 字段。

管理 vCenter Single Sign-On 策略

vCenter Single Sign-On 策略通常会强制实施本地帐户和令牌的安全规则。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) 中的用户。

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

请参见更改 [vCenter Single Sign-On 密码](#)。

注 管理员帐户 (administrator@vsphere.local) 不会被锁定，它的密码也不会过期。正确的安全做法是审核此帐户的登录名，并定期轮换密码。

步骤

- 1 使用 vSphere Client 登录 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 单击本地帐户选项卡。
- 5 单击密码策略行对应的编辑。
- 6 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。

选项	描述
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。
字符要求	<p>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：</p> <ul style="list-style-type: none"> ■ 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 ■ 相同的相邻字符数：该值必须大于 0。例如，如果输入 1，则不允许使用以下密码：p@\$\$word. <p>字母字符最小数目不得小于大写和小写字符的总和。</p> <p>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。</p>

7 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 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**本地帐户**选项卡。

- 5 单击**锁定策略**行对应的**编辑**。

可能需要向下滚动才能看到**锁定策略**行。

6 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。

7 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 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 单击本地帐户选项卡。
- 5 单击令牌的可信度行对应的编辑。

可能需要向下滚动才能看到令牌的可信度行。

- 6 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。

选项	描述
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。

7 单击保存。

编辑 Active Directory（集成 Windows 身份验证）用户的密码过期通知

Active Directory 密码过期通知与 vCenter ServerSSO 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 可控制过期通知。您可以更改默认过期通知以满足您公司的安全标准。

前提条件

- 启用 SSH，以通过 SSH 登录到 vCenter Server。请参见[使用 vCenter Server Shell 管理 vCenter Server](#)。

步骤

- 1 以具有管理员特权的用户身份登录到 vCenter Server shell。
具有超级管理员角色的默认用户是 root。
- 2 将目录更改为 vSphere Clientwebclient.properties 文件所在的位置。

```
cd /etc/vmware/vsphere-ui
```

- 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 vSphere Client。

```
service-control --stop vsphere-ui
service-control --start vsphere-ui
```

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。

vSphere Client 会显示 vSphere 域（默认情况下为 vsphere.local）中的用户和组的视图。在此视图中，您可以添加、编辑和停用用户。您还可以添加组并管理组成员资格。

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 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**。
- 6 输入新用户的用户名和密码。
用户名最多包含 300 个字符。
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**。

结果

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](#)。

停用和激活 vCenter Single Sign-On 用户

停用 vCenter Single Sign-On 用户帐户后，除非管理员激活该帐户，否则用户无法登录到 vCenter Single Sign-On 服务器。您可以从其中一个 vCenter Single Sign-On 管理界面停用和激活帐户。

停用的用户帐户在 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 Server 的**用户和组**页面中停用和激活帐户。

前提条件

您必须是 vCenter Single Sign-On 管理员组的成员才能停用和激活 vCenter Single Sign-On 用户。

步骤

- 1 使用 vSphere Client 登录 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 选择用户名，单击**更多**，然后单击**禁用**。
- 5 单击**确定**。
- 6 要再次激活用户，请单击**更多**，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 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。
- 6 单击**删除**。

请谨慎执行后续操作。您无法撤消此操作。
- 7 单击**移除**。

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 > 本地帐户 > 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 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 选择用户，然后单击**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**保存**。

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 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**。
- 5 输入组的名称和描述。

组名称最多包含 300 个字符。创建组后，将不能更改组名称。
- 6 从**添加成员**下拉菜单中，选择包含要添加到组的成员的标识源。

如果配置了外部身份提供程序（如 AD FS），则可以在**添加成员**下拉菜单中选择该身份提供程序的域。
- 7 输入搜索词。
- 8 选择成员。

您可添加多个成员。
- 9 单击**添加**。

后续步骤

请参见向 [vCenter Single Sign-On 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 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 从**添加成员**下拉菜单中，选择包含要添加到组的成员的标识源。

如果配置了外部身份提供程序（如 AD FS），则可以在**添加成员**下拉菜单中选择该身份提供程序的域。

- 6 输入搜索词。

- 7 选择成员。

您可添加多个成员。

- 8 单击**保存**。

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 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**。

结果

用户将从组中移除，但在系统中仍然可用。

更改 vCenter Single Sign-On 密码

本地域（默认为 vsphere.local）中的用户可以从 vSphere Client 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 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 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，单击您的用户名以弹出下拉菜单，然后选择**更改密码**。
- 4 输入当前密码。
- 5 输入新密码并确认。

该密码必须符合密码策略。

- 6 单击**确认**。

或者，也可以选择 **Single Sign On > 用户和组**，选择用户，然后单击**编辑**。

了解其他 vSphere 身份验证选项

在 vSphere 7.0 及更高版本中，外部身份提供程序联合是 vCenter Server 的首选身份验证方法。您仍然可以通过使用 Windows 会话身份验证 (SSPI)、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。

外部身份提供程序联合

通过外部身份提供程序联合，您可以使用外部身份提供程序支持的身份验证机制，包括多因素身份验证。

智能卡身份验证

智能卡身份验证仅允许在所登录的计算机上接入了物理卡读取器的用户进行访问。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 vCenter Server 已配置为指向 RSA 服务器，并且如果已激活 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 vCenter Server 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。设置包括激活智能卡身份验证和配置证书吊销策略。
- 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 vCenter Server 身份验证方法

可以使用 `sso-config` 分别激活或停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。

注 在 vSphere 7.0 Update 2 及更高版本中，可以在 vCenter Server 上启用 FIPS。请参见《vSphere 安全性》文档。启用 FIPS 后，不支持 RSA SecureID 和 CAC 身份验证。使用外部身份提供程序联合进行 MFA 身份验证。请参见[配置 vCenter Server 身份提供程序联合](#)。

系统将提示登录到 vCenter Server 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，浏览器将读取卡上的证书。
- 2 浏览器提示用户选择证书，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。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 如果证书为 vCenter Single Sign-On 已知且未被吊销，则用户通过身份验证，可以执行该用户有权执行的任务。

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，停用用户名和密码身份验证并激活智能卡身份验证。随后，vSphere 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 vCenter Server 来重新激活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当用户从 vCenter Server 连接到 vSphere Client 时需要智能卡身份验证。

配置智能卡身份验证需要先设置反向代理，然后再启用并配置智能卡身份验证本身。可以使用 sso-config 实用程序管理智能卡身份验证。

配置反向代理以请求客户端证书

激活智能卡身份验证之前，必须在 vCenter Server 系统上配置反向代理。

vSphere 6.5 及更高版本需要配置反向代理。

配置使用端口 3128，该端口自动进行设置和打开。

前提条件

将证书颁发机构 (CA) 证书复制到 vCenter Server 系统。

注 vCenter Server 7.0 支持 HTTP/2 协议。所有现代浏览器和应用程序（包括 vSphere Client）都使用 HTTP/2 连接到 vCenter Server。但是，智能卡身份验证需要使用 HTTP/1.1 协议。激活智能卡身份验证将对 HTTP/2 取消激活应用程序层协议协商 (ALPN, <https://tools.ietf.org/html/rfc7301>)，从而有效阻止浏览器使用 HTTP/2。仅使用 HTTP/2 而不依赖 ALPN 的应用程序将继续工作。

步骤

- 1 以 root 用户身份登录设备 vCenter Server shell。
- 2 创建可信客户端 CA 存储。

此存储包含 CA 颁发的用于客户端证书的可信证书。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 vCenter Server 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
```

- 3 备份包含反向代理定义的 /etc/vmware-rhttpproxy/config.xml 文件，然后在编辑器中打开 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 STS 服务。

```
service-control --restart sts
```

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。

可以在以下位置找到 sso-config 脚本：

```
/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 vCenter Server 实例之间复制。

如果停用了用户名和密码身份验证，并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 vCenter Server 命令行打开用户名和密码身份验证。以下命令可激活用户名和密码身份验证。

```
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，请改为使用 CRL（证书吊销列表）。

前提条件

- 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“扩展密钥用法”字段中指定“客户端身份验证”，否则浏览器将不显示证书。
- 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。
- 确保已设置反向代理并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。

- 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 vCenter Server 上的 /usr/lib/vmware-sso/vmware-sts/conf。
- d (可选) 停用 Shell，如下所示。

```
chsh -s "/bin/appliancesh" root
```

- 2 要启用智能卡身份验证，请运行以下命令。

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

例如：

```
sso-config.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 要停用所有其他身份验证方法，请运行以下命令。

```
sso-config.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) 要设置证书策略允许列表，请运行以下命令。

```
sso-config.sh -set_authn_policy -certPolicies policies
```

要指定多个策略，请用逗号进行分隔，例如：

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

此允许列表指定证书的证书策略扩展中所允许策略的对象 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.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.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.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.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.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.sh -get_authn_policy -t tenantName
```

使用 vSphere Client 管理智能卡身份验证

可以从 vSphere Client 启用和停用智能卡身份验证、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停用了其他身份验证方法，则用户必须使用智能卡身份验证进行登录。

如果停用了用户名和密码身份验证，并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 vCenter Server 命令行打开用户名和密码身份验证。以下命令可激活用户名和密码身份验证。

```
sso-config.sh -set_authn_policy -pwdAuthn true -t tenant_name
```

前提条件

- 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“扩展密钥用法”字段中指定“客户端身份验证”，否则浏览器将不显示证书。
- 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。
- 确保已设置反向代理并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。

- a 直接或者使用 SSH 登录到 vCenter Server 控制台。
- b 停用 Shell，如下所示。

```
shell
chsh -s "/bin/bash" root
chsh -s "bin/appliance/sh" root
```

- c 使用 WinSCP 或类似实用程序将证书复制到 vCenter Server 上的 /usr/lib/vmware-sso/vmware-sts/conf 目录。
- d (可选) 停用设备 Shell，如下所示。

```
chsh -s "/bin/appliancesh" root
```

- 2 使用 vSphere Client 登录 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**身份提供程序**选项卡下，单击**智能卡身份验证**，然后单击**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。您无法从此 Web 界面激活或停用 RSA SecurID 身份验证。但是，如果已通过命令行启用了 RSA SecurID，状态将显示在 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 vCenter Server 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。

- 如果已停用吊销检查，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。
- 如果已激活吊销检查，则设置取决于 PKI 设置。

仅 OCSP

如果发证 CA 支持 OCSP 响应者，则激活 **OCSP** 并停用 **CRL** 作为 OCSP 的故障切换。

仅 CRL

如果发证 CA 不支持 OCSP，则激活 **CRL 检查**并停用 **OCSP 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，请同时激活 **OCSP 检查**和 **CRL 检查**，并停用 **CRL** 作为 OCSP 的故障切换。

- 如果已激活吊销检查，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，请停用此选项。

CRL 位置

如果停用**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“扩展密钥用法”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 vCenter Server 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。

步骤

- 1 使用 vSphere Client 登录 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 在**身份提供程序**选项卡下，单击**智能卡身份验证**。
- 5 单击**证书吊销**，然后单击**编辑**以激活或停用吊销检查。
- 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 vCenter Server 主机名，以及 vCenter Server 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。要查找 sdconf.rec 文件，请解压缩生成的 AM_Config.zip 文件。
- 将 sdconf.rec 文件复制到 vCenter Server 节点。

步骤

- 1 更改到 sso-config 脚本所在的目录。

```
/opt/vmware/bin
```

- 2 要激活 RSA SecurID 身份验证，请运行以下命令。

```
sso-config.sh -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）要停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 -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 实例或集群。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 <code>sdconf.rec</code> 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 -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。（仅支持基于 LDAP 的 Active Directory 标识源。）

`userID` 属性确定哪个 LDAP 属性用作 RSA `userID`。

```
sso-config.sh -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
```

结果

如果停用了用户名和密码身份验证并激活了 RSA 身份验证，则用户必须使用其用户名和 RSA 令牌登录。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 vSphere Client 登录页面的登录消息

可以创建在 vSphere Client 登录页面上显示的消息。

您可以设置消息、免责声明或条款和条件。此外，还可以将消息配置为要求在登录之前确认消息。

管理 vSphere Client 登录页面的登录消息

可以在 vSphere Client 登录页面中添加登录消息。还可以配置自定义登录消息，并提供用户同意复选框。

步骤

- 1 使用 vSphere Client 登录 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。
“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**。

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，请遵循这些 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。

配置网络时间协议

使用网络时间协议 (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。

有关使用 NTP 配置时间同步的说明，请参见《vSphere 安全性》文档。

对 vCenter Server 身份验证进行故障排除

5

以下主题提供对 vCenter Server 身份验证问题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 Directory Service 复制需要较长时间
- 导出 vCenter Server 支持包
- vCenter Server 身份验证服务日志参考

确定 Lookup Service 错误的原因

vCenter Single Sign-On 安装显示有关 vCenter Server 或 vSphere 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
<code>java.net.ConnectException: Connection timed out: connect</code>	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。
<code>java.net.ConnectException: Connection refused: connect</code>	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 vmware-ss0 守护进程的状态，验证 vCenter Single Sign-On 是否运行正常。 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。
<code>Unexpected status code: 404. SSO Server failed during initialization</code>	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 <code>Could not connect to vCenter Single Sign-On 开头</code>	您还会看到返回码 <code>SslHandshakeFailed</code> 。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 <code>VM_ssoreg.log</code> 中，找到包含以下消息的行。 <code>host name in certificate did not match: <install-configured FQDN or IP> != <A> or or <C></code> ，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 <code>!=</code> 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 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`）。

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。

如果更改默认标识源无法解决此问题，请执行以下额外的故障排除步骤。

- 1 同步 vCenter Server 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 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，然后重新加入域。请参见《vCenter Server 配置》文档。
- 4 关闭连接到 vCenter Server 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 登录页面登录 vCenter Server 时，出现指示帐户被锁定的错误。

问题

多次尝试均失败后，将无法使用 vCenter Single Sign-On 登录到 vSphere 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 Directory Service 复制需要较长时间

如果环境中包括多个通过增强型链接模式连接的 vCenter Server 实例，其中一个 vCenter Server 实例不可用时，环境仍会继续运行。该 vCenter Server 再次可用时，通常会使用通过增强型链接模式连接的合作伙伴在 30 秒内复制用户数据和其他信息。但是，在某些情况下，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 vCenter Server 实例，并在某个 vCenter Server 实例不可用时进行重大更改，则无法立即查看 VMware Directory Service 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 vCenter Server 实例的新用户。复制可能需要较长时间，具体取决于增强型链接模式拓扑。

原因

在正常操作期间，在一个 vCenter Server 实例（节点）上对 VMware Directory Service (vmdir) 实例所做的更改大约会在 30 秒内显示在其直接复制合作伙伴中。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 vCenter Server 支持包

可以从 vSphere Client 或使用 API 导出包含 vCenter Server 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。

有关 API 的详细信息，请参见《vCenter Server 管理编程指南》。

前提条件

确认 vCenter Server 已成功部署和运行。

步骤

- 1 在 Web 浏览器中，输入 `https://vCenter Server vcenter_server_ip:5480` 连接至配置管理界面。
- 2 以 vCenter Server 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。

vCenter Server 身份验证服务日志参考

vCenter Server 身份验证服务使用 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. vCenter Server 身份验证服务日志

服务	描述
VMware Directory Service	默认情况下，vmdir 日志记录在 <code>/var/log/messages</code> 或 <code>/var/log/vmware/vmmdir/</code> 中。 对于部署时的问题， <code>/var/log/vmware/vmdir/vmafdvmdirclient.log</code> 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 <code>/var/log/vmware/sso/</code> 中。
VMware Certificate Authority (VMCA)	VMCA 服务日志位于 <code>/var/log/vmware/vmca/vmca-syslog.log</code> 。
VMware Endpoint Certificate Store (VECS)	VECS 服务日志位于 <code>/var/log/vmware/vmafd/vmafd-syslog.log</code> 。
VMware Lookup Service	查找服务日志位于 <code>/var/log/vmware/sso/lookupServer.log</code> 。