

vSphere 安全性

Update 2

修改日期：2022 年 4 月 27 日

VMware vSphere 6.0

VMware ESXi 6.0

vCenter Server 6.0

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 © 2009-2022 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

目录

关于 vSphere 安全性 13

更新信息 15

1 vSphere 环境中的安全性 17

确保 ESXi 虚拟化管理程序安全 17

确保 vCenter Server 系统及关联服务安全 19

确保虚拟机安全 20

确保虚拟网络连接层安全 20

vSphere 环境中的密码 22

安全性最佳做法与资源 23

2 使用 vCenter Single Sign-On 进行 vSphere 身份验证 24

了解 vCenter Single Sign-On 25

如何使用 vCenter Single Sign-On 保护您的环境 25

vCenter Single Sign-On 组件 27

vCenter Single Sign-On 如何影响安装 28

vCenter Single Sign-On 如何影响升级 28

通过 vSphere 使用 vCenter Single Sign-On 30

vsphere.local 域中的组 32

vCenter Server 密码要求和锁定行为 33

配置 vCenter Single Sign-On 标识源 34

vCenter Server 和 vCenter Single Sign-On 的标识源 35

设置 vCenter Single Sign-On 的默认域 36

添加 vCenter Single Sign-On 标识源 36

Active Directory 标识源设置 38

Active Directory LDAP Server 和 OpenLDAP Server 标识源设置 39

编辑 vCenter Single Sign-On 标识源 40

删除 vCenter Single Sign-On 标识源 40

vCenter Single Sign-On 使用 Windows 会话身份验证 41

vCenter Server 双因素身份验证 41

为 vCenter Single Sign-On 配置智能卡身份验证 42

使用命令行配置智能卡身份验证 43

使用 Platform Services Controller Web 界面管理智能卡身份验证 46

设置智能卡身份验证的吊销策略 49

设置 RSA SecurID 身份验证 50

管理登录横幅 52

将 vCenter Single Sign-On 用作其他服务提供程序的身份提供程序	53
添加 SAML 服务提供程序	53
安全令牌服务 (STS)	55
在设备上生成新的 STS 签名证书	55
在 Windows 上安装 vCenter 时生成新的 STS 签名证书	57
刷新安全令牌服务证书	58
确定 LDAPS SSL 证书的过期日期	59
管理 vCenter Single Sign-On 策略	60
编辑 vCenter Single Sign-On 密码策略	60
编辑 vCenter Single Sign-On 锁定策略	61
编辑 vCenter Single Sign-On 令牌策略	62
管理 vCenter Single Sign-On 用户和组	62
添加 vCenter Single Sign-On 用户	63
禁用和启用 vCenter Single Sign-On 用户	64
删除 vCenter Single Sign-On 用户	64
编辑 vCenter Single Sign-On 用户	65
添加 vCenter Single Sign-On 组	65
向 vCenter Single Sign-On 组添加成员	66
从 vCenter Single Sign-On 组中移除成员	67
删除 vCenter Single Sign-On 解决方案用户	67
更改 vCenter Single Sign-On 密码	68
vCenter Single Sign-On 安全性最佳做法	68
对 vCenter Single Sign-On 进行故障排除	69
确定 Lookup Service 错误的原因	69
无法使用 Active Directory 域身份验证进行登录	70
由于用户帐户被锁定，vCenter Server 登录失败	72
VMware Directory Service 复制需要较长时间	72

3 vSphere 安全证书 73

不同解决方案途径的证书要求	74
证书管理概览	77
证书替换概述	79
vSphere 6.0 用户证书的位置	81
VMCA 和 VMware 核心标识服务	83
VMware Endpoint 证书存储概述	83
管理证书吊销	85
大型部署中的证书替换	85
使用 Platform Services Controller Web 界面管理证书	87
从 Platform Services Controller Web 界面浏览证书存储	87
从 Platform Services Controller Web 界面将证书替换为新的 VMCA 签名证书	88
通过 Platform Services Controller Web 界面将 VMCA 设为中间证书颁发机构	90

从 Platform Services Controller 将系统设置为使用自定义证书	91
使用 vSphere 证书管理器生成证书签名请求（自定义证书）	92
将可信根证书添加到证书存储	93
从 Platform Services Controller 添加自定义证书	93
使用 vSphere 证书管理器实用程序管理证书	94
通过重新发布旧证书恢复上次执行的操作	95
重置所有证书	96
重新生成新的 VMCA 根证书并替换所有证书	96
将 VMCA 设为中间证书颁发机构（证书管理器）	97
使用 vSphere 证书管理器生成 CSR 并准备 root 证书（中间 CA）	97
将 VMCA 根证书替换为自定义签名证书并替换所有证书	98
将计算机 SSL 证书替换为 VMCA 证书（中间 CA）	99
将解决方案用户证书替换为 VMCA 证书（中间 CA）	100
将所有证书替换为自定义证书（证书管理器）	101
使用 vSphere 证书管理器生成证书签名请求（自定义证书）	101
将计算机 SSL 证书替换为自定义证书	102
将解决方案用户证书替换为自定义证书	103
手动证书替换	105
了解启动和停止服务	105
将现有 VMCA 签名证书替换为新的 VMCA 签名证书	105
生成新的 VMCA 签名根证书	106
将计算机 SSL 证书替换为 VMCA 签名证书	108
将解决方案用户证书替换为新的 VMCA 签名证书	111
在混合模式环境中替换 VMware Directory Service 证书	116
使用 VMCA 作为中间证书颁发结构	116
替换根证书（中间 CA）	117
替换计算机 SSL 证书（中间 CA）	119
替换解决方案用户证书（中间 CA）	122
替换 VMware Directory Service 证书	128
在混合模式环境中替换 VMware Directory Service 证书	129
在 vSphere 中使用第三方证书	130
请求证书并导入自定义根证书	130
将计算机 SSL 证书替换为自定义证书	132
将解决方案用户证书替换为自定义证书	134
替换 VMware Directory Service 证书	135
在混合模式环境中替换 VMware Directory Service 证书	136
通过 CLI 命令管理证书和服务	137
证书管理操作所需的特权	138
更改 certool 配置	139
certool 初始化命令参考	140
certool 管理命令参考	142

vecs-cli 命令参考 145

dir-cli 命令参考 148

通过 vSphere Web Client 查看 vCenter 证书 153

为 vCenter 证书过期警告设置阈值 153

4 vSphere 权限和用户管理任务 154

了解 vSphere 中的授权 155

了解 vCenter Server 权限模型 155

权限的层次结构继承 157

多项权限设置 159

示例 1: 继承多个权限 160

示例 2: 子权限替代父权限 160

示例 3: 用户角色替代组角色 161

管理 vCenter 组件的权限 161

将权限添加到清单对象 162

更改权限 163

移除权限 163

更改权限验证设置 163

全局权限 164

添加全局权限 164

标记对象的权限 165

使用角色分配特权 166

vCenter Server 系统角色 168

创建自定义角色 168

克隆角色 169

编辑角色 169

角色和权限的最佳做法 170

常见任务的所需特权 170

5 确保 ESXi 主机安全 173

使用脚本管理主机配置设置 174

使用主机配置文件配置 ESXi 主机 175

常规 ESXi 安全建议 176

ESXi 密码和帐户锁定 177

ESXi 网络连接安全建议 179

禁用 Managed Object Browser (MOB) 179

禁用授权 (SSH) 密钥 179

ESXi 主机的证书管理 180

主机升级和证书 182

ESXi 证书默认设置 183

查看多个 ESXi 主机的证书过期信息 184

- 查看单个 ESXi 主机的证书详细信息 184
- 续订或刷新 ESXi 证书 185
- 更改证书默认设置 186
- 了解证书模式切换 186
- 更改证书模式 188
- 替换 ESXi SSL 证书和密钥 188
 - ESXi 证书签名请求的要求 189
 - 从 ESXi Shell 替换默认证书和密钥 189
 - 通过 vifs 命令替换默认证书和密钥 190
 - 通过 HTTPS PUT 替换默认证书 191
 - 更新 vCenter Server TRUSTED_ROOTS 存储（自定义证书） 192
- 在 Auto Deploy 中使用自定义证书 192
- 还原 ESXi 证书和密钥文件 194
- 使用安全配置文件自定义主机 195
 - ESXi 防火墙配置 195
 - 管理 ESXi 防火墙设置 195
 - 为 ESXi 主机添加允许的 IP 地址 196
 - ESXi 主机的入站和出站防火墙端口 197
 - NFS 客户端防火墙行为 199
 - ESXi ESXCLI 防火墙命令 200
 - 从安全配置文件自定义 ESXi 服务 200
 - 在安全配置文件中启用或禁用服务 201
 - 锁定模式 202
 - 锁定模式行为 204
 - 使用 vSphere Web Client 启用锁定模式 205
 - 使用 vSphere Web Client 禁用锁定模式 205
 - 从直接控制台用户界面启用或禁用正常锁定模式 206
 - 指定在锁定模式下拥有访问特权的帐户 206
 - 检查主机和 VIB 的接受程度 208
- 为 ESXi 分配权限 209
 - root 用户特权 210
 - vpxuser 特权 210
 - dcui 用户特权 211
- 使用 Active Directory 管理 ESXi 用户 211
 - 安装或升级 vSphere Authentication Proxy 211
 - 配置主机以使用 Active Directory 212
 - 将主机添加到目录服务域 213
 - 查看目录服务设置 214
- 使用 vSphere Authentication Proxy 214
 - 安装或升级 vSphere Authentication Proxy 214
 - 配置主机以使用 vSphere Authentication Proxy 进行身份验证 216

- 设置 vSphere Authentication Proxy 217
 - 导出 vSphere Authentication Proxy 证书 217
 - 将 Proxy 服务器证书导入 ESXi 217
 - 使用 vSphere Authentication Proxy 将主机添加到域 218
 - 替换 ESXi 主机的 Authentication Proxy 证书 219
- ESXi 安全性最佳做法 219
 - PCI 和 PCIe 设备和 ESXi 220
- 配置 ESXi 的智能卡身份验证 220
 - 启用智能卡身份验证 221
 - 禁用智能卡身份验证 221
 - 如果出现连接问题, 对用户凭据进行身份验证 222
 - 在锁定模式下使用智能卡身份验证 222
- ESXi SSH 密钥 222
 - SSH 安全 222
 - 使用 vifs 命令上载 SSH 密钥 223
 - 使用 HTTPS PUT 上载 SSH 密钥 223
- 使用 ESXi Shell 224
 - 使用 vSphere Web Client 启用对 ESXi Shell 的访问 225
 - 在 vSphere Web Client 中为 ESXi Shell 可用性创建超时 226
 - 在 vSphere Web Client 中为闲置的 ESXi Shell 会话创建超时 226
 - 使用直接控制台用户界面 (DCUI) 启用对 ESXi Shell 的访问 227
 - 在直接控制台用户界面中为 ESXi Shell 可用性创建超时 227
 - 为闲置 ESXi Shell 会话创建超时 228
 - 登录 ESXi Shell 以进行故障排除 228
- 修改 ESXi Web 代理设置 228
- vSphere Auto Deploy 安全注意事项 229
- 管理 ESXi 日志文件 230
 - 在 ESXi 主机上配置 Syslog 230
 - ESXi 日志文件地址 231
 - 确保 Fault Tolerance 日志记录通信的安全 232

6 确保 vCenter Server 系统安全 233

- vCenter Server 安全性最佳做法 233
 - vCenter Server 访问控制的最佳做法 233
 - 设置 vCenter Server 密码策略 235
 - 保护 vCenter Server Windows 主机 235
 - 从失败的安装中移除过期和撤销的证书和日志 235
 - 限制 vCenter Server 网络连接 236
 - 考虑限制 Linux 客户端的使用 236
 - 检查已安装的插件 237
 - vCenter Server Appliance 安全性最佳做法 237

- 验证旧版 ESXi 主机的指纹 237
- 验证“对网络文件复制的 SSL 证书验证”是否已启用 238
- vCenter Server TCP 和 UDP 端口 239
- 控制基于 CIM 的硬件监控工具访问 240

7 确保虚拟机安全 242

- 限制信息性消息从虚拟机流向 VMX 文件 242
- 防止虚拟磁盘压缩 243
- 虚拟机安全性最佳做法 243
 - 虚拟机常规保护 244
 - 使用模板来部署虚拟机 244
 - 尽量少用虚拟机控制台 245
 - 防止虚拟机取代资源 245
 - 禁用虚拟机中不必要的功能 245
 - 移除不必要的硬件设备 246
 - 禁用未使用的显示功能 246
 - 禁用未公开的功能 247
 - 禁用 HGFS 文件传输 248
 - 禁用客户机操作系统和远程控制台之间的复制和粘贴操作 248
 - 限制公开复制到剪贴板中的敏感数据 249
 - 限制用户在虚拟机中运行命令 249
 - 阻止虚拟机用户或进程与设备断开连接 250
 - 修改客户机操作系统的可变内存限制 250
 - 阻止客户机操作系统进程向主机发送配置消息 251
 - 避免使用独立非持久磁盘 251

8 确保 vSphere 网络安全 252

- vSphere 网络安全简介 252
- 使用防火墙确保网络安全 253
 - 针对有 vCenter Server 的配置设立防火墙 254
 - 通过防火墙连接到 vCenter Server 254
 - 针对没有 vCenter Server 的配置设立防火墙 255
 - 通过防火墙连接 ESXi 主机 255
 - 通过防火墙连接到虚拟机控制台 255
- 确保物理交换机安全 256
- 使用安全策略确保标准交换机端口安全 256
- 确保 vSphere 标准交换机的安全 257
 - MAC 地址更改 258
 - 伪传输 258
 - 混杂模式运行 258
- 确保 vSphere Distributed Switch 和分布式端口组的安全 258

- 通过 VLAN 确保虚拟机安全 259
 - VLAN 安全注意事项 260
 - 确保 VLAN 安全 261
- 在单台 ESXi 主机上创建网络 DMZ 261
- 在单台 ESXi 主机中创建多个网络 263
- Internet 协议安全 264
 - 列出可用的安全关联 265
 - 添加 IPsec 安全关联 265
 - 移除 IPsec 安全关联 266
 - 列出可用的 IPsec 安全策略 266
 - 创建 IPsec 安全策略 266
 - 移除 IPsec 安全策略 268
- 确保 SNMP 配置正确 268
- 仅在需要时才在 vSphere Network Appliance API 中使用虚拟交换机 268
- vSphere 网络连接安全性最佳做法 269
 - 常规网络连接安全建议 269
 - 标记网络组件 270
 - 记录和检查 vSphere VLAN 环境 270
 - 采用可靠的网络隔离做法 271

9 涉及多个 vSphere 组件的最佳做法 273

- 同步 vSphere 网络连接上的时钟 273
 - 使 ESXi 时钟与网络时间服务器同步 273
 - 在 vCenter Server Appliance 中配置时间同步设置 274
 - 使用 VMware Tools 时间同步 274
 - 在 vCenter Server Appliance 配置中添加或替换 NTP 服务器 275
 - 将 vCenter Server Appliance 中的时间与 NTP 服务器同步 276
- 存储安全性最佳做法 276
 - 确保 iSCSI 存储器安全 276
 - 确保 iSCSI 设备安全 277
 - 保护 iSCSI SAN 277
 - 屏蔽 SAN 资源并对其进行分区 278
 - 对 NFS 4.1 使用 Kerberos 凭据 278
- 验证是否已禁止向客户机发送主机性能数据 278
- 为 ESXi Shell 和 vSphere Web Client 设置超时 279

10 使用 TLS 重新配置实用程序管理 TLS 协议配置 280

- 支持禁用 TLS 版本的端口 280
- 在 vSphere 中禁用 TLS 版本 282
- 安装 TLS 配置实用程序 282
- 执行可选手动备份 283

- 禁用 vCenter Server 系统上的 TLS 版本 285
- 禁用 ESXi 主机上的 TLS 版本 285
- 在 Platform Services Controller 系统上禁用 TLS 版本 287
- 恢复 TLS 配置更改 288
- 在 vSphere Update Manager 上禁用 TLS 版本 290
 - 为 Update Manager 端口 9087 禁用早期 TLS 版本 290
 - 为 Update Manager 端口 8084 禁用早期 TLS 版本 291
 - 为 Update Manager 端口 9087 重新启用已禁用的 TLS 版本 292
 - 为 Update Manager 端口 8084 重新启用已禁用的 TLS 版本 292

11 定义的特权 294

- 警报特权 295
- Auto Deploy 和镜像配置文件特权 296
- 证书特权 297
- 内容库特权 297
- 数据中心特权 299
- 数据存储特权 299
- 数据存储集群特权 300
- Distributed Switch 特权 300
- ESX Agent Manager 特权 301
- 扩展特权 302
- 文件夹特权 302
- 全局特权 302
- 主机 CIM 特权 303
- 主机配置特权 304
- 主机清单 305
- 主机本地操作特权 305
- 主机 vSphere Replication 特权 306
- 主机配置文件特权 306
- Inventory Service 提供商特权 307
- Inventory Service 标记特权 307
- 网络特权 308
- 性能特权 308
- 权限特权 309
- 配置文件驱动的存储特权 309
- 资源特权 309
- 已调度任务特权 310
- 会话特权 311
- 存储视图特权 311
- 任务特权 311
- Transfer Service 特权 312

VRM 策略特权	312
虚拟机配置特权	312
虚拟机客户机操作特权	313
虚拟机交互特权	314
虚拟机清单特权	319
虚拟机置备特权	320
虚拟机服务配置特权	321
虚拟机快照管理特权	321
虚拟机 vSphere Replication 特权	322
dvPort 组特权	322
vApp 特权	323
vServices 特权	324

关于 vSphere 安全性

《vSphere 安全性》提供了有关确保 VMware® vCenter® Server 和 VMware ESXi 的 vSphere® 环境安全的信息。

为了帮助保护 vSphere 环境，本文档介绍了可用的安全功能，以及可采取的保护该环境免受攻击的措施。

为了帮助保护 vSphere 环境，本文档介绍了可用的安全功能，以及可采取的保护该环境免受攻击的措施。

表 1-1. 《vSphere 安全性》内容要点

主题	内容要点
使用 vCenter Single Sign-On 身份验证	<ul style="list-style-type: none">■ vCenter Single Sign-On 功能和服务。■ 添加和管理标识源。■ vCenter Single Sign-On 策略。■ 用户和组。
权限和用户管理	<ul style="list-style-type: none">■ 权限模型（角色、组、对象）。■ 创建自定义角色。■ 设置权限。■ 管理全局权限。
证书管理	<ul style="list-style-type: none">■ ESXi 证书管理■ vCenter Server 和相关服务的证书管理。<ul style="list-style-type: none">■ 使用 UI 管理证书。■ 使用 Certificate Manager 实用程序管理证书。■ 使用 CLI 手动管理证书（包括示例）。
主机安全功能	<ul style="list-style-type: none">■ 锁定模式和其他安全配置文件功能。■ 主机智能卡身份验证。■ vSphere Authentication Proxy。
安全性最佳做法与强化	<p>最佳做法和 VMware 安全专家的建议。</p> <ul style="list-style-type: none">■ vCenter Server 安全。■ 主机安全。■ 虚拟机安全。■ 网络安全。
vSphere 特权	此版本中支持的所有 vSphere 特权的完整列表。

相关文档

除本文档外，VMware 还针对每个版本的 vSphere 发布了《强化指南》，网址为：<http://www.vmware.com/security/hardening-guides.html>。强化指南是包含了不同潜在安全问题条目的电子表格。它包括三个不同风险配置文件的项目。本《vSphere 安全性》文档不包括风险配置文件 1（安全性最高的环境，如绝密政府机构）的信息。

目标读者

本信息的目标读者为熟悉虚拟机技术和数据中心操作且具有丰富经验的 Windows 或 Linux 系统管理员。

更新信息

本《《vSphere 安全性》》文档随产品的每个版本更新或在必要时更新。

下表提供了《《vSphere 安全性》》文档的更新历史记录。

修订版本	描述
2022 年 4 月 27 日	■ 对存储视图特权进行了微小更新。
2021 年 11 月 05 日	■ 对 ESXi 安全性最佳做法 进行了微小更新。 ■ 更正了禁用 ESXi 主机上的 TLS 版本 ，说明您应登录到 vCenter Server。
2020 年 8 月 14 日	VMware 非常重视包容性。为了在我们的客户、合作伙伴和内部社区中促进此原则的实施，我们正着手替换文档内容中的一些术语。我们更新了本指南，移除了非包容性语言的实例。 ■ 对 确保虚拟机安全 进行了微小更新。
2017 年 10 月 4 日	■ 在 了解证书模式切换 中，说明将主机置于维护模式和断开主机连接可以执行模式切换。不需要移除主机。
ZH_CN-001949-07	■ 添加了详细介绍证书要求的新主题 不同解决方案途径的证书要求 。移除了包含较少详细信息的旧主题。 ■ 添加了新章节第 10 章 使用 TLS 重新配置实用程序管理 TLS 协议配置 。
ZH_CN-001949-06	■ 更新了 使用命令行配置智能卡身份验证 ，明确说明不允许在以逗号分隔的证书列表中使用空格。 ■ 在 使用命令行配置智能卡身份验证 中包含了脚本位置。 ■ 在 将解决方案用户证书替换为自定义证书 中阐明了需要完整的证书链。 ■ 解决了 多项权限设置简介 中的问题。
ZH_CN-001949-05	■ 更改权限验证设置 中添加了有关验证和验证周期的信息。
ZH_CN-001949-04	■ 验证“对网络文件复制的 SSL 证书验证”是否已启用 中修复了参数名称错误。 ■ 通过 CLI 命令管理证书和服务 中添加了有关 Windows 上 service-control 命令位置的信息。
ZH_CN-001949-03	■ 标记对象的权限 中添加了有关标记权限的信息。 ■ 使用 vSphere 证书管理器生成 CSR 并准备 root 证书（中间 CA） 中阐明了证书顺序。
ZH_CN-001949-02	■ 第 2 章 使用 vCenter Single Sign-On 进行 vSphere 身份验证 中添加了有关使用 vSphere Client 登录的说明。 ■ Active Directory 标识源设置 中阐明了某些信息。必须将系统加入到 Active Directory 名称，且域名必须可通过 DNS 解析。

修订版本	描述
ZH_CN-001949-01	<ul style="list-style-type: none"> ■ 使用 vSphere 证书管理器生成 CSR 并准备 root 证书（中间 CA）中更正了证书顺序。 ■ 更新了 ESXi 密码和帐户锁定。默认情况下不启用密码短语。 ■ 使用命令行配置智能卡身份验证中更正了访问设备 shell 的步骤。 ■ 更改 vCenter Single Sign-On 密码 中进行了修复。如果您的密码已过期，则必须与管理员联系。 ■ 使用脚本管理主机配置设置中更新了 PowerCLI 脚本。 ■ 更新了 vCenter Single Sign-On 如何影响安装 中 vCenter Server 实例的数量的信息。 ■ 使用命令行配置智能卡身份验证、使用 Platform Services Controller Web 界面管理智能卡身份验证和设置 RSA SecurID 身份验证进行了若干更新。 ■ vCenter Server TCP 和 UDP 端口进行了若干更正。例如，端口 903 和端口 5900-5964 在主机上使用，但不在 vCenter Server 系统上使用，其他一些端口（例如 9090）仅在内部使用。 ■ 移除了使用 vifs 命令上载 SSH 密钥中有关 DSA 密钥的信息。 ■ 更新了安全令牌服务 (STS)，添加了生成新 STS 签名证书的过程。
ZH_CN-001949-00	初始版本。

vSphere 环境中的安全性

1

通过证书、授权、每个 ESXi 上的防火墙、受限访问等大量功能，vSphere 环境的组件开箱即可确保安全。您可以通过多种方式修改默认设置 - 例如，可以在 vCenter 对象上设置权限、打开防火墙端口或更改默认证书。这将在确保 vCenter Server 系统、ESXi 主机和虚拟机安全方面实现最大的灵活性。

您也可以关注 vSphere 各领域的高级别概述，这有助于您规划安全策略。也可以从 VMware 网站的其他 vSphere 安全资源中获取帮助。

本章讨论了以下主题：

- 确保 ESXi 虚拟化管理程序安全
- 确保 vCenter Server 系统及关联服务安全
- 确保虚拟机安全
- 确保虚拟网络连接层安全
- vSphere 环境中的密码
- 安全性最佳做法与资源

确保 ESXi 虚拟化管理程序安全

ESXi 虚拟化管理程序开箱时即受到安全保护。通过使用锁定模式和其他内置的功能，可以进一步保护 ESXi 主机。如果设置引用主机并基于该主机的主机配置文件对所有主机进行更改，或如果执行脚本式管理，则确保将更改应用到所有主机可进一步保护您的环境。

使用本指南中详细介绍的以下功能，可增强对 vCenter Server 管理的 ESXi 主机的保护。另请参见《VMware vSphere Hypervisor 的安全性》白皮书。

限制 ESXi 访问

默认情况下，ESXi Shell 和 SSH 服务不会运行，只有 root 用户才能登录到直接控制台用户界面 (DCUI)。如果决定启用 ESXi 或 SSH 访问，则可以设置超时以限制未经授权的访问风险。

可以访问 ESXi 主机的用户必须具有管理主机的权限。您可以在管理主机的 vCenter Server 中设置对主机对象的权限。

使用指定用户和最小特权

默认情况下，root 用户可以执行许多任务。您可以从 vCenter Server 权限管理界面将不同的主机配置特权应用于不同的指定用户，而不是允许管理员使用 root 用户帐户登录到 ESXi 主机。您可以在

vSphere Web Client 中创建自定义角色、将特权分配给该角色，并将该角色与指定用户和 ESXi 主机对象关联。

在单个主机方案中，您可以直接管理用户。请参见《使用 vSphere Client 管理 vSphere》文档。

尽可能减少打开的 ESXi 防火墙端口数

默认情况下，只有启动相应的服务时，才会打开 ESXi 主机上的防火墙端口。可以使用 vSphere Web Client 或 ESXCLI 或 PowerCLI 命令检查和管理防火墙端口状态。

请参见 [ESXi 防火墙配置](#)。

自动化 ESXi 主机管理

由于使同一数据中心内的不同主机保持同步通常十分重要，因此请使用脚本式安装或 vSphere Auto Deploy 置备主机。您可以使用脚本管理主机。除脚本式管理之外，还可以使用主机配置文件。您可以设置引用主机、导出主机配置文件并将主机配置文件应用到主机。可以直接应用主机配置文件，也可以在使用 Auto Deploy 置备时应用主机配置文件。

有关 vSphere Auto Deploy 的信息，请参见[使用脚本管理主机配置设置](#)和《vSphere 安装和设置》。

使用锁定模式

在锁定模式下，默认只能通过 vCenter Server 访问 ESXi 主机。从 vSphere 6.0 开始，您可以选择严格锁定模式或正常锁定模式，且可以定义异常用户以允许直接访问服务帐户（如备份代理）。

请参见[锁定模式](#)。

检查 VIB 软件包完整性

每个 VIB 软件包均有关联的接受程度。只有在接受程度与主机的接受程度相同或更高时，才能将 VIB 添加到 ESXi 主机。除非明确更改主机的接受程度，否则无法将 CommunitySupported 或 PartnerSupported VIB 添加到主机。

请参见[检查主机和 VIB 的接受程度](#)。

管理 ESXi 证书

在 vSphere 6.0 及更高版本中，默认情况下，VMware 证书颁发机构 (VMCA) 将使用以 VMCA 作为根证书颁发机构的签名证书置备每个 ESXi 主机。如果公司策略有相关要求，则可以将现有证书替换为第三方 CA 签名的证书。

请参见 [ESXi 主机的证书管理](#)

智能卡身份验证

从 vSphere 6.0 开始，ESXi 提供了智能卡身份验证选项，而不是用户名和密码身份验证。

请参见配置 [ESXi 的智能卡身份验证](#)。

ESXi 帐户锁定

从 vSphere 6.0 开始，系统将支持对通过 SSH 和通过 vSphere Web Services SDK 进行的访问进行帐户锁定。直接控制台界面 (DCUI) 和 ESXi Shell 不支持帐户锁定。默认情况下，允许最多 10 次尝试，当这些尝试均失败后，才会锁定帐户。默认情况下，帐户将在两分钟后解锁。

请参见 [ESXi 密码和帐户锁定](#)。

各独立主机需要考虑的安全注意事项相似，尽管管理任务可能有所不同。请参见《使用 vSphere Client 管理 vSphere》文档。

确保 vCenter Server 系统及关联服务安全

通过 vCenter Single Sign-On 进行身份验证和通过 vCenter Server 权限模型进行授权可保护 vCenter Server 系统及关联服务。您可以修改默认行为，且可以采取其他措施来保护对环境的访问。

在保护 vSphere 环境时，请考虑必须保护与 vCenter Server 实例关联的所有服务。在某些环境中，您可以保护多个 vCenter Server 实例及一个或多个 Platform Services Controller 实例。

强化对所有 vCenter 主机的保护

保护 vCenter 环境的第一步是强化对运行 vCenter Server 或关联服务的每台计算机的保护。物理机或虚拟机需要考虑类似的注意事项。始终为操作系统安装最新的安全修补程序，并遵循行业标准最佳做法以保护主机。

了解 vCenter 证书模型

默认情况下，VMware Certificate Authority 将为每个 ESXi 主机、环境中的每台计算机以及每个解决方案用户置备 VMCA 签名的证书。环境可以即装即用，但如果公司策略需要，则可以更改默认行为。请参见第 3 章 [vSphere 安全证书](#)。

如需其他保护，请务必明确移除过期和撤销的证书以及失败的安装。

配置 vCenter Single Sign-On

vCenter Single Sign-On 身份验证框架可保护 vCenter Server 和关联服务。首次安装该软件时，请指定 administrator@vsphere.local 用户的密码，且只能将该域作为标识源。您可以添加其他标识源（Active Directory 或 LDAP），并设置默认标识源。从今往后，凡是能够向标识源进行身份验证的用户均可以查看对象并执行任务（如果其拥有相关权限）。请参见第 2 章 [使用 vCenter Single Sign-On 进行 vSphere 身份验证](#)。

向用户或组分配角色

为了实现更好的日志记录，请将授予给对象的每个权限与指定用户或组以及预定义角色或自定义角色相关联。vSphere 6.0 权限模型提供了较大的灵活性，允许通过多种方式授权用户或组。请参见 [了解 vSphere 中的授权和常见任务的所需特权](#)。

务必限制管理员特权及管理员角色的使用。如果可能，请不要使用匿名管理员用户。

设置 NTP

为环境中的每个节点设置 NTP。证书基础架构需要准确的时间戳，如果节点不同步，则证书基础架构将无法正常运行。

请参见 [同步 vSphere 网络连接上的时钟](#)。

确保虚拟机安全

要确保虚拟机安全，请保持修补客户机操作系统并保护您的环境，就像保护物理机一样。请考虑禁用不必要的功能，尽量少用虚拟机控制台并遵循其他最佳做法。

保护客户机操作系统

要保护客户机操作系统，请确保其使用最新的修补程序及（如果适用）反间谍软件和反恶意软件应用程序。请参见客户机操作系统供应商提供的文档以及（如果可能）手册中或 [Internet](#) 上提供的有关该操作系统的其他信息。

禁用不必要的功能

检查是否已禁用不必要的功能，以最大限度地减少潜在攻击点。默认情况下，不经常使用的许多功能处于禁用状态。移除不必要的硬件并禁用某些功能（如主机客户机文件系统 (HFSG)），或在虚拟机和远程控制台之间进行复制和粘贴操作。

请参见[禁用虚拟机中不必要的功能](#)。

使用模板和本式管理

通过虚拟机模板，您可以设置操作系统以使其符合您的要求，并使用相同的设置创建其他虚拟机。

如果要在初始部署后更改虚拟机设置，请考虑使用脚本（如 [PowerCLI](#)）。本文档介绍了如何使用 GUI 执行任务。请考虑使用脚本而非 GUI 来保持环境的一致性。在大型环境中，您可以将虚拟机分组到文件夹以优化脚本。

有关模板的信息，请参见[使用模板来部署虚拟机](#)和《vSphere 虚拟机管理》。有关 [PowerCLI](#) 的信息，请参见 [VMware PowerCLI 文档](#)。

尽量少用虚拟机控制台

虚拟机控制台为虚拟机提供的功能与物理服务器上的监视器相同。具有虚拟机控制台访问权限的用户可以访问虚拟机电源管理和可移除的设备连接控制。因此，虚拟机控制台访问权限可能会造成对虚拟机的恶意攻击。

确保虚拟网络连接层安全

虚拟网络连接层包括虚拟网络适配器、虚拟交换机、分布式虚拟交换机及端口和端口组。ESXi 依赖虚拟网络连接层来支持虚拟机与其用户之间的通信。此外，ESXi 可使用虚拟网络连接层与 iSCSI SAN 和 NAS 存储器等进行通信。

vSphere 包括安全网络基础架构所需的全套功能。您可以单独确保基础架构中每个元素（如虚拟交换机、分布式虚拟交换机和虚拟网络适配器等）的安全。此外，请考虑以下准则，这些准则将在[第 8 章 确保 vSphere 网络安全](#)中进行更详细的介绍。

隔离网络流量

网络流量隔离对保护 ESXi 环境安全至关重要。不同的网络需要不同的访问权限和隔离级别。管理网络将客户端流量、命令行界面 (CLI) 或 API 流量，以及第三方软件流量与正常流量隔离。此网络应仅供系统、网络和安全管理员访问。

请参见 [ESXi 网络连接安全建议](#)。

使用防火墙确保虚拟网络元素的安全

您可以打开和关闭防火墙端口，并单独确保虚拟网络中每个元素的安全。防火墙规则可将服务与相应的防火墙关联，并可以根据服务的状态打开和关闭 ESXi 防火墙。

请参见 [ESXi 防火墙配置](#)。

考虑网络安全策略

网络安全策略可保护流量免受 MAC 地址模拟和有害端口扫描的威胁。在网络协议堆栈的第 2 层（数据链路层）执行标准交换机或 Distributed Switch 的安全策略。安全策略的三大要素是混杂模式、MAC 地址更改和伪信号。

有关说明，请参见《vSphere 网络连接》文档。

确保虚拟机网络安全

可确保虚拟机网络安全的方法取决于所安装的客户机操作系统、虚拟机是否运行于可信环境及各种其他因素。与其他常见安全措施（例如，安装防火墙）结合使用时，虚拟交换机和分布式虚拟交换机的保护作用会大大增强。

请参见第 8 章 [确保 vSphere 网络安全](#)。

考虑使用 VLAN 保护您的环境

ESXi 支持可用于为虚拟机网络或存储器配置提供进一步保护的 IEEE 802.1q VLAN。通过 VLAN，可对物理网络进行分段，以便使同一物理网络中的两台计算机无法互相收发数据包，除非它们位于同一 VLAN 上。

请参见[通过 VLAN 确保虚拟机安全](#)。

确保虚拟化存储连接的安全

虚拟机可在虚拟磁盘上存储操作系统文件、程序文件以及其他数据。从虚拟机的角度而言，每个虚拟磁盘看上去都好像是与 SCSI 控制器连接的 SCSI 驱动器。虚拟机与存储详细信息隔离，且无法访问有关其虚拟磁盘所在的 LUN 的信息。

虚拟机文件系统 (VMFS) 是向 ESXi 主机提供虚拟卷的分布式文件系统和卷管理器。您必须确保存储连接的安全。例如，如果使用 iSCSI 存储器，则可以将您的环境设置为使用 CHAP；如果公司策略需要，则可通过 vSphere Web Client 或 CLI 设置为使用双向 CHAP。

请参见 [存储安全性最佳做法](#)。

评估 IPsec 的使用

ESXi 支持 IPv6 上的 IPsec。不能使用 IPv4 上的 IPsec。

请参见 [Internet 协议安全](#)。

此外，请评估 VMware NSX for vSphere 是否是确保环境中网络连接层安全的有效解决方案。

vSphere 环境中的密码

vSphere 环境中的密码限制、锁定和过期取决于用户的目标系统、用户身份以及策略设置。

ESXi 密码

ESXi 密码限制由 Linux PAM 模块 `pam_passwdqc` 确定。请参见 [ESXi 密码和帐户锁定](#)。

vCenter Server 及其他 vCenter 服务的密码

vCenter Single Sign-On 管理登录到 vCenter Server 及其他 vCenter 服务的所有用户的身份验证。密码限制、锁定和过期取决于用户的域以及用户身份。

administrator@vsphere.local

如果在安装期间选择了不同域，则 `administrator@vsphere.local` 用户或 `administrator@mydomain` 用户的密码不会过期，并且不受锁定策略限制。在所有其他情况下，密码必须遵循 vCenter Single Sign-On 密码策略中设置的限制。请参见 [编辑 vCenter Single Sign-On 密码策略](#)。

如果忘记此类用户的密码，请搜索 VMware 知识库系统，了解有关重置密码的信息。

其他 vsphere.local 用户

其他 `vsphere.local` 用户或您在安装期间指定的本地域用户的密码必须遵循由 vCenter Single Sign-On 密码策略和锁定策略设置的限制。请参见 [编辑 vCenter Single Sign-On 密码策略](#) 和 [编辑 vCenter Single Sign-On 锁定策略](#)。默认情况下，这些密码将在 90 天后过期，但是根据密码策略管理员可以更改过期时间。

如果用户忘记其 `vsphere.local` 密码，管理员用户可以使用 `dir-cli` 命令重置密码。

其他用户

所有其他用户的密码限制、锁定和过期由用户对其进行身份验证的域（标识源）决定。

vCenter Single Sign-On 支持默认标识源，用户可以仅使用其用户名登录到 vSphere Client。域可确定密码参数。如果用户希望以非默认域中的用户身份登录，用户可以包括该域名，即，指定 `user@domain` 或 `domain\user`。在这种情况下，域密码参数也适用。

vCenter Server Appliance 直接控制台用户界面用户的密码

vCenter Server Appliance 是基于 Linux 的预配置虚拟机，针对在 Linux 上运行 vCenter Server 及关联服务进行了优化。

部署 vCenter Server Appliance 时，为设备 Linux 操作系统的 `root` 用户指定密码，并为 `administrator@vsphere.local` 用户指定密码。可以从直接控制台用户界面更改 `root` 用户密码并执行其他 vCenter Server Appliance 本地用户管理任务。请参见《vCenter Server Appliance 配置》。

安全性最佳做法与资源

如果您按照最佳做法进行操作，ESXi 和 vCenter Server 可以与不包含虚拟化的环境一样安全，安全性甚至更高。

本手册包括 vSphere 基础架构的不同组件的最佳做法。

表 1-1. 安全性最佳做法

vSphere 组件	资源
ESXi 主机	ESXi 安全性最佳做法
vCenter Server 系统	vCenter Server 安全性最佳做法
虚拟机	虚拟机安全性最佳做法
vSphere 网络	vSphere 网络连接安全性最佳做法

本手册只是确保环境安全所需的其中一种资源。

VMware 安全资源（包括安全警示和下载）通过 Web 提供。

表 1-2. Web 上的 VMware 安全资源

主题	资源
VMware 安全策略、最新安全警示、安全下载及安全主题重点讨论。	http://www.vmware.com/go/security
公司安全响应策略	http://www.vmware.com/support/policies/security_response.html VMware 致力于帮助维护安全的环境。安全问题是需要及时更正的。 VMware 安全响应策略中作出了解决其产品中可能存在的漏洞之承诺。
第三方软件支持策略	http://www.vmware.com/support/policies/ VMware 支持各种存储系统和软件代理（如备份代理及系统管理代理等）。 可以通过在 http://www.vmware.com/vmtn/resources/ 上搜索 ESXi 兼容性指南，找到支持 ESXi 的代理、工具及其他软件的列表。 VMware 不可能对此行业中的所有产品和配置进行测试。如果 VMware 未在兼容性指南中列出某种产品或配置，其技术支持人员将尝试帮助解决任何相关问题，但不能保证该产品或配置的可用性。请始终对不受支持的产品或配置进行安全风险评估。
合规性和安全标准，以及关于虚拟化和合规性的合作伙伴解决方案和深入内容	http://www.vmware.com/go/compliance
针对于不同 vSphere 组件版本的安全认证和验证（如 CCEVS 和 FIPS）的相关信息。	https://www.vmware.com/support/support-resources/certifications.html
不同 vSphere 版本和其他 VMware 产品的强化指南。	https://www.vmware.com/support/support-resources/hardening-guides.html
《VMware vSphere Hypervisor 的安全性》白皮书	http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf

使用 vCenter Single Sign-On 进行 vSphere 身份验证

2

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

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

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

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

在用户能够使用 vCenter Single Sign-On 进行身份验证之后，您可以授权该用户执行特定任务。在大多数情况下，您可以分配 vCenter Server 特权，但 vSphere 还包括其他权限模型。请参见 [了解 vSphere 中的授权](#)。

注 如果希望 Active Directory 用户能够使用具有 SSPI 的 vSphere Client 登录 vCenter Server 实例，则必须将 vCenter Server 实例加入到 Active Directory 域。有关将具有外部 Platform Services Controller 部署的 vCenter Server Appliance 加入到 Active Directory 域的信息，请参见 VMware 知识库文章，网址为 <http://kb.vmware.com/kb/2118543>。

本章讨论了以下主题：

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

■ 对 vCenter Single Sign-On 进行故障排除

了解 vCenter Single Sign-On

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



vCenter Single Sign-On 6.0 域和站点

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_y9pxac75/uiConfId/49694343/)

如何使用 vCenter Single Sign-On 保护您的环境

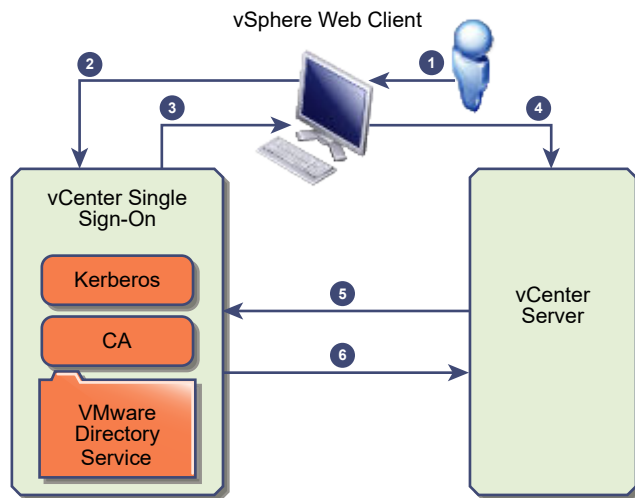
vCenter Single Sign-On 允许 vSphere 组件通过安全的令牌机制互相通信，而不需要用户分别通过每个组件的身份验证。

vCenter Single Sign-On 使用 STS（安全令牌服务）、用于实现安全通信的 SSL 以及通过 Active Directory 或 OpenLDAP 对人工用户及通过证书对解决方案用户进行身份验证的组合。

人工用户的 vCenter Single Sign-On 握手

下图显示了人工用户的握手。

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



- 1 用户使用用户名和密码登录 vSphere Web Client 以访问 vCenter Server 系统或其他 vCenter 服务。
用户还可以不使用密码而选中**使用 Windows 会话身份验证**复选框进行登录。
- 2 vSphere Web Client 将登录信息传递到 vCenter Single Sign-On 服务，该服务将检查 vSphere Web Client 的 SAML 令牌。如果 vSphere Web 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 Web Client 的用户的令牌。
- 4 vSphere Web 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，从而利用 vCenter Server 授权框架以允许用户访问。

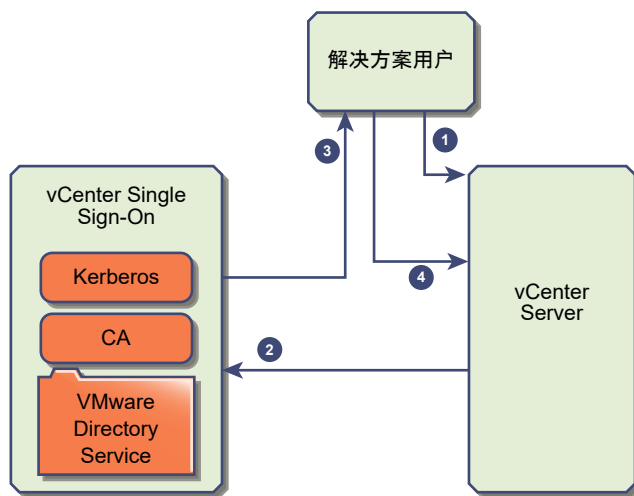
用户现在可以进行身份验证，并可以查看和修改用户角色具有特权的任何对象。

注 首先，每个用户都分配有“无权访问”角色。vCenter Server 管理员必须至少为用户分配“只读”角色，用户才能登录。请参见[将权限添加到清单对象](#)。

解决方案用户的 vCenter Single Sign-On 握手

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

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



对于解决方案用户，交互将以如下方式继续进行：

- 1 解决方案用户尝试连接到 vCenter 服务。
- 2 解决方案用户被重定向到 vCenter Single Sign-On。如果解决方案用户是 vCenter Single Sign-On 的新用户，则必须提供有效的证书。
- 3 如果证书有效，vCenter Single Sign-On 将向解决方案用户分配 SAML 令牌（持有者令牌）。令牌由 vCenter Single Sign-On 签名。
- 4 然后，解决方案用户被重定向到 vCenter Single Sign-On，并可以基于其权限执行任务。
- 5 下次解决方案用户必须进行身份验证时，可以使用 SAML 令牌登录到 vCenter Server。

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

vCenter Single Sign-On 组件

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

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

STS (Security Token Service)

STS 服务会发出安全断言标记语言 (SAML) 令牌。这些安全令牌表示 vCenter Single Sign-On 支持的标识源类型之一中的用户标识。SAML 令牌允许成功通过 vCenter Single Sign-On 身份验证的人工用户和解决方案用户使用 vCenter Single Sign-On 支持的所有 vCenter，而无需再次经过每个服务的身份验证。

vCenter Single Sign-On 服务会使用签名证书对所有令牌进行签名，并在磁盘上存储令牌签名证书。该服务本身的证书也会存储在磁盘上。

管理服务器

管理服务器允许用户具有 vCenter Single Sign-On 的管理员特权，以便配置 vCenter Single Sign-On 服务器并管理 vSphere Web Client 中的用户和组。最初，仅 `administrator@your_domain_name` 用户具有这些特权。在 vSphere 5.5 中，该用户为 `administrator@vsphere.local`。在 vSphere 6.0 中，在使用新的 Platform Services Controller 安装 vCenter Server 或部署 vCenter Server Appliance 时，可以更改 vSphere 域。请勿使用 Microsoft Active Directory 或 OpenLDAP 域名命名该域名。

VMware Directory Service (vmdir)

VMware Directory Service (vmdir) 与安装期间您指定的域相关联，并且包含在每个嵌入式部署和每个 Platform Services Controller 中。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。此服务仍然使用端口 11711，以便向后兼容 vSphere 5.5 及更低版本的系统。

如果您的环境包含多个 Platform Services Controller 实例，则一个 vmdir 实例中的 vmdir 内容更新会传播到所有其他 vmdir 实例。

自 vSphere 6.0 起，VMware Directory Service 不仅会存储 vCenter Single Sign-On 信息，而且还会存储证书信息。

Identity Management Service

处理标识源和 STS 身份验证请求。

vCenter Single Sign-On 如何影响安装

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

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

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

安装顺序非常重要。

首次安装

如果安装为分布式，则必须先安装 Platform Services Controller，然后再安装 vCenter Server 或部署 vCenter Server Appliance。对于嵌入式部署，将自动执行正确的安装顺序。

后续安装

如果最多大约四个 vCenter Server 实例，一个 Platform Services Controller 可以为整个 vSphere 环境提供服务。您可以将新的 vCenter Server 实例连接到同一个 Platform Services Controller。如果超过大约四个 vCenter Server 实例，您可以安装额外的 Platform Services Controller 以获得更佳的性能。每个 Platform Services Controller 上的 vCenter Single Sign-On 服务会与所有其他实例同步身份验证数据。准确数量取决于 vCenter Server 实例的使用程度以及其他因素。

vCenter Single Sign-On 如何影响升级

如果将简单安装环境升级到 vCenter Server 6 嵌入式部署，则需要无缝升级。如果升级自定义安装，则升级后，vCenter Single Sign-On 服务属于 Platform Services Controller 的一部分。升级后哪些用户可以登录 vCenter Server 取决于升级前的版本以及部署配置。

在升级过程中，您可以定义其他要使用的 vCenter Single Sign-On 域名，而不是 vsphere.local。

升级路径

升级结果取决于您选择的安装选项以及您要升级到的部署模型。

表 2-1. 升级路径

源	结果
vSphere 5.5 及早期版本简单安装	具有嵌入式 Platform Services Controller 的 vCenter Server。
vSphere 5.5 及早期版本自定义安装	<p>如果 vCenter Single Sign-On 所在节点与 vCenter Server 不同，则环境中将安装外部 Platform Services Controller。</p> <p>如果 vCenter Single Sign-On 所在节点与 vCenter Server 相同，但其他服务位于不同的节点上，则环境中将安装嵌入式 Platform Services Controller。</p> <p>如果自定义安装包括多个复制的 vCenter Single Sign-On 服务器，则环境中将安装多个复制的 Platform Services Controller 实例。</p>

哪些用户可以在简单安装升级后登录

如果升级使用“简单安装”选项置备的环境，则结果通常是安装嵌入式 Platform Services Controller。授权哪些用户登录取决于源环境中是否包括 vCenter Single Sign-On。

表 2-2. 简单安装环境升级后的登录特权

源版本	登录访问对象	备注
vSphere 5.0	本地操作系统用户 administrator@vsphere.local	<p>由于用户存储中存在更改，系统可能会在安装过程中提示您输入 vSphere 清单层次结构中根文件夹的管理员。</p> <p>如果您之前的安装支持 Active Directory 用户，则可以将 Active Directory 域添加为标识源。</p>
vSphere 5.1	本地操作系统用户 administrator@vsphere.local Admin@SystemDomain	<p>从 vSphere 5.5 开始，vCenter Single Sign-On 仅支持一个默认标识源。</p> <p>可以设置默认标识源。</p> <p>非默认域中的用户在登录（<i>DOMAIN\user</i> 或 <i>user@DOMAIN</i>）时可以指定域。</p>
vSphere 5.5	administrator@vsphere.local 或在升级过程中指定的域管理员。 所有标识源中的所有用户仍可以像先前一样登录。	

如果从 vSphere 5.0（不包括 vCenter Single Sign-On）升级到包括 vCenter Single Sign-On 的版本，则本地操作系统用户将远不如目录服务（如 Active Directory）中的用户重要。因此，很难，或甚至是无法保留本地操作系统用户作为经过身份验证的用户。

哪些用户可以在自定义安装升级后登录

如果升级使用“自定义安装”选项置备的环境，则结果取决于初始选择：

- 如果 vCenter Single Sign-On 所在节点与 vCenter Server 系统相同，则结果是安装嵌入式 Platform Services Controller。

- 如果 vCenter Single Sign-On 所在节点与 vCenter Server 系统不同，则结果是安装外部 Platform Services Controller。
- 如果从 vSphere 5.0 升级，则可以在升级时选择外部或嵌入式 Platform Services Controller。

升级后的登录特权取决于多种因素。

表 2-3. 自定义安装环境升级后的登录特权

源版本	登录访问对象	备注
vSphere 5.0	<p>vCenter Single Sign-On 可识别安装有 Platform Services Controller 的计算机（而不是安装有 vCenter Server 的计算机）的本地操作系统用户。</p> <p>注 不建议使用本地操作系统用户进行管理，尤其是在联合环境中。</p> <p>administrator@vsphere.local 可以作为管理员用户登录到 vCenter Single Sign-On 和每个 vCenter Server 实例。</p>	<p>如果 5.0 安装支持 Active Directory 用户，则这些用户在升级后将不再具有访问权限。可以添加 Active Directory 域作为标识源。</p>
vSphere 5.1 或 vSphere 5.5	<p>vCenter Single Sign-On 可识别安装有 Platform Services Controller 的计算机（而不是安装有 vCenter Server 的计算机）的本地操作系统用户。</p> <p>注 不建议使用本地操作用户进行管理，尤其是在联合环境中。</p> <p>administrator@vsphere.local 可以作为管理员用户登录到 vCenter Single Sign-On 和每个 vCenter Server 实例。</p> <p>对于从 vSphere 5.1 升级，Admin@SystemDomain 所拥有的特权与 administrator@vsphere.local 相同。</p>	<p>从 vSphere 5.5 开始，vCenter Single Sign-On 仅支持一个默认标识源。</p> <p>可以设置默认标识源。</p> <p>非默认域中的用户在登录（<code>DOMAIN\user</code> 或 <code>user@DOMAIN</code>）时可以指定域。</p>

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 Web 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 管理员可以通过 vSphere Web Client 中的[管理 > 权限](#)界面分配这些权限，而不是通过 vCenter Single Sign-On 进行分配。请参见第 4 章 [vSphere 权限和用户管理任务](#)。

vCenter Single Sign-On 和 vCenter Server 用户

用户可使用 vSphere Web Client，通过在 vSphere Web Client 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。请参见第 4 章 [vSphere 权限和用户管理任务](#)。

安装后，administrator@vsphere.local 用户将拥有对 vCenter Single Sign-On 和 vCenter Server 的管理员访问权限。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 (vsphere.local) 中的用户和组。

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

vCenter Single Sign-On 管理员用户

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

要配置 vCenter Single Sign-On 并管理 vCenter Single Sign-On 用户和组，用户 administrator@vsphere.local 或 vCenter Single Sign-On 管理员组中的用户必须登录到 vSphere Web Client。根据身份验证，该用户可以通过 vSphere Web 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。请参见[配置 vCenter Single Sign-On 标识源](#)。

注 无法重命名 administrator@vsphere.local 用户。为提高安全性，请考虑在 vsphere.local 域中创建其他命名的用户，并为其分配管理权限。然后，可以停止使用 administrator@vsphere.local。

vSphere 的不同版本中的身份验证

如果用户连接到 5.0.x 或早期版本的 vCenter Server 系统，则 vCenter Server 将根据 Active Directory 域或本地操作系统用户列表来对用户进行身份验证。在 vCenter Server 5.1 及更高版本中，用户将通过 vCenter Single Sign-On 进行身份验证。

注 您无法使用 vSphere Web Client 来管理 vCenter Server 5.0 或更早版本。将 vCenter Server 升级至 5.1 或更高版本。

ESXi 用户

ESXi 未与 vCenter Single Sign-On 集成。将 ESXi 主机明确添加到 Active Directory 域。请参见[配置主机以使用 Active Directory](#)。

仍可以使用 vSphere Client、vCLI 或 PowerCLI 创建本地 ESXi 用户。vCenter Server 不会识别 ESXi 的本地用户。ESXi 不会识别 vCenter Server 用户。

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

用户从 vSphere Web Client 登录到 vCenter Server 系统时，登录行为取决于用户是否位于默认域，即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。

注 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信息。

vsphere.local 域中的组

vsphere.local 域包含多个预定义组。如果将用户分配给其中一个组，则可以执行相应的操作。

对于 vCenter Server 层次结构中的所有对象，请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的读取特权。

对于不由 vCenter Server 直接管理的某些服务，将按其中一个 vCenter Single Sign-On 组的成员资格来确定相关特权。例如，属于管理员组成员的用户可以管理 vCenter Single Sign-On。属于 CAAdmins 组成员的用户可以管理 VMware Certificate Authority，而属于 LicenseService.Administrators 组的用户可以管理许可证。

vsphere.local 中预定义了以下组。

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

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

表 2-4. vsphere.local 域中的组

特权	描述
用户	vsphere.local 域中的用户。
SolutionUsers	解决方案用户组 vCenter 服务。每个解决方案用户将使用证书单独向 vCenter Single Sign-On 进行身份验证。默认情况下，VMCA 将为解决方案用户置备证书。不要向该组明确添加成员。
CAAdmins	CAAdmins 组的成员拥有 VMCA 的管理员特权。通常不建议向这些组添加成员。
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 Web Client 执行相应的任务。
SystemConfiguration.BashShellAdministrators	此组仅适用于 vCenter Server Appliance 部署。 此组中的用户可以启用和禁用对 BASH shell 的访问。默认情况下，使用 SSH 连接到 vCenter Server Appliance 的用户只能访问受限 shell 中的命令。此组中的用户可以访问 BASH shell。
ActAsUsers	Act-As Users 的成员可以从 vCenter Single Sign-On 获取 actas 令牌。
ExternalIPDUsers	vSphere 未使用此组。与 VMware vCloud Air 一起使用时需要此组。
SystemConfiguration.Administrators	SystemConfiguration.Administrators 组的成员可以在 vSphere Web 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、查看可用的节点以及管理这些节点。
DCClients	此组在内部使用，以便允许管理节点访问 VMware Directory Service 中的数据。 注 不要修改此组。任何更改都可能会影响证书基础架构。
ComponentManager.Administrators	ComponentManager.Administrators 组的成员可以调用组件管理器 API 以注册或取消注册服务，即修改服务。对服务进行读取访问不需要此组中的成员资格。
LicenseService.Administrators	LicenseService.Administrators 的成员对所有与许可相关的数据具有完全的写入访问权限，且可以为已在许可服务中注册的所有产品资产添加、移除、分配和取消分配序列密钥。
管理员	VMware Directory Service (vmdir) 的管理员。此组的成员可以执行 vCenter Single Sign-On 管理任务。通常不建议向此组添加成员。

vCenter Server 密码要求和锁定行为

要管理您的环境，必须了解 vCenter Single Sign-On 密码策略、vCenter Server 密码和锁定行为。

vCenter Single Sign-On 管理员密码

administrator@vsphere.local 的密码必须满足以下要求：

- 至少 8 个字符
- 至少一个小写字符
- 至少一个数字字符
- 至少一个特殊字符

administrator@vsphere.local 的密码长度不能超过 20 个字符。仅允许可见的 ASCII 字符。这意味着，例如，不能使用空格字符。

vCenter Server 密码

在 vCenter Server 中，密码要求由 vCenter Single Sign-On 或配置的标识源规定，这些配置的标识源可以是 Active Directory、OpenLDAP 或 vCenter Single Sign-On 服务器的本地操作系统（不推荐）。

锁定行为

在连续尝试预设次数失败后，用户将被锁定。默认情况下，用户在三分钟内连续五次尝试失败后将被锁定，锁定的帐户在五分钟后将自动解锁。您可以使用锁定策略更改这些默认值。请参见[编辑 vCenter Single Sign-On 锁定策略](#)。

自 vSphere 6.0 起，默认情况下，锁定策略不会影响系统域管理员 administrator@vsphere.local。

任何用户都可以使用 `dir-cli password change` 命令更改其密码。如果用户忘记密码，则管理员可以使用 `dir-cli password reset` 命令重置密码。

有关 ESXi 本地用户的密码的探讨，请参见 [ESXi 密码和帐户锁定](#)。

配置 vCenter Single Sign-On 标识源

用户登录时，vCenter Single Sign-On 会检查默认标识源是否该用户可以进行身份验证。可以添加标识源、移除标识源和更改默认值。

可从 vSphere Web 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。默认情况下，在全新安装中，只有用户 administrator@vsphere.local 才具有 vCenter Single Sign-On 服务器上的管理员特权。

- [vCenter Server 和 vCenter Single Sign-On 的标识源](#)

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

- [设置 vCenter Single Sign-On 的默认域](#)

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

- [添加 vCenter Single Sign-On 标识源](#)

仅当用户位于已添加为 vCenter Single Sign-On 标识源的域中时，才可以登录 vCenter Server。vCenter Single Sign-On 管理员用户可从 vSphere Web Client 中添加标识源。

- [编辑 vCenter Single Sign-On 标识源](#)

vSphere 用户在标识源中定义。您可以编辑与 vCenter Single Sign-On 相关联的标识源的详细信息。

- [删除 vCenter Single Sign-On 标识源](#)

vSphere 用户在标识源中定义。可从注册的标识源列表中移除标识源。

■ 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)。要使该复选框显示在登录页面上，必须安装客户端集成插件。

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。

标识源是用户和组数据的集合。用户和组数据存储在 Active Directory 中、OpenLDAP 中或者存储到本地安装了 vCenter Single Sign-On 的计算机操作系统。

在安装后，vCenter Single Sign-On 的每个实例都有标识源 *your_domain_name*，例如，*vsphere.local*。此标识源在 vCenter Single Sign-On 内部。vCenter Single Sign-On 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。

标识源的类型

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

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

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

- vCenter Single Sign-On 系统用户。每次安装 vCenter Single Sign-On 时都会创建一个名为 *vsphere.local* 的系统标识源。在 vSphere Web Client 中显示为 **vsphere.local**。

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

vCenter Single Sign-On 标识源由 vCenter Single Sign-On 管理员用户管理。

可以将多个标识源添加到一个 vCenter Single Sign-On 服务器实例中。远程标识源仅限用于 Active Directory 和 OpenLDAP 服务器实施。

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，则在登录时必须包含域名。

用户从 vSphere Web Client 登录到 vCenter Server 系统时，登录行为取决于用户是否位于默认域，即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。

步骤

- 1 以 administrator@vsphere.local 或拥有 vCenter Single Sign-On 管理员特权的其他用户的身份登录到 vSphere Web Client。
具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。
- 2 浏览到**管理 > Single Sign-On > 配置**。
- 3 在**标识源**选项卡上，选择一个标识源，然后单击**设置为默认域**图标。
在域显示屏幕中，默认域显示在“域”列中（默认设置）。

添加 vCenter Single Sign-On 标识源

仅当用户位于已添加为 vCenter Single Sign-On 标识源的域中时，才可以登录 vCenter Server。vCenter Single Sign-On 管理员用户可从 vSphere Web Client 中添加标识源。

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

一旦完成安装，以下默认标识源和用户立即可用：

localos

所有本地操作系统用户。如果要进行升级，已能够进行身份验证的用户可以继续进行身份验证。在使用 Platform Services Controller 的环境中使用 localos 标识源没有意义。

vsphere.local

包含 vCenter Single Sign-On 内部用户。

前提条件

要添加为标识源的域必须对正在运行 vCenter Single Sign-On 的计算机可用。如果使用的是 vCenter Server Appliance，请参见《vCenter Server Appliance 配置》文档。

步骤

- 1 以 administrator@vsphere.local 或拥有 vCenter Single Sign-On 管理员特权的其他用户的身份登录到 vSphere Web Client。
具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。
- 2 浏览到**管理 > Single Sign-On > 配置**。
- 3 在**标识源**选项卡上，单击**添加标识源**图标。
- 4 选择标识源的类型，然后输入标识源设置。

选项	描述
Active Directory (已集成 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 。
Active Directory 作为 LDAP 服务器	此选项可用于向后兼容性。这需要您指定域控制器和其他信息。请参见 Active Directory LDAP Server 和 OpenLDAP Server 标识源设置。
OpenLDAP	对于 OpenLDAP 标识源，请使用此选项。请参见 Active Directory LDAP Server 和 OpenLDAP Server 标识源设置。
LocalOS	使用此选项可添加本地操作系统以作为标识源。系统仅提示您输入本地操作系统的名称。如果选择此选项，则指定计算机上的所有用户都对 vCenter Single Sign-On 可见，即使这些用户不属于其他域也是如此。

注 如果用户帐户已锁定或禁用，Active Directory 域中的身份验证以及组和用户搜索将失败。用户帐户必须具有用户和组 OU 的只读访问权限，并且必须能够读取用户和组属性。这是身份验证权限的默认 Active Directory 域配置。VMware 建议使用特殊服务用户。

- 5 如果配置 Active Directory 作为 LDAP 服务器或 OpenLDAP 标识源，则单击**测试连接**以确保您可以连接到标识源。
- 6 单击**确定**。

后续步骤

添加标识源后，所有用户均可进行身份验证，但只有**无权访问**角色。具有 vCenter Server **修改权限**特权的用户可向单个用户或一组用户分配特权，以便他们能够登录 vCenter Server 并查看和管理对象。请参见《vSphere 安全性》文档。

Active Directory 标识源设置

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

使用 Active Directory 标识源的必备条件

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

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

注 Active Directory（集成 Windows 身份验证）始终使用 Active Directory 域林的 root 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 [2070433](#)。

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

注 在 vSphere 5.5 中，即使指定 SPN，vCenter Single Sign-On 仍会使用计算机帐户。请参见 VMware 知识库文章 [2087978](#)。

表 2-5. 添加标识源设置

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

Active Directory LDAP Server 和 OpenLDAP Server 标识源设置

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

配置 OpenLDAP 标识源时，请参见 VMware 知识库文章 [2064977](#)，以了解其他要求。

表 2-6. LDAP Server Active Directory 和 OpenLDAP 设置

字段	描述
名称	标识源的名称。
用户的基本 DN	用户的基本识别名。
域名	域的 FDQN，例如，example.com。请勿在此字段提供 IP 地址。
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。
组的基本 DN	组的基本识别名。
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。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: 连接，而 3269 用于 ldaps: 连接。 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。
选择证书	如果要将 LDAPS 与 Active Directory LDAP 服务器或 OpenLDAP 服务器标识源配合使用，则在 URL 字段中键入 ldaps:// 后，“选择证书”按钮变为可用。不需要辅助 URL。
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	由“用户名”指定的用户的密码。

编辑 vCenter Single Sign-On 标识源

vSphere 用户在标识源中定义。您可以编辑与 vCenter Single Sign-On 相关联的标识源的详细信息。

步骤

- 1 以 administrator@vsphere.local 或拥有 vCenter Single Sign-On 管理员特权的其他用户的身份登录到 vSphere Web Client。
具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。
- 2 浏览到**管理 > Single Sign-On > 配置**。
- 3 单击**标识源**选项卡。
- 4 在表中右键单击标识源，然后选择**编辑标识源**。
- 5 编辑标识源设置。可用选项取决于所选标识源的类型。

选项	描述
Active Directory (已集成 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 。
Active Directory 作为 LDAP 服务器	此选项可用于向后兼容性。这需要您指定域控制器和其他信息。请参见 Active Directory LDAP Server 和 OpenLDAP Server 标识源设置 。
OpenLDAP	对于 OpenLDAP 标识源，请使用此选项。请参见 Active Directory LDAP Server 和 OpenLDAP Server 标识源设置 。
LocalOS	使用此选项可添加本地操作系统以作为标识源。系统仅提示您输入本地操作系统的名称。如果选择此选项，则指定计算机上的所有用户都对 vCenter Single Sign-On 可见，即使这些用户不属于其他域也是如此。

- 6 单击**测试连接**以确保可以连接到该标识源。
- 7 单击**确定**。

删除 vCenter Single Sign-On 标识源

vSphere 用户在标识源中定义。可从注册的标识源列表中移除标识源。

步骤

- 1 以 administrator@vsphere.local 或拥有 vCenter Single Sign-On 管理员特权的其他用户的身份登录到 vSphere Web Client。
具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。
- 2 浏览到**管理 > Single Sign-On > 配置**。
- 3 在**标识源**选项卡上，选择一个标识源，然后单击**删除标识源**图标。
- 4 遇到确认提示时，请单击**是**。

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)。要使该复选框显示在登录页面上，必须安装客户端集成插件。

使用 SSPI 可为当前已登录计算机的用户加快登录速度。

前提条件

必须正确设置 Windows 域。请参见 VMware 知识库文章 [2064250](#)。

步骤

- 1 导航到 vSphere Web Client 登录页面。
- 2 如果使用 **Windows 会话身份验证** 复选框不可用，请单击位于登录页面底部的 **下载客户端集成插件**。
- 3 如果浏览器通过发出证书错误或运行弹出窗口阻止程序阻止安装，请按照浏览器的“帮助”说明解决问题。
- 4 如果系统提示您关闭其他浏览器，则执行此操作。
安装后，此插件将适用于所有浏览器。如果浏览器需要此插件，则可能必须允许此插件用于单个会话或用于所有会话。
- 5 退出然后重新启动浏览器。
重新启动后，便可以选中 **使用 Windows 会话身份验证** 复选框。

vCenter Server 双因素身份验证

vCenter Single Sign-On 允许您通过使用对 vCenter Single Sign-On 已知的标识源中的用户名和密码，或者使用 Active Directory 标识源的 Windows 会话身份验证来进行身份验证。从 vSphere 6.0 Update 2 开始，还可以通过使用智能卡（基于 UPN 的通用访问卡或 CAC）或者通过使用 RSA SecurID 令牌来进行身份验证。

双因素身份验证方法

政府机构或大型企业通常需要双因素身份验证方法。

通用访问卡 (CAC) 身份验证

CAC 身份验证仅允许将物理卡附加到他们所登录的计算机的 USB 驱动器的用户进行访问。如果部署了 PKI，使智能卡证书成为由 CA 颁发的唯一客户端证书，则仅为用户提供智能卡证书。用户选择一个证书，然后系统提示他输入 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 SecureID 身份验证，您的环境必须包括正确配置的 RSA Authentication Manager。如果 Platform Services Controller 已配置为指向 RSA 服务器，并且如果已启用 RSA SecurID 身份验证，则用户可以通过其用户名和令牌进行登录。

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

指定非默认身份验证方法

管理员可以从 Platform Services Controller Web 界面，或者通过使用 sso-config 脚本（Windows 上的 sso-config.bat 和设备上的 sso-config.sh）来执行设置。

- 对于通用访问卡身份验证，通过使用 sso-config 脚本来设置 Web 浏览器，这样可以从 Platform Services Controller Web 界面或者通过使用 sso-config 来执行 vCenter Single Sign-On 设置。设置包括启用 CAC 身份验证、配置证书吊销策略以及设置登录横幅。
- 对于 RSA SecureID，使用 sso-config 脚本为域配置 RSA Authentication Manager，并启用 RSA 令牌身份验证。如果已启用，身份验证方法将显示在 Platform Services Controller Web 界面中，但是无法从 Web 界面配置 RSA SecureID 身份验证。

结合使用不同的身份验证方法

可以使用 sso-config 分别启用或禁用每个身份验证方法。例如，以下做法可能是有意义的：在测试双因素身份验证方法之一时最初让用户名和密码身份验证处于启用状态，然后仅将一个身份验证方法设置为启用状态。

为 vCenter Single Sign-On 配置智能卡身份验证

可以将您的环境设置为当用户从 vSphere Web Client 连接到 vCenter Server 或关联的 Platform Services Controller 时需要智能卡身份验证。

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。通用访问卡在每个计算机都包括智能卡读取器以及通常预装了管理通用访问卡的智能卡硬件驱动程序的环境中使用。

为 vCenter Single Sign-On 配置智能卡身份验证时，将提示登录到 vCenter Server 或 Platform Services Controller 系统的用户通过智能卡和 PIN 的组合进行身份验证，如下所述：

- 1 用户将智能卡插入智能卡读取器时，vCenter Single Sign-On 读取卡上的证书。
- 2 vCenter Single Sign-On 提示用户选择证书，然后提示用户输入该证书的 PIN。
- 3 vCenter Single Sign-On 检查智能卡上的证书是否已知以及 PIN 是否正确。如果打开吊销检查，则 vCenter Single Sign-On 还会检查证书是否已被吊销。

- 4 如果证书是已知的且不是已吊销的证书，则用户通过身份验证，然后可以执行该用户有权执行的任务。

注 大多数情况下，在测试期间保持用户名和密码身份验证处于启用状态很有意义。测试完成后，禁用用户名和密码身份验证并启用智能卡身份验证。之后，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 Platform Services Controller 来重新启用用户名和密码。

使用命令行配置智能卡身份验证

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

从命令行配置智能卡身份验证时，请始终先使用 sso-config 命令设置 Platform Services Controller。然后，可以通过使用 Platform Services Controller Web 界面执行其他任务。

- 1 配置 Platform Services Controller，以便 Web 浏览器在用户登录时请求提交智能卡证书。
- 2 配置身份验证策略。您可以通过使用 sso-config 脚本或 Platform Services Controller Web 界面配置策略。支持的身份验证类型和吊销设置的配置存储在 VMware Directory Service 中，且在 vCenter Single Sign-On 域中的所有 Platform Services Controller 实例之间复制。

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

如果从 vSphere Web Client 登录不起作用，并且如果用户名和密码身份验证已关闭，则 root 用户或管理员用户可以通过运行以下命令从 Platform Services Controller 命令行重新打开用户名和密码身份验证。该示例用于 Windows；对于 Linux，请使用 sso-config.sh。

```
sso-config.bat -set_authn_policy -pwdAuthn true
```

您可以在以下位置找到 sso-config 脚本：

Windows C:\Program Files\VMware\VCenter server\VMware Identity Services\sso-config.bat

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

前提条件

- 确认您的环境使用 Platform Services Controller 6.0 Update 2 或更高版本，且使用 vCenter Server 6.0 或更高版本。将版本 5.5 节点升级到版本 6.0。
- 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) 对应于使用者备用名称 (SAN) 扩展名中的 Active Directory 帐户。
 - 必须在证书的“应用程序策略”或“增强型密钥用法”字段中指定客户端身份验证，否则浏览器将不显示该证书。
- 验证 Platform Services Controller Web 界面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。
- 配置 Active Directory 标识源，并将其作为标识源添加到 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。然后那些用户可以进行身份验证，因为他们在 Active Directory 组中，并且具有 vCenter Server 管理员特权。
administrator@vsphere.local 用户无法执行智能卡身份验证。
- 如果要在您的环境中使用 Platform Services Controller HA 解决方案，请在设置智能卡身份验证之前完成所有 HA 配置。请参见 VMware 知识库文章 [2112085 \(Windows\)](#) 或 [2113315 \(vCenter Server Appliance\)](#)。

步骤

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

选项	描述
Windows	登录到 Platform Services Controller Windows 安装，并使用 WinSCP 或类似的实用程序复制文件。
Appliance	<ol style="list-style-type: none"> 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。 <pre>shell.set --enabled True shell chsh -s "/bin/bash" root csh -s "bin/appliance/sh" root</pre> c 使用 WinSCP 或类似的实用程序将证书复制到 Platform Services Controller 上的 /usr/lib/vmware-sso/vmware-sts/conf。 d 选择性禁用设备 shell，如下所示。 <pre>chsh -s "bin/appliancesh" root</pre>

2 在每个 Platform Services Controller 节点上，通过使用 sso-config CLI 配置智能卡身份验证设置。

- a 转到 sso-config 脚本所在的目录。

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

- b 运行下列命令：

```
sso-config.[bat|sh] -set_tc_cert_authn -switch true -cacerts
[FirstTrustedCA.cer,SecondTrustedCA.cer,...] -t tenant
```

例如：

```
sso-config.bat -set_tc_cert_authn -switch true -cacerts MySmartCA1.cer -t vsphere.local
```

- c 重新启动虚拟机或物理机。

```
service-control --stop vmware-std
service-control --start vmware-std
```

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

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

例如：

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

如果指定多个证书，不允许在证书之间使用空格。

4 要禁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
```

您可以根据需要使用以下命令启用和禁用其他身份验证方法。

5 （可选）要设置证书策略允许列表，请运行以下命令。

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

要指定多个策略，请用逗号分隔它们，例如：

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

此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。

6 （可选）要列出配置信息，请运行以下命令。

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

使用 Platform Services Controller Web 界面管理智能卡身份验证

可以从 Platform Services Controller Web 界面启用和禁用智能卡身份验证、自定义登录横幅以及设置吊销策略。

从命令行配置智能卡身份验证时，请始终先使用 `sso-config` 命令设置 Platform Services Controller。然后，可以通过使用 Platform Services Controller Web 界面执行其他任务。

- 1 配置 Platform Services Controller，以便 Web 浏览器在用户登录时请求提交智能卡证书。
- 2 配置身份验证策略。您可以通过使用 `sso-config` 脚本或 Platform Services Controller Web 界面配置策略。支持的身份验证类型和吊销设置的配置存储在 VMware Directory Service 中，且在 vCenter Single Sign-On 域中的所有 Platform Services Controller 实例之间复制。

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

如果从 vSphere Web Client 登录不起作用，并且如果用户名和密码身份验证已关闭，则 `root` 用户或管理员用户可以通过运行以下命令从 Platform Services Controller 命令行重新打开用户名和密码身份验证。该示例用于 Windows；对于 Linux，请使用 `sso-config.sh`。

```
sso-config.bat -set_authn_policy -pwdAuthn true
```

前提条件

- 确认您的环境使用 Platform Services Controller 6.0 Update 2 或更高版本，且使用 vCenter Server 6.0 或更高版本。将版本 5.5 节点升级到版本 6.0。
- 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) 对应于使用者备用名称 (SAN) 扩展名中的 Active Directory 帐户。
 - 必须在证书的“应用程序策略”或“增强型密钥用法”字段中指定客户端身份验证，否则浏览器将不显示该证书。
- 验证 Platform Services Controller Web 界面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。
- 配置 Active Directory 标识源，并将其作为标识源添加到 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。然后那些用户可以进行身份验证，因为他们在 Active Directory 组中，并且具有 vCenter Server 管理员特权。`administrator@vsphere.local` 用户无法执行智能卡身份验证。

- 如果要在您的环境中使用 Platform Services Controller HA 解决方案，请在设置智能卡身份验证之前完成所有 HA 配置。请参见 VMware 知识库文章 [2112085](#) (Windows) 或 [2113315](#) (vCenter Server Appliance)。

步骤

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

选项	描述
Windows	登录到 Platform Services Controller Windows 安装，并使用 WinSCP 或类似的实用程序复制文件。
Appliance	<ol style="list-style-type: none"> 直接或者使用 SSH 登录到设备控制台。 启用设备 shell，如下所示。 <div data-bbox="678 661 1426 798" data-label="Text"> <pre>shell.set --enabled True shell chsh -s "/bin/bash" root csh -s "bin/appliance/sh" root</pre> </div> 使用 WinSCP 或类似的实用程序将证书复制到 Platform Services Controller 上的 /usr/lib/vmware-sso/vmware-sts/conf。 选择性禁用设备 shell，如下所示。 <div data-bbox="678 913 1426 976" data-label="Text"> <pre>chsh -s "bin/appliancesh" root</pre> </div>

- 2 在每个 Platform Services Controller 节点上，通过使用 sso-config CLI 配置智能卡身份验证设置。

- a 转到 sso-config 脚本所在的目录。

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

- b 运行下列命令：

```
sso-config.[bat|sh] -set_tc_cert_authn -switch true -cacerts
[FirstTrustedCA.cer,SecondTrustedCA.cer,...] -t tenant
```

例如：

```
sso-config.bat -set_tc_cert_authn -switch 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。

- c 重新启动虚拟机或物理机。

```
service-control --stop vmware-std
service-control --start vmware-std
```

- 3 在 Web 浏览器中，通过指定以下 URL 连接到 Platform Services Controller：

`https://psc_hostname_or_IP/psc`

在嵌入式部署中，Platform Services Controller 主机名或 IP 地址与 vCenter Server 主机名或 IP 地址相同。

- 4 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。

- 5 浏览到 **Single Sign-On > 配置**。

- 6 单击**智能卡配置**，并选择**可信 CA 证书**选项卡。

- 7 要添加一个或多个可信证书，请单击**添加证书**，单击**浏览**，从可信 CA 选择所有证书，然后单击**确定**。

- 8 要指定身份验证配置，请单击**身份验证配置**旁边的**编辑**，然后选择或取消选择身份验证方法。

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

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

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

仅 OCSP

如果发证 CA 支持 OCSP 响应者，则启用 OCSP 并禁止使用 CRL 进行故障切换。

仅 CRL

如果发证 CA 不支持 OCSP，则启用 CRL 检查并禁用 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，请同时启用 OCSP 检查和 CRL 检查，并启用 CRL 作为 OCSP 的故障切换。

- 如果已启用吊销检查，则高级用户可以指定以下其他设置。

OCSP URL

默认情况下，vCenter Single Sign-On 检查在被验证的证书中定义的 OCSP 响应者的位置。如果证书中缺少授权信息访问扩展，或者如果要替代它（例如，因为它在您的环境中不可用），则可以显式指定一个位置。

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。证书中缺少 CRL 分发点扩展或者您要替代默认值时，请禁用此选项。

CRL 位置

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

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

前提条件

- 验证您的环境是否使用 Platform Services Controller 版本 6.0 Update 2 或更高版本，以及是否使用 vCenter Server 版本 6.0 或更高版本。将版本 5.5 节点升级到版本 6.0。
- 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) 对应于使用者备用名称 (SAN) 扩展名中的 Active Directory 帐户。
 - 必须在证书的“应用程序策略”或“增强型密钥用法”字段中指定客户端身份验证，否则浏览器将不显示该证书。

- 验证 Platform Services Controller Web 界面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。
- 配置 Active Directory 标识源，并将其作为标识源添加到 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。然后那些用户可以进行身份验证，因为他们在 Active Directory 组中，并且具有 vCenter Server 管理员特权。
administrator@vsphere.local 用户无法执行智能卡身份验证。
- 如果要在您的环境中使用 Platform Services Controller HA 解决方案，请在设置智能卡身份验证之前完成所有的 HA 配置。请参见 VMware 知识库文章 [2113085 \(Windows\)](#) 或 [2113315 \(vCenter Server Appliance\)](#)。

步骤

- 1 在 Web 浏览器中，通过指定以下 URL 连接到 Platform Services Controller:

`https://psc_hostname_or_IP/psc`

在嵌入式部署中，Platform Services Controller 主机名或 IP 地址与 vCenter Server 主机名或 IP 地址相同。

- 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 浏览到 **Single Sign-On > 配置**。
- 4 单击**证书吊销设置**并启用或禁用吊销检查。
- 5 如果证书策略在您的环境中是有效的，则可以在**已接受的证书策略**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 令牌而不是密码登录。仅支持从命令行进行 SecurID 设置。

有关详细信息，请参见两个有关 [RSA SecurID 设置](#) 的 vSphere 博客帖子。

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

前提条件

- 验证您的环境是否使用 Platform Services Controller 版本 6.0 Update 2 或更高版本，以及是否使用 vCenter Server 版本 6.0 或更高版本。将版本 5.5 节点升级到版本 6.0。
- 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 vCenter Single Sign-On 标识源](#)。

- 验证 RSA Authentication Manager 系统是否可以解析 Platform Services Controller 主机名，以及 Platform Services Controller 系统是否可以解析 RSA Authentication Manager 主机名。
- 通过选择访问 > 身份验证代理 > 生成配置文件，从 RSA Manager 导出 sdconf.rec 文件。解压缩生成的 AM_Config.zip 文件以查找 sdconf.rec 文件。
- 将 sdconf.rec 文件复制到 Platform Services Controller 节点。

步骤

- 1 更改到 sso-config 脚本所在的目录。

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

- 2 要启用 RSA SecurID 身份验证，请运行以下命令。

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

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

- 3 （可选）要禁用其他身份验证方法，请运行以下命令。

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

- 4 要配置环境以使当前站点的租户使用 RSA 站点，请运行以下命令。

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

例如：

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

可以指定以下选项。

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

- 5 （可选） 要将租户配置更改为非默认值，请运行以下命令。

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

通常情况下，默认值是合适的，例如：

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

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

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

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

例如：

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

- 7 要显示当前设置，请运行以下命令。

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

结果

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

管理登录横幅

从 vSphere 6.0 Update 2 开始，可以在您的环境中包括登录横幅。可以显示某些文本，也可以要求用户单击复选框来表示诸如他们接受条款和条件。可以启用和禁用登录横幅，并且可以要求用户单击用于表示明确同意的复选框。

步骤

- 1 在 Web 浏览器中，通过指定以下 URL 连接到 Platform Services Controller：

`https://psc_hostname_or_IP/psc`

在嵌入式部署中，Platform Services Controller 主机名或 IP 地址与 vCenter Server 主机名或 IP 地址相同。

- 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 Single Sign-On 下，选择**配置**，然后单击**登录横幅**选项卡。

4 单击**编辑**并配置登录横幅。

选项	描述
状态	单击 已启用 复选框以启用登录横幅。除非单击此复选框，否则无法更改其他字段。
明确同意	单击 明确同意 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。
标题	横幅的标题。默认情况下，登录横幅文本是 I agree to the（我同意）。可以向其添加内容，例如 Terms and Conditions（条款和条件）。
消息	用户在单击横幅时看到的消息。例如，条款和条件的文本。如果使用明确同意，则消息是必需的。

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

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

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

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

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

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

1 将 IDP 元数据导出到文件，然后将其导入到 SP。

2 导出 SP 元数据并将其导入到 IDP。

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

注 服务必须完全支持 SAML 2.0 标准，否则集成将不起作用。

添加 SAML 服务提供程序

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

如果要将 VMware vRealize Automation 7.0 和更高版本附带的 Single Sign-On 解决方案与 vCenter Single Sign-On 身份提供程序集成在一起，或者如果使用的是其他外部 SAML 服务提供程序，则使用此过程。

该过程包括将元数据从 SAML 服务提供程序导入到 vCenter Single Sign-On，以及将 vCenter Single Sign-On 元数据导入到 SAML 服务提供程序，以便两个提供程序可共享所有数据。

前提条件

目标服务必须完全支持 SAML 2.0 标准。

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

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

当前无法从 vSphere Web Client 导入 SAML IDP 元数据。

步骤

- 1 将元数据从服务提供程序导出到文件。
- 2 将服务提供程序的元数据导入到 vCenter Single Sign-On 中。
 - a 以 administrator@vsphere.local 或拥有 vCenter Single Sign-On 管理员特权的其他用户的身份登录到 vSphere Web Client。
具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。
 - b 浏览到 **Single Sign-On > 配置**。
 - c 选择 **SAML 服务提供程序** 选项卡。
 - d 在您的 **SAML 服务提供程序中的元数据** 字段中，单击 **导入** 并将 XML 字符串粘贴到对话框中，或单击 **从文件导入** 以导入文件，然后单击 **导入**。
- 3 导出 vCenter Single Sign-On 元数据。
 - a 在您的 **SAML 服务提供程序中的元数据** 字段中，单击 **下载**。
 - b 指定一个文件位置。
- 4 转到 SAML 服务提供程序（例如 VMware vRealize Automation 7.0 或更高版本），并按照用于 SAML 服务提供程序的说明将 vCenter Single Sign-On 元数据添加到该服务提供程序。

有关导入元数据的详细信息，请参见 vRealize Automation 文档。

安全令牌服务 (STS)

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

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

用户

vCenter Single Sign-On 标识源中提供的用户名和密码。

应用程序用户

有效证书。

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

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

在设备上生成新的 STS 签名证书

如果要替换默认的 vCenter Single Sign-On Security Token Service (STS) 签名证书，您必须生成新证书并将其添加到 Java 密钥库。此过程说明了在嵌入式部署设备或外部 Platform Services Controller 设备上执行该操作的步骤。

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

如果运行的是 Platform Services Controller Windows 安装，请参见在 [Windows 上安装 vCenter](#) 时生成新的 STS 签名证书。

步骤

- 1 创建顶级目录以保存新证书并确认该目录的位置。

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

- 2 将 certtool.cfg 文件复制到新目录中。

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

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

国家/地区为必填字段且必须是两个字符，如以下示例所示。

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

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

- 4 生成密钥。

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

- 5 生成证书

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

- 6 将证书转换为 PK12 格式。

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

- 7 将证书添加到 Java 密钥库 (JKS)。

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

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

- 8 出现提示时，键入 **Yes** 接受证书以将其添加到密钥库。

后续步骤

现在即可导入新证书。请参见[刷新安全令牌服务证书](#)。

在 Windows 上安装 vCenter 时生成新的 STS 签名证书

如果要替换默认的 STS 签名证书，必须先生成一个新证书并将其添加到 Java 密钥库。以下过程说明了 Windows 中的安装步骤。

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

如果使用虚拟设备，请参见[在设备上生成新的 STS 签名证书](#)。

步骤

- 1 创建一个新目录以存放新证书。

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

- 2 创建 certtool.cfg 文件的副本并将其放入新目录中。

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

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

国家/地区是必填项，且必须包含两个字符。以下示例说明了这一点。

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

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

- 4 生成密钥。

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

- 5 生成证书

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

6 将证书转换为 PK12 格式。

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

7 将证书添加到 Java 密钥库 (JKS)。

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

后续步骤

现在即可导入新证书。请参见[刷新安全令牌服务证书](#)。

刷新安全令牌服务证书

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

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

解决方案用户

有效证书

其他用户

vCenter Single Sign-On 标识源中提供的用户名和密码。

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

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

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

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

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

前提条件

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

Platform Services Controller 设备

`certificate_location/keys/root-trust.jks` 例如: `/keys/root-trust.jks`

例如:

`/root/newsts/keys/root-trust.jks`

Windows 安装

`certificate_location\root-trust.jks`

例如:

`C:\Program Files\VMware\vCenter Server\jre\bin\root-trust.jks`

步骤

- 1 以 `administrator@vsphere.local` 或拥有 vCenter Single Sign-On 管理员特权的其他用户的身份登录到 vSphere Web Client。
具有 vCenter Single Sign-On 管理员特权的用户位于 `vsphere.local` 域的管理员组中。
- 2 依次选择**证书**选项卡和 **STS 签名**子选项卡，然后单击**添加 STS 签名证书**图标。
- 3 添加证书。
 - a 单击**浏览**浏览到包含新证书的密钥库 JKS 文件，然后单击**打开**。
 - b 出现提示时键入密码。
 - c 单击 STS 别名链的顶部，然后单击**确定**。
 - d 出现提示时再次键入密码。
- 4 单击**确定**。
- 5 重新启动 Platform Services Controller 节点，以启动 STS 服务和 vSphere Web Client。
重新启动之前，身份验证无法正常运行，因此必须重新启动。

确定 LDAPS SSL 证书的过期日期

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

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

步骤

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

具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。

- 2 浏览到**系统管理 > Single Sign-On > 配置**。
- 3 单击**证书**选项卡，然后单击**标识源信任库**子选项卡。
- 4 查找证书并在**有效期至**文本框中确认过期日期。

您可能会在选项卡的顶部看到一个警告，表示证书将要过期。

管理 vCenter Single Sign-On 策略

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

编辑 vCenter Single Sign-On 密码策略

vCenter Single Sign-On 密码策略是对 vCenter Single Sign-On 用户密码格式和使用期限的一组规则和限制。此密码策略仅适用于 vCenter Single Sign-On 域 (vsphere.local) 中的用户。

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

步骤

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

具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。

- 2 浏览到**管理 > Single Sign-On > 配置**。
- 3 单击**策略**选项卡，然后选择**密码策略**。
- 4 单击**编辑**。
- 5 编辑密码策略参数。

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可存在的最大天数。
限制重用	不能选择的用户之前的密码个数。例如，如果用户不能重用最近六个密码中的任何一个，则键入 6。
最大长度	允许密码包含的最大字符数。
最小长度	密码必须包含的最少字符数。最小长度不得小于字母、数字和特殊字符要求的最小总和。

选项	描述
字符要求	<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 <p>字母字符最小数目不得小于大写和小写要求的总和。</p> <p>在 vSphere 6.0 及更高版本中，密码中允许使用非 ASCII 字符。在 vCenter Single Sign-On 的早期版本中，支持的字符存在限制。</p>
相同的相邻字符数	<p>密码中允许的连续相同字符的最大个数。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>

6 单击确定。

编辑 vCenter Single Sign-On 锁定策略

vCenter Single Sign-On 锁定策略指定用户帐户锁定条件，在用户尝试使用不正确的凭据登录时，系统会依据这些条件锁定用户的 vCenter Single Sign-On 帐户。您可以编辑锁定策略。

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，您可指定最多失败登录尝试次数，以及失败尝试之间经过的时长。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 以 administrator@vsphere.local 或拥有 vCenter Single Sign-On 管理员特权的其他用户的身份登录到 vSphere Web Client。
具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。
- 2 浏览到 **系统管理 > Single Sign-On > 配置**。
- 3 单击 **策略** 选项卡，然后选择 **锁定策略**。
- 4 单击 **编辑**。
- 5 编辑参数。

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

6 单击确定。

编辑 vCenter Single Sign-On 令牌策略

vCenter Single Sign-On 令牌策略指定时钟容错、续订次数以及其他令牌属性。您可以编辑 vCenter Single Sign-On 令牌策略以确保令牌规范遵从贵公司的安全标准。

步骤

- 1 登录到 vSphere Web Client。
- 2 选择**管理 > Single Sign-On**，然后选择**配置**。
- 3 单击**策略**选项卡，然后选择**令牌策略**。

vSphere Web Client 将显示当前的配置设置。如果您未修改默认设置，vCenter Single Sign-On 将使用这些设置。

- 4 编辑令牌策略配置参数。

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

- 5 单击**确定**。

管理 vCenter Single Sign-On 用户和组

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

vCenter Single Sign-On 管理员用户可以执行以下任务。

■ 添加 vCenter Single Sign-On 用户

vSphere Web Client 的**用户**选项卡中列出的用户在 vCenter Single Sign-On 内部，属于 vsphere.local 域。

■ 禁用和启用 vCenter Single Sign-On 用户

如果禁用 vCenter Single Sign-On 用户帐户，则用户无法登录到 vCenter Single Sign-On 服务器，除非管理员启用该帐户。可从 vSphere Web Client 界面禁用和启用用户。

■ 删除 vCenter Single Sign-On 用户

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

■ 编辑 vCenter Single Sign-On 用户

您可从 vSphere Web Client 中更改 vCenter Single Sign-On 用户的密码或其他详细信息。无法在 vsphere.local 域中重命名用户。这意味着您无法重命名 administrator@vsphere.local。

■ 添加 vCenter Single Sign-On 组

在 vCenter Single Sign-On 中，**组**选项卡上列出的组在 vCenter Single Sign-On 内部。通过组可以为组成员（主要用户）集合创建容器。

■ 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 Web Client 中添加新成员。

■ 从 vCenter Single Sign-On 组中移除成员

可以通过 vSphere Web Client 从 vCenter Single Sign-On 组中移除成员。从本地组中移除某成员（用户或组）时，不是从系统中删除该成员。

■ 删除 vCenter Single Sign-On 解决方案用户

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

■ 更改 vCenter Single Sign-On 密码

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

添加 vCenter Single Sign-On 用户

vSphere Web Client 的**用户**选项卡中列出的用户在 vCenter Single Sign-On 内部，属于 vsphere.local 域。

您可以选择其他域并查看有关这些域中用户的信息，但是，您无法从 vSphere Web Client 的 vCenter Single Sign-On 管理界面将用户添加到其他域。

步骤

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

具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。

- 2 单击**主页**，然后浏览到**管理 > Single Sign-On > 用户和组**。

- 3 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。

- 4 在**用户**选项卡上，单击**新建用户**图标。
- 5 键入新用户的用户名和密码。
创建用户后，将不能更改其用户名。
密码必须符合系统的密码策略要求。
- 6 （可选）键入新用户的名字和姓氏。
- 7 （可选）输入此用户的电子邮件地址和描述。
- 8 单击**确定**。

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](#)。

禁用和启用 vCenter Single Sign-On 用户

如果禁用 vCenter Single Sign-On 用户帐户，则用户无法登录到 vCenter Single Sign-On 服务器，除非管理员启用该帐户。可从 vSphere Web Client 界面禁用和启用用户。

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

前提条件

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

步骤

- 1 以 administrator@vsphere.local 或拥有 vCenter Single Sign-On 管理员特权的其他用户的身份登录到 vSphere Web Client。
具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。
- 2 单击**主页**，然后浏览到**管理 > Single Sign-On > 用户和组**。
- 3 选择一个用户，单击**禁用**图标，然后在系统提示时单击**是**。
- 4 要再次启用此用户，请右键单击该用户，选择**启用**，然后在系统提示时单击**是**。

删除 vCenter Single Sign-On 用户

可以从 vCenter Single Sign-On 删除 vsphere.local 域中的用户。无法从 vSphere Web Client 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 以 administrator@vsphere.local 或拥有 vCenter Single Sign-On 管理员特权的其他用户的身份登录到 vSphere Web Client。

具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。

- 2 单击**主页**，然后浏览到**管理 > Single Sign-On > 用户和组**。
- 3 选择**用户**选项卡，然后选择 vsphere.local 域。
- 4 在用户列表中，选择要删除的用户，然后单击**删除**图标。

请谨慎执行后续操作。您无法撤消此操作。

编辑 vCenter Single Sign-On 用户

您可从 vSphere Web Client 中更改 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 vSphere Web Client 中查看 vCenter Single Sign-On 密码策略。作为 administrator@vsphere.local 登录并选择**配置 > 策略 > 密码策略**。

步骤

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

具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。

- 2 单击**主页**，然后浏览到**管理 > Single Sign-On > 用户和组**。
- 3 单击**用户**选项卡。
- 4 右键单击用户，然后选择**编辑用户**。

- 5 对用户进行更改。

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。

- 6 单击**确定**。

添加 vCenter Single Sign-On 组

在 vCenter Single Sign-On 中，**组**选项卡上列出的组在 vCenter Single Sign-On 内部。通过组可以为组成员（主要用户）集合创建容器。

从 vCenter Single Sign-On 管理界面添加 vSphere Web Client 组时，该组将添加到 vsphere.local 域。

步骤

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

具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。

- 2 单击**主页**，然后浏览到**管理 > Single Sign-On > 用户和组**。
- 3 选择**组**选项卡上，单击**新建组**图标。
- 4 输入组的名称和描述。

创建组后，将不能更改组名称。

- 5 单击**确定**。

后续步骤

- 向组添加成员。

向 vCenter Single Sign-On 组添加成员

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

您可以向 vCenter Single Sign-On 组添加 Microsoft Active Directory 或 OpenLDAP 组成员。不能向 vCenter Single Sign-On 组添加来自外部标识源的组。

在 vSphere Web Client 的**组**选项卡上列出的组是 vsphere.local 域的一部分。请参见 [vsphere.local 域中的组](#)。

步骤

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

具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。

- 2 单击**主页**，然后浏览到**管理 > Single Sign-On > 用户和组**。
- 3 单击**组**选项卡，然后单击组（例如“管理员”）。
- 4 在“组成员”区域中，单击**添加成员**图标。
- 5 选择包含要添加到组中的成员的标识源。
- 6 （可选）输入搜索词，然后单击**搜索**。
- 7 选择成员，然后单击**添加**。

可以同时添加多个成员。

- 8 单击**确定**。

从 vCenter Single Sign-On 组中移除成员

可以通过 vSphere Web Client 从 vCenter Single Sign-On 组中移除成员。从本地组中移除某成员（用户或组）时，不是从系统中删除该成员。

步骤

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

具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。

- 2 单击**主页**，然后浏览到**管理 > Single Sign-On > 用户和组**。
- 3 选择**组**选项卡，然后单击组。
- 4 在组成员列表中，选择要移除的用户或组，然后单击**移除成员**图标。
- 5 单击**确定**。

结果

用户将从组中移除，但在系统中仍然可用。

删除 vCenter Single Sign-On 解决方案用户

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

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

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

步骤

- 1 以 administrator@vsphere.local 或拥有 vCenter Single Sign-On 管理员特权的其他用户的身份登录到 vSphere Web Client。
- 具有 vCenter Single Sign-On 管理员特权的用户位于 vsphere.local 域的管理员组中。
- 2 单击**主页**，然后浏览到**管理 > Single Sign-On > 用户和组**。
 - 3 单击**解决方案用户**选项卡，然后单击解决方案用户名。
 - 4 单击**删除解决方案用户**图标。
 - 5 单击**是**。

结果

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

更改 vCenter Single Sign-On 密码

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

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

注 仅当密码未过期时才能更改密码。

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

步骤

- 1 在 Web 浏览器中，通过指定以下 URL 连接到 Platform Services Controller：

`https://psc_hostname_or_IP/psc`

在嵌入式部署中，Platform Services Controller 主机名或 IP 地址与 vCenter Server 主机名或 IP 地址相同。

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

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

- 3 在上方的导航窗格中“帮助”菜单的左侧，单击您的用户名以弹出下拉菜单。

除此之外，还可以选择 **Single Sign-On > 用户和组**，然后从右键菜单中选择**编辑用户**。

- 4 选择**更改密码**，然后键入您的新密码。

- 5 键入新密码并确认。

该密码必须符合密码策略。

- 6 单击**确定**。

vCenter Single Sign-On 安全性最佳做法

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

vSphere 6.0 身份验证和证书基础架构可增强 vSphere 环境的安全性。要确保该基础架构不受影响，请遵循 vCenter Single Sign-On 最佳做法。

检查密码到期

vCenter Single Sign-On 默认密码策略的密码生命周期为 90 天。90 天之后，密码过期且登录将受影响。检查是否过期并及时刷新密码。

配置 NTP

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

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

对 vCenter Single Sign-On 进行故障排除

配置 vCenter Single Sign-On 的过程可能很复杂。

以下主题提供对 vCenter Single Sign-On 进行故障排除的起始步骤。有关其他指示，请搜索此文档中心和 VMware 知识库系统。

确定 Lookup Service 错误的原因

vCenter Single Sign-On 安装显示有关 vCenter Server 或 vSphere Web Client 的错误。

问题

vCenter Server 和 Web Client 安装程序显示错误 无法联系 Lookup Service。请检查 VM_ssoreg.log... (Could not contact Lookup Service. Please check VM_ssoreg.log...)。

原因

导致该问题的原因有多种，包括主机上的时钟未同步、防火墙阻止以及必须启动的服务未启动等。

解决方案

- 1 验证运行 vCenter Single Sign-On、vCenter Server 和 Web Client 的主机上的时钟是否同步。
- 2 查看错误消息中指明的特定日志文件。

在该消息中，系统临时文件夹指的是 %TEMP%。

3 在日志文件中，搜索以下消息。

该日志文件包含所有安装尝试的输出内容。找到最后一条消息，其中显示 `Initializing registration provider...`

消息	原因和解决方案
java.net.ConnectException:连接超时: 连接	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），并且安装有 vCenter Single Sign-On 的计算机拥有足够多可用的 CPU、I/O 及 内存容量。
java.net.ConnectException:连接被拒绝: 连接	IP 地址或 FQDN 不正确，并且 vCenter Single Sign-On 服务未启动或曾经启动过，但当前已停止运行。 通过检查 vCenter Single Sign-On 服务 (Windows) 和 vmware-ssod 守护进程 (Linux) 的状态，确认 vCenter Single Sign-On 运行正常。 重新启动服务。如果这未能解决问题，请参见《vSphere 故障排除指南》的“恢复”部分。
异常状态代码: 404. 初始化期间 SSO Server 发生故障	重新启动 vCenter Single Sign-On。如果这未能解决问题，请参见《vSphere 故障排除指南》的“恢复”部分。
UI 中显示的错误，以无法连接到 vCenter Single Sign-on (Could not connect to vCenter Single Sign-on) 开头。	您还会看到返回码 <code>SslHandshakeFailed</code> 。这种错误并不常见。它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 IP 地址或 FQDN。 在 <code>%TEMP%\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 != 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 Web Client 登录 vCenter Server 组件。使用您的 Active Directory 用户名和密码。身份验证失败。

问题

可将 Active Directory 标识源添加到 vCenter Single Sign-On，但用户无法登录 vCenter Server。

原因

用户使用他们的用户名和密码登录到默认域。对于所有其他域，用户必须包含域名（`user@domain` 或 `DOMAIN\user`）。

如果使用的是 vCenter Server Appliance，则可能存在其他问题。

解决方案

对于所有 vCenter Single Sign-On 部署，您可以更改默认标识源。执行此更改后，用户只能使用用户名和密码来登录默认标识源。

要使用 Active Directory 林中的子域配置集成的 Windows 身份验证标识源，请参见 VMware 知识库文章 [2070433](#)。默认情况下，集成的 Windows 身份验证使用 Active Directory 林的根域。

如果使用的是 vCenter Server Appliance，且更改默认标识源并未解决此问题，则请执行以下额外的故障排除步骤。

- 1 同步 vCenter Server Appliance 和 Active Directory 域控制器之间的时钟。
- 2 验证每个域控制器在 Active Directory 域 DNS 服务中是否均有指针记录 (PTR)，并验证 PTR 记录信息与控制器的 DNS 名称是否匹配。使用 vCenter Server Appliance 时，可以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 controller IP address
...
```

```
# dig -x <controller IP address>
```

相关地址位于回答部分，如以下示例中所示：

```
;; ANSWER SECTION:
IP-in-reverse.in-addr.arpa. (...) IN PTR my-controller.my-ad.com
...
```

- 3 如果执行上述步骤未能解决问题，请从 Active Directory 域中移除 vCenter Server Appliance，然后重新加入域。请参见《vCenter Server Appliance 配置》文档。
- 4 关闭连接到 vCenter Server Appliance 的所有浏览器会话，然后重新启动所有服务。

```
/bin/service-control --restart --all
```

由于用户帐户被锁定，vCenter Server 登录失败

从 vSphere Web 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 Web Client。您会看到消息指明您的帐户被锁定。

原因

您已超出失败登录尝试次数上限。

解决方案

- ◆ 如果作为系统域 (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。或者，如果在密码策略中将此锁定设置为过期，则可以等待帐户解锁。vCenter Single Sign-On 管理员可使用 CLI 命令解锁您的帐户。
- ◆ 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 Platform Services Controller 实例，其中一个 Platform Services Controller 实例不可用时，环境会继续工作。Platform Services Controller 再次可用时，通常会在 60 秒内复制用户数据和其他信息。但是，在某些特殊情况下，复制可能需要较长时间。

问题

在某些情况下，例如，如果环境中包括多个位于不同位置的 Platform Services Controller 实例，并在某个 Platform Services Controller 实例不可用时进行重大更改，则无法立即查看 VMware 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 Platform Services Controller 实例的新用户。

原因

在正常操作期间，在一个 Platform Services Controller 实例（节点）上对 VMware Directory Service (vmdir) 实例所做的更改大约会在 60 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。

vSphere 组件使用 SSL 彼此进行安全通信，并与 ESXi 进行安全通信。SSL 通信可确保数据的保密性和完整性。数据将受到保护，因此在传输过程中只要遭到修改，就将被检测到。

vCenter Server 服务（如 vSphere Web Client）也使用证书对 vCenter Single Sign-On 进行初始身份验证。vCenter Single Sign-On 会为每个组件置备一个 SAML 令牌，之后组件将使用相应的 SAML 令牌进行身份验证。

在 vSphere 6.0 及更高版本中，VMware Certificate Authority (VMCA) 使用默认由 VMCA 签名的证书置备每个 ESXi 主机和每个 vCenter Server 服务。

可以将现有证书替换为新的 VMCA 签名证书，将 VMCA 设为辅助 CA，或将所有证书替换为自定义证书。您具有多个选择：

表 3-1. 不同的证书替换方法

选项	请参见
使用 Platform Services Controller Web 界面（vSphere 6.0 Update 1 及更高版本）。	使用 Platform Services Controller Web 界面 管理证书
从命令行使用 vSphere Certificate Manager 实用程序。	使用 vSphere 证书管理器实用程序 管理证书
使用 CLI 命令执行手动证书替换。	通过 CLI 命令 管理证书和服务



vSphere 证书管理

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_ejp3dqkt/uiConfId/49694343/)

本章讨论了以下主题：

- 不同解决方案途径的证书要求
- 证书管理概览
- 使用 [Platform Services Controller Web 界面](#) 管理证书
- 使用 [vSphere 证书管理器实用程序](#) 管理证书
- 手动证书替换
- 通过 [CLI 命令](#) 管理证书和服务
- 通过 [vSphere Web Client](#) 查看 vCenter 证书

- 为 vCenter 证书过期警告设置阈值

不同解决方案途径的证书要求

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

在开始之前，请确保环境中所有节点的时间都已同步。

对所有已导入证书的要求

- 密钥大小：2048 位或更大（PEM 编码）
- PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。将密钥添加到 VECS 时，它们将转换为 PKCS8。
- x509 版本 3
- SubjectAltName 必须包含 DNS Name=*machine_FQDN*
- CRT 格式
- 包含以下密钥用法：数字签名、不可否认性、密钥加密。
- 客户端身份验证和服务器身份验证不能存在于“增强型密钥用法”下。

VMCA 不支持以下证书。

- 使用通配符的证书
- 不建议使用的算法包括 md2WithRSAEncryption 1.2.840.113549.1.1.2、md5WithRSAEncryption 1.2.840.113549.1.1.4 和 sha1WithRSAEncryption 1.2.840.113549.1.1.5。
- 不支持 OID 为 1.2.840.113549.1.1.10 的算法 RSASSA-PSS。

证书符合 RFC 2253 规范

证书必须符合 RFC 2253 规范。

如果不使用证书管理器生成 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

String	X.500 AttributeType
DC	domainComponent
UID	userid

如果使用证书管理器生成 CSR，系统会提示您输入以下信息，然后证书管理器将对应的字段添加到 CSR 文件。

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

使用 VMCA 作为中间 CA 时的要求

当您将 VMCA 用作中间 CA 时，证书必须满足以下要求。

证书类型	证书要求
Root 证书	<ul style="list-style-type: none"> ■ 可以使用 vSphere 证书管理器创建 CSR。请参见使用 vSphere 证书管理器生成 CSR 并准备 root 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 位或更大 ■ PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。密钥添加到 VECS 后，会转换为 PKCS8 ■ x509 版本 3 ■ 如果您当前使用的是自定义证书，对于 root 证书，CA 扩展必须设置为 true，并且证书签名必须在要求列表中。 ■ 必须启用 CRL 签名。 ■ 增强型密钥使用不得包含客户端身份验证或服务器身份验证。 ■ 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>请参见 VMware 知识库文章 2112009《在 vSphere 6.0 中创建 Microsoft 证书颁发机构模板以创建 SSL 证书》以获取使用 Microsoft 证书颁发机构的示例。</p>
计算机 SSL 证书	<p>可以使用 vSphere 证书管理器创建 CSR，或者手动创建 CSR。</p> <p>如果您手动创建 CSR，它必须满足上面对所有已导入证书的要求下列出的要求。您还必须为主机指定 FQDN。</p>
解决方案用户证书	<p>可以使用 vSphere 证书管理器创建 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 证书管理器，该工具将提示您输入每个解决方案用户的证书信息。vSphere 证书管理器将信息存储在 certtool.cfg 中。请参见证书管理器提示输入的信息。</p>

对自定义证书的要求

当您希望使用自定义证书时，这些证书必须满足以下要求。

证书类型	证书要求
计算机 SSL 证书	<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"> ■ 您可以使用 vSphere 证书管理器生成 CSR，或手动创建 CSR。CSR 必须满足上面对导入的所有证书的要求下列出的要求。 ■ 如果使用 vSphere 证书管理器，该工具将提示您输入每个解决方案用户的证书信息。vSphere 证书管理器将信息存储在 certtool.cfg 中。请参见证书管理器提示输入的信息。 ■ 对于大多数字段，可以接受默认值或提供特定于站点的值。计算机的 FQDN 为必需值。
解决方案用户证书	<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 证书管理器生成 CSR，或自己准备 CSR。CSR 必须满足上面对导入的所有证书的要求下列出的要求。 ■ 如果使用 vSphere 证书管理器，该工具将提示您输入每个解决方案用户的证书信息。vSphere 证书管理器将信息存储在 certtool.cfg 中。请参见证书管理器提示输入的信息。 <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>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>

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

证书管理概览

新证书基础架构的影响取决于您的环境要求，取决于执行全新安装还是升级，以及考虑 ESXi 还是 vCenter Server。

未替换 VMware 证书的管理员

如果您是当前未替换 VMware 证书的管理员，VMCA 可以为您处理所有证书管理。VMCA 使用将 VMCA 用作根证书颁发机构的证书置备 vCenter Server 组件和 ESXi 主机。如果要从之前版本的 vSphere 升级到 vSphere 6，所有自签名证书都会替换为由 VMCA 签名的证书。

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证书颁发机构签名的证书或需要自定义证书信息，则管理员有以下选择。

- 将 VMCA 根证书替换为 CA 签名证书。在这种情况下，VMCA 证书是此第三方 CA 的中间证书。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，必须明确替换这些证书。可以使用 vSphere 证书管理器实用程序，或使用证书管理 CLI 执行手动证书替换。

升级使用自定义证书的环境时，可以保留某些证书。

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

在 vCenter Server 升级后，管理员可以将证书模式设置为“自定义”（请参见[更改证书模式](#)）。如果证书模式是默认的 VMCA，且用户从 vSphere Web Client 执行证书刷新，VMCA 签名证书将替换自定义证书。

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

在这种情况下，将保留现有 vCenter Server 和 vCenter Single Sign-On 证书，并将其用作计算机 SSL 证书。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，因此可能无需替换解决方案用户证书。

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

vCenter 证书界面

对于 vCenter Server，可以使用以下工具和界面查看和替换证书。

vSphere 证书管理器实用程序

从命令行执行所有常见证书替换任务。

证书管理 CLI

使用 `dir-cli`、`certool` 和 `vecs-cli` 执行所有证书管理任务。

vSphere Web Client 证书管理

查看证书，包括过期信息。

对于 ESXi，从 vSphere Web Client 执行证书管理。证书由 VMCA 置备，并且仅存储在 ESXi 主机本地，而不是 vmdir 或 VECS 中。请参见 [ESXi 主机的证书管理](#)。

受支持的 vCenter 证书

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

- 由 VMware 证书颁发机构 (VMCA) 生成和签名的证书。

- 自定义证书。
 - 从内部 PKI 生成的企业证书。
 - 由外部 PKI（如 Verisign、GoDaddy 等）生成的第三方 CA 签名证书。

使用不包含根 CA 的 OpenSSL 创建的自签名证书不受支持。

证书替换概述

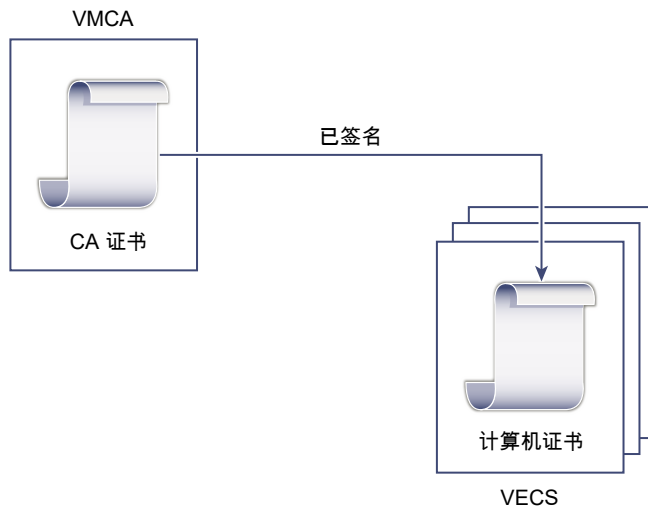
可以根据公司策略和正配置的系统的要求来执行不同类型的证书替换。可以使用 vSphere 证书管理器实用程序执行每个替换，也可以通过使用安装中包含的 CLI 手动执行每个替换。

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。

使用由 VMCA 签名的证书替换

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 根证书在十年后过期，且由 VMCA 签名的所有证书都会在根证书过期时过期，即在最多十年后过期。

图 3-1. 由 VMCA 签名的证书存储在 VECS 中

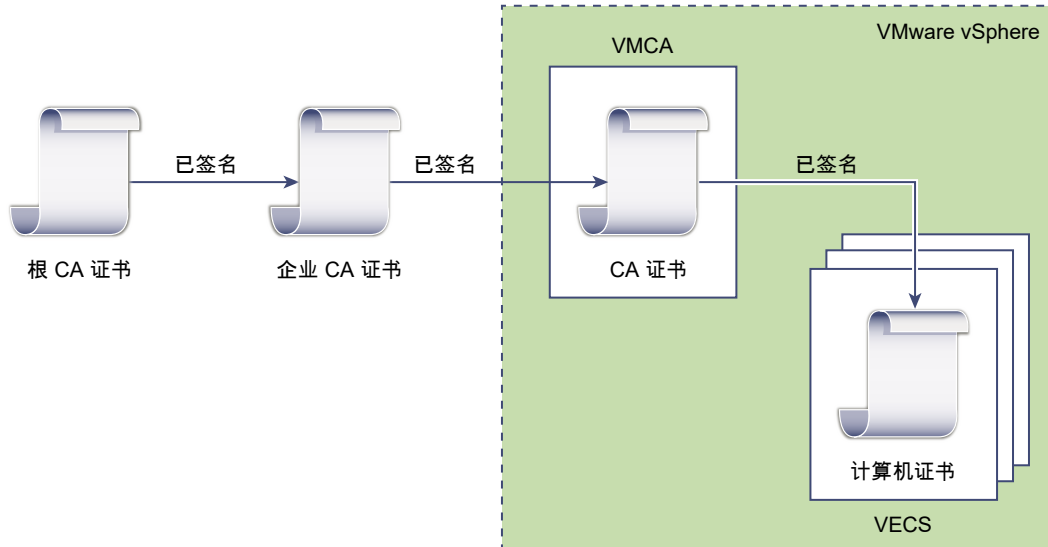


使 VMCA 成为中间 CA

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

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

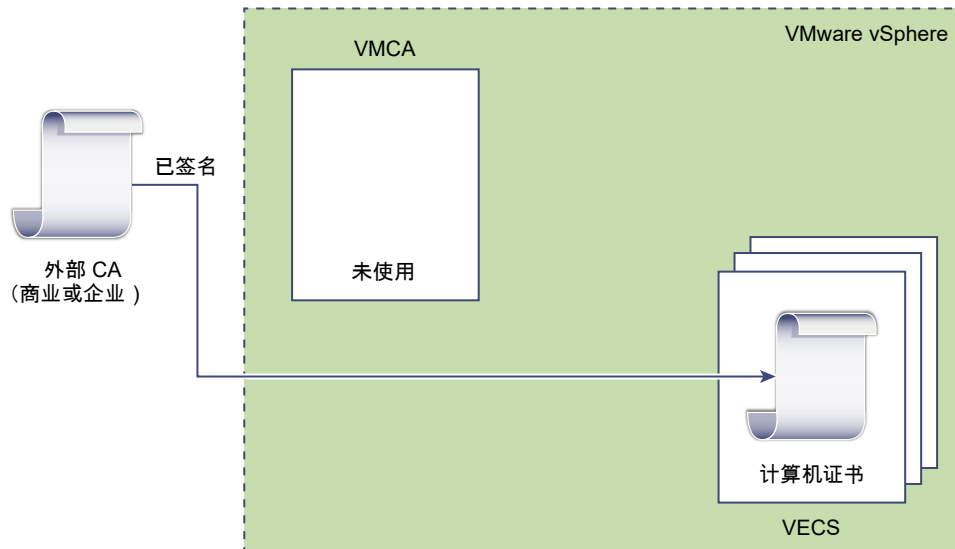
图 3-2. 由第三方或企业 CA 签名的证书使用 VMCA 作为中间 CA



不要使用 VMCA，使用自定证书进行置备

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

图 3-3. 外部证书直接存储在 VECS 中



混合部署

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

ESXi 证书替换

对于 ESXi 主机，您可以从 vSphere Web Client 更改证书置备行为。

VMware 证书颁发机构模式（默认值）

从 vSphere Web 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 6.0 用户证书的位置

在 vSphere 6.0 及更高版本中，VMware 证书颁发机构 (VMCA) 会使用证书置备您的环境。这些证书包括用于安全连接的计算机 SSL 证书，对 vCenter Single Sign-On 进行身份验证的解决方案用户证书，以及已添加到 vCenter Server 的 ESXi 主机的证书。

以下证书正在使用中。

表 3-2. vSphere 6.0 中的证书

证书	置备方式	已存储
ESXi 证书	VMCA（默认）	在 ESXi 主机本地
计算机 SSL 证书	VMCA（默认）	VECS
解决方案用户证书	VMCA（默认）	VECS
vCenter Single Sign-On SSL 签名证书	在安装期间置备。	在 vSphere Web Client 中管理此证书。 警告 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 (vmmdir) SSL 证书	在安装期间置备。	在某些个别案例中，您可能必须替换此证书。请参见 替换 VMware Directory Service 证书 。

ESXi

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

计算机 SSL 证书

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

所有服务通过反向代理进行通信。出于兼容性考虑，之前版本的 vSphere 中可用的服务也使用特定端口。例如，vpxd 服务使用 MACHINE_SSL_CERT 公开其端点。

每个节点（嵌入式部署、管理节点或 Platform Services Controller）均拥有其各自的计算机 SSL 证书。该节点上正在运行的所有服务均使用此计算机 SSL 证书公开其 SSL 端点。

计算机 SSL 证书使用情况如下：

- 由 Platform Services Controller 节点上的反向代理服务使用。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。
- 由管理节点和嵌入式节点上的 vCenter 服务 (vpxd) 使用。
- 由基础架构节点和嵌入式节点上的 VMware Directory Service (vmdir) 使用。

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

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，并通过 SAML 令牌交换使用证书对 vCenter Single Sign-On 进行身份验证。每个解决方案用户都必须对 vCenter Single Sign-On 进行身份验证。

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

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

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

- machine：由组件管理器、许可证服务器和日志记录服务使用。

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

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

此计算机库还包括在每个 Platform Services Controller 节点中。

vCenter Single Sign-On 证书

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

vCenter Single Sign-On 签名证书

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

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

可以在 vSphere Web Client 中替换此证书。请参见[刷新安全令牌服务证书](#)。

VMware Directory Service SSL 证书

如果使用的是自定义证书，可能必须明确地替换 VMware Directory Service SSL 证书。请参见[替换 VMware Directory Service 证书](#)。

VMCA 和 VMware 核心标识服务

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

VMware 核心标识服务包括多个组件。

表 3-3. 核心标识服务

服务	描述	包括在
VMware Directory Service (vmdir)	处理 SAML 证书管理以及与 vCenter Single Sign-On 一起进行身份验证。	Platform Services Controller 嵌入式部署
VMware 证书颁发机构 (VMCA)	颁发 VMware 解决方案用户的证书、正在运行服务的计算机的计算机证书以及 ESXi 主机证书。VMCA 可以立即使用或作为中间证书颁发机构。 VMCA 仅会对可以在同一域中对 vCenter Single Sign-On 进行身份验证的客户端颁发证书。	Platform Services Controller 嵌入式部署
VMware 身份验证框架守护进程 (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；内部使用其他服务。	Platform Services Controller vCenter Server 嵌入式部署

VMware Endpoint 证书存储概述

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

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

对于 TRUSTED_ROOTS 存储的更新内容，VECS 会定期轮询 VMware Directory Service (vmdir)。还可以使用 `vecs-cli` 命令显式管理 VECS 中的证书和密钥。请参见[vecs-cli 命令参考](#)。

VECS 包括以下库。

表 3-4. 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) 在嵌入式部署和每个 Platform Services Controller 节点上使用。 <p>vSphere 6.0 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>
受信任的根库 (TRUSTED_ROOTS)	包含所有受信任的根证书。
解决方案用户库 <ul style="list-style-type: none"> ■ machine ■ vpxd ■ vpxd-extensions ■ vsphere-webclient 	<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题必须是唯一的，例如计算机证书不能具有与 vpxd 证书相同的主题。</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。在嵌入式部署中，所有解决方案用户证书都位于相同的系统中。</p> <p>以下解决方案用户证书存储包括在每个管理节点和每个嵌入式部署的 VECS 中：</p> <ul style="list-style-type: none"> ■ machine：由组件管理器、许可证服务器和日志记录服务使用。 <p>注 计算机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 服务守护程序 (vpxd) 库位于管理节点和嵌入式部署上。vpxd 使用此库中存储的解决方案用户证书对 vCenter Single Sign-On 进行身份验证。 ■ vpxd-extensions：vCenter 扩展库。包括 Auto Deploy 服务、Inventory Service 以及不属于其他解决方案用户的其他服务。 ■ vsphere-webclient：vSphere Web Client 库。还包括其他一些服务，例如性能图表服务。 <p>此计算机库还包括在每个 Platform Services Controller 节点中。</p>
vSphere 证书管理器实用程序备份库 (BACKUP_STORE)	由 VMCA（VMware 证书管理器）用来支持证书恢复。仅将最近的状态存储为备份，无法返回多个步骤。
其他库	<p>解决方案可能会添加其他库。例如，虚拟卷解决方案会添加 SMS 库。请勿修改这些库中的证书，除非 VMware 文档或 VMware 知识库文章指示进行此类修改。</p> <p>注 但是，在 vSphere 6.0 中不支持 CRLS，删除 TRUSTED_ROOTS_CRLS 库可能会损坏证书基础架构。请勿删除或修改 TRUSTED_ROOTS_CRLS 库。</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 vSphere Web Client 更改令牌签名证书。

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。

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

管理证书吊销

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

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

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

大型部署中的证书替换

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

包括负载均衡器的高可用性环境中的证书替换

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

具有多个管理节点的环境中的计算机 SSL 证书替换

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

vSphere 证书管理器

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

手动证书替换

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

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

具有多个管理节点的环境中的解决方案用户证书替换

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

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

vSphere 证书管理器

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

手动证书替换

- 1 生成或请求证书。需要以下证书：
 - Platform Services Controller 上计算机解决方案用户的证书。
 - 每个管理节点上计算机解决方案用户的证书。
 - 每个管理节点上以下每个解决方案用户的证书：
 - vpxd 解决方案用户
 - vpxd-extension 解决方案用户
 - vsphere-webclient 解决方案用户
- 2 在每个节点上替换证书。确切过程取决于您将执行的证书替换类型。请参见[使用 vSphere 证书管理器实用程序管理证书](#)

有关详细信息，请参见以下主题：

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

如果公司策略要求替换所有证书，还必须替换 Platform Services Controller 上的 VMware Directory Service (vmdir) 证书。请参见[替换 VMware Directory Service 证书](#)。

在包含外部解决方案的环境中替换证书

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

您可以通过运行 `ls_update_certs` 脚本解决此问题。有关详细信息，请参见 [VMware 知识库文章 2109074](#)。

使用 Platform Services Controller Web 界面管理证书

您可以通过登录 Platform Services Controller Web 界面查看和管理证书。使用 vSphere 证书管理器实用程序或使用此 Web 界面，可以执行许多证书管理任务。

Platform Services Controller Web 界面允许执行以下管理任务。

- 查看当前的证书存储，以及添加和移除证书存储条目。
- 查看与此 Platform Services Controller 关联的 VMware Certificate Authority (VMCA) 实例。
- 查看由 VMware Certificate Authority 生成的证书。
- 续订现有证书或替换证书。

大多数证书替换 workflow 在 Platform Services Controller Web 界面中完全受支持。为了生成 CSR，可以使用 vSphere 证书管理器实用程序。

支持的工作流

安装 Platform Services Controller 后，默认情况下该节点上的 VMware Certificate Authority 为环境中的所有其他节点置备证书。可以使用以下工作流之一续订或替换证书。

续订证书

您可以让 VMCA 生成新的根证书，并从 Platform Services Controller Web 界面续订环境中的所有证书。

使 VMCA 成为中间 CA

可以使用 vSphere 证书管理器实用程序生成 CSR，编辑从 CSR 接收的证书以将 VMCA 添加到链中，然后向环境添加证书链和专用密钥。之后续订所有证书时，VMCA 将为所有计算机和解决方案用户置备由整个链签名的证书。

将证书替换为自定义证书

如果不希望使用 VMCA，可以为要替换的证书生成 CSR。CA 将为每个 CSR 返回根证书和签名证书。可以从 Platform Services Controller 上载根证书和自定义证书。

如果必须替换 VMware Directory Service (vmdir) 根证书，或者如果公司策略要求替换混合模式环境中的 vCenter Single Sign-On 证书，则可以在替换其他证书之后使用 CLI 命令替换这些证书。请参见[替换 VMware Directory Service 证书](#)和[在混合模式环境中替换 VMware Directory Service 证书](#)。

从 Platform Services Controller Web 界面浏览证书存储

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

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

前提条件

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

步骤

- 1 在 Web 浏览器中，通过指定以下 URL 连接到 Platform Services Controller:

`https://psc_hostname_or_IP/psc`

在嵌入式部署中，Platform Services Controller 主机名或 IP 地址与 vCenter Server 主机名或 IP 地址相同。

- 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“证书”下，单击**证书存储**并浏览该存储。

- 4 从下拉菜单中选择要浏览的 VMware Endpoint 证书存储 (VECS) 内部存储。

[VMware Endpoint 证书存储概述](#)介绍了各个存储中的具体内容。

- 5 要查看某证书的详细信息，请选择该证书，然后单击**显示详细信息**图标。

- 6 要删除选定存储中的条目，请单击**删除条目**图标。

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。

从 Platform Services Controller Web 界面将证书替换为新的 VMCA 签名证书

可以将所有的 VMCA 签名证书替换为新的 VMCA 签名证书；此过程称为续订证书。您可以从 Platform Services Controller Web 界面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 在 Web 浏览器中，通过指定以下 URL 连接到 Platform Services Controller:

`https://psc_hostname_or_IP/psc`

在嵌入式部署中，Platform Services Controller 主机名或 IP 地址与 vCenter Server 主机名或 IP 地址相同。

- 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“证书”下，选择**证书管理**并指定 Platform Services Controller 的主机名或 IP 地址，以及本地域的管理员（默认为 administrator@vsphere.local）用户名和密码，然后单击**提交**。
- 4 续订本地系统的计算机 SSL 证书。
 - a 单击**计算机证书**选项卡。
 - b 选择证书，单击**续订**，并在出现提示时回答**是**。
- 5 （可选）续订本地系统的解决方案用户证书。
 - a 单击**解决方案用户证书**选项卡。
 - b 选择证书并单击**续订**以续订所选的各个证书，或者单击**全部续订**以续订所有的解决方案用户证书。
 - c 在出现提示时回答**是**。
- 6 如果您的环境包括外部 Platform Services Controller，则可以续订每个 vCenter Server 系统的证书。
 - a 单击“证书管理”面板中的**注销**按钮。
 - b 出现提示时，指定 vCenter Server 系统的 IP 地址或 FQDN 以及可以向 vCenter Single Sign-On 进行身份验证的 vCenter Server 管理员的用户名和密码。
 - c 续订 vCenter Server 上的计算机 SSL 证书和（可选）每个解决方案用户证书。
 - d 如果您的环境中包含多个 vCenter Server 系统，则对每个系统重复该过程。

后续步骤

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

Windows

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

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

vCenter Server Appliance

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

通过 Platform Services Controller Web 界面将 VMCA 设为中间证书颁发机构

可以由其他 CA 签名 VMCA 证书，以便 VMCA 成为中间 CA。接下来，VMCA 生成的所有证书都将包括整个链。

可以使用 vSphere 证书管理器实用程序、使用 CLI 或从 Platform Services Controller Web 界面执行该设置。

前提条件

- 1 生成 CSR。
- 2 编辑收到的证书，并将当前 VMCA 根证书置于底部。

使用 [vSphere 证书管理器生成 CSR 并准备 root 证书（中间 CA）](#) 介绍了这两个步骤。

步骤

- 1 在 Web 浏览器中，通过指定以下 URL 连接到 Platform Services Controller:

`https://psc_hostname_or_IP/psc`

在嵌入式部署中，Platform Services Controller 主机名或 IP 地址与 vCenter Server 主机名或 IP 地址相同。

- 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 要将现有证书替换为链式证书，请按照以下步骤操作：

- a 在“证书”下，单击**证书颁发机构**，然后选择**根证书**选项卡。
- b 单击**替换证书**。添加专用密钥文件和证书文件（整个链），然后单击**确定**。
- c 在**替换根证书**对话框中，单击**浏览**并选择专用密钥，再次单击**浏览**并选择证书，然后单击**确定**。

接下来，VMCA 使用新的链式根证书对它颁发的所有证书进行签名。

- 4 续订本地系统的计算机 SSL 证书。

- a 在“证书”下，单击**证书管理**，然后单击**计算机证书**选项卡。
- b 选择证书，单击**续订**，并在出现提示时回答**是**。

VMCA 将计算机 SSL 证书替换为由新 CA 签名的证书。

- 5 （可选）续订本地系统的解决方案用户证书。

- a 单击**解决方案用户证书**选项卡。
- b 选择证书并单击**续订**以续订所选的各个证书，或者单击**全部续订**以替换所有证书并在出现提示时回答**是**。

VMCA 将该解决方案用户证书或所有解决方案用户证书替换为由新 CA 签名的证书。

- 6 如果您的环境包括外部 Platform Services Controller，则可以续订每个 vCenter Server 系统的证书。
 - a 单击“证书管理”面板中的**注销**按钮。
 - b 出现提示时，指定 vCenter Server 系统的 IP 地址或 FQDN 以及可以向 vCenter Single Sign-On 进行身份验证的 vCenter Server 管理员的用户名和密码。
 - c 续订 vCenter Server 上的计算机 SSL 证书和（可选）每个解决方案用户证书。
 - d 如果您的环境中包含多个 vCenter Server 系统，则对每个系统重复该过程。

后续步骤

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

Windows

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

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

vCenter Server Appliance

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

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

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

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

使用 vSphere 证书管理器生成证书签名请求（自定义证书）

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

可以按如下方式从命令行运行证书管理器工具：

Windows

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

Linux

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

前提条件

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

- 生成任何 CSR 时，系统会提示您输入 administrator@vsphere.local 用户的密码，或当前所连接的 vCenter Single Sign-On 域的管理员的密码。
- 如果您要在具有外部 Platform Services Controller 的环境中生成 CSR，则系统会提示您输入 Platform Services Controller 的主机名或 IP 地址。
- 要为计算机 SSL 证书生成 CSR，您需要按提示提供证书属性，这些属性存储在 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。

步骤

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

在此流程中，您还必须提供一个目录。证书管理器将证书和密钥文件放在此目录中。

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

后续步骤

执行证书替换。

将可信根证书添加到证书存储

如果要在您的环境中使用第三方证书，则必须将可信根证书添加到证书存储。

前提条件

从第三方或内部 CA 获取自定义根证书。

步骤

- 1 在 Web 浏览器中，通过指定以下 URL 连接到 Platform Services Controller:

`https://psc_hostname_or_IP/psc`

在嵌入式部署中，Platform Services Controller 主机名或 IP 地址与 vCenter Server 主机名或 IP 地址相同。

- 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“证书”下，选择**证书管理**并指定 Platform Services Controller 的主机名或 IP 地址，以及本地域的管理员（默认为 administrator@vsphere.local）用户名和密码，然后单击**提交**。

- 4 选择**可信根证书**，并单击**添加证书**。

- 5 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。

后续步骤

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

从 Platform Services Controller 添加自定义证书

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

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

前提条件

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

步骤

- 1 在 Web 浏览器中，通过指定以下 URL 连接到 Platform Services Controller:

`https://psc_hostname_or_IP/psc`

在嵌入式部署中，Platform Services Controller 主机名或 IP 地址与 vCenter Server 主机名或 IP 地址相同。

- 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“证书”下，选择**证书管理**并指定 Platform Services Controller 的主机名或 IP 地址，以及本地域的管理员（默认为 administrator@vsphere.local）用户名和密码，然后单击**提交**。
- 4 要替换计算机证书，请按照以下步骤操作：
 - a 选择**计算机证书**选项卡，然后单击要替换的证书。
 - b 单击**替换**，再单击**浏览**以替换证书链，然后单击**浏览**以替换专用密钥。
- 5 要替换解决方案用户证书，请按照以下步骤操作：
 - a 选择**解决方案用户证书**选项卡，然后单击组件四个证书中的第一个，例如 **machine**。
 - b 单击**替换**，再单击**浏览**以替换证书链，然后单击**浏览**以替换专用密钥。
 - c 对同一组件的其他三个证书重复上述过程。

后续步骤

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

Windows

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

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

vCenter Server Appliance

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

使用 vSphere 证书管理器实用程序管理证书

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

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

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

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

可以按如下方式在命令行上运行该工具：

Windows

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

Linux

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

步骤

1 通过重新发布旧证书恢复上次执行的操作

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

2 重置所有证书

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

3 重新生成新的 VMCA 根证书并替换所有证书

可以重新生成 VMCA 根证书，并将本地计算机 SSL 证书和本地解决方案用户证书替换为 VMCA 签名证书。在多节点部署中，可以在 Platform Services Controller 上运行具有此选项的 vSphere 证书管理器，然后在所有其他节点上重新运行该实用程序并选择将计算机 SSL 证书替换为 VMCA 证书和将解决方案用户证书替换为 VMCA 证书。

4 将 VMCA 设为中间证书颁发机构（证书管理器）

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

5 将所有证书替换为自定义证书（证书管理器）

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

通过重新发布旧证书恢复上次执行的操作

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

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

重置所有证书

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

使用此选项时，会覆盖当前在 VECS 中的所有自定义证书。

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

替换的证书取决于您选择的选项。

重新生成新的 VMCA 根证书并替换所有证书

可以重新生成 VMCA 根证书，并将本地计算机 SSL 证书和本地解决方案用户证书替换为 VMCA 签名证书。在多节点部署中，可以在 Platform Services Controller 上运行具有此选项的 vSphere 证书管理器，然后在所有其他节点上重新运行该实用程序并选择将计算机 SSL 证书替换为 VMCA 证书和将解决方案用户证书替换为 VMCA 证书。

运行此命令时，vSphere 证书管理器会提示您输入密码和证书信息，并将除密码之外的所有信息存储在 certool.cfg 文件中。之后，会自动执行停止服务、替换所有证书以及重新启动进程。系统会提示您输入以下信息：

- 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
- 状况
- 局部性
- 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
- Platform Services Controller 的 IP 地址（如果正在管理节点上运行该命令）

前提条件

必须了解您要生成新的 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。IP 地址是可选的。

后续步骤

在多节点部署中替换 root 证书后，必须在所有具有外部 Platform Services Controller 的 vCenter Server 节点上重新启动服务。

将 VMCA 设为中间证书颁发机构（证书管理器）

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

使用 vSphere 证书管理器生成 CSR 并准备 root 证书（中间 CA）

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

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

请参见 VMware 知识库文章 2112009 《在 vSphere 6.0 中创建 Microsoft 证书颁发机构模板以创建 SSL 证书》以获取使用 Microsoft 证书颁发机构的示例。

前提条件

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

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

步骤

- 1 启动 vSphere 证书管理器并选择选项 2。
首先，使用此选项生成 CSR，而不是替换证书。
- 2 按照提示提供密码和 Platform Services Controller 的 IP 地址或主机名。

3 选择选项 1 以生成 CSR 并按提示提供信息。

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

4 将证书发送到企业或外部 CA 进行签名，并将文件命名为 root_signing_cert.cer。

5 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-----
```

6 将文件保存为 root_signing_chain.cer。

后续步骤

将现有 root 证书替换为链式 root 证书。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](#)。

将 VMCA 根证书替换为自定义签名证书并替换所有证书

可以将 VMCA 根证书替换为在证书链中包括 VMCA 作为中间证书的 CA 签名证书。从今往后，VMCA 生成的所有证书都将包括完整链。

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

vSphere 证书管理器提示您输入以下信息：

前提条件

- 生成 CSR。
 - 可以使用 vSphere 证书管理器创建 CSR。请参见[使用 vSphere 证书管理器生成 CSR 并准备 root 证书（中间 CA）](#)
 - 如果希望手动创建 CSR，则发送以进行签名的证书必须满足以下要求：
 - 密钥大小：2048 位或更大
 - PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。密钥添加到 VECS 后，会转换为 PKCS8
 - x509 版本 3
 - 如果您当前使用的是自定义证书，对于 root 证书，CA 扩展必须设置为 true，并且证书签名必须在要求列表中。
 - 必须启用 CRL 签名。

- 增强型密钥使用不得包含客户端身份验证或服务器身份验证。
- 对证书链的长度没有明确限制。VMCA 使用 OpenSSL 默认设置，即 10 个证书。
- 不支持包含通配符或多个 DNS 名称的证书。
- 不能创建 VMCA 的附属 CA。

请参见 VMware 知识库文章 2112009《在 vSphere 6.0 中创建 Microsoft 证书颁发机构模板以创建 SSL 证书》以获取使用 Microsoft 证书颁发机构的示例。

- 从第三方或企业 CA 收到证书后，将其与初始 VMCA 根证书组合在一起以生成整个链，其中 VMCA 根证书置于底部。请参见[使用 vSphere 证书管理器生成 CSR 并准备 root 证书（中间 CA）](#)。
- 收集所需的信息。
 - administrator@vsphere.local 的密码。
 - Root 的有效自定义证书（.crt 文件）。
 - 有效的自定义根密钥（.key file）。

步骤

- 1 在嵌入式安装或外部 Platform Services Controller 上启动 vSphere 证书管理器，然后选择选项 2。
- 2 选择选项 2 开始证书替换并根据提示提供信息。
 - a 出现提示后指定根证书的完整路径。
 - 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。
- 3 如果在多节点部署中替换根证书，则必须在所有 vCenter Server 上重新启动服务。
- 4 在多节点部署中，使用选项 3（“将计算机 SSL 证书替换为 VMCA 证书”）和 6（“将解决方案用户证书替换为 VMCA 证书”）在每个 vCenter Server 实例上重新生成所有证书。

替换证书时，VMCA 会通过整个链进行签名。

后续步骤

根据您的环境，您可能必须明确替换其他证书。

- 如果公司策略要求替换所有证书，请替换 vmdir 根证书。请参见[替换 VMware Directory Service 证书](#)
- 如果从 vSphere 5.x 环境升级，可能必须替换 vmdir 中的 vCenter Single Sign-On 证书。请参见在[混合模式环境中替换 VMware Directory Service 证书](#)

将计算机 SSL 证书替换为 VMCA 证书（中间 CA）

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

将现有计算机 SSL 证书替换为新的 VMCA 签名证书时，vSphere 证书管理器会提示您输入信息，并将除 Platform Services Controller 密码和 IP 地址以外的所有值输入到 `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
- 状况
- 局部性
- IP 地址（可选）
- 电子邮件
- 主机名，即要替换证书的计算机的完全限定域名。如果主机名与 FQDN 不匹配，则证书替换无法正确完成，且环境可能最终会处于不稳定状态。
- Platform Services Controller 的 IP 地址（如果正在管理节点上运行该命令）

前提条件

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

步骤

- 1 启动 vSphere 证书管理器并选择选项 3。
- 2 对提示做出响应。

证书管理器将信息存储在 `certtool.cfg` 文件中。

结果

vSphere 证书管理器替换计算机 SSL 证书。

将解决方案用户证书替换为 VMCA 证书（中间 CA）

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

前提条件

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

步骤

- 1 启动 vSphere 证书管理器并选择选项 6。
- 2 对提示做出响应。

结果

vSphere 证书管理器替换所有解决方案用户证书。

将所有证书替换为自定义证书（证书管理器）

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

一个方法是仅使用 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，需要使用自定义证书置备添加到环境中的每个节点。VMCA 仍使用 VMCA 签名证书，您需要替换这些证书。您可以使用 vSphere 证书管理器实用程序，或使用 CLI 执行手动证书替换。证书存储在 VECS 中。

使用 vSphere 证书管理器生成证书签名请求（自定义证书）

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

可以按如下方式从命令行运行证书管理器工具：

Windows

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

Linux

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

前提条件

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

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

- 如果您要在具有外部 Platform Services Controller 的环境中生成 CSR，则系统会提示您输入 Platform Services Controller 的主机名或 IP 地址。
- 要为计算机 SSL 证书生成 CSR，您需要按提示提供证书属性，这些属性存储在 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。

步骤

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

在此流程中，您还必须提供一个目录。证书管理器将证书和密钥文件放在此目录中。

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

后续步骤

执行证书替换。

将计算机 SSL 证书替换为自定义证书

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

前提条件

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

- 1 要使用 vSphere 证书管理器生成 CSR，请参见[使用 vSphere 证书管理器生成证书签名请求（自定义证书）](#)。
- 2 要明确生成 CSR，请从第三方或企业 CA 为每个计算机请求一个证书。证书必须满足以下要求：
 - 密钥大小：2048 位或更大（PEM 编码）
 - CRT 格式
 - x509 版本 3
 - SubjectAltName 必须包含 DNS Name=<machine_FQDN>

- 包含以下密钥使用：数字签名、不可否认性、密钥加密

另请参见 VMware 知识库文章 [2112014](#)，从 [Microsoft](#) 证书颁发机构获取 vSphere 证书。

步骤

- 1 启动 vSphere 证书管理器并选择选项 1。
- 2 选择选项 2 开始证书替换并根据提示提供信息。

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

后续步骤

根据您的环境，您可能必须明确替换其他证书。

- 如果公司策略要求替换所有证书，请替换 vmdir 根证书。请参见[替换 VMware Directory Service 证书](#)
- 如果从 vSphere 5.x 环境升级，可能必须替换 vmdir 中的 vCenter Single Sign-On 证书。请参见在[混合模式环境中替换 VMware Directory Service 证书](#)

将解决方案用户证书替换为自定义证书

许多公司仅要求替换可从外部进行访问的服务的证书。但是，证书管理器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 Web Client 关联的所有服务。在多节点部署中，替换 Platform Services Controller 上的计算机解决方案用户证书，以及每个管理节点上的整组解决方案用户。

当提示您输入解决方案用户证书时，请提供第三方 CA 的完整签名证书链。

格式应类似于以下内容。

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

前提条件

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

- 1 要使用 vSphere 证书管理器生成 CSR，请参见使用 [vSphere 证书管理器生成证书签名请求（自定义证书）](#)。
- 2 从第三方或企业 CA 为每个节点上的每个解决方案用户请求一个证书。您可以使用 vSphere 证书管理器生成 CSR 或自己准备 CSR。CSR 必须满足以下要求：
 - 密钥大小：2048 位或更大（PEM 编码）
 - CRT 格式
 - x509 版本 3
 - SubjectAltName 必须包含 DNS Name=<machine_FQDN>
 - 每个解决方案用户证书必须具有不同的 Subject。例如，考虑包含解决方案用户名（如 vpxd）或其他唯一标识符。
 - 包含以下密钥使用：数字签名、不可否认性、密钥加密

另请参见 VMware 知识库文章 [2112014](#)，从 [Microsoft](#) 证书颁发机构获取 vSphere 证书。

步骤

- 1 启动 vSphere 证书管理器并选择选项 5。
- 2 选择选项 2 开始证书替换并根据提示提供信息。

vSphere 证书管理器提示您输入以下信息：

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

后续步骤

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

手动证书替换

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

了解启动和停止服务

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

请遵循以下经验规则。

- 请勿停止服务以生成新公用/专用密钥对新证书。
- 如果您是唯一的管理员，则在添加新根证书时无需停止服务。旧根证书仍然可用，并且所有服务仍使用该证书进行身份验证。在添加根证书后停止并立即重新启动所有服务，以避免主机出现问题。
- 如果您的环境包括多个管理员，则在添加新根证书之前停止服务，并在添加新证书后重新启动服务。
- 请先停止服务，然后再执行以下任务：
 - 在 VECS 中删除计算机 SSL 证书或任何解决方案用户证书。
 - 替换 vmdir (VMware Directory Service) 中的解决方案用户证书。

将现有 VMCA 签名证书替换为新的 VMCA 签名证书

如果 VMCA 根证书在不久的将来会过期或者出于其他原因需要替换该证书，则可以生成新的根证书并将其添加到 VMware Directory Service。然后，可以使用新的根证书生成新的计算机 SSL 证书和解决方案用户证书。

大多数情况下，可以使用 vSphere 证书管理器实用程序替换证书。

如果需要精细控制，则此方案会为使用 CLI 命令替换一组完整的证书提供详细的分步说明。但是，也可以使用对应的任务中的步骤仅单独替换各个证书。

前提条件

仅有 administrator@vsphere.local 或 CAAdmins 组中的其他用户可以执行证书管理任务。请参见向 [vCenter Single Sign-On 组添加成员](#)。

步骤

1 生成新的 VMCA 签名根证书

使用 certool CLI 生成新的 VMCA 签名证书并将其发布到 vmdir。

2 将计算机 SSL 证书替换为 VMCA 签名证书

在生成新的 VMCA 签名根证书后，可以替换您环境中的所有计算机 SSL 证书。

3 将解决方案用户证书替换为新的 VMCA 签名证书

替换完计算机 SSL 证书后，可以替换所有解决方案用户证书。解决方案用户证书必须有效（即，不能过期），但证书中的其他所有信息可供证书基础架构使用。

4 在混合模式环境中替换 VMware Directory Service 证书

在升级过程中，您的环境可能暂时包括 vCenter Single Sign-On 版本 5.5 和 vCenter Single Sign-On 版本 6.x。在此情况下，如果替换正在运行 vCenter Single Sign-On 服务的节点的 SSL 证书，则必须执行其他步骤才能替换 VMware Directory Service SSL 证书。

生成新的 VMCA 签名根证书

使用 certool CLI 生成新的 VMCA 签名证书并将其发布到 vmdir。

在多节点部署中，在 Platform Services Controller 上运行根证书生成命令。

步骤

- 1 生成新的自签名证书和专用密钥。

```
certool --genselfcacert --outprivkey <key_file_path> --outcert <cert_file_path> --config <config_file>
```

- 2 将现有根证书替换为新证书。

```
certool --rootca --cert <cert_file_path> --privkey <key_file_path>
```

该命令会生成证书，将其添加到 vmdir，然后将其添加到 VECS。

- 3 停止所有服务，启动处理证书创建、传播和存储的服务。

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

Windows

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

vCenter Server Appliance

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

运行此命令时，会立即更新 vmdir 的所有实例。另外，传播到所有实例可能需要一些时间。

- 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 信息和生成根证书的一组完整步骤。

- 1 （可选）列出 VMCA 根证书以确保其位于证书存储中。

- 在 Platform Services Controller 节点或嵌入式安装中：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca
```

- 在管理节点（外部安装）中：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --getrootca --server=<psc-  
ip-or-fqdn>
```

输入类似于以下内容：

```
output:  
Certificate:  
Data:  
Version:3 (0x2)  
Serial Number:  
cf:2d:ff:49:88:50:e5:af  
...
```

- 2 （可选）列出 VECS TRUSTED_ROOTS 库，并将证书序列号与步骤 1 中输出的序列号进行比较。

此命令可在 Platform Services Controller 和管理节点上运行，因为 VECS 会轮询 vmdir。

```
"C:\Program Files\VMware\vCenter Server\vmaddd\"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。将证书添加到 VECS 和 vmdir（VMware Directory Service）中的 TRUSTED_ROOTS 库。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --selfca --config="C:\Program  
Files\VMware\vCenter Server\vmcad\certool.cfg"
```

在 Windows 中，可以选择 --config，因为该命令使用默认的 certool.cfg 文件。

将计算机 SSL 证书替换为 VMCA 签名证书

在生成新的 VMCA 签名根证书后，可以替换您环境中的所有计算机 SSL 证书。

每台计算机都必须拥有可用于与其他服务进行安全通信的计算机 SSL 证书。在多节点部署中，必须在每个节点上运行计算机 SSL 证书生成命令。使用 `--server` 参数从具有外部 Platform Services Controller 的 vCenter Server 指向 Platform Services Controller。

前提条件

准备好停止所有服务，启动处理证书传播和存储的服务。

步骤

- 1 为需要新证书的每台计算机复制一份 `certtool.cfg`。

可以在以下位置找到 `certtool.cfg`：

操作系统	路径
Windows	C:\Program Files\VMware\vCenter Server\vmcad
Linux	/usr/lib/vmware-vmca/share/config/

- 2 编辑每台计算机的自定义配置文件以包括该计算机的 FQDN。

对计算机的 IP 地址运行 `NSLookup`，以查看名称的 DNS 列表，并在文件的“主机名”字段中使用该名称。

- 3 为每个文件生成公用/专用密钥文件对和证书，通过刚刚自定义的配置文件进行传递。

例如：

```
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。

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

Windows

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

vCenter Server Appliance

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

5 将新证书添加到 VECS。

所有计算机都需要本地证书存储中的新证书来通过 SSL 进行通信。首先删除现有条目，然后添加新条目。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert machine1.cert
--key machine1.priv
```

6 重新启动所有服务。

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

示例：将计算机证书替换为 VMCA 签名证书

1 为 SSL 证书创建配置文件，并在当前目录中将其保存为 ssl-config.cfg。

```
Country = US
Name = vmca-<PSC-FQDN-example>
Organization = <my_company>
OrgUnit = <my_company Engineering>
State = <my_state>
Locality = <mytown>
Hostname = <FQDN>
```

2 为计算机 SSL 证书生成密钥对。在每个管理节点和 Platform Services Controller 节点上运行此命令；不需要 --server 选项。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

将在当前目录中创建 ssl-key.priv 和 ssl-key.pub 文件。

3 生成新的计算机 SSL 证书。此证书为 VMCA 签名证书。如果将 VMCA 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。

■ 在 Platform Services Controller 节点或嵌入式安装中：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

■ 在 vCenter Server 中（外部安装）：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

将在当前目录中创建 new-vmca-ssl.crt 文件。

4 （可选）列出 VECS 的内容。

```
"C:\Program Files\VMware\Center Server\vmadd\"vecs-cli store list
```

- Platform Services Controller 中的输出:

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- vCenter Server 中的输出:

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

5 将 VECS 中的计算机 SSL 证书替换为新的计算机 SSL 证书。--store 和 --alias 值必须与默认名称完全匹配。

- 在 Platform Services Controller 中，请运行以下命令以更新 MACHINE_SSL_CERT 存储中的计算机 SSL 证书。

```
C:\>"C:\Program Files\VMware\Center Server\vmadd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\Center Server\vmadd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- 在每个管理节点或嵌入式部署中，请运行以下命令以更新 MACHINE_SSL_CERT 存储中的计算机 SSL 证书。由于每个计算机具有不同的 FQDN，因此必须单独更新每个计算机的证书。

```
C:\>"C:\Program Files\VMware\Center Server\vmadd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\Center Server\vmadd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

后续步骤

您还可以替换 ESXi 主机的证书。请参见《vSphere 安全性》出版物。

在多节点部署中替换 root 证书后，必须在所有具有外部 Platform Services Controller 的 vCenter Server 节点上重新启动服务。

将解决方案用户证书替换为新的 VMCA 签名证书

替换完计算机 SSL 证书后，可以替换所有解决方案用户证书。解决方案用户证书必须有效（即，不能过期），但证书中的其他所有信息可供证书基础架构使用。

替换每个管理节点和每个 Platform Services Controller 节点上的计算机解决方案用户证书。只能替换每个管理节点上的其他解决方案用户证书。在具有外部 Platform Services Controller 的管理节点上运行命令时，请使用 `--server` 参数指向 Platform Services Controller。

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

前提条件

准备好停止所有服务，启动处理证书传播和存储的服务。

步骤

- 1 复制一份 `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`。

您可以从命令行以生成的一部分命名证书。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。

```
C:\Program Files\VMware\vCenter Server\vmadd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

在多节点部署中列出解决方案用户证书时，`dir-cli` 列表输出将包含所有节点的所有解决方案用户。运行 `vmafd-cli get-machine-id --server-name localhost` 以查找每个主机的本地计算机 ID。每个解决方案用户名称均包括计算机 ID。

- 4 停止所有服务，启动处理证书创建、传播和存储的服务。

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

Windows

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

vCenter Server Appliance

```
service-control --stop --all
service-control --start 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 vpxd 服务的证书。

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

注 如果不替换 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 为每个解决方案用户生成公用/专用密钥对。其中包括每个 Platform Services Controller 和每个管理节点上的计算机解决方案用户的密钥对和每个管理节点上的每个其他解决方案用户（vpxd、vpxd-extension、vsphere-webclient）的密钥对。
 - a 为嵌入式部署的计算机解决方案用户或 Platform Services Controller 的计算机解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- b （可选）对于使用外部 Platform Services Controller 的部署，请为每个管理节点上的计算机解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```


- c 为每个管理节点上的 **vpzd** 解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --genkey --privkey=vpzd-key.priv --pubkey=vpzd-key.pub"
```

- d 为每个管理节点上的 **vpzd-extension** 解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --genkey --privkey=vpzd-extension-key.priv --pubkey=vpzd-extension-key.pub"
```

- e 为每个管理节点上的 **vsphere-webclient** 解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub"
```

- 2 为每个 **Platform Services Controller** 和每个管理节点上的计算机解决方案用户以及每个管理节点上的每个其他解决方案用户 (**vpzd**、**vpzd-extension**、**vsphere-webclient**) 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，例如，**vpzd** 或 **vpzd-extension**，可便于查看证书与解决方案用户之间的映射关系。

- a 在 **Platform Services Controller** 节点上运行以下命令可为该节点上的计算机解决方案用户生成解决方案用户证书。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine"
```

- b 为每个管理节点上的计算机解决方案用户生成证书。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>"
```

- c 为每个管理节点上的 **vpzd** 解决方案用户生成证书。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-vpzd.crt --privkey=vpzd-key.priv --Name=vpzd --server=<psc-ip-or-fqdn>"
```

- d 为每个管理节点上的 **vpzd-extensions** 解决方案用户生成证书。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-vpzd-extension.crt --privkey=vpzd-extension-key.priv --Name=vpzd-extension --server=<psc-ip-or-fqdn>"
```

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

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>"
```

3 将 VECS 中的解决方案用户证书替换为新的解决方案用户证书。

注 --store 和 --alias 参数必须与服务的默认名称完全匹配。

- a 在 Platform Services Controller 节点上，请运行以下命令以替换计算机解决方案用户证书：

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

- b 替换每个管理节点上的计算机解决方案用户证书：

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

- c 替换每个管理节点上的 vpxd 解决方案用户证书。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd --alias vpxd
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

- d 替换每个管理节点上的 vpxd-extension 解决方案用户证书。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

- e 替换每个管理节点上的 vsphere-webclient 解决方案用户证书。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

4 使用新的解决方案用户证书更新 VMware Directory Service (vmdir)。系统将提示您输入 vCenter Single Sign-On 管理员密码。

- a 运行 dir-cli service list 可获取每个解决方案用户的唯一服务 ID 后缀。可以在 Platform Services Controller 或 vCenter Server 系统上运行此命令。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
```

```

2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69

```

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

- b 在 Platform Services Controller 上替换 `vmdir` 中的计算机证书。例如，如果 `machine-29a45d00-60a7-11e4-96ff-00505689639a` 为 Platform Services Controller 中的计算机解决方案用户，请运行此命令：

```
C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\dir-cli service update --name machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt
```

- c 替换每个管理节点上的 `vmdir` 中的计算机证书。例如，如果 `machine-6fd7f140-60a9-11e4-9e28-005056895a69` 为 vCenter Server 中的计算机解决方案用户，请运行此命令：

```
C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\dir-cli service update --name machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt
```

- d 替换每个管理节点上的 `vmdir` 中的 `vpxd` 解决方案用户证书。例如，如果 `vpxd-6fd7f140-60a9-11e4-9e28-005056895a69` 为 `vpxd` 解决方案用户 ID，请运行此命令：

```
C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\dir-cli service update --name vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt
```

- e 替换每个管理节点上的 `vmdir` 中的 `vpxd-extension` 解决方案用户证书。例如，如果 `vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69` 为 `vpxd-extension` 解决方案用户 ID，请运行此命令：

```
C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\dir-cli service update --name vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt
```

- f 替换每个管理节点上的 `vsphere-webclient` 解决方案用户证书。例如，如果 `vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69` 为 `vsphere-webclient` 解决方案用户 ID，请运行此命令：

```
C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\dir-cli service update --name vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt
```

后续步骤

重新启动每个 Platform Services Controller 节点和每个管理节点上的所有服务。

在混合模式环境中替换 VMware Directory Service 证书

在升级过程中，您的环境可能暂时包括 vCenter Single Sign-On 版本 5.5 和 vCenter Single Sign-On 版本 6.x。在此情况下，如果替换正在运行 vCenter Single Sign-On 服务的节点的 SSL 证书，则必须执行其他步骤才能替换 VMware Directory Service SSL 证书。

vmdir 使用 VMware Directory Service SSL 证书可在执行 vCenter Single Sign-On 复制的 Platform Services Controller 节点之间执行握手操作。

同时包括 vSphere 6.0 和 vSphere 6.5 节点的混合模式环境不需要执行这些步骤。仅在以下情况下需要执行这些步骤：

- 环境中同时包括 vCenter Single Sign-On 5.5 和 vCenter Single Sign-On 6.x 服务。
- vCenter Single Sign-On 服务设置为复制 vmdir 数据。
- 对于运行 vCenter Single Sign-On 6.x 服务的节点，计划将默认 VMCA 签名证书替换为自定义证书。

注 最佳做法是在重新启动服务之前先升级整个环境。通常不建议替换 VMware Directory Service 证书。

步骤

- 1 在运行 vCenter Single Sign-On 6.x 服务的节点上，替换 vmdird SSL 证书和密钥。
请参见[替换 VMware Directory Service 证书](#)。
- 2 在运行 vCenter Single Sign-On 5.5 服务的节点上，请先设置环境以便熟悉 vCenter Single Sign-On 6.x 服务。
 - a 备份所有文件 C:\ProgramData\VMware\CIS\cfg\vmdird。
 - b 在 6.x 节点上创建 vmdircert.pem 文件的副本，并将其重命名为 <sso_node2.domain.com>.pem，其中 <sso_node2.domain.com> 是 6.x 节点的 FQDN。
 - c 将重命名的证书复制到 C:\ProgramData\VMware\CIS\cfg\vmdird 以替换现有的复制证书。
- 3 在已替换证书的所有计算机上重新启动 VMware Directory Service。
可以从 vSphere Web Client 中重新启动服务或使用 service-control 命令。

使用 VMCA 作为中间证书颁发结构

可以将 VMCA 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。此方法将结合第三方 CA 签名证书的安全性和自动证书管理的便捷性。

步骤

- 1 [替换根证书（中间 CA）](#)
将 VMCA 证书替换为自定义证书的第一步是生成 CSR 并添加作为根证书返回到 VMCA 的证书。
- 2 [替换计算机 SSL 证书（中间 CA）](#)
当您收到 CA 的签名证书并使其成为 VMCA 根证书后，您可以替换所有计算机 SSL 证书。

3 替换解决方案用户证书（中间 CA）

在替换计算机 SSL 证书后，可以替换解决方案用户证书。

4 替换 VMware Directory Service 证书

如果决定使用新的 VMCA 根证书，并且取消发布在置备环境中已使用的 VMCA 根证书，则必须替换计算机 SSL 证书、解决方案用户证书和某些内部服务的证书。

5 在混合模式环境中替换 VMware Directory Service 证书

在升级过程中，您的环境可能暂时包括 vCenter Single Sign-On 版本 5.5 和 vCenter Single Sign-On 版本 6.x。在此情况下，如果替换正在运行 vCenter Single Sign-On 服务的节点的 SSL 证书，则必须执行其他步骤才能替换 VMware Directory Service SSL 证书。

替换根证书（中间 CA）

将 VMCA 证书替换为自定义证书的第一步是生成 CSR 并添加作为根证书返回到 VMCA 的证书。

您发送以进行签名的证书必须满足以下要求：

- 密钥大小：2048 位或更大
- PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。密钥添加到 VECS 后，会转换为 PKCS8
- x509 版本 3
- 如果您当前使用的是自定义证书，对于 root 证书，CA 扩展必须设置为 true，并且证书签名必须在要求列表中。
- 必须启用 CRL 签名。
- 增强型密钥使用不得包含客户端身份验证或服务器身份验证。
- 对证书链的长度没有明确限制。VMCA 使用 OpenSSL 默认设置，即 10 个证书。
- 不支持包含通配符或多个 DNS 名称的证书。
- 不能创建 VMCA 的附属 CA。

请参见 VMware 知识库文章 2112009《在 vSphere 6.0 中创建 Microsoft 证书颁发机构模板以创建 SSL 证书》以获取使用 Microsoft 证书颁发机构的示例。

替换根证书时，VMCA 会验证以下证书属性：

- 密钥大小：2048 位或更多
- 密钥用法：证书签名
- 基本限制：主题类型 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 rootcal.crt。

可以通过将 PEM 格式的所有 CA 证书复制到单个文件完成此过程。必须以 VMCA 根证书开头，并以根 CA PEM 证书结尾。例如：

```
-----BEGIN CERTIFICATE-----
<Certificate of VMCA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of intermediary CA>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Certificate of Root CA>
-----END CERTIFICATE-----
```

- 3 停止所有服务，启动处理证书创建、传播和存储的服务。

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

Windows

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

vCenter Server Appliance

```
service-control --stop --all
service-control --start 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证书位置。
- 将自定义根证书附加到 VECS 中的 TRUSTED_ROOTS 库中（延迟后）。
- 将自定义根证书附加到 vmdird（延迟后）。

- 5 （可选）要将更改传播到 vmdird（VMware Directory Service）的所有实例，请将新根证书发布到 vmdird，并提供每个文件的完整文件路径。

例如：

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

每 30 秒进行一次 `vmdir` 节点之间的复制。无需将根证书显式添加到 VECS，因为 VECS 会每 5 分钟轮询 `vmdir` 中的新根证书文件。

- 6 （可选）如有必要，可以强制刷新 VECS。

```
vecs-cli force-refresh
```

- 7 重新启动所有服务。

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

示例：替换根证书

使用 `certool` 命令和 `--rootca` 选项将 VMCA 根证书替换为自定义 CA 根证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\certool" --rootca --cert=C:\custom-  
certs\root.pem --privkey=C:\custom-certs\root.key
```

运行此命令时，会执行以下操作：

- 将新的自定义根证书添加到文件系统中的证书位置。
- 将自定义根证书附加到 VECS 中的 TRUSTED_ROOTS 库中。
- 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。如果移除了该根证书，必须刷新这些内部证书：

- 替换 vCenter Single Sign-On 签名证书。请参见[刷新安全令牌服务证书](#)。
- 替换 VMware Directory Service 证书。请参见[替换 VMware Directory Service 证书](#)。

替换计算机 SSL 证书（中间 CA）

当您收到 CA 的签名证书并使其成为 VMCA 根证书后，您可以替换所有计算机 SSL 证书。

这些步骤实际上与替换为使用 VMCA 作为证书颁发机构的证书的步骤相同。但是，在这种情况下，VMCA 会对整个链中的所有证书进行签名。

每台计算机都必须拥有可用于与其他服务进行安全通信的计算机 SSL 证书。在多节点部署中，必须在每个节点上运行计算机 SSL 证书生成命令。使用 `--server` 参数从具有外部 Platform Services Controller 的 vCenter Server 指向 Platform Services Controller。

前提条件

对于每个计算机 SSL 证书，SubjectAltName 必须包含 DNS Name=<Machine FQDN>。

步骤

- 1 为需要新证书的每台计算机复制一份 `certtool.cfg`。

可以在以下位置找到 `certtool.cfg`:

Windows

`C:\Program Files\VMware\vCenter Server\vmcad`

Linux

`/usr/lib/vmware-vmca/share/config/`

- 2 编辑每台计算机的自定义配置文件以包括该计算机的 FQDN。

对计算机的 IP 地址运行 `NSLookup`，以查看名称的 DNS 列表，并在文件的“主机名”字段中使用该名称。

- 3 传递刚自定义的配置文件为每个计算机生成公用/专用密钥文件对。

例如:

```
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。

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

Windows

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

vCenter Server Appliance

```
service-control --stop --all
service-control --start 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-<PSC-FQDN-example>
Organization = VMware
OrgUnit = VMware Engineering
State = California
Locality = Palo Alto
Hostname = <FQDN>
```

- 2 为计算机 SSL 证书生成密钥对。在每个管理节点和 Platform Services Controller 节点上运行此命令；不需要 `--server` 选项。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --genkey --privkey=ssl-key.priv
--pubkey=ssl-key.pub
```

将在当前目录中创建 `ssl-key.priv` 和 `ssl-key.pub` 文件。

- 3 生成新的计算机 SSL 证书。此证书为 VMCA 签名证书。如果将 VMCA 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。

- 在 Platform Services Controller 节点或嵌入式安装中：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg
```

- 在 vCenter Server 中（外部安装）：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmcad\"certool --gencert --cert=new-vmca-ssl.crt --privkey=ssl-key.priv --config=ssl-config.cfg --server=<psc-ip-or-fqdn>
```

将在当前目录中创建 `new-vmca-ssl.crt` 文件。

- 4 （可选）列出 VECS 的内容。

```
"C:\Program Files\VMware\vCenter Server\vmaddd\"vecs-cli store list
```

- Platform Services Controller 中的输出：

```
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
```

- vCenter Server 中的输出：

```
output (on vCenter):
MACHINE_SSL_CERT
TRUSTED_ROOTS
TRUSTED_ROOT_CRLS
machine
vpxd
vpxd-extension
vsphere-webclient
sms
```

5 将 VECS 中的计算机 SSL 证书替换为新的计算机 SSL 证书。--store 和 --alias 值必须与默认名称完全匹配。

- 在 Platform Services Controller 中，请运行以下命令以更新 MACHINE_SSL_CERT 存储中的计算机 SSL 证书。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

- 在每个管理节点或嵌入式部署中，请运行以下命令以更新 MACHINE_SSL_CERT 存储中的计算机 SSL 证书。由于每个计算机具有不同的 FQDN，因此必须单独更新每个计算机的证书。

```
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
C:\>"C:\Program Files\VMware\ vCenter Server\vmafdd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert new-vmca-ssl.crt --key ssl-key.priv
```

后续步骤

您还可以替换 ESXi 主机的证书。请参见《vSphere 安全性》出版物。

在多节点部署中替换 root 证书后，必须在所有具有外部 Platform Services Controller 的 vCenter Server 节点上重新启动服务。

替换解决方案用户证书（中间 CA）

在替换计算机 SSL 证书后，可以替换解决方案用户证书。

替换每个管理节点和每个 Platform Services Controller 节点上的计算机解决方案用户证书。只能替换每个管理节点上的其他解决方案用户证书。在具有外部 Platform Services Controller 的管理节点上运行命令时，请使用 --server 参数指向 Platform Services Controller。

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

前提条件

每个解决方案用户证书必须具有不同的 Subject。例如，考虑包含解决方案用户名（如 **vpzd**）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`。

您可以从命令行生成的一部分命名证书。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=vpzd.priv --pubkey=vpzd.pub
certtool --gencert --privkey=vpzd.priv --cert vpzd.crt --Name=VPXD_1 --config sol_usr.cfg
```

- 3 查找每个解决方案用户的名称。

```
dir-cli service list
```

可以使用替换证书时返回的唯一 ID。输入和输出可能显示如下。

```
C:\Program Files\VMware\vCenter Server\vmafd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpzd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpzd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

在多节点部署中列出解决方案用户证书时，`dir-cli` 列表输出将包含所有节点的所有解决方案用户。运行 `vmafd-cli get-machine-id --server-name localhost` 以查找每个主机的本地计算机 ID。每个解决方案用户名称均包括计算机 ID。

- 4 停止所有服务，启动处理证书创建、传播和存储的服务。

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

Windows

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

vCenter Server Appliance

```
service-control --stop --all
service-control --start 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 <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登录到 vCenter Single Sign-On。

- 6 重新启动所有服务。

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

示例：替换解决方案用户证书（中间 CA）

- 1 为每个解决方案用户生成公用/专用密钥对。其中包括每个 Platform Services Controller 和每个管理节点上的计算机解决方案用户的密钥对和每个管理节点上的每个其他解决方案用户（vpzd、vpzd-extension、vsphere-webclient）的密钥对。
 - a 为嵌入式部署的计算机解决方案用户或 Platform Services Controller 的计算机解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\VCServer\vmcad\certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- b （可选）对于使用外部 Platform Services Controller 的部署，请为每个管理节点上的计算机解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\VCServer\vmcad\certool --genkey --privkey=machine-key.priv --pubkey=machine-key.pub
```

- c 为每个管理节点上的 **vpzd** 解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --genkey --privkey=vpzd-key.priv --pubkey=vpzd-key.pub"
```

- d 为每个管理节点上的 **vpzd-extension** 解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --genkey --privkey=vpzd-extension-key.priv --pubkey=vpzd-extension-key.pub"
```

- e 为每个管理节点上的 **vsphere-webclient** 解决方案用户生成密钥对。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --genkey --privkey=vsphere-webclient-key.priv --pubkey=vsphere-webclient-key.pub"
```

- 2 为每个 **Platform Services Controller** 和每个管理节点上的计算机解决方案用户以及每个管理节点上的每个其他解决方案用户 (**vpzd**、**vpzd-extension**、**vsphere-webclient**) 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，例如，**vpzd** 或 **vpzd-extension**，可便于查看证书与解决方案用户之间的映射关系。

- a 在 **Platform Services Controller** 节点上运行以下命令可为该节点上的计算机解决方案用户生成解决方案用户证书。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine"
```

- b 为每个管理节点上的计算机解决方案用户生成证书。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-machine.crt --privkey=machine-key.priv --Name=machine --server=<psc-ip-or-fqdn>"
```

- c 为每个管理节点上的 **vpzd** 解决方案用户生成证书。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-vpzd.crt --privkey=vpzd-key.priv --Name=vpzd --server=<psc-ip-or-fqdn>"
```

- d 为每个管理节点上的 **vpzd-extensions** 解决方案用户生成证书。

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-vpzd-extension.crt --privkey=vpzd-extension-key.priv --Name=vpzd-extension --server=<psc-ip-or-fqdn>"
```

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

```
C:\>"C:\Program Files\VMware\VMware vCenter Server\vmcad\certool --gencert --cert=new-vsphere-webclient.crt --privkey=vsphere-webclient-key.priv --Name=vsphere-webclient --server=<psc-ip-or-fqdn>"
```

3 将 VECS 中的解决方案用户证书替换为新的解决方案用户证书。

注 --store 和 --alias 参数必须与服务的默认名称完全匹配。

- a 在 Platform Services Controller 节点上，请运行以下命令以替换计算机解决方案用户证书：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine.crt --key machine-key.priv
```

- b 替换每个管理节点上的计算机解决方案用户证书：

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store machine --alias machine
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store machine --alias machine --cert new-machine-vc.crt --key machine-vc-key.priv
```

- c 替换每个管理节点上的 vpxd 解决方案用户证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd --alias vpxd
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd --alias vpxd --cert new-vpxd.crt --key vpxd-key.priv
```

- d 替换每个管理节点上的 vpxd-extension 解决方案用户证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vpxd-extension --alias vpxd-extension
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vpxd-extension --alias vpxd-extension --cert new-vpxd-extension.crt --key vpxd-extension-key.priv
```

- e 替换每个管理节点上的 vsphere-webclient 解决方案用户证书。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry delete --store vsphere-webclient --alias vsphere-webclient
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"vecs-cli entry create --store vsphere-webclient --alias vsphere-webclient --cert new-vsphere-webclient.crt --key vsphere-webclient-key.priv
```

4 使用新的解决方案用户证书更新 VMware Directory Service (vmdir)。系统将提示您输入 vCenter Single Sign-On 管理员密码。

- a 运行 dir-cli service list 可获取每个解决方案用户的唯一服务 ID 后缀。可以在 Platform Services Controller 或 vCenter Server 系统上运行此命令。

```
C:\>"C:\Program Files\VMware\vCenter Server\vmafdd\"dir-cli>dir-cli service list
output:
1. machine-29a45d00-60a7-11e4-96ff-00505689639a
```

```

2. machine-6fd7f140-60a9-11e4-9e28-005056895a69
3. vpxd-6fd7f140-60a9-11e4-9e28-005056895a69
4. vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69
5. vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69

```

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

- b 在 Platform Services Controller 上替换 `vmdir` 中的计算机证书。例如，如果 `machine-29a45d00-60a7-11e4-96ff-00505689639a` 为 Platform Services Controller 中的计算机解决方案用户，请运行此命令：

```

C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\dir-cli service update --name
machine-29a45d00-60a7-11e4-96ff-00505689639a --cert new-machine-1.crt

```

- c 替换每个管理节点上的 `vmdir` 中的计算机证书。例如，如果 `machine-6fd7f140-60a9-11e4-9e28-005056895a69` 为 vCenter Server 中的计算机解决方案用户，请运行此命令：

```

C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\dir-cli service update --name
machine-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-machine-2.crt

```

- d 替换每个管理节点上的 `vmdir` 中的 `vpxd` 解决方案用户证书。例如，如果 `vpxd-6fd7f140-60a9-11e4-9e28-005056895a69` 为 `vpxd` 解决方案用户 ID，请运行此命令：

```

C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\dir-cli service update --name
vpxd-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd.crt

```

- e 替换每个管理节点上的 `vmdir` 中的 `vpxd-extension` 解决方案用户证书。例如，如果 `vpxd-extension-6fd7f140-60a9-11e4-9e28-005056895a69` 为 `vpxd-extension` 解决方案用户 ID，请运行此命令：

```

C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\dir-cli service update --name vpxd-
extension-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vpxd-extension.crt

```

- f 替换每个管理节点上的 `vsphere-webclient` 解决方案用户证书。例如，如果 `vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69` 为 `vsphere-webclient` 解决方案用户 ID，请运行此命令：

```

C:\>"C:\Program Files\VMware\VCenter Server\vmafdd\dir-cli service update --name
vsphere-webclient-6fd7f140-60a9-11e4-9e28-005056895a69 --cert new-vsphere-webclient.crt

```

替换 VMware Directory Service 证书

如果决定使用新的 VMCA 根证书，并且取消发布在置备环境中已使用的 VMCA 根证书，则必须替换计算机 SSL 证书、解决方案用户证书和某些内部服务的证书。

如果取消发布 VMCA 根证书，则必须替换由 vCenter Single Sign-On 使用的 SSL 签名证书。请参见[刷新安全令牌服务证书](#)。还必须替换 VMware Directory Service (vmdir) 证书。

前提条件

为第三方的 vmdir 或企业 CA 请求证书。

步骤

- 1 停止 vmdir。

Linux

```
service-control --stop vmdird
```

Windows

```
service-control --stop VMWareDirectoryService
```

- 2 复制刚刚生成到 vmdir 位置的证书和密钥。

Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

Windows

```
copy vmdir.crt C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem
copy vmdir.priv C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

- 3 从 vSphere Web Client 或使用 service-control 命令重新启动 vmdir。

Linux

```
service-control --start vmdird
```

Windows

```
service-control --start VMWareDirectoryService
```


在混合模式环境中替换 VMware Directory Service 证书

在升级过程中，您的环境可能暂时包括 vCenter Single Sign-On 版本 5.5 和 vCenter Single Sign-On 版本 6.x。在此情况下，如果替换正在运行 vCenter Single Sign-On 服务的节点的 SSL 证书，则必须执行其他步骤才能替换 VMware Directory Service SSL 证书。

vmdir 使用 VMware Directory Service SSL 证书可在执行 vCenter Single Sign-On 复制的 Platform Services Controller 节点之间执行握手操作。

同时包括 vSphere 6.0 和 vSphere 6.5 节点的混合模式环境不需要执行这些步骤。仅在以下情况下需要执行这些步骤：

- 环境中同时包括 vCenter Single Sign-On 5.5 和 vCenter Single Sign-On 6.x 服务。
- vCenter Single Sign-On 服务设置为复制 vmdir 数据。
- 对于运行 vCenter Single Sign-On 6.x 服务的节点，计划将默认 VMCA 签名证书替换为自定义证书。

注 最佳做法是在重新启动服务之前先升级整个环境。通常不建议替换 VMware Directory Service 证书。

步骤

- 1 在运行 vCenter Single Sign-On 6.x 服务的节点上，替换 vmdird SSL 证书和密钥。
请参见[替换 VMware Directory Service 证书](#)。
- 2 在运行 vCenter Single Sign-On 5.5 服务的节点上，请先设置环境以便熟悉 vCenter Single Sign-On 6.x 服务。
 - a 备份所有文件 C:\ProgramData\VMware\CIS\cfg\vmdird。
 - b 在 6.x 节点上创建 vmdircert.pem 文件的副本，并将其重命名为 <sso_node2.domain.com>.pem，其中 <sso_node2.domain.com> 是 6.x 节点的 FQDN。
 - c 将重命名的证书复制到 C:\ProgramData\VMware\CIS\cfg\vmdird 以替换现有的复制证书。
- 3 在已替换证书的所有计算机上重新启动 VMware Directory Service。
可以从 vSphere Web Client 中重新启动服务或使用 service-control 命令。

在 vSphere 中使用第三方证书

如果公司策略有相关要求，则可以将 vSphere 中使用的所有证书替换为第三方 CA 签名证书。如果这样做，则 VMCA 将不在您的证书链中，但所有 vCenter 证书必须存储在 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用于在适当的时候对 vCenter Single Sign-On 进行身份验证。

注 如果不需要使用 VMCA，则您必须负责亲自替换所有证书、使用证书置备新的组件以及跟踪证书过期情况。

步骤

1 请求证书并导入自定义根证书

如果公司策略不允许使用中间 CA，则 VMCA 无法为您生成证书。可以使用企业或第三方 CA 的自定义证书。

2 将计算机 SSL 证书替换为自定义证书

收到自定义证书后，可以替换每个计算机证书。

3 将解决方案用户证书替换为自定义证书

在替换计算机 SSL 证书后，可以将 VMCA 签名解决方案用户证书替换为第三方或企业证书。

4 替换 VMware Directory Service 证书

如果决定使用新的 VMCA 根证书，并且取消发布在置备环境中已使用的 VMCA 根证书，则必须替换计算机 SSL 证书、解决方案用户证书和某些内部服务的证书。

5 在混合模式环境中替换 VMware Directory Service 证书

在升级过程中，您的环境可能暂时包括 vCenter Single Sign-On 版本 5.5 和 vCenter Single Sign-On 版本 6.x。在此情况下，如果替换正在运行 vCenter Single Sign-On 服务的节点的 SSL 证书，则必须执行其他步骤才能替换 VMware Directory Service SSL 证书。

请求证书并导入自定义根证书

如果公司策略不允许使用中间 CA，则 VMCA 无法为您生成证书。可以使用企业或第三方 CA 的自定义证书。

前提条件

证书必须满足以下要求：

- 密钥大小：2048 位或更大（PEM 编码）
- PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。密钥添加到 VECS 后，会转换为 PKCS8
- x509 版本 3
- 对于 root 证书，CA 扩展必须设置为 true，并且 cert 签名必须在要求列表中。
- SubjectAltName 必须包含 DNS Name=<machine_FQDN>

- CRT 格式
- 包含以下密钥使用：数字签名、不可否认性、密钥加密
- 比当前时间早一天的开始时间
- CN（和 SubjectAltName）设置为 vCenter Server 清单中的 ESXi 主机的主机名（或 IP 地址）。

步骤

- 1 向企业或第三方证书提供商发送以下证书的 CSR。

- 每个计算机具有一个计算机 SSL 证书。对于计算机 SSL 证书，SubjectAltName 字段必须包含完全限定域名 (DNS NAME=*machine_FQDN*)
- 此外，每个嵌入式系统或管理节点具有四个解决方案用户证书。解决方案用户证书不应包括 IP 地址、主机名或电子邮件地址。每个证书必须具有不同的证书主题。

通常，结果为信任链的 PEM 文件以及每个 Platform Services Controller 或管理节点的签名 SSL 证书。

- 2 列出 TRUSTED_ROOTS 存储和计算机 SSL 存储。

```
vecs-cli store list
```

- a 确保当前根证书和所有计算机 SSL 证书均为 VMCA 签名证书。
- b 请记住“序列号”、“颁发者”和“主题 CN”字段。
- c （可选）使用 Web 浏览器，打开与将替换证书的节点的 HTTPS 连接，检查证书信息，并确保该信息与计算机 SSL 证书相匹配。

- 3 停止所有服务，启动处理证书创建、传播和存储的服务。

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

Windows

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

vCenter Server Appliance

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

- 4 发布自定义根证书，该证书为第三方 CA 的签名证书。

```
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。如果移除了该根证书，必须刷新这些内部证书：

- 替换 vCenter Single Sign-On 签名证书。请参见[刷新安全令牌服务证书](#)。
- 替换 VMware Directory Service 证书。请参见[替换 VMware Directory Service 证书](#)。

将计算机 SSL 证书替换为自定义证书

收到自定义证书后，可以替换每个计算机证书。

每台计算机都必须拥有可用于与其他服务进行安全通信的计算机 SSL 证书。在多节点部署中，必须在每个节点上运行计算机 SSL 证书生成命令。使用 `--server` 参数从具有外部 Platform Services Controller 的 vCenter Server 指向 Platform Services Controller。

必须具有以下信息才能开始替换证书：

- administrator@vsphere.local 的密码。
- 有效的计算机 SSL 自定义证书（.crt 文件）。
- 有效的计算机 SSL 自定义密钥（.key 文件）。
- Root 的有效自定义证书（.crt 文件）。
- 如果您在多节点部署中具有外部 Platform Services Controller 的 vCenter Server 上运行命令，则需要 Platform Services Controller 的 IP 地址。

前提条件

必须已从第三方或企业证书颁发机构收到每个计算机的证书。

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

步骤

- 1 停止所有服务，启动处理证书创建、传播和存储的服务。

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

Windows

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

vCenter Server Appliance

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

- 2 登录到每个节点，然后将您从 CA 接收到的新的计算机证书添加到 VECS。

所有计算机都需要本地证书存储中的新证书来通过 SSL 进行通信。

```
vecs-cli entry delete --store MACHINE_SSL_CERT --alias __MACHINE_CERT
vecs-cli entry create --store MACHINE_SSL_CERT --alias __MACHINE_CERT --cert <cert-file-path>
--key <key-file-path>
```

- 3 重新启动所有服务。

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

示例：将计算机 SSL 证书替换为自定义证书

可以以同样方法替换每个节点上的计算机 SSL 证书。

- 1 首先，删除 VECS 中的现有证书。

```
"C:\Program Files\VMware\vCenter Server\vmaddd\"vecs-cli entry delete --store
MACHINE_SSL_CERT --alias __MACHINE_CERT
```

- 2 接下来，添加替换证书。

```
"C:\Program Files\VMware\vCenter Server\vmaddd\"vecs-cli entry create --store
MACHINE_SSL_CERT --alias __MACHINE_CERT --cert E:\custom-certs\ms-ca\signed-ssl\custom-wl-
vim-cat-dhcp-094.eng.vmware.com.crt --key E:\custom-certs\ms-ca\signed-ssl\custom-x3-vim-
cat-dhcp-1128.vmware.com.priv
```

后续步骤

您还可以替换 ESXi 主机的证书。请参见《vSphere 安全性》出版物。

在多节点部署中替换 root 证书后，必须在所有具有外部 Platform Services Controller 的 vCenter Server 节点上重新启动服务。

将解决方案用户证书替换为自定义证书

在替换计算机 SSL 证书后，可以将 VMCA 签名解决方案用户证书替换为第三方或企业证书。

解决方案用户仅使用证书对 vCenter Single Sign-On 进行身份验证。如果证书有效，vCenter Single Sign-On 将向解决方案用户分配 SAML 令牌，并且解决方案用户将使用该 SAML 令牌对其他 vCenter 组件进行身份验证。

请考虑在您的环境中是否需要替换解决方案用户证书。因为解决方案用户位于代理服务器后面，并且计算机 SSL 证书用于安全的 SSL 流量，因此解决方案用户证书可能存在的安全问题较少。

替换每个管理节点和每个 Platform Services Controller 节点上的计算机解决方案用户证书。只能替换每个管理节点上的其他解决方案用户证书。在具有外部 Platform Services Controller 的管理节点上运行命令时，请使用 `--server` 参数指向 Platform Services Controller。

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

前提条件

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

步骤

- 1 停止所有服务，启动处理证书创建、传播和存储的服务。

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

- 2 查找每个解决方案用户的名称。

```
dir-cli service list
```

可以使用替换证书时返回的唯一 ID。输入和输出可能显示如下。

```
C:\Program Files\VMware\vmCenter Server\vmafdd>dir-cli service list
Enter password for administrator@vsphere.local:
1. machine-1d364500-4b45-11e4-96c2-020011c98db3
2. vpxd-1d364500-4b45-11e4-96c2-020011c98db3
3. vpxd-extension-1d364500-4b45-11e4-96c2-020011c98db3
4. vsphere-webclient-1d364500-4b45-11e4-96c2-020011c98db3
```

在多节点部署中列出解决方案用户证书时，dir-cli 列表输出将包含所有节点的所有解决方案用户。运行 vmafd-cli get-machine-id --server-name localhost 以查找每个主机的本地计算机 ID。每个解决方案用户名称均包括计算机 ID。

3 对于每个解决方案用户，请依次替换 VECS 和 vmdir 中的现有证书。

必须以该顺序添加证书。

```
vecs-cli entry delete --store vpxd --alias vpxd
vecs-cli entry create --store vpxd --alias vpxd --cert vpxd.crt --key vpxd.priv
dir-cli service update --name <vpxd-xxxx-xxx-xxxxxx> --cert vpxd.crt
```

注 如果不替换 vmdir 中的证书，则解决方案用户无法对 vCenter Single Sign-On 进行身份验证。

4 重新启动所有服务。

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

替换 VMware Directory Service 证书

如果决定使用新的 VMCA 根证书，并且取消发布在置备环境中已使用的 VMCA 根证书，则必须替换计算机 SSL 证书、解决方案用户证书和某些内部服务的证书。

如果取消发布 VMCA 根证书，则必须替换由 vCenter Single Sign-On 使用的 SSL 签名证书。请参见[刷新安全令牌服务证书](#)。还必须替换 VMware Directory Service (vmdir) 证书。

前提条件

为第三方的 vmdir 或企业 CA 请求证书。

步骤

1 停止 vmdir。

Linux

```
service-control --stop vmdird
```

Windows

```
service-control --stop VMWareDirectoryService
```

2 复制刚刚生成到 vmdir 位置的证书和密钥。

Linux

```
cp vmdir.crt /usr/lib/vmware-vmdir/share/config/vmdircert.pem  
cp vmdir.priv /usr/lib/vmware-vmdir/share/config/vmdirkey.pem
```

Windows

```
copy vmdir.crt C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdircert.pem  
copy vmdir.priv C:\programdata\vmware\vCenterServer\cfg\vmdird\vmdirkey.pem
```

3 从 vSphere Web Client 或使用 service-control 命令重新启动 vmdir。

Linux

```
service-control --start vmdird
```

Windows

```
service-control --start VMWareDirectoryService
```

在混合模式环境中替换 VMware Directory Service 证书

在升级过程中，您的环境可能暂时包括 vCenter Single Sign-On 版本 5.5 和 vCenter Single Sign-On 版本 6.x。在此情况下，如果替换正在运行 vCenter Single Sign-On 服务的节点的 SSL 证书，则必须执行其他步骤才能替换 VMware Directory Service SSL 证书。

vmdir 使用 VMware Directory Service SSL 证书可在执行 vCenter Single Sign-On 复制的 Platform Services Controller 节点之间执行握手操作。

同时包括 vSphere 6.0 和 vSphere 6.5 节点的混合模式环境不需要执行这些步骤。仅在以下情况下需要执行这些步骤：

- 环境中同时包括 vCenter Single Sign-On 5.5 和 vCenter Single Sign-On 6.x 服务。
- vCenter Single Sign-On 服务设置为复制 vmdir 数据。

- 对于运行 vCenter Single Sign-On 6.x 服务的节点，计划将默认 VMCA 签名证书替换为自定义证书。

注 最佳做法是在重新启动服务之前先升级整个环境。通常不建议替换 VMware Directory Service 证书。

步骤

- 1 在运行 vCenter Single Sign-On 6.x 服务的节点上，替换 vmdird SSL 证书和密钥。
请参见[替换 VMware Directory Service 证书](#)。
- 2 在运行 vCenter Single Sign-On 5.5 服务的节点上，请先设置环境以便熟悉 vCenter Single Sign-On 6.x 服务。
 - a 备份所有文件 C:\ProgramData\VMware\CIS\cfg\vmdird。
 - b 在 6.x 节点上创建 vmdircert.pem 文件的副本，并将其重命名为 <sso_node2.domain.com>.pem，其中 <sso_node2.domain.com> 是 6.x 节点的 FQDN。
 - c 将重命名的证书复制到 C:\ProgramData\VMware\CIS\cfg\vmdird 以替换现有的复制证书。
- 3 在已替换证书的所有计算机上重新启动 VMware Directory Service。
可以从 vSphere Web Client 中重新启动服务或使用 service-control 命令。

通过 CLI 命令管理证书和服务

一组 CLI 可用于管理 VMCA（VMware Certificate Authority）、VECS（VMware Endpoint 证书存储）以及 VMware Directory Service (vmdir)。vSphere 证书管理器实用程序同时支持许多相关任务，但手动证书管理需要 CLI。

表 3-5. 用于管理证书和关联服务的 CLI 工具

CLI	描述	请参见
certool	生成并管理证书和密钥。属于 VMCA。	certool 初始化命令参考
vecs-cli	管理 VMware 证书存储实例的内容。属于 VMAFD。	vecs-cli 命令参考
dir-cli	在 VMware Directory Service 中创建并更新证书。属于 VMAFD。	dir-cli 命令参考
service-control	启动或停止服务，例如，在证书替换 workflow 中。	

证书管理工具位置

默认情况下，可以在每个节点的以下位置查找工具：

Windows

C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe

C:\Program Files\VMware\vCenter Server\vmafdd\dir-cli.exe

```
C:\Program Files\VMware\vCenter Server\vmcad\certool.exe
VCENTER_INSTALL_PATH\bin\service-control
```

Linux

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

在 Linux 上，service-control 命令不要求您指定路径。

如果从使用外部 Platform Services Controller 的管理节点运行命令，则可以使用 --server 参数指定 Platform Services Controller。

证书管理操作所需的特权

对于大多数 vCenter 证书管理操作，您必须是 vsphere.local 域中的 CAAdmins 组的成员。administrator@vsphere.local 用户位于 CAAdmins 组中。某些操作可供所有用户执行。

如果运行 vCenter 证书管理器实用程序，系统会提示您输入 administrator@vsphere.local 的密码。如果手动替换证书，则不同的证书管理 CLI 的不同选项需要不同的特权。

dir-cli

您必须是 vsphere.local 域中的 CAAdmins 组的成员。每次运行 dir-cli 命令时，系统均会提示您输入用户名和密码。

vecs-cli

最初，仅存储所有者有权访问存储。存储所有者在 Windows 系统中是管理员用户，在 Linux 系统中是 root 用户。存储所有者可以提供对其他用户的访问权限。

MACHINE_SSL_CERT 和 TRUSTED_ROOTS 存储属于特殊存储。仅有 root 用户或管理员用户（取决于安装的类型）拥有完整的访问权限。

certool

大多数 certool 命令需要该用户是 CAAdmins 组的成员。administrator@vsphere.local 用户位于 CAAdmins 组中。所有用户可以运行以下命令：

- genselfcacert
- initscr
- getdc
- waitVMDIR
- waitVMCA
- genkey

■ viewcert

对于 ESXi 主机的证书管理，您必须具有 **证书.管理证书** 特权。可以从 vSphere Web Client 中设置该特权。

更改 certool 配置

运行 `certool --gencert` 和某些其他证书初始化或管理命令时，CLI 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 (`certool.cfg`) 或替代其他值。

配置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
```

可以按如下方式更改配置中的值：

- 创建配置文件的备份，然后编辑该文件。如果使用的是默认配置文件，则无需指定该文件。否则，例如，如果已更改配置文件名称，请使用 `--config` 命令行选项。
- 替代命令行上的配置文件值。例如，要替代局部性，请运行以下命令：

```
certool --gencert --privkey=private.key --Locality="Mountain View"
```

指定 `--Name` 以替换证书的主题名称的 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 的原因是由于 SSL 客户端在验证计算机的主机名时会检查证书的主题名称的 CN 字段。由于计算机可以包含多个别名，因此证书具有您可以指定其他名称（DNS 名称、IP 地址等）的“主题备用名称”字段扩展。但是，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。

`--Hostname` 参数用于指定证书的 `SubAltName` 的 `DNSName`。

certool 初始化命令参考

certool 初始化命令可以生成证书签名请求、查看和生成 VMCA 签名的证书和密钥、导入根证书以及执行其他证书管理操作。

在许多情况下，您可以将配置文件传递到 certool 命令中。请参见[更改 certool 配置](#)。有关一些用法示例，请参见将现有 VMCA 签名证书替换为新的 VMCA 签名证书。

certool --initcsr

生成证书签名请求 (CSR)。此命令可生成 PKCS10 文件和专用密钥。

选项	描述
--initcsr	生成 CSR 时为必需项。
--privkey <key_file>	专用密钥文件的名称。
--pubkey <key_file>	公用密钥文件的名称。
--csrfile <csr_file>	发送到 CA 提供程序的 CSR 文件的文件名。
--config <config_file>	配置文件的可选名称。默认为 certool.cfg。

例如：

```
certool --initcsr --privkey=<filename> --pubkey=<filename> --csrfile=<filename>
```

certool --selfca

创建自签名证书并使用自签名的根 CA 置备 VMCA 服务器。使用此选项是置备 VMCA 服务器最简单的方法之一。您也可以改用第三方根证书置备 VMCA 服务器，从而使 VMCA 成为中间 CA。请参见[使用 VMCA 作为中间证书颁发结构](#)。

此命令将生成日期早三天的证书以避免出现时区冲突。

选项	描述
--selfca	生成自签名证书时为必需项。
--predate <number_of_minutes>	允许您将根证书的“有效起始日期”字段设置为当前时间之前的指定分钟数。此选项有助于解决潜在的时区问题。最大值为三天。
--config <config_file>	配置文件的可选名称。默认为 certool.cfg。
--server <server>	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。

例如：

```
machine-70-59:/usr/lib/vmware-vmca/bin # ./certool --predate=2280 --selfca --server=
192.0.2.24 --srp-upn=administrator@vsphere.local
```

certool --rootca

导入根证书。将指定的证书和专用密钥添加到 VMCA。VMCA 总是使用最新的根证书进行签名，但其他根证书仍然可用。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>	配置文件的可选名称。默认为 certool.cfg。
--privkey <key_file>	专用密钥文件的名称。该文件必须是 PEM 编码的格式。
--server <server>	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。

例如：

```
certool --rootca --cert=root.cert --privkey=privatekey.pem
```

certool --getdc

返回 vmdir 使用的默认域名。

选项	描述
--server <server>	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。
--port <port_num>	可选的端口号。默认为端口 389。

例如：

```
certool --getdc
```

certool --waitVMDIR

等待 VMware Directory Service 运行或等待 --wait 指定的超时结束。将此选项与其他选项配合使用可调度特定任务，例如返回默认域名。

选项	描述
--wait	可选的等待分钟数。默认值为“3”。
--server <server>	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。
--port <port_num>	可选的端口号。默认为端口 389。

例如：

```
certool --waitVMDIR --wait 5
```

certool --waitVMCA

等待 VMCA 服务运行或等待指定的超时结束。将此选项与其他选项配合使用可调度特定任务，例如生成证书。

选项	描述
<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 <code>localhost</code> 。
<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 <code>localhost</code> 。

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。可以使用该证书置备计算机或解决方案用户。

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 <code>localhost</code> 。

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。

选项	描述
--gencert	生成证书时为必需项。
--cert <certfile>	证书文件的名称。该文件必须是 PEM 编码的格式。
--privkey <keyfile>	专用密钥文件的名称。该文件必须是 PEM 编码的格式。
--config <config_file>	配置文件的可选名称。默认为 certool.cfg。
--server <server>	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。

例如：

```
certool --gencert --privkey=<filename> --cert=<filename>
```

certool --getrootca

以人工可读形式打印当前根 CA 证书。如果要在管理节点中运行此命令，请使用 Platform Services Controller 节点的计算机名称来检索根 CA。此输出无法用作证书，它将更改为人工可读。

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

例如：

```
certool --getrootca --server=remoteserver
```

certool --viewcert

以人工可读形式打印证书中的所有字段。

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

例如：

```
certool --viewcert --cert=<filename>
```

certool --enumcert

列出 VMCA 服务器了解的所有证书。通过所需的筛选器选项，可以列出所有证书或仅列出已吊销、活动或过期的证书。

选项	描述
--enumcert	列出所有证书时为必需项。
--filter [all active]	所需的筛选器。指定所有或活动。当前不支持已吊销和过期选项。

例如：

```
certool --enumcert --filter=active
```

certool --status

向 VMCA 服务器发送指定的证书以检查该证书是否已吊销。打印证书：已吊销，如果该证书已吊销；否则，则为证书：活动。

选项	描述
--status	检查证书状态时为必需项。
--cert <certfile>	配置文件的可选名称。默认为 certool.cfg。
--server <server>	VMCA 服务器的可选名称。默认情况下，该命令使用 localhost。

例如：

```
certool --status --cert=<filename>
```

certool --genselfcacert

根据配置文件中的值生成一个自签名证书。此命令将生成日期早三天的证书以避免出现时区冲突。

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

例如：

```
certool --genselfcert --privkey=<filename> --cert=<filename>
```

vecs-cli 命令参考

`vecs-cli` 命令集可用于管理 VMware Certificate Store (VECS) 实例。将这些命令与 `dir-cli` 和 `certool` 配合使用可管理证书基础架构。

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。

例如：

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

vecs-cli store delete

删除证书存储。无法删除由系统预定义的证书存储。

选项	描述
<code>--name <name></code>	要删除的证书存储的名称。

例如：

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

vecs-cli store list

列出证书存储。

VECS 包括以下库。

表 3-6. 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) 在嵌入式部署和每个 Platform Services Controller 节点上使用。 <p>vSphere 6.0 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 <code>vpzd</code>）仍使其自身的端口处于打开状态。</p>
受信任的根库 (TRUSTED_ROOTS)	包含所有受信任的根证书。

表 3-6. VECS 中的库（续）

库	描述
解决方案用户库 <ul style="list-style-type: none"> ■ machine ■ vpxd ■ vpxd-extensions ■ vsphere-webclient 	<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题必须是唯一的，例如计算机证书不能具有与 vpxd 证书相同的主题。</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。在嵌入式部署中，所有解决方案用户证书都位于相同的系统中。</p> <p>以下解决方案用户证书存储包括在每个管理节点和每个嵌入式部署的 VECS 中：</p> <ul style="list-style-type: none"> ■ machine：由组件管理器、许可证服务器和日志记录服务使用。 <p>注 计算机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 服务守护程序 (vpxd) 库位于管理节点和嵌入式部署上。vpxd 使用此库中存储的解决方案用户证书对 vCenter Single Sign-On 进行身份验证。 ■ vpxd-extensions：vCenter 扩展库。包括 Auto Deploy 服务、Inventory Service 以及不属于其他解决方案用户的其他服务。 ■ vsphere-webclient：vSphere Web Client 库。还包括其他一些服务，例如性能图表服务。 <p>此计算机库还包括在每个 Platform Services Controller 节点中。</p>
vSphere 证书管理器实用程序备份库 (BACKUP_STORE)	由 VMCA（VMware 证书管理器）用来支持证书恢复。仅将最近的状态存储为备份，无法返回多个步骤。
其他库	<p>解决方案可能会添加其他库。例如，虚拟卷解决方案会添加 SMS 库。请勿修改这些库中的证书，除非 VMware 文档或 VMware 知识库文章指示进行此类修改。</p> <p>注 但是，在 vSphere 6.0 中不支持 CRLS，删除 TRUSTED_ROOTS_CRLS 库可能会损坏证书基础架构。请勿删除或修改 TRUSTED_ROOTS_CRLS 库。</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。

存储的所有者拥有其存储的所有控制权，包括授予和撤销权限。管理员拥有对所有存储的所有特权，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 entry create

在 VECS 中创建一个条目。使用此命令向存储中添加一个专用密钥或证书。

选项	描述
<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。

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。
<code>--text</code>	显示证书的人工可读版本。

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。

vecs-cli entry getkey

检索存储在 VECS 中的密钥。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>	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。

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。

vecs-cli force-refresh

强制刷新 vecs-cli。发生此情况时，vecs-cli 将更新以使用 vmdir 中的最新信息。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。

dir-cli 命令参考

使用 dir-cli 实用程序，您可以创建和更新解决方案用户、创建其他用户帐户，以及管理 vmdir 中的证书和密码。将此实用程序与 vecs-cli 和 certool 配合使用可管理证书基础架构。

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
<code>--name <name></code>	要创建的解决方案用户的名称
<code>--cert <cert file></code>	证书文件的路径。这可以是 VMCA 签名的证书或第三方证书。
<code>--login <admin_user_id></code>	默认情况下，为 administrator@vsphere.local。该管理员可以将其他用户添加到 CAAdmins vCenter Single Sign-On 组以向其授予管理员特权。
<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 service list

列出 dir-cli 了解的解决方案用户。

选项	描述
<code>--login <admin_user_id></code>	默认情况下，为 <code>administrator@vsphere.local</code> 。该管理员可以将其他用户添加到 CAAdmins vCenter Single Sign-On 组以向其授予管理员特权。
<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 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
<code>--name</code>	要删除的解决方案用户的名称。
<code>--login <admin_user_id></code>	默认情况下，为 <code>administrator@vsphere.local</code> 。该管理员可以将其他用户添加到 CAAdmins vCenter Single Sign-On 组以向其授予管理员特权。
<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 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
<code>--name <name></code>	要更新的解决方案用户的名称。
<code>--cert <cert_file></code>	要分配给服务的证书名称。
<code>--login <admin_user_id></code>	默认情况下，为 <code>administrator@vsphere.local</code> 。该管理员可以将其他用户添加到 CAAdmins vCenter Single Sign-On 组以向其授予管理员特权。
<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 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。只能在原型制作期间使用此命令。

选项	描述
<code>--account <name></code>	要创建的 vCenter Single Sign-On 用户的名称。
<code>--user-password <password></code>	用户的初始密码。
<code>--first-name <name></code>	用户的名字。
<code>--last-name <name></code>	用户的姓氏。

选项	描述
--login <admin_user_id>	默认情况下，为 administrator@vsphere.local。该管理员可以将其他用户添加到 CAAdmins vCenter Single Sign-On 组以向其授予管理员特权。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli user delete

删除 vmdir 中的指定用户。

选项	描述
--account <name>	要删除的 vCenter Single Sign-On 用户的名称。
--login <admin_user_id>	默认情况下，为 administrator@vsphere.local。该管理员可以将其他用户添加到 CAAdmins vCenter Single Sign-On 组以向其授予管理员特权。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli group modify

将用户或组添加到已存在的组。

选项	描述
--name <name>	vmdir 中组的名称。
--add <user_or_group_name>	要添加的用户或组的名称。
--login <admin_user_id>	默认情况下，为 administrator@vsphere.local。该管理员可以将其他用户添加到 CAAdmins vCenter Single Sign-On 组以向其授予管理员特权。
--password <admin_password>	管理员用户的密码。如果未指定密码，将会收到提示。

dir-cli group list

列出指定的 vmdir 组。

选项	描述
--name <name>	vmdir 中组的可选名称。此选项可用于检查组是否存在。
--login <admin_user_id>	默认情况下，为 administrator@vsphere.local。该管理员可以将其他用户添加到 CAAdmins vCenter Single Sign-On 组以向其授予管理员特权。
--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
<code>--cert <file></code>	证书文件的路径。
<code>--login <admin_user_id></code>	默认情况下，为 <code>administrator@vsphere.local</code> 。该管理员可以将其他用户添加到 CAAdmins vCenter Single Sign-On 组以向其授予管理员特权。
<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 unpublsh

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>--crl <file></code>	与此证书关联的 CRL 文件的路径。当前未使用。
<code>--login <admin_user_id></code>	默认情况下，为 <code>administrator@vsphere.local</code> 。该管理员可以将其他用户添加到 CAAdmins vCenter Single Sign-On 组以向其授予管理员特权。
<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 <code>administrator@vsphere.local</code> 。该管理员可以将其他用户添加到 CAAdmins vCenter Single Sign-On 组以向其授予管理员特权。
<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。ID 将显示在 <code>dir-cli trustedcert list</code> 命令中。
<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。

选项	描述
<code>--login <admin_user_id></code>	默认情况下，为 <code>administrator@vsphere.local</code> 。该管理员可以将其他用户添加到 CAAdmins vCenter Single Sign-On 组以向其授予管理员特权。
<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 <code>administrator@vsphere.local</code> 。该管理员可以将其他用户添加到 CAAdmins vCenter Single Sign-On 组以向其授予管理员特权。
<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 <code>administrator@vsphere.local</code> 。该管理员可以将其他用户添加到 CAAdmins vCenter Single Sign-On 组以向其授予管理员特权。
<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。

通过 vSphere Web Client 查看 vCenter 证书

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

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

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

步骤

- 1 以 administrator@vsphere.local 或 CAAAdmins vCenter Single Sign-On 组的另一个用户的身份登录到 vCenter Server。
- 2 选择**系统管理**，再依次单击**部署**和**系统配置**。
- 3 单击**节点**，并选择要查看或管理其证书的节点。
- 4 依次单击**管理**选项卡和**证书颁发机构**。
- 5 单击要查看证书信息的证书类型。

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

- 6 选择证书，然后单击**显示证书详细信息**按钮以查看证书详细信息。
详细信息包括主题名称、颁发者、有效性和算法。

为 vCenter 证书过期警告设置阈值

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

步骤

- 1 登录到 vSphere Web Client。
- 2 选择 vCenter Server 对象，然后依次选择**管理**选项卡和**设置**子选项卡。
- 3 单击**高级设置**，选择**编辑**，然后筛选阈值。
- 4 将 `vpzd.cert.threshold` 的设置更改为所需值，然后单击**确定**。

vSphere 权限和用户管理任务

4

vCenter Single Sign-On 支持身份验证，这表明它可以确定用户究竟是否可以访问 vSphere 组件。此外，必须授权每位用户查看或操作 vSphere 对象。

vSphere 支持多种不同的授权机制，如[了解 vSphere 中的授权](#)中所述。本部分中的信息重点关注 vCenter Server 权限模型以及如何执行用户管理任务。

vCenter Server 允许通过权限和角色对授权进行精细控制。向 vCenter Server 对象层次结构中的对象分配权限时，请指定哪个用户或组对该对象具有哪些特权。要指定特权，请使用角色（即特权集）。

最初只授权用户 `administrator@vsphere.local` 登录 vCenter Server 系统。授权后，该用户可以执行如下操作：

- 1 将在其中定义了其他用户和组的标识源添加到 vCenter Single Sign-On 中。请参见[添加 vCenter Single Sign-On 标识源](#)。
- 2 向用户或组授予特权，方法是选择虚拟机或 vCenter Server 系统等对象并将针对该对象的角色分配给相应的用户或组。



角色、特权和权限

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8vla7txu/uiConfId/49694343/)

本章讨论了以下主题：

- [了解 vSphere 中的授权](#)
- [了解 vCenter Server 权限模型](#)
- [权限的层次结构继承](#)
- [多项权限设置](#)
- [管理 vCenter 组件的权限](#)
- [全局权限](#)
- [使用角色分配特权](#)
- [角色和权限的最佳做法](#)
- [常见任务的所需特权](#)

了解 vSphere 中的授权

在 vSphere 中授权用户或组的主要方式是 vCenter Server 权限。根据要执行的任务，您可能需要其他授权。

vSphere 6.0 及更高版本允许有特权的用户以下列方式授予其他用户执行任务的权限。这些方法大多数互相排斥；但是，您可以使用全局权限授予某些用户对所有解决方案的权限，以及使用本地 vCenter Server 权限授予其他用户对各个 vCenter Server 系统的权限。

vCenter Server 权限

vCenter Server 系统的权限模型需要向该 vCenter Server 对象层次结构中的对象分配权限。每种权限都会向一个用户或组授予一组特权，即选定对象的角色。例如，您可以选择一台 ESXi 主机并向一组用户分配角色，以授予这些用户对该主机的相应特权。

全局权限

全局权限应用到跨多个解决方案的全局根对象。例如，如果已安装 vCenter Server 和 vCenter Orchestrator，则可以使用全局权限向这两个对象层次结构中的所有对象授予权限。

系统会在整个 vsphere.local 域中复制全局权限。全局权限不会为通过 vsphere.local 组管理的服务提供授权。请参见[全局权限](#)。

vsphere.local 组中的组成员资格

用户 administrator@vsphere.local 可以执行与 Platform Services Controller 附带的服务相关联的任务。此外，vsphere.local 组的成员可以执行相应的任务。例如，如果您是 LicenseService.Administrators 组的成员，则可以执行许可证管理。请参见[vsphere.local 域中的组](#)。

ESXi 本地主机权限

如果要管理不受 vCenter Server 系统管理的独立 ESXi 主机，则可以向用户分配其中一个预定义的角色。请参见《使用 vSphere Client 管理 vSphere》文档。

了解 vCenter Server 权限模型

vCenter Server 系统的权限模型需要向 vSphere 对象层次结构中的对象分配权限。每种权限都会向一个用户或组授予一组特权，即选定对象的角色。

您需要了解以下概念：

权限

vCenter Server 对象层次结构中的每个对象都具有关联的权限。每个权限为一个组或用户指定该组或用户具有对象的哪些特权。

用户和组

在 vCenter Server 系统中，可以仅向经过身份验证的用户或经过身份验证的用户组分配特权。用户通过 vCenter Single Sign-On 进行身份验证。必须在 vCenter Single Sign-On 正用于进行身份验证的标识源中定义用户和组。使用您的标识源（例如 Active Directory）中的工具定义用户和组。

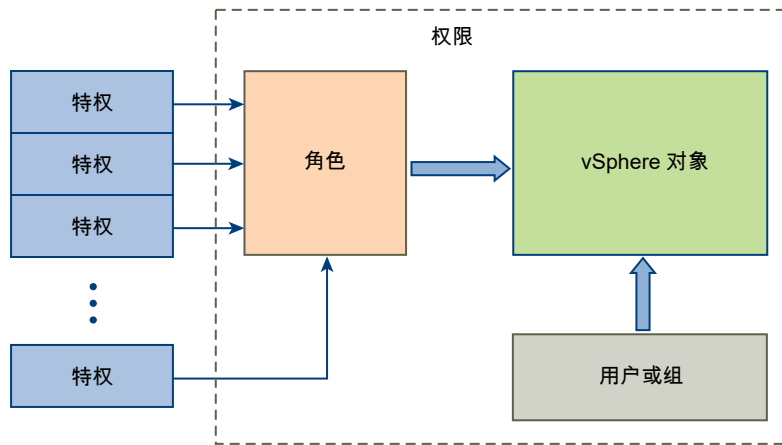
角色

角色允许您基于用户执行的一系列典型任务分配对对象的权限。默认角色（例如管理员）已在 vCenter Server 中预定义，不能更改。其他角色（例如资源池管理员）是预定义的样本角色。可以从头开始或者通过克隆和修改样本角色创建自定义角色。

特权

特权是精细的访问控制。可以将这些特权分组到角色中，然后可以将其映射到用户或组。

图 4-1. vSphere 权限



要向对象分配权限，请执行以下步骤：

- 1 在 vCenter 对象层次结构中选择要对其应用权限的对象。
- 2 选择应对该对象具有特权的组或用户。
- 3 选择组或用户针对该对象应具有的角色（即一组特权）。默认情况下，权限会传播，即组或用户对选定对象及其子对象具有选定角色。

借助权限模型，您可以通过提供预定义的角色轻松完成操作。还可以将特权组合在一起以创建自定义角色。有关所有特权以及可对其应用特权的对象的参考信息，请参见第 11 章 [定义的特权](#)。有关执行这些任务时所需的权限集的示例，请参见[常见任务的所需特权](#)。

在许多情况下，必须同时定义对源对象和目标对象的权限。例如，如果要移动虚拟机，您需要对该虚拟机具有某些特权，同时还需要对目标数据中心具有特权。

独立 ESXi 主机的权限模型比较简单。请参见[ESXi 分配权限](#)

vCenter Server 用户验证

使用目录服务的 vCenter Server 系统将根据用户目录域定期验证用户和组。验证将根据 vCenter Server 设置中指定的固定时间间隔执行。例如，如果为用户 Smith 分配了对多个对象的角色，并在域中将用户名更改为 Smith2，则在下次验证发生时主机会认为 Smith 已不存在，并从 vSphere 对象中移除与该用户关联的权限。

同样，如果将用户 Smith 从域中移除，则在下次验证发生时与该用户关联的所有权限都将被移除。如果在下次验证发生之前将新用户 Smith 添加到域，新用户 Smith 会接替旧用户 Smith 获得对任意对象的权限。

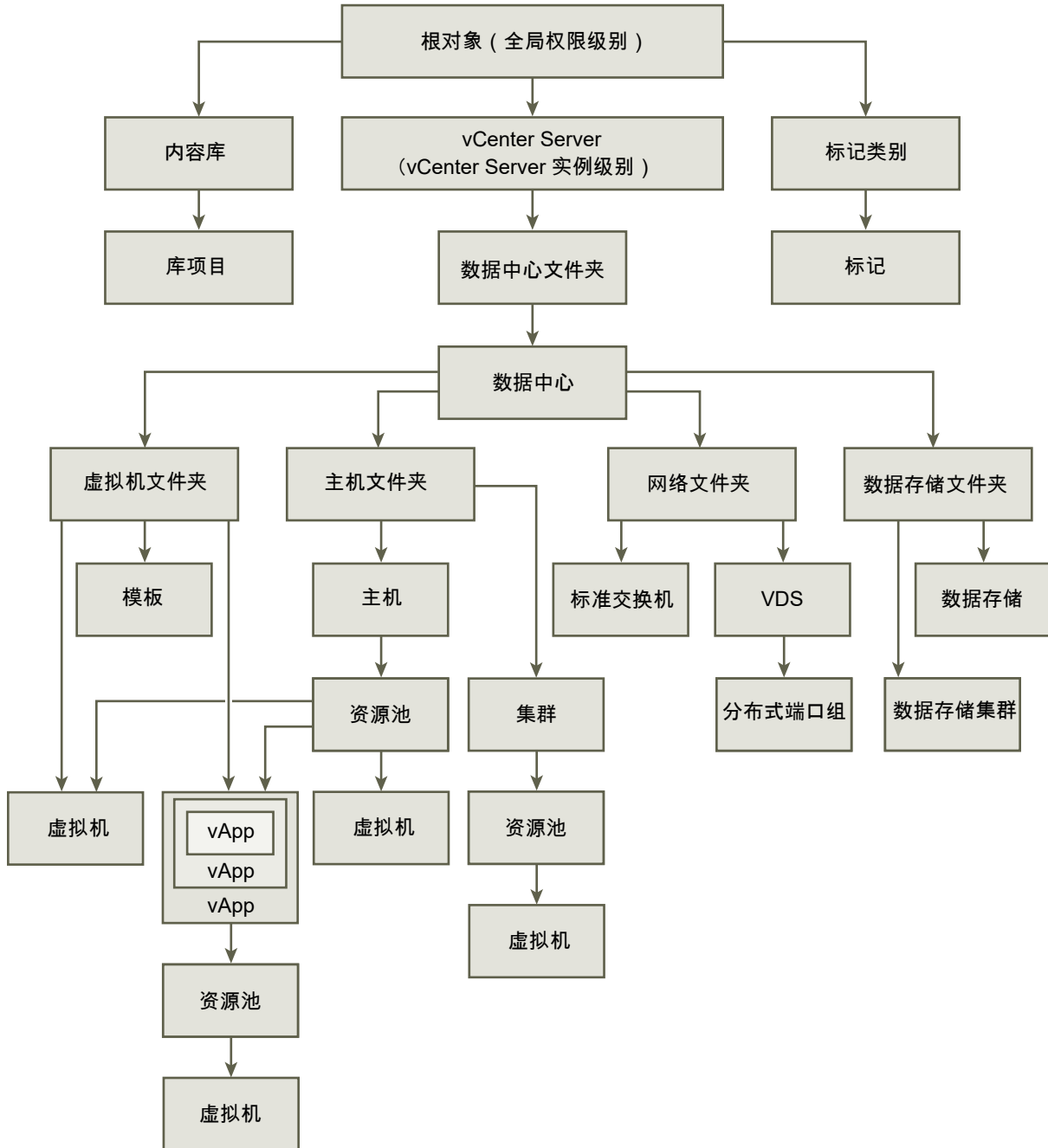
权限的层次结构继承

当向对象授予权限时，可以选择是否允许其沿对象层次结构向下传播。为每个权限设置传播。传播并非普遍适用。为子对象定义的权限将总是替代从父对象中传播的权限。

该图说明了清单层次结构和权限传播的路径。

注 全局权限支持从全局根对象跨多个解决方案分配特权。请参见[全局权限](#)。

图 4-2. vSphere 清单层次结构



大多数清单对象在层次结构中从单一父对象继承权限。例如，数据存储从其父数据存储文件夹或父数据中心继承权限。虚拟机同时从父虚拟机文件夹和父主机、集群或资源池继承权限。

例如，可为 **Distributed Switch** 及其关联的分布式端口组设置权限，方法是设置对父对象（例如文件夹或数据中心）的权限。此外，还必须选择将这些权限传播给子对象的选项。

权限在层次结构中有多种形式：

受管实体

特权用户可以对受管实体定义权限。

- 集群
- 数据中心
- 数据存储
- 数据存储集群
- 文件夹
- 主机
- 网络（vSphere Distributed Switch 除外）
- 分布式端口组
- 资源池
- 模板
- 虚拟机
- vSphere vApp

全局实体

不能修改从根 vCenter Server 系统中派生权限的实体的权限。

- 自定义字段
- 许可证
- 角色
- 统计间隔
- 会话

多项权限设置

对象可能拥有多种权限，但每个用户或组只拥有一种权限。例如，一种权限可能指定组 A 对某个对象具有管理员特权。另一种权限可能指定组 B 对同一个对象具有虚拟机管理员特权。

如果某个对象从两个父对象继承了权限，则对一个对象的权限将添加到对另一个对象的权限中。例如，如果某个虚拟机位于虚拟机文件夹中，同时还属于资源池，该虚拟机将同时从虚拟机文件夹和资源池继承所有权限设置。

在子对象上应用的权限始终会替代在父对象上应用的权限。请参见[示例 2：子权限替代父权限](#)。

如果对同一对象定义了多个组权限，且用户属于这些组中的两个或多个组，则可能出现以下两种情况：

- 如果没有为用户定义对该对象的权限，则用户将获得分配给该对象的组的一系列特权。
- 如果为用户定义了对该对象的权限，则该用户权限将优先于所有组权限。

示例 1：继承多个权限

此示例说明了对象如何从组（在父对象上授予了权限）中继承多个权限。

在此示例中，为两个不同组中的同一对象分配两种权限。

- 角色 1 可启动虚拟机。
- 角色 2 可对虚拟机执行快照。
- 在虚拟机文件夹上为组 A 授予角色 1，并将权限设置为传播到子对象。
- 在虚拟机文件夹上为组 B 授予角色 2，并将权限设置传播到子对象。
- 用户 1 未获得特定特权。

属于组 A 和组 B 的用户 1 登录。用户 1 可以同时启动虚拟机 A 和虚拟机 B 并对其执行快照。

图 4-3. 示例 1：继承多个权限



示例 2：子权限替代父权限

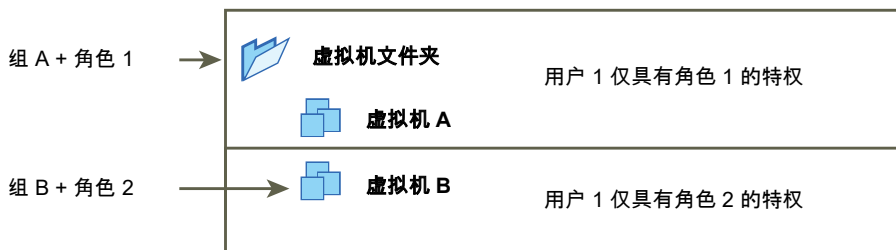
此示例说明了为子对象分配的权限如何覆盖为父对象分配的权限。可以使用此替代行为限制用户访问清单的特定区域。

在此示例中，权限在两个不同组的两个不同对象上定义。

- 角色 1 可启动虚拟机。
- 角色 2 可对虚拟机执行快照。
- 在虚拟机文件夹上为组 A 授予角色 1，并将权限设置为传播到子对象。
- 在虚拟机 B 上为组 B 授予角色 2。

属于组 A 和组 B 的用户 1 登录。因为在层次结构中，角色 2 被分配在角色 1 之下，所以它将在虚拟机 B 上替代角色 1。用户 1 可以启动虚拟机 A，但不能执行快照。用户 1 可对虚拟机 B 执行快照但无法将其启动。

图 4-4. 示例 2：子权限替代父权限



示例 3：用户角色替代组角色

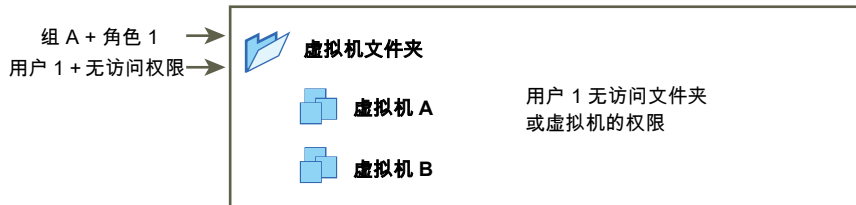
下例说明了直接分配给单个用户的角色如何替代与分配给组的角色关联的特权。

在此示例中，权限在相同的对象上定义。一种权限与包含某个角色的组相关联，另一种权限与包含某个角色的单个用户相关联。用户属于组成员。

- 角色 1 可启动虚拟机。
- 在虚拟机文件夹上为组 A 授予角色 1。
- 在虚拟机文件夹上为用户 1 授予无权访问角色。

属于组 A 的用户 1 登录。在虚拟机文件夹上为用户 1 授予的无权访问角色替代分配给组的角色。用户 1 无权访问虚拟机文件夹或虚拟机 A 和 B。

图 4-5. 示例 3：用户权限替代组权限



管理 vCenter 组件的权限

权限在 vCenter 对象层次结构中的对象上设置。每种权限与包含用户或组的对象以及该组或用户的访问角色相关联。例如，您可以选择一个虚拟机对象，添加一种权限用于向组 1 授予 **ReadOnly** 角色，然后添加另一种权限用于将管理员角色授予用户 2。

通过将不同角色分配给不同对象的用户组，您可控制这些用户能够在 vSphere 环境中执行的任务。例如，要允许组配置主机内存，请选择该主机并添加用于向该组授予角色的权限，包括**主机.配置.内存配置**特权。

要从 vSphere Web Client 管理权限，需要了解以下概念：

权限

vCenter Server 对象层次结构中的每个对象都具有关联的权限。每个权限为一个组或用户指定该组或用户具有对象的哪些特权。

用户和组

在 vCenter Server 系统中，可以仅向经过身份验证的用户或经过身份验证的用户组分配特权。用户通过 vCenter Single Sign-On 进行身份验证。必须在 vCenter Single Sign-On 正用于进行身份验证的标识源中定义用户和组。使用您的标识源（例如 Active Directory）中的工具定义用户和组。

角色

角色允许您基于用户执行的一系列典型任务分配对对象的权限。默认角色（例如管理员）已在 vCenter Server 中预定义，不能更改。其他角色（例如资源池管理员）是预定义的样本角色。可以从头开始或者通过克隆和修改样本角色创建自定义角色。

特权

特权是精细的访问控制。可以将这些特权分组到角色中，然后可以将其映射到用户或组。

可以在不同的层次结构级别为对象分配权限，例如，可以为主机对象或包含所有主机对象的文件夹对象分配权限。请参见[权限的层次结构继承](#)。还可以向全局根对象分配权限，以将权限应用于所有解决方案中的所有对象。请参见[全局权限](#)。

将权限添加到清单对象

在创建用户和组并定义角色后，必须将用户和组及其角色分配给相关的清单对象。通过将对象移动到文件夹并在文件夹上设置权限，可以同时将相同的权限分配给多个对象。

从 vSphere Web Client 分配权限时，用户和组名称必须与 Active Directory 精确匹配，包括大小写。如果从 vSphere 的早期版本进行升级，则在遇到组问题时，请检查大小写是否不一致。

前提条件

在要修改其权限的对象上，必须具有包含[权限.修改权限](#)特权的角色。

步骤

- 1 在 vSphere Web Client 对象导航器中，浏览到要为其分配权限的对象。
- 2 单击**管理**选项卡，然后选择**权限**。
- 3 单击“添加”图标，然后单击**添加**。
- 4 确定将拥有选定角色所定义的特权的用户或组。
 - a 从**域**下拉菜单中，选择用户或组所处的域。
 - b 在“搜索”框中键入名称，或者从列表中选择名称。
系统会搜索用户名、组名称和相关描述。
 - c 选择用户或组，然后单击**添加**。
名称将添加到**用户或组**列表中。
 - d （可选）单击**检查名称**验证标识源中是否存在该用户或该组。
 - e 单击**确定**。
- 5 在**分配的角色**下拉菜单中选择角色。
分配给该对象的角色会显示在菜单中。该角色中包含的特权将在角色标题下面的区域中列出。
- 6 （可选）要限制传播，取消选中**传播到子对象**复选框。
角色只应用于选定对象，而不会传播给子对象。
- 7 单击**确定**以添加权限。

更改权限

在为清单对象设置用户或组和角色对后，可以更改与用户或组配对的角色或更改**传播**复选框的设置。还可移除权限设置。

步骤

- 1 在 vSphere Web Client 对象导航器中，浏览到对象。
- 2 单击**管理**选项卡，然后选择**权限**。
- 3 单击行项目以选择用户或组和角色对。
- 4 单击**针对权限更改角色**。
- 5 在**分配的角色**下拉菜单中为用户或组选择角色。
- 6 要将特权传播至分配的清单对象的子对象，请单击**传播**复选框，然后单击**确定**。

移除权限

您可以为单个用户或组移除在对象层次结构中对象上的权限。执行此操作后，用户将不再拥有与对象上该角色关联的特权。

步骤

- 1 在 vSphere Web Client 对象导航器中，浏览到对象。
- 2 单击**管理**选项卡，然后选择**权限**。
- 3 单击适当的行项目以选择用户或组和角色对。
- 4 单击**移除权限**。

结果

vCenter Server 会移除权限设置。

更改权限验证设置

vCenter Server 定期根据用户目录中的用户和组验证其用户和组列表。根据验证结果，它会移除该域中不再存在的用户或组。可以禁用验证或更改两次验证之间的时间间隔。如果域中有数千个用户或组，或者如果完成搜索需要很长时间，则可以考虑调整搜索设置。

对于早于 vCenter Server 5.0 的 vCenter Server 版本，这些设置适用于与 vCenter Server 关联的 Active Directory。对于 vCenter Server 5.0 及更高版本，这些设置适用于 vCenter Single Sign-On 标识源。

注 此步骤仅适用于 vCenter Server 用户列表。不能用同样的方法搜索 ESXi 用户列表。

步骤

- 1 在 vSphere Web Client 对象导航器中，浏览到 vCenter Server 系统。
- 2 选择**管理**选项卡，然后单击**设置**。

- 3 依次单击**常规**和**编辑**。
- 4 选择**用户目录**。
- 5 根据需要更改值。

选项	描述
用户目录超时	连接到 Active Directory 服务器的超时时间间隔（以秒为单位）。该值指定 vCenter Server 允许搜索在所选域上运行的最大时间。搜索大型域需要很长时间。
查询限制	选中此复选框以设置 vCenter Server 显示的用户和组的最大数目。
查询限制大小	在 选择用户或组 对话框中指定 vCenter Server 显示所选域中的用户和组的最大数目。如果输入 0（零），则所有用户和组均会出现。
验证	取消选中复选框以禁用验证
验证周期	指定 vCenter Server 验证权限的频率（以分钟为单位）。

- 6 单击**确定**。

全局权限

全局权限应用到跨多个解决方案的全局根对象，例如，vCenter Server 和 vCenter Orchestrator。使用全局权限可为用户或组提供所有对象层次结构中所有对象的特权。

每个解决方案自身的对象层次结构中都有一个根对象。全局根对象用作每个解决方案对象的父对象。您可以向用户或组分配全局权限，确定每个用户或组的角色。角色确定一组特权。您可以分配预定义角色，也可以创建自定义角色。请参见[使用角色分配特权](#)。重要的是对 vCenter Server 权限与全局权限加以区分。

vCenter Server 权限

在多数情况下，权限应用到 vCenter Server 清单对象，如 ESXi 主机或虚拟机。操作时，指定拥有一组对象特权的用户或组（叫做角色）。

全局权限

全局权限向用户和组提供查看或管理部署的每个清单层次结构中所有对象的特权。

如果已分配全局权限且未选择传播，则与此权限关联的用户或组无法访问层次结构中的对象。这些用户和组仅拥有某些功能的访问权限，如创建角色。

重要事项 使用全局权限时要小心谨慎。确认您确实希望分配对所有清单层次结构中所有对象的权限。

添加全局权限

可以使用全局权限向用户或组授予对您的部署中所有清单层次结构中的所有对象的特权。

使用全局权限时要小心谨慎。确认您确实希望分配对所有清单层次结构中所有对象的权限。

前提条件

您必须对所有清单层次结构的根对象具有**权限.修改权限**特权，才能执行此任务。

步骤

- 1 单击**管理**，然后在“访问控制”区域中选择**全局权限**。
- 2 单击**管理**，然后单击“添加权限”图标。
- 3 确定将拥有选定角色所定义的特权的用户或组。
 - a 从**域**下拉菜单中，选择用户或组所处的域。
 - b 在“搜索”框中键入名称，或者从列表中选择名称。
系统会搜索用户名、组名称和相关描述。
 - c 选择用户或组，然后单击**添加**。
名称将添加到**用户或组**列表中。
 - d （可选）单击**检查名称**验证标识源中是否存在该用户或该组。
 - e 单击**确定**。
- 4 在**分配的角色**下拉菜单中选择角色。
分配给该对象的角色会显示在菜单中。该角色中包含的特权将在角色标题下面的区域中列出。
- 5 在大多数情况下，请保持选中“传播到子对象”复选框。
如果已分配全局权限且未选择传播，则与此权限关联的用户或组无法访问层次结构中的对象。这些用户和组仅拥有某些功能的访问权限，如创建角色。
- 6 单击**确定**。

标记对象的权限

在 vCenter Server 对象层次结构中，标记对象不是 vCenter Server 的子项，而是在 vCenter Server root 级别创建的。在具有多个 vCenter Server 实例的环境中，标记对象在 vCenter Server 实例间共享。标记对象权限的工作方式不同于 vCenter Server 对象层次结构中其他对象的权限。

只有全局权限或分配给标记对象的权限适用

如果将权限授予 vCenter Server 清单对象（例如 ESXi 主机或虚拟机）上的某个用户，那么该用户无法对该对象执行标记操作。

例如，如果将**分配 vSphere 标记**特权授予主机 TPA 上的用户 Dana，该权限对 Dana 能否在主机 TPA 上分配标记没有影响。Dana 必须拥有 root 级别的**分配 vSphere 标记**特权（即全局权限）或者必须拥有针对该标记对象的特权。

表 4-1. 全局权限和标记对象权限如何影响用户可以执行的操作

全局权限	标记级别的权限	vCenter Server 对象级别的权限	有效权限
未分配标记特权	Dana 拥有标记的 分配或取消分配 vSphere 标记 特权。	Dana 在 ESXi 主机 TPA 上拥有 删除 vSphere 标记 特权	Dana 拥有标记的 分配或取消分配 vSphere 标记 特权。
Dana 拥有 分配或取消分配 vSphere 标记 特权。	未分配标记特权。	Dana 在 ESXi 主机 TPA 上拥有 删除 vSphere 标记 特权	Dana 拥有 分配或取消分配 vSphere 标记 全局特权。这包括标记级别的特权。
未分配标记特权	未分配标记特权。	Dana 在 ESXi 主机 TPA 上拥有 分配或取消分配 vSphere 标记 特权	Dana 在任何对象（包括主机 TPA）上均没有标记特权。

全局权限是标记对象权限的补充

全局权限，即在 root 对象上分配的权限，可在标记对象权限更为严格时作为标记对象权限的补充。vCenter Server 权限不会影响标记对象。

例如，假设您在 root 级别（也就是使用全局权限）向用户 Robin 分配了**删除 vSphere 标记**权限。对于标记“生产”，您未向 Robin 分配**删除 vSphere 标记**特权。这种情况下，Robin 对标记“生产”仍拥有特权，因为 Robin 拥有全局权限。除非修改全局权限，否则您无法限制特权。

表 4-2. 全局权限是标记级别权限的补充

全局权限	标记级别的权限	有效权限
Robin 拥有 删除 vSphere 标记 特权	Robin 没有标记的 删除 vSphere 标记 特权。	Robin 拥有 删除 vSphere 标记 特权。
未分配标记特权	Robin 没有针对标记分配的 删除 vSphere 标记 特权。	Robin 没有 删除 vSphere 标记 特权

标记级别权限可以扩展全局权限

您可以使用标记级别权限扩展全局权限。这意味着用户可以同时对标记拥有全局权限和标记级别权限。

表 4-3. 全局权限可以扩展标记级别权限

全局权限	标记级别的权限	有效权限
Lee 拥有 分配或取消分配 vSphere 标记 特权。	Lee 拥有 删除 vSphere 标记 特权。	Lee 拥有标记的 分配 vSphere 标记 特权和 删除 vSphere 标记 特权。
未分配标记特权。	Lee 拥有针对标记分配的 删除 vSphere 标记 特权。	Lee 拥有标记的 删除 vSphere 标记 特权。

使用角色分配特权

角色是一组预定义的特权。特权定义了执行操作和读取属性所需的权限。例如，虚拟机管理员角色包含读取属性和执行操作的一组权限。该角色允许用户读取和更改虚拟机属性。

分配权限时，可将用户或组与角色配对，并将该配对与清单对象关联。对于清单中的不同对象，单个用户或组可能有不同角色。

例如，如果清单中有两个资源池（池 A 和池 B），可以为特定用户在池 A 上分配虚拟机用户角色而在池 B 上分配只读角色。执行上述分配后，该用户可以打开池 A 中的虚拟机，而只能查看池 B 中的虚拟机。

默认情况下，vCenter Server 可提供系统角色和样本角色：

系统角色

系统角色是永久的。不能编辑与这些角色关联的特权。

样本角色

VMware 可为某些频繁执行的任务组合提供样本角色。您可以克隆、修改或删除这些角色。

注 为避免丢失样本角色中的预定义设置，请先克隆角色，然后再对克隆进行修改。无法将样本重置为其默认设置。

用户只有在创建任务时其角色包含执行该任务所需的特权的情况下，才能调度任务。

注 即使所涉及到的用户已登录，对角色和特权的更改也会立即生效。但搜索除外，更改会在用户注销再重新登录之后才生效。

vCenter Server 和 ESXi 中的自定义角色

可以为 vCenter Server 及其管理的所有对象或者为各个主机创建自定义角色。

vCenter Server 自定义角色（推荐）

可使用 vSphere Web Client 中的角色编辑功能创建自定义角色，以创建符合用户需求的特权组。

ESXi 自定义角色

可以使用 CLI 或 vSphere Client 为各个主机创建自定义角色。请参见《使用 vSphere Client 管理 vSphere》文档。自定义主机角色无法从 vCenter Server 进行访问。

如果通过 vCenter Server 管理 ESXi 主机，则在主机和 vCenter Server 中维护自定义角色可能会导致混淆和误用。在大多数情况下，建议定义 vCenter Server 角色。

使用 vCenter Server 管理主机时，可以通过 vCenter Server 创建与该主机关联的权限并将其存储在 vCenter Server 上。如果直接连接到主机，则只有直接在主机上创建的角色才可用。

注 如果添加自定义角色，并不向其分配任何权限，则角色将创建为只读角色，且具有以下三个系统定义的权限：**System.Anonymous**、**System.View** 和 **System.Read**。



在 vSphere Web Client 中创建角色

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_egsyxkp4/uiConfId/49694343/)

vCenter Server 系统角色

角色是一组预定义的特权。向对象添加权限时，请将用户或组与角色配对。vCenter Server 包括多种无法更改的系统角色。

vCenter Server 系统角色

vCenter Server 提供少量默认角色。不能更改与默认角色关联的特权。默认角色以层次结构方式进行组织；每个角色将继承前一个角色的特权。例如，管理员角色继承只读角色的特权。您创建的角色不继承任何系统角色的特权。

管理员角色

分配有管理员角色的对象用户可在对象上查看和执行所有操作。此角色也包括只读角色固有的所有特权。如果您使用管理员角色对对象执行操作，可以将特权分配给各个用户和组。如果您使用管理员角色在 vCenter Server 中进行操作，可以将特权分配给默认 vCenter Single Sign-On 标识源中的用户和组。支持的身份服务包括 Windows Active Directory 和 OpenLDAP 2.4。

默认情况下，安装后，`administrator@vsphere.local` 用户将对 vCenter Single Sign-On 和 vCenter Server 具有管理员角色。该用户之后可以将其他用户与 vCenter Server 上的管理员角色相关联。

无权访问角色

分配有无权访问角色的对象用户不能以任何方式查看或更改对象。默认情况下向新用户和组分配此角色。可以逐对象更改角色。

`administrator@vsphere.local` 用户、`root` 用户和 `vpxuser` 用户是默认未分配无权访问角色的唯一用户。相反，它们分配有管理员角色。只要首先在 `root` 级别使用管理员角色创建替代权限并将此权限与另一个用户相关联，就可以从移除 `root` 用户的所有权限或将其角色更改为无权访问。

只读角色

分配有只读角色的对象用户可查看对象的状况和详细信息。具有此角色的用户可查看虚拟机、主机和资源池属性。该用户不能查看主机的远程控制台。通过菜单和工具栏执行的所有操作均被禁止。

创建自定义角色

您可以创建 vCenter Server 自定义角色，以满足环境的访问控制需求。

如果在与其他 vCenter Server 系统属于同一个 vCenter Single Sign-On 域的 vCenter Server 系统上创建或编辑一个角色，VMware Directory Service (vmdir) 会将您所做的更改传播到该组中的所有其他 vCenter Server 系统。对特定用户和对象的角色分配不会在 vCenter Server 系统上共享。

前提条件

验证您是否以具有管理员特权的用户身份登录。

步骤

- 1 通过 vSphere Web Client 登录到 vCenter Server。
- 2 选择“主页”，然后依次单击**管理**和**角色**。

- 3 单击**创建角色操作 (+)** 按钮。
- 4 键入新角色的名称。
- 5 选择角色的特权，然后单击**确定**。

克隆角色

可复制现有角色、重命名该角色，以及编辑该角色。在复制时，新角色不会应用到任何用户或组以及对象中。必须向用户或组以及对象分配该角色。

如果在与其他 vCenter Server 系统属于同一个 vCenter Single Sign-On 域的 vCenter Server 系统上创建或编辑一个角色，VMware Directory Service (vmdir) 会将您所做的更改传播到该组中的所有其他 vCenter Server 系统。对特定用户和对象的角色分配不会在 vCenter Server 系统上共享。

前提条件

验证您是否以具有管理员特权的用户身份登录。

步骤

- 1 通过 vSphere Web Client 登录到 vCenter Server。
- 2 选择“主页”，然后依次单击**管理**和**角色**。
- 3 选择某个角色，然后单击**克隆角色操作**图标。
- 4 键入克隆角色的名称。
- 5 为该角色选择或取消选择特权，然后单击**确定**。

编辑角色

编辑角色时，可更改为该角色选择的特权。完成后，这些特权将应用于分配了编辑后角色的所有用户或组。

如果在与其他 vCenter Server 系统属于同一个 vCenter Single Sign-On 域的 vCenter Server 系统上创建或编辑一个角色，VMware Directory Service (vmdir) 会将您所做的更改传播到该组中的所有其他 vCenter Server 系统。对特定用户和对象的角色分配不会在 vCenter Server 系统上共享。

前提条件

验证您是否以具有管理员特权的用户身份登录。

步骤

- 1 通过 vSphere Web Client 登录到 vCenter Server。
- 2 选择“主页”，然后依次单击**管理**和**角色**。
- 3 选择某一角色，然后单击**编辑角色操作**按钮。
- 4 为该角色选择或取消选择特权，然后单击**确定**。

角色和权限的最佳做法

使用角色和权限的最佳做法可充分提高 vCenter Server 环境的安全性和易管理性。

在 vCenter Server 环境中配置角色和权限时，VMware 建议采用以下最佳做法：

- 如果可能，请向组分配角色，而不要向单个用户分配角色，以便向该组授予特权。
- 仅授予对被需要对象的权限，仅向必须拥有特权的用户或组分配特权。使用最少权限数使得了解和管理权限结构变得更容易。
- 如果要为组分配限制性角色，请检查该组是否不包括管理员用户或其他具有管理特权的用户。否则，您可能无意识地限制了部分清单层次结构（已从中向该组分配了限制性角色）中管理员的特权。
- 使用文件夹对对象进行分组。例如，如果要授予对一组主机的修改权限并授予对另一组主机的查看权限，请将各组主机置于一个文件夹中。
- 向根 vCenter Server 对象添加权限时要小心。具有根级别特权的用户有权访问 vCenter Server 上的全局数据，例如，角色、自定义属性、vCenter Server 设置。
- 在大多数情况下，向对象分配权限时启用传播功能。这可确保当向清单层次结构中插入新对象时，它们会继承权限并且用户可以对其进行访问。
- 使用“无权访问”角色可屏蔽您希望特定用户或组无权访问的对象层次结构中的特定区域。
- 对许可证所做的更改会传播到链接到同一 Platform Services Controller 或同一 vCenter Single Sign-On 域中 Platform Services Controller 的所有 vCenter Server 系统，即使用户并未对所有 vCenter Server 系统拥有特权也会传播。

常见任务的所需特权

许多任务需要清单中多个对象的权限。您可查看执行任务所需的适用的特权以及适合的样本角色。

下表列出了需要多个特权的常见任务。可以通过将用户与其中一个预定义的角色配对来添加对清单对象的权限，或者可以创建具有所需特权集的自定义角色以多次使用。

如果要执行的任务不在此表中，以下规则可帮助您确定必须将权限分配到的位置以允许执行特定操作：

- 消耗存储空间的任何操作（例如创建虚拟磁盘或生成快照）都需要目标数据存储上的**数据存储.分配空间**特权，以及自我执行的特权。
- 在清单层次结构中移动对象需要对象自身、源父对象（如文件夹或群集）和目标父对象上的适当特权。
- 每个主机和群集有其自身的固有资源池，其中包含该主机或群集的所有资源。将虚拟机直接部署到主机或群集需要**资源.将虚拟机分配给资源池**特权。

表 4-4. 常见任务的所需特权

任务	所需特权	适用角色
创建虚拟机	在目标文件夹或数据中心上： <ul style="list-style-type: none"> ■ 虚拟机.清单.新建 ■ 虚拟机.配置.添加新磁盘（如果要创建新虚拟磁盘） ■ 虚拟机.配置.添加现有磁盘（如果使用现有虚拟磁盘） ■ 虚拟机.配置.裸设备（如果使用 RDM 或 SCSI 直通设备） 	管理员
	在目标主机、群集或资源池上： 资源.将虚拟机分配给资源池	资源池管理员或管理员
	在包含数据存储的目标数据存储或文件夹上： 数据存储.分配空间	数据存储用户或管理员
	在虚拟机将分配到的网络上： 网络.分配网络	网络用户或管理员
从模板部署虚拟机	在目标文件夹或数据中心上： <ul style="list-style-type: none"> ■ 虚拟机.清单.从现有项创建 ■ 虚拟机.配置.添加新磁盘 	管理员
	在模板或模板的文件夹上： 虚拟机.置备.部署模板	管理员
	在目标主机、群集或资源池上： 资源.将虚拟机分配给资源池	管理员
	在目标数据存储或数据存储的文件夹上： 数据存储.分配空间	数据存储用户或管理员
	在虚拟机将分配到的网络上： 网络.分配网络	网络用户或管理员
生成虚拟机快照	在虚拟机或虚拟机的文件夹上： 虚拟机.快照管理.创建快照	虚拟机超级用户或管理员
将虚拟机移动到资源池中	在虚拟机或虚拟机的文件夹上： <ul style="list-style-type: none"> ■ 资源.将虚拟机分配给资源池 ■ 虚拟机.清单.移动 	管理员
	在目标资源池上： 资源.将虚拟机分配给资源池	管理员
在虚拟机上安装客户机操作系统	在虚拟机或虚拟机的文件夹上： <ul style="list-style-type: none"> ■ 虚拟机.交互.回答问题 ■ 虚拟机.交互.控制台交互 ■ 虚拟机.交互.设备连接 ■ 虚拟机.交互.关闭电源 ■ 虚拟机.交互.打开电源 ■ 虚拟机.交互.重置 ■ 虚拟机.交互.配置 CD 媒体（如果从 CD 安装） ■ 虚拟机.交互.配置软盘媒体（如果从软盘安装） ■ 虚拟机.交互.VMware Tools 安装 	虚拟机超级用户或管理员

表 4-4. 常见任务的所需特权（续）

任务	所需特权	适用角色
	在包含安装媒体 ISO 映像的数据存储上： 数据存储.浏览数据存储 （如果从数据存储上的 ISO 映像安装） 在向其上载安装介质 ISO 映像的数据存储上： ■ 数据存储.浏览数据存储 ■ 数据存储.低级别文件操作	虚拟机超级用户或管理员
通过 vMotion 迁移虚拟机	在虚拟机或虚拟机的文件夹上： ■ 资源.迁移已打开电源的虚拟机 ■ 资源.将虚拟机分配给资源池 （如果目标资源池与源资源池不同）	资源池管理员或管理员
	在目标主机、群集或资源池上（如果与源主机、群集或资源池不同）： 资源.将虚拟机分配给资源池	资源池管理员或管理员
冷迁移（重定位）虚拟机	在虚拟机或虚拟机的文件夹上： ■ 资源.迁移已关闭电源的虚拟机 ■ 资源.将虚拟机分配给资源池 （如果目标资源池与源资源池不同）	资源池管理员或管理员
	在目标主机、群集或资源池上（如果与源主机、群集或资源池不同）： 资源.将虚拟机分配给资源池	资源池管理员或管理员
	在目标数据存储上（如果与源数据存储不同）： 数据存储.分配空间	数据存储用户或管理员
通过 Storage vMotion 迁移虚拟机	在虚拟机或虚拟机的文件夹上： 资源.迁移已打开电源的虚拟机	资源池管理员或管理员
	在目标数据存储上： 数据存储.分配空间	数据存储用户或管理员
将主机移动到群集	在主机上： 主机.清单.将主机添加到群集	管理员
	在目标群集上： 主机.清单.将主机添加到群集	管理员

确保 ESXi 主机安全

5

ESXi 虚拟化管理程序架构具有许多内置安全功能，如 CPU 隔离、内存隔离和设备隔离。您可以配置锁定模式、证书替换和智能卡身份验证等其他功能以增强安全性。

ESXi 主机还受防火墙保护。您可以根据需要打开入站和出站流量的端口，但应限制对服务和端口的访问。使用 ESXi 锁定模式并限制对 ESXi Shell 的访问有助于进一步构建更加安全的环境。从 vSphere 6.0 开始，ESXi 主机将加入证书基础架构。默认情况下，主机将使用 VMware 证书颁发机构 (VMCA) 签名的证书进行置备。

有关 ESXi 安全性的其他信息，请参见 VMware 白皮书《VMware vSphere Hypervisor 的安全性》。

本章讨论了以下主题：

- 使用脚本管理主机配置设置
- 使用主机配置文件配置 ESXi 主机
- 常规 ESXi 安全建议
- ESXi 主机的证书管理
- 使用安全配置文件自定义主机
- 为 ESXi 分配权限
- 使用 Active Directory 管理 ESXi 用户
- 使用 vSphere Authentication Proxy
- ESXi 安全性最佳做法
- 配置 ESXi 的智能卡身份验证
- ESXi SSH 密钥
- 使用 ESXi Shell
- 修改 ESXi Web 代理设置
- vSphere Auto Deploy 安全注意事项
- 管理 ESXi 日志文件

使用脚本管理主机配置设置

在包含许多主机的环境中，使用脚本管理主机比在 vSphere Web Client 中管理主机更快且不容易出错。

vSphere 包括用于主机管理的多种脚本编制语言。有关参考信息和编程提示，请参见《vSphere 命令行文档》和《vSphere API/SDK 文档》；有关脚本式管理的其他提示，请参见 VMware 社区。vSphere 管理员文档重点介绍了如何使用 vSphere Web Client 进行管理。

vSphere PowerCLI

VMware vSphere PowerCLI 是 vSphere API 的 Windows PowerShell 接口。vSphere PowerCLI 包括用于管理 vSphere 组件的 PowerShell cmdlet。

vSphere PowerCLI 包含超过 200 个 cmdlet、一组示例脚本和用于管理和自动化的函数库。请参见《vSphere PowerCLI 文档》。

vSphere Command-Line Interface (vCLI)

vCLI 包含用于管理 ESXi 主机和虚拟机的一组命令。此安装程序还会安装 vSphere SDK for Perl，它会运行 Windows 或 Linux 系统，并将安装 ESXCLI 命令、vicfg- 命令以及一组其他 vCLI 命令。请参见《vSphere Command-Line Interface 文档》。

从 vSphere 6.0 开始，还可以对 vCloud Suite SDK（如 vCloud Suite SDK for Python）使用其中一个脚本界面。

步骤

- 1 创建具有有限特权的自定义角色。

例如，考虑创建一个角色，该角色具有一组管理主机的特权但没有管理虚拟机、存储或网络的特权。如果只要使用脚本提取信息，则可为主机创建具有只读特权的角色。

- 2 在 vSphere Web Client 中，创建服务帐户并为其分配自定义角色。

如果要严格限制对特定主机的访问权限，则可以创建具有不同访问权限级别的多个自定义角色。

3 编写脚本以执行参数检查或修改，然后运行脚本。

例如，您可以检查或设置主机的 shell 交互式超时，如下所示：

语言	命令
vCLI (ESXCLI)	<pre>esxcli <conn_options> system settings advanced get / UserVars/ESXiShellTimeout esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list grep /UserVars/ ESXiShellTimeout</pre>
PowerCLI	<pre>#List UserVars.ESXiShellInteractiveTimeout for each host Get-VMHost Select Name, @{N="UserVars.ESXiShellInteractiveTimeout";E={\$_ Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeout Select -ExpandProperty Value}} # Set UserVars.ESXiShellTimeout to 900 on all hosts Get-VMHost Foreach { Get-AdvancedSetting -Entity \$_ -Name UserVars.ESXiShellInteractiveTimeout Set- AdvancedSetting -Value 900 }</pre>

- 在大型环境中，创建具有不同访问特权的角色并根据要执行的任务将主机分组到文件夹。然后从不同服务帐户对不同文件夹运行脚本。
- 运行命令后，确认更改已生效。

使用主机配置文件配置 ESXi 主机

使用主机配置文件，您可以设置 ESXi 主机的标准配置和自动化这些配置设置的合规性。使用主机配置文件，您可以控制主机配置的许多方面，其中包括内存、存储、网络等。

可以从 vSphere Web Client 中配置引用主机的主机配置文件，并将该主机配置文件应用到共享引用主机的特性的所有主机。还可以使用主机配置文件监控主机是否存在主机配置更改。请参见《vSphere 主机配置文件》文档。

可以将主机配置文件附加到群集以将其应用于群集中的所有主机。

步骤

- 设置引用主机规范并创建主机配置文件。
- 将配置文件附加到主机或群集。
- 将引用主机的主机配置文件应用到其他主机或群集。

常规 ESXi 安全建议

为了避免 ESXi 主机遭到未经授权的入侵和误用，VMware 对几个参数、设置和活动施加了一些限制。可以根据配置需求而放宽这些限制。但这样做之前，要确保在受信任的环境中工作且已经采取了足够的其他安全措施，以便保护整个网络和连接到主机的设备。

内置的安全功能

可如下降低主机的风险：

- 默认情况下，ESXi Shell 和 SSH 处于禁用状态。
- 默认情况下，只会打开有限的防火墙端口数目。您可以明确打开与特定服务关联的额外防火墙端口。
- ESXi 仅运行管理其功能所不可或缺的服务。分发仅限于运行 ESXi 所需的功能。
- 默认情况下，并非专用于对主机进行管理访问的所有端口均处于关闭状态。如果需要其他服务，则必须专门打开相应的端口。
- 默认情况下，弱密码被禁用，来自客户端的通信将通过 SSL 进行保护。用于保护通道安全的确切算法取决于 SSL 握手。在 ESXi 上创建的默认证书会使用带有 RSA 加密的 PKCS#1 SHA-256 作为签名算法。
- ESXi 在内部曾使用 Tomcat Web 服务来支持 Web 客户端进行的访问。Tomcat Web 服务经过修改后，仅运行 Web 客户端进行管理和监控所需的功能。因此，ESXi 不易遇到在更广泛的应用中所发现的 Tomcat 安全问题。
- VMware 监控可能影响 ESXi 安全的所有安全警示，并发布安全修补程序（如果需要）。
- 未安装诸如 FTP 和 Telnet 之类的不安全服务，且这些服务的端口在默认情况下是关闭的。由于 SSH 和 SFTP 等更为安全的服务易于获取，因此，请避免使用这些不安全的服务来支持更为安全的替代方案。例如，如果 SSH 不可用，请避免使用带有 SSL 的 Telnet 访问虚拟串行端口，而必须使用 Telnet。

如果必须使用不安全的服务，且已为主机实施了充分的保护措施，则可以明确打开相应端口以支持这些服务。

其他安全措施

评估主机安全和管理时请考虑以下建议。

限制访问

如果决定启用对直接控制台用户界面 (DCUI)、ESXi Shell 或 SSH 的访问，请实施严格的访问安全策略。

ESXi Shell 具有访问主机的某些部分的特权。只向信任的用户提供 ESXi Shell 登录访问权限。

请勿直接访问受管主机

使用 vSphere Web Client 来管理受 vCenter Server 管理的 ESXi 主机。请勿通过 vSphere Client 直接访问受管主机，且不要从主机的 DCUI 对受管主机执行更改。

如果使用脚本界面或 API 管理主机，请不要直接将主机作为目标。而是将管理主机的 vCenter Server 系统作为目标，并指定主机名称。

使用 vSphere Client 或 VMware CLI 或 API 管理独立 ESXi 主机

使用 vSphere Client、其中一个 VMware CLI 或 API 管理 ESXi 主机。以 root 用户身份从 DCUI 或 ESXi Shell 访问主机仅能进行故障排除。如果决定使用 ESXi Shell，请限制具有访问权限的帐户并设置超时。

仅使用 VMware 源来升级 ESXi 组件。

主机运行各种第三方软件包来支持管理界面或必须执行的任务。VMware 不支持从 VMware 源以外的任何其他源升级这些软件包。如果使用来自另一个源的下载文件或修补程序，就可能危及管理界面的安全或功能。定期查看第三方供应商站点和 VMware 知识库，以获知安全警示。

注 请遵循以下位置的 VMware 安全建议：<http://www.vmware.com/security/>。

ESXi 密码和帐户锁定

对于 ESXi 主机，您需要使用符合预定义要求的密码。您可以使用 `Security.PasswordQualityControl` 高级选项更改所需长度和字符类别要求或允许密码短语。

ESXi 使用 Linux PAM 模块 `pam_passwdqc` 进行密码管理和控制。有关详细信息，请参见 `pam_passwdqc` 的手册页。

注 ESXi 密码的默认要求因版本而异。您可以使用 `Security.PasswordQualityControl` 高级选项检查并更改默认的密码限制。

ESXi 密码

ESXi 对从直接控制台用户界面、ESXi Shell、SSH 或 vSphere Client 进行的访问强制执行密码要求。默认情况下，创建密码时必须包括四类字符：小写字母、大写字母、数字和特殊字符（如下划线或短划线）。

注 密码开头的大写字母不算入使用的字符类别数。密码结尾的数字不算入使用的字符类别数。

密码不能包含字典单词或部分字典单词。

ESXi 密码示例

以下候选密码说明选项设置如下时可以使用的密码。

```
retry=3 min=disabled,disabled,disabled,7,7
```

使用此设置时，不允许使用包含一种或两种类别字符的密码或不允许使用密码短语，因为前三项已禁用。使用三种和四种类别字符的密码需要 7 个字符。有关详细信息，请参见 `pam_passwdqc` 的手册页。

使用这些设置时，允许使用以下密码。

- **xQaTEhb!:** 包含由三类字符组成的八个字符。

- **xQaT3#A:** 包含由四类字符组成的七个字符。

下列候选密码不符合要求。

- **Xqat3hi:** 以大写字符开头，将有效字符类别数减少为两种。需要的最少字符类别数为三种。
- **xQaTEh2:** 以数字结尾，将有效字符种类数减少到两种。需要的最少字符类别数为三种。

ESXi 密码短语

您还可以使用密码短语代替密码，但是，默认情况下，密码短语处于禁用状态。您可以在 vSphere Web Client 中使用 `Security.PasswordQualityControl` 高级选项更改此默认值或其他设置。

例如，您可以将该选项更改为以下值。

```
retry=3 min=disabled,disabled,16,7,7
```

此示例允许密码短语的长度至少为 16 个字符，且至少包含 3 个单词，以空格分隔。

对于旧版主机，仍然支持更改 `/etc/pamd/passwd` 文件，但在将来的版本中将不再支持更改此文件。将来的版本将改用 `Security.PasswordQualityControl` 高级选项。

更改默认密码限制

您可以使用 ESXi 主机的 `Security.PasswordQualityControl` 高级选项更改密码或密码短语的默认限制。有关设置 ESXi 高级选项的信息，请参见《vCenter Server 和主机管理》文档。

例如，您可以将默认值更改为要求包含最少 15 个字符和最少 4 个字，如下所示：

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

有关详细信息，请参见 `pam_passwdqc` 的手册页。

注 并非 `pam_passwdqc` 选项的所有可能的组合均已经过测试。请在更改默认密码设置后执行额外的测试。

ESXi 帐户锁定行为

从 vSphere 6.0 开始，系统将支持对通过 SSH 和通过 vSphere Web Services SDK 进行的访问进行帐户锁定。直接控制台界面 (DCUI) 和 ESXi Shell 不支持帐户锁定。默认情况下，允许最多 10 次尝试，当这些尝试均失败后，才会锁定帐户。默认情况下，帐户将在两分钟后解锁。

配置登录行为

可以使用以下高级选项配置 ESXi 主机的登录行为：

- `Security.AccountLockFailures`。在锁定用户帐户之前允许的最多失败登录尝试次数。“零”将禁用帐户锁定。
- `Security.AccountUnlockTime`。用户被锁定的秒数。

有关设置 ESXi 高级选项的信息，请参见《vCenter Server 和主机管理》文档。

ESXi 网络连接安全建议

网络流量隔离对保护 ESXi 环境安全至关重要。不同的网络需要不同的访问权限和隔离级别。

您的 ESXi 主机使用了多个网络。针对每个网络采用适当的安全措施，并针对特定应用程序和功能隔离流量。例如，确保 vSphere vMotion 流量不会通过虚拟机所在的网络进行传输。隔离会阻止侦听。出于性能考虑，建议使用独立的网络。

- vSphere 基础架构网络用于 VMware vSphere vMotion®、VMware vSphere Fault Tolerance 和存储等功能。这些网络视为将针对其特定功能而隔离，并且通常不会在服务器机架的单个物理集外进行路由。
- 管理网络将客户端流量、命令行界面 (CLI) 或 API 流量，以及第三方软件流量与正常流量隔离。此网络应仅供系统、网络和安全管理员访问。使用跳转盒或虚拟专用网络 (VPN) 安全访问管理网络。严格控制在此网络内对潜在恶意软件源的访问。
- 虚拟机流量可以通过一个或多个网络流动。可以通过在虚拟网络控制器设置了防火墙规则的虚拟防火墙解决方案增强虚拟机的隔离。这些设置通过虚拟机传输，就像在您的 vSphere 环境中将其从主机迁移到主机一样。

禁用 Managed Object Browser (MOB)

Managed Object Browser 提供了一个浏览 VMkernel 对象模型的途径。但是，攻击者可以使用此界面执行恶意配置更改或操作，因为您可以使用 Managed Object Browser 更改主机配置。请仅在进行调试时使用 Managed Object Browser，并且请务必在生产系统中禁用该功能。

从 vSphere 6.0 开始，默认情况下禁用 MOB。但是，对于某些任务（如从系统提取旧证书），必须使用 MOB。

步骤

- 1 在 vSphere Web Client 中选择主机，然后转至**高级系统设置**。
- 2 检查 **Config.HostAgent.plugins.solo.enableMob** 的值，并根据需要进行更改。

不再建议从 ESXi Shell 中使用 `vim-cmd`。

禁用授权 (SSH) 密钥

通过授权密钥，您可在无需用户身份验证的情况下，通过 SSH 启用对 ESXi 主机的访问。为了提高主机安全性，请不要允许用户使用授权密钥访问主机。

如果某个用户的公用密钥在主机上的 `/etc/ssh/keys-root/authorized_keys` 文件中，则将其视为可信用户。允许可信远程用户在不提供密码的情况下访问主机。

步骤

- ◆ 对于日常操作，请禁用 ESXi 主机上的 SSH。
- ◆ 即使临时启用了 SSH，也要监控 `/etc/ssh/keys-root/authorized_keys` 文件的内容，确保不允许任何用户在未进行适当身份验证的情况下访问主机。

- ◆ 监控 `/etc/ssh/keys-root/authorized_keys` 文件，验证其是否为空且未将任何 SSH 密钥添加到该文件中。
- ◆ 如果发现 `/etc/ssh/keys-root/authorized_keys` 文件不为空，请移除所有密钥。

结果

禁用授权密钥远程访问可能会限制您在不提供有效登录名的情况下在主机上远程运行命令的能力。例如，这可能会阻止您运行无需人工干预的远程脚本。

ESXi 主机的证书管理

在 vSphere 6.0 及更高版本中，默认情况下，VMware Certificate Authority (VMCA) 将使用将 VMware 作为根证书颁发机构的签名证书置备每个新 ESXi 主机。在主机明确或作为安装或升级到 ESXi 6.0 或更高版本的一部分添加到 vCenter Server 时，便会进行置备。

您可以通过 vSphere Web Client 以及通过在 vSphere Web Services SDK 中使用 `vim.CertificateManager` API 来查看和管理这些证书。无法使用可用于管理 vCenter Server 证书的证书管理 CLI 查看或管理 ESXi 证书。

vSphere 5.5 和 vSphere 6.0 中的证书

在 ESXi 与 vCenter Server 进行通信时，二者将使用 SSL 处理几乎所有管理流量。

在 vSphere 5.5 及更低版本中，仅通过用户名、密码和指纹的组合来保护 SSL 端点。用户可以将对应的自签名证书替换为其自己的证书。请参见 vSphere 5.5 文档中心。

在 vSphere 6.0 及更高版本中，vCenter Server 支持 ESXi 主机的以下证书模式。

表 5-1. ESXi 主机的证书模式

证书模式	描述
VMware Certificate Authority (默认值)	<p>如果 VMCA 作为顶级 CA 或中间 CA 置备所有 ESXi 主机，则使用此模式。</p> <p>默认情况下，VMCA 将使用证书置备 ESXi 主机。</p> <p>在此模式中，您可以从 vSphere Web Client 刷新和续订证书。</p>
自定义证书颁发机构	<p>如果希望仅使用第三方 CA 签名的自定义证书，则使用此模式。</p> <p>在此模式中，您必须管理证书。您无法从 vSphere Web Client 刷新和续订证书。</p> <p>注 除非将证书模式更改为自定义证书颁发机构，否则在 vSphere Web Client 中选择续订等情况下，VMCA 可能会替换自定义证书。</p>
指纹模式	<p>vSphere 5.5 使用指纹模式，且此模式在 vSphere 6.0 中作为后备选项仍然可用。在此模式中，vCenter Server 会检查证书格式是否正确，但不会检查证书是否有效。甚至会接受已过期的证书。</p> <p>除非使用其他两种模式之一时遇到无法解决的问题，否则不要使用此模式。某些 vCenter 6.0 及更高版本服务在指纹模式下可能无法正常运行。</p>

证书过期

从 vSphere 6.0 开始，您可以在 vSphere Web Client 中查看有关由 VMCA 或第三方 CA 签名的证书的证书过期信息。您可以查看由 vCenter Server 管理的所有主机或单个主机的信息。如果证书处于**马上过期**状态（少于 8 个月），则将发出黄色警报。如果证书处于**快要过期**状态（少于 2 个月），则将发出红色警报。

ESXi 置备和 VMCA

从安装介质引导 ESXi 主机时，主机最初使用自动生成的证书。当主机添加到 vCenter Server 系统时，将使用 VMCA 作为根 CA 签名的证书置备主机。

该过程与使用 Auto Deploy 置备主机类似。但是，这些主机不会存储任何状态，因此签名的证书将由 Auto Deploy 服务器存储在其本地证书存储中。在 ESXi 主机后续引导时，将重新使用该证书。Auto Deploy 服务器是嵌入式部署或管理节点的一部分。

如果首次引导 Auto Deploy 主机时 VMCA 不可用，则主机将先尝试连接，然后在关闭和重新引导之间循环，直到 VMCA 可用且可以使用签名证书置备主机。

主机名称和 IP 地址更改

在 vSphere 6.0 及更高版本中，主机名称或 IP 地址更改会影响 vCenter Server 是否将主机的证书视为有效。将主机添加到 vCenter Server 的方式将影响是否需要人工干预。人工干预是指重新连接主机或从 vCenter Server 中移除主机，然后再重新添加该主机。

表 5-2. 主机名称或 IP 地址更改时需要人工干预

将主机添加到 vCenter Server 所使用的方式...	主机名称更改	IP 地址更改
主机名称	vCenter Server 连接问题。需要人工干预。	无需干预。
IP 地址	无需干预。	vCenter Server 连接问题。需要人工干预。



ESXi 证书管理

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_vkuyp3rf/uiConfId/49694343/)

主机升级和证书

如果将 ESXi 主机升级到 ESXi 6.0 或更高版本，升级过程会将自签名证书替换为 VMCA 签名证书。此过程会保留自定义证书，即使这些证书已过期或无效亦如此。

建议的升级工作流程取决于当前证书。

使用指纹证书置备的主机

如果主机当前使用指纹证书，则在升级过程中会自动为其分配 VMCA 证书。

注 无法使用 VMCA 证书置备旧版主机。您必须升级到 ESXi 6.0 或更高版本。

使用自定义证书置备的主机

如果主机使用自定义证书（通常是第三方 CA 签名的证书）置备，则这些证书将保留在原地。将证书模式更改为“自定义”以确保不会意外替换证书。

注 如果环境处于 VMCA 模式下，且您在 vSphere Web Client 中刷新证书，则任何现有证书将替换为 VMCA 签名的证书。

从今往后，vCenter Server 将在 vSphere Web Client 中监控证书并显示有关证书到期等的信息。

如果决定不将主机升级到 vSphere 6.0 或更高版本，则主机会保留其当前使用的证书，即使主机由使用 VMCA 证书的 vCenter Server 系统管理亦如此。

对于使用 Auto Deploy 置备的主机，在其首次使用 ESXi 6.0 软件引导时，将始终为其分配新证书。当升级使用 Auto Deploy 置备的主机时，Auto Deploy 服务器将为主机生成证书签名请求 (CSR) 并将其提交至 VMCA。VMCA 将存储主机的签名证书。Auto Deploy 服务器置备主机时，将从 VMCA 中检索证书并将其作为置备过程的一部分。

您可以将 Auto Deploy 与自定义证书配合使用。

ESXi 证书默认设置

vCenter Server 向 ESXi 主机请求证书签名请求 (CSR) 时，会使用默认设置。在许多情形下，大多数默认值都适用，但可以更改公司特定的信息。

考虑更改组织和位置信息。可以使用 vSphere Web Client 更改许多默认设置。请参见[更改证书默认设置](#)。

表 5-3. CSR 设置

参数	默认值	高级选项
密钥大小	2048	不适用
密钥算法	RSA	不适用
证书签名算法	sha256WithRSAEncryption	不适用
公用名称	如果按主机名称将主机添加到 vCenter Server，则为主机的名称。 如果按 IP 地址将主机添加到 vCenter Server，则为主机的 IP 地址。	不适用
国家/地区	美国	vpzd.certmgmt.certs.cn.country
电子邮件地址	vmca@vmware.com	vpzd.certmgmt.certs.cn.email
地点（市/县）	Palo Alto	vpzd.certmgmt.certs.cn.localityName
组织单位名称	VMware Engineering	vpzd.certmgmt.certs.cn.organizationalUnitName
组织名称	VMware	vpzd.certmgmt.certs.cn.organizationName
省/自治区/直辖市	加利福尼亚州	vpzd.certmgmt.certs.cn.state
证书的有效天数。	1825	vpzd.certmgmt.certs.cn.daysValid
证书到期的硬阈值。达到此阈值时，vCenter Server 会发出红色警报。	30 天	vpzd.certmgmt.certs.cn.hardThreshold
vCenter Server 证书有效性检查的轮询间隔。	5 天	vpzd.certmgmt.certs.cn.pollIntervalDays
证书到期的软阈值。达到此阈值时，vCenter Server 会引发事件。	240 天	vpzd.certmgmt.certs.cn.softThreshold
vCenter Server 用户确定是否替换现有证书的模式。更改此模式以在升级过程中保留自定义证书。请参见 主机升级和证书 。	默认值为 vmca 您还可以指定指纹或自定义。请参见 更改证书模式 。	vpzd.certmgmt.mode

查看多个 ESXi 主机的证书过期信息

如果使用的是 ESXi 6.0 及更高版本，则可以查看由 vCenter Server 系统管理的所有主机的证书状态。通过该显示，您可以确定任何证书是否即将过期。

可以在 vSphere Web Client 中查看正在使用 VMCA 模式的主机和正在使用自定义模式的主机的证书状态信息。无法查看处于指纹模式中的主机的证书状态信息。

步骤

- 1 浏览到 vSphere Web Client 清单层次结构中的主机。

默认情况下，主机显示不包含查证书状态。

- 2 右键单击“名称”字段，然后选择**显示/隐藏列**。

- 3 选择**证书有效期至**，单击**确定**，并根据需要滚动到右侧。

证书信息将显示证书过期的时间。

如果将主机添加到 vCenter Server 或主机在断开连接后重新连接，则 vCenter Server 会续订状态为“已过期”、“即将过期”、“马上过期”或“快要过期”的证书。如果证书有效期少于八个月，则状态为即将过期；如果证书有效期少于两个月，则状态为马上过期；如果证书有效期少于一个月，则状态为快要过期。

- 4 （可选）取消选择其他列可更方便地查看您所关注的内容。

后续步骤

续订即将过期的证书。请参见[续订或刷新 ESXi 证书](#)。

查看单个 ESXi 主机的证书详细信息

对于处于 VMCA 模式或自定义模式的 ESXi 6.0 及更高版本的主机，可以从 vSphere Web Client 中查看证书详细信息。有关证书的信息对调试很有帮助。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。

- 2 依次单击**管理**选项卡和**设置**。

- 3 选择**系统**，然后单击**证书**。

您可以检查以下信息。此信息仅在单主机视图中可用。

字段	描述
主题	在证书生成期间使用的主题。
颁发者	证书的颁发者。
有效期自	生成证书的日期。

字段	描述
有效期至	证书过期的日期。
状态	证书的状态，以下状态之一。
	<p>正常</p> <p>正常操作。</p> <p>即将过期</p> <p>证书即将过期。</p> <p>不久即将过期</p> <p>证书离过期还有 8 个月或少于 8 个月（默认）。</p> <p>即将过期</p> <p>证书离过期还有 2 个月或少于 2 个月（默认）。</p> <p>已过期</p> <p>证书无效，因为已过期。</p>

续订或刷新 ESXi 证书

如果 VMCA 将证书分配给 ESXi 主机（6.0 及更高版本），则可以从 vSphere Web Client 续订这些证书。您还可以刷新与 vCenter Server 关联的 TRUSTED_ROOTS 存储中的所有证书。

如果您的证书即将过期，或者如果由于其他原因要使用新证书置备主机，则可以续订证书。如果证书已过期，则必须与主机断开连接，然后重新进行连接。

默认情况下，每次将主机添加到清单或重新连接主机时，vCenter Server 都会续订状态为“已过期”、“立即过期”或“即将过期”的主机证书。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 依次单击**管理**选项卡和**设置**。
- 3 选择**系统**，然后单击**证书**。
可以查看有关所选主机证书的详细信息。
- 4 单击**续订或刷新 CA 证书**。

选项	描述
续订	从 VMCA 检索主机的全新签名证书。
刷新 CA 证书	将 vCenter Server VECS 存储的 TRUSTED_ROOTS 存储中的所有证书推送到主机。

- 5 单击**是**确认。

更改证书默认设置

当主机添加到 vCenter Server 系统时，vCenter Server 将向 VMCA 发送主机的证书签名请求 (CSR)。您可以使用 vSphere Web Client 中的 vCenter Server “高级设置” 更改 CSR 中的某些默认设置。

更改特定于公司的默认证书设置。有关默认设置的完整列表，请参见 [ESXi 证书默认设置](#)。某些默认设置不能更改。

步骤

- 1 在 vSphere Web Client 中，选择管理主机的 vCenter Server 系统。
- 2 依次单击**管理**选项卡和**设置**。
- 3 单击**高级设置**，然后单击**编辑**。
- 4 在“筛选器”方框中，输入 **certmgmt** 以仅显示证书管理参数。
- 5 根据公司策略更改现有参数的值，然后单击**确定**。

下次将主机添加到 vCenter Server 时，新的设置将用于 vCenter Server 发送到 VMCA 的 CSR 以及分配给主机的证书。

后续步骤

对证书元数据所做的更改只会影响新证书。如果要更改已由 vCenter Server 系统管理的主机的证书，则可以断开并重新连接主机。

了解证书模式切换

从 vSphere 6.0 开始，默认情况下，ESXi 主机将由 VMCA 使用证书进行置备。您可以改用自定义证书模式或用于调试的指纹模式。在大多数情况下，模式切换会造成破坏且没有必要。如果需要进行模式切换，请在开始之前检查潜在的影响。

在 vSphere 6.0 及更高版本中，vCenter Server 支持 ESXi 主机的以下证书模式。

表 5-4. ESXi 主机的证书模式

证书模式	描述
VMware Certificate Authority (默认值)	默认情况下，VMware Certificate Authority 将作为 ESXi 主机证书的 CA。默认情况下，VMCA 为根 CA，但可将其设置为其他 CA 的中间 CA。在此模式中，用户可以从 vSphere Web Client 中管理证书。如果 VMCA 是辅助证书，也将使用 VMCA。
自定义证书颁发机构	某些客户可能更愿意管理其自己的外部证书颁发机构。在此模式中，客户负责管理证书但无法在 vSphere Web Client 中管理证书。
指纹模式	vSphere 5.5 使用指纹模式，且此模式在 vSphere 6.0 中作为后备选项仍然可用。除非使用其他两种模式之一时遇到无法解决的问题，否则不要使用此模式。某些 vCenter 6.0 及更高版本服务在指纹模式下可能无法正常运行。

使用自定义 ESXi 证书

如果公司策略要求使用 VMCA 以外的根 CA，则可以在仔细规划后在您的环境中切换证书模式。建议的工作流如下：

- 1 获取要使用的证书。
- 2 将一个或多个主机置于维护模式，然后断开它们与 vCenter Server 的连接。
- 3 将自定义 CA 根证书添加到 VECS。
- 4 将自定义 CA 证书部署到每个主机，然后在该主机上重新启动服务。
- 5 切换到自定义 CA 模式。请参见[更改证书模式](#)。
- 6 将一个或多个主机连接到 vCenter Server 系统。

从自定义 CA 模式切换到 VMCA 模式

如果要使用自定义 CA 模式，且确定在您的环境中使用 VMCA 后会具有更优的性能，则可以在仔细规划后执行模式切换。建议的工作流如下：

- 1 移除 vCenter Server 系统中的所有主机。
- 2 在 vCenter Server 系统中，从 VECS 中移除第三方 CA 的根证书。
- 3 切换到 VMCA 模式。请参见[更改证书模式](#)。
- 4 将主机添加到 vCenter Server 系统。

注 此模式切换的任何其他工作流可能导致不可预知的行为。

在升级过程中保留指纹模式证书

如果使用 VMCA 证书时遇到问题，则可能需要从 VMCA 模式切换为指纹模式。在指纹模式中，vCenter Server 系统仅检查证书是否存在和是否正确格式化，而不会检查证书是否有效。有关说明，请参见[更改证书模式](#)。

从指纹模式切换到 VMCA 模式

如果使用指纹模式且要开始使用 VMCA 签名证书，则切换需要进行一些规划。建议的工作流如下：

- 1 移除 vCenter Server 系统中的所有主机。
- 2 切换到 VMCA 证书模式。请参见[更改证书模式](#)。
- 3 将主机添加到 vCenter Server 系统。

注 此模式切换的任何其他工作流可能导致不可预知的行为。

从自定义 CA 模式切换到指纹模式

如果在使用自定义 CA 时遇到问题，请考虑暂时切换到指纹模式。要实现顺利切换，请按照[更改证书模式](#)中的说明进行操作。模式切换之后，vCenter Server 系统将只检查证书的格式，不再检查证书本身是否有效。

从指纹模式切换到自定义 CA 模式

如果在故障排除期间将环境设置为指纹模式，且希望开始使用自定义 CA 模式，则必须首先生成所需的证书。建议的工作流如下：

- 1 移除 vCenter Server 系统中的所有主机。
- 2 将自定义 CA 根证书添加到 vCenter Server 系统上 VECS 中的 TRUSTED_ROOTS 存储区。请参见[更新 vCenter Server TRUSTED_ROOTS 存储（自定义证书）](#)。
- 3 对于每个 ESXi 主机：
 - a 部署自定义 CA 证书和密钥。
 - b 在主机上重新启动服务。
- 4 切换到自定义模式。请参见[更改证书模式](#)。
- 5 将主机添加到 vCenter Server 系统。

更改证书模式

在大多数情况下，使用 VMCA 在环境中置备 ESXi 主机是最佳解决方案。如果公司策略要求使用具有不同根 CA 的自定义证书，则可以编辑 vCenter Server 高级选项，以便在刷新证书时，不会使用 VMCA 证书自动置备主机。然后，您必须负责环境中的证书管理。

您可以使用 vCenter Server 高级设置更改为指纹模式或自定义 CA 模式。只能将指纹模式用作后备选项。

步骤

- 1 选择管理主机的 vCenter Server，然后单击**设置**。
- 2 单击**高级设置**，然后单击**编辑**。
- 3 在“筛选器”框中，输入 `certmgmt` 以仅显示证书管理密钥。
- 4 如果要管理自己的证书，请将 `vpxd.certmgmt.mode` 的值更改为**自定义**；如果要临时使用指纹模式，请将该值更改为**指纹**，然后单击**确定**。
- 5 重新启动 vCenter Server 服务。

替换 ESXi SSL 证书和密钥

您的安全策略可能要求您在每台主机上将默认的 ESXi SSL 证书替换为第三方 CA 签名的证书。

默认情况下，vSphere 组件使用在安装过程中创建的 VMCA 签名证书和密钥。如果意外删除 VMCA 签名证书，请从其 vCenter Server 系统中移除该主机，然后再重新添加该主机。在添加主机时，vCenter Server 会请求由 VMCA 颁发的新证书，并使用该证书置备主机。

如果公司策略有相关要求，则可以将 VMCA 签名证书替换为由受信任的 CA（商业 CA 或组织 CA）颁发的证书。

默认证书位于与 vSphere 5.5 证书相同的位置。您可以通过多种方式来将默认证书替换为受信任的证书。

注 您也可以使用 vSphere Web Services SDK 中的 `vim.CertificateManager` 和 `vim.host.CertificateManager` 受管对象。请参见 vSphere Web Services SDK 文档。

替换证书后，您必须在管理主机的 vCenter Server 系统上更新 VECS 中的 TRUSTED_ROOTS 存储，以确保 vCenter Server 和 ESXi 主机建立信任关系。

- **ESXi 证书签名请求的要求**

如果要使用第三方 CA（VMCA 作为辅助机构或自定义证书颁发机构）签名的证书，则必须将证书签名请求 (CSR) 发送至 CA。

- **从 ESXi Shell 替换默认证书和密钥**

可以从 ESXi Shell 替换默认的 VMCA 签名的 ESXi 证书。

- **通过 vifs 命令替换默认证书和密钥**

可以通过 vifs 命令替换默认的 VMCA 签名的 ESXi 证书。

- **通过 HTTPS PUT 替换默认证书**

可以使用第三方应用程序上载证书和密钥。支持 HTTPS PUT 操作的应用程序可以与 ESXi 包含的 HTTPS 接口配合使用。

- **更新 vCenter Server TRUSTED_ROOTS 存储（自定义证书）**

如果将 ESXi 主机设置为使用自定义证书，则必须在管理主机的 vCenter Server 系统上更新 TRUSTED_ROOTS 存储。

ESXi 证书签名请求的要求

如果要使用第三方 CA（VMCA 作为辅助机构或自定义证书颁发机构）签名的证书，则必须将证书签名请求 (CSR) 发送至 CA。

使用具有以下特性的 CSR：

- 2048 位
- PKCS1
- 无通配符
- 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）。

从 ESXi Shell 替换默认证书和密钥

可以从 ESXi Shell 替换默认的 VMCA 签名的 ESXi 证书。

前提条件

- 如果要使用第三方 CA 签名证书，请生成证书请求、将其发送至证书颁发机构，并将证书存储在每个 ESXi 主机上。

- 如果需要，从 vSphere Web Client 启用 ESXi Shell 或启用 SSH 流量。请参见《vSphere 安全性》出版物，了解有关启用对 ESXi Shell 访问的信息。
- 所有的文件传输和其他通信均通过安全 HTTPS 会话进行。用于验证会话的用户必须在主机上拥有**主机.配置.高级配置**特权。请参见《vSphere 安全性》出版物，了解有关通过角色分配特权的信息。

步骤

- 1 以管理员权限用户的身份登录 ESXi Shell，可直接从 DCUI 登录，也可从 SSH 客户端登录。
- 2 在 /etc/vmware/ssl 目录中，使用以下命令重命名现有证书。

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

- 3 将要使用的证书复制到 /etc/vmware/ssl。
- 4 将新证书和密钥重命名为 rui.crt 和 rui.key。
- 5 安装新证书之后重新启动主机。

或者也可以将主机置于维护模式，安装新证书，使用直接控制台用户界面 (DCUI) 重新启动管理代理，并将主机设置为退出维护模式。

后续步骤

更新 vCenter Server TRUSTED_ROOTS 存储。请参见 [更新 vCenter Server TRUSTED_ROOTS 存储（自定义证书）](#)。

通过 vifs 命令替换默认证书和密钥

可以通过 vifs 命令替换默认的 VMCA 签名的 ESXi 证书。

前提条件

- 如果要使用第三方 CA 签名证书，请生成证书请求、将其发送至证书颁发机构，并将证书存储在每个 ESXi 主机上。
- 如果需要，从 vSphere Web Client 启用 ESXi Shell 或启用 SSH 流量。请参见《vSphere 安全性》出版物，了解有关启用对 ESXi Shell 访问的信息。
- 所有的文件传输和其他通信均通过安全 HTTPS 会话进行。用于验证会话的用户必须在主机上拥有**主机.配置.高级配置**特权。请参见《vSphere 安全性》出版物，了解有关通过角色分配特权的信息。

步骤

- 1 备份现有证书。
- 2 按照证书颁发机构的说明生成证书请求。
- 3 如果拥有证书，请使用 vifs 命令通过与主机的 SSH 连接将证书上载到主机上合适的位置。

```
vifs --server hostname --username username --put rui.crt /host/ssl_cert
vifs --server hostname --username username --put rui.key /host/ssl_key
```

4 重新启动主机。

后续步骤

更新 vCenter Server TRUSTED_ROOTS 存储。请参见 [更新 vCenter Server TRUSTED_ROOTS 存储（自定义证书）](#)。

通过 HTTPS PUT 替换默认证书

可以使用第三方应用程序上载证书和密钥。支持 HTTPS PUT 操作的应用程序可以与 ESXi 包含的 HTTPS 接口配合使用。

前提条件

- 如果要使用第三方 CA 签名证书，请生成证书请求、将其发送至证书颁发机构，并将证书存储在每个 ESXi 主机上。
- 如果需要，从 vSphere Web Client 启用 ESXi Shell 或启用 SSH 流量。请参见《vSphere 安全性》出版物，了解有关启用对 ESXi Shell 访问的信息。
- 所有的文件传输和其他通信均通过安全 HTTPS 会话进行。用于验证会话的用户必须在主机上拥有**主机.配置.高级配置**特权。请参见《vSphere 安全性》出版物，了解有关通过角色分配特权的信息。

步骤

- 1 备份现有证书。
- 2 在上载应用程序中，如下处理每个文件：
 - a 打开文件。
 - b 将文件发布到以下位置之一。

选项	描述
证书	<code>https://hostname/host/ssl_cert</code>
密钥	<code>https://hostname/host/ssl_key</code>

位置 `/host/ssl_cert` 和 `host/ssl_key` 链接到 `/etc/vmware/ssl` 中的证书文件。

3 重新启动主机。

后续步骤

更新 vCenter Server TRUSTED_ROOTS 存储。请参见 [更新 vCenter Server TRUSTED_ROOTS 存储（自定义证书）](#)。

更新 vCenter Server TRUSTED_ROOTS 存储（自定义证书）

如果将 ESXi 主机设置为使用自定义证书，则必须在管理主机的 vCenter Server 系统上更新 TRUSTED_ROOTS 存储。

前提条件

将每台主机上的证书替换为自定义证书。

步骤

- 1 登录到管理 ESXi 主机的 vCenter Server 系统。
登录到已安装该软件的 Windows 系统，或登录到 vCenter Server Appliance shell。
- 2 运行 `vecs-cli` 以将新证书添加到 TRUSTED_ROOTS 存储，例如：

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt
--cert /etc/vmware/ssl/custom1.crt
```

选项	描述
Linux	<pre>/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert /etc/vmware/ssl/custom1.crt</pre>
Windows	<pre>C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert c:\ssl\custom1.crt</pre>

后续步骤

将证书模式设置为“自定义”。如果证书模式是默认值 **VMCA**，且您刷新证书，则自定义证书将替换为 **VMCA** 签名的证书。请参见[更改证书模式](#)。

在 Auto Deploy 中使用自定义证书

默认情况下，Auto Deploy 服务器使用 **VMCA** 签名的证书置备每个主机。您可以将 Auto Deploy 服务器设置为使用未经 **VMCA** 签名的自定义证书置备所有主机。在这种情况下，Auto Deploy 服务器将成为第三方 CA 的辅助证书颁发机构。

前提条件

- 从您的 CA 请求符合您的要求的证书。
 - 密钥大小：2048 位或更大（PEM 编码）
 - PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。密钥添加到 VECS 后，会转换为 PKCS8
 - x509 版本 3
 - 对于 root 证书，CA 扩展必须设置为 **true**，并且 **cert** 签名必须在要求列表中。

- SubjectAltName 必须包含 DNS Name=<machine_FQDN>
- CRT 格式
- 包含以下密钥使用：数字签名、不可否认性、密钥加密
- 比当前时间早一天的开始时间
- CN（和 SubjectAltName）设置为 vCenter Server 清单中的 ESXi 主机的主机名（或 IP 地址）。
- 将证书和密钥文件分别命名为 rbd-ca.crt 和 rbd-ca.key。

步骤

- 1 备份默认的 ESXi 证书。
该证书位于 /etc/vmware-rbd/ssl/ 中。
- 2 在 vSphere Web Client 中，停止 Auto Deploy 服务。
 - a 选择**系统管理**，然后在**部署**下单击**系统配置**。
 - b 单击**服务**。
 - c 右键单击要停止的服务，然后选择**停止**。
- 3 在运行 Auto Deploy 服务的系统上，将 /etc/vmware-rbd/ssl/ 中的 rbd-ca.crt 和 rbd-ca.key 替换为您的自定义证书和密钥文件。
- 4 在运行 Auto Deploy 服务的系统上，更新 VECS 中的 TRUSTED_ROOTS 存储以使用您的新证书。

```
vecs-cli entry delete --store TRUSTED_ROOTS --alias
                        rbd_cert
vecs-cli entry create --store TRUSTED_ROOTS --alias
                        rbd_cert --cert /etc/vmware-rbd/ssl/rbd-ca.crt
```

Windows

C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli.exe

Linux

/usr/lib/vmware-vmafd/bin/vecs-cli

- 5 创建包含 TRUSTED_ROOTS 中内容的 castore.pem 文件，并将该文件放入 /etc/vmware-rbd/ssl/ 目录中。
在自定义模式中，您必须维护此文件。
- 6 将 vCenter Server 系统的证书模式更改为**自定义**。
请参见[更改证书模式](#)。
- 7 重新启动 vCenter Server 服务，然后启动 Auto Deploy 服务。

结果

下次置备设置为使用 Auto Deploy 的主机时，Auto Deploy 服务器将使用您刚添加到 TRUSTED_ROOTS 存储的根证书生成证书。

还原 ESXi 证书和密钥文件

使用 vSphere Web Services SDK 替换 ESXi 主机上的证书时，之前的证书和密钥将附加到 .bak 文件。通过将 .bak 文件中的信息移动到当前证书和密钥文件中，可以还原之前的证书。

主机证书和密钥位于 /etc/vmware/ssl/rui.crt 和 /etc/vmware/ssl/rui.key 中。使用 vSphere Web Services SDK vim.CertificateManager 受管对象替换主机证书和密钥时，之前的密钥和证书将附加到 /etc/vmware/ssl/rui.bak 文件。

注 如果通过 HTTP PUT、vifs 或 ESXi Shell 替换证书，则现有证书不会附加到 .bak 文件。

步骤

- 1 在 ESXi 主机上，找到 /etc/vmware/ssl/rui.bak 文件。

该文件具有以下格式：

```
#
# Host private key and certificate backup from 2014-06-20 08:02:49.961
#

-----BEGIN PRIVATE KEY-----
previous key
-----END PRIVATE KEY-----

-----BEGIN CERTIFICATE-----
previous cert
-----END CERTIFICATE-----
```

- 2 将开头为 -----BEGIN PRIVATE KEY----- 且结尾为 -----END PRIVATE KEY----- 的文本复制到 /etc/vmware/ssl/rui.key 文件中。

包括 -----BEGIN PRIVATE KEY----- 和 -----END PRIVATE KEY-----。

- 3 将 -----BEGIN CERTIFICATE----- 与 -----END CERTIFICATE----- 之间的文本复制到 /etc/vmware/ssl/rui.crt 文件中。

包括 -----BEGIN CERTIFICATE----- 和 -----END CERTIFICATE-----。

- 4 重新启动主机或将 ssl_reset 事件发送至使用密钥的所有服务。

```
for s in /etc/init.d/*; do $s | grep ssl_reset > /dev/null; if [ $?== 0 ]; then $s
ssl_reset; fi; done
```

使用安全配置文件自定义主机

可以通过 vSphere Web Client 中提供的“安全配置文件”面板自定义大多数基本安全设置。“安全配置文件”对单台主机管理特别有用。如果要管理多台主机，请考虑使用 CLI 或 SDK 之一，并自动执行自定义。

ESXi 防火墙配置

ESXi 包括默认启用的防火墙。

安装时，会配置 ESXi 防火墙以阻止除主机安全配置文件中启用的服务相关的流量之外的所有入站和出站流量。

打开防火墙端口时，应考虑不限制访问 ESXi 主机上运行的服务可能使主机遭受外部攻击及未经授权的访问。通过将 ESXi 防火墙配置为仅允许从授权网络访问来降低该风险。

注 此防火墙还允许 Internet 控制消息协议 (ICMP) ping 及与 DHCP 和 DNS（仅 UDP）客户端的通信。

可以如下所示管理 ESXi 防火墙端口：

- 在 vSphere Web Client 中使用每个主机的安全配置文件。请参见管理 [ESXi 防火墙设置](#)
- 从命令行或在脚本中使用 ESXCLI 命令。请参见 [ESXi ESXCLI 防火墙命令](#)。
- 如果安全配置文件中不包括要打开的端口，则使用自定义 VIB。

可以使用 VMware Lab 提供的 vibauthor 工具创建自定义 VIB。要安装自定义 VIB，必须将 ESXi 主机的接受程度改为 CommunitySupported。请参见 VMware 知识库文章 [2007381](#)。

注 如果请求 VMware 技术支持调查安装了 CommunitySupported VIB 的 ESXi 主机上的问题，VMware 支持可能会在故障排除过程中请求卸载此 CommunitySupported VIB 作为故障排除步骤，以确定该 VIB 是否与调查的问题相关。



ESXi 防火墙概念

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_8qp59yqe/uiConfId/49694343/)

NFS 客户端规则集 (nfsClient) 的行为与其他规则集不同。启用 NFS 客户端规则集后，将在允许的 IP 地址列表中打开目标主机的所有出站 TCP 端口。有关详细信息，请参见 [NFS 客户端防火墙行为](#)。

管理 ESXi 防火墙设置

可以通过 vSphere Web Client 或在命令行中为服务或管理代理配置入站和出站防火墙连接。

注 如果不同的服务具有重叠的端口规则，则启用一项服务可能会隐式启用其他服务。为了避免此问题，可以指定允许哪些 IP 地址访问主机上的各个服务。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 依次单击**管理**选项卡和**设置**。

3 单击**安全配置文件**。

vSphere Web Client 将显示相应防火墙端口的活动入站和出站连接列表。

4 在“防火墙”部分中，单击**编辑**。

屏幕将显示防火墙规则集，其中包括规则的名称和相关信息。

5 选择要启用的规则集，或取消选择要禁用的规则集。

列	描述
入站端口和出站端口	vSphere Web Client 为服务打开的端口
协议	服务使用的协议。
守护进程	与服务关联的守护进程的状态

6 对于某些服务，可以管理服务详细信息。

- 使用**启动**、**停止**或**重新启动**按钮可临时更改服务的状态。
- 更改“启动策略”让服务根据主机或端口使用情况启动。

7 对于某些服务，可以明确指定允许连接的 IP 地址。

请参见 为 ESXi 主机添加允许的 IP 地址。

8 单击**确定**。

为 ESXi 主机添加允许的 IP 地址

默认情况下，可以通过每个服务的防火墙访问所有 IP 地址。要限制流量，请更改每个服务，以便仅允许来自管理子网的流量。如果您的环境不使用某些服务，也可以取消选择这些服务。

可以使用 vSphere Web Client、vCLI 或 PowerCLI 更新服务的允许的 IP 列表。默认情况下，服务允许所有 IP 地址。



将允许的 IP 地址添加到 ESXi 防火墙

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_Ougsspa2/uiConfId/49694343/)

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 依次单击**管理**选项卡和**设置**。
- 3 在“系统”下，单击**安全配置文件**。
- 4 在“防火墙”部分中，单击**编辑**，然后从列表中选择服务。
- 5 在“允许的 IP 地址”部分中，取消选择**允许从任何 IP 地址连接**，然后输入允许连接到主机的网络的 IP 地址。

使用逗号分隔 IP 地址。可以使用以下地址格式：

- 192.168.0.0/24

- 192.168.1.2, 2001::1/64
- fd3e:29a6:0a81:e478::/64

6 单击**确定**。

ESXi 主机的入站和出站防火墙端口

通过 vSphere Web Client，您可以打开和关闭每个服务的防火墙端口或允许来自选定 IP 地址的流量。

下表列出了为通常所安装的服务配置的防火墙。如果在主机上安装其他 VIB，则可能还会配置其他服务和防火墙端口。

表 5-5. 入站防火墙连接

服务	端口	备注
CIM 服务器	5988 (TCP)	适用于 CIM（公用信息模型）的服务器。
CIM 安全服务器	5989 (TCP)	适用于 CIM 的安全服务器。
CIM SLP	427 (TCP、UDP)	CIM 客户端使用服务位置协议版本 2 (SLPv2) 查找 CIM 服务器。
DHCPv6	546 (TCP、UDP)	IPv6 的 DHCP 客户端。
DVSSync	8301、8302 (UDP)	DVSSync 端口可用于同步已启用 VMware FT 记录/重放的主机之间的分布式虚拟端口的状况。只有运行主虚拟机或备份虚拟机的主机才须打开这些端口。未使用 VMware FT 的主机无需打开这些端口。
NFC	902 (TCP)	网络文件复制 (NFC) 可为 vSphere 组件提供文件类型感知 FTP 服务。默认情况下，ESXi 将 NFC 用于在数据存储之间复制和移动数据等操作。
Virtual SAN 群集服务	12345、23451 (UDP)	Virtual SAN 群集监控和成员资格目录服务。使用基于 UDP 的 IP 多播可建立群集成员并向所有群集成员分发 Virtual SAN 元数据。如果禁用，则 Virtual SAN 无法工作。
DHCP 客户端	68 (UDP)	IPv4 的 DHCP 客户端。
DNS 客户端	53 (UDP)	DNS 客户端。
Fault Tolerance	8200、8100、8300 (TCP、UDP)	主机之间的流量，用于 vSphere Fault Tolerance (FT)。
NSX 分布式逻辑路由器服务	6999 (UDP)	NSX 虚拟分布式路由器服务。如果已安装 NSX VIB 且已创建 VDR 模块，则与此服务关联的防火墙端口将打开。如果没有 VDR 实例与主机关联，则该端口无需打开。 此服务在此产品的早期版本中称为“NSX 分布式逻辑路由器”。
Virtual SAN 传输	2233 (TCP)	Virtual SAN 可靠数据报传输。使用 TCP，并用于 Virtual SAN 存储 IO。如果禁用，则 Virtual SAN 无法工作。
SNMP 服务器	161 (UDP)	允许主机连接到 SNMP 服务器。

表 5-5. 入站防火墙连接（续）

服务	端口	备注
SSH 服务器	22 (TCP)	SSH 访问时为必需项。
vMotion	8000 (TCP)	通过 vMotion 迁移虚拟机时为必需项。
vSphere Web Client	902、443 (TCP)	客户端连接
vsanvp	8080 (TCP)	VSAN VASA 供应商提供程序。由 vCenter 中的存储管理服务 (SMS) 使用，以访问有关 Virtual SAN 存储配置文件、功能和合规性的信息。如果禁用，则 Virtual SAN 基于存储配置文件的管理 (SPBM) 无法工作。
vSphere Web Access	80 (TCP)	“欢迎使用”页面，包含不同界面的下载链接。
RFB 协议	5900-5964 (TCP)	由 VNC 等管理工具使用。

表 5-6. 出站防火墙连接

服务	端口	备注
CIM SLP	427 (TCP、UDP)	CIM 客户端使用服务位置协议版本 2 (SLPv2) 查找 CIM 服务器。
DHCPv6	547 (TCP、UDP)	IPv6 的 DHCP 客户端。
DVSSync	8301、8302 (UDP)	DVSSync 端口可用于同步已启用 VMware FT 记录/重放的主机之间的分布式虚拟端口的状况。只有运行主虚拟机或备份虚拟机的主机才须打开这些端口。未使用 VMware FT 的主机无需打开这些端口。
HBR	44046、31031 (TCP)	用于 vSphere Replication 和 VMware Site Recovery Manager 的持续复制流量。
NFC	902 (TCP)	网络文件复制 (NFC) 可为 vSphere 组件提供文件类型感知 FTP 服务。默认情况下，ESXi 将 NFC 用于在数据存储之间复制和移动数据等操作。
WOL	9 (UDP)	由 Wake on LAN 使用。
Virtual SAN 群集服务	12345、23451 (UDP)	由 Virtual SAN 使用的群集监控、成员资格和目录服务。
DHCP 客户端	68 (UDP)	DHCP 客户端。
DNS 客户端	53 (TCP、UDP)	DNS 客户端。
Fault Tolerance	80、8200、8100、8300 (TCP、UDP)	支持 VMware Fault Tolerance。
软件 iSCSI 客户端	3260 (TCP)	支持软件 iSCSI。
NSX 分布式逻辑路由器服务	6999 (UDP)	如果已安装 NSX VIB 且已创建 VDR 模块，则与此服务关联的防火墙端口将打开。如果没有 VDR 实例与主机关联，则该端口无需打开。

表 5-6. 出站防火墙连接（续）

服务	端口	备注
rabbitmqproxy	5671 (TCP)	在 ESXi 主机上运行的代理，允许虚拟机内部运行的应用程序与 vCenter 网络域中运行的 AMQP 代理进行通信。虚拟机不必位于网络中，即无需网卡。代理将连接到 vCenter 网络域中的代理。因此，出站连接 IP 地址应至少包括当前正在使用的代理或未来的代理。如果客户要扩展，则可以添加代理。
Virtual SAN 传输	2233 (TCP)	用于 Virtual SAN 节点之间的 RDT 流量（单播点对点通信）。
vMotion	8000 (TCP)	通过 vMotion 迁移虚拟机时为必需项。
VMware vCenter Agent	902 (UDP)	vCenter Server 代理。
vsanvp	8080 (TCP)	用于 Virtual SAN 供应商提供程序流量。

NFS 客户端防火墙行为

NFS 客户端防火墙规则集的行为方式与其他 ESXi 防火墙规则集不同。挂载或卸载 NFS 数据存储时，ESXi 将配置 NFS 客户端设置。对于不同版本的 NFS，行为有所不同。

添加、挂载或卸载 NFS 数据存储时，产生的行为取决于 NFS 版本。

NFS v3 防火墙行为

添加或挂载 NFS v3 数据存储时，ESXi 将检查 NFS 客户端 (nfsClient) 防火墙规则集的状态。

- 如果禁用了 nfsClient 规则集，则 ESXi 将启用规则集，并通过将 allowedAll 标记设置为 FALSE 来禁用“允许所有 IP 地址”策略。NFS 服务器的 IP 地址将会添加到允许的出站 IP 地址的列表中。
- 如果启用了 nfsClient 规则集，则规则集状态和允许的 IP 地址策略将不会更改。NFS 服务器的 IP 地址将会添加到允许的出站 IP 地址的列表中。

注 如果手动启用 nfsClient 规则集或手动设置“允许所有 IP 地址”策略，则将 NFS v3 数据存储添加到系统之前或之后，卸载最新 NFS v3 数据存储时将替代您的设置。卸载所有 NFS v3 数据存储时，将禁用 nfsClient 规则集。

移除或卸载 NFS v3 数据存储时，ESXi 会执行以下操作之一。

- 如果未从已卸载数据存储的服务器挂载任何剩余的 NFS v3 数据存储，则 ESXi 将从出站 IP 地址列表中移除该服务器的 IP 地址。
- 如果执行卸载操作后没有剩余任何挂载的 NFS v3 数据存储，则 ESXi 将禁用 nfsClient 防火墙规则集。

NFS v4.1 防火墙行为

挂载第一个 NFS v4.1 数据存储时，ESXi 将启用 nfs41client 规则集并将其 allowedAll 标记设置为 TRUE。此操作将打开所有 IP 地址的端口 2049。卸载 NFS v4.1 数据存储不会影响防火墙状态。也就是说，第一个 NFS v4.1 挂载将打开端口 2049，除非明确关闭该端口，否则该端口将保持启用状态。

ESXi ESXCLI 防火墙命令

如果环境包含多个 ESXi 主机，则建议使用 ESXCLI 命令或 vSphere Web Services SDK 自动化防火墙配置。

可以使用 ESXi Shell 或 vSphere CLI 命令在命令行处配置 ESXi 以自动化防火墙配置。有关介绍，请参见 vSphere Command-Line Interface 入门；有关使用 ESXCLI 操作防火墙和防火墙规则的示例，请参见《vSphere 命令行界面概念和示例》。

表 5-7. 防火墙命令

命令	描述
<code>esxcli network firewall get</code>	返回防火墙的启用或禁用状态，并列出默认操作。
<code>esxcli network firewall set --default-action</code>	设置为 true 可设置要传递的默认操作；设置为 false 可设置要丢弃的默认操作。
<code>esxcli network firewall set --enabled</code>	启用或禁用 ESXi 防火墙。
<code>esxcli network firewall load</code>	加载防火墙模块和规则集配置文件。
<code>esxcli network firewall refresh</code>	如果已加载防火墙模块，则通过读取规则集文件来刷新防火墙配置。
<code>esxcli network firewall unload</code>	破坏过滤器并卸载防火墙模块。
<code>esxcli network firewall ruleset list</code>	列出规则集信息。
<code>esxcli network firewall ruleset set --allowed-all</code>	设置为 true 可允许对所有 IP 具有完全访问权限；设置为 false 可使用允许的 IP 地址的列表。
<code>esxcli network firewall ruleset set --enabled --ruleset-id=<string></code>	将 enabled 设置为 true 或 false 可启用或禁用指定的规则集。
<code>esxcli network firewall ruleset allowedip list</code>	列出指定规则集允许的 IP 地址。
<code>esxcli network firewall ruleset allowedip add</code>	允许从指定的 IP 地址或 IP 地址范围访问规则集。
<code>esxcli network firewall ruleset allowedip remove</code>	从指定的 IP 地址或 IP 地址范围移除对规则集的访问。
<code>esxcli network firewall ruleset rule list</code>	列出防火墙中的每个规则集的规则。

从安全配置文件自定义 ESXi 服务

ESXi 主机包含默认情况下处于运行状态的多项服务。其他服务（例如 SSH）包含在主机的安全配置文件中。如果公司策略允许，则可以根据需要启用或禁用这些服务。

使用 vSphere Web Client 启用对 ESXi Shell 的访问是如何启用某项服务的示例。

注 启用服务会影响主机的安全性。除非绝对必要，否则不要启用服务。

可用服务取决于 ESXi 主机上安装的 VIB。如果未安装 VIB，则无法添加服务。某些 VMware 产品（例如 vSphere HA）会在主机上安装 VIB，并使服务和相应的防火墙端口可用。

在默认安装中，可以在 vSphere Web Client 中修改以下服务的状态。

表 5-8. 安全配置文件中的 ESXi 服务

服务	默认	描述
直接控制台 UI	正在运行	通过直接控制台用户界面 (DCUI) 服务，您可以使用基于文本的菜单从本地控制台主机与 ESXi 主机进行交互。
ESXi Shell	已停止	ESXi Shell 可在直接控制台用户界面中使用，并包含一组完全受支持的命令和一组用于故障排除和修复的命令。必须从每个系统的直接控制台启用对 ESXi Shell 的访问。可以启用对本地 ESXi Shell 的访问或对 ESXi Shell 和 SSH 的访问。
SSH	已停止	允许通过安全 Shell 进行远程连接的主机的 SSH 客户端服务。
基于负载的成组守护进程	正在运行	基于负载的成组。
本地安全身份验证服务器 (Active Directory 服务)	已停止	Active Directory 服务的一部分。为 Active Directory 配置 ESXi 时，将启动此服务。
I/O 重定向器 (Active Directory 服务)	已停止	Active Directory 服务的一部分。为 Active Directory 配置 ESXi 时，将启动此服务。
网络登录服务器 (Active Directory 服务)	已停止	Active Directory 服务的一部分。为 Active Directory 配置 ESXi 时，将启动此服务。
NTP 守护进程	已停止	网络时间协议守护进程。
CIM 服务器	正在运行	公用信息模型 (CIM) 应用程序可以使用的服务。
SNMP 服务器	已停止	SNMP 守护进程。有关配置 SNMP v1、v2 和 v3 的信息，请参见《vSphere 监控和性能》。
Syslog 服务器	已停止	Syslog 守护进程。可以在 vSphere Web Client 的“高级系统设置”中启用 syslog。请参见《vSphere 安装和设置》。
vSphere High Availability Agent	已停止	支持 vSphere High Availability 功能。
VProbe 守护进程	已停止	VProbe 守护进程。
VMware vCenter Agent	正在运行	vCenter Server 代理。允许 vCenter Server 连接到 ESXi 主机。具体来说，vpxa 是与 ESXi 内核通信的主机守护进程的通信媒介。
X.Org 服务器	已停止	X.Org 服务器。此可选功能在内部用于虚拟机的 3D 图形。

在安全配置文件中启用或禁用服务

您可以从 vSphere Web Client 启用和禁用“安全配置文件”中列出的服务之一。

安装完成后，默认情况下某些服务处于运行状态，而其他服务为停止状态。在某些情况下，需要先进行其他设置，然后才能在 vSphere Web Client UI 中使用某项服务。例如，NTP 服务是获取准确时间信息的一种方式，但此服务只能在防火墙中打开所需端口的情况下运作。

前提条件

使用 vSphere Web Client 连接到 vCenter Server。

步骤

- 1 在 vSphere Web Client 清单中浏览到某个主机，然后选择该主机。
- 2 依次单击**管理**选项卡和**设置**。
- 3 在“系统”下，选择**安全配置文件**，然后单击**编辑**。
- 4 滚动到要更改的服务。
- 5 在“服务详细信息”窗格中，选择**启动**、**停止**或**重新启动**以对主机状态进行一次性更改，或从**启动策略**菜单中进行选择，以更改重新引导过程中主机的状态。
 - **如果任何端口打开则自动启动，如果所有端口关闭则停止：**这些服务的默认设置。如果任何端口打开，则客户端会尝试联系服务的网络资源。如果某些端口已打开，但特定服务的端口已关闭，则该尝试将失败。当适用的出站端口打开时，此服务将开始完成其启动。
 - **与主机一起启动和停止：**服务在主机启动后立即启动，并在主机关机前不久关闭。此选项与**如果任何端口打开则自动启动，如果所有端口关闭则停止**非常相似，都意味着此服务定期尝试完成其任务（例如尝试连接指定的 NTP 服务器）。如果端口先是处于关闭状态，但随后又打开了，客户端将在此后不久开始完成其任务。
 - **手动启动和停止：**无论端口打开与否，主机都会保留用户指定的服务设置。当用户启动 NTP 服务后，只要主机仍然开启，该服务会一直运行。如果服务已启动且主机已关闭，该服务将在关机过程中停止，但是，主机一启动，该服务将再次启动，保留用户确定的状况。

注 这些设置仅适用于通过 vSphere Web Client 配置的服务设置或使用 vSphere Web Services SDK 创建的应用程序。通过其他方式（例如通过 ESXi Shell 或配置文件）进行的配置不会受这些设置的影响。

锁定模式

要提高 ESXi 主机的安全性，可以将其置于锁定模式。在锁定模式下，默认情况下，操作必须通过 vCenter Server 执行。

从 vSphere 6.0 开始，您可以选择正常锁定模式或严格锁定模式，这两种模式可提供不同的锁定程度。vSphere 6.0 还引入了“例外用户”列表。主机进入锁定模式时，例外用户不会丢失其特权。使用“例外用户”列表可添加在主机处于锁定模式时需要直接访问主机的第三方解决方案和外部应用程序帐户。请参见**指定锁定模式异常用户**。



vSphere 6 中的锁定模式

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_zg4ylgu0/uiConfId/49694343/)

正常锁定模式和严格锁定模式

从 vSphere 6.0 开始，您可以选择正常锁定模式或严格锁定模式，这两种模式可提供不同的锁定程度。

正常锁定模式

在正常锁定模式下，DCUI 服务未停止。如果与 vCenter Server 系统的连接断开且无法再通过 vSphere Web Client 进行访问，则特权帐户可以登录到 ESXi 主机的直接控制台界面并退出锁定模式。只有以下帐户可以访问直接控制台用户界面：

- 锁定模式下“例外用户”列表中对主机具有管理员特权的帐户。“例外用户”列表针对用于执行非常特殊的任务的服务帐户提供。将 ESXi 管理员添加到此列表违背了锁定模式的初衷。
- 在主机的 DCUI.Access 高级选项中定义的用户。此选项用于在与 vCenter Server 的连接断开时紧急访问直接控制台界面。这些用户不需要拥有对主机的管理特权。

严格的锁定模式

在严格锁定模式（该模式是 vSphere 6.0 中的新功能）下，DCUI 服务已停止。如果与 vCenter Server 的连接断开且 vSphere Web Client 不再可用，则 ESXi 主机将变为不可用，除非启用 ESXi Shell 和 SSH 服务并定义例外用户。如果无法恢复与 vCenter Server 系统的连接，则必须重新安装主机。

锁定模式及 ESXi Shell 和 SSH 服务

严格锁定模式会停止 DCUI 服务。但是，ESXi Shell 和 SSH 服务不受锁定模式影响。要使锁定模式成为有效的安全措施，请确保 ESXi Shell 和 SSH 服务也处于禁用状态。默认情况下，这些服务处于禁用状态。

在主机处于锁定模式下时，如果“例外用户”列表中的用户拥有对主机的管理员角色，则可以从 ESXi Shell 及通过 SSH 访问主机。即使在严格锁定模式下也可以进行此访问。保留 ESXi Shell 服务和 SSH 服务禁用状态是最安全的选项。

注 “例外用户”列表针对用于执行特定任务（例如主机备份）的服务帐户提供，而非针对管理员提供。将管理员用户添加到“例外用户”列表违背了锁定模式的初衷。

启用和禁用锁定模式

特权用户可以通过多种方式启用锁定模式：

- 使用**添加主机**向导将主机添加到 vCenter Server 系统时。
- 使用 vSphere Web Client。请参见[使用 vSphere Web Client 启用锁定模式](#)。您可以从 vSphere Web Client 中启用正常锁定模式和严格锁定模式。
- 使用直接控制台用户界面 (DCUI)。请参见[从直接控制台用户界面启用或禁用正常锁定模式](#)。

特权用户可从 vSphere Web Client 中禁用锁定模式。这些用户可以从直接控制台界面禁用正常锁定模式，但无法从直接控制台界面禁用严格锁定模式。

注 如果使用直接控制台用户界面启用或禁用锁定模式，则主机上用户和组的权限都将丢失。要保留这些权限，可以使用 vSphere Web Client 启用和禁用锁定模式。

锁定模式行为

在锁定模式下，一些服务会被禁用，一些服务只允许特定用户访问。

面向不同用户的锁定模式服务

当主机正在运行时，可用服务取决于锁定模式是否启用以及锁定模式的类型。

- 在严格锁定模式和正常锁定模式下，特权用户可以通过 vCenter Server 或通过 vSphere Web Client 或使用 vSphere Web Services SDK 访问主机。
- 严格锁定模式和正常锁定模式下的直接控制台界面行为有所不同。
 - 在严格锁定模式下，直接控制台用户界面 (DCUI) 服务处于禁用状态。
 - 在正常锁定模式下，异常用户列表中具有管理员特权的帐户和 DCUI.Access 高级系统设置中指定的用户可以访问直接控制台界面。
- 如果已启用 ESXi Shell 或 SSH 且将主机置于严格锁定模式或正常锁定模式，则异常用户列表中具有管理员特权的帐户可以使用这些服务。对于所有其他用户，ESXi Shell 或 SSH 访问处于禁用状态。从 vSphere 6.0 开始，不具备管理员特权的用户的 ESXi 或 SSH 会话将终止。

严格锁定模式和正常锁定模式下的所有访问均会记入日志。

表 5-9. 锁定模式行为

服务	正常模式	正常锁定模式	严格的锁定模式
vSphere Web Services API	所有用户，基于权限	vCenter (vpxuser) 异常用户，基于权限 vCloud Director (vsiauser, 如果可用)	vCenter (vpxuser) 异常用户，基于权限 vCloud Director (vsiauser, 如果可用)
CIM 提供程序	具有主机管理员特权的用户	vCenter (vpxuser) 异常用户，基于权限。 vCloud Director (vsiauser, 如果可用)	vCenter (vpxuser) 异常，基于权限。 vCloud Director (vsiauser, 如果可用)
直接控制台 UI (DCUI)	具有主机管理员特权的用户 和 DCUI.Access 高级选项 中指定的用户	DCUI.Access 高级选项中 定义的用户 具有主机管理员特权的异常 用户	DCUI 服务停止
ESXi Shell (如果已启用)	具有主机管理员特权的用户	DCUI.Access 高级选项中 定义的用户 具有主机管理员特权的异常 用户	DCUI.Access 高级选项中定义的用户 具有主机管理员特权的异常用户
SSH (如果已启用)	具有主机管理员特权的用户	DCUI.Access 高级选项中 定义的用户 具有主机管理员特权的异常 用户	DCUI.Access 高级选项中定义的用户 具有主机管理员特权的异常用户

启用锁定模式时登录到 ESXi Shell 的用户

在启用锁定模式之前，如果用户已登录 ESXi Shell 或通过 SSH 访问主机，则异常用户列表中具有主机管理员特权的用户仍保持登录状态。从 vSphere 6.0 开始，所有其他用户的该会话将终止。在正常锁定模式和严格锁定模式下均适用。

使用 vSphere Web Client 启用锁定模式

启用锁定模式以要求所有配置更改都通过 vCenter Server 进行。vSphere 6.0 及更高版本支持正常锁定模式和严格锁定模式。

要完全禁用对主机的所有直接访问，可以选择严格锁定模式。启用严格锁定模式后，如果 vCenter Server 不可用，并且 SSH 和 ESXi Shell 处于禁用状态，用户将无法访问主机。请参见[锁定模式行为](#)。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 依次单击**管理**选项卡和**设置**。
- 3 在“系统”下，选择**安全配置文件**。
- 4 在“锁定模式”面板中，单击**编辑**。
- 5 单击**锁定模式**，然后选择其中一个锁定模式选项。

选项	描述
正常	可以通过 vCenter Server 访问主机。只有位于“异常用户”列表中且具有管理员特权的用户能够登录直接控制台用户界面。如果启用了 SSH 或 ESXi Shell，则可以访问。
严格	只能通过 vCenter Server 访问主机。如果启用了 SSH 或 ESXi Shell，DCUI.Access 高级选项中的帐户以及具有管理员特权的“异常用户”帐户的正在运行的会话仍处于启用状态。所有其他会话将终止。

- 6 单击**确定**。

使用 vSphere Web Client 禁用锁定模式

禁用锁定模式可允许配置更改通过直接连接传递到 ESXi 主机。保留锁定模式处于启用状态可增强环境的安全性。

在 vSphere 6.0 中，可以按如下所示禁用锁定模式：

从 vSphere Web Client 中

用户可以从 vSphere Web Client 中禁用正常锁定模式和严格锁定模式。

从直接控制台用户界面

能够在 ESXi 主机上访问直接控制台用户界面的用户可以禁用正常锁定模式。在严格锁定模式下，直接控制台界面服务已停止。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 依次单击**管理**选项卡和**设置**。
- 3 在“系统”下，选择**安全配置文件**。
- 4 在“锁定模式”面板中，单击**编辑**。
- 5 单击**锁定模式**，然后选择**无**以禁用锁定模式。

结果

系统将退出锁定模式，vCenter Server 将显示一条警报，并向审核日志中添加一个条目。

从直接控制台用户界面启用或禁用正常锁定模式

可以从直接控制台用户界面 (DCUI) 启用和禁用正常锁定模式。只能从 vSphere Web Client 启用和禁用严格锁定模式。

主机处于正常锁定模式时，以下帐户可以访问直接控制台用户界面：

- “异常用户”列表中对主机具有管理员特权的帐户。“异常用户”列表针对服务帐户（例如备份代理）提供。
- 在主机的 DCUI.Access 高级选项中定义的用户。此选项可在出现灾难性故障时用于启用访问权限。

在 ESXi 6.0 及更高版本中，用户权限在您从直接控制台界面启用锁定模式时预留，在您禁用锁定模式时还原。

注 如果您在未退出锁定模式的情况下将处于锁定模式的主机升级到 ESXi 6.0，并且在升级后退出锁定模式，则在进入锁定模式之前定义的所有权限将丢失。系统会将管理员角色分配给在 DCUI.Access 高级选项中找到所有用户，以保证主机仍可访问。

要保留权限，请在升级之前从 vSphere Web Client 禁用主机的锁定模式。

步骤

- 1 在主机的直接控制台用户界面上，按 F2 并登录。
- 2 滚动至**配置锁定模式**设置并按 Enter 切换当前设置。
- 3 按 Esc 直到返回到直接控制台用户界面的主菜单。

指定在锁定模式下拥有访问特权的帐户

您可以指定能够直接访问 ESXi 主机的服务帐户，方法是将这些帐户添加到“异常用户”列表。如果出现灾难性 vCenter Server 故障，您可以指定能够访问 ESXi 主机的单个用户。

启用锁定模式后不同的帐户默认能够执行的操作以及如何更改默认行为取决于 vSphere 环境的版本。

- 在 vSphere 5.1 之前的 vSphere 版本中，只有 root 用户能够在锁定模式下的 ESXi 主机上登录到直接控制台用户界面。

- 在 vSphere 5.1 及更高版本中，您可以将用户添加到每个主机的 DCUI.Access 高级系统设置中。该选项在出现灾难性 vCenter Server 故障时使用，拥有此访问权限的用户的密码通常锁入保险箱内。DCUI.Access 列表中的用户不需要拥有对主机的完全管理特权。
- 在 vSphere 6.0 及更高版本中，仍支持 DCUI.Access 高级系统设置。此外，vSphere 6.0 及更高版本还支持“异常用户”列表，该列表面向必须直接登录主机的服务帐户提供。“异常用户”列表中拥有管理员特权的帐户可以登录 ESXi Shell。此外，这些用户还可以在正常锁定模式下登录主机的 DCUI，并且能够退出锁定模式。

请从 vSphere Web Client 指定异常用户。

注 异常用户是指具有在本地为 ESXi 主机定义的特权的主机本地用户或 Active Directory 用户。当主机处于锁定模式时，作为 Active Directory 组成员的用户会丢失其权限。

将用户添加到 DCUI.Access 高级选项

如果您无法从 vCenter Server 访问主机，DCUI.Access 高级选项的主要用途是允许您在出现灾难性故障时退出锁定模式。可以通过从 vSphere Web Client 编辑主机的“高级设置”向列表中添加用户。

注 无论具有何种特权，DCUI.Access 列表中的用户都可以更改锁定模式设置。这会影响到主机的安全性。对于需要直接访问主机的服务帐户，请考虑改为将用户添加到“异常用户”列表中。异常用户只能执行自己有权执行的任务。请参见[指定锁定模式异常用户](#)。

步骤

- 1 在 vSphere Web Client 对象导航器中，浏览到主机。
- 2 单击**管理**选项卡，然后选择**设置**。
- 3 单击**高级系统设置**，然后选择 **DCUI.Access**。
- 4 单击**编辑**，输入用户名并用逗号分隔开。

默认情况下，已指定 root 用户。请考虑从 DCUI.Access 列表中移除 root 用户并指定帐户以增强可审核性。

- 5 单击**确定**。

指定锁定模式异常用户

在 vSphere 6.0 及更高版本中，您可以从 vSphere Web Client 将用户添加到“异常用户”列表。主机进入锁定模式时，这些用户不会丢失其权限。将备份代理等服务帐户添加到“异常用户”列表是有意义的。

主机进入锁定模式时，异常用户不会丢失其特权。这些帐户通常表示需要在锁定模式下继续运行的第三方解决方案和外部应用程序。

注 “异常用户”列表针对用于执行非常特殊的任务的服务帐户提供，而非针对管理员提供。将管理员用户添加到“异常用户”列表违背了锁定模式的初衷。

异常用户是指具有在本地为 ESXi 主机定义的特权的主机本地用户或 Active Directory 用户。他们不是 Active Directory 组的成员，也不是 vCenter Server 用户。根据其权限，不允许这些用户在主机上执行操作。例如，这意味着只读用户无法在主机上禁用锁定模式。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 依次单击**管理**选项卡和**设置**。
- 3 在“系统”下，选择**安全配置文件**。
- 4 在“锁定模式”面板中，单击**编辑**。
- 5 单击**异常用户**，然后单击加号图标以添加异常用户。

检查主机和 VIB 的接受程度

为保护 ESXi 主机的完整性，请不要允许用户安装未签名的（团体支持的）VIB。未签名的 VIB 包含未由 VMware 或其合作伙伴认证、接受或支持的代码。团体支持的 VIB 没有数字签名。

可以使用 ESXCLI 命令来设置主机的接受程度。该主机的接受程度限制必须与要添加到该主机的任何 VIB 的接受程度相同或更少。为了保护 ESXi 主机的安全性和完整性，请勿允许在生产系统的主机上安装未签名 (CommunitySupported) VIB。

支持以下接受程度。

VMwareCertified

VMwareCertified 接受程度具有最严格的要求。此程度的 VIB 能够完全通过全面测试，该测试等效于相同技术的 VMware 内部质量保证测试。现在，只有 IOVP 驱动程序是以此程度发布的。VMware 受理此接受程度的 VIB 的支持致电。

VMwareAccepted

此接受程度的 VIB 通过验证测试，但是这些测试并未对软件的每个功能都进行全面测试。合作伙伴运行测试，VMware 验证结果。现在，以此程度发布的 VIB 包括 CIM 提供程序和 PSA 插件。VMware 将此接受程度的 VIB 支持致电转交给合作伙伴的支持组织。

PartnerSupported

接受程度为 PartnerSupported 的 VIB 是由 VMware 信任的合作伙伴发布的。合作伙伴执行所有测试。VMware 不验证结果。合作伙伴想要在 VMware 系统中启用的新的或非主流的技术将使用此程度。现在，驱动程序 VIB 技术（例如 Infiniband、ATAoE 和 SSD）处于此程度，且具有非标准的硬件驱动程序。VMware 将此接受程度的 VIB 支持致电转交给合作伙伴的支持组织。

CommunitySupported

CommunitySupported 接受程度用于由 VMware 合作伙伴程序外部的个人或公司创建的 VIB。此程度的 VIB 尚未通过任何 VMware 批准的测试程序，且不受 VMware 技术支持或 VMware 合作伙伴的支持。

步骤

- 1 连接至每个 ESXi 主机并通过运行以下命令确认已将接受程度设置为 VMwareCertified 或 VMwareAccepted。

```
esxcli software acceptance get
```

- 2 如果该主机的接受程度不是 VMwareCertified 或 VMwareAccepted，请通过运行以下命令确认是否有任何 VIB 的接受程度未设置为 VMwareCertified 或 VMwareAccepted。

```
esxcli software vib list
esxcli software vib get -n vibname
```

- 3 通过运行以下命令删除接受程度设置为 PartnerSupported 或 CommunitySupported 的任何 VIB。

```
esxcli software vib remove --vibname vib
```

- 4 通过运行以下命令更改主机的接受程度。

```
esxcli software acceptance set --level acceptance_level
```

为 ESXi 分配权限

在大多数情况下，通过为 vCenter Server 系统管理的 ESXi 主机对象分配权限，可向用户授予特权。如果使用的是独立 ESXi 主机，则可以直接分配特权。

为 vCenter Server 管理的 ESXi 主机分配权限

如果 ESXi 主机由 vCenter Server 管理，请通过 vSphere Web Client 执行管理任务。

您可以在 vCenter Server 对象层次结构中选择 ESXi 主机对象，并将管理员角色分配给有限的几个用户，使其能够直接管理 ESXi 主机。请参见[使用角色分配特权](#)。

最佳做法是至少创建一个指定用户帐户，并为其分配对主机的完全管理特权，然后使用该帐户，而不是 root 帐户。为 root 帐户设置一个高度复杂的密码，并限制 root 帐户的使用。（不要移除 root 帐户。）

为独立的 ESXi 主机分配权限

如果您的环境不包含 vCenter Server 系统，则会预定义以下用户。

- root 用户。请参见[root 用户特权](#)。
- vpxuser。请参见[vpxuser 特权](#)。
- dcui 用户。请参见[dcui 用户特权](#)。

可以在 vSphere Client 的“管理”选项卡中添加本地用户及定义自定义角色。

对于所有版本的 ESXi，都可以在 `/etc/passwd` 文件中查看预定义用户列表。

系统预定义了以下角色：

只读

允许用户查看与 ESXi 主机关联的对象，但不允许对对象进行任何更改。

管理员

管理员角色。

无权访问

无权访问。这是默认行为。您可以根据需要替代此默认行为。

您可以使用直接连接到 ESXi 主机的 vSphere Client 管理本地用户和组以及将本地自定义角色添加到 ESXi 主机。

从 vSphere 6.0 开始，您可以使用 ESXCLI 帐户管理命令管理 ESXi 本地用户帐户。您可以使用 ESXCLI 权限管理命令设置或移除对 Active Directory 帐户（用户和组）及对 ESXi 本地帐户（仅限用户）的权限。

注 如果通过直接连接到 ESXi 主机为该主机定义一个用户，而 vCenter Server 中也存在同名的用户，则这两个用户不同。如果为其中一个用户分配某个角色，则不会为另一个用户分配同一角色。

root 用户特权

默认情况下，每个 ESXi 主机都有一个具有管理员角色的 root 用户帐户。该 root 用户帐户可用于本地管理，并可用于将主机连接到 vCenter Server。

此公共 root 帐户可以更方便地访问 ESXi 主机，但难以确定特定管理员执行的操作。

为 root 帐户设置一个高度复杂的密码，并限制 root 帐户的使用，例如向 vCenter Server 添加主机时使用 root 帐户。不要移除 root 帐户。在 vSphere 5.1 及更高版本中，仅允许使用 root 用户向 vCenter Server 中添加主机，而不允许使用其他具有管理员角色的指定用户。

最佳做法是确保将 ESXi 主机上具有管理员角色的任何帐户分配给具有指定帐户的特定用户。如果可能，请使用 ESXi Active Directory 功能，以便管理 Active Directory 凭据。

重要事项 如果您要移除 root 用户的访问特权，则必须首先在 root 级别创建另一个权限，以便向另一用户分配管理员角色。

vpxuser 特权

管理主机的活动时，vCenter Server 使用 vpxuser 特权。

vCenter Server 对其管理的主机拥有管理员特权。例如，vCenter Server 可将虚拟机移至和移离主机，并执行支持虚拟机所必需的配置更改。

vCenter Server 管理员可在主机上执行可以由 Root 用户执行的大多数任务，并调度任务和处理模板等。但是，vCenter Server 管理员不能为主机直接创建、删除或编辑本地用户和组。这些任务只能由具有管理员权限的用户直接在每个主机上执行。

注 不能使用 Active Directory 管理 vpxuser。

小心 不要以任何方式更改 vpxuser。不要更改其密码。不要更改其权限。如果进行了更改，在通过 vCenter Server 处理主机时可能会出现問題。

dcui 用户特权

dcui 用户以管理员权限在主机上操作。此用户的主要目的是从直接控制台用户界面 (DCUI) 配置锁定模式的主机。

此用户将充当直接控制台的代理，无法由交互式用户来修改或使用。

使用 Active Directory 管理 ESXi 用户

可以将 ESXi 配置为使用像 Active Directory 这样的目录服务来管理用户。

如果要在每台主机上都创建本地用户帐户，则涉及到必须在多个主机间同步帐户名和密码的问题。若将 ESXi 主机加入到 Active Directory 域中，则无需再创建和维护本地用户帐户。使用 Active Directory 进行用户身份验证可以简化 ESXi 主机配置，并能降低可导致出现未授权访问的配置问题的风险。

当使用活动目录时，将主机添加到域时用户会提供活动目录凭据以及活动目录服务器的域名。

安装或升级 vSphere Authentication Proxy

安装 vSphere Authentication Proxy 使 ESXi 主机能够加入域而无需使用 Active Directory 凭据。由于不需要在主机配置中存储 Active Directory 凭据，vSphere Authentication Proxy 可以增强 PXE 引导的主机和使用 Auto Deploy 置备的主机的安全性。

如果在系统中已安装早期版本的 vSphere Authentication Proxy，此过程会将 vSphere Authentication Proxy 升级到当前版本。

可以将 vSphere Authentication Proxy 安装在与关联的 vCenter Server 相同的计算机上，也可以将其安装在与 vCenter Server 具有网络连接的其他计算机上。vCenter Server 5.0 及更高版本支持 vSphere Authentication Proxy。

vSphere Authentication Proxy 服务绑定到 IPv4 地址中以与 vCenter Server 进行通信，且不支持 IPv6。vCenter Server 实例可位于纯 IPv4、IPv4/IPv6 混合模式或纯 IPv6 网络环境中的主机上，但是通过 vSphere Web Client 连接到 vCenter Server 的计算机必须具有 IPv4 地址，以便 vSphere Authentication Proxy 服务能够正常运行。

前提条件

- 在要安装 vSphere Authentication Proxy 的计算机上安装 Microsoft .NET Framework 3.5。
- 确认您具有管理员特权。

- 确认主机具有支持的处理器和操作系统。
- 确认主机具有有效的 IPv4 地址。可以在纯 IPv4 网络环境或 IPv4/IPv6 混合模式网络环境中的计算机上安装 vSphere Authentication Proxy，但不能在纯 IPv6 环境中的计算机上安装 vSphere Authentication Proxy。
- 如果将 vSphere Authentication Proxy 安装到 Windows Server 2008 R2 主机上，可以从 support.microsoft.com 网站下载 Windows 知识库文章 981506 中所述的 Windows 热修补程序并进行安装。如果未安装此热修补程序，vSphere Authentication Proxy 适配器将无法进行初始化。出现该问题的同时还会在 `camadapter.log` 中显示类似于无法将 CAM 网站与 CTL 进行绑定 (Failed to bind CAM website with CTL) 和无法初始化 CAMAdapter (Failed to initialize CAMAdapter) 的错误消息。
- 下载 vCenter Server 安装程序。

要完成安装或升级需收集以下信息：

- 安装 vSphere Authentication Proxy 的位置（如果不使用默认位置）。
- vSphere Authentication Proxy 将连接到的 vCenter Server 的地址和凭据：IP 地址或名称、HTTP 端口、用户名和密码。
- 在网络中识别 vSphere Authentication Proxy 的主机名或 IP 地址。

步骤

- 1 将要安装身份验证代理服务的主机添加到域中。
- 2 使用域管理员帐户登录此主机。
- 3 在软件安装程序目录中，双击 `autorun.exe` 文件启动安装程序。
- 4 选择 **VMware vSphere Authentication Proxy**，然后单击**安装**。
- 5 按照向导提示完成安装或升级。

在安装过程中，身份验证服务向注册了 Auto Deploy 的 vCenter Server 实例进行注册。

结果

安装 vSphere Authentication Proxy 服务时，安装程序会创建一个具有相应特权的域帐户，以便运行身份验证代理服务。帐户名称以前缀 `CAM-` 开始，并有一个随机生成的 32 个字符的密码与其关联。密码设置为永不过期。请勿更改帐户设置。

配置主机以使用 Active Directory

可以对主机进行配置，以便使用目录服务（如 Active Directory）来管理用户和组。

向 Active Directory 中添加 ESXi 主机时，如果存在 DOMAIN 组 **ESX Admins**，则将其分配对主机的完全管理访问权限。如果不希望分配完全管理权限，请参见 VMware 知识库文章 1025569 获取解决办法。

如果使用 Auto Deploy 置备主机，则 Active Directory 凭据无法存储在主机上。您可以使用 vSphere Authentication Proxy 将主机加入到 Active Directory 域中。由于 vSphere Authentication Proxy 与主机之间存在信任链，因此 Authentication Proxy 可以将主机加入到 Active Directory 域中。请参见[使用 vSphere Authentication Proxy](#)。

注 在 Active Directory 中定义用户帐户设置时，可以按计算机名称限制用户能够登录的计算机。默认情况下，未对用户帐户设置任何相关限制。如果设置了此限制，对用户帐户的 LDAP 绑定请求将失败，并显示消息 LDAP 绑定失败 (LDAP binding not successful)，即使该请求来自列出的计算机也是如此。可以通过将 Active Directory 服务器的 netBIOS 名称添加到用户帐户能够登录的计算机列表来避免此问题。

前提条件

- 确认您拥有 Active Directory 域。请参见目录服务器文档。
- 确认 ESXi 的主机名完全符合 Active Directory 林的域名条件。

全限定域名 = 主机名.域名

步骤

- 1 使用 NTP 将 ESXi 和目录服务系统的时间同步。

有关如何使用 Microsoft 域控制器同步 ESXi 时间的信息，请参阅[使 ESXi 时钟与网络时间服务器同步](#)或 VMware 知识库。

- 2 确保为主机配置的 DNS 服务器可以解析 Active Directory 控制器的主机名。
 - a 在 vSphere Web Client 对象导航器中，浏览到主机。
 - b 依次单击**管理**选项卡和**网络**。
 - c 单击“DNS”，然后验证该主机的主机名和 DNS 服务器信息是否正确。

后续步骤

使用 vSphere Web Client 加入目录服务域。对于使用 Auto Deploy 置备的主机，请设置 vSphere Authentication Proxy。请参见[使用 vSphere Authentication Proxy](#)。

将主机添加到目录服务域

要让主机使用目录服务，必须将主机加入到目录服务域。

可以使用以下两种方法之一输入域名：

- **name.tld**（例如 **domain.com**）：在默认容器下会创建该帐户。
- **name.tld/container/path**（例如 **domain.com/OU1/OU2**）：在特定组织单元 (OU) 下会创建该帐户。

要使用 vSphere Authentication Proxy 服务，请参见[使用 vSphere Authentication Proxy](#)。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 依次单击**管理**选项卡和**设置**。
- 3 在“系统”下，选择**身份验证服务**。
- 4 单击**加入域**。
- 5 输入域。
使用 `name.tld` 或 `name.tld/container/path` 形式。
- 6 输入有权将主机加入域的目录服务用户的用户名和密码，然后单击**确定**。
- 7 （可选）如果要使用身份验证代理，请输入代理服务器的 IP 地址。
- 8 单击**确定**关闭“目录服务配置”对话框。

查看目录服务设置

可以查看目录服务器的类型（如果有），主机将使用此类型对用户和目录服务器设置进行身份验证。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 依次单击**管理**选项卡和**设置**。
- 3 在“系统”下，选择**身份验证服务**。
“身份验证服务”页面将显示目录服务和域设置。

使用 vSphere Authentication Proxy

使用 vSphere Authentication Proxy 时，无需将 Active Directory 凭据传输到主机。用户将主机添加到域时，会提供 Active Directory 服务器的域名和身份验证代理服务器的 IP 地址。

与 Auto Deploy 结合使用时，vSphere Authentication Proxy 特别有用。您可以设置指向 Authentication Proxy 的引用主机，并设置规则以将引用主机的配置文件应用于使用 Auto Deploy 置备的任何 ESXi 主机。即使在使用 VMCA 置备的证书或第三方证书的环境中使用 vSphere Authentication Proxy，只要遵循有关将自定义证书与 Auto Deploy 配合使用的说明，即可无缝运行有关过程。请参见在 [Auto Deploy 中使用自定义证书](#)。

注 不能在仅支持 IPv6 的环境中使用 vSphere Authentication Proxy。

安装或升级 vSphere Authentication Proxy

安装 vSphere Authentication Proxy 使 ESXi 主机能够加入域而无需使用 Active Directory 凭据。由于不需要在主机配置中存储 Active Directory 凭据，vSphere Authentication Proxy 可以增强 PXE 引导的主机和使用 Auto Deploy 置备的主机的安全性。

如果在系统中已安装早期版本的 vSphere Authentication Proxy，此过程会将 vSphere Authentication Proxy 升级到当前版本。

可以将 vSphere Authentication Proxy 安装在与关联的 vCenter Server 相同的计算机上，也可以将其安装在与 vCenter Server 具有网络连接的其他计算机上。vCenter Server 5.0 及更高版本支持 vSphere Authentication Proxy。

vSphere Authentication Proxy 服务绑定到 IPv4 地址中以与 vCenter Server 进行通信，且不支持 IPv6。vCenter Server 实例可位于纯 IPv4、IPv4/IPv6 混合模式或纯 IPv6 网络环境中的主机上，但是通过 vSphere Web Client 连接到 vCenter Server 的计算机必须具有 IPv4 地址，以便 vSphere Authentication Proxy 服务能够正常运行。

前提条件

- 在要安装 vSphere Authentication Proxy 的计算机上安装 Microsoft .NET Framework 3.5。
- 确认您具有管理员特权。
- 确认主机具有支持的处理器和操作系统。
- 确认主机具有有效的 IPv4 地址。可以在纯 IPv4 网络环境或 IPv4/IPv6 混合模式网络环境中的计算机上安装 vSphere Authentication Proxy，但不能在纯 IPv6 环境中的计算机上安装 vSphere Authentication Proxy。
- 如果将 vSphere Authentication Proxy 安装到 Windows Server 2008 R2 主机上，可以从 support.microsoft.com 网站下载 Windows 知识库文章 981506 中所述的 Windows 热修补程序并进行安装。如果未安装此热修补程序，vSphere Authentication Proxy 适配器将无法进行初始化。出现该问题的同时还会在 `camadapter.log` 中显示类似于无法将 CAM 网站与 CTL 进行绑定 (Failed to bind CAM website with CTL) 和无法初始化 CAMAdapter (Failed to initialize CAMAdapter) 的错误消息。
- 下载 vCenter Server 安装程序。

要完成安装或升级需收集以下信息：

- 安装 vSphere Authentication Proxy 的位置（如果不使用默认位置）。
- vSphere Authentication Proxy 将连接到的 vCenter Server 的地址和凭据：IP 地址或名称、HTTP 端口、用户名和密码。
- 在网络中识别 vSphere Authentication Proxy 的主机名或 IP 地址。

步骤

- 1 将要安装身份验证代理服务的主机添加到域中。
- 2 使用域管理员帐户登录此主机。
- 3 在软件安装程序目录中，双击 `autorun.exe` 文件启动安装程序。
- 4 选择 **VMware vSphere Authentication Proxy**，然后单击**安装**。
- 5 按照向导提示完成安装或升级。

在安装过程中，身份验证服务向注册了 Auto Deploy 的 vCenter Server 实例进行注册。

结果

安装 vSphere Authentication Proxy 服务时，安装程序会创建一个具有相应特权的域帐户，以便运行身份验证代理服务。帐户名称以前缀 **CAM-** 开始，并有一个随机生成的 32 个字符的密码与其关联。密码设置为永不过期。请勿更改帐户设置。

配置主机以使用 vSphere Authentication Proxy 进行身份验证

安装 vSphere Authentication Proxy 服务（CAM 服务）后，必须配置主机以使用身份验证代理服务器对用户进行身份验证。

前提条件

在主机上安装 vSphere Authentication Proxy 服务（CAM 服务）。请参见[安装或升级 vSphere Authentication Proxy](#)。

步骤

1 使用主机上的 IIS 管理器设置 DHCP 范围。

通过设置范围，在管理网络中使用 DHCP 的主机可以使用身份验证代理服务。

选项	操作
适用于 IIS 6	<ol style="list-style-type: none"> 浏览到计算机帐户管理网站。 右键单击虚拟目录 CAM ISAPI。 选择属性 > 目录安全 > 编辑 IP 地址和域名限制 > 添加计算机组。
适用于 IIS 7	<ol style="list-style-type: none"> 浏览到计算机帐户管理网站。 在左窗格中单击 CAM ISAPI 虚拟目录，然后打开 IPv4 地址和域限制。 选择添加允许条目 > IPv4 地址范围。

2 如果 Auto Deploy 未置备某个主机，请将默认 SSL 证书更改为自签名证书或由商业证书颁发机构 (CA) 签名的证书。

选项	描述
VMCA 证书	<p>如果使用默认的 VMCA 签名证书，则必须确保身份验证代理主机信任 VMCA 证书。</p> <ol style="list-style-type: none"> 手动将 VMCA 证书添加到“受信任根证书授权机构”证书存储。 将 VMCA 签名证书 (root.cer) 添加到安装了身份验证代理服务的系统上的本地信任证书存储。可以在 C:\ProgramData\VMware\CIS\data\vmca 中找到该文件。 重新启动 vSphere Authentication Proxy 服务。
第三方 CA 签名的证书	<p>将 CA 签名证书（DER 编码）添加到安装了身份验证代理服务的系统上的本地信任证书存储，然后重新启动 vSphere Authentication Proxy 服务。</p> <ul style="list-style-type: none"> ■ 对于 Windows 2003，将证书文件复制到 C:\Documents and Settings\All Users\Application Data\VMware\vsphere Authentication Proxy\trust。 ■ 对于 Windows 2008，将证书文件复制到 C:\Program Data\VMware\vsphere Authentication Proxy\trust。

设置 vSphere Authentication Proxy

如果 ESXi 主机具有 Authentication Proxy 证书信息，则可以使用 vSphere Authentication Proxy。只需对服务器进行一次身份验证。

注 ESXi 和 Authentication Proxy 服务器必须能够进行身份验证。确保始终启用此身份验证功能。如果必须禁用身份验证功能，则可使用“高级设置”对话框将 `UserVars.ActiveDirectoryVerifyCAMCertificate` 属性设置为 0。

导出 vSphere Authentication Proxy 证书

要针对 ESXi 对 vSphere Authentication Proxy 进行身份验证，必须为 ESXi 提供代理服务器证书。

前提条件

在主机上安装 vSphere Authentication Proxy (CAM 服务)。请参见[安装或升级 vSphere Authentication Proxy](#)。

步骤

- 1 在身份验证代理服务器系统中，使用 IIS Manager 导出证书。

选项	操作
适用于 IIS 6	<ol style="list-style-type: none"> a 右键单击计算机帐户管理网站。 b 选择属性 > 目录安全 > 查看证书。
适用于 IIS 7	<ol style="list-style-type: none"> a 在左窗格中，单击计算机帐户管理网站。 b 选择绑定打开“站点绑定”对话框。 c 选择 https 绑定。 d 选择编辑 > 查看 SSL 证书。

- 2 选择详细信息 > 复制到文件。
- 3 选择选项不要导出专用密钥和 Base-64 编码 X.509 (CER)。

后续步骤

将证书导入到 ESXi。

将 Proxy 服务器证书导入 ESXi

要针对 ESXi 对 vSphere Authentication Proxy 服务器进行身份验证，请将代理服务器证书上载到 ESXi。

使用 vSphere Web Client 用户界面将 vSphere Authentication Proxy 服务器证书上载到 ESXi 主机。

前提条件

在主机上安装 vSphere Authentication Proxy 服务 (CAM 服务)。请参见[安装或升级 vSphere Authentication Proxy](#)。

导出 vSphere Authentication Proxy 服务器证书，如导出 [vSphere Authentication Proxy](#) 证书中所述。

步骤

- 1 浏览到主机，然后依次单击**管理**选项卡、**设置**和**身份验证服务**。
- 2 单击**导入证书**。
- 3 输入到主机上身份验证代理服务器证书文件的完整路径和身份验证代理服务器的 IP 地址。
使用 “[*数据存储名称*] *文件路径*” 形式输入代理服务器的路径。
- 4 单击**确定**。

使用 vSphere Authentication Proxy 将主机添加到域

将主机加入目录服务域时，可以使用 vSphere Authentication Proxy 服务器进行身份验证，而不传输用户提供的 Active Directory 凭据。

可以使用以下两种方法之一输入域名：

- **name.tld**（例如 **domain.com**）：在默认容器下会创建该帐户。
- **name.tld/container/path**（例如 **domain.com/OU1/OU2**）：在特定组织单元 (OU) 下会创建该帐户。

前提条件

- 通过 vSphere Web Client 连接到 vCenter Server 系统。
- 如果 ESXi 配置了 DHCP 地址，请设置 DHCP 范围。
- 如果 ESXi 使用静态 IP 地址进行了配置，请验证其关联配置文件是否已配置为使用 vSphere Authentication Proxy 服务来加入域，以便身份验证代理服务器可以信任 ESXi IP 地址。
- 如果 ESXi 使用的是 VMCA 签名证书，请确认是否已将主机添加到 vCenter Server。这可使身份验证代理服务器信任 ESXi。
- 如果 ESXi 使用的是 CA 签名证书且未使用 Auto Deploy 置备，请验证 CA 证书是否已添加到身份验证代理服务器的本地可信证书存储，如 [配置主机以使用 vSphere Authentication Proxy 进行身份验证](#)中所述。
- 针对主机对 vSphere Authentication Proxy 服务器进行身份验证。

步骤

- 1 在 vSphere Web Client 中浏览到主机，然后单击**管理**选项卡。
- 2 单击**设置**，然后选择**身份验证服务**。
- 3 单击**加入域**。
- 4 输入域。
使用 **name.tld** 或 **name.tld/container/path** 形式。
- 5 选择**使用代理服务器**。
- 6 输入身份验证代理服务器的 IP 地址。

7 单击确定。

替换 ESXi 主机的 Authentication Proxy 证书

您可以导入 vSphere Web Client 中可信证书颁发机构颁发的证书

前提条件

- 将 Authentication Proxy 证书文件上载到 ESXi 主机。

步骤

- 1 在 vSphere Web Client 中选择 ESXi 主机。
- 2 在设置选项卡中，选择系统区域内的身份验证服务。
- 3 单击导入证书。
- 4 输入 SSL 证书路径和 vSphere Authentication Proxy 服务器。

ESXi 安全性最佳做法

遵循 ESXi 安全性最佳做法可以确保 vSphere 部署的完整性。有关其他信息，请参见强化指南。

验证安装介质

在下载 ISO、脱机包或修补程序后始终检查文件的哈希以确保已下载文件的完整性和真实性。如果从 VMware 获取物理介质，而安全封装已损坏，请将软件退回 VMware 进行替换。

下载介质后，请使用 MD5 总和数值验证下载介质的完整性。将 MD5 总和输出与 VMware 网站上发布的值进行比较。每个操作系统拥有不同的检查 MD5 总和数值的方法和工具。对于 Linux，请使用“md5sum”命令。对于 Microsoft Windows，可以下载附加设备产品

手动检查 CRL

默认情况下，ESXi 主机不支持 CRL 检查。必须手动搜索和移除已吊销的证书。这些证书通常是从企业 CA 或第三方 CA 生成的自定义证书。许多公司使用脚本来查找和替换 ESXi 主机上的已吊销 SSL 证书。

监控 ESX Admins Active Directory 组

vSphere 使用的 Active Directory 组由 `plugins.hostsvc.esxAdminsGroup` 高级系统设置定义。默认情况下，此选项设置为 ESX Admins。将授予 ESX Admins 组的所有成员对域中所有 ESXi 主机的完全管理权限。监控此组创建的 Active Directory 并将成员资格限制为高度受信任的用户和组。

监控配置文件

尽管大多数 ESXi 配置设置使用 API 控制，但有限数量的配置文件仍直接影响主机。这些文件通过使用 HTTPS 的 vSphere 文件传输 API 进行公开。如果对这些文件进行更改，则必须同时执行相应的管理操作（例如更改配置）。

注 请勿尝试监控不会通过此文件传输 API 公开的文件。

使用 vmkfstools 擦除敏感数据

删除包含敏感数据的 VMDK 文件时，请关闭或停止虚拟机，然后对该文件发出 vCLI 命令 `vmkfstools --writezeros`。然后，您可以从数据存储中删除该文件。

PCI 和 PCIe 设备和 ESXi

使用 VMware DirectPath I/O 功能将 PCI 或 PCIe 设备直通到虚拟机会导致潜在的安全漏洞。该漏洞可能会由错误代码或恶意代码触发，如客户机操作系统中以特权模式运行的设备驱动程序。行业标准硬件和固件当前无法提供足够的错误控制支持，导致 ESXi 无法完全关闭漏洞。

VMware 建议仅在虚拟机由可信实体所有和管理时，才使用 PCI 或 PCIe 直通到此虚拟机。必须确保此实体不会尝试通过虚拟机破坏或利用主机。

主机可能会因以下原因受到威胁。

- 客户机操作系统可能生成了不可恢复的 PCI 或 PCIe 错误。此类错误不会损坏数据，但是可能会导致 ESXi 主机崩溃。出现此类错误可能是由于正在直通的硬件设备中存在缺陷或不兼容，或者客户机操作系统的驱动程序存在问题。
- 客户机操作系统可能会生成直接内存访问 (DMA) 操作，此操作导致 ESXi 主机上出现 IOMMU 页面故障，例如，当 DMA 操作指向虚拟机内存的外部地址时。在一些计算机上，主机固件将 IOMMU 故障配置为通过不可屏蔽的中断 (NMI) 报告致命错误，这会导致 ESXi 主机崩溃。发生此问题可能是由于客户机操作系统的驱动程序存在问题。
- 如果 ESXi 主机上的操作系统未使用中断重新映射，客户机操作系统可能会在任意向量上向 ESXi 主机插入一个虚假中断。当前，ESXi 在可以使用中断重新映射的 Intel 平台上使用中断重新映射；中断映射是 Intel VT-d 功能集的一部分。ESXi 在 AMD 平台上不使用中断映射。虚假中断很可能会导致 ESXi 主机崩溃；但是，理论上可能存在利用这些中断的其他方式。

配置 ESXi 的智能卡身份验证

可以使用智能卡身份验证登录到 ESXi 直接控制台用户界面 (DCUI)，方法是使用个人身份验证 (PIV)、通用访问卡 (CAC) 或 SC650 智能卡，而不是默认提示输入用户名和密码。

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基于智能卡的双重身份验证来提高其系统的安全性和遵循安全法规。

在 ESXi 主机上启用智能卡身份验证后，DCUI 会提示您提供有效的智能卡和 PIN 组合，而不是默认提示输入用户名和密码。

- 1 将智能卡插入到智能卡读卡器时，ESXi 主机会读取该卡上的凭据。
- 2 ESXi DCUI 会显示您的登录 ID，并提示您输入 PIN。

- 3 输入 PIN 后，ESXi 主机将其与存储在智能卡上的 PIN 匹配，并使用 Active Directory 验证智能卡上的证书。
- 4 成功验证智能卡证书后，ESXi 将让您登录到 DCUI。

按下 F3 即可从 DCUI 切换到用户名和密码身份验证。

在连续几次输入错误的 PIN（通常三次）后，智能卡上的芯片将锁定。如果智能卡已锁定，则只有选定人员才能将其解锁。

启用智能卡身份验证

启用智能卡身份验证可提示提供智能卡和 PIN 组合来登录到 ESXi DCUI。

前提条件

- 设置基础架构以处理智能卡身份验证，例如 Active Directory 域中的帐户、智能读卡器和智能卡。
- 将 ESXi 配置为加入一个支持智能卡身份验证的 Active Directory 域。有关详细信息，请参见 [使用 Active Directory 管理 ESXi 用户](#)。
- 使用 vSphere Web Client 添加根证书。请参见 [ESXi 主机的证书管理](#)。

步骤

- 1 在 vSphere Web Client 中，浏览到主机。
- 2 依次单击**管理**选项卡和**设置**。
- 3 在“系统”下，选择**身份验证服务**。
您将看到当前智能卡身份验证状态和一个包含已导入证书的列表。
- 4 在“智能卡身份验证”面板中，单击**编辑**。
- 5 在“编辑智能卡身份验证”对话框中，选择“证书”页面。
- 6 添加可信证书颁发机构 (CA) 颁发的证书，例如根和中间 CA 证书。
- 7 打开“智能卡身份验证”页面，选中**启用智能卡身份验证**复选框，然后单击**确定**。

禁用智能卡身份验证

禁用智能卡身份验证以返回 ESXi DCUI 登录的默认用户名和密码身份验证。

步骤

- 1 在 vSphere Web Client 中，浏览到主机。
- 2 依次单击**管理**选项卡和**设置**。
- 3 在“系统”下，选择**身份验证服务**。
您将看到当前智能卡身份验证状态和一个包含已导入证书的列表。
- 4 在“智能卡身份验证”面板中，单击**编辑**。
- 5 在“智能卡身份验证”页面上，取消选中**启用智能卡身份验证**复选框，然后单击**确定**。

如果出现连接问题，对用户凭据进行身份验证

如果无法访问 Active Directory (AD) 域服务器，则可以使用用户名和密码身份验证登录到 ESXi DCUI 以在主机上执行应急操作。

在异常情况下，由于连接问题、网络故障或灾难，无法访问 AD 域服务器以对智能卡上的用户凭据进行身份验证。如果与 AD 服务器断开连接，则可以使用本地 ESXi 用户的凭据登录到 ESXi DCUI。这可让您执行诊断或其他应急操作。此时将记录回退到用户名和密码登录。与 AD 的连接恢复后，请再次启用智能卡身份验证。

注 如果 Active Directory (AD) 域服务器可用，则丢失与 vCenter Server 的网络连接不会影响智能卡身份验证。

在锁定模式下使用智能卡身份验证

启用时，ESXi 主机上的锁定模式可提高主机的安全性并限制对 DCUI 的访问。锁定模式可能禁用智能卡身份验证功能。

在正常锁定模式下，只有“异常用户”列表中具有管理员特权的用户才能访问 DCUI。异常用户是指具有在本地为 ESXi 主机定义的特权的主机本地用户或 Active Directory 用户。如果要在正常锁定模式下使用智能卡身份验证，则必须从 vSphere Web Client 将用户添加到“异常用户”列表。主机进入正常锁定模式时，这些用户不会丢失其权限且可以登录到 DCUI。有关详细信息，请参见[指定锁定模式异常用户](#)。

在严格锁定模式下，DCUI 服务已停止。因此，无法使用智能卡身份验证访问主机。

ESXi SSH 密钥

可以使用 SSH 密钥限制、控制以及保护 ESXi 主机的访问权限。可以利用 SSH 密钥允许受信任的用户或脚本在不指定密码的情况下即可登录主机。

可以使用 `vifs` vSphere CLI 命令将 SSH 密钥复制到主机。有关安装和使用 vSphere CLI 命令集的信息，请参见《vSphere 命令行界面入门指南》。也可以使用 HTTPS PUT 将 SSH 密钥复制到主机。

您无需在外部生成密钥并进行上载，而是可以在 ESXi 主机上创建密钥，然后进行下载。请参见 VMware 知识库文章 [1002866](#)。

启用 SSH 并将 SSH 密钥添加到主机具有内在的风险，建议不在强化环境中使用。请参见[禁用授权 \(SSH\) 密钥](#)。

注 对于 ESXi 5.0 及更早版本，即使主机处于锁定模式，具有 SSH 密钥的用户也可以访问主机。ESXi 5.1 中已修复此问题。

SSH 安全

可以使用 SSH 远程登录到 ESXi Shell 并执行针对主机的故障排除任务。

ESXi 中的 SSH 配置得到了增强，能够提供较高的安全级别。

禁用第 1 版 SSH 协议

VMware 不再支持第 1 版 SSH 协议，而是以独占方式使用第 2 版协议。第 2 版消除了第 1 版中存在的某些安全问题，且提供了一个安全的方式与管理接口进行通信。

提高了密码强度

SSH 对连接仅支持 256 位和 128 位 AES 密码。

这些设置旨在为通过 SSH 传输到管理接口的数据提供可靠保护。不能更改这些设置。

使用 vifs 命令上载 SSH 密钥

如果您决定要使用授权密钥通过 SSH 登录到主机，则可以使用 `vifs` 命令上载授权密钥。

注 由于授权密钥允许 SSH 访问而无需用户身份验证，请认真考虑是否要在环境中使用 SSH 密钥。

授权密钥允许您对主机的远程访问进行身份验证。当用户或脚本尝试通过 SSH 访问主机时，密钥提供身份验证，并且不需要密码。使用授权密钥，可以自动进行身份验证，这在编写脚本以执行例程任务时非常有用。

可以将以下类型的 SSH 密钥上载到主机。

- root 用户的授权密钥
- RSA 密钥
- RSA 公用密钥

从 vSphere 6.0 Update 2 版本开始，不再支持 DSS/DSA 密钥。

重要事项 请不要修改 `/etc/ssh/sshd_config` 文件。

步骤

- ◆ 在命令行或管理服务器中，使用 `vifs` 命令将 SSH 密钥上载到 ESXi 主机上合适的位置。

```
vifs --server hostname --username username --put filename /host/ssh_host_dsa_key_pub
```

密钥类型	位置
root 用户的授权密钥文件	/host/ssh_root_authorized_keys 您必须具有完全管理员特权才可上载此文件。
RSA 密钥	/host/ssh_host_rsa_key
RSA 公用密钥	/host/ssh_host_rsa_key_pub

使用 HTTPS PUT 上载 SSH 密钥

可以使用授权密钥通过 SSH 登录主机。可以使用 HTTPS PUT 上载授权密钥。

授权密钥允许您对主机的远程访问进行身份验证。当用户或脚本尝试通过 SSH 访问主机时，密钥提供身份验证，并且不需要密码。使用授权密钥，可以自动进行身份验证，这在编写脚本以执行例程任务时非常有用。

可以使用 HTTPS PUT 将以下类型的 SSH 密钥上传到主机：

- root 用户的授权密钥
- DSA 密钥
- DSA 公用密钥
- RSA 密钥
- RSA 公用密钥

重要事项 请不要修改 `/etc/ssh/sshd_config` 文件。

步骤

- 1 在上载应用程序中，打开密钥文件。
- 2 将文件发布到以下位置。

密钥类型	位置
root 用户的授权密钥文件	<code>https://hostname_or_IP_address/host/ssh_root_authorized_keys</code> 您必须对主机具有完全管理员特权才可上载此文件。
DSA 密钥	<code>https://hostname_or_IP_address/host/ssh_host_dsa_key</code>
DSA 公用密钥	<code>https://hostname_or_IP_address/host/ssh_host_dsa_key_pub</code>
RSA 密钥	<code>https://hostname_or_IP_address/host/ssh_host_rsa_key</code>
RSA 公用密钥	<code>https://hostname_or_IP_address/host/ssh_host_rsa_key_pub</code>

使用 ESXi Shell

默认情况下，ESXi 主机上的 ESXi Shell 处于禁用状态。如有必要，可以启用对 shell 的本地或远程访问。要降低未经授权访问的风险，请启用 ESXi Shell 仅用于故障排除。

ESXi Shell 不受锁定模式影响。即使主机在锁定模式下运行，您仍然可以登录到 ESXi Shell（如果已启用）。

ESXi Shell

启用此服务以本地访问 ESXi Shell。

SSH

启用此服务以使用 SSH 远程访问 ESXi Shell。

请参见《vSphere 安全性》。

Root 用户和具有管理员角色的用户可以访问 ESXi Shell。属于 Active Directory 组 ESX Admins 的用户将自动分配有管理员角色。默认情况下，只有 root 用户才能使用 ESXi Shell 执行系统命令（例如 `vmware -v`）。

注 只有在真正需要访问 ESXi Shell 时才启用它。

- **使用 vSphere Web Client 启用对 ESXi Shell 的访问**

可以使用 vSphere Web Client 启用对 ESXi Shell 的本地和远程 (SSH) 访问，并设置空闲时间和可用性超时。

- **使用直接控制台用户界面 (DCUI) 启用对 ESXi Shell 的访问**

通过直接控制台用户界面 (DCUI)，您可以使用基于文本的菜单在本地与主机进行交互。请仔细评估您的环境安全要求是否支持启用直接控制台用户界面。

- **登录 ESXi Shell 以进行故障排除**

使用 vSphere Web Client、vSphere CLI 或 vSphere PowerCLI 执行 ESXi 配置任务。登录 ESXi Shell（以前称为技术支持模式或 TSM）仅进行故障排除。

使用 vSphere Web Client 启用对 ESXi Shell 的访问

可以使用 vSphere Web Client 启用对 ESXi Shell 的本地和远程 (SSH) 访问，并设置空闲时间和可用性超时。

注 使用 vSphere Web Client、远程命令行工具（vCLI 和 PowerCLI）和已发布的 API 来访问主机。除非是在要求启用 SSH 访问的特殊情况下，否则不要启用使用 SSH 远程访问主机的功能。

前提条件

如果要使用授权 SSH 密钥，可以上载该密钥。请参见 [ESXi SSH 密钥](#)。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 依次单击**管理**选项卡和**设置**。
- 3 在“系统”下，选择**安全配置文件**。
- 4 在“服务”面板中，单击**编辑**。
- 5 从列表中选择一种服务。
 - ESXi Shell
 - SSH
 - 直接控制台 UI
- 6 单击**服务详细信息**，然后选择**手动启动和停止**启动策略。

如果选择**手动启动和停止**，则重新引导主机时不会启动服务。如果要在重新引导主机时启动服务，请选择**与主机一起启动和停止**。

7 选择**启动**以启用该服务。

8 单击**确定**。

后续步骤

设置 ESXi Shell 的可用性和闲置超时。请参见 [在 vSphere Web Client 中为 ESXi Shell 可用性创建超时](#) 和 [在 vSphere Web Client 中为闲置的 ESXi Shell 会话创建超时](#)

在 vSphere Web Client 中为 ESXi Shell 可用性创建超时

默认情况下，ESXi Shell 处于禁用状态。您可设置 ESXi Shell 可用性超时，提高启用 shell 时的安全性。

可用性超时设置是在启用 ESXi Shell 之后和必须登录之前，可以经过的时间量。超过超时期限之后，该服务会禁用，并且不允许用户登录。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 依次单击**管理**选项卡和**设置**。
- 3 在“系统”下，选择**高级系统设置**。
- 4 选择 UserVars.ESXiShellTimeOut，然后单击**编辑**图标。
- 5 输入闲置超时设置。
您必须重新启动 SSH 服务和 ESXi Shell 服务，超时才能生效。
- 6 单击**确定**。

结果

如果在经过超时期限后您已登录，您的会话将持续。但是，您注销或您的会话终止后，用户将无法登录。

在 vSphere Web Client 中为闲置的 ESXi Shell 会话创建超时

如果用户在主机上启用了 ESXi Shell，但却忘记了注销会话，则闲置会话将无限期保持连接状态。打开的连接会提高他人获得主机访问特权的可能性。您可以通过为闲置会话设置超时来防止出现此问题。

闲置超时是指用户从闲置交互式会话注销之前可以经过的时间量。您可以从直接控制台界面 (DCUI) 或 vSphere Web Client 中控制本地和远程 (SSH) 会话的时间量。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 依次单击**管理**选项卡和**设置**。
- 3 在“系统”下，选择**高级系统设置**。
- 4 选择 UserVars.ESXiShellInteractiveTimeOut，单击**编辑**图标，然后输入超时设置。
- 5 重新启动 ESXi Shell 服务和 SSH 服务，以使此超时生效。

结果

如果该会话闲置，则用户将在超时期限过后注销。

使用直接控制台用户界面 (DCUI) 启用对 ESXi Shell 的访问

通过直接控制台用户界面 (DCUI)，您可以使用基于文本的菜单在本地与主机进行交互。请仔细评估您的环境安全要求是否支持启用直接控制台用户界面。

可以使用直接控制台用户界面启用对 ESXi Shell 的本地和远程访问。

注 使用直接控制台用户界面、vSphere Web Client、ESXCLI 或其他管理工具对主机进行的更改，会每隔一小时或在正常关机时提交到永久存储。如果在提交这些更改之前主机出现故障，则可能会丢失这些更改。

步骤

- 1 从直接控制台用户界面中，按 F2 访问“系统自定义”菜单。
- 2 选择**故障排除选项**，然后按 Enter。
- 3 从“故障排除模式选项”菜单中，选择要启用的服务。
 - 启用 ESXi Shell
 - 启用 SSH
- 4 按 Enter 以启用该服务。
- 5 按 Esc 直到返回到直接控制台用户界面的主菜单。

后续步骤

设置 ESXi Shell 的可用性和闲置超时。请参见在直接控制台用户界面中为 [ESXi Shell 可用性创建超时](#) 和为 [闲置 ESXi Shell 会话创建超时](#)。

在直接控制台用户界面中为 ESXi Shell 可用性创建超时

默认情况下，ESXi Shell 处于禁用状态。您可设置 ESXi Shell 可用性超时，提高启用 shell 时的安全性。

可用性超时设置是在启用 ESXi Shell 之后和必须登录之前，可以经过的时间量。超过超时期限之后，该服务会禁用，并且不允许用户登录。

步骤

- 1 从“故障排除模式选项”菜单中，选择**修改 ESXi Shell 和 SSH 超时**，然后按 Enter。
- 2 输入可用性超时。

您必须重新启动 SSH 服务和 ESXi Shell 服务，超时才能生效。
- 3 按 Enter 并按 Esc 直到返回到直接控制台用户界面的主菜单。
- 4 单击**确定**。

结果

如果在经过超时期限后您已登录，您的会话将持续。但是，您注销或您的会话终止后，用户将无法登录。

为闲置 ESXi Shell 会话创建超时

如果用户在主机上启用了 ESXi Shell，但却忘记了注销会话，则闲置会话将无限期保持连接状态。打开的连接会提高他人获得主机访问特权的可能性。您可以通过为闲置会话设置超时来防止出现此问题。

闲置超时是用户从闲置交互式会话注销之前可以经过的时间量。对闲置超时的更改会在下次用户登录到 ESXi Shell 时应用，而不会影响现有会话。

您可以在直接控制台用户界面中设置以秒为单位的超时值，或在 vSphere Web Client 中设置以分钟为单位的超时值。

步骤

- 1 从“故障排除模式选项”菜单中，选择**修改 ESXi Shell 和 SSH 超时**，然后按 Enter。
- 2 输入闲置超时值（以秒为单位）。
您必须重新启动 SSH 服务和 ESXi Shell 服务，超时才能生效。
- 3 按 Enter 并按 Esc 直到返回到直接控制台用户界面的主菜单。

结果

如果该会话闲置，则用户将在超时期限过后注销。

登录 ESXi Shell 以进行故障排除

使用 vSphere Web Client、vSphere CLI 或 vSphere PowerCLI 执行 ESXi 配置任务。登录 ESXi Shell（以前称为技术支持模式或 TSM）仅进行故障排除。

步骤

- 1 使用以下方法之一登录 ESXi Shell。
 - 如果可以直接访问主机，请在计算机的物理控制台上按 **Alt+F1** 打开登录页面。
 - 如果要远程连接到主机，请使用 SSH 或其他远程控制台连接在主机上启动会话。
- 2 输入能够由主机识别的用户名和密码。

修改 ESXi Web 代理设置

当修改 Web 代理设置时，需要考虑若干加密和用户安全准则。

注 对主机目录或身份验证机制做出任何更改之后重新启动主机进程。

- 不要设置使用密码或密码短语的证书。ESXi 不支持使用密码或密码短语（也称为加密密钥）的 Web 代理。如果设置需要密码或密码短语的 Web 代理，则 ESXi 进程将无法启动。

- 为了支持对用户名、密码和数据包进行加密，将在默认情况下针对 vSphere Web Services SDK 连接启用 SSL。如果要配置这些连接以使它们不对传输进行加密，请对 vSphere Web Services SDK 连接禁用 SSL，方法是将连接从 HTTPS 切换至 HTTP。

仅当为这些客户端创建了完全可信的环境时才考虑禁用 SSL，在这样的环境中，安装有防火墙，而且与主机之间的传输是完全隔离的。禁用 SSL 可提高性能，因为省却了执行加密所需的开销。

- 为了防止误用 ESXi 服务，大多数内部 ESXi 服务只能通过端口 443（用于 HTTPS 传输的端口）来访问。端口 443 用作 ESXi 的反向代理。通过 HTTP 欢迎使用页面可看到 ESXi 上的服务列表，但如果未经适当授权，则不能直接访问存储适配器服务。

可对此配置进行更改，以便可通过 HTTP 连接直接访问各个服务。除非是在完全可信的环境中使用 ESXi，否则不要进行此更改。

- 在升级您的环境时，证书会保留在原位。

vSphere Auto Deploy 安全注意事项

要最有效地保护您的环境，请注意 Auto Deploy 与主机配置文件结合使用时可能存在的安全风险。

网络安全

保护您的网络，就像其他任何基于 PXE 的部署方法一样。vSphere Auto Deploy 通过 SSL 传输数据，以防止意外干扰和侦听。但是，在 PXE 引导期间不会检查客户端或 Auto Deploy 服务器的真实性。

通过完全隔离在其中使用 Auto Deploy 的网络，可以大幅降低 Auto Deploy 的安全风险。

引导映像和主机配置文件安全

vSphere Auto Deploy 服务器下载到计算机中的引导映像可以具有以下组件。

- 映像配置文件所包含的 VIB 软件包始终包含在引导映像中。
- 如果 Auto Deploy 规则设置为使用主机配置文件或主机自定义设置置备主机，则主机配置文件和主机自定义便包含在引导映像中。
 - 主机配置文件和主机自定义附带的管理员（根帐户）密码和用户密码进行了 MD5 加密。
 - 与配置文件关联的其他任何密码均采用明文形式。如果使用主机配置文件设置 Active Directory，则密码不受保护。

使用 vSphere Authentication Service 设置 Active Directory 以避免公开 Active Directory 密码。如果使用主机配置文件设置 Active Directory，则密码不受保护。

- 主机的公用和专用 SSL 密钥和证书都包含在引导映像中。

管理 ESXi 日志文件

日志文件是对攻击进行故障排除和获取有关违反主机安全的信息的一个重要组件。在安全、集中式日志服务器上记录日志有助于防止日志篡改。远程日志记录也能提供长期的审核记录。

采取下列措施来提高主机的安全性。

- 配置持久日志记录到数据存储。默认情况下，ESXi 主机上的日志存储在内存文件系统中。因此，当您重新引导主机时，日志将会丢失，并且仅存储 24 小时的日志数据。当启用持久日志记录时，您将会有专用的服务器活动记录用于主机。
- 中央主机上的远程日志记录可让您将日志文件收集到中央主机上，其中您使用单一工具便能监控所有主机。您也可以执行汇总分析和搜索日志数据，这可能会泄漏某些信息，例如对多个主机的协同攻击。
- 使用远程命令行（例如 vCLI 或 PowerCLI）或使用 API 客户端在 ESXi 主机上配置远程安全 syslog。
- 查询 syslog 配置以确保配置了有效的 syslog 服务器，包括正确的端口。

在 ESXi 主机上配置 Syslog

所有 ESXi 主机均运行 syslog 服务 (vmsyslogd)，该服务将来自 VMkernel 和其他系统组件的消息记录到日志文件中。

可以使用 vSphere Web Client 或 `esxcli system syslog vCLI` 命令来配置 syslog 服务。

有关使用 vCLI 命令的详细信息，请参见 vSphere Command-Line Interface 入门。

步骤

- 1 在 vSphere Web Client 清单中，选择主机。
- 2 单击**管理**选项卡。
- 3 在“系统”面板中，单击**高级系统设置**。
- 4 查找“高级系统设置”列表中的 **Syslog** 部分。
- 5 要全局设置日志记录，请选择要更改的设置，然后单击“编辑”图标。

选项	描述
Syslog.global.defaultRotate	设置要保留的存档的最大数目。可以在全局范围内设置该数目，也可以为单个子记录器设置该数目。
Syslog.global.defaultSize	在系统轮换日志前，设置日志的默认大小 (KB)。可以在全局范围内设置该数目，也可以为单个子记录器设置该数目。
Syslog.global.LogDir	存储日志的目录。该目录可能位于挂载的 NFS 或 VMFS 卷中。只有本地文件系统 中的 /scratch 目录在重新引导后仍然存在。目录应指定为 [数据存储名称] 文件路径，其中，路径是相对于支持数据存储卷的根目录的路径。例如，路径 [storage1] /systemlogs 将映射为路径 /vmfs/volumes/storage1/systemlogs。

选项	描述
Syslog.global.logDirUnique	选择此选项将使用 ESXi 主机的名称在 Syslog.global.LogDir 指定的目录下创建子目录。如果多个 ESXi 主机使用同一个 NFS 目录，则唯一的目录非常有用。
Syslog.global.LogHost	向其转发 syslog 消息的远程主机，以及远程主机在其上接收 syslog 消息的端口。可以包括协议和端口，例如 <code>ssl://hostName1:1514</code> 。支持 UDP（默认）、TCP 和 SSL。远程主机必须安装并正确配置 syslog 以接收转发的 syslog 消息。有关配置的信息，请参见远程主机上所安装的 syslog 服务的文档。

6 （可选）覆盖任何日志的默认日志大小和日志轮换。

- a 单击要自定义的日志的名称。
- b 单击“编辑”图标，然后输入所需的轮换和日志大小数量。

7 单击确定。

结果

对 syslog 选项的更改将立即生效。

ESXi 日志文件地址

ESXi 通过使用 syslog 功能，在日志文件中记录主机活动。

组件	位置	用途
VMkernel	<code>/var/log/vmkernel.log</code>	记录与虚拟机以及 ESXi 有关的活动。
VMkernel 警告	<code>/var/log/vmkwarning.log</code>	记录与虚拟机有关的活动。
VMkernel 摘要	<code>/var/log/vmksummary.log</code>	用于确定 ESXi 的正常运行时间和可用性统计信息（以逗号分隔）。
ESXi 主机代理日志	<code>/var/log/hostd.log</code>	包含管理和配置 ESXi 主机及其虚拟机的代理的有关信息。
vCenter 代理日志	<code>/var/log/vpxa.log</code>	包含与 vCenter Server 通信的代理的有关信息（如果主机由 vCenter Server 管理）。
Shell 日志	<code>/var/log/shell.log</code>	包含键入 ESXi Shell 的所有命令以及 Shell 事件（例如启用 Shell）的记录。
身份验证	<code>/var/log/auth.log</code>	包含与本地系统身份验证相关的所有事件。
系统消息	<code>/var/log/syslog.log</code>	包含所有常规日志消息，并且可用于进行故障排除。该信息以前位于消息日志文件中。
虚拟机	与受影响虚拟机的配置文件（名为 <code>vmware.log</code> 和 <code>vmware*.log</code> ）具有相同目录。例如， <code>/vmfs/volumes/datastore/virtual machine/vmware.log</code>	包含虚拟机电源事件、系统故障信息、Tools 状态和活动、时间同步、虚拟硬件更改、vMotion 迁移和虚拟机克隆等等。

确保 Fault Tolerance 日志记录通信的安全

当启用 Fault Tolerance (FT) 时，VMware vLockstep 可捕获主虚拟机上发生的输入和事件，并将这些输入和事件发送到正在另一主机上运行的辅助虚拟机。

主虚拟机和辅助虚拟机之间的此日志记录通信未加密，并且包含客户机网络和存储 I/O 数据以及客户机操作系统的内存内容。此通信可以包含敏感数据，如纯文本格式的密码。要避免泄露这类数据，请确保此网络的安全，特别是避免遭受“中间人”攻击。例如，将专用网络用于 FT 日志记录通信。

确保 vCenter Server 系统安全

6

确保 vCenter Server 安全包括确保运行 vCenter Server 的主机的安全性、遵守分配特权和角色的最佳实践，并验证连接到 vCenter Server 的客户端的完整性。

本章讨论了以下主题：

- vCenter Server 安全性最佳做法
- 验证旧版 ESXi 主机的指纹
- 验证“对网络文件复制的 SSL 证书验证”是否已启用
- vCenter Server TCP 和 UDP 端口
- 控制基于 CIM 的硬件监控工具访问

vCenter Server 安全性最佳做法

遵循 vCenter Server 安全性最佳做法有助于确保 vSphere 环境的完整性。

vCenter Server 访问控制的最佳做法

严格控制对不同 vCenter Server 组件的访问，以增强系统的安全性。

以下准则有助于确保环境的安全性。

使用指定帐户

- 如果本地 Windows 管理员帐户当前对 vCenter Server 拥有完全管理权限，请移除这些访问权限，并将这些权限授予一个或多个指定的 vCenter Server 管理员帐户。仅可将完全管理权限授予需要该权限的管理员。请勿将该特权授予其成员未受到严格控制的任何组。

注 从 vSphere 6.0 开始，默认情况下，本地管理员不再对 vCenter Server 拥有完全管理权限。建议不要使用本地操作系统用户。

- 请使用服务帐户而不是 Windows 帐户安装 vCenter Server。服务帐户必须是本地计算机上的管理员。
- 请确保应用程序在连接到 vCenter Server 系统时使用唯一的服务帐户。

最大程度地减少访问

避免允许用户直接登录到 vCenter Server 主机。登录到 vCenter Server 的用户可能会更改设置以及修改进程，从而会有意或无意地造成危害。这些用户还可能访问 vCenter 凭据，例如 SSL 证书。请仅允许要执行合法任务的用户登录到系统，并确保对登录事件进行审核。

监控 vCenter Server 管理员用户的特权

并非所有管理员用户都必须具有管理员角色。而是应该创建具有一组适当特权的自定义角色，并将其分配给其他管理员。

具有 vCenter Server 管理员角色的用户对层次结构中的所有对象都拥有特权。例如，默认情况下，管理员角色允许用户与虚拟机客户机操作系统内的文件和程序交互。将该角色分配给过多的用户可能会降低虚拟机数据的保密性、可用性或完整性。请创建一个角色，以便向管理员授予他们所需的特权，但移除部分虚拟机管理特权。

为 vCenter Server 数据库用户授予最小的特权

数据库用户仅需要特定于数据库访问的某些特权。此外，某些特权仅在进行安装和升级时需要。在安装或升级产品后，可以移除这些特权。

限制数据存储浏览器访问

数据存储浏览器功能允许具有适当特权的用户通过 Web 浏览器或 vSphere Web Client 在与 vSphere 部署关联的数据存储中查看、上载或下载文件。仅将**数据存储.浏览数据存储**特权分配给真正需要的用户或组。

限制用户在虚拟机中运行命令

默认情况下，具有 vCenter Server 管理员角色的用户可与虚拟机客户机操作系统内的文件和程序交互。为了降低损害客户机保密性、可用性或完整性的风险，请创建没有**客户机操作**特权的非客户机访问角色。请参见[限制用户在虚拟机中运行命令](#)。

验证 vpxuser 的密码策略

默认情况下，vCenter Server 会每 30 天自动更改一次 vpxuser 密码。请确保此设置符合您的策略，或将策略配置为符合公司的密码时效策略。请参见[设置 vCenter Server 密码策略](#)。

注 请确保密码时效策略的时间不能太短。

在 vCenter Server 重新启动后检查特权

请在重新启动 vCenter Server 时检查特权的重新分配情况。如果在根文件夹上分配了管理员角色的用户或用户组在重新启动期间无法被验证为有效的用户或组，则该角色会从该用户或组中移除。vCenter Server 会在其所在的位置向 vCenter Single Sign-On 帐户 administrator@vsphere.local 授予管理员角色。然后，此帐户可以充当管理员。

请重新建立一个指定的管理员帐户并为该帐户分配管理员角色，以避免使用匿名 administrator@vsphere.local 帐户。

使用高 RDP 加密级别

在基础架构中的每台 Windows 计算机上，请务必设置远程桌面主机配置设置，以确保适用于您环境的加密级别最高。

验证 vSphere Web Client 证书

指示其中一个 vSphere Web Client 或其他客户端应用程序的用户切勿忽略证书验证警告。若不进行证书验证，用户可能会受到 MiTM 攻击。

设置 vCenter Server 密码策略

默认情况下，vCenter Server 会每 30 天自动更改一次 vpxuser 密码。可以从 vSphere Web Client 中更改该值。

步骤

- 1 在 vSphere Web Client 对象层次结构中选择 vCenter Server。
- 2 依次单击**管理**选项卡和**设置**子选项卡。
- 3 单击**高级设置**，然后在筛选框中输入 **VimPasswordExpirationInDays**。
- 4 根据您的要求设置 `VirtualCenter.VimPasswordExpirationInDays`。

保护 vCenter Server Windows 主机

通过尽可能地确保主机环境的安全，保护运行 vCenter Server 的 Windows 主机免遭漏洞和攻击的威胁。

- 为 vCenter Server 系统维持一个支持的操作系统、数据库和硬件。如果 vCenter Server 未在受支持的操作系统上运行，则可能无法正常运行，从而使 vCenter Server 易受攻击。
- 使 vCenter Server 系统保持适当地修补。通过使操作系统及时更新最新的修补程序，可让 vCenter Server 不容易受到攻击。
- 对 vCenter Server 主机提供操作系统保护。提供的保护包括防病毒软件和反恶意软件。
- 在基础架构中的每台 Windows 计算机上，请务必根据行业标准准则或内部准则设置远程桌面 (RDP) 主机配置设置，以确保加密级别最高。

有关操作系统和数据库兼容性的信息，请参见 vSphere 兼容性列表。

从失败的安装中移除过期和撤销的证书和日志

在 vCenter Server 系统上保留已过期或已撤销的证书或者有关安装失败的 vCenter Server 安装日志会危及您的环境。

需要移除已过期或已撤销的证书，原因如下。

- 如果未从 vCenter Server 系统中移除已过期或已撤销的证书，则环境可能会受到 MiTM 攻击
- 在某些情况下，如果 vCenter Server 安装失败，则会在系统上创建一个包含纯文本数据库密码的日志文件。侵入 vCenter Server 系统的攻击者可能会访问该密码，同时获得对 vCenter Server 数据库的访问权限。

限制 vCenter Server 网络连接

为提高安全性，请避免将 vCenter Server 系统放置在管理网络之外的任何网络上，并确保 vSphere 管理流量位于受限网络上。通过限制网络连接，可以限制特定类型的攻击。

vCenter Server 仅需要访问管理网络。避免将 vCenter Server 系统放置在其他网络（如生产网络、存储网络或有权访问 Internet 的任何网络）上。vCenter Server 不需要访问 vMotion 在其中运行的网络。

vCenter Server 需要与以下系统建立网络连接。

- 所有 ESXi 主机。
- vCenter Server 数据库。
- 其他 vCenter Server 系统（如果 vCenter Server 系统是用于复制标记、权限等的常见 vCenter Single Sign-On 域的一部分）。
- 有权运行管理客户端的系统。例如，vSphere Web Client（您在其中使用 PowerCLI 的 Windows 系统）或任何其他基于 SDK 的客户端。
- 运行加载项组件（例如 VMware vSphere Update Manager）的系统。
- 基础架构服务，例如 DNS、Active Directory 和 NTP。
- 运行对 vCenter Server 系统功能至关重要的组件的其他系统。

使用运行 vCenter Server 系统的 Windows 系统上的本地防火墙或使用网络防火墙。包含基于 IP 的访问限制，这样只有必要的组件才能与 vCenter Server 系统通信。

考虑限制 Linux 客户端的使用

默认情况下，客户端组件与 vCenter Server 系统或 ESXi 主机之间的通信由基于 SSL 的加密进行保护。这些组件的 Linux 版本不会执行证书验证。考虑限制 Linux 客户端的使用。

即使您已将 vCenter Server 系统和 ESXi 主机上的 VMCA 签名证书替换为由第三方 CA 签名的证书，但与 Linux 客户端的某些通信仍然容易受到中间人的攻击。以下组件在 Linux 操作系统上运行时易受攻击。

- vCLI 命令
- vSphere SDK for Perl 脚本
- 使用 vSphere Web Services SDK 编写的程序

如果强制执行适当的控制，则可放宽对使用 Linux 客户端的限制。

- 仅限授权系统访问管理网络。
- 使用防火墙确保只允许授权主机访问 vCenter Server。
- 使用跳转盒系统确保 Linux 客户端受跳转限制。

检查已安装的插件

vSphere Web Client 扩展在登录用户的相同特权级别下运行。恶意扩展可以伪装成有用的插件并执行有害的操作，例如盗取凭据或更改系统配置。为增强安全性，请使用仅包含来自受信任源的授权扩展的 vSphere Web Client 安装。

vCenter 安装包含 vSphere Web Client 可扩展性框架，其提供通过菜单选项或工具栏图标（提供对 vCenter 加载项组件或外部基于 Web 的功能的访问）来扩展 vSphere Web Client 的功能。在此灵活性下，存在引入意外功能的风险。例如，如果管理员在 vSphere Web Client 的一个实例中安装插件，则该插件可以使用该管理员的特权级别执行任意命令。

为了保护 vSphere Web Client 免受潜在的危害，可以定期检查所有已安装的插件并确保所有插件均来自受信任的源。

前提条件

您必须具有访问 vCenter Single Sign-On 服务的特权。这些特权与 vCenter Server 特权不同。

步骤

- 1 以 administrator@vsphere.local 或拥有 vCenter Single Sign-On 特权用户的身份登录到 vSphere Web Client。
- 2 在主页上，选择**管理**，然后选择**解决方案**下的**客户端插件**
- 3 检查客户端插件列表。

vCenter Server Appliance 安全性最佳做法

遵循确保 vCenter Server 系统安全的所有最佳做法，进而确保 vCenter Server Appliance 安全。下述额外步骤将有助于提高环境的安全性。

配置 NTP

确保所有系统使用相同的相对时间源（包括相关的本地化偏移），并且相对时间源可以与商定的时间标准（如协调世界时-UTC）相关联。同步的系统对于证书有效性至关重要。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。请参见[将 vCenter Server Appliance 中的时间与 NTP 服务器同步](#)。

限制 vCenter Server Appliance 网络访问

仅限与 vCenter Server Appliance 通信所需的基本组件访问。阻止不必要的系统访问可降低操作系统遭受常见攻击的可能性。仅限这些基本组件访问，可将风险降至最低。

验证旧版 ESXi 主机的指纹

在 vSphere 6 及更高的版本中，默认情况下，将为主机分配 VMCA 证书。如果将证书模式更改为指纹，则可以继续为旧版主机使用指纹模式。您可以在 vSphere Web Client 中验证指纹。

注 默认情况下，证书在各次升级中均被保留。

步骤

- 1 在 vSphere Web Client 对象导航器中，浏览到 vCenter Server 系统。
- 2 选择**管理**选项卡，然后依次单击**设置**和**常规**。
- 3 单击**编辑**。
- 4 单击 **SSL 设置**。
- 5 如果任何 ESXi 或更低的版本的主机需要手动验证，则可以比较主机列出的指纹和主机控制台中的指纹。

要获取主机指纹，请使用直接控制台用户界面 (DCUI)。

- a 登录到直接控制台并按 F2 以访问“系统自定义”菜单。
- b 选择**查看支持信息**。

在右侧列中将显示主机指纹。

- 6 如果指纹匹配，则选中主机旁边的**验证**复选框。

单击**确定**之后，未选中的主机将断开连接。

- 7 单击**确定**。

验证“对网络文件复制的 SSL 证书验证”是否已启用

网络文件复制 (NFC) 可为 vSphere 组件提供文件类型感知 FTP 服务。从 vSphere 5.5 开始，默认情况下，ESXi 会使用 NFC 执行在数据存储之间复制和移动数据等操作，但如果 NFC 处于禁用状态，则需要启用它。

如果启用了基于 NFC 的 SSL，则通过 NFC 在 vSphere 组件之间建立的连接将是安全的。该连接有助于防止数据中心内受到中间人攻击。

由于通过 SSL 使用 NFC 会造成性能降低，因此在某些开发环境中您可能会考虑禁用此高级设置。

注 如果使用脚本检查此值，请将此值明确设为 True。

步骤

- 1 通过 vSphere Web Client 连接到 vCenter Server。
- 2 选择**设置**选项卡，然后单击**高级设置**。
- 3 单击**编辑**。
- 4 在对话框的底部，输入以下“键”和“值”。

字段	值
键	config.nfc.useSSL
值	true

- 5 单击**确定**。

vCenter Server TCP 和 UDP 端口

vCenter Server 可通过预定的 TCP 和 UDP 端口进行访问。若要从防火墙外管理网络组件，可能需重新配置防火墙以允许在适当端口的访问。

下表列出了 TCP 和 UDP 端口，以及每个端口的用途和类型。在安装时默认打开的端口用（默认）进行指示。有关不同版本 vSphere 的所有 vSphere 组件的最新端口列表，请参见 [VMware 知识库文章 1012382](#)。

表 6-1. vCenter Server TCP 和 UDP 端口

端口	用途
80（默认）	HTTP 访问 vCenter Server 需要使用端口 80 进行直接 HTTP 连接。端口 80 将请求重定向到 HTTPS 端口 443。如果意外使用 <code>http://server</code> 而非 <code>https://server</code> ，则此重定向将有所帮助 WS 管理（也需要打开端口 443）
88、2013	Kerberos 的控制接口 RPC，由 vCenter Single Sign-On 使用。
123	NTP 客户端
135（默认）	对于 vCenter Server Appliance，指定此端口用于 Active Directory 身份验证。 对于 vCenter Server Windows 安装，此端口用于链接模式，而端口 88 用于 Active Directory 身份验证。
161（默认）	SNMP 服务器。这是 ESXi 主机和 vCenter Server Appliance 上的默认端口。
389	vCenter Single Sign-On LDAP（6.0 及更高版本）
636	vCenter Single Sign-On LDAPS（6.0 及更高版本）
443（默认）	vCenter Server 系统使用端口 443 监控从 SDK 客户端传输的数据。 此端口也用于以下服务： <ul style="list-style-type: none"> ■ WS 管理（也需要打开端口 80） ■ 第三方网络管理客户端与 vCenter Server 的连接 ■ 第三方网络管理客户端对主机的访问
2012	VMware Directory Service (vmdir) 的 RPC 端口。
2014	VMware Certificate Authority (VMCA) 服务的 RPC 端口。
2020	VMware Authentication Framework Service (vmafd) 的 RPC 端口。
31031、44046（默认）	vSphere Replication
7444	vCenter Single Sign-On HTTPS。
8093	客户端集成插件使用本地环回主机名，并使用端口 8093 和范围为 50100 到 60099 的随机端口。客户端集成插件将端口 8093 仅用于本地通信。该端口可以保持由防火墙阻止的状态。
8109	VMware Syslog Collector。
9443	vSphere Web Client 对 ESXi 主机进行 HTTP 访问。
10080	Inventory Service。

表 6-1. vCenter Server TCP 和 UDP 端口（续）

端口	用途
11711	vCenter Single Sign-On LDAP（从 vSphere 5.5 升级的环境）
11712	vCenter Single Sign-On LDAPS（从 vSphere 5.5 升级的环境）
12721	VMware Identity Management Service。
15005	ESX Agent Manager (EAM)。ESX Agent 可以是虚拟机或可选的 VIB。该代理可扩展 ESXi 主机的功能，提供诸如 NSX-v 或 vRealize Automation 等 vSphere 解决方案需要的其他服务。
15007	vService Manager (VSM)。此服务用于注册 vCenter Server 扩展。仅当要使用的扩展需要时才打开此端口。
50100-60099	客户端集成插件使用本地环回主机名，并使用端口 8093 和范围为 50100 到 60099 的随机端口。客户端集成插件将此端口范围仅用于本地通信。该端口可以保持由防火墙阻止的状态。

除了这些端口外，您可以根据需要配置其他端口。

控制基于 CIM 的硬件监控工具访问

公用信息模型 (CIM) 系统提供了一个接口，便于使用一组标准 API 从远程应用程序进行硬件级别管理。为了确保 CIM 接口安全，请仅为这些应用程序提供必需的最小访问权限。如果某个应用程序已经置备有根或完全管理员帐户且该应用程序受到影响，则整个虚拟环境就可能会受到影响。

CIM 是一种开放式标准，用于为 ESXi 硬件资源的无代理且基于标准的监控定义一个框架。该框架由一个 CIM 对象管理器（通常称为“CIM 代理程序”）和一组 CIM 提供程序构成。

CIM 提供程序用作提供设备驱动程序和基础硬件管理访问权限的机制。硬件供应商（包括服务器制造商和特定硬件设备供应商）可编写提供程序，以便对其特定设备进行监控和管理。VMware 还会编写一些提供程序，用于对服务器硬件、ESXi 存储基础架构和虚拟化特定资源实施监控。这些提供程序在 ESXi 系统内运行，因此极其轻量且侧重于特定管理任务。CIM 代理程序从所有 CIM 提供程序获取信息，并通过标准 API（最常见的一个是 WS-MAN）将其呈现给外界。

请不要为远程应用程序提供访问 CIM 接口的 root 凭据。而是应该创建这些应用程序专用的服务帐户，并为 ESXi 系统上定义的任何本地帐户以及 vCenter Server 中定义的任何角色授予对 CIM 信息的只读访问权限。

步骤

- 1 创建特定于 CIM 应用程序的服务帐户。
- 2 授予在 ESXi 系统中定义的所有本地帐户以及在 vCenter Server 中定义的所有角色对 CIM 信息的只读访问权限。
- 3 （可选）如果应用程序需要对 CIM 接口的写入访问权限，请创建一个要应用于服务帐户的角色，使其仅拥有以下两项特权：
 - 主机.配置.系统管理
 - 主机.CIM.CIM 交互

根据监控应用程序的工作方式，该角色可以是主机上的本地角色，也可以在 vCenter Server 中集中定义。

结果

当用户使用为 CIM 应用程序创建的服务帐户登录主机时，该用户仅拥有**系统管理**和 **CIM 交互**特权或只读访问权限。

确保虚拟机安全

7

在虚拟机中运行的客户机操作系统会与物理系统一样遭遇相同的安全风险。请像保护物理计算机一样确保虚拟机的安全。

本章讨论了以下主题：

- 限制信息性消息从虚拟机流向 VMX 文件
- 防止虚拟磁盘压缩
- 虚拟机安全性最佳做法

限制信息性消息从虚拟机流向 VMX 文件

限制信息性消息从虚拟机流向 VMX 文件，从而避免填充数据存储和造成拒绝服务 (DoS)。如果您不控制虚拟机的 VMX 文件的大小，并且 VMX 的信息量超过数据存储的容量，则会造成拒绝服务。

默认情况下，包含信息性名称值对的配置文件将限制为 1 MB。此容量在大多数情况下是足够的，但是在必要时可以更改此值。例如，如果向配置文件中存储的自定义信息较多，可以增加该限制值。

注 请仔细考量所需要的信息量。如果信息量超过数据存储的容量，则可能会造成拒绝服务。

即使高级选项中未列出 `tools.setInfo.sizeLimit` 参数，也会应用 1 MB 的默认限制。

步骤

- 1 在 vSphere Web Client 清单中查找虚拟机。
 - a 选择数据中心、文件夹、群集、资源池或主机。
 - b 单击**相关对象**选项卡，然后单击**虚拟机**。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 选择**虚拟机选项**。
- 4 单击**高级**，然后单击**编辑配置**。
- 5 添加或编辑 `tools.setInfo.sizeLimit` 参数。

防止虚拟磁盘压缩

客户机操作系统中的非管理用户能够压缩虚拟磁盘。压缩虚拟磁盘将回收未使用的磁盘空间。但是，如果重复压缩虚拟磁盘，磁盘会变得不可用且造成拒绝服务。为了避免这种情况，请禁用压缩虚拟磁盘的功能。

前提条件

- 关闭虚拟机。
- 验证您是否对虚拟机拥有 root 或管理员特权。

步骤

- 1 在 vSphere Web Client 清单中查找虚拟机。
 - a 选择数据中心、文件夹、群集、资源池或主机。
 - b 单击**相关对象**选项卡，然后单击**虚拟机**。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 选择**虚拟机选项**。
- 4 单击**高级**，然后单击**编辑配置**。
- 5 添加或编辑以下参数。

名称	值
isolation.tools.diskWiper.disable	TRUE
isolation.tools.diskShrink.disable	TRUE

- 6 单击**确定**。

结果

如果禁用此功能，当数据存储空间不足时您将无法压缩虚拟机磁盘。

虚拟机安全性最佳做法

遵循虚拟机安全性最佳做法有助于确保 vSphere 部署的完整性。

- **虚拟机常规保护**
虚拟机在大多数情况下等同于物理服务器。在虚拟机中采用与物理系统相同的安全措施。
- **使用模板来部署虚拟机**
在虚拟机上手动安装客户机操作系统和应用程序时，会带来配置错误的风险。通过使用模板捕捉未安装任何应用程序的强化基础操作系统映像，可以确保通过已知的安全基准级别创建所有虚拟机。
- **尽量少用虚拟机控制台**
虚拟机控制台为虚拟机提供的功能与物理服务器上的监视器相同。具有虚拟机控制台访问权限的用户可以访问虚拟机电源管理和可拆除设备连接控制，从而可能造成对虚拟机的恶意攻击。

■ 防止虚拟机取代资源

当一个虚拟机消耗过多主机资源而使主机上的其他虚拟机无法执行其预期功能时，可能会出现拒绝服务 (DoS)。为防止虚拟机造成 DoS 问题，请使用主机资源管理功能（例如设置份额和使用资源池）。

■ 禁用虚拟机中不必要的功能

虚拟机中运行的任何服务都有可能引发攻击。通过禁用不必要的系统组件（不是支持系统上运行的应用程序或服务所必需的），可减少会受到攻击的组件数量。

虚拟机常规保护

虚拟机在大多数情况下等同于物理服务器。在虚拟机中采用与物理系统相同的安全措施。

请遵循以下这些最佳做法以保护您的虚拟机：

修补程序及其他保护措施

保持所有安全措施最新，包括应用适当的修补程序。跟踪已关闭电源的休眠虚拟机中的更新特别重要，因为这些虚拟机常常会被忽略。例如，确保对您虚拟基础架构中的每台虚拟机均启用防病毒软件、防间谍软件、入侵检测及其他保护措施。还应确保您具有足够的空间来存储虚拟机日志。

防病毒扫描

由于每台虚拟机都承载着标准操作系统，因此必须安装防病毒软件，使其免遭病毒感染。根据虚拟机的使用方式，可能还需要安装软件防火墙。

请错开病毒扫描的调度，尤其是在具有大量虚拟机的部署中。如果同时扫描所有虚拟机，环境中的系统性能将大幅下降。因为软件防火墙和防病毒软件需要占用大量虚拟化资源，因此您可以根据虚拟机性能平衡这两个安全措施的需求，尤其是在您确信虚拟机处于充分可信的环境中时。

串行端口

串行端口是用于将外围设备连接到虚拟机的接口。串行端口通常用于物理系统上，以提供与服务器控制台的直接、低级别连接，且虚拟串行端口允许对虚拟机进行相同的访问。串行端口允许低级别访问，此类访问通常没有诸如登录或特权之类的严格控制。

使用模板来部署虚拟机

在虚拟机上手动安装客户机操作系统和应用程序时，会带来配置错误的风险。通过使用模板捕捉未安装任何应用程序的强化基础操作系统映像，可以确保通过已知的安全基准级别创建所有虚拟机。

您可以使用包含已强化、修补且正确配置的操作系统的模板来创建其他特定于应用程序的模板，也可以使用应用程序模板来部署虚拟机。

步骤

- ◆ 提供模板来创建虚拟机，模板中包含强化、修补且正确配置的操作系统的部署。

如果可能，还可在模板中部署应用程序。确保应用程序不依赖于特定于要部署的虚拟机的信息。

后续步骤

有关模板的详细信息，请参见《vSphere 虚拟机管理》文档。

尽量少用虚拟机控制台

虚拟机控制台为虚拟机提供的功能与物理服务器上的监视器相同。具有虚拟机控制台访问权限的用户可以访问虚拟机电源管理和可拆除设备连接控制，从而可能造成对虚拟机的恶意攻击。

步骤

- 1 请使用本机远程管理服务（如终端服务和 SSH）与虚拟机进行交互。

请只在需要时才授予对虚拟机控制台的访问权限。

- 2 将控制台的连接数限制为尽量少的连接。

例如，在高度安全的环境中，将连接数限制为一。在某些环境中，您可以根据完成正常任务所需的并发连接数增加此限额。

防止虚拟机取代资源

当一个虚拟机消耗过多主机资源而使主机上的其他虚拟机无法执行其预期功能时，可能会出现拒绝服务 (DoS)。为防止虚拟机造成 DoS 问题，请使用主机资源管理功能（例如设置份额和使用资源池）。

默认情况下，ESXi 主机上的所有虚拟机平均共享资源。可以使用份额和资源池以防止出现拒绝服务攻击，从而导致一个虚拟机消耗过多主机资源，使同一主机上的其他虚拟机无法执行其预期功能。

除非完全了解有关影响，否则不要使用限制。

步骤

- 1 为每个虚拟机置备刚好足以正常运行的资源（CPU 和内存）。
- 2 使用“份额”保证资源分配给关键的虚拟机。
- 3 将具有类似要求的虚拟机分组到资源池。
- 4 在每个资源池中，保持将“份额”设置为默认值，以确保池中的每个虚拟机获得大致相同的资源优先级。

使用此设置，单个虚拟机无法使用比资源池中其他虚拟机更多的资源。

后续步骤

有关共享和限制的信息，请参见《vSphere 资源管理》文档。

禁用虚拟机中不必要的功能

虚拟机中运行的任何服务都有可能引发攻击。通过禁用不必要的系统组件（不是支持系统上运行的应用程序或服务所必需的），可减少会受到攻击的组件数量。

通常，虚拟机需要的服务或功能不像物理服务器那样多。对系统进行虚拟化时，请评估特定服务或功能是否必要。

步骤

- ◆ 禁用操作系统中未使用的服务。

例如，如果系统运行文件服务器，则应关闭所有 Web 服务。

- ◆ 断开未使用的物理设备（例如 CD/DVD 驱动器、软盘驱动器和 USB 适配器）的连接。
- ◆ 禁用未使用的功能，例如未使用的显示功能或 HGFS（主机客户机文件系统）。
- ◆ 关闭屏幕保护程序。
- ◆ 除非必要，否则不要在 Linux、BSD 或 Solaris 客户机操作系统上运行 X Window 系统。

移除不必要的硬件设备

启用或连接的任何设备都可能成为攻击渠道。虚拟机上不具有特权的用户和进程可以连接或断开硬件设备（如网络适配器和 CD-ROM 驱动器）。攻击者可利用该能力破坏虚拟机安全性。移除不需要的硬件设备有助于阻止攻击。

具有虚拟机访问权限的攻击者可以连接已断开的硬件设备并访问遗留在驱动器中介质上的敏感信息，或者断开网络适配器以将虚拟机与其网络隔离，从而造成拒绝服务。

- 确保未连接未授权的设备，并移除所有不需要或不使用的硬件设备。
- 从虚拟机中禁用不必要的虚拟设备。
- 确保不会将任何不需要的设备连接到虚拟机。串行和并行端口很少在数据中心中用于虚拟机，而 CD/DVD 驱动器在软件安装期间通常仅进行临时连接。

步骤

- 1 使用 vSphere Web Client 登录到 vCenter Server 系统。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 检查每个硬件设备并确保其处于已连接状态。

包括检查以下设备：

- 软盘驱动器
- 串行端口
- 并行端口
- USB 控制器
- CD-ROM 驱动器

禁用未使用的显示功能

攻击者可以使用未使用的显示功能作为将恶意代码插入环境的向量。禁用环境中未使用的功能。

步骤

- 1 在 vSphere Web Client 清单中查找虚拟机。
 - a 选择数据中心、文件夹、群集、资源池或主机。
 - b 单击**相关对象**选项卡，然后单击**虚拟机**。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 选择**虚拟机选项**。

- 4 单击**高级**，然后单击**编辑配置**。
- 5 在适当的情况下，添加或编辑（如适用）以下参数以对其进行设置。

选项	描述
<code>svga.vgaonly</code>	如果将此参数设置为 <code>TRUE</code> ，则高级图形功能将不再运行。仅字符单元控制台模式可用。如果使用此设置，则 <code>mks.enable3d</code> 不起作用。 注 将此设置仅应用到不需要虚拟化显卡的虚拟机。
<code>mks.enable3d</code>	在不需要 3D 功能的虚拟机上将此参数设置为 <code>FALSE</code> 。

禁用未公开的功能

VMware 虚拟机在 vSphere 系统与托管虚拟化平台（例如 Workstation 和 Fusion）上都能运行。在 vSphere 系统上运行虚拟机时，无需启用某些虚拟机参数。禁用这些参数可降低出现漏洞的可能性。

前提条件

关闭虚拟机。

步骤

- 1 在 vSphere Web Client 清单中查找虚拟机。
 - a 选择数据中心、文件夹、群集、资源池或主机。
 - b 单击**相关对象**选项卡，然后单击**虚拟机**。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 选择**虚拟机选项**。
- 4 单击**高级**，然后单击**编辑配置**。
- 5 添加或编辑以下参数以将其设置为 `TRUE`。
 - `isolation.tools.unity.push.update.disable`
 - `isolation.tools.ghi.launchmenu.change`
 - `isolation.tools.memSchedFakeSampleStats.disable`
 - `isolation.tools.getCreds.disable`
 - `isolation.tools.ghi.autologon.disable`
 - `isolation.bios.bbs.disable`
 - `isolation.tools.hgfsServerSet.disable`
- 6 单击**确定**。

禁用 HGFS 文件传输

某些操作（如 Tools 自动升级）会使用称为主机客户机文件系统 (HGFS) 的虚拟化管理程序中的组件。在高安全性环境中，您可以禁用此组件以将攻击者可能使用 HGFS 在客户机操作系统中传输文件的风险降到最低。

步骤

- 1 在 vSphere Web Client 清单中查找虚拟机。
 - a 选择数据中心、文件夹、群集、资源池或主机。
 - b 单击**相关对象**选项卡，然后单击**虚拟机**。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 选择**虚拟机选项**。
- 4 单击**高级**，然后单击**编辑配置**。
- 5 验证 `isolation.tools.hgfsServerSet.disable` 参数是否已设置为 TRUE。

结果

如果更改此值，VMX 进程将不再响应 Tools 进程的命令。使用 HGFS 将文件传入和传出客户机操作系统的 API（例如某些 VIX 命令或 VMware Tools 自动升级实用程序）将不再运行。

禁用客户机操作系统和远程控制台之间的复制和粘贴操作

默认情况下，客户机操作系统和远程控制台之间的复制和粘贴操作处于禁用状态。为了确保环境安全，请保留默认设置。如果需要复制和粘贴操作，则必须使用 vSphere Web Client 将其启用。

默认情况下，这些选项设置为建议的值。但是，如果要启用审核工具来检查设置是否正确，则必须将这些选项明确设为 true。

前提条件

关闭虚拟机。

步骤

- 1 使用 vSphere Web Client 登录到 vCenter Server 系统。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 单击**虚拟机选项**，然后单击**编辑配置**。
- 4 确保“名称”和“值”列中存在以下值，或单击**添加行**进行添加。

名称	建议的值
<code>isolation.tools.copy.disable</code>	有效
<code>isolation.tools.paste.disable</code>	有效
<code>isolation.tools.setGUIOptions.enable</code>	无效

这些选项将替代在客户机操作系统的 VMware Tools 控制面板中做出的任何设置。

- 5 单击**确定**。
- 6 （可选）如果更改了配置参数，则要重新启动虚拟机。

限制公开复制到剪贴板中的敏感数据

默认情况下，已禁用针对主机的复制和粘贴操作，以防止公开已复制到剪贴板中的敏感数据。

当在运行 VMware Tools 的虚拟机上启用复制和粘贴时，可以在客户机操作系统和远程控制台之间进行复制和粘贴。控制台窗口获得焦点时，虚拟机中运行的非特权用户和进程均可以访问虚拟机控制台的剪贴板。如果用户在使用控制台前将敏感信息复制到剪贴板中，就可能在无意中向虚拟机暴露敏感数据。为防止此问题，默认情况下已禁用针对客户机操作系统的复制和粘贴操作。

可以在必要时为虚拟机启用复制和粘贴操作。

限制用户在虚拟机中运行命令

默认情况下，具有 vCenter Server 管理员角色的用户可与虚拟机客户机操作系统内的文件和程序交互。为了降低损害客户机保密性、可用性或完整性的风险，请创建没有**客户机操作**特权的非客户机访问角色。

为安全起见，请严格限制对虚拟数据中心的访问，严格程度与限制对物理数据中心的访问相同。为避免授予用户完全管理员访问权限，请创建禁用客户机访问的自定义角色，并将该角色应用于需要管理员特权但无权与客户机操作系统内的文件和程序交互的用户。

例如，某项配置可能包括其上带有敏感信息的基础架构中的虚拟机。通过 vMotion 和 Storage vMotion 进行迁移等任务要求 IT 角色有权访问该虚拟机。在这种情况下，应禁用客户机操作系统中的部分远程操作，以确保该 IT 角色无法访问敏感信息。

前提条件

验证您对在其上创建该角色的 vCenter Server 系统是否拥有**管理员**特权。

步骤

- 1 以对要在其上创建该角色的 vCenter Server 系统拥有**管理员**特权的用户身份登录 vSphere Web Client。
- 2 单击**系统管理**，然后选择**角色**。
- 3 单击**创建角色操作**图标，然后键入角色的名称。
例如，键入**无客户机访问权限的管理员**。
- 4 选择**所有特权**。
- 5 通过取消选择**所有特权.虚拟机.客户机操作**，移除一组客户机操作特权。
- 6 单击**确定**。

后续步骤

选择 vCenter Server 系统或主机，并分配权限，该权限可将应具有新特权的用户或组配对到新创建的角色。从默认管理员角色中移除这些用户。

阻止虚拟机用户或进程与设备断开连接

虚拟机内不具有 root 或管理员特权的用户和进程能够连接设备（如网络适配器和 CD-ROM 驱动器）或断开设备的连接，还能够修改设备设置。若要提高虚拟机安全性，请移除这些设备。如果不想永久移除设备，可以阻止虚拟机用户或进程在客户机操作系统中连接设备或与设备断开连接。

前提条件

关闭虚拟机。

步骤

- 1 在 vSphere Web Client 清单中查找虚拟机。
 - a 选择数据中心、文件夹、群集、资源池或主机。
 - b 单击**相关对象**选项卡，然后单击**虚拟机**。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 选择**虚拟机选项**。
- 4 单击**高级**，然后单击**编辑配置**。
- 5 验证以下值是否在“名称”和“值”列中，或者单击**添加行**来添加这些值。

名称	值
isolation.device.connectable.disable	有效
isolation.device.edit.disable	有效

这些选项将替代在客户机操作系统的 VMware Tools 控制面板中做出的任何设置。

- 6 单击**确定**以关闭“配置参数”对话框，然后再次单击**确定**。

修改客户机操作系统的可变内存限制

如果配置文件中存储的自定义信息较多，可以增加客户机操作系统的可变内存限制。

前提条件

关闭虚拟机。

步骤

- 1 在 vSphere Web Client 清单中查找虚拟机。
 - a 选择数据中心、文件夹、群集、资源池或主机。
 - b 单击**相关对象**选项卡，然后单击**虚拟机**。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 选择**虚拟机选项 > 高级**，然后单击**编辑配置**。
- 4 添加或编辑参数 `tools.setInfo.sizeLimit`，并将值设置为字节数。
- 5 单击**确定**。

阻止客户机操作系统进程向主机发送配置消息

可以阻止客户机将任何名称/值对写入到配置文件中。该选择适合必须阻止客户机操作系统修改配置设置的情况。

前提条件

关闭虚拟机。

步骤

- 1 在 vSphere Web Client 清单中查找虚拟机。
 - a 选择数据中心、文件夹、群集、资源池或主机。
 - b 单击**相关对象**选项卡，然后单击**虚拟机**。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 选择**虚拟机选项**。
- 4 单击**高级**，然后单击**编辑配置**。
- 5 单击**添加行**，并在“名称”和“值”列中键入以下值。
 - 在“名称”列中：**isolation.tools.setinfo.disable**
 - 在“值”列中：**有效**
- 6 单击**确定**以关闭“配置参数”对话框，然后再次单击**确定**。

避免使用独立非持久磁盘

如果使用的是独立非持久磁盘，成功入侵的攻击者可以通过关机或重新启动系统来销毁计算机受到影响的证据。如果虚拟机上没有持久的活动记录，管理员可能对攻击一无所知。因此，应该避免使用独立非持久磁盘。

步骤

- ◆ 确保虚拟机活动已远程记录在单独的服务器（例如 syslog 服务器或等同的基于 Windows 的事件收集器）上。

如果未对客户机配置事件和活动的远程日志记录，scsiX:Y. 模式应为以下设置之一：

 - 不存在
 - 未设置为独立非持久

结果

如果未启用非持久模式，则重新引导系统时，不能将虚拟机回滚至已知状态。

确保 vSphere 网络安全

8

确保 vSphere 网络安全是保护环境的至关重要的一部分。可以通过不同的方式确保不同 vSphere 组件的安全。有关 vSphere 环境中的网络的详细信息，请参见《vSphere 网络连接》文档。

本章讨论了以下主题：

- vSphere 网络安全简介
- 使用防火墙确保网络安全
- 确保物理交换机安全
- 使用安全策略确保标准交换机端口安全
- 确保 vSphere 标准交换机的安全
- 确保 vSphere Distributed Switch 和分布式端口组的安全
- 通过 VLAN 确保虚拟机安全
- 在单台 ESXi 主机上创建网络 DMZ
- 在单台 ESXi 主机中创建多个网络
- Internet 协议安全
- 确保 SNMP 配置正确
- 仅在需要时才在 vSphere Network Appliance API 中使用虚拟交换机
- vSphere 网络连接安全性最佳做法

vSphere 网络安全简介

vSphere 环境中的网络安全不仅具有保护物理网络环境的特性，而且具有一些仅适用于虚拟机的特性。

防火墙

为虚拟网络增加防火墙保护，方法是在其中的部分或所有虚拟机上安装和配置基于主机的防火墙。

为提高效率，可设置专用虚拟机以太网或虚拟网络。有了虚拟网络，可在网络最前面的虚拟机上安装基于主机的防火墙。此防火墙可以充当物理网络适配器和虚拟网络中剩余虚拟机之间的保护性缓存。

由于基于主机的防火墙会降低性能，因此请先根据性能目标对安全需求进行权衡，然后再决定在虚拟网络中的其他虚拟机上安装基于主机的防火墙。

请参见[使用防火墙确保网络安全](#)。

分段

将主机中的不同虚拟机区域置于不同网络段上。如果将每个虚拟机区域隔离在自己的网络段中，可以大大降低虚拟机区域间泄漏数据的风险。分段可防止多种威胁，包括地址解析协议 (ARP) 欺骗，即攻击者操作 ARP 表格以重新映射 MAC 和 IP 地址，从而访问进出主机的网络流量。攻击者使用 ARP 欺骗生成中间人 (MITM) 攻击、执行拒绝服务 (DoS) 攻击，劫持目标系统并以其他方式破坏虚拟网络。

仔细计划分段可降低虚拟机区域间传输数据包的几率，从而防止嗅探攻击（此类攻击需向受害者发送网络流量）。此外，攻击者无法使用一个虚拟机区域中的不安全服务访问主机中的其他虚拟机区域。可以使用两种方法之一实施分段。每种方法具有不同优势。

- 为虚拟机区域使用单独的物理网络适配器以确保将区域隔离。为虚拟机区域使用单独的物理网络适配器可能是最安全的方法，并且更不容易在初次创建段之后出现配置错误。
- 设置虚拟局域网 (VLAN) 以帮助保护网络。VLAN 几乎能够提供以物理方式实施单独网络所具有的所有安全优势，但省去了硬件开销，可为您节省部署和维护附加设备、线缆等硬件的成本，是一种可行的解决方案。请参见[通过 VLAN 确保虚拟机安全](#)。

阻止未授权的访问

如果将虚拟机网络连接到物理网络，则其遭到破坏的风险不亚于由物理机组成的网络。即使虚拟机网络已与任何物理网络隔离，虚拟机也可能遭到网络中其他虚拟机的攻击。用于确保虚拟机安全的要求通常与确保物理机安全的要求相同。

虚拟机是相互独立的。一个虚拟机无法读取或写入另一个虚拟机的内存、访问其数据、使用其应用程序等等。但在网络中，任何虚拟机或虚拟机组仍可能遭到其他虚拟机的未授权访问，因此可能需要通过外部手段加强保护。

使用防火墙确保网络安全

安全管理员使用防火墙保护网络或网络中的选定组件免遭侵袭。

防火墙可控制对其保护范围内的设备的访问，方法是关闭除管理员显式或隐式指定的授权端口之外的所有端口。管理员打开的端口允许防火墙内外设备间的流量。

重要事项 ESXi 5.5 及更高版本中的 ESXi 防火墙不允许按网络筛选 vMotion 流量。因此，必须在外部防火墙上安装规则，才能确保 vMotion 套接字没有入站连接。

在虚拟机环境中，可以为组件之间的防火墙规划布局。

- 物理机（例如，vCenter Server 系统）和 ESXi 主机之间的防火墙。
- 一个虚拟机与另一个虚拟机之间的防火墙（例如，在作为外部 Web 服务器的虚拟机与连接到公司内部网络的虚拟机之间）。
- 物理机与虚拟机之间的防火墙（例如，在物理网络适配器卡和虚拟机之间设立防火墙）。

防火墙在 ESXi 配置中的使用方式取决于您计划如何使用网络以及给定的组件所需的安全性。例如，如果在您创建的虚拟网络中的每个虚拟机专用于运行同一部门的不同基准测试套件，那么从一个虚拟机对另一个虚拟机进行不利访问的风险极小。因此，防火墙存在于虚拟机之间的配置不是必需的。但是，为了防止干扰外部主机的测试运行，可在虚拟网络的入口点配置防火墙来保护整组虚拟机。

有关防火墙端口图，请参见 VMware 知识库文章 [2131180](#)。

针对有 vCenter Server 的配置设立防火墙

如果要通过 vCenter Server 访问 ESXi 主机，则通常会使用防火墙保护 vCenter Server。该防火墙可为网络提供基本保护。

防火墙可能位于客户端和 vCenter Server 之间。或者，根据您的部署情况，vCenter Server 和客户端可能均受防火墙保护。重点是确保在您认为的系统入口点有防火墙。

有关 TCP 和 UDP 端口的完整列表，包括用于 vSphere vMotion™ 和 vSphere Fault Tolerance 的端口，请参见 [vCenter Server TCP 和 UDP 端口](#)。

配置有 vCenter Server 的网络可以通过 vSphere Web Client 或第三方网络管理客户端接收通信，这些客户端使用 SDK 与主机相连接。在正常操作期间，vCenter Server 会在指定的端口上侦听其受管主机和客户端的数据。vCenter Server 还假设其受管主机会在指定的端口上侦听 vCenter Server 的数据。如果任何这些元素之间有防火墙，必须确保防火墙中有打开的端口以支持数据传输。

视您计划如何使用网络及各种设备所需安全级别而定，可能还需要在网络中的许多其他访问点设立防火墙。根据为网络配置确定的安全风险选择防火墙位置。下面列出了 ESXi 实施中常用的防火墙位置。

- vSphere Web Client 或第三方网络管理客户端与 vCenter Server 之间。
- Web 浏览器与 ESXi 主机之间（如果用户通过 Web 浏览器访问虚拟机）。
- vSphere Web Client 与 ESXi 主机之间（如果用户通过 vSphere Web Client 访问虚拟机）。此连接是 vSphere Web Client 与 vCenter Server 之间连接的补充，它需要一个不同的端口。
- vCenter Server 与 ESXi 主机之间。
- 网络中的 ESXi 主机之间。尽管主机之间的流量通常被认为是可信的，但是，如果您关注计算机的安全漏洞，可在主机间添加防火墙。

如果在 ESXi 主机间添加防火墙并打算在服务器间迁移虚拟机、执行克隆操作或使用 vMotion，还必须在用来将源主机和目标主机隔开的防火墙中打开端口，以便源主机与目标主机进行通信。

- ESXi 主机和网络存储器（例如 NFS 或 iSCSI 存储器）之间。这些端口并非专用于 VMware，您可以根据网络规范进行配置。

通过防火墙连接到 vCenter Server

vCenter Server 使用 TCP 端口 443 侦听其客户端的数据传输。如果 vCenter Server 及其客户端之间设有防火墙，则必须配置一个可供 vCenter Server 接收其客户端数据的连接。

在防火墙中打开 TCP 端口 443 以允许 vCenter Server 从 vSphere Web Client 接收数据。防火墙配置取决于您的站点所用策略，有关信息，请咨询您本地的防火墙系统管理员。

如果不希望将端口 443 用作 vSphere Web Client 与 vCenter Server 通信的端口，则可以通过在 vSphere Web Client 中更改 vCenter Server 设置来切换到其他端口。请参见《vCenter Server 和主机管理》文档。

如果仍然使用 vSphere Client，请参见《使用 vSphere Client 管理 vSphere》文档。

针对没有 vCenter Server 的配置设立防火墙

可以将客户端直接连接到 ESXi 网络，而不使用 vCenter Server。

如果未配置 vCenter Server，网络会通过 vSphere Client、任一 vSphere 命令行界面、vSphere Web Services SDK 或第三方客户端来接收通信。在多数情况下，其防火墙需求会与配置有 vCenter Server 的情况基本相同，但有几个重要区别。

- 与包含 vCenter Server 的配置一样，应确保有防火墙保护 ESXi 层，或保护客户端及 ESXi 层，具体取决于您的配置。该防火墙可为网络提供基本保护。
- 此类配置中的许可证是您在每个主机上安装的 ESXi 包的一部分。由于许可功能驻留在服务器上，因此不需要单独的许可证服务器。这就免除了在许可证服务器与 ESXi 网络间设立防火墙的需要。

可以使用 ESXCLI、vSphere Client 或防火墙规则配置防火墙端口。请参见 [ESXi 防火墙配置](#)。

通过防火墙连接 ESXi 主机

如果在两台 ESXi 主机间设有防火墙，并希望允许主机间的事务或使用 vCenter Server 执行任何源或目标活动（例如 vSphere High Availability (vSphere HA) 通信、迁移、克隆或 vMotion），则必须配置一个可供受管主机接收数据的连接。

要配置用于接收数据的连接，请打开用于 vSphere High Availability、vMotion、vSphere Fault Tolerance 等服务的通信的端口。有关配置文件、vSphere Web Client 访问权限以及防火墙命令的讨论，请参见 [ESXi 防火墙配置](#)。有关端口列表，请参见 [ESXi 主机的入站和出站防火墙端口](#)。有关配置端口的其他信息，请咨询防火墙系统管理员。

通过防火墙连接到虚拟机控制台

必须打开某些端口，供用户和管理员与虚拟机控制台进行通信。必须打开的端口取决于虚拟机控制台的类型，以及是要通过 vCenter Server 使用 vSphere Web Client 进行连接还是从 vSphere Client 直接连接到 ESXi 主机。

通过 vSphere Web Client 连接到基于浏览器的虚拟机控制台

使用 vSphere Web Client 进行连接时，您始终连接到用于管理 ESXi 主机的 vCenter Server 系统，并从该处访问虚拟机控制台。

如果使用 vSphere Web Client 连接到基于浏览器的虚拟机控制台，则必须允许进行以下访问：

- 防火墙必须允许 vSphere Web Client 访问端口 9443 上的 vCenter Server。
- 防火墙必须允许 vCenter Server 访问端口 902 上的 ESXi 主机。

通过 vSphere Web Client 连接到独立虚拟机控制台

如果使用 vSphere Web Client 连接到独立虚拟机控制台，则必须允许进行以下访问：

- 防火墙必须允许 vSphere Web Client 访问端口 9443 上的 vCenter Server。
- 防火墙必须允许独立虚拟机控制台访问端口 9443 上的 vCenter Server 和端口 902 上的 ESXi 主机。

使用 vSphere Client 直接连接到 ESXi 主机

如果直接连接到 ESXi 主机，则可以使用 vSphere Client 虚拟机控制台。

注 不要使用 vSphere Client 直接连接到由 vCenter Server 系统管理的主机。如果从 vSphere Client 对这些主机进行更改，则会导致环境不稳定。

防火墙必须允许访问端口 443 和 902 上的 ESXi 主机

vSphere Client 使用端口 902 为虚拟机上的客户机操作系统 MKS 活动提供连接。用户正是通过此端口与虚拟机的客户机操作系统及应用程序交互。VMware 不支持为此功能配置不同端口。

确保物理交换机安全

确保每个 ESXi 主机上物理交换机的安全，以防止攻击者获取对主机及其虚拟机的访问权限。

为了最好地保护主机，请确保物理交换机端口已配置为禁用跨树，并确保为外部物理交换机和虚拟交换机标记 (VST) 模式下的虚拟机之间的中继链接配置了非协商选项。

步骤

- 1 登录物理交换机并确保禁用了跨树协议，或确保为连接 ESXi 主机的所有物理交换机端口配置了 Port Fast。
- 2 对于执行桥接或路由的虚拟机，定期检查第一个上游物理交换机端口是否配置为禁用 BPDU Guard 和 Port Fast，但启用跨树协议。
在 vSphere 5.1 及更高版本中，为了防止物理交换机受到潜在的拒绝服务 (DoS) 攻击，可以在 ESXi 主机上启动客户机 BPDU 筛选器。
- 3 登录物理交换机并确保连接 ESXi 主机的物理交换机端口上未启用动态中继协议 (DTP)。
- 4 如果物理交换机端口连接虚拟交换机 VLAN 中继端口，则定期检查物理交换机端口以确保它们被正确配置为中继端口。

使用安全策略确保标准交换机端口安全

就物理网络适配器而言，虚拟机网络适配器可以发送可能来自不同计算机的帧，或者模拟另一台计算机，以便能够接收针对该计算机的网络帧。同样，与物理网络适配器相同，可以对虚拟机网络适配器进行配置，以便其可以接收针对其他计算机的帧。这两种情形都具有一定的安全风险。

为网络创建标准交换机时，将在 vSphere Web Client 中添加端口组，以便为附加到该交换机上的虚拟机和 VMkernel 适配器强制执行系统流量策略。

在为标准交换机添加 VMkernel 端口组或虚拟机端口组的过程中，ESXi 会为组中的端口配置安全策略。可以使用此安全策略确保主机能防止其虚拟机的客户机操作系统模拟网络中的其他计算机。实施此安全功能的目的在于使负责模拟的客户机操作系统检测不到模拟行为已被阻止。

安全策略决定您对虚拟机执行的防模拟和截断攻击保护的强度。为了正确使用安全配置文件中的设置，必须了解虚拟机网络适配器如何控制传送及此级别的攻击如何进行。请参见《vSphere 网络连接》出版物中的“安全策略”部分。

确保 vSphere 标准交换机的安全

可以通过使用交换机的安全设置限制一些 MAC 地址模式来保护标准交换机流量不受第 2 层的攻击。

每个虚拟机网络适配器均包含一个初始 MAC 地址和一个有效 MAC 地址。

初始 MAC 地址

创建适配器时将分配初始 MAC 地址。尽管可以从客户机操作系统外部重新配置初始 MAC 地址，但不能由客户机操作系统进行更改。

有效 MAC 地址

每个适配器均具有一个有效 MAC 地址，可筛选与该有效 MAC 地址不同的目标 MAC 地址的进站网络流量。客户机操作系统负责设置有效 MAC 地址，并通常将有效 MAC 地址与初始 MAC 地址保持一致。

虚拟机网络适配器一经创建后，其有效 MAC 地址与初始 MAC 地址相同。客户机操作系统可随时将有效 MAC 地址更改为其他值。如果操作系统更改了有效 MAC 地址，其网络适配器将接收传至新 MAC 地址的网络流量。

通过网络适配器发送数据包时，客户机操作系统通常将其适配器的有效 MAC 地址输入以太网帧的源 MAC 地址字段中。它还将接收网络适配器的 MAC 地址输入目标 MAC 地址字段中。接收网络适配器仅在数据包中的目标 MAC 地址与其自身有效的 MAC 地址匹配时才接受数据包。

操作系统可发送带有模拟源 MAC 地址的帧。这意味着操作系统便可通过模拟接收网络授权的网络适配器对网络中的设备进行恶意攻击。

通过在端口组或端口上配置安全策略，保护虚拟流量免受模拟和第 2 层拦截攻击。

分布式端口组和端口上的安全策略包括以下选项：

- 混杂模式（请参见[混杂模式运行](#)）
- MAC 地址更改（请参见[MAC 地址更改](#)）
- 伪信号（请参见[伪传输](#)）

您可以通过从 vSphere Web Client 选择与主机关联的虚拟交换机来查看和更改默认设置。请参见《vSphere 网络连接》文档。

MAC 地址更改

虚拟交换机的安全策略包括一个 **MAC 地址更改** 选项。此选项影响虚拟机接收的流量。

当 **Mac 地址更改** 选项设置为 **接受** 时，ESXi 接受将有效 MAC 地址更改为非初始 MAC 地址的其他地址的请求。

当 **Mac 地址更改** 选项设置为 **拒绝** 时，ESXi 不接受将有效 MAC 地址更改为非初始 MAC 地址的其他地址的请求。此选项可保护主机免受 MAC 模拟的威胁。虚拟机适配器用于发送请求的端口将被禁用，必须在有效 MAC 地址与初始 MAC 地址匹配后虚拟机适配器才能再接收帧。客户机操作系统检测不到 MAC 地址更改请求已被拒绝。

注 iSCSI 启动器依赖于能够从某些类型的存储器获取 MAC 地址更改。如果将 ESXi iSCSI 与 iSCSI 存储器一起使用，则将 **MAC 地址更改** 选项设置为 **接受**。

有时您可能确实需要多个适配器在网络中使用同一 MAC 地址（例如在单播模式中使用 Microsoft 网络负载均衡时）。在标准多播模式下使用 Microsoft 网络负载均衡时，适配器不能共享 MAC 地址。

伪传输

伪信号 选项将影响从虚拟机传输的流量。

当 **伪信号** 选项设置为 **接受** 时，ESXi 不会比较源 MAC 地址和有效 MAC 地址。

要防止 MAC 模拟，可将 **伪信号** 选项设置为 **拒绝**。这样，主机将对客户机操作系统传输的源 MAC 地址与其虚拟机适配器的有效 MAC 地址进行比较，以确认是否匹配。如果地址不匹配，ESXi 主机将丢弃数据包。

客户机操作系统检测不到其虚拟机适配器无法使用模拟 MAC 地址发送数据包。ESXi 主机会在带有模拟地址的任何数据包递送之前将其截断，而客户机操作系统可能假设数据包已被丢弃。

混杂模式运行

混杂模式会清除虚拟机适配器执行的任何接收筛选，以便客户机操作系统接收在网络上观察到的所有流量。默认情况下，虚拟机适配器不能在混杂模式中运行。

尽管混杂模式对于跟踪网络活动很有用，但它是一种不安全的运行模式，因为混杂模式中的任何适配器均可访问数据包，即使某些数据包是否仅由特定的网络适配器接收也是如此。这意味着虚拟机中的管理员或根用户可以查看发往其他客户机或主机操作系统的流量。

注 有时您可能确实需要将标准虚拟交换机或分布式虚拟交换机配置为在混杂模式中运行（例如运行网络入侵检测软件或数据包嗅探器时）。

确保 vSphere Distributed Switch 和分布式端口组的安全

管理员可选择多种方式来确保其 vSphere 环境中的 vSphere Distributed Switch 安全。

步骤

- 1 对于具有静态绑定的分布式端口组，验证已禁用了自动扩展功能。

默认情况下，自动扩展在 vSphere 5.1 及更高版本中处于启用状态。

要禁用自动扩展，请使用 vSphere Web Services SDK 或命令行界面配置分布式端口组下的 `autoExpand` 属性。请参见《vSphere Web Services SDK》文档。

- 2 确保已完整记录所有 vSphere Distributed Switch 的全部专用 VLAN ID。
- 3 如果您在 dvPortgroup 上使用 VLAN 标记，则 VLAN ID 必须与外部可识别 VLAN 的上游交换机上的 ID 相对应。如果未完整跟踪 VLAN ID，错误地重用 ID 可能会使不适当的物理机和虚拟机之间产生流量。同样，VLAN ID 错误或缺失可能导致无法在物理机和虚拟机之间传递流量。
- 4 确保与 vSphere Distributed Switch 关联的虚拟端口组上不存在任何未使用的端口。
- 5 标记所有 vSphere Distributed Switch。

与 ESXi 主机关联的 vSphere Distributed Switch 需要交换机名称字段。此标签可以充当交换机的功能描述符，就像与物理交换机关联的主机名称一样。vSphere Distributed Switch 上的标签表示交换机的功能或 IP 子网。例如，可以将交换机标记为内部交换机，以表示该交换机仅用于虚拟机的专用虚拟交换机之间的内部网络，并且未绑定任何物理网络适配器。

- 6 如果当前未使用 vSphere Distributed Switch 的网络健康检查功能，请禁用该功能。

默认情况下，网络健康检查功能处于禁用状态。启用后，健康检查包将包含有关攻击者可能使用的主机、交换机和端口的信息。网络健康检查功能仅用于故障排除，完成故障排除后应将其关闭。

- 7 通过在端口组或端口上配置安全策略，保护虚拟流量免受模拟和第 2 层拦截攻击。

分布式端口组和端口上的安全策略包括以下选项：

- 混杂模式（请参见[混杂模式运行](#)）
- MAC 地址更改（请参见[MAC 地址更改](#)）
- 伪信号（请参见[伪传输](#)）

您可以查看和更改当前设置，方法是从 Distributed Switch 的右键菜单中选择**管理分布式端口组**，然后在向导中选择**安全性**。请参见《vSphere 网络连接》文档。

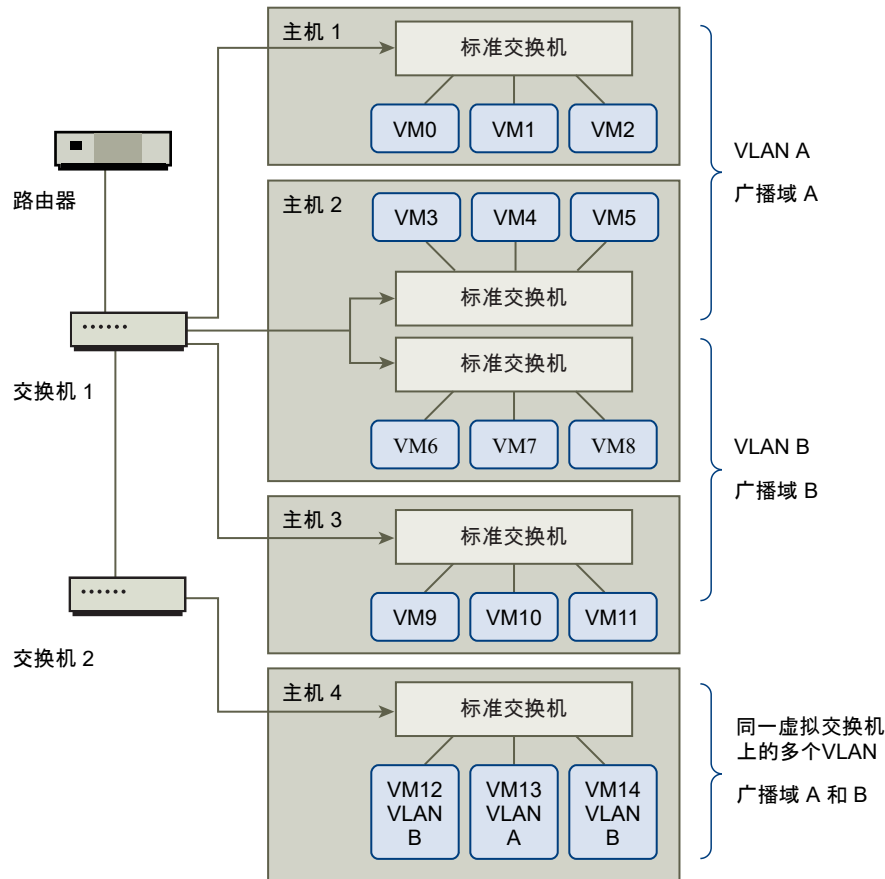
通过 VLAN 确保虚拟机安全

网络可能是任何系统中最脆弱的环节之一。虚拟机网络需要的保护丝毫不应少于物理网络。使用 VLAN 可以提高您的环境的网络安全性。

VLAN 是一种 IEEE 标准的网络方案，通过特定的标记方法将数据包的传送限制在 VLAN 中的端口内。若配置正确，VLAN 将是您保护一组虚拟机免遭意外或恶意侵袭的可靠方法。

VLAN 可让您对物理网络进行分段，以便只有属于相同 VLAN 的网络中的两个虚拟机才能相互传输数据包。例如，会计记录和会计帐务是一家公司最敏感的内部信息。如果公司的销售、货运和会计员工均使用同一物理网络中的虚拟机，可设置 VLAN 以保护会计部门的虚拟机。

图 8-1. VLAN 布局示例



在此配置中，会计部门的所有员工均使用 VLAN A 中的虚拟机，销售部门的员工使用 VLAN B 中的虚拟机。

路由器将包含会计数据的数据包转发至交换机。这些数据包将被标记为仅分发至 VLAN A。因此，数据将被局限在广播域 A 内，无法传送到广播域 B，除非对路由器进行此配置。

该 VLAN 配置可防止销售人员截取传至会计部门的数据包。还可防止会计部门接收传至销售组的数据包。一个虚拟交换机可为不同 VLAN 中的虚拟机服务。

VLAN 安全注意事项

如何设置 VLAN 以确保网络组件安全取决于客户机操作系统以及网络设备的配置方式。

ESXi 配备完整的符合 IEEE 802.1q 的 VLAN 实施。VMware 不能对如何设置 VLAN 提出具体建议，但当您使用 VLAN 部署作为安全执行策略一部分时，应考虑以下因素。

确保 VLAN 安全

管理员可使用几个选项确保其 vSphere 环境中 VLAN 的安全。

步骤

- 1 确保端口组未配置为上游物理交换机预留的 VLAN 值

请勿使用为物理交换机预留的值设置 VLAN ID。

- 2 确保端口组未配置为 VLAN 4095，除非用于虚拟客户机标记 (VGT)。

vSphere 中存在三种 VLAN 标记类型：

- 外部交换机标记 (EST)
- 虚拟交换机标记 (VST) - 虚拟交换机使用已配置的 VLAN ID 标记传入附加虚拟机的流量，并将 VLAN 标记从传出虚拟机的流量中移除。要设置 VST 模式，请分配 1 到 4095 之间的 VLAN ID。
- 虚拟客户机标记 (VGT) - 虚拟机处理 VLAN 流量。要激活 VGT 模式，请将 VLAN ID 设置为 4095。在 Distributed Switch 上，还可以使用 **VLAN 中继** 选项允许基于 VLAN 的虚拟机流量。

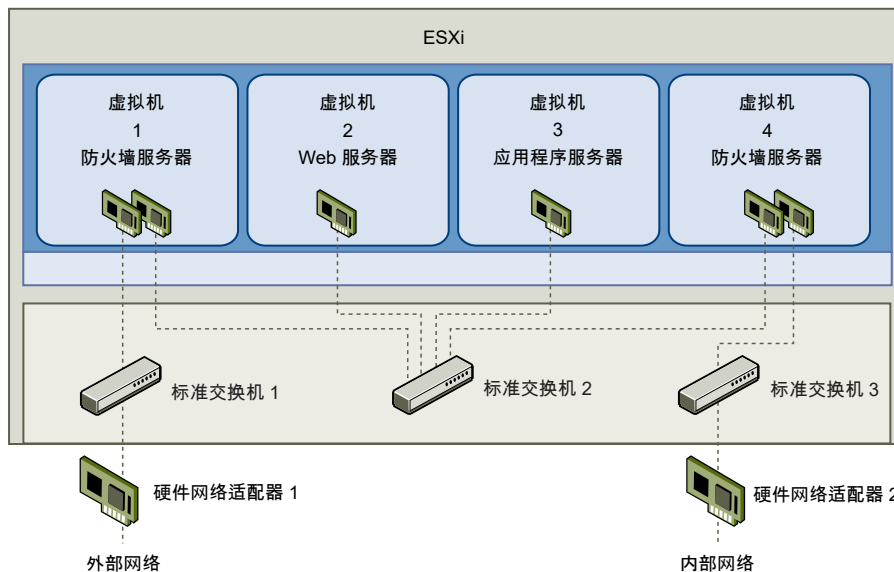
在标准交换机上，可以在交换机或端口组级别上配置 VLAN 网络连接模式，而在 Distributed Switch 上，则在分布式端口组或端口级别。

- 3 确保完全记录了每台虚拟交换机上的所有 VLAN，而且每台虚拟交换机有且仅有所需的 VLAN。

在单台 ESXi 主机上创建网络 DMZ

在单台主机上创建网络隔离区 (DMZ) 是使用 ESXi 隔离和虚拟网络功能配置安全环境的一个示例。

图 8-2. 在单台 ESXi 主机上配置的 DMZ



在此示例中，将四个虚拟机配置为在标准交换机 2 上创建虚拟 DMZ：

- 虚拟机 1 和虚拟机 4 运行防火墙，并通过标准交换机连接到物理网络适配器。这两个虚拟机均使用多个交换机。
- 虚拟机 2 运行 Web 服务器，同时虚拟机 3 作为应用程序服务器运行。这两个虚拟机均连接到一个虚拟交换机。

Web 服务器和应用程序服务器占用两个防火墙之间的 DMZ。这两个元素之间的媒介是用来连接防火墙和服务器的标准交换机 2。此交换机未与 DMZ 之外的任何元素进行直接连接，且通过两个防火墙与外部流量相隔离。

从运行角度来看，外部流量通过硬件网络适配器 1（由标准交换机 1 路由）从 Internet 进入虚拟机 1，并由此虚拟机上安装的防火墙进行验证。如果经防火墙授权，流量可路由至 DMZ 中的标准交换机，即标准交换机 2。由于 Web 服务器和应用程序服务器也连接至此交换机，因此，它们可以满足外部请求。

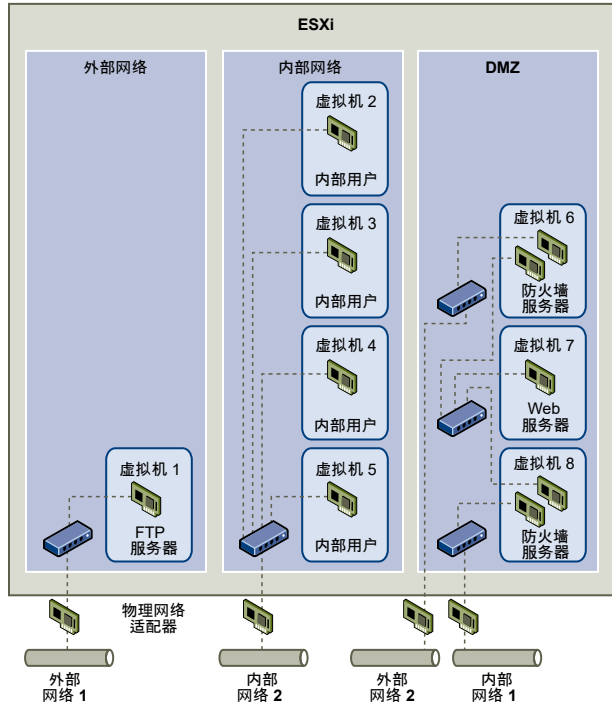
标准交换机 2 还与虚拟机 4 相连。此虚拟机在 DMZ 和内部企业网络之间提供防火墙。此防火墙对来自 Web 服务器和应用程序服务器的数据包进行筛选。验证后的数据包将通过标准交换机 3 路由至硬件网络适配器 2。硬件网络适配器 2 与内部企业网络相连。

在单台主机上创建 DMZ 时，可使用相当轻量的防火墙。尽管此配置中的虚拟机无法直接控制其他虚拟机或访问其内存，但是所有虚拟机仍然通过虚拟网络处于连接状态。此网络可能会传播病毒，或成为其他类型攻击的对象。DMZ 中虚拟机的安全性等同于连接到同一网络的独立物理机。

在单台 ESXi 主机中创建多个网络

ESXi 系统的设计可让您将一些虚拟机组连接至内部网络，并将一些虚拟机组连接至外部网络，而将另一些虚拟机组同时连接至外部和内部网络，而这一切都在同一主机上进行。此功能是由对虚拟机的基本隔离和对虚拟网络连接功能的有计划使用组合而成的。

图 8-3. 单台 ESXi 主机上配置的外部网络、内部网络和 DMZ



在图中，系统管理员将主机配置到三个不同的虚拟机区域中：FTP 服务器、内部虚拟机和 DMZ。每个区域均提供唯一功能。

FTP 服务器

虚拟机 1 是使用 FTP 软件配置的，可作为从外部资源（例如，由供应商本地化的表单和辅助材料）发出及向其发送的数据的存储区域。

此虚拟机仅与外部网络相关联。它自身拥有可用来与外部网络 1 相连接的虚拟交换机和物理网络适配器。此网络专用于公司在从外部来源接收数据时所使用的服务器。例如，公司使用外部网络 1 从供应商接收 FTP 流量，并允许供应商通过 FTP 访问存储在外部可用服务器上的数据。除了服务于虚拟机 1，外部网络 1 也服务于在整个站点内不同 ESXi 主机上配置的 FTP 服务器。

由于虚拟机 1 不与主机中的任何虚拟机共享虚拟交换机或物理网络适配器，因此，其他驻留的虚拟机无法通过虚拟机 1 网络收发数据包。此限制可防止嗅探攻击（嗅探攻击需向受害者发送网络流量）。更为重要的是，攻击者再也无法使用 FTP 固有的漏洞来访问任何主机的其他虚拟机。

内部虚拟机

虚拟机 2 至 5 仅供内部使用。这些虚拟机用来处理和存储公司机密数据（例如，医疗记录、法律裁决和欺诈调查）。因此，系统管理员必须确保为这些虚拟机提供最高级别的保护。

这些虚拟机通过其自身的虚拟交换机和网络适配器连接到内部网络 2。内部网络 2 仅供内部人员使用（例如，索赔专员、内部律师或调解员）。

虚拟机 2 至 5 可通过虚拟交换机与另一个虚拟机进行通信，也可通过物理网络适配器与内部网络 2 上其他位置的内部虚拟机进行通信。它们不能与对外计算机进行通信。如同 FTP 服务器一样，这些虚拟机不能通过其他虚拟机网络收发数据包。同样，主机的其他虚拟机不能通过虚拟机 2 至 5 收发数据包。

DMZ

虚拟机 6 至 8 配置为可供营销小组用于发布公司外部网站的 DMZ。

这组虚拟机与外部网络 2 和内部网络 1 相关联。公司使用外部网络 2 来支持营销部门和财务部门用来托管公司网站的 Web 服务器及公司为外部用户托管的其他 Web 设施。内部网络 1 是营销部门用于向公司网站发布内容、张贴下载内容及维护服务（例如，用户论坛）的媒介。

由于这些网络与外部网络 1 和内部网络 2 相隔离，因此虚拟机无任何共享联络点（交换机或适配器），FTP 服务器或内部虚拟机组也不存在任何攻击风险。

通过利用虚拟机隔离、正确配置虚拟交换机及维护网络独立，系统管理员可在同一 ESXi 主机上容纳所有三个虚拟机区域，并完全不用担心数据或资源流失。

公司使用多个内部和外部网络，并确保每组的虚拟交换机和物理网络适配器与其他组的虚拟交换机和物理网络适配器完全独立，从而在虚拟机组中强制实施隔离。

由于没有任何虚拟交换机横跨虚拟机区域，因此系统管理员可成功地消除虚拟机区域之间的数据包泄漏风险。虚拟机本身无法向另一个虚拟交换机直接泄漏数据包。仅在以下情况下，数据包才会在虚拟交换机之间移动：

- 这些虚拟交换机连接到同一物理 LAN。
- 这些虚拟交换机连接到可用于传输数据包的公用虚拟机。

这些条件均未出现在样本配置中。如果系统管理员要确认不存在公用虚拟交换路径，则可通过在 vSphere Web Client 中查看网络交换机布局，以检查是否可能存在共享联系点。

为了保护虚拟机的资源，系统管理员为每台虚拟机配置了资源预留和限制，从而降低了 DoS 和 DDoS 攻击的风险。系统管理员在 DMZ 的前后端安装了软件防火墙，确保主机受到物理防火墙的保护，并配置了联网的存储器资源以使每个资源均有自己的虚拟交换机，从而为 ESXi 主机和虚拟机提供了进一步保护。

Internet 协议安全

Internet 协议安全 (IPsec) 用于确保进出主机的 IP 通信安全。ESXi 主机支持使用 IPv6 的 IPsec。

在主机上设置 IPsec 时，可对入站和出站数据包启用身份验证和加密。对 IP 流量进行加密的时间和方式取决于如何设置系统的安全关联和安全策略。

安全关联确定系统对流量进行加密的方式。在创建安全关联时，可指定安全关联的源和目标、加密参数以及名称。

安全策略确定系统应对流量进行加密的时间。安全策略包括源和目标信息、要加密的流量的协议和方向、模式（transport 或 tunnel）以及要使用的安全关联。

列出可用的安全关联

ESXi 可提供可供安全策略使用的所有安全关联的列表。该列表包含用户创建的安全关联，以及 VMkernel 使用 Internet 密钥交换安装的任何安全关联。

可以使用 `esxcli vSphere CLI` 命令获取可用安全关联的列表。

步骤

- ◆ 在命令提示符下，输入命令 **`esxcli network ip ipsec sa list`**。

结果

ESXi 将显示所有可用安全关联的列表。

添加 IPsec 安全关联

添加安全关联以指定关联的 IP 流量的加密参数。

可以使用 `esxcli vSphere CLI` 命令添加安全关联。

步骤

- ◆ 在命令提示符下输入命令 **`esxcli network ip ipsec sa add`** 并使用下列一个或多个选项。

选项	描述
<code>--sa-source=</code> <i>源地址</i>	必需。指定源地址。
<code>--sa-destination=</code> <i>目标地址</i>	必需。指定目标地址。
<code>--sa-mode=</code> <i>模式</i>	必需。指定模式 <code>transport</code> 或 <code>tunnel</code> 。
<code>--sa-spi=</code> <i>安全参数索引</i>	必需。指定安全参数索引。安全参数索引标识与主机的安全关联。它必须是一个十六进制数并带有 <code>0x</code> 前缀。所创建的每个安全关联都必须具有协议和安全参数索引的唯一组合。
<code>--encryption-algorithm=</code> <i>加密算法</i>	必需。使用以下参数之一指定加密算法。 <ul style="list-style-type: none"> ■ <code>3des-cbc</code> ■ <code>aes128-cbc</code> ■ <code>null</code>（不提供任何加密）
<code>--encryption-key=</code> <i>加密密钥</i>	在指定加密算法时为必填项。指定加密密钥。可以使用 <code>0x</code> 前缀输入 ASCII 文本或十六进制形式的密钥。
<code>--integrity-algorithm=</code> <i>身份验证算法</i>	必需。指定身份验证算法 <code>hmac-sha1</code> 或 <code>hmac-sha2-256</code> 。
<code>--integrity-key=</code> <i>身份验证密钥</i>	必需。指定身份验证密钥。可以使用 <code>0x</code> 前缀输入 ASCII 文本或十六进制形式的密钥。
<code>--sa-name=</code> <i>名称</i>	必需。提供一个安全关联名称。

示例：新安全关联命令

为了方便阅读，下面的示例包含额外的换行符。

```
esxcli network ip ipsec sa add
--sa-source 3ffe:501:ffff:0::a
--sa-destination 3ffe:501:ffff:0001:0000:0000:0000:0001
--sa-mode transport
--sa-spi 0x1000
--encryption-algorithm 3des-cbc
--encryption-key 0x6970763672656164796c6f676f336465736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x6970763672656164796c6f67736861316f757432
--sa-name sal
```

移除 IPsec 安全关联

可以使用 ESXCLI vSphere CLI 命令移除安全关联。

前提条件

验证要使用的安全关联当前未在使用中。如果尝试移除正在使用中的安全关联，则移除操作将失败。

步骤

- ◆ 在命令提示符下，输入命令 **esxcli network ip ipsec sa remove --sa-name 安全关联名称**

列出可用的 IPsec 安全策略

可以使用 ESXCLI vSphere CLI 命令列出可用的安全策略。

步骤

- ◆ 在命令提示符下，输入命令 **esxcli network ip ipsec sp list**。

结果

主机将显示所有可用安全策略的列表。

创建 IPsec 安全策略

创建安全策略可以确定何时使用在安全关联中设置的身份验证和加密参数。可以使用 ESXCLI vSphere CLI 命令添加安全策略。

前提条件

在创建安全策略之前，可按[添加 IPsec 安全关联](#)中所述，添加具有相应身份验证和加密参数的安全关联。

步骤

- ◆ 在命令提示符下输入命令 **esxcli network ip ipsec sp add** 并使用下列一个或多个选项。

选项	描述
--sp-source= 源地址	必需。指定源 IP 地址和前缀长度。
--sp-destination= 目标地址	必需。指定目标地址和前缀长度。
--source-port= 端口	必需。指定源端口。源端口号必须是介于 0 和 65535 之间的一个数字。
--destination-port= 端口	必需。指定目标端口。源端口号必须是介于 0 和 65535 之间的一个数字。
--upper-layer-protocol= 协议	使用以下参数之一指定上层协议。 <ul style="list-style-type: none"> ■ tcp ■ udp ■ icmp6 ■ 任意
--flow-direction= 方向	使用 in 或 out 指定要监控流量的方向。
--action= 操作	使用以下参数之一指定在遇到具有指定参数的流量时要采取的操作。 <ul style="list-style-type: none"> ■ none: 不采取任何操作。 ■ discard: 不允许数据进出。 ■ ipsec: 使用安全关联中提供的身份验证和加密信息来确定数据是否来自受信任的源。
--sp-mode= 模式	指定模式 tunnel 或 transport。
--sa-name= 安全关联名称	必需。为要使用的安全策略提供安全关联名称。
--sp-name= 名称	必需。请提供一个安全策略名称。

示例：新安全策略命令

为了方便阅读，下面的示例包含额外的换行符。

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sal
--sp-name=sp1
```

移除 IPsec 安全策略

可以使用 ESXCLI vSphere CLI 命令移除 ESXi 主机中的安全策略。

前提条件

验证要使用的安全策略当前未在使用中。如果尝试移除正在使用中的安全策略，则移除操作将失败。

步骤

- ◆ 在命令提示符下，输入命令

```
esxcli network ip ipsec sp remove --sa-name 安全策略名称。
```

要移除所有安全策略，请输入命令 **esxcli network ip ipsec sp remove --remove-all**。

确保 SNMP 配置正确

如果未正确配置 SNMP，则监控信息可能会被发送到恶意主机。然后恶意主机可能会使用此信息计划实施攻击。

步骤

- 1 运行 **esxcli system snmp get** 确定当前是否使用 SNMP。
- 2 如果您的系统确实需要 SNMP，请运行 **esxcli system snmp set --enable true** 命令确保它正在运行。
- 3 如果您的系统使用 SNMP，请参见监控和性能出版物了解 SNMP 3 的安装信息。
必须在每台 ESXi 主机上配置 SNMP。可以使用 vCLI、PowerCLI 或 vSphere Web Services SDK 进行配置。

仅在需要时才在 vSphere Network Appliance API 中使用虚拟交换机

如果您未使用运用 vSphere Network Appliance API (DvFilter) 的产品，请勿将主机配置为向虚拟机发送网络信息。如果 vSphere Network Appliance API 处于启用状态，则攻击者可能会尝试将虚拟机连接到筛选器。此连接可能会提供对主机上其他虚拟机网络的访问。

如果您正在使用运用此 API 的产品，请验证是否已正确配置主机。请参见《开发和部署 vSphere 解决方案、vService 和 ESX 代理》中有关 DvFilter 的部分。如果您的主机设置为使用 API，请确保 `Net.DVFilterBindIpAddress` 参数的值与使用 API 的产品相匹配。

步骤

- 1 要确保 `Net.DVFilterBindIpAddress` 内核参数的值正确，请使用 vSphere Web Client 找到该参数。
 - a 选择主机，然后单击**管理**选项卡。
 - b 在“系统”下，选择**高级系统设置**。
 - c 向下滚动至 `Net.DVFilterBindIpAddress`，并验证该参数的值是否为空。
 参数并非严格按照字母顺序排列。在“筛选器”字段中键入 **DVFilter** 以显示所有相关的参数。
- 2 如果未使用 DvFilter 设置，请确保值为空。
- 3 如果使用 DvFilter 设置，请确保该参数的值与使用 DvFilter 的产品所使用的值相匹配。

vSphere 网络连接安全性最佳做法

遵循网络安全最佳做法有助于确保 vSphere 部署的完整性。

常规网络连接安全建议

遵循常规网络连接安全建议是确保网络环境安全的第一步。然后可以转到特殊区域，例如使用防火墙或使用 IPsec 确保网络安全。

- 如果启用跨树，请确保为物理交换机端口配置了 **Portfast**。由于 VMware 虚拟交换机不支持 STP，如果启用跨树，则连接到 ESXi 主机的物理交换机端口必须配置 **Portfast** 以避免物理交换机网络内出现循环。如果未设置 **Portfast**，则可能出现潜在性能和连接问题。
- 确保分布式虚拟交换机的 **Netflow** 流量仅发送至授权的收集器 IP 地址。**Netflow** 导出未加密且可能包含有关虚拟网络的信息，从而增加了中间人成功攻击的可能性。如果需要 **Netflow** 导出，请确保所有 **Netflow** 目标 IP 地址正确。
- 确保仅授权管理员可以使用基于角色的访问控制来访问虚拟网络连接组件。例如，虚拟机管理员应仅有权访问其虚拟机驻留的端口组。网络管理员应具有对所有虚拟网络连接组件的权限，但无权访问虚拟机。限制访问可降低意外或恶意配置错误的风险，并强制执行职责分离和最小特权的主要安全概念。
- 确保未将端口组配置为本机 VLAN 的值。物理交换机使用 **VLAN 1** 作为其本机 VLAN。本机 VLAN 上的帧不会标记为 1。ESXi 没有本机 VLAN。在端口组中指定了 VLAN 的帧具有标记，而在端口组中未指定 VLAN 的帧则没有标记。此配置可能会导致出现问题，因为标记为 1 的虚拟机最终会属于物理交换机的本机 VLAN。

例如，Cisco 物理交换机中 VLAN 1 上的帧没有标记，因为 VLAN 1 是该物理交换机上的本机 VLAN。但是，ESXi 主机上指定为 VLAN 1 的帧会标记为 1；因此，ESXi 主机上发往本机 VLAN 的流量无法正确路由，因为它标记为 1，而不是没有标记。物理交换机上来自本机 VLAN 的流量不可见，因为它没有标记。如果 ESXi 虚拟交换机端口组使用本机 VLAN ID，则从该端口发出的虚拟机流量对于该交换机上的本机 VLAN 不可见，因为该交换机应接收不带标记的流量。

- 确保未将端口组配置为上游物理交换机预留的 VLAN 值。物理交换机预留了某些 VLAN ID 以供内部使用，并且通常会禁止接收配置为这些值的流量。例如，Cisco Catalyst 交换机通常会预留 VLAN 1001 – 1024 和 4094。使用预留的 VLAN 可能会导致网络上出现拒绝服务问题。

- 确保未将端口组配置为 VLAN 4095（采用虚拟客户机标记 (VGT) 时除外）。将端口组设置为 VLAN 4095 会激活 VGT 模式。在此模式下，虚拟交换机会将所有网络帧传递给虚拟机，而不会修改 VLAN 标记，相反，它会将其留给虚拟机进行处理。
- 限制分布式虚拟交换机上的端口级配置替代。默认情况下，端口级配置替代处于禁用状态。如果启用了替代，则将允许虚拟机使用与端口组级设置不同的安全设置。某些虚拟机需要采用唯一配置，但必须进行监控。如果不对替代进行监控，则在虚拟机采用安全性较低的分布式虚拟交换机配置时，任何用户只要能够访问该虚拟机，就可能试图利用该访问权限漏洞。
- 确保分布式虚拟交换机端口镜像流量仅发送至授权的收集器端口或 VLAN。vSphere Distributed Switch 可以将流量从一个端口镜像至另一端口，以使数据包捕获设备可以收集特定的流量。端口镜像操作会将所有指定流量的副本以未加密格式发送。此镜像流量包含捕获的数据包中的全部数据，如果定向错误，可能会全面危及这些数据的安全。如果需要使用端口镜像功能，请确认所有端口镜像目标 VLAN、端口和上行链路 ID 都正确无误。

标记网络组件

标识网络架构的不同组件非常关键，有助于确保网络发展过程中不会引入错误。

遵循以下最佳实践：

- 确保端口组配置了明确的网络标签。这些标签可以作为端口组的功能描述符，帮助您在网络愈发复杂时标识每个端口组的功能。
- 确保每个 vSphere Distributed Switch 具有明确的网络标签，可指示交换机的功能或 IP 子网。此标签可以作为交换机的功能描述符，就像物理交换机需要主机名称一样。例如，您可以将交换机标记为内部，以表示此交换机用于内部网络。无法更改标准虚拟交换机的标签。

记录和检查 vSphere VLAN 环境

定期检查 VLAN 环境以避免解决问题。完整记录 VLAN 环境并确保 VLAN ID 仅使用一次。您的文档有助于进行故障排除，且在要扩展环境时至关重要。

步骤

1 确保已完整记录所有 vSwitch 和 VLANS ID

如果要在虚拟交换机上使用 VLAN 标记，则 ID 必须与外部可识别 VLAN 的上游交换机上的 ID 相对应。如果未完全跟踪 VLAN ID，则错误重用的 ID 可能允许错误物理机和虚拟机之间的流量。同样，如果 VLAN ID 错误或缺失，则在希望流量通过的物理机和虚拟机之间的流量可能被阻止。

2 确保已完整记录所有分布式虚拟端口组（dvPortgroup 实例）的 VLAN ID。

如果要在 dvPortgroup 上使用 VLAN 标记，则 ID 必须与外部可识别 VLAN 的上游交换机上的 ID 相对应。如果未完全跟踪 VLAN ID，则错误重用的 ID 可能允许错误物理机和虚拟机之间的流量。同样，如果 VLAN ID 错误或缺失，则在希望流量通过的物理机和虚拟机之间的流量可能被阻止。

3 确保已完整记录所有分布式虚拟交换机的专用 VLAN ID。

分布式虚拟交换机的专用 VLAN (PVLAN) 需要主 VLAN ID 和辅助 VLAN ID。这些 ID 必须与外部可识别 PVLAN 的上游交换机上的 ID 相对应。如果未完全跟踪 VLAN ID，则错误重用的 ID 可能允许错误物理机和虚拟机之间的流量。同样，如果 PVLAN ID 错误或缺失，则在希望流量通过的物理机和虚拟机之间的流量可能被阻止。

4 验证 VLAN 中继链接只连接到充当中继链接的物理交换机端口。

在将虚拟交换机连接到 VLAN 中继端口时，必须在上行链路端口上正确配置虚拟交换机和物理交换机。如果未正确配置物理交换机，具有 VLAN 802.1q 标头的帧将被转发到不该接收这些帧的交换机。

采用可靠的网络隔离做法

采用可靠的网络隔离做法可显著增强 vSphere 环境的网络安全性。

隔离管理网络

通过 vSphere 管理网络可以访问每个组件上的 vSphere 管理界面。在管理界面上运行的服务会让攻击者有机会获得系统的访问特权。远程攻击可能从获取对本网络的访问权限开始。如果攻击者获得了对管理网络的访问权限，则会为进一步入侵提供集结基础。

通过按 ESXi 主机或群集上运行的最安全虚拟机的安全级别保护管理网络，严格控制对管理网络的访问。无论以何种方式限制管理网络，管理员都必须能够访问此网络以配置 ESXi 主机和 vCenter Server 系统。

将 vSphere 管理端口组置于通用 vSwitch 上的专用 VLAN 中。只要 vSphere 管理端口组的 VLAN 未用于生产虚拟机，就可以与生产（虚拟机）流量共享 vSwitch。确认网络段未路由到其他网络，但如果网络中存在管理相关的其他实体（例如，与 vSphere Replication 一起使用时），则可以路由到该网络。尤其要注意的是，确保不可将生产虚拟机流量路由到此网络。

可通过以下方法之一严格控制对管理功能的访问。

- 对于特别敏感的环境，可配置受控网关或其他控制方法以访问管理网络。例如，要求管理员通过 VPN 连接到管理网络，且只允许受信任的管理员访问管理网络。
- 配置运行管理客户端的跳转盒。

隔离存储流量

请确保隔离基于 IP 的存储流量。基于 IP 的存储包括 iSCSI 和 NFS。虚拟机可能与基于 IP 的存储配置共享虚拟交换机和 VLAN。此类型的配置可能会向未经授权的虚拟机用户公开基于 IP 的存储流量。

基于 IP 的存储通常未加密，任何可以访问此网络的人均可对其进行查看。要限制未经授权的用户查看基于 IP 的存储流量，请采用逻辑方式将基于 IP 的存储网络流量与生产流量分隔开来。在与 VMkernel 管理网络分隔开来的 VLAN 或网络段上配置基于 IP 的存储适配器，以限制未经授权的用户查看该流量。

隔离 vMotion 流量

vMotion 迁移信息以纯文本形式传输。可以访问此信息流经的网络的任何人均可查看此信息。潜在的攻击者可能会拦截 vMotion 流量以获取虚拟机的内存内容。攻击者还可能筹划 MiTM 攻击以在迁移期间修改有关内容。

请在隔离的网络中将 VMotion 流量与生产流量分隔开来。请将网络设置为不可路由，即确保第 3 层路由器未跨越此网络和其他网络，以防止外部对网络进行访问。

VMotion 端口组应位于通用 vSwitch 上的专用 VLAN 中。只要 VMotion 端口组的 VLAN 未用于生产虚拟机，就可以与生产（虚拟机）流量共享 vSwitch。

涉及多个 vSphere 组件的最佳做法

9

一些安全性最佳做法（如在环境中设置 NTP）可影响多个 vSphere 组件。在配置环境时，请考虑这些建议。

请查看第 5 章 确保 ESXi 主机安全和第 7 章 确保虚拟机安全了解相关信息。

本章讨论了以下主题：

- 同步 vSphere 网络连接上的时钟
- 存储安全性最佳做法
- 验证是否已禁止向客户机发送主机性能数据
- 为 ESXi Shell 和 vSphere Web Client 设置超时

同步 vSphere 网络连接上的时钟

确保 vSphere 网络上所有组件的时钟均已同步。如果 vSphere 网络连接中计算机的时钟未同步，则在网络计算机相互通信时，可能会将对时间敏感的 SSL 证书视为无效。

未同步的时钟可能会导致身份验证问题，从而使安装失败或使 vCenter Server Appliance vpxd 服务无法启动。

请确保运行 vCenter 组件的任一 Windows 主机都与 NTP 服务器保持同步。请参见知识库文章 <http://kb.vmware.com/kb/1318>。

- 使 ESXi 时钟与网络时间服务器同步
在安装 vCenter Server 或部署 vCenter Server Appliance 之前，请确保 vSphere 网络连接中所有计算机的时钟均已同步。
- 在 vCenter Server Appliance 中配置时间同步设置
您可以在部署后更改 vCenter Server Appliance 中的时间同步设置。

使 ESXi 时钟与网络时间服务器同步

在安装 vCenter Server 或部署 vCenter Server Appliance 之前，请确保 vSphere 网络连接中所有计算机的时钟均已同步。

此任务将介绍如何从 vSphere Client 设置 NTP。您可以改用 `vicfg-ntp` vCLI 命令。请参见《vSphere 命令行界面参考》。

步骤

- 1 启动 vSphere Client，然后连接到 ESXi 主机。
- 2 在配置选项卡上，单击时间配置。
- 3 单击属性，然后单击选项。
- 4 选择 NTP 设置。
- 5 单击添加。
- 6 在“添加 NTP 服务器”对话框中，输入要与其同步的 NTP 服务器的 IP 地址或完全限定域名。
- 7 单击确定。

此时，主机时间将与 NTP 服务器同步。

在 vCenter Server Appliance 中配置时间同步设置

您可以在部署后更改 vCenter Server Appliance 中的时间同步设置。

部署 vCenter Server Appliance 时，可以通过使用 NTP 服务器或 VMware Tools 来选择时间同步方法。如果 vSphere 网络中的时间设置发生更改，可以通过使用设备 shell 中的命令来编辑 vCenter Server Appliance 并配置时间同步设置。

启用周期性时间同步时，VMware Tools 将客户机操作系统的时间设置为与主机的时间相同。

执行时间同步之后，VMware Tools 会每分钟检查一次，以确定客户机操作系统和主机上的时钟是否仍然匹配。如果不匹配，则将同步客户机操作系统上的时钟以与主机上的时钟匹配。

本机时间同步软件（例如网络时间协议 (NTP)）通常比 VMware Tools 周期性时间同步更准确，因此成为用户的首选。您可以在 vCenter Server Appliance 中仅使用一种形式的周期性时间同步。如果您决定使用本机时间同步软件，则会禁用 vCenter Server Appliance VMware Tools 周期性时间同步，反之亦然。

使用 VMware Tools 时间同步

您可以将 vCenter Server Appliance 设置为使用 VMware Tools 时间同步。

步骤

- 1 访问设备 shell 并以具有管理员或超级管理员角色的用户身份登录。
具有超级管理员角色的默认用户是 root。

- 2 运行以下命令以启用 VMware Tools 时间同步。

```
timesync.set --mode host
```

- 3 （可选）运行以下命令，确认您已成功应用 VMware Tools 时间同步。

```
timesync.get
```

命令返回时间同步处于主机模式。

结果

设备的时间已与 ESXi 主机的时间同步。

在 vCenter Server Appliance 配置中添加或替换 NTP 服务器

要设置 vCenter Server Appliance 以使用基于 NTP 的时间同步，必须将 NTP 服务器添加到 vCenter Server Appliance 配置中。

步骤

- 1 访问设备 shell 并以具有管理员或超级管理员角色的用户身份登录。

具有超级管理员角色的默认用户是 root。

- 2 通过运行 `ntp.server.add` 命令将 NTP 服务器添加到 vCenter Server Appliance 配置中。

例如，运行以下命令：

```
ntp.server.add --servers IP-addresses-or-host-names
```

此处，*IP-addresses-or-host-names* 是 NTP 服务器的 IP 地址或主机名的逗号分隔列表。

此命令可将 NTP 服务器添加到配置中。如果时间同步基于 NTP 服务器，则将重新启动 NTP 守护进程以重新加载新的 NTP 服务器。否则，此命令仅将新的 NTP 服务器添加到现有 NTP 配置中。

- 3 （可选）要删除旧的 NTP 服务器并将新的 NTP 服务器添加到 vCenter Server Appliance 配置中，请运行 `ntp.server.set` 命令。

例如，运行以下命令：

```
ntp.server.set --servers IP-addresses-or-host-names
```

此处，*IP-addresses-or-host-names* 是 NTP 服务器的 IP 地址或主机名的逗号分隔列表。

此命令可从配置中删除旧的 NTP 服务器，并在配置中设置输入 NTP 服务器。如果时间同步基于 NTP 服务器，则将重新启动 NTP 守护进程以重新加载新的 NTP 配置。否则，此命令仅使用您作为输入提供的服务器替换 NTP 配置中的服务器。

- 4 （可选）运行以下命令，确认您已成功应用新的 NTP 配置设置。

```
ntp.get
```

命令返回配置以进行 NTP 同步的服务器的空格分隔列表。如果已启用 NTP 同步，此命令返回 NTP 配置处于启用状态。如果已禁用 NTP 同步，此命令返回 NTP 配置处于禁用状态。

后续步骤

如果已禁用 NTP 配置，您可以将 vCenter Server Appliance 中的时间同步设置配置为基于 NTP 服务器。请参见[将 vCenter Server Appliance 中的时间与 NTP 服务器同步](#)。

将 vCenter Server Appliance 中的时间与 NTP 服务器同步

您可以将 vCenter Server Appliance 中的时间同步设置配置为基于 NTP 服务器。

前提条件

在 vCenter Server Appliance 配置中设置一个或多个网络时间协议 (NTP) 服务器。请参见在 [vCenter Server Appliance 配置中添加或替换 NTP 服务器](#)。

步骤

- 1 访问设备 shell 并以具有管理员或超级管理员角色的用户身份登录。

具有超级管理员角色的默认用户是 root。

- 2 运行以下命令以启用基于 NTP 的时间同步。

```
timesync.set --mode NTP
```

- 3 (可选) 运行以下命令，确认您已成功应用 NTP 同步。

```
timesync.get
```

命令返回时间同步处于 NTP 模式。

存储安全性最佳做法

遵循存储安全供应商概述的存储安全性最佳做法。您也可以利用 CHAP 和双向 CHAP 确保 iSCSI 存储器的安全、屏蔽 SAN 资源并对其进行分区以及配置 NFS 4.1 的 Kerberos 凭据。

另请参见《管理 VMware Virtual SAN》文档。

确保 iSCSI 存储器安全

为主机配置的存储器可能包括一个或多个使用 iSCSI 的存储区域网络 (SAN)。在主机上配置 iSCSI 时，可采取几种措施最小化安全风险。

iSCSI 是一种使用 TCP/IP 协议通过网络端口（而不是通过直接连接 SCSI 设备）来访问 SCSI 设备和交换数据记录的方法。在 iSCSI 事务中，原始 SCSI 数据块被封装在 iSCSI 记录中并传输至请求数据的设备或用户。

iSCSI SAN 可让您有效地利用现有以太网架构为主机提供对其可动态共享的资源的访问。iSCSI SAN 可为依赖公用存储池服务多个用户的环境提供经济的存储解决方案。与任何网络系统一样，iSCSI SAN 也可能遭到安全破坏。

注 用于确保 iSCSI SAN 安全的要求和过程与可用于主机的 iSCSI 硬件适配器和通过主机直接配置的 iSCSI 相同。

确保 iSCSI 设备安全

确保 iSCSI 设备免遭不利入侵的一种方法就是，每当主机尝试访问目标 LUN 上的数据时都要求 iSCSI 设备（或称目标）对主机（或称启动器）进行身份验证。

身份验证的目的是证明启动器具有访问目标的权利，这是在您配置身份验证时授予的权利。

对于 iSCSI，ESXi 不支持安全远程协议 (SRP) 或公用密钥身份验证方法。您只能将 Kerberos 与 NFS 4.1 配合使用。

ESXi 支持 CHAP 和双向 CHAP 身份验证。《vSphere 存储》文档介绍了如何为 iSCSI 设备选择最佳的身份验证方法以及如何设置 CHAP。

确保 CHAP 密钥的唯一性。每个主机的双向身份验证密钥应不同；如果可能，向服务器进行身份验证的每个客户端的密钥也应不同。这将确保在单个主机受到影响时，攻击者无法创建其他任意主机并向存储设备进行身份验证。使用单个共享密钥时，如果一个主机受到影响，则可能允许攻击者向存储设备进行身份验证。

保护 iSCSI SAN

计划 iSCSI 配置时，应采取一些措施提高 iSCSI SAN 的整体安全。iSCSI 配置是否安全取决于 IP 网络，因此在设置网络时执行良好的安全标准可帮助保护 iSCSI 存储器。

下面是执行良好安全标准的一些具体建议。

保护传输数据

iSCSI SAN 中的一个主要安全风险便是攻击者会嗅探传输的存储数据。

采取其他措施以防止攻击者能够轻易看见 iSCSI 数据。无论是 iSCSI 硬件适配器还是 ESXi iSCSI 启动器，均不会对其传输至目标和从目标接收的数据进行加密，这会造成数据更易遭到嗅探攻击。

允许虚拟机与 iSCSI 配置共享标准交换机和 VLAN 可能导致 iSCSI 流量遭到虚拟机攻击者滥用。为帮助确保入侵者无法侦听 iSCSI 传送数据，请确保任何虚拟机都无法看到 iSCSI 存储网络。

要实现这一目的，您可以这么操作：如果使用 iSCSI 硬件适配器，请确保 iSCSI 适配器和 ESXi 物理网络适配器未由于共享交换机或某种其他方式而无意地在主机外部连接。如果直接通过 ESXi 主机配置 iSCSI，可以不与虚拟机使用同一标准交换机，而改用其他标准交换机来配置 iSCSI 存储器。

除了通过提供专用标准交换机来保护 iSCSI SAN 外，还可以在 iSCSI SAN 自己的 VLAN 上对其进行配置以提高性能和安全性。将 iSCSI 配置放在单独的 VLAN 上可确保只有 iSCSI 适配器可以看到 iSCSI SAN 内的传送数据。此外，来自其他来源的网络拥堵不会影响 iSCSI 流量。

保护 iSCSI 端口安全

当运行 iSCSI 设备时，ESXi 不会打开任何侦听网络连接的端口。此措施可降低入侵者通过空闲端口侵入 ESXi 并控制主机的几率。因此，运行 iSCSI 不会在连接的 ESXi 端产生任何额外安全风险。

您运行的任何 iSCSI 目标设备都必须具有一个或多个打开的 TCP 端口以侦听 iSCSI 连接。如果 iSCSI 设备软件中存在任何安全漏洞，则数据遭遇的风险并非 ESXi 所造成。要降低此风险，请安装存储设备制造商提供的所有安全修补程序并对连接 iSCSI 网络的设备进行限制。

屏蔽 SAN 资源并对其进行分区

可以使用分区域和 LUN 屏蔽分隔 SAN 活动并限制对存储设备的访问。

通过对您的 SAN 资源使用区域分配和 LUN 屏蔽，可以在 vSphere 环境中保护对存储的访问。例如，可以管理定义的区域以在 SAN 中进行独立测试，从而使其不会干扰生产区域中的活动。同样，还可以为不同的部门设置不同的区域。

设置区域时，请考虑在 SAN 设备上设置的任何主机组。

每个 SAN 交换机和磁盘阵列的区域分配和屏蔽功能以及用于管理 LUN 屏蔽的工具且因供应商而异。

请参见 SAN 供应商的文档和《vSphere 存储》文档。

对 NFS 4.1 使用 Kerberos 凭据

使用 NFS 版本 4.1 时，ESXi 支持 Kerberos 身份验证机制。

Kerberos 是一项身份验证服务，可允许 ESXi 上安装的 NFS 4.1 客户端在挂载 NFS 共享之前向 NFS 服务器证明其身份。Kerberos 在不安全的网络连接中使用加密进行工作。适用于 NFS 4.1 的 Kerberos 的 vSphere 实施仅支持对客户端和服务端进行身份验证，但不提供数据完整性和保密性服务。

使用 Kerberos 身份验证时，需要考虑以下注意事项：

- ESXi 将 Kerberos 版本 5 与 Active Directory 域和密钥分发中心 (KDC) 配合使用。
- 作为 vSphere 管理员，您可以指定 Active Directory 凭据以向 NFS 用户提供对 NFS 4.1 Kerberos 数据存储的访问权限。一组凭据可用于访问在该主机上挂载的所有 Kerberos 数据存储。
- 多个 ESXi 主机共享同一个 NFS 4.1 数据存储时，必须对访问共享数据存储的所有主机使用相同的 Active Directory 凭据。您可以通过设置主机配置文件中的用户并将该配置文件应用到所有 ESXi 主机来自动化此操作。
- NFS 4.1 不支持 AUTH_SYS 和 Kerberos 同时挂载。
- 使用 Kerberos 的 NFS 4.1 不支持 IPv6。仅支持 IPv4。

验证是否已禁止向客户机发送主机性能数据

在安装了 VMware Tools 的 Windows 操作系统中，vSphere 会包含虚拟机性能计数器。通过性能计数器，虚拟机所有者可在客户机操作系统内进行准确的性能分析。默认情况下，vSphere 不会向客户机虚拟机公开主机信息。

默认情况下，向客户机虚拟机发送主机性能数据的功能处于禁用状态。此默认设置将阻止虚拟机获取有关物理主机的详细信息，并且在出现违反虚拟机安全的行为时，使主机数据不可用。

注 以下步骤说明了基本过程。改用 vSphere 或 vSphere 命令行界面（vCLI、PowerCLI 等）之一在所有主机上同时执行此任务。

步骤

- 1 在托管虚拟机的 ESXi 系统上，浏览到 VMX 文件。

虚拟机配置文件位于 `/vmfs/volumes/datastore` 目录中，其中 *datastore* 是存储虚拟机文件的存储设备的名称。

- 2 在 VMX 文件中，验证是否设置了以下参数。

```
tools.guestlib.enableHostInfo=FALSE
```

- 3 保存并关闭文件。

结果

您无法从客户机虚拟机中检索有关主机的性能信息。

为 ESXi Shell 和 vSphere Web Client 设置超时

要防止入侵者使用闲置会话，请务必为 ESXi Shell 和 vSphere Web Client 设置超时。

ESXi Shell 超时

对于 ESXi Shell，您可以在 vSphere Web Client 及在直接控制台用户界面 (DCUI) 中设置以下超时。

可用性超时

可用性超时设置是在启用 ESXi Shell 之后和必须登录之前，可以经过的时间量。超过超时期限之后，该服务会禁用，并且不允许用户登录。

闲置超时

闲置超时是用户从闲置交互式会话注销之前可以经过的时间量。对闲置超时的更改会在下次用户登录到 ESXi Shell 时应用，而不会影响现有会话。

vSphere Web Client 超时

默认情况下，vSphere Web Client 会话会在 120 分钟后终止。您可以在 `webclient.properties` 文件中更改此默认值，如《vCenter Server 和主机管理》文档中所述。

使用 TLS 重新配置实用程序管理 TLS 协议配置

10

您可以使用 TLS 重新配置实用程序启用或禁用 TLS 协议版本。您可以在 vSphere 环境中禁用 TLS 1.0，或者同时禁用 TLS 1.0 和 TLS 1.1。从 vSphere 6.5 开始，默认启用 TLS 协议版本 1.0、1.1 和 1.2。

对于重新配置，环境中的 vCenter Server、Platform Services Controller、vSphere Update Manager 和 ESXi 主机运行的软件版本必须允许进行禁用。请参见 VMware 知识库文章 [2145796](#) 获取支持禁用 TLS 1.0 的 VMware 产品列表。

禁用 TLS 1.0 之前，您还必须确保其他 VMware 产品和第三方产品支持已启用的 TLS 协议。根据您的配置，它可能是 TLS 1.2 或 TLS 1.1 和 TLS 1.2。

本章讨论了以下主题：

- 支持禁用 TLS 版本的端口
- 在 vSphere 中禁用 TLS 版本
- 安装 TLS 配置实用程序
- 执行可选手动备份
- 禁用 vCenter Server 系统上的 TLS 版本
- 禁用 ESXi 主机上的 TLS 版本
- 在 Platform Services Controller 系统上禁用 TLS 版本
- 恢复 TLS 配置更改
- 在 vSphere Update Manager 上禁用 TLS 版本

支持禁用 TLS 版本的端口

在 vSphere 环境中运行 TLS Configurator 实用程序时，可以对 vCenter Server、Platform Services Controller 和 ESXi 主机上使用 TLS 的不同端口禁用 TLS。可以禁用 TLS 1.0，或同时禁用 TLS 1.0 和 TLS 1.1。

下表列出了这些端口。如果未包含某端口，则该实用程序不会影响到它。

表 10-1. 受 TLS Configurator 实用程序影响的 vCenter Server 和 Platform Services Controller

服务	在 Windows 上的名称	在 Linux 上的名称	端口
VMware HTTP Reverse Proxy	rhttpproxy	vmware-rhttpproxy	443
VMware Directory Service	VMWareDirectoryService	vmldird	636
VMware Syslog Collector (*)	vmwaresyslogcollector (*)	rsyslogd	1514
vSphere Auto Deploy Waiter	vmware-autodeploy-waiter	vmware-rbd-watchdog	6501 6502
VMware 安全令牌服务	VMwareSTS	vmware-stsd	7444
vSphere Update Manager 服务 (**)	vmware-ufad-vci (**)	vmware-updatemgr	8084 9087
vSphere Web Client	vspherewebclientsvc	vsphere-client	9443
VMware Directory Service	VMWareDirectoryService	vmldird	11712

(*)TLS 由这些服务的加密列表控制。无法进行细化管理。仅支持 TLS 1.2 或所有 TLS 1.x 版本。

(**) 在 vCenter Server Appliance 上，vSphere Update Manager 与 vCenter Server 位于同一系统上。在 Windows 中的 vCenter Server 上，可以通过编辑配置文件配置 TLS。请参见在 [vSphere Update Manager 上禁用 TLS 版本](#)。

表 10-2. 受 TLS Configurator 实用程序影响的 ESXi 端口

服务	服务名称	端口
VMware HTTP Reverse Proxy 和主机守护进程	Hostd	443
VMware VSAN VASA 供应商提供程序	vSANVP	8080
VMware 故障域管理器	FDM	8182
适用于 IO 筛选器的 VMware vSphere API	ioFilterVPServer	9080
VMware 授权守护进程	vmware-authd	902

注意事项和说明

- 确保由 vCenter Server 管理的旧版 ESXi 主机支持启用的 TLS 版本（TLS 1.1 和 TLS 1.2 或者仅 TLS 1.2）。禁用 vCenter Server 6.5 上的 TLS 版本时，vCenter Server 无法再管理旧版 ESXi 主机 5.x 和主机 6.0。请将这些主机升级到支持 TLS 1.1 或 TLS 1.2 的版本。
- 无法仅使用 TLS 1.2 连接到外部 Microsoft SQL Server 或外部 Oracle 数据库。
- 请勿对 Windows Server 2008 上运行的 vCenter Server 或 Platform Services Controller 实例禁用 TLS 1.0。Windows 2008 仅支持 TLS 1.0。请参见 Microsoft TechNet 文章《服务器角色和技术指南》中的 TLS/SSL 设置。

- 在以下情况下，在应用 TLS 配置更改后必须重新启动主机服务。
 - 如果直接对 ESXi 主机应用更改。
 - 如果使用主机配置文件来通过群集配置应用更改。

在 vSphere 中禁用 TLS 版本

禁用 TLS 版本是一个多阶段过程。以正确的顺序禁用 TLS 版本将确保您的环境在此过程中正常运行。

- 1 如果您的环境包含 Windows 上的 vSphere Update Manager，并且 vSphere Update Manager 在单独的系统中，请通过编辑配置文件明确禁用协议。请参见在 [vSphere Update Manager 上禁用 TLS 版本](#)。

vCenter Server Appliance 上的 vSphere Update Manager 始终随 vCenter Server 系统一起提供，并且脚本会更新对应的端口。
- 2 在 vCenter Server 和 Platform Services Controller 上安装 TLS 配置实用程序。如果您的环境使用嵌入式 Platform Services Controller，请仅在 vCenter Server 上安装该实用程序。
- 3 在 vCenter Server 上运行该实用程序。
- 4 在 vCenter Server 管理的每个 ESXi 主机上运行该实用程序。您可以为每个主机或群集中的所有主机执行此任务。
- 5 如果您的环境使用一个或多个 Platform Services Controller 实例，请在每个实例上运行该实用程序。

前提条件

您可以在运行 vSphere 6.0 U3 的系统和运行 vSphere 6.5 的系统上执行此配置。您具有两个选项。

- 禁用 TLS 1.0 并启用 TLS 1.1 和 TLS 1.2。
- 禁用 TLS 1.0 和 TLS 1.1 并启用 TLS 1.2。

安装 TLS 配置实用程序

您可以从 MyVMware.com 下载 TLS 配置实用程序，并将其安装到本地计算机上。安装完成后，可以使用两个脚本。一个脚本用于配置 vCenter Server 和 Platform Services Controller，另一个脚本用于 ESXi 配置。

在 vCenter Server Appliance 上，通过脚本更新 vSphere Update Manager 端口。在 vCenter Server 上，可编辑 vSphere Update Manager 配置文件。请参见在 [vSphere Update Manager 上禁用 TLS 版本](#)。

前提条件

您需要 MyVMware 帐户才能下载脚本。

步骤

- 1 登录到您的 MyVMware 帐户并转到 vSphere。
- 2 找到已获许可的产品和产品版本，选择 VMware vCenter Server，然后单击 [转到下载](#)。

3 选择 VMware vSphere TLS Configurator 并下载以下文件。

操作系统	文件
Windows	VMware-vSphereTlsReconfigurator-version-build_number.x86_64.msi
Linux	VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm

4 将文件上载到 vCenter Server 并安装这些脚本。

在具有外部 Platform Services Controller 的环境中，还要将文件上载到 Platform Services Controller。

操作系统	过程
Windows	<ol style="list-style-type: none"> 以具有管理员特权的用户身份登录。 复制刚刚下载的 VMware-vSphereTlsReconfigurator-version-build_number.x86_64.msi 文件。 安装该 MSI 文件。
Linux	<ol style="list-style-type: none"> 使用 SSH 连接到设备并以具有脚本运行特权的用户身份登录。 使用 SCP 客户端将 VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm 文件复制到设备。 如果当前未启用 Bash shell，请运行以下命令。 <div data-bbox="681 1031 999 1081" data-label="Text"> <pre>shell.set --enabled true shell</pre> </div> 转到上载的 rpm 文件所在的目录，并运行以下命令。 <div data-bbox="681 1169 1324 1222" data-label="Text"> <pre>rpm -Uvh VMware-vSphereTlsReconfigurator-version-build_number.x86_64.rpm</pre> </div>

结果

安装完成后，您会在以下位置找到这些脚本。

操作系统	位置
Windows	<ul style="list-style-type: none"> ■ C:\Program Files\VMware\CIS\vsphereTLSReconfigurator\VcTlsReconfigurator ■ C:\Program Files\VMware\CIS\vsphereTLSReconfigurator\EsxTlsReconfigurator
Linux	<ul style="list-style-type: none"> ■ /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator ■ /usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator

执行可选手动备份

每次脚本修改 vCenter Server、Platform Services Controller 或 vSphere Update Manager 时，TLS 配置实用程序都会执行备份。如果需要备份到特定目录，可以执行手动备份。

Windows 和设备的默认目录有所不同。

操作系统 备份目录Windows `c:\users\current_user\appdata\local\temp\yearmonthdayTtime`Linux `/tmp/yearmonthdayTtime`**步骤**

- 1 将目录更改为 vSphereTlsReconfigurator，然后更改为 VcTlsReconfigurator 子目录。

操作系统	命令
Windows	<code>C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\ cd VcTlsReconfigurator</code>
Linux	<code>cd /usr/lib/vmware-vsphereTlsReconfigurator/ cd VcTlsReconfigurator</code>

- 2 运行以下命令以备份到特定目录。

操作系统	命令
Windows	<code>directory_path\VcTlsReconfigurator> reconfigureVc backup -d backup_directory_path</code>
Linux	<code>directory_path/VcTlsReconfigurator> ./ reconfigureVc backup -d backup_directory_path</code>

- 3 确认备份成功完成。

成功的备份类似于以下示例。

```
vCenter Transport Layer Security reconfigurator, version=6.0.0, build=8482376
For more information, refer to the following article: https://kb.vmware.com/kb/2148819"
Log file: "C:\ProgramData\VMware\vCenterServer\logs\vmware\vsphere-
TlsReconfigurator\VcTlsReconfigurator.log".
===== Backing up vCenter Server TLS configuration =====
Using backup directory: c:\users\admini~1\appdata\local\temp\1\20170202T054311
Backing up: vmsyslogcollector
Backing up: vspherewebclientsvc
Backing up: vmware-autodeploy-waiter
Backing up: rhttpproxy
Backing up: VMwareSTS
Backing up: VMWareDirectoryService
```

- 4 (可选) 如果稍后必须执行还原，可以运行以下命令。

```
reconfigure restore -d tmp directory or custom backup directory path
```

禁用 vCenter Server 系统上的 TLS 版本

您可以使用 TLS 配置实用程序禁用 vCenter Server 系统上的 TLS 版本。作为该过程的一部分，可以启用 TLS 1.1 和 TLS 1.2，或仅启用 TLS 1.2。

前提条件

确保 vCenter Server 管理的主机和服务可以使用仍保持启用状态的 TLS 版本进行通信。对于仅使用 TLS 1.0 进行通信的产品，将丢失连接。

步骤

- 1 以可以运行脚本并访问脚本所在目录的用户身份登录到 vCenter Server 系统。

操作系统	命令
Windows	<code>cd C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator</code>
Linux	<code>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</code>

- 2 运行以下命令，具体取决于您的操作系统和要使用的 TLS 版本。

- 要禁用 TLS 1.0 并启用 TLS 1.1 和 TLS 1.2，请运行以下命令。

操作系统	命令
Windows	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2</code>
Linux	<code>directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2</code>

- 要禁用 TLS 1.0 和 TLS 1.1 并仅启用 TLS 1.2，请运行以下命令。

操作系统	命令
Windows	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2</code>
Linux	<code>directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2</code>

- 3 如果您的环境中包括其他 vCenter Server 系统，请在每个 vCenter Server 系统上重复执行此过程。
- 4 在每个 ESXi 主机和每个 Platform Services Controller 上重复该配置。

禁用 ESXi 主机上的 TLS 版本

您可以使用 TLS 配置实用程序禁用 ESXi 主机上的 TLS 版本。作为该过程的一部分，可以启用 TLS 1.1 和 TLS 1.2，或仅启用 TLS 1.2。

对于 ESXi 主机，使用与 vSphere 环境中其他组件不同的脚本。

注 除非您指定 `-p` 选项，否则该脚本将禁用 TLS 1.0 和 TLS 1.1。

前提条件

确保与 ESXi 主机关联的任何产品或服务都可以使用 TLS 1.1 或 TLS 1.2 进行通信。对于仅使用 TLS 1.0 进行通信的产品，将丢失连接。

步骤

- 1 以可以运行脚本并访问脚本所在目录的用户身份登录到 vCenter Server 主机。

操作系统	命令
Windows	<code>C:\Program Files\VMware\CIS\vsphereTLSReconfigurator\EsxTlsReconfigurator</code>
Linux	<code>/usr/lib/vmware-vSphereTlsReconfigurator/EsxTlsReconfigurator</code>

- 2 要在集群中的所有主机上禁用 TLS，请运行以下命令之一。

- 要在集群中的所有主机上禁用 TLS 1.0 并启用 TLS 1.1 和 TLS 1.2，请运行以下命令。

操作系统	命令
Windows	<code>reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.1 TLSv1.2</code>

- 要在集群中的所有主机上禁用 TLS 1.0 和 TLS 1.1 并仅启用 TLS 1.2，请运行以下命令。

操作系统	命令
Windows	<code>reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterCluster -c Cluster_Name -u Administrative_User -p TLSv1.2</code>

- 3 要在单个主机上禁用 TLS，请运行以下命令之一。

- 要在单个主机上禁用 TLS 1.0 并启用 TLS 1.1 和 TLS 1.2，请运行以下命令。

操作系统	命令
Windows	<code>reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.1 TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.1 TLSv1.2</code>

- 要在单个主机上禁用 TLS 1.0 和 TLS 1.1 并仅启用 TLS 1.2，请运行以下命令。

操作系统	命令
Windows	<code>reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.2</code>
Linux	<code>./reconfigureEsx vCenterHost -h <ESXi_Host_Name> -u Administrative_User -p TLSv1.2</code>

4 重新引导 ESXi 主机以完成 TLS 协议更改。

在 Platform Services Controller 系统上禁用 TLS 版本

如果您的环境包括一个或多个 Platform Services Controller 系统，可以使用 TLS 配置实用程序更改要支持的 TLS 版本。

如果您的环境仅使用嵌入式 Platform Services Controller，则不必执行此任务。

注 只有在确认每个 vCenter Server 系统都在运行兼容版本的 TLS 后，才应继续执行此任务。vCenter Server 6.0.x 或 5.5.x 的实例连接到 vCenter Server 后，如果禁用 TLS 版本，则这些实例将停止与 Platform Services Controller 通信。

您可以禁用 TLS 1.0 和 TLS 1.1 并将 TLS 1.2 保留为启用状态，或者可以仅禁用 TLS 1.0 并将 TLS 1.1 和 TLS 1.2 保留为启用状态。

前提条件

确保 Platform Services Controller 连接到的主机和服务可以使用受支持的协议进行通信。因为身份验证和证书管理由 Platform Services Controller 处理，所以请认真考虑哪些服务可能会受到影响。对于仅使用不受支持的协议进行通信的服务，将丢失连接。

步骤

- 1 以可以运行脚本并访问脚本所在目录的用户身份登录到 Platform Services Controller。

操作系统	命令
Windows	<code>cd C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator</code>
Linux	<code>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</code>

- 2 您可以在 Windows 上的 Platform Services Controller 中或者在 Platform Services Controller 设备上执行此任务。

- 要禁用 TLS 1.0 并启用 TLS 1.1 和 TLS 1.2，请运行以下命令。

操作系统	命令
Windows	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.1 TLSv1.2</code>
Linux	<code>directory_path\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2</code>

- 要禁用 TLS 1.0 和 TLS 1.1 并仅启用 TLS 1.2，请运行以下命令。

操作系统	命令
Windows	<code>directory_path\VcTlsReconfigurator> reconfigureVc update -p TLSv1.2</code>
Linux	<code>directory_path\VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2</code>

- 3 如果您的环境中包括其他 Platform Services Controller 系统，请重复执行此过程。

恢复 TLS 配置更改

TLS 配置实用程序可用于恢复配置更改。恢复更改时，系统将使用 TLS Configurator 实用程序启用已禁用的协议。

仅当之前已备份配置时，才可以执行恢复。ESXi 主机不支持恢复更改。

按以下顺序执行恢复。

- 1 vSphere Update Manager。

如果您的环境在 Windows 系统上运行单独的 vSphere Update Manager 实例，则必须先更新 vSphere Update Manager。

- 2 vCenter Server
- 3 Platform Services Controller

步骤

- 1 连接到 Windows 计算机或设备。

2 登录到要恢复更改的系统。

操作系统	过程
Windows	<ol style="list-style-type: none"> 1 以具有管理员特权的用户身份登录。 2 转到 VcTlsReconfigurator 目录。 <pre>cd C:\Program Files\VMware\CIS\vsphereTlsReconfigurator\VcTlsReconfigurator</pre>
Linux	<ol style="list-style-type: none"> 1 使用 SSH 连接到设备并以具有脚本运行特权的用户身份登录。 2 如果当前未启用 Bash shell，请运行以下命令。 <pre>shell.set --enabled true shell</pre> <ol style="list-style-type: none"> 3 转到 VcTlsReconfigurator 目录。 <pre>cd /usr/lib/vmware-vSphereTlsReconfigurator/VcTlsReconfigurator</pre>

3 查看以前的备份。

操作系统	过程
Windows	<pre>C:\ProgramData\VMware\vCenterServer\logs\vsphere-TlsReconfigurator\VcTlsReconfigurator.log</pre> <p>输出类似于以下示例。</p> <pre>c:\users\username\appdata\local\temp\20161108T161539 c:\users\username\appdata\local\temp\20161108T171539</pre>
Linux	<pre>grep "backup directory" /var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log</pre> <p>输出类似于以下示例。</p> <pre>2016-11-17T17:29:20.950Z INFO Using backup directory: /tmp/20161117T172920 2016-11-17T17:32:59.019Z INFO Using backup directory: /tmp/20161117T173259</pre>

4 运行以下其中一项命令以执行还原。

操作系统	过程
Windows	<pre>reconfigureVc restore -d Directory_path_from_previous_step</pre> <p>例如</p> <pre>reconfigureVc restore -d c:\users\username\appdata\local\temp\20161108T171539</pre>
Linux	<pre>reconfigureVc restore -d Directory_path_from_previous_step</pre> <p>例如</p> <pre>reconfigureVc restore -d /tmp/20161117T172920</pre>

- 5 对任何其他 vCenter Server 实例重复此过程。
- 6 对任何其他 Platform Services Controller 实例重复此过程。

在 vSphere Update Manager 上禁用 TLS 版本

在 vSphere Update Manager 6.0 Update 3 和更高版本中，TLS 协议版本 1.0、1.1 和 1.2 都默认为启用状态。您可以禁用 TLS 版本 1.0 和 TLS 版本 1.1，但是无法禁用 TLS 版本 1.2。

您可以使用 TLS 配置实用程序管理其他服务的 TLS 协议配置。但是对于 vSphere Update Manager，必须手动重新配置 TLS 协议。

修改 TLS 协议配置可能涉及以下任何任务。

- 禁用 TLS 版本 1.0，而将 TLS 版本 1.1 和 TLS 版本 1.2 保留为启用状态。
- 禁用 TLS 版本 1.0 和 TLS 版本 1.1，而将 TLS 版本 1.2 保留为启用状态。
- 重新启用已禁用的 TLS 协议版本。

为 Update Manager 端口 9087 禁用早期 TLS 版本

您可以通过修改 `jetty-vum-ssl.xml` 配置文件为端口 9087 禁用早期版本的 TLS。端口 8084 的该过程有所不同。

注 禁用 TLS 版本之前，请确保与 vSphere Update Manager 进行通信的任何服务都未使用该版本。

前提条件

停止 vSphere Update Manager 服务。请参见安装和管理 VMware vSphere Update Manager 文档。

步骤

- 1 停止 vSphere Update Manager 服务。
- 2 导航到 Update Manager 安装目录，vSphere 6.0 和 vSphere 6.5 的该目录有所不同。

版本	位置
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 为 `jetty-vum-ssl.xml` 文件创建备份，然后打开该文件。

4 通过更改文件禁用早期版本的 TLS。

选项	描述
禁用 TLS 1.0。将 TLS 1.1 和 TLS 1.2 保留为启用状态。	<pre><Set name="ExcludeProtocols"> <Array type="java.lang.String"> <Item>TLSv1</Item> </Array> </Set></pre>
禁用 TLS 1.0 和 TLS 1.1。将 TLS 1.2 保留为启用状态。	<pre><Set name="ExcludeProtocols"> <Array type="java.lang.String"> <Item>TLSv1</Item> <Item>TLSv1.1</Item> </Array> </Set></pre>

5 保存文件。

6 重新启动 vSphere Update Manager 服务。

为 Update Manager 端口 8084 禁用早期 TLS 版本

您可以通过修改 `vci-integrity.xml` 配置文件为端口 8084 禁用早期版本的 TLS。该过程与用于端口 9087 的过程不同。

注 禁用 TLS 版本之前，请确保与 vSphere Update Manager 进行通信的任何服务都未使用该版本。

前提条件

停止 vSphere Update Manager 服务。请参见安装和管理 VMware vSphere Update Manager 文档。

步骤

- 1 停止 vSphere Update Manager 服务。
- 2 导航到 Update Manager 安装目录，6.0 版和 6.5 版的该目录有所不同。

版本	位置
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 为 `vci-integrity.xml` 文件创建备份，然后打开该文件。
- 4 在 `vci-integrity.xml` 文件中添加 `<sslOptions>` 标记。

```
<ssl>
  <handshakeTimeoutMs>120000</handshakeTimeoutMS>
  <sslOptions>sslOptions_value</sslOptions>
</ssl>

<ssl>
```

```
<privateKey>ssl/rui.key</privateKey>
<certificate>ssl/rui.crt</certificate>
<sslOptions>sslOptions_value</sslOptions>
</ssl>
```

- 5 根据要禁用的 TLS 版本，在 <sslOptions> 标记中使用以下某个十进制值。
 - 要仅禁用 TLSv1.0，请使用十进制值 117587968。
 - 要禁用 TLSv1.0 和 TLSv1.1，请使用十进制值 386023424
- 6 保存文件。
- 7 重新启动 vSphere Update Manager 服务。

为 Update Manager 端口 9087 重新启用已禁用的 TLS 版本

如果为 Update Manager 端口 9087 禁用 TLS 版本时遇到问题，可以重新启用该版本。该过程不同于重新启用端口 8084 的过程。

重新启用具有安全影响的早期 TLS 版本。

步骤

- 1 停止 vSphere Update Manager 服务。
- 2 导航到 Update Manager 安装目录，6.0 版和 6.5 版的该目录有所不同。

版本	位置
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 为 jetty-vum-ssl.xml 文件创建备份，然后打开该文件。
- 4 移除与要启用的 TLS 协议版本相对应的 TLS 标记。
例如，移除 jetty-vum-ssl.xml 文件中的 <Item>TLSv1.1</Item> 以启用 TLSv1.1。
- 5 保存文件。
- 6 重新启动 vSphere Update Manager 服务。

为 Update Manager 端口 8084 重新启用已禁用的 TLS 版本

如果为 Update Manager 端口 8084 禁用 TLS 版本时遇到问题，可以重新启用该版本。该过程与用于端口 9087 的过程不同。

重新启用具有安全影响的早期 TLS 版本。

步骤

- 1 停止 vSphere Update Manager 服务。

- 2 导航到 Update Manager 安装目录，6.0 版和 6.5 版的该目录有所不同。

版本	位置
vSphere 6.0	C:\Program Files (x86)\VMware\Infrastructure\Update Manager
vSphere 6.5	C:\Program Files\VMware\Infrastructure\Update Manager

- 3 为 vci-integrity.xml 文件创建备份，然后打开该文件。
- 4 更改 <sslOptions> 标记中使用的十进制值或者删除该标记以允许使用所有 TLS 版本。
 - 要启用 TLS 1.1，但将 TLS 1.0 保留为禁用状态，请使用十进制值 117587968。
 - 要重新启用 TLS 1.1 和 TLS 1.0，请移除该标记。
- 5 保存文件。
- 6 重新启动 vSphere Update Manager 服务。

定义的特权

11

下表列出了一些默认特权，为角色选定这些特权时，可以与用户配对，也可以将其分配给对象。此附录中的表使用 VC 表示 vCenter Server，使用 HC 表示主机客户端（一个独立的 ESXi 或 Workstation 主机）。

在设置权限时，确认对所有对象类型的每项特定操作均设置了适当的特权。除了要拥有对正待操作的对象的操作权限之外，有些操作还需要对根文件夹或父文件夹的操作权限。有些操作需要对父文件夹及相关对象的访问权限或执行权限。

vCenter Server 扩展可能定义未在此处列出的其他特权。有关这些特权的详细信息，请参见扩展文档。

本章讨论了以下主题：

- 警报特权
- Auto Deploy 和镜像配置文件特权
- 证书特权
- 内容库特权
- 数据中心特权
- 数据存储特权
- 数据存储集群特权
- Distributed Switch 特权
- ESX Agent Manager 特权
- 扩展特权
- 文件夹特权
- 全局特权
- 主机 CIM 特权
- 主机配置特权
- 主机清单
- 主机本地操作特权
- 主机 vSphere Replication 特权

- 主机配置文件特权
- **Inventory Service** 提供商特权
- **Inventory Service** 标记特权
- 网络特权
- 性能特权
- 权限特权
- 配置文件驱动的存储特权
- 资源特权
- 已调度任务特权
- 会话特权
- 存储视图特权
- 任务特权
- **Transfer Service** 特权
- **VRM** 策略特权
- 虚拟机配置特权
- 虚拟机客户机操作特权
- 虚拟机交互特权
- 虚拟机清单特权
- 虚拟机置备特权
- 虚拟机服务配置特权
- 虚拟机快照管理特权
- 虚拟机 vSphere Replication 特权
- dvPort 组特权
- **vApp** 特权
- **vServices** 特权

警报特权

警报特权控制在清单对象上创建、修改警报并对其作出响应的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-1. 警报特权

特权名称	描述	要求
警报.确认警报	允许阻止对所有已触发警报的所有警报操作。	对其定义了警报的对象
警报.创建警报	允许创建新警报。 如果通过自定义操作创建警报，则在用户创建警报时，将验证执行操作的特权。	对其定义了警报的对象
警报.禁用警报操作	允许阻止警报操作在触发警报后发生。此操作不会禁用警报。	对其定义了警报的对象
警报.修改警报	允许更改警报的属性。	对其定义了警报的对象
警报.移除警报	允许删除警报。	对其定义了警报的对象
警报.设置警报状态	允许更改所配置的事件警报的状态。状态可以更改为 正常 、 警告 或 警示 。	对其定义了警报的对象

Auto Deploy 和镜像配置文件特权

Auto Deploy 特权控制可以对 Auto Deploy 规则执行不同任务的用户和可以关联主机的用户。Auto Deploy 特权还用于控制可以创建或编辑映像配置文件的用户。

下表说明了可以管理 Auto Deploy 规则和规则集的用户以及可以创建和编辑映像配置文件的用户。请参见《vSphere 安装和设置》。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-2. Auto Deploy 特权

特权名称	描述	要求
Auto Deploy.主机.管理计算机	允许用户关联主机与计算机。	vCenter Server
Auto Deploy.映像配置文件.创建	允许创建映像配置文件。	vCenter Server
Auto Deploy.映像配置文件.编辑	允许编辑映像配置文件。	vCenter Server
Auto Deploy.规则.创建	允许创建 Auto Deploy 规则。	vCenter Server

表 11-2. Auto Deploy 特权（续）

特权名称	描述	要求
Auto Deploy.规则.删除	允许删除 Auto Deploy 规则。	vCenter Server
Auto Deploy.规则.编辑	允许编辑 Auto Deploy 规则。	vCenter Server
Auto Deploy.规则集.激活	允许激活 Auto Deploy 规则集。	vCenter Server
Auto Deploy.规则集.编辑	允许编辑 Auto Deploy 规则集。	vCenter Server

证书特权

证书特权控制哪些用户可以管理 ESXi 证书。

此特权决定哪些用户可以对 ESXi 主机执行证书管理。请参见[证书管理操作所需的特权](#)了解有关 vCenter Server 证书管理的信息。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-3. 主机证书特权

特权名称	描述	要求
证书.管理证书	允许对 ESXi 主机进行证书管理。	vCenter Server

内容库特权

内容库可简单、有效地管理虚拟机模板和 vApp。内容库特权控制可以查看或管理内容库不同方面的用户。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-4. 内容库特权

特权名称	描述	要求
内容库.添加库项目	允许在库中添加项目。	库
内容库.创建本地库	允许在指定的 vCenter Server 系统上创建本地库。	vCenter Server
内容库.创建已订阅库	允许创建已订阅库。	vCenter Server
内容库.删除库项目	允许删除库项目。	库。将此权限设置为传播到所有库项目。
内容库.删除本地库	允许删除本地库。	库
内容库.删除已订阅库	允许删除已订阅库。	库
内容库.下载文件	允许从内容库下载文件。	库
内容库.逐出库项目	允许逐出项目。可以缓存也可以不缓存已订阅库的内容。如果缓存内容，则可以通过逐出库项目来发布该库项目（如果您具有此特权）。	库。将此权限设置为传播到所有库项目。
内容库.逐出已订阅库	允许逐出已订阅库。可以缓存也可以不缓存已订阅库的内容。如果缓存内容，则可以通过逐出库来发布该库（如果您具有此特权）。	库
内容库.导入存储	如果源文件 URL 以 ds:// 或 file:// 开头，则允许用户导入库项目。默认情况下，将禁用内容库管理员的此特权，因为从存储 URL 导入意味着导入内容，只有在需要时以及在要执行导入的用户当前存在安全问题时，才启用此特权。	库
内容库.探查订阅信息	此特权允许解决方案用户和 API 探查远程库的订阅信息，包括 URL、SSL 证书和密码。由此产生的结构将说明订阅配置是否成功或是否存在 SSL 错误等问题。	库
内容库.读取存储	允许读取内容库存储。	库
内容库.同步库项目	允许同步库项目。	库。将此权限设置为传播到所有库项目。
内容库.同步已订阅库	允许同步已订阅库。	库
内容库.类型自检	允许解决方案用户或 API 自检内容库服务的类型支持插件。	库
内容库.更新配置设置	允许更新配置设置。 没有与此特权关联的 vSphere Web Client 用户界面元素。	库
内容库.更新文件	允许将内容上载到内容库。还允许从库项目中移除文件。	库
内容库.更新库	允许更新内容库。	库
内容库.更新库项目	允许更新库项目。	库。将此权限设置为传播到所有库项目。
内容库.更新本地库	允许更新本地库。	库
内容库.更新已订阅库	允许更新已订阅库的属性。	库
内容库.查看配置设置	允许查看配置设置。 没有与此特权关联的 vSphere Web Client 用户界面元素。	库

数据中心特权

数据中心特权控制在 vSphere Web Client 清单中创建和编辑数据中心的能力。

所有数据中心特权仅用于 vCenter Server。**创建数据中心**特权在数据中心文件夹或根对象上定义。所有其他数据中心特权与数据中心、数据中心文件夹或根对象配对。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-5. 数据中心特权

特权名称	描述	要求
数据中心.创建数据中心	允许创建新数据中心。	数据中心文件夹或根对象
数据中心.移动数据中心	允许移动数据中心。 特权必须存在于源位置和目标位置。	数据中心、源和目标
数据中心.网络协议配置文件配置	允许为数据中心配置网络配置文件。	数据中心
数据中心.查询 IP 池分配	允许 IP 地址池的配置。	数据中心
数据中心.重新配置数据中心	允许重新配置数据中心。	数据中心
数据中心.释放 IP 分配	允许为数据中心发布分配的 IP 分配。	数据中心
数据中心.移除数据中心	允许移除数据中心。 为了有执行此操作的权限，必须将此特权分配给该对象及其父对象。	数据中心加父对象
数据中心.重命名数据中心	允许更改数据中心的名称。	数据中心

数据存储特权

数据存储特权控制在数据存储上浏览、管理和分配空间的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-6. 数据存储特权

特权名称	描述	要求
数据存储.分配空间	允许在数据存储上为虚拟机、快照、克隆或虚拟磁盘分配空间。	数据存储
数据存储.浏览数据存储	允许浏览数据存储上的文件。	数据存储
数据存储.配置数据存储	允许配置数据存储。	数据存储
数据存储.低级别文件操作	允许在数据存储浏览器中执行读取、写入、删除和重命名操作。	数据存储

表 11-6. 数据存储特权（续）

特权名称	描述	要求
数据存储.移动数据存储	允许在文件夹之间移动数据存储。 特权必须存在于源位置和目标位置。	数据存储、源位置和目标位置
数据存储.移除数据存储	允许移除数据存储。 此特权已弃用。 要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。	数据存储
数据存储.移除文件	允许在数据存储中删除文件。 此特权已弃用。分配 低级别文件操作 特权。	数据存储
数据存储.重命名数据存储	允许重命名数据存储。	数据存储
数据存储.更新虚拟机文件	允许在对数据存储进行再签名之后，更新指向数据存储中虚拟机文件的文件路径。	数据存储
数据存储.更新虚拟机元数据	允许更新与数据存储关联的虚拟机元数据。	数据存储

数据存储集群特权

数据存储集群特权可控制数据存储集群的配置，以实现 Storage DRS。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-7. 数据存储集群特权

特权名称	描述	要求
数据存储集群.配置数据存储集群	允许创建和配置数据存储集群设置，以实现 Storage DRS。	数据存储集群

Distributed Switch 特权

Distributed Switch 特权控制执行与 Distributed Switch 管理相关的任务的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-8. vSphere Distributed Switch 特权

特权名称	描述	要求
Distributed Switch.创建	允许创建 Distributed Switch。	数据中心、网络文件夹
Distributed Switch.删除	允许移除 Distributed Switch。 要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。	Distributed Switch

表 11-8. vSphere Distributed Switch 特权（续）

特权名称	描述	要求
Distributed Switch.主机操作	允许更改 Distributed Switch 的主机成员。	Distributed Switch
Distributed Switch.修改	允许更改 Distributed Switch 的配置。	Distributed Switch
Distributed Switch.移动	允许将 vSphere Distributed Switch 移动到其他文件夹。	Distributed Switch
Distributed Switch.Network I/O Control 操作	允许更改 vSphere Distributed Switch 的资源设置。	Distributed Switch
Distributed Switch.策略操作	允许更改 vSphere Distributed Switch 的策略。	Distributed Switch
Distributed Switch.端口配置操作	允许更改 vSphere Distributed Switch 中端口的配置。	Distributed Switch
Distributed Switch.端口设置操作	允许更改 vSphere Distributed Switch 中端口的设置。	Distributed Switch
Distributed Switch.VSPAN 操作	允许更改 vSphere Distributed Switch 的 VSPAN 配置。	Distributed Switch

ESX Agent Manager 特权

ESX Agent Manager 特权控制与 ESX Agent Manager 和代理虚拟机相关的操作。ESX Agent Manager 这项服务允许您安装管理虚拟机，这些虚拟机与主机绑定在一起，不受用于迁移虚拟机的 VMware DRS 或其他服务的影响。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-9. ESX Agent Manager

特权名称	描述	要求
ESX Agent Manager.配置	允许在主机或集群上部署代理虚拟机。	虚拟机
ESX Agent Manager.修改	允许对代理虚拟机进行修改，如关闭电源或删除虚拟机。	虚拟机
ESX Agent View.查看	允许查看代理虚拟机。	虚拟机

扩展特权

扩展特权控制安装和管理扩展的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-10. 扩展特权

特权名称	描述	要求
扩展.注册扩展	允许注册扩展（插件）。	根 vCenter Server
扩展.取消注册扩展	允许取消注册扩展（插件）。	根 vCenter Server
扩展.更新扩展	允许更新扩展（插件）。	根 vCenter Server

文件夹特权

文件夹特权控制创建和管理文件夹的功能。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-11. 文件夹特权

特权名称	描述	要求
文件夹.创建文件夹	允许创建新文件夹。	文件夹
文件夹.删除文件夹	允许删除文件夹。 要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。	文件夹
文件夹.移动文件夹	允许移动文件夹。 特权必须存在于源位置和目标位置。	文件夹
文件夹.重命名文件夹	允许更改文件夹的名称。	文件夹

全局特权

全局特权控制与任务、脚本和扩展相关的全局任务。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-12. 全局特权

特权名称	描述	要求
全局.充当 vCenter Server	允许准备或启动 vMotion 发送操作或 vMotion 接收操作。	根 vCenter Server
全局.取消任务	允许取消正在运行或已排队的任务。	与任务相关的清单对象
全局.容量规划	允许使用容量规划来规划物理机到虚拟机的整合。	根 vCenter Server
全局.诊断	允许检索诊断文件、日志头、二进制文件或诊断捆绑包的列表。 要避免潜在的安全破坏，请将此特权限制为 vCenter Server 管理员角色。	根 vCenter Server
全局.禁用方法	允许 vCenter Server 扩展的服务器对 vCenter Server 管理的对象禁用某些操作。	根 vCenter Server
全局.启用方法	允许 vCenter Server 扩展的服务器对 vCenter Server 管理的对象启用某些操作。	根 vCenter Server
全局.全局标记	允许添加或移除全局标记。	根主机或 vCenter Server
全局.健康状况	允许查看 vCenter Server 组件的健康状况。	根 vCenter Server
全局.许可证	允许查看安装的许可证并添加或移除许可证。	根主机或 vCenter Server
全局.记录事件	允许针对特定的受管实体记录用户定义的事件。	任何对象
全局.管理自定义属性	允许添加、移除或重命名自定义字段定义。	根 vCenter Server
全局.代理	允许访问内部接口以将端点添加到代理或从代理移除端点。	根 vCenter Server
全局.脚本操作	允许调度与警报一起使用的脚本操作。	任何对象
全局.服务管理器	允许在 vSphere CLI 中使用 <code>resxstop</code> 命令。	根主机或 vCenter Server
全局.设置自定义属性	允许查看、创建或移除受管对象的自定义属性。	任何对象
全局.设置	允许读取并修改运行时 vCenter Server 配置设置。	根 vCenter Server
全局.系统标记	允许添加或移除系统标记。	根 vCenter Server

主机 CIM 特权

主机 CIM 特权控制主机健康状况监控的 CIM 使用。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-13. 主机 CIM 特权

特权名称	描述	要求
主机.CIM.CIM 交互	允许客户端获取用于 CIM 服务的票证。	主机

主机配置特权

主机配置特权控制配置主机的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-14. 主机配置特权

特权名称	描述	要求
主机.配置.高级设置	允许设置高级主机配置选项。	主机
主机.配置.身份验证存储	允许配置 Active Directory 身份验证存储。	主机
主机.配置.更改 PciPassthru 设置	允许更改主机的 PciPassthru 设置。	主机
主机.配置.更改 SNMP 设置	允许更改主机的 SNMP 设置。	主机
主机.配置.更改日期和时间设置	允许更改主机上的日期和时间设置。	主机
主机.配置.更改设置	允许在 ESXi 主机上设置锁定模式。	主机
主机.配置.连接	允许更改主机的连接状态（已连接或已断开连接）。	主机
主机.配置.固件	允许更新 ESXi 主机的固件。	主机
主机.配置.超线程	允许启用和禁用主机 CPU 调度程序中的超线程。	主机
主机.配置.映像配置	允许更改与主机关联的映像。	
主机.配置.维护	允许使主机进入和退出维护模式，以及关闭和重新启动主机。	主机
主机.配置.内存配置	允许修改主机配置。	主机
主机.配置.网络配置	允许配置网络、防火墙和 vMotion 网络。	主机
主机.配置.电源	允许配置主机电源管理设置。	主机
主机.配置.查询修补程序	允许查询可安装的修补程序并将修补程序安装在主机上。	主机
主机.配置.安全配置文件和防火墙	允许配置 Internet 服务，如 SSH、Telnet、SNMP 和主机防火墙。	主机
主机.配置.存储器分区配置	允许管理 VMFS 数据存储和诊断分区。具有此特权的用户可以扫描新存储设备并管理 iSCSI。	主机
主机.配置.系统管理	允许扩展以便操作主机上的文件系统。	主机

表 11-14. 主机配置特权（续）

特权名称	描述	要求
主机.配置.系统资源	允许更新系统资源层次结构的配置。	主机
主机.配置.虚拟机自动启动配置	允许更改单个主机上虚拟机的自动启动和自动停止顺序。	主机

主机清单

主机清单特权控制向清单添加主机、向集群添加主机以及在清单中移动主机等操作。

下表描述了在清单中添加和移动主机和集群所需的特权。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-15. 主机清单特权

特权名称	描述	要求
主机.清单.将主机添加到群集	允许将主机添加到现有集群。	群集
主机.清单.添加独立主机	允许添加独立主机。	主机文件夹
主机.清单.创建群集	允许创建新集群。	主机文件夹
主机.清单.修改群集	允许更改集群的属性。	群集
主机.清单.移动群集或独立主机	允许在文件夹之间移动集群或独立主机。 特权必须存在于源位置和目标位置。	群集
主机.清单.移动主机	允许将一组现有主机移入或移出集群。 特权必须存在于源位置和目标位置。	群集
主机.清单.移除群集	允许删除集群或独立主机。 要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。	集群、主机
主机.清单.移除主机	允许移除主机。 要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。	主机加父对象
主机.清单.重命名群集	允许重命名集群。	群集

主机本地操作特权

主机本地操作特权控制当 vSphere Client 直接连接到主机时执行的操作。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-16. 主机本地操作特权

特权名称	描述	要求
主机.本地操作.将主机添加到 vCenter	允许安装和卸载主机上的 vCenter 代理，如 vpxa 和 aam。	根主机
主机.本地操作.创建虚拟机	允许在磁盘上从头开始创建新的虚拟机，而不在主机上注册。	根主机
主机.本地操作.删除虚拟机	允许在磁盘上删除虚拟机。支持注册和未注册的虚拟机。	根主机
主机.本地操作.提取 NVRAM 内容	允许提取主机的 NVRAM 内容。	
主机.本地操作.管理用户组	允许在主机上管理本地帐户。	根主机
主机.本地操作.重新配置虚拟机	允许对虚拟机进行重新配置。	根主机
主机.本地操作.重新布局快照	允许更改虚拟机快照的布局。	根主机

主机 vSphere Replication 特权

主机 vSphere Replication 特权控制 VMware vCenter Site Recovery Manager™ 对主机使用虚拟机复制。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-17. 主机 vSphere Replication 特权

特权名称	描述	要求
主机.vSphere Replication.管理复制	允许管理此主机上的虚拟机复制。	主机

主机配置文件特权

主机配置文件特权控制与创建和修改主机配置文件相关的操作。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-18. 主机配置文件特权

特权名称	描述	要求
主机配置文件.清除	允许清除配置文件相关信息。	根 vCenter Server
主机配置文件.创建	允许创建主机配置文件。	根 vCenter Server
主机配置文件.删除	允许删除主机配置文件。	根 vCenter Server

表 11-18. 主机配置文件特权（续）

特权名称	描述	要求
主机配置文件.编辑	允许编辑主机配置文件。	根 vCenter Server
主机配置文件.导出	允许导出主机配置文件。	根 vCenter Server
主机配置文件.查看	允许查看主机配置文件。	根 vCenter Server

Inventory Service 提供商特权

Inventory Service 提供商特权仅供内部使用。不使用。

Inventory Service 标记特权

Inventory Service 标记特权控制创建和删除标记和标记类别的功能，并分配和移除 vSphere 清单对象上的标记。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-19. vCenter Inventory Service 特权

特权名称	描述	要求
Inventory Service.vSphere 标记.分配或取消分配 vSphere 标记	允许对 vCenter Server 清单中的对象分配标记或取消分配标记。	任何对象
Inventory Service.vSphere 标记.创建 vSphere 标记	允许创建标记。	任何对象
Inventory Service.vSphere 标记.创建 vSphere 标记类别	允许创建标记类别。	任何对象
Inventory Service.vSphere 标记.创建 vSphere 标记范围	允许创建标记范围。	任何对象
Inventory Service.vSphere 标记.删除 vSphere 标记	允许删除标记类别。	任何对象
Inventory Service.vSphere 标记.删除 vSphere 标记类别	允许删除标记类别。	任何对象
Inventory Service.vSphere 标记.删除 vSphere 标记范围	允许删除标记范围。	任何对象
Inventory Service.vSphere 标记.编辑 vSphere 标记	允许编辑标记。	任何对象
Inventory Service.vSphere 标记.编辑 vSphere 标记类别	允许编辑标记类别。	任何对象
Inventory Service.vSphere 标记.编辑 vSphere 标记范围	允许编辑标记范围。	任何对象

表 11-19. vCenter Inventory Service 特权（续）

特权名称	描述	要求
Inventory Service.vSphere 标记.修改类别的 UsedBy 字段	允许更改标记类别的 UsedBy 字段。	任何对象
Inventory Service.vSphere 标记.修改标记的 UsedBy 字段	允许更改标记的 UsedBy 字段。	任何对象

网络特权

网络特权控制与网络管理相关的任务。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-20. 网络特权

特权名称	描述	要求
网络.分配网络	允许将网络分配到虚拟机。	网络、虚拟机
网络.配置	允许配置网络。	网络、虚拟机
网络.移动网络	允许在文件夹之间移动网络。 特权必须存在于源位置和目标位置。	网络
网络.移除	允许移除网络。 此特权已弃用。 要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。	网络

性能特权

性能特权对修改性能统计信息设置进行控制。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-21. 性能特权

特权名称	描述	要求
性能.修改时间间隔	允许创建、移除和更新性能数据收集时间间隔。	根 vCenter Server

权限特权

权限特权控制角色和权限的分配。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-22. 权限特权

特权名称	描述	要求
权限.修改权限	允许为实体定义一个或多个权限规则，或者如果实体上的特定用户或组已经有规则，则更新规则。 要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。	任何对象加父对象
权限.修改特权	允许修改特权的组或描述。 没有与此特权关联的 vSphere Web Client 用户界面元素。	
权限.修改角色	允许更新角色名称以及与角色关联的特权。	任何对象
权限.重新指定角色权限	允许将某角色的所有权限重新分配给其他角色。	任何对象

配置文件驱动的存储特权

配置文件驱动的存储特权控制与存储配置文件相关的操作。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-23. 配置文件驱动的存储特权

特权名称	描述	要求
配置文件驱动的存储.配置文件驱动的存储更新	允许对存储配置文件进行更改，如创建和更新存储功能和虚拟机存储配置文件。	根 vCenter Server
配置文件驱动的存储.配置文件驱动的存储视图	允许查看定义的 Storage Capabilities 和存储配置文件。	根 vCenter Server

资源特权

资源特权控制资源池的创建和管理，以及虚拟机的迁移。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-24. 资源特权

特权名称	描述	要求
资源.应用建议	允许接受服务器提供的建议以通过 vMotion 执行迁移。	群集
资源.将 vApp 分配给资源池	允许将 vApp 分配到资源池。	资源池
资源.将虚拟机分配给资源池	允许将虚拟机分配到资源池。	资源池
资源.创建资源池	允许创建资源池。	资源池、集群
资源.迁移已关闭电源的虚拟机	允许将已关闭电源的虚拟机迁移到其他资源池或主机。	虚拟机
资源.迁移已打开电源的虚拟机	允许通过 vMotion 将已打开电源的虚拟机迁移到其他资源池或主机。	
资源.修改资源池	允许更改资源池的分配。	资源池
资源.移动资源池	允许移动资源池。 特权必须存在于源位置和目标位置。	资源池
资源.查询 vMotion	允许查询虚拟机与一组主机的一般 vMotion 兼容性。	根 vCenter Server
资源.移除资源池	允许删除资源池。 要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。	资源池
资源.重命名资源池	允许重命名资源池。	资源池

已调度任务特权

已调度任务特权控制已调度任务的创建、编辑和移除。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-25. 已调度任务特权

特权名称	描述	要求
已调度任务.创建任务	允许调度任务。在调度时，需要一定的特权来执行已调度的操作。	任何对象
已调度任务.修改任务	允许重新配置已调度任务的属性。	任何对象
已调度任务.移除任务	允许移除队列中的已调度任务。	任何对象
已调度任务.运行任务	允许立即运行已调度任务。 创建和运行已调度任务也需要执行关联操作的权限。	任何对象

会话特权

会话特权控制扩展打开 vCenter Server 系统上的会话的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-26. 会话特权

特权名称	描述	要求
会话.模拟用户	允许模拟其他用户。该功能由扩展使用。	根 vCenter Server
会话.消息	允许在消息中设置全局日志。	根 vCenter Server
会话.验证会话	允许验证会话有效性。	根 vCenter Server
会话.查看和停止会话	允许查看会话以及强制注销一个或多个已登录的用户。	根 vCenter Server

存储视图特权

存储视图特权控制存储监控服务 API 的特权。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-27. 存储视图特权

特权名称	描述	要求
存储视图.配置服务	允许特权用户使用所有存储监控服务 API。对于只读存储监控服务 API 的特权，使用 存储视图.查看 。	根 vCenter Server
存储视图.查看	允许特权用户使用只读存储监控服务 API。	根 vCenter Server

任务特权

任务特权控制扩展在 vCenter Server 上创建和更新任务的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-28. 任务特权

特权名称	描述	要求
任务.创建任务	允许扩展创建用户定义的任务。 没有与此特权关联的 vSphere Web Client 用户界面元素。	根 vCenter Server
任务.更新任务	允许扩展更新用户定义的任务。 没有与此特权关联的 vSphere Web Client 用户界面元素。	根 vCenter Server

Transfer Service 特权

Transfer Service 特权是 VMware 的内部特权。请勿使用这些特权。

VRM 策略特权

VRM 策略特权是 VMware 的内部特权。请勿使用这些特权。

虚拟机配置特权

虚拟机配置特权控制配置虚拟机选项和设备的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-29. 虚拟机配置特权

特权名称	描述	要求
虚拟机.配置.添加现有磁盘	允许将现有虚拟磁盘添加到虚拟机。	虚拟机
虚拟机.配置.添加新磁盘	允许创建新虚拟磁盘以添加到虚拟机。	虚拟机
虚拟机.配置.添加或移除设备	允许添加或移除任何非磁盘设备。	虚拟机
虚拟机.配置.高级	允许在虚拟机的配置文件中添加或修改高级参数。	虚拟机
虚拟机.配置.更改 CPU 计数	允许更改虚拟 CPU 的数目。	虚拟机
虚拟机.配置.更改资源	允许更改给定资源池中一组虚拟机节点的资源配置。	虚拟机
虚拟机.配置.配置管理者	允许扩展或解决方案将虚拟机标记为由该扩展或解决方案管理。	虚拟机
虚拟机.配置.磁盘更改跟踪	允许启用或禁用虚拟机的磁盘更改跟踪。	虚拟机
虚拟机.配置.磁盘租用	允许磁盘为虚拟机租用操作。	虚拟机
虚拟机.配置.显示连接设置	允许配置虚拟机远程控制台选项。	虚拟机
虚拟机.配置.扩展虚拟磁盘	允许扩展虚拟磁盘的大小。	虚拟机
虚拟机.配置.主机 USB 设备	允许将基于主机的 USB 设备连接到虚拟机。	虚拟机

表 11-29. 虚拟机配置特权（续）

特权名称	描述	要求
虚拟机.配置.内存	允许更改分配给虚拟机的内存量。	虚拟机
虚拟机.配置.修改设备设置	允许更改现有设备的属性。	虚拟机
虚拟机.配置.查询 Fault Tolerance 兼容性	允许检查虚拟机的兼容性是否符合 Fault Tolerance 的要求。	虚拟机
虚拟机.配置.查询无所有者的文件	允许查询无所有者的文件。	虚拟机
虚拟机.配置.裸设备	允许添加或移除裸磁盘映射或 SCSI 直通设备。 设置此参数将替代用于修改裸设备（包括连接状况）的任何其他特权。	虚拟机
虚拟机.配置.基于路径重新加载	允许更改虚拟机配置路径，而保留虚拟机的标识。诸如 VMware vCenter Site Recovery Manager 等解决方案使用此操作在故障切换和故障恢复期间保持虚拟机的标识。	虚拟机
虚拟机.配置.移除磁盘	允许移除虚拟磁盘设备。	虚拟机
虚拟机.配置.重命名	允许重命名虚拟机或修改虚拟机的相关注释。	虚拟机
虚拟机.配置.重置客户机信息	允许编辑虚拟机的客户机操作系统信息。	虚拟机
虚拟机.配置.设置注释	允许添加或编辑虚拟机注释。	虚拟机
虚拟机.配置.设置	允许更改常规虚拟机设置。	虚拟机
虚拟机.配置.交换文件放置位置	允许更改虚拟机的交换文件放置策略。	虚拟机
虚拟机.配置.解锁虚拟机	允许对虚拟机进行解密。	虚拟机
虚拟机.配置.升级虚拟机兼容性	允许升级虚拟机的虚拟机兼容性版本。	虚拟机

虚拟机客户机操作特权

虚拟机客户机操作特权控制使用 API 与虚拟机的客户机操作系统中的文件和程序交互的能力。

有关这些操作的详细信息，请参见《VMware vSphere API 参考》。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-30. 虚拟机客户机操作

特权名称	描述	要求
虚拟机.客户机操作.客户机操作别名修改	允许对虚拟机别名进行修改的虚拟机客户机操作。	虚拟机
虚拟机.客户机操作.客户机操作别名查询	允许对虚拟机别名进行查询的虚拟机客户机操作。	虚拟机

表 11-30. 虚拟机客户机操作 （续）

特权名称	描述	要求
虚拟机.客户机操作.客户机操作修改	允许在虚拟机中对客户机操作系统进行修改的虚拟机客户机操作，如向虚拟机传输文件。 没有与此特权关联的 vSphere Web Client 用户界面元素。	虚拟机
虚拟机.客户机操作.客户机操作程序执行	允许在虚拟机中执行程序的虚拟机客户机操作。 没有与此特权关联的 vSphere Web Client 用户界面元素。	虚拟机
虚拟机.客户机操作.客户机操作查询	允许对客户机操作系统进行查询的虚拟机客户机操作，如在客户机操作系统中列出文件。 没有与此特权关联的 vSphere Web Client 用户界面元素。	虚拟机

虚拟机交互特权

虚拟机交互特权控制与虚拟机控制台交互、配置媒体、执行电源操作和安装 VMware Tools 的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-31. 虚拟机交互

特权名称	描述	要求
虚拟机.交互.回答问题	允许解决虚拟机状态转换的问题或运行时错误。	虚拟机
虚拟机.交互.备份虚拟机上的操作	允许对虚拟机执行备份操作。	虚拟机
虚拟机.交互.配置 CD 媒体	允许配置虚拟 DVD 或 CD-ROM 设备。	虚拟机
虚拟机.交互.配置软盘媒体	允许配置虚拟软盘设备。	虚拟机

表 11-31. 虚拟机交互（续）

特权名称	描述	要求
虚拟机.交互.控制台交互	允许与虚拟机的虚拟鼠标、键盘和屏幕交互。	虚拟机
虚拟机.交互.创建屏幕截图	允许创建虚拟机屏幕截图。	虚拟机
虚拟机.交互.对所有磁盘执行碎片整理	允许对虚拟机上的所有磁盘执行碎片整理操作。	虚拟机
虚拟机.交互.设备连接	允许更改虚拟机的可断开虚拟设备的连接状况。	虚拟机
虚拟机.交互.禁用 Fault Tolerance	允许使用 Fault Tolerance 禁用虚拟机的辅助虚拟机。	虚拟机
虚拟机.交互.拖放	允许在虚拟机和远程客户端之间拖放文件。	虚拟机

表 11-31. 虚拟机交互（续）

特权名称	描述	要求
虚拟机.交互.启用 Fault Tolerance	允许使用 Fault Tolerance 启用虚拟机的辅助虚拟机。	虚拟机
虚拟机.交互.通过 VIX API 执行客户机操作系统管理	允许通过 VIX API 管理虚拟机的操作系统。	虚拟机
虚拟机.交互.插入 USB HID 扫描代码	允许插入 USB HID 扫描代码。	虚拟机
虚拟机.交互.暂停/取消暂停	允许暂停或取消暂停虚拟机。	虚拟机
虚拟机.交互.执行擦除或压缩操作	允许对虚拟机执行擦除或压缩操作。	虚拟机
虚拟机.交互.关闭电源	允许关闭已打开电源的虚拟机的电源。此操作将关闭客户机操作系统。	虚拟机

表 11-31. 虚拟机交互（续）

特权名称	描述	要求
虚拟机.交互.打开电源	允许打开已关闭电源的虚拟机的电源，以及恢复挂起的虚拟机。	虚拟机
虚拟机.交互.记录虚拟机上的会话	允许记录虚拟机上的会话。	虚拟机
虚拟机.交互.重放虚拟机上的会话	允许重放虚拟机上已记录的会话。	虚拟机
虚拟机.交互.重置	允许重置虚拟机并重新引导客户机操作系统。	虚拟机
虚拟机.交互.恢复 Fault Tolerance	允许恢复虚拟机的 Fault Tolerance 功能。	虚拟机
虚拟机.交互.挂起	允许挂起已打开电源的虚拟机。此操作将客户机置于待机模式。	虚拟机

表 11-31. 虚拟机交互 （续）

特权名称	描述	要求
虚拟机.交互.挂起 Fault Tolerance	允许暂停虚拟机的 Fault Tolerance 功能。	虚拟机
虚拟机.交互.测试故障切换	允许通过使辅助虚拟机成为主虚拟机测试 Fault Tolerance 故障切换。	虚拟机
虚拟机.交互.测试重新启动辅助虚拟机	允许使用 Fault Tolerance 终止虚拟机的辅助虚拟机。	虚拟机
虚拟机.交互.关闭 Fault Tolerance	允许关闭虚拟机的 Fault Tolerance 功能。	虚拟机

表 11-31. 虚拟机交互（续）

特权名称	描述	要求
虚拟机.交互.打开 Fault Tolerance	允许打开虚拟机的 Fault Tolerance 功能。	虚拟机
虚拟机.交互.VMware Tools 安装	允许以 CD-ROM 形式为客户机操作系统装载和卸载 VMware Tools CD 安装程序。	虚拟机

虚拟机清单特权

虚拟机清单特权控制虚拟机的添加、移动和移除。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-32. 虚拟机清单特权

特权名称	描述	要求
虚拟机.清单.从现有项创建	允许通过从模板克隆或部署，基于现有虚拟机或模板创建虚拟机。	群集、主机、虚拟机文件夹
虚拟机.清单.新建	允许创建虚拟机并为其执行分配资源。	群集、主机、虚拟机文件夹
虚拟机.清单.移动	允许在层次结构中重定位虚拟机。 特权必须存在于源位置和目标位置。	虚拟机
虚拟机.清单.注册	允许将现有虚拟机添加到 vCenter Server 或主机清单。	群集、主机、虚拟机文件夹

表 11-32. 虚拟机清单特权（续）

特权名称	描述	要求
虚拟机.清单.移除	允许删除虚拟机。删除操作将从磁盘移除虚拟机的基础文件。 要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。	虚拟机
虚拟机.清单.取消注册	允许从 vCenter Server 或主机清单中取消注册虚拟机。 要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。	虚拟机

虚拟机置备特权

虚拟机置备特权控制与部署和自定义虚拟机相关的活动。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-33. 虚拟机置备特权

特权名称	描述	要求
虚拟机.置备.允许访问磁盘	允许打开虚拟机上的磁盘进行随机读写访问。常用于远程磁盘装载。	虚拟机
虚拟机.置备.允许对磁盘进行只读访问	允许打开虚拟机上的磁盘进行随机读取访问。常用于远程磁盘装载。	虚拟机
虚拟机.置备.允许下载虚拟机	允许读取与虚拟机关联的文件，包括 vmx、磁盘文件、日志和 nvram。	根主机或 vCenter Server
虚拟机.置备.允许上载虚拟机文件	允许写入与虚拟机关联的文件，包括 vmx、磁盘文件、日志和 nvram。	根主机或 vCenter Server
虚拟机.置备.克隆模板	允许克隆模板。	模板
虚拟机.置备.克隆虚拟机	允许克隆现有虚拟机和资源分配。	虚拟机
虚拟机.置备.从虚拟机创建模板	允许从虚拟机创建新模板。	虚拟机
虚拟机.置备.自定义	允许自定义虚拟机的客户机操作系统，而不移动虚拟机。	虚拟机
虚拟机.置备.部署模板	允许从模板部署虚拟机。	模板
虚拟机.置备.标记为模板	允许将现有已关闭电源的虚拟机标记为模板。	虚拟机
虚拟机.置备.标记为虚拟机	允许将现有模板标记为虚拟机。	模板
虚拟机.置备.修改自定义规范	允许创建、修改或删除自定义规范。	根 vCenter Server
虚拟机.置备.升级磁盘	允许升级虚拟机的磁盘。	虚拟机
虚拟机.置备.读取自定义规范	允许读取自定义规范。	虚拟机

虚拟机服务配置特权

虚拟机服务配置特权控制哪些用户可以执行有关服务配置的监控和管理任务。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

注 在 vSphere 6.0 中，不能使用 vSphere Web Client 分配或移除此特权。

表 11-34. 虚拟机服务配置特权

特权名称	描述
虚拟机.服务配置.允许通知	允许生成和使用有关服务状态的通知。
虚拟机.服务配置.允许轮询全局事件通知	允许查询是否存在任何通知。
虚拟机.服务配置.管理服务配置	允许创建、修改和删除虚拟机服务。
虚拟机.服务配置.修改服务配置	允许修改现有的虚拟机服务配置。
虚拟机.服务配置.查询服务配置	允许检索虚拟机服务的列表。
虚拟机.服务配置.读取服务配置	允许检索现有的虚拟机服务配置。

虚拟机快照管理特权

虚拟机快照管理特权控制执行、删除、重命名和恢复快照的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-35. 虚拟机状况特权

特权名称	描述	要求
虚拟机.快照管理.创建快照	允许按照虚拟机的当前状况创建快照。	虚拟机
虚拟机.快照管理.移除快照	允许从快照历史记录移除快照。	虚拟机
虚拟机.快照管理.重命名快照	允许使用新名称和/或新描述重命名快照。	虚拟机
虚拟机.快照管理.恢复快照	允许将虚拟机设置为在给定快照中所处的状况。	虚拟机

虚拟机 vSphere Replication 特权

虚拟机 vSphere Replication 特权控制 VMware vCenter Site Recovery Manager™ 对虚拟机使用复制。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-36. 虚拟机 vSphere Replication

特权名称	描述	要求
虚拟机.vSphere Replication.配置复制	允许对虚拟机进行复制配置。	虚拟机
虚拟机.vSphere Replication.管理复制	允许在复制时触发完全同步、联机同步或脱机同步。	虚拟机
虚拟机.vSphere Replication.监控复制	允许监控复制。	虚拟机

dvPort 组特权

分布式虚拟端口组特权控制创建、删除和修改分布式虚拟端口组的能力。

下表描述创建和配置分布式虚拟端口组所需的特权。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-37. 分布式虚拟端口组特权

特权名称	描述	要求
dvPort 组.创建	允许创建分布式虚拟端口组。	虚拟端口组
dvPort 组.删除	允许删除分布式虚拟端口组。 要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。	虚拟端口组
dvPort 组.修改	允许修改分布式虚拟端口组的配置。	虚拟端口组
dvPort 组.策略操作	允许设置分布式虚拟端口组的策略。	虚拟端口组
dvPort 组.范围操作	允许设置分布式虚拟端口组的范围。	虚拟端口组

vApp 特权

vApp 特权控制与部署和配置 vApp 相关的操作。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-38. vApp 特权

特权名称	描述	要求
vApp.添加虚拟机	允许将虚拟机添加到 vApp。	vApp
vApp.分配资源池	允许将资源池分配到 vApp。	vApp
vApp.分配 vApp	允许将一个 vApp 分配给另一个 vApp	vApp
vApp.克隆	允许克隆 vApp。	vApp
vApp.创建	允许创建 vApp。	vApp
vApp.删除	允许删除 vApp。 要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。	vApp
vApp.导出	允许从 vSphere 导出 vApp。	vApp
vApp.导入	允许将 vApp 导入 vSphere。	vApp
vApp.移动	允许将 vApp 移动到新清单位置。	vApp
vApp.关闭电源	允许对 vApp 执行关闭电源操作。	vApp
vApp.打开电源	允许对 vApp 执行打开电源操作。	vApp
vApp.重命名	允许重命名 vApp。	vApp
vApp.挂起	允许暂停 vApp。	vApp
vApp.取消注册	允许取消注册 vApp。 要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。	vApp
vApp.查看 OVF 环境	允许在 vApp 中查看已打开电源的虚拟机的 OVF 环境。	vApp
vApp.vApp 应用程序配置	允许修改 vApp 的内部结构，例如产品信息和属性。	vApp
vApp.vApp 实例配置	允许修改 vApp 的实例配置，例如策略。	vApp

表 11-38. vApp 特权（续）

特权名称	描述	要求
vApp.vApp 管理者配置	允许扩展或解决方案将 vApp 标记为由该扩展或解决方案管理。 没有与此特权关联的 vSphere Web Client 用户界面元素。	vApp
vApp.vApp 资源配置	允许修改 vApp 的资源配置。 要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。	vApp

vServices 特权

vService 特权控制创建、配置和更新虚拟机和 vApp 的 vService 依赖关系的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-39. vService

特权名称	描述	要求
vService.创建依赖关系	允许创建虚拟机或 vApp 的 vService 依赖关系。	vApp 和虚拟机
vService.破坏依赖关系	允许移除虚拟机或 vApp 的 vService 依赖关系。	vApp 和虚拟机
vService.重新配置依赖关系配置	允许重新配置依赖关系以更新提供程序或绑定。	vApp 和虚拟机
vService.更新依赖关系	允许更新依赖关系以配置名称或描述。	vApp 和虚拟机