

# vSphere 安全性

修改日期：2022 年 11 月 23 日

VMware vSphere 8.0

VMware ESXi 8.0

vCenter Server 8.0

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://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](http://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](http://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](http://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 14

更新信息 16

## 1 vSphere 环境中的安全性 17

确保 ESXi Hypervisor 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 21

在 vSphere 环境中保护密码 23

vCenter Server 和 ESXi 安全最佳做法与资源 24

## 2 vSphere 权限和用户管理任务 26

了解 vSphere 中的授权 27

vSphere 中的权限层级继承 30

多个权限设置在 vSphere 中如何工作 32

示例 1: 从多个组继承权限 33

示例 2: 子权限替代父权限 33

示例 3: 用户角色替代组角色 34

管理 vCenter Server 组件的权限 35

将权限添加到清单对象 35

更改或移除清单对象的权限 36

更改 vCenter Server 用户验证设置 36

使用 vCenter Server 全局权限 37

添加全局权限 37

标记对象的 vCenter Server 权限 38

使用 vCenter Server 角色分配特权 39

创建 vCenter Server 自定义角色 41

针对 vCenter Server 角色和权限的最佳做法 42

常见任务的所需 vCenter Server 特权 43

## 3 确保 ESXi 主机安全 46

常规 ESXi 安全建议 47

ESXi 高级系统设置 48

使用主机配置文件配置 ESXi 主机 50

使用脚本管理 ESXi 主机配置设置 51

ESXi 密码和帐户锁定 52

ESXi 加密密钥生成	54
ESXi 中的 SSH 安全性	55
使用 HTTPS PUT 上载 SSH 密钥	55
PCI 和 PCIe 设备和 ESXi	56
停用 vSphere Managed Object Browser	57
ESXi 网络连接安全建议	57
修改 ESXi Web 代理设置	57
vSphere Auto Deploy 安全注意事项	58
基于 CIM 的硬件监控工具的控制访问	59
vSphere Distributed Services Engine 安全性最佳做法	60
控制 ESXi 熵	60
管理 ESXi 主机的证书	62
ESXi 主机升级和证书	63
ESXi 证书模式切换工作流	64
ESXi 证书默认设置	66
更改 ESXi 证书默认设置	67
查看 ESXi 主机的证书过期信息	67
续订或刷新 ESXi 证书	69
更改 ESXi 证书模式	70
替换 ESXi SSL 证书和密钥	70
ESXi 证书签名请求的要求	71
从 ESXi Shell 替换默认证书和密钥	72
通过 HTTPS PUT 替换默认证书	72
更新 vCenter Server TRUSTED_ROOTS 存储（自定义证书）	73
将 Auto Deploy 设为辅助证书颁发机构	74
在 Auto Deploy 中使用自定义证书	75
还原 ESXi 证书和密钥文件	79
自定义 ESXi 主机安全性	80
配置 ESXi 防火墙	80
管理 ESXi 防火墙设置	81
为 ESXi 主机添加允许的 IP 地址	82
ESXi 主机的入站和出站防火墙端口	82
NFS 客户端防火墙行为	83
使用 ESXCLI 防火墙命令配置 ESXi 行为	83
激活或停用 ESXi 服务	84
在 ESXi 主机上配置和管理锁定模式	86
锁定模式行为	86
从 vSphere Client 激活锁定模式	87
从 vSphere Client 停用锁定模式	88
从直接控制台用户界面激活或停用正常锁定模式	88
指定在锁定模式下拥有访问特权的帐户	89

使用 vSphere 安装包执行安全更新	91
管理 ESXi 主机和 vSphere 安装包的接受级别	91
为 ESXi 主机分配特权	93
使用 Active Directory 管理 ESXi 用户	95
配置 ESXi 主机以使用 Active Directory	95
将 ESXi 主机添加到目录服务域	96
查看 ESXi 主机的目录服务设置	97
使用 vSphere Authentication Proxy	97
启动 vSphere Authentication Proxy 服务	98
使用 vSphere Client 将域添加到 vSphere Authentication Proxy	99
使用 camconfig 命令向 vSphere Authentication Proxy 添加域	99
使用 vSphere Authentication Proxy 将主机添加到域	100
为 vSphere Authentication Proxy 激活客户端身份验证	100
将 vSphere Authentication Proxy 证书导入到 ESXi 主机	101
为 vSphere Authentication Proxy 生成新证书	102
设置 vSphere Authentication Proxy 以使用自定义证书	102
为 ESXi 配置和管理智能卡身份验证	104
激活智能卡身份验证	105
停用智能卡身份验证	105
如果出现连接问题，使用用户名和密码进行身份验证	106
在锁定模式下使用智能卡身份验证	106
使用 ESXi Shell	106
使用 vSphere Client 设置 ESXi Shell 的闲置超时	107
使用 vSphere Client 设置 ESXi Shell 的可用性超时	108
使用 DCUI 设置 ESXi Shell 的可用性超时或闲置超时	108
使用 vSphere Client 激活对 ESXi Shell 的访问	109
使用 DCUI 激活对 ESXi Shell 的访问	110
登录 ESXi Shell 以进行故障排除	110
ESXi 主机的 UEFI 安全引导	111
在升级后的 ESXi 主机上运行安全引导验证脚本	112
使用可信平台模块保护 ESXi 主机	113
查看 ESXi 主机认证状态	114
对 ESXi 主机认证问题进行故障排除	115
ESXi 日志文件	115
在 ESXi 主机上配置 Syslog	115
ESXi Syslog 选项	116
ESXi 日志文件地址	120
确保 Fault Tolerance 日志记录通信的安全	121
激活 Fault Tolerance 加密	121
管理 ESXi 审核记录	122
确保 ESXi 配置安全	123

- 管理 ESXi 安全配置 125
  - 列出 ESXi 安全配置恢复密钥的内容 125
  - 轮换 ESXi 安全配置恢复密钥 126
  - ESXi 安全配置的故障排除和恢复 126
  - 恢复 ESXi 安全配置 127
  - 激活或停用安全引导实施以获得安全的 ESXi 配置 127
  - 激活或停用 `execInstalledOnly` 实施以获得安全的 ESXi 配置 130
- 停用 `execInstalledOnly` 高级配置运行时选项 133

## 4 确保 vCenter Server 系统安全 134

- vCenter Server 访问控制的最佳做法 134
  - 设置 vCenter Server 密码策略 136
  - 从失败的安装中移除过期和撤销的证书和日志 136
- 限制 vCenter Server 网络连接 136
  - 评估 Linux 客户端与 CLI 和 SDK 的结合使用 137
  - 检查 vSphere Client 插件 137
- vCenter Server 安全性最佳做法 138
- vCenter 密码要求和锁定行为 138
- 验证旧版 ESXi 主机的指纹 139
- vCenter Server 的所需端口 140

## 5 确保虚拟机安全 141

- 为虚拟机激活或停用 UEFI 安全引导 141
- 限制信息性消息从虚拟机流向 VMX 文件 143
- 虚拟机安全性最佳做法 143
  - 虚拟机常规保护 144
  - 使用模板来部署虚拟机 144
  - 尽量少用虚拟机控制台 145
  - 防止虚拟机取代资源 145
  - 停用虚拟机中不必要的功能 146
    - 从虚拟机中移除不必要的硬件设备 146
    - 停用虚拟机上未使用的显示功能 147
    - 停用客户机操作系统和远程控制台之间的复制和粘贴操作 147
    - 限制公开复制到虚拟机控制台剪贴板中的敏感数据 148
    - 限制用户在虚拟机中运行命令 148
    - 阻止虚拟机用户或进程与设备断开连接 149
    - 阻止客户机操作系统进程向主机发送配置消息 149
    - 避免使用独立非持久磁盘 150
- 使用 Intel Software Guard Extensions 确保虚拟机安全 150
  - vSGX 入门 151
  - 在虚拟机上启用 vSGX 152

在现有虚拟机上启用 vSGX	153
从虚拟机中移除 vSGX	153
使用 AMD Secure Encrypted Virtualization-Encrypted State 保护虚拟机	154
vSphere 和 AMD Secure Encrypted Virtualization-Encrypted State	154
使用 vSphere Client 向虚拟机添加 AMD Secure Encrypted Virtualization-Encrypted State	155
向虚拟机添加 AMD Secure Encrypted Virtualization-Encrypted State	156
使用 vSphere Client 在现有虚拟机上激活 AMD Secure Encrypted Virtualization-Encrypted State	157
在现有虚拟机上激活 AMD Secure Encrypted Virtualization-Encrypted State	158
使用 vSphere Client 在虚拟机上停用 AMD Secure Encrypted Virtualization-Encrypted State	159
在虚拟机上停用 AMD Secure Encrypted Virtualization-Encrypted State	160
<b>6 虚拟机加密</b>	<b>161</b>
vSphere 密钥提供程序比较	162
vSphere 虚拟机加密如何保护您的环境	164
vSphere 虚拟机加密组件	167
加密过程流	169
虚拟磁盘加密	171
虚拟机加密错误	172
虚拟机加密任务的必备条件和必需特权	173
加密 vSphere vMotion	174
虚拟机加密最佳做法	177
虚拟机加密限制	179
虚拟机加密互操作性	180
ESXi 主机上的 vSphere 密钥持久性	183
<b>7 配置和管理标准密钥提供程序</b>	<b>185</b>
标准密钥提供程序概览	185
设置标准密钥提供程序	186
使用 vSphere Client 添加标准密钥提供程序	186
通过交换证书建立标准密钥提供程序可信连接	187
使用“根 CA 证书”选项建立标准密钥提供程序可信连接	188
使用“证书”选项建立标准密钥提供程序可信连接	189
使用“上载证书和私钥”选项建立标准密钥提供程序可信连接	189
使用“新建证书签名请求”选项建立标准密钥提供程序可信连接	190
完成标准密钥提供程序的信任设置	190
为不同用户设置不同的密钥提供程序	191
<b>8 配置和管理 vSphere Native Key Provider</b>	<b>192</b>
vSphere Native Key Provider 概览	192
vSphere Native Key Provider 过程流	195

- 配置 vSphere Native Key Provider 195
- 备份 vSphere Native Key Provider 197
- 在增强型链接模式配置中导入 vSphere Native Key Provider 198
- 恢复 vSphere Native Key Provider 199
  - 使用 vSphere Client 还原 vSphere Native Key Provider 199
- 更新 vSphere Native Key Provider 200
- 删除 vSphere Native Key Provider 201

## 9 vSphere Trust Authority 202

- vSphere Trust Authority 概念和功能 202
  - vSphere Trust Authority 如何保护您的环境 202
  - 可信基础架构概述 206
  - vSphere Trust Authority 过程流 208
  - vSphere Trust Authority 拓扑 211
  - vSphere Trust Authority 的必备条件和所需特权 211
  - vSphere Trust Authority 最佳做法、局限性和互操作性 213
  - vSphere Trust Authority 生命周期 214
- 配置 vSphere Trust Authority 216
  - 设置工作站以配置 vSphere Trust Authority 218
  - 启用 Trust Authority 管理员 219
  - 启用 Trust Authority 状态 219
  - 收集有关要信任的 ESXi 主机和 vCenter Server 的信息 221
    - 导出和导入 TPM 认可密钥证书 226
  - 将受信任主机信息导入到 Trust Authority 集群 231
  - 在 Trust Authority 集群上创建密钥提供程序 234
    - 上载客户端证书以建立可信密钥提供程序可信连接 239
    - 上载证书和私钥以建立可信密钥提供程序可信连接 240
    - 创建证书签名请求以建立可信密钥提供程序可信连接 242
  - 导出 Trust Authority 集群信息 243
  - 将 Trust Authority 集群信息导入到受信任主机 245
  - 使用 vSphere Client 为受信任主机配置可信密钥提供程序 249
  - 使用命令行为受信任主机配置可信密钥提供程序 250
- 管理 vSphere 环境中的 vSphere Trust Authority 252
  - 启动、停止和重新启动 vSphere Trust Authority 服务 252
  - 查看 Trust Authority 主机 252
  - 查看 vSphere Trust Authority 集群状态 252
  - 重新启动受信任主机服务 253
  - 添加和移除 vSphere Trust Authority 主机 253
  - 使用 vSphere Client 将主机添加到受信任集群 253
  - 使用 CLI 将主机添加到受信任集群 254
  - 取消配置受信任集群中的受信任主机 255



- 备份 vSphere Trust Authority 配置 256
- 更改可信密钥提供程序的主要密钥 256
- 受信任主机证明报告 258
  - 查看受信任集群证明状态 258
- 对受信任主机认证问题进行故障排除 259
- 检查和修复受信任集群的运行状况 260
  - 检查受信任集群的运行状况 261
  - 修复受信任集群 261

## 10 在 vSphere 环境中使用加密 263

- 创建加密存储策略 264
- 明确激活主机加密模式 264
- 使用 API 停用主机加密模式 265
- 创建加密虚拟机 266
- 克隆加密虚拟机 267
- 加密现有虚拟机或虚拟磁盘 270
- 解密加密虚拟机或虚拟磁盘 270
- 更改虚拟磁盘的加密策略 271
- 解决缺失加密密钥问题 272
- 解锁锁定的虚拟机 274
- 解决 ESXi 主机加密模式问题 274
- 重新激活 ESXi 主机加密模式 275
- 设置密钥服务器证书过期阈值 275
- vSphere 虚拟机加密和核心转储 276
  - 为使用加密的 ESXi 主机收集 vm-support 软件包 277
  - 解密或重新加密已加密核心转储 278
- 在 ESXi 主机上激活和停用密钥持久性 279
- 使用 vSphere Client 对加密虚拟机进行重新加密 280
- 使用 vSphere Client 设置默认密钥提供程序 281
- 使用 CLI 设置默认密钥提供程序 281

## 11 使用虚拟可信平台模块保护虚拟机 283

- 什么是虚拟可信平台模块 283
- 创建具有虚拟可信平台模块的虚拟机 285
- 将虚拟可信平台模块添加到现有虚拟机 286
- 从虚拟机中移除虚拟可信平台模块 287
- 确定已启用虚拟可信平台模块的虚拟机 287
- 查看虚拟可信平台模块设备证书 288
- 导出和替换虚拟可信平台模块设备证书 289

## 12 使用基于虚拟化的安全保护 Windows 客户机操作系统 290

vSphere 基于虚拟化的安全最佳做法	290
在虚拟机上激活基于虚拟化的安全	292
在现有虚拟机上激活基于虚拟化的安全	293
在客户机操作系统上激活基于虚拟化的安全	294
停用基于虚拟化的安全	294
标识已启用 VBS 的虚拟机	295
<b>13 确保 vSphere 网络安全</b>	<b>296</b>
使用防火墙确保网络安全	297
针对有 vCenter Server 的配置设立防火墙	298
通过防火墙连接到 vCenter Server	299
通过防火墙连接 ESXi 主机	299
针对没有 vCenter Server 的配置设立防火墙	299
通过防火墙连接到虚拟机控制台	299
确保物理交换机安全	300
使用安全策略确保标准交换机端口安全	301
确保 vSphere 标准交换机的安全	301
MAC 地址更改	302
伪传输	302
混杂模式运行	303
标准交换机保护和 VLAN	303
确保 vSphere Distributed Switch 和分布式端口组的安全	304
通过 VLAN 确保虚拟机安全	305
VLAN 安全注意事项	306
确保 VLAN 安全	307
在单台 ESXi 主机中创建多个网络	308
在 ESXi 主机上使用 Internet 协议安全	309
列出可用的安全关联	310
添加 IPsec 安全关联	310
移除 IPsec 安全关联	311
列出可用的 IPsec 安全策略	311
创建 IPsec 安全策略	312
移除 IPsec 安全策略	313
确保 SNMP 配置正确	313
vSphere 网络连接安全性最佳做法	314
常规 vSphere 网络安全建议	314
标记 vSphere 网络组件	315
记录和检查 vSphere VLAN 环境	315
在 vSphere 中采用网络隔离做法	316
仅在需要时才在 vSphere Network Appliance API 中使用虚拟交换机	317

<b>14</b>	<b>涉及多个 vSphere 组件的最佳做法</b>	<b>318</b>
	同步 vSphere 网络连接上的时钟	318
	使 ESXi 时钟与网络时间服务器同步	319
	配置 vCenter Server 中的时间同步设置	319
	使用 VMware Tools 时间同步	320
	在 vCenter Server 配置中添加或替换 NTP 服务器	320
	将 vCenter Server 中的时间与 NTP 服务器同步	321
	存储安全性最佳做法	321
	确保 iSCSI 存储安全	322
	确保 iSCSI 设备安全	322
	保护 iSCSI SAN	322
	屏蔽 SAN 资源并对其进行分区	323
	对 NFS 4.1 使用 Kerberos	323
	验证是否已停用向客户机发送主机性能数据	324
	为 ESXi Shell 和 vSphere Client 设置超时	325
<b>15</b>	<b>使用 TLS Configurator 实用程序管理 vSphere TLS 协议配置</b>	<b>326</b>
	执行可选的 vCenter Server TLS 手动备份	327
	在 vCenter Server 系统上激活或停用 TLS 版本	328
	扫描 vCenter Server 上的 TLS 协议	328
	恢复 vCenter Server TLS 配置更改	329
<b>16</b>	<b>定义的特权</b>	<b>331</b>
	警报特权	334
	Auto Deploy 和镜像配置文件特权	334
	证书特权	335
	证书颁发机构特权	336
	证书管理特权	336
	Cns 特权	337
	计算策略特权	337
	内容库特权	337
	加密操作特权	340
	dvPort 组特权	342
	Distributed Switch 特权	343
	数据中心特权	343
	数据存储特权	344
	数据存储集群特权	345
	ESX Agent Manager 特权	346
	扩展特权	346
	外部统计信息提供程序特权	347

- 文件夹特权 347
- 全局特权 347
- 混合链接模式特权 349
- 运行状况更新提供程序特权 349
- 主机 CIM 特权 349
- 主机配置特权 349
- 主机熵池特权 351
- 主机 Intel Software Guard Extensions 特权 352
- 主机清单特权 352
- 主机本地操作特权 353
- 主机统计信息特权 353
- 托管可信平台模块特权 354
- 主机 vSphere Replication 特权 354
- 主机配置文件特权 354
- vCenter Server 配置文件特权 355
- vSphere with Tanzu 特权 355
- 网络特权 356
- NSX 特权 357
- VMware 可观察性特权 357
- OvfManager 特权 357
- 与合作伙伴 Rest 守护进程交互特权 357
- 性能特权 358
- 插件特权 358
- 权限特权 358
- 资源特权 359
- 已调度任务特权 360
- 会话特权 360
- 虚拟机存储策略特权 361
- 存储视图特权 361
- 主管服务特权 362
- 任务特权 362
- 租户管理特权 363
- Transfer Service 特权 363
- VcTrusts/VcIdentity 特权 363
- 可信基础架构管理员特权 363
- vApp 特权 364
- VcIdentityProviders 特权 366
- VMware vSphere Lifecycle Manager 配置特权 366
- VMware vSphere Lifecycle Manager ESXi 运行状况视图特权 367
- VMware vSphere Lifecycle Manager 常规特权 367
- VMware vSphere Lifecycle Manager 硬件兼容性特权 368

VMware vSphere Lifecycle Manager 映像特权	368
VMware vSphere Lifecycle Manager 映像修复特权	369
VMware vSphere Lifecycle Manager 设置特权	370
VMware vSphere Lifecycle Manager 管理基准特权	370
VMware vSphere Lifecycle Manager 管理修补程序和升级特权	370
VMware vSphere Lifecycle Manager 上载文件特权	371
虚拟机更改配置特权	371
虚拟机客户机操作特权	373
虚拟机交互特权	374
虚拟机编辑清单特权	376
虚拟机置备特权	377
虚拟机服务配置特权	379
虚拟机快照管理特权	379
虚拟机 vSphere Replication 特权	380
虚拟机类特权	380
vSAN 特权	381
vSphere 区域特权	381
vService 特权	381
vSphere 标记特权	382
vSphere Client 特权	382

## 17 了解 vSphere 强化与合规性 383

vSphere 环境中的安全与合规性	383
了解《vSphere 安全性配置指南》	385
关于美国国家标准与技术研究院	386
关于 DISA STIG	386
关于 VMware 安全开发生命周期	386
vSphere 中的审核日志记录	387
单点登录审核事件	387
了解安全与合规的后续步骤	388
vCenter Server 和 FIPS	389
FIPS 模块	389
在 vCenter Server Appliance 上激活和停用 FIPS	390
使用 FIPS 时的注意事项	390

# 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。

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

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
权限和用户管理	<ul style="list-style-type: none"><li>■ 权限模型（角色、组、对象）。</li><li>■ 创建自定义角色。</li><li>■ 设置权限。</li><li>■ 管理全局权限。</li></ul>
主机安全功能	<ul style="list-style-type: none"><li>■ 锁定模式和其他安全配置文件功能。</li><li>■ 主机智能卡身份验证。</li><li>■ vSphere Authentication Proxy。</li><li>■ UEFI 安全引导。</li><li>■ 可信平台模块 (TPM)。</li><li>■ VMware® vSphere Trust Authority™。</li><li>■ 安全的 ESXi 配置和配置封装</li></ul>
虚拟机加密	<ul style="list-style-type: none"><li>■ VMware vSphere® Native Key Provider™。</li><li>■ 虚拟机加密的工作方式是什么？</li><li>■ KMS 设置。</li><li>■ 加密和解密虚拟机。</li><li>■ 故障排除和最佳做法。</li></ul>
客户机操作系统安全	<ul style="list-style-type: none"><li>■ 虚拟可信平台模块 (vTPM)。</li><li>■ 基于虚拟化的安全 (VBS)。</li></ul>
管理 TLS 协议配置	使用命令行实用程序更改 TLS 协议配置。
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"><li>■ vCenter Server 安全</li><li>■ 主机安全</li><li>■ 虚拟机安全</li><li>■ 网络安全</li></ul>
vSphere 特权	此版本中支持的所有 vSphere 特权的完整列表。

## 相关文档

相关文档《vSphere 身份验证》说明了如何使用身份验证服务，例如，管理向 vCenter Single Sign-On 进行身份验证以及管理 vSphere 环境中的证书。

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

## Platform Services Controller 发生了什么情况

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

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

## 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系统管理员。

## 认证

VMware 公开发布了已完成通用标准认证的 VMware 产品列表。要检查某特定的 VMware 产品版本是否已经过认证，请参见“通用标准评估和验证”网页，网址为 <https://www.vmware.com/security/certifications/common-criteria.html>。

# 更新信息

本《《vSphere 安全性》》文档随产品的每个版本一起更新或在必要时进行更新。

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 11 月 23 日	<ul style="list-style-type: none"><li>■ 对使用 <b>vCenter Server</b> 角色分配特权进行了微小更新。</li><li>■ 更新了 <b>ESXi</b> 主机上的 <b>vSphere</b> 密钥持久性和在 <b>ESXi</b> 主机上激活和停用密钥持久性，添加了有关 <b>vSphere Native Key Provider</b> 的其他信息。</li><li>■ 对确保 <b>VLAN</b> 安全进行了微小更新。</li><li>■ 在第 16 章 定义的特权一章中添加了主题。</li></ul>
2022 年 10 月 27 日	<ul style="list-style-type: none"><li>■ 对使用命令行为受信任主机配置可信密钥提供程序进行了微小更新。</li><li>■ 对使用 <b>vSphere Client</b> 设置默认密钥提供程序进行了微小更新。</li><li>■ 添加了使用 <b>CLI</b> 设置默认密钥提供程序。</li><li>■ 在第 16 章 定义的特权一章中添加了多个主题。</li></ul>
2022 年 10 月 13 日	<ul style="list-style-type: none"><li>■ 对 <b>vSphere</b> 基于虚拟化的安全最佳做法、在虚拟机上激活基于虚拟化的安全和在现有虚拟机上激活基于虚拟化的安全进行了微小更新。</li><li>■ 移除了对 <b>vifs</b> 命令的引用。请参见 <b>VMware</b> 知识库文章，网址为 <a href="https://kb.vmware.com/article/78473">https://kb.vmware.com/article/78473</a>。</li></ul>
2022 年 10 月 11 日	初始版本。



# vSphere 环境中的安全性

# 1

通过身份验证、授权、每个 ESXi 主机上的防火墙等大量功能，vSphere 环境的组件安装即可确保安全。您可以通过多种方式修改默认设置。例如，您可以设置 vCenter Server 对象的权限、打开防火墙端口或更改默认证书。可以针对不同 vSphere 对象采取安全措施，例如，vCenter Server 系统、ESXi 主机、虚拟机以及网络 and 存储对象。

您可以关注 vSphere 各领域的高级别概述，这有助于规划安全策略。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 Hypervisor 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
- 在 vSphere 环境中保护密码
- vCenter Server 和 ESXi 安全最佳做法与资源

## 确保 ESXi Hypervisor 安全

ESXi Hypervisor 安装时即受到安全保护。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。为了保持一致性，您可以设置引用主机，并将所有主机与引用主机的主机配置文件保持同步。也可以通过执行脚本式管理保护您的环境，以便确保将更改应用到所有主机。

您可以通过以下操作提高对 vCenter Server 管理的 ESXi 主机的保护。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《vSphere 单台主机管理 - VMware Host Client》文档。

### 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。您可以从管理主机的 vCenter Server 系统中设置对主机对象的权限。

请参见使用 [ESXi Shell](#)。

## 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。不允许管理员使用 root 用户帐户登录 ESXi 主机，而是从 vCenter Server 创建指定管理员用户，并为这些用户分配管理员角色。您还可以为这些用户分配自定义角色。请参见[创建 vCenter Server 自定义角色](#)。

如果在主机上直接管理用户，则角色管理选项受限制。请参见《vSphere 单台主机管理 - VMware Host Client》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 Client 或 ESXCLI 或 PowerCLI 命令检查和管理防火墙端口状态。

请参见[配置 ESXi 防火墙](#)。

## 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所有主机。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 ESXi 主机配置设置](#)和《vCenter Server 安装和设置》文档。

## 使用 ESXi 锁定模式

在锁定模式下，默认只能通过 vCenter Server 访问 ESXi 主机。可以选择严格锁定模式或正常锁定模式。可以定义例外用户以允许直接访问服务帐户（如备份代理）。

请参见在[ESXi 主机上配置和管理锁定模式](#)。

## 检查 VIB 软件包完整性

每个 vSphere 安装包 (VIB) 均有关联的接受级别。只有在 VIB 接受级别与主机的接受级别相同或比其更高时，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[管理 ESXi 主机和 vSphere 安装包的接受级别](#)。

## 管理 ESXi 证书

默认情况下，VMware Certificate Authority (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或企业证书颁发机构签名的证书。

请参见[管理 ESXi 主机的证书](#)。

## 为 ESXi 考虑使用智能卡身份验证

ESXi 支持使用智能卡身份验证，而不是用户名和密码身份验证。vCenter Server 还支持双因素身份验证。您可以同时配置用户名和密码身份验证以及智能卡身份验证。

请参见 [ESXi 配置和管理智能卡身份验证](#)。

## 考虑使用 ESXi 帐户锁定

对于通过 SSH 和通过 vSphere Web Services SDK 进行的访问，支持帐户锁定。默认情况下，最多允许 5 次尝试，当这些尝试均失败后，便会锁定帐户。默认情况下，帐户将在 15 分钟后解锁。

---

**注** 直接控制台界面 (DCUI) 和 ESXi Shell 不支持帐户锁定。

---

请参见 [ESXi 密码和帐户锁定](#)。

## 确保 vCenter Server 系统及关联服务安全

通过 vCenter Single Sign-On 进行身份验证并通过 vCenter Server 权限模型进行授权，可保护 vCenter Server 系统和关联的服务。您可以修改默认行为，且可以采取的措施来限制对环境的访问。

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，您可能保护多个 vCenter Server 实例。

## vCenter Server 使用加密通信

默认情况下（“开箱即用”时），vCenter Server 系统与其他 vSphere 组件之间的所有数据通信均会进行加密。在某些情况下，根据环境的配置方式，一些流量可能未加密。例如，可以为电子邮件警示配置未加密的 SMTP，为监控配置未加密的 SNMP。DNS 流量也未加密。vCenter Server 侦听端口 80 (TCP) 和端口 443 (TCP)。端口 443 (TCP) 是行业标准的 HTTPS（安全 HTTP）端口，并使用 TLS 1.2 加密进行保护。端口 80 (TCP) 是行业标准的 HTTP 端口，不使用加密。端口 80 的用途是将请求从端口 80 重定向到端口 443，以确保这些请求的安全。

## 强化 vCenter Server 系统

保护 vCenter Server 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 vSphere 证书模型

默认情况下，VMware Certificate Authority (VMCA) 将为环境中的每个 ESXi 主机以及每台计算机置备 VMCA 签名的证书。如果您的公司策略需要，可以更改默认行为。有关详细信息，请参见《vSphere 身份验证》文档。

如需其他保护，请明确移除过期或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。首次安装软件时，为 vCenter Single Sign-On 域的管理员（默认为 administrator@vsphere.local）指定密码。仅该域最初可用作标识源。可以添加外部身份提供程序进行联合身份验证，如 Microsoft Active Directory 联合身份验证服务 (AD FS)。您可以添加其他标识源（Active Directory 或 LDAP），并设置默认标识源。能够向其中任一标识源进行身份验证的用户可以查看对象并执行任务（如果拥有相关权限）。有关详细信息，请参见《vSphere 身份验证》文档。

## 向指定用户或组分配 vCenter Server 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 权限模型提供了出色的灵活性，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 vCenter Server 特权](#)。

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。

## 设置精确时间协议或网络时间协议

为环境中的每个节点设置精度时间协议 (PTP) 或网络时间协议 (NTP)。vSphere 证书基础架构需要准确的时间戳，如果节点不同步，则无法正常工作。

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虚拟环境，就像保护物理机一样。请考虑停用不必要的功能，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。

## 停用不必要的虚拟机功能

检查是否已停用不必要的功能，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停用状态。移除不必要的硬件并停用某些功能（如主机客户机文件系统 (HGFS)），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[停用虚拟机中不必要的功能](#)。

## 使用虚拟机模板和脚本化管理

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 PowerCLI 脚本。本文档主要介绍如何使用 vSphere Client 执行任务。请考虑使用脚本而非 vSphere Client 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》文档。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。

## 考虑虚拟机的 UEFI 安全引导

可以将虚拟机配置为使用 UEFI 引导。如果操作系统支持 UEFI 安全引导，则可以为虚拟机选择该选项以获取其他安全性。请参见[为虚拟机激活或停用 UEFI 安全引导](#)。

## 考虑使用 Carbon Black Cloud Workload

您可以安装并使用 Carbon Black Cloud 工作负载来识别风险、防止攻击并检测异常活动。由于 AppDefense 功能内置于 Carbon Black Cloud 平台中，Carbon Black Cloud Workload 是 AppDefense 的后继产品。

## 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）的安全。此外，请考虑以下准则，这些准则将在[第 13 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。确保管理网络仅供系统、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。对于 ESXi 主机，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防火墙。

您也可以明确打开 vCenter Server 实例上的端口。

有关 VMware 产品（包括 vSphere 和 vSAN）中所有受支持的端口和协议的列表，请参见 <https://ports.vmware.com/> 中的 VMware Ports and Protocols Tool™。您可以按 VMware 产品搜索端口，创建自定义端口列表，以及打印或保存端口列表。

## 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

用于确保虚拟机网络连接安全的方法取决于多种因素，包括：

- 安装的客户机操作系统
- 虚拟机是否在受信任的环境中运行

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提供的保护作用非常显著。

请参见第 13 章 [确保 vSphere 网络安全](#)。

## 考虑使用 VLAN 保护您的环境

ESXi 支持 IEEE 802.1q VLAN。通过 VLAN，可对物理网络进行分段。可以使用 VLAN 为虚拟机网络或存储配置提供进一步保护。使用 VLAN 时，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、应用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，如果您使用的是 iSCSI 存储，则可以将您的环境设置为使用 Challenge Handshake Authentication Protocol (CHAP)。如果公司策略要求，可以设置双向 CHAP。使用 vSphere Client 或 CLI 设置 CHAP。

请参见 [存储安全性最佳做法](#)。

## 评估 Internet 协议安全的使用

ESXi 支持 IPv6 上的 Internet 协议安全 (IPSec)。不能使用 IPv4 上的 IPSec。

请参见在 [ESXi 主机上使用 Internet 协议安全](#)。



## 在 vSphere 环境中保护密码

vSphere 环境中的密码限制、密码过期和帐户锁定取决于用户的目标系统、用户身份以及策略设置。

ESXi 密码限制由某些要求所决定。请参见 [ESXi 密码和帐户锁定](#)。

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、密码过期和帐户锁定取决于用户的域和用户的身份。

### vCenter Single Sign-On 管理员的密码

如果在安装期间选择了不同的域，则 `administrator@vsphere.local` 用户或 `administrator@mydomain` 用户的密码不会过期，并且不受锁定策略的限制。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。有关详细信息，请参见《vSphere 身份验证》文档。

如果忘记此用户的密码，请搜索 VMware 知识库系统，了解有关重置密码的信息。重置需要其他特权，例如对 vCenter Server 系统的 root 访问权限。

### vCenter Single Sign-On 域其他用户的密码

其他 `vsphere.local` 用户的密码或安装期间指定域的用户密码必须遵循 vCenter Single Sign-On 密码策略和锁定策略设置的限制。有关详细信息，请参见《vSphere 身份验证》文档。默认情况下，这些密码将在 90 天后过期。作为密码策略的一部分，管理员可以更改过期时间。

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

### 其他标识源中用户的密码

所有其他用户的密码限制、密码过期和帐户锁定由用户对其进行身份验证的域（标识源）决定。

vCenter Single Sign-On 支持一个默认标识源。用户可以通过 vSphere Client 使用其用户名登录到相应的域。如果用户希望登录到非默认域，用户可以包括该域名，即，指定 `user@domain` 或 `domain\user`。域密码参数适用于每个域。

### vCenter Server 直接控制台用户界面用户的密码

vCenter Server Appliance 是针对运行 vCenter Server 及关联服务而优化的预配置虚拟机。

部署 vCenter Server 时，指定这些密码。

- root 用户的密码。
- vCenter Single Sign-On 域管理员（默认为 `administrator@vsphere.local`）的密码。

可以从 vCenter Server 管理界面更改 root 用户密码并执行其他 vCenter Server 本地用户管理任务。请参见《vCenter Server 配置》文档。

## vCenter Server 和 ESXi 安全最佳做法与资源

如果您按照最佳做法进行操作，ESXi 主机和 vCenter Server 系统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。本手册只是必须用于确保环境安全的其中一种资源。

### vSphere 安全资源

要了解有关特定 vSphere 安全方面的更多信息，请使用本手册中的以下内容。

表 1-1. 安全性最佳做法

vSphere 组件	资源
ESXi 主机	<a href="#">第 3 章 确保 ESXi 主机安全</a>
vCenter Server 系统	<a href="#">第 4 章 确保 vCenter Server 系统安全</a>
虚拟机	<a href="#">虚拟机安全性最佳做法</a>
vSphere 网络连接	<a href="#">vSphere 网络连接安全性最佳做法</a>

### Web 上的 VMware 安全资源

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
ESXi 和 vCenter Server 安全性和操作相关信息，包括安全配置和 Hypervisor 安全性。	<a href="https://core.vmware.com/security">https://core.vmware.com/security</a>
VMware 安全策略、最新安全警示、安全下载及安全主题重点讨论。	<a href="http://www.vmware.com/go/security">http://www.vmware.com/go/security</a>
公司安全响应策略	<a href="http://www.vmware.com/support/policies/security_response.html">http://www.vmware.com/support/policies/security_response.html</a> 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	<a href="http://www.vmware.com/support/policies/">http://www.vmware.com/support/policies/</a> 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 <a href="http://www.vmware.com/vmtn/resources/">http://www.vmware.com/vmtn/resources/</a> 搜索 ESXi 兼容性指南，找到支持 ESXi 的代理、工具及其他软件列表。 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	<a href="https://core.vmware.com/compliance">https://core.vmware.com/compliance</a>
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。	<a href="https://www.vmware.com/support/support-resources/certifications.html">https://www.vmware.com/support/support-resources/certifications.html</a>



表 1-2. Web 上的 VMware 安全资源（续）

主题	资源
针对不同 vSphere 版本和其他 VMware 产品的安全性配置指南（以前称为强化指南）。	<a href="https://core.vmware.com/security-configuration-guide">https://core.vmware.com/security-configuration-guide</a>
《VMware vSphere Hypervisor 的安全性》白皮书	<a href="http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf">http://www.vmware.com/files/pdf/techpaper/vmw-wp-secrty-vsphr-hyprvsr-uslet-101.pdf</a>

# vSphere 权限和用户管理任务

## 2

身份验证和授权控制对 vSphere 环境的访问。vCenter Single Sign-On 支持身份验证，这表明它可以确定用户究竟是否能够登录 vSphere 组件。每个用户还必须获得授权，才能查看或操作 vSphere 对象。

有关使用 vSphere Client 分配角色和权限的概览，请观看以下视频。



(使用 vSphere Client 分配角色和权限)

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，仅 vCenter Single Sign-On 域的管理员用户有权登录到 vCenter Server 系统。默认域为 vsphere.local，默认管理员为 administrator@vsphere.local。您可以在安装 vSphere 期间更改默认域。

作为管理员用户，您可以：

- 1 将在其中定义了用户和组的标识源添加到 vCenter Single Sign-On 中。请参见《vSphere 身份验证》文档。
- 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。

本章讨论了以下主题：

- 了解 vSphere 中的授权
- 多个权限设置在 vSphere 中如何工作
- 管理 vCenter Server 组件的权限
- 使用 vCenter Server 全局权限
- 使用 vCenter Server 角色分配特权
- 针对 vCenter Server 角色和权限的最佳做法
- 常见任务的所需 vCenter Server 特权

## 了解 vSphere 中的授权

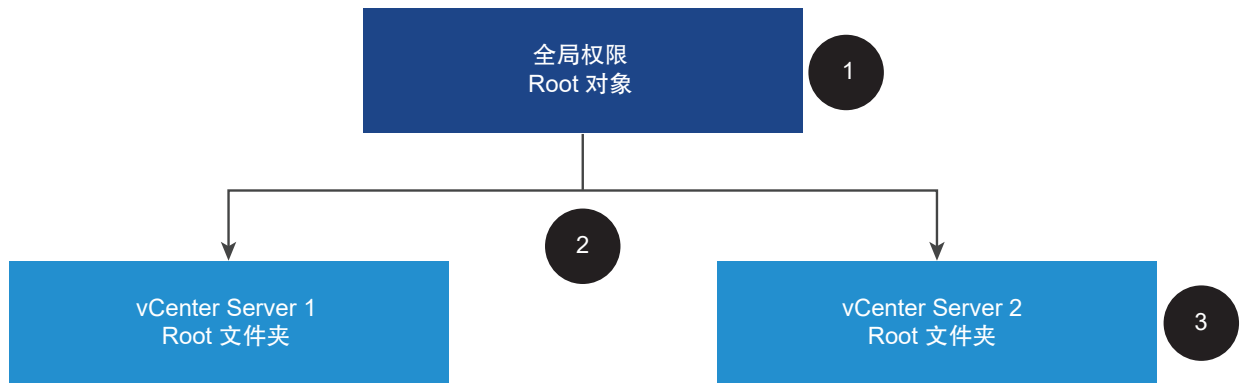
vSphere 支持多种模型，用于确定是否允许用户执行某项任务。vCenter Single Sign-On 组中的组成员资格决定了允许您执行的操作。您对某个对象具有的角色或全局权限决定了是否允许您执行其他任务。

### 权限在 vSphere 中如何工作

vSphere 允许有特权的用户授予其他用户执行任务的权限。可以使用全局权限，也可以使用本地 vCenter Server 权限以授权其他用户处理各个 vCenter Server 实例。

下图说明了全局权限和本地权限的工作方式。

图 2-1. 全局权限和本地权限



在此图中：

- 1 您可以在根对象级别分配全局权限并选择“传播到子对象”。
- 2 vCenter Server 将权限传播到环境中的 vCenter Server 1 和 vCenter Server 2 对象层次结构。
- 3 vCenter Server 2 中根文件夹的本地权限会覆盖全局权限。

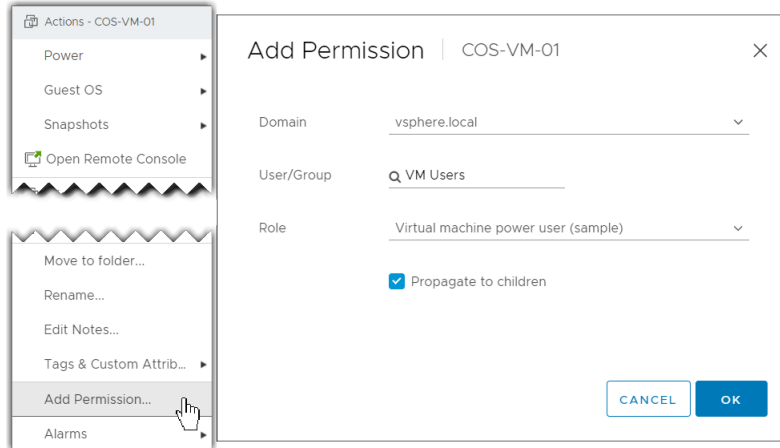
### vCenter Server 权限

vCenter Server 系统的权限模型需要向对象层次结构中的对象分配权限。用户可通过以下方式获取权限。

- 来自用户或用户所属组的特定权限
- 来自对象的权限或通过父对象的权限继承

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。您可以使用 vSphere Client 添加权限。例如，您可以右键单击虚拟机，选择**添加权限**，然后完成对话框，为一组用户分配角色。该角色授予这些用户对该虚拟机的相应特权。

图 2-2. 使用 vSphere Client 向虚拟机添加权限



## 全局权限

全局权限向用户和组提供查看或管理部署中解决方案的每个清单层次结构中所有对象的特权。也就是说，全局权限将应用于跨多个解决方案清单层次结构的全局根对象。（解决方案包括 vCenter Server、vRealize Orchestrator 等。）全局权限还将应用于全局对象，如标记和内容库。例如，考虑包含两个解决方案（vCenter Server 和 vRealize Orchestrator）的部署。您可以使用全局权限向一组用户分配角色，该用户组对 vCenter Server 和 vRealize Orchestrator 对象层次结构中的所有对象具有只读特权。

将跨 vCenter Single Sign-On 域（默认为 vsphere.local）复制全局权限。全局权限不会为通过 vCenter Single Sign-On 域组管理的服务提供授权。请参见[使用 vCenter Server 全局权限](#)。

## vCenter Single Sign-On 组中的组成员资格

vCenter Single Sign-On 域组的成员可以执行特定任务。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 身份验证》文档。

## 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《vSphere 单台主机管理 - VMware Host Client》文档。

对于受管主机，请向 vCenter Server 清单中的 ESXi 主机对象分配角色。

## 了解对象级别权限模型

您授权用户或组使用对象上的权限在 vCenter Server 对象上执行任务。从编程角度来看，当用户尝试执行操作时，将执行 API 方法。vCenter Server 将检查该方法的权限，以查看用户是否有权执行操作。例如，当用户尝试添加主机时，会调用 AddStandaloneHost\_Task 方法。此方法要求用户的角色具有 Host.Inventory.AddStandaloneHost 特权。如果检查未找到此特权，则用户添加主机的权限将被拒绝。

以下概念非常重要。

## 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。权限可以传播到子对象。

## 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 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。

## 特权

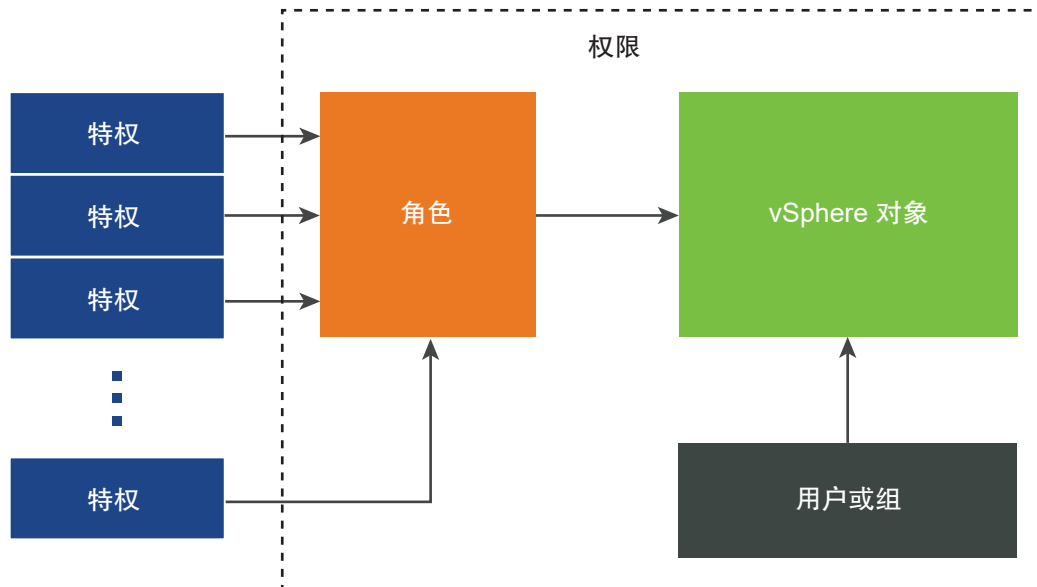
特权是精细的访问控制。可以将这些特权分组到角色中，然后可以将其映射到用户或组。

## 角色

角色是指一组特权。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。系统角色（例如管理员）已在 vCenter Server 中预定义，不能更改。vCenter Server 还提供了一些可以修改的默认示例角色，例如，资源池管理员。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。请参见[创建 vCenter Server 自定义角色](#)。

下图说明了如何根据特权和角色构造权限，以及如何将权限分配给 vSphere 对象的用户或组。

图 2-3. vSphere 权限



要向对象分配权限，请执行以下步骤：

- 1 在 vCenter Server 对象层次结构中选择要应用权限的对象。
- 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各种特权或某个角色（即一组特权）。

默认情况下，未选择“传播到子对象”。必须选中该复选框，组或用户才能具有选定对象及其子对象的选定角色。

vCenter Server 提供合并了常用权限集的示例角色。也可通过合并一组角色创建自定义角色。

通常，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，您需要针对该虚拟机的特权，同时还需要针对目标数据中心的特权。

请参见下面的信息。

要了解...	请参见...
创建自定义角色。	<a href="#">创建 vCenter Server 自定义角色</a>
所有特权以及可对其应用特权的对象	<a href="#">第 16 章 定义的特权</a>
对不同对象执行不同任务所需的特权集。	<a href="#">常见任务的所需 vCenter Server 特权</a>

独立 ESXi 主机的权限模型比较简单。请参见[为 ESXi 主机分配特权](#)。

## 什么是 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，假设为用户 Smith 分配了对多个对象的角色，域管理员将该名称更改为 Smith2，下次进行验证时主机将认为 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。

## vSphere 中的权限层级继承

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。

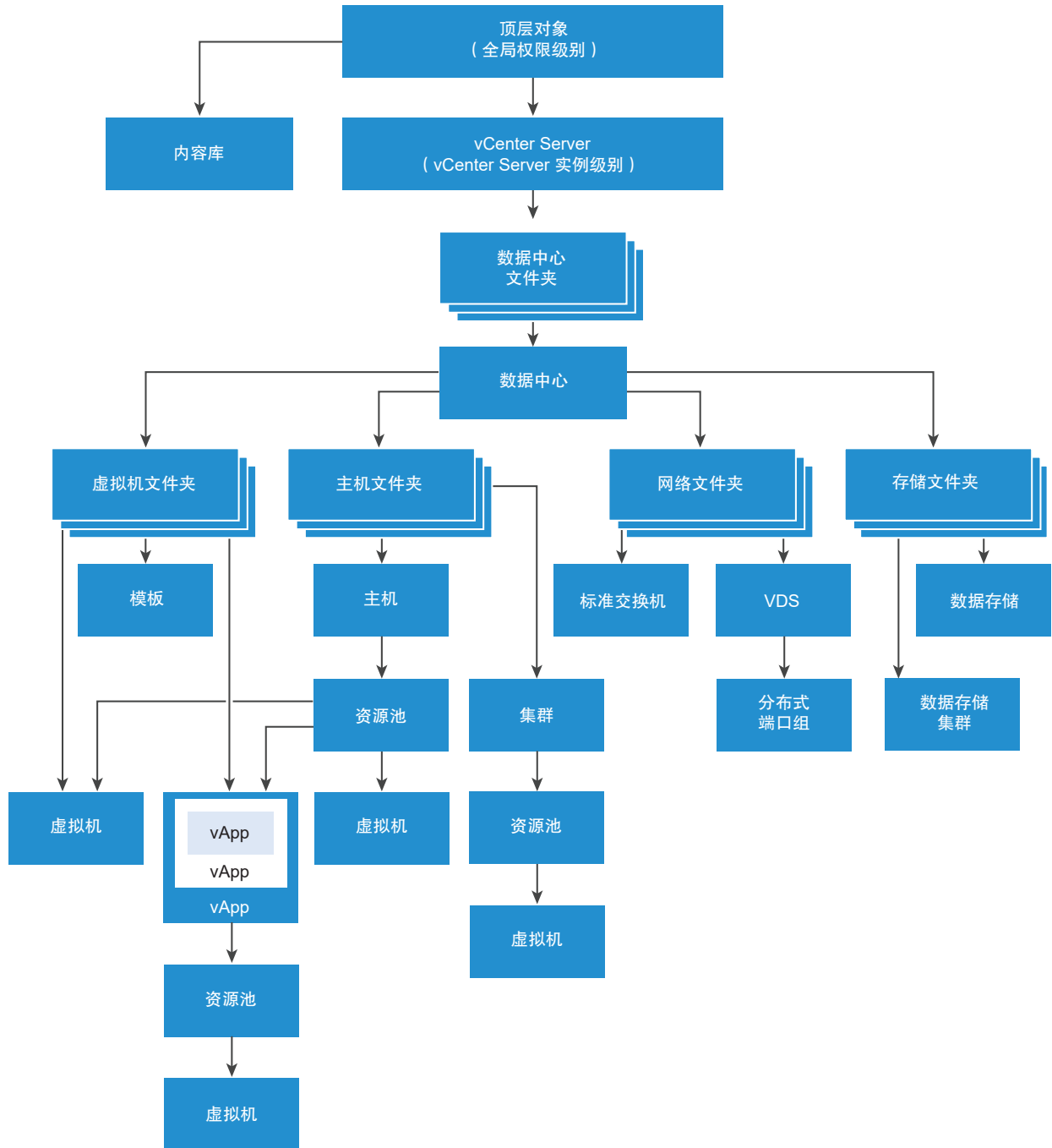
下图说明了清单层次结构和权限传播的路径。

---

**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[使用 vCenter Server 全局权限](#)。

---

图 2-4. vSphere 清单层次结构



关于此图：

- 您不能对虚拟机、主机、网络 and 存储文件夹设置直接权限。也就是说，这些文件夹充当容器，因此对用户不可见。
- 您无法对标准交换机设置权限。

**注** 为了能够设置权限并将其传播到 vSphere Distributed Switch (VDS) 上的子项，交换机对象必须驻留在数据中心上创建的网络文件夹中。

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

受管实体指的是以下 vSphere 对象。受管实体提供的特定操作因实体类型而异。特权用户可以对受管实体定义权限。有关 vSphere API 对象、属性和方法的详细信息，请参见 vSphere API 文档。

- 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

## 多个权限设置在 vSphere 中如何工作

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 GroupAdmin 对某个对象具有管理员角色。另一种权限可能指定 GroupVMAdmin 对同一个对象具有虚拟机管理员角色。但是，GroupVMAdmin 组不能对该对象具有同一个 GroupVMAdmin 的其他权限。



如果父对象传播属性设置为 **true**，则子对象将继承其父对象的权限。直接在子对象上设置的权限将取代父对象中的权限。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角色，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：

- 没有任何用户权限是直接对象上定义的。在这种情况下，用户拥有各组对该对象所拥有权限的集合。
- 用户的权限是直接对象上定义的。在这种情况下，用户的权限将优先于所有组权限。

## 示例 1：从多个组继承权限

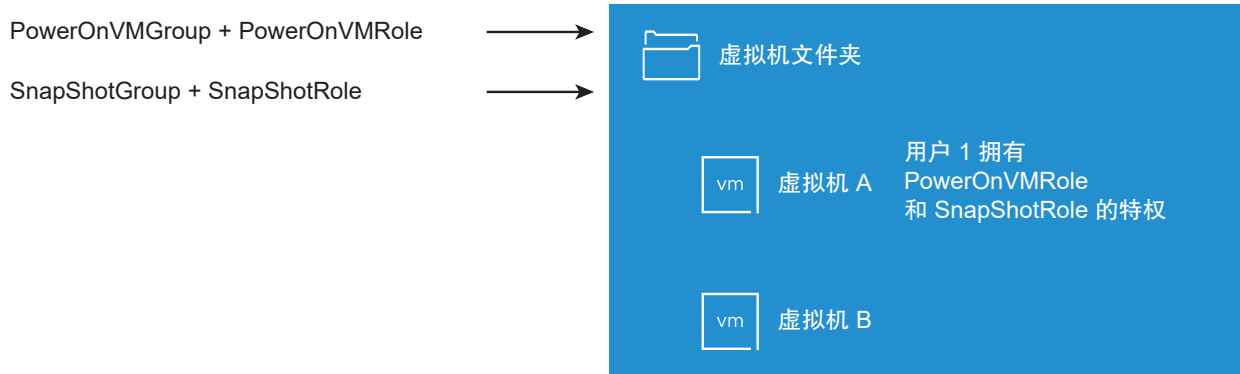
此示例说明了对象如何从组（在父对象上授予了权限）中继承多个权限。

在此示例中，为两个不同组中的同一对象分配两种权限。

- **PowerOnVMRole** 可启动虚拟机。
- **SnapshotRole** 可以拍摄虚拟机快照。
- 在虚拟机文件夹上为 **PowerOnVMGroup** 授予 **PowerOnVMRole**，并将权限设置为传播到子对象。
- 在虚拟机文件夹上为 **SnapshotGroup** 授予 **SnapshotRole**，并将权限设置为传播到子对象。
- 用户 1 未获得特定特权。

同时属于 **PowerOnVMGroup** 和 **SnapshotGroup** 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 2-5. 示例 1：从多个组继承权限



## 示例 2：子权限替代父权限

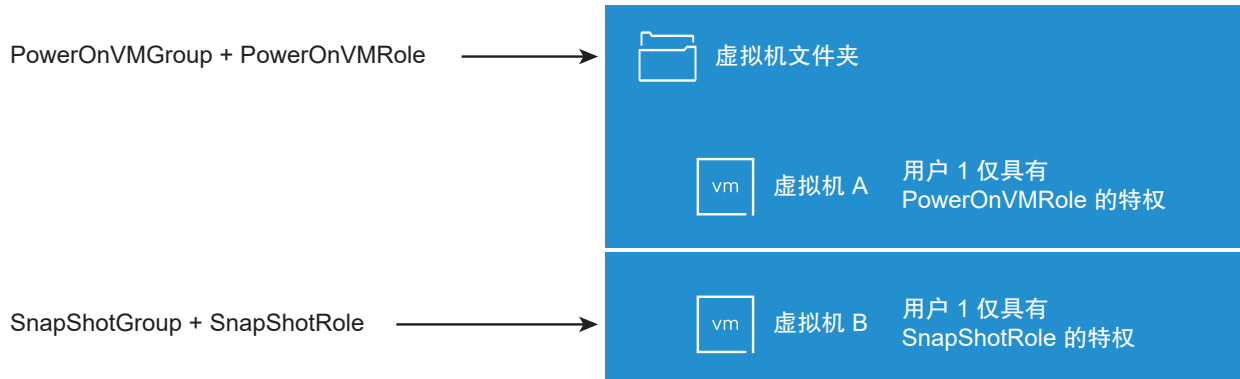
此示例说明了为子对象分配的权限如何覆盖为父对象分配的权限。可以使用此替代行为限制用户访问清单的特定区域。

在此示例中，权限在两个不同组的两个不同对象上定义。

- **PowerOnVMRole** 可启动虚拟机。
- **SnapshotRole** 可以拍摄虚拟机快照。
- 在虚拟机文件夹上为 **PowerOnVMGroup** 授予 **PowerOnVMRole**，并将权限设置为传播到子对象。
- 在虚拟机 B 上为 **SnapshotGroup** 授予 **SnapshotRole**。

同时属于 PowerOnVMGroup 和 SnapShotGroup 的用户 1 登录。因为在层次结构中，SnapShotRole 被分配在 PowerOnVMRole 之下，所以它将在虚拟机 B 上替代 PowerOnVMRole。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 2-6. 示例 2：子权限替代父权限



### 示例 3：用户角色替代组角色

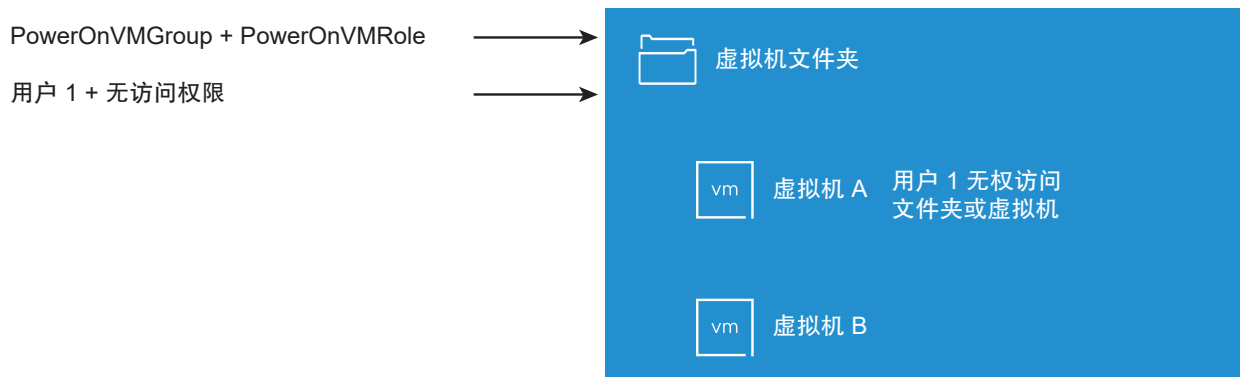
下例说明了直接分配给单个用户的角色如何替代与分配给组的角色关联的特权。

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。

- PowerOnVMRole 可启动虚拟机。
- 在虚拟机文件夹上为 PowerOnVMGroup 授予 PowerOnVMRole。
- 在虚拟机文件夹上为用户 1 授予 NoAccess 角色。

属于 PowerOnVMGroup 的用户 1 登录。在虚拟机文件夹上为用户 1 授予的 NoAccess 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 和虚拟机 B。虚拟机 A 和 B 在层次结构中对用户 1 不可见。

图 2-7. 示例 3：用户权限替代组权限



## 管理 vCenter Server 组件的权限

在 vCenter Server 对象层次结构中的对象上设置权限。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 授予只读角色，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。

有关权限的概念信息，请参见[了解对象级别权限模型](#)中的讨论。

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[vSphere 中的权限层级继承](#)。还可以向全局根对象分配传播权限，以将权限应用于所有解决方案中的所有对象。请参见[使用 vCenter Server 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，可以同时为相同的传播权限分配给多个对象。

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 Client 对象导航器中，浏览到要为其分配权限的对象。
- 2 单击**权限**选项卡。
- 3 单击**添加**。
- 4 （可选）如果为联合身份验证配置了外部身份提供程序，则可以在**域**下拉菜单中选择该身份提供程序的域。
- 5 选择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，选择用户或组所在域。
  - b 在“搜索”框中输入名称。  
系统将搜索用户名和组名称。
  - c 选择用户或组。
- 6 从**角色**下拉菜单中选择角色。
- 7 （可选）要传播权限，请选中**传播到子对象**复选框。  
角色将应用于选定对象，并传播到子对象。
- 8 单击**确定**。

## 更改或删除清单对象的权限

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**传播到子项**复选框的设置。还可移除权限设置。

### 步骤

- 1 在 vSphere Client 对象导航器中，浏览到对象。
- 2 单击**权限**选项卡。
- 3 单击某行以选择权限。

任务	步骤
更改权限	<ol style="list-style-type: none"> <li>a 单击<b>编辑</b>。</li> <li>b 从<b>角色</b>下拉菜单中为用户或组选择一个角色。</li> <li>c 切换<b>传播到子项</b>复选框以更改权限继承。</li> <li>d 单击<b>确定</b>。</li> </ol>
移除权限	<ol style="list-style-type: none"> <li>a 单击<b>删除</b>。</li> <li>b 单击<b>移除</b>。</li> </ol>

## 更改 vCenter Server 用户验证设置

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。可以停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。

这些设置适用于 vCenter Single Sign-On 标识源，而不是可能与 vCenter Server 关联的外部标识源，例如 Active Directory。

**注** 此步骤仅适用于 vCenter Server 用户列表。您无法以相同的方式搜索 ESXi 用户列表。

### 步骤

- 1 在 vSphere Client 对象导航器中，浏览到 vCenter Server 系统。
- 2 选择**配置**，然后单击**设置 > 常规**。
- 3 单击**编辑**，然后选择**用户目录**。
- 4 根据需要更改值，然后单击**保存**。

选项	描述
用户目录超时	搜索此 vCenter Server 安装的超时时间间隔（以秒为单位）。
查询限制	启用此选项可设置 vCenter Server 显示的最大用户和组数目。
查询限制大小	在 <b>选择用户或组</b> 对话框中 vCenter Server 显示所选域中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。

## 使用 vCenter Server 全局权限

在 vCenter Server 中，全局权限应用到跨多个 VMware 解决方案的全局根对象。在内部部署 SDDC 中，全局权限可能同时跨 vCenter Server 和 vRealize Orchestrator。但是，对于任何 vSphere SDDC，全局权限将应用于全局对象，如标记和内容库。

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。角色确定用户或组针对层次结构中所有对象所具有的一组特权。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 vCenter Server 角色分配特权](#)。

重要的是对 vCenter Server 权限与全局权限加以区分。

**表 2-1. vCenter Server 权限与全局权限之间的差异**

权限类型	描述
vCenter Server	vCenter Server 权限适用于清单层次结构中的特定对象，如主机、虚拟机、数据存储等。分配 vCenter Server 权限时，指定拥有对象角色（特权集）的用户或组。
全局	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。全局权限还将应用于全局对象，如标记和内容库。请参见 <a href="#">标记对象的 vCenter Server 权限</a> 。 如果分配了全局权限但未选择“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。

## 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。

**重要说明** 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 使用 vSphere Client 登录 vCenter Server。
- 2 选择**系统管理**，然后在“访问控制”区域中单击**全局权限**。
- 3 从**权限提供程序**下拉菜单中选择域。
- 4 （可选）如果为联合身份验证配置了外部身份提供程序，则可以在**域**下拉菜单中选择该身份提供程序的域。
- 5 单击**添加**。

## 6 选择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，选择用户或组所在域。

b 在“搜索”框中输入名称。

系统将搜索用户名和组名称。

c 选择用户或组。

## 7 从**角色**下拉菜单中选择角色。

## 8 通过选中**传播到子对象**复选框，决定是否传播权限。

如果分配了全局权限但未选中**传播到子对象**，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。

## 9 单击**确定**。

# 标记对象的 vCenter Server 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 顶层创建的。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（例如虚拟机）上的某个用户，则该用户可以执行与该权限相关的任务。但是，用户无法对对象执行标记操作。

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 必须拥有顶层的**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 2-2. 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 <b>分配或取消分配 vSphere 标记</b> 特权。	Dana 在 ESXi 主机 TPA 上拥有 <b>删除 vSphere 标记</b> 特权。	Dana 拥有标记的 <b>分配或取消分配 vSphere 标记</b> 特权。
Dana 拥有 <b>分配或取消分配 vSphere 标记</b> 特权。	未分配标记特权。	Dana 在 ESXi 主机 TPA 上拥有 <b>删除 vSphere 标记</b> 特权。	Dana 拥有 <b>分配或取消分配 vSphere 标记</b> 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 <b>分配或取消分配 vSphere 标记</b> 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，即在顶层对象上分配的权限，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，假设您在顶层使用全局权限向用户 Robin 分配了**删除 vSphere 标记**特权。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”拥有特权，因为 Robin 拥有全局权限，而全局权限可从顶层传播。除非修改全局权限，否则您无法限制特权。

表 2-3. 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 <b>删除 vSphere 标记</b> 特权	Robin 没有标记的 <b>删除 vSphere 标记</b> 特权。	Robin 拥有 <b>删除 vSphere 标记</b> 特权。
未分配标记特权	Robin 没有针对标记分配的 <b>删除 vSphere 标记</b> 特权。	Robin 没有 <b>删除 vSphere 标记</b> 特权

## 标记级别权限可以扩展全局权限

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。

**注** 此行为与继承 vCenter Server 特权的方式不同。在 vCenter Server 中，为子对象定义的权限将总是替代从父对象中传播的权限。

表 2-4. 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 <b>分配或取消分配 vSphere 标记</b> 特权。	Lee 拥有 <b>删除 vSphere 标记</b> 特权。	Lee 拥有标记的 <b>分配 vSphere 标记</b> 特权和 <b>删除 vSphere 标记</b> 特权。
未分配标记特权。	Lee 拥有针对标记分配的 <b>删除 vSphere 标记</b> 特权。	Lee 拥有标记的 <b>删除 vSphere 标记</b> 特权。

## 使用 vCenter Server 角色分配特权

在 vCenter Server 中，角色是一组预定义的特权，用于定义执行操作和读取属性的权限。通过将角色分配给对象的用户或组来创建权限。默认情况下，vCenter Server 可提供系统角色和样本角色。也可创建自定义角色。

## 在 vCenter Server 中分配权限

在 vCenter Server 中分配权限时，可将用户或组与角色配对，并将该配对与清单对象关联。例如，可以使用虚拟机用户样本角色允许用户读取和更改虚拟机属性。

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，假设清单中有两个资源池（池 A 和池 B）。您可以为组 Sales 在池 A 上分配虚拟机用户样本角色，而在池 B 上分配只读角色。执行上述分配后，组 Sales 中的用户可以打开池 A 中的虚拟机，但只能查看池 B 中的虚拟机。

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。

## 什么是预定义的 vCenter Server 角色

如下表所示，vCenter Server 提供预定义的角色。

表 2-5. 预定义的 vCenter Server 角色

角色类型	角色名称	描述
系统	管理员、只读和无权访问。	系统角色是永久的。您无法删除系统角色，也无法编辑与这些角色关联的特权。系统角色按层次结构进行组织。每个角色都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。有关系统角色的更多详细信息，请参见以下部分。
样本	vSphere 提供了许多样本角色，例如 AutoUpdateUser、资源池管理员和虚拟机用户。	vSphere 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。  <b>注</b> 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。

要查看与某个角色关联的特权，请在 vSphere Client 中导航到该角色（**菜单 > 系统管理 > 角色**），然后单击**特权**选项卡。

要查看所有 vSphere 特权和描述，请参见第 16 章 定义的特权。

**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 系统角色

无法修改或删除系统角色。

### 管理员角色

具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的所有特权。如果您在某个对象上具有管理员角色，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。有关支持的身份服务，请参见《vSphere 身份验证》文档。

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。

**提示** 最佳做法是在 root 级别创建一个用户并向其分配管理员角色。创建一个具有管理员特权的指定用户后，可以移除 root 用户的所有权限或将其角色更改为“无权访问”。

### 只读角色

具有“只读”角色的对象用户可查看对象的状态和详细信息。例如，具有此角色的用户可查看虚拟机、主机和资源池属性，但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。

### 无权访问角色

具有“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。



vCenter Single Sign-On 域的管理员（默认为 administrator@vsphere.local）、root 用户和 vpxuser 默认分配有管理员角色。其他用户默认分配有“无权访问”角色。

## 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 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 VMware Host Client 为各个主机创建自定义角色。请参见《vSphere 单台主机管理 - VMware Host Client》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，请勿保留主机和 vCenter Server 中的自定义角色。在 vCenter Server 级别定义角色。

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** 如果您添加自定义角色而不向其分配任何特权，则该角色将创建为只读角色，且具有以下三个系统定义的特权：**系统.匿名**、**系统.查看**和**系统.读取**。这些特权在 vSphere Client 中不显示，但用于读取某些受管对象的某些属性。vCenter Server 中的所有预定义角色都包含这三个系统定义的特权。有关详细信息，请参见《vSphere Web Services API》。

---

## 创建 vCenter Server 自定义角色

为了满足环境的访问控制需求，可以创建 vCenter Server 自定义角色。可以创建角色或克隆现有角色。

您可以在与其他 vCenter Server 系统属于同一个 vCenter Single Sign-On 域的 vCenter Server 系统上创建或编辑角色。VMware Directory Service (vmdir) 会将您所做的角色更改传播到组中的所有其他 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

验证您对创建角色所在的 vCenter Server 系统是否拥有管理员特权。

### 步骤

- 1 使用 vSphere Client 登录 vCenter Server。
- 2 选择**系统管理**，然后在**访问控制**区域中单击**角色**。

### 3 创建角色。

选项	描述
创建角色	<p>a 单击<b>新建</b>。</p> <p>b 输入新角色的名称。</p> <p>c 选择和取消选择角色的特权。</p> <p>滚动特权类别，然后为该类别选择所有特权或一部分特权。可以显示所有、已选择或未选择的类别。还可以显示所有、已选择或未选择的特权。有关详细信息，请参见第 16 章 定义的特权。</p> <p>d 单击<b>创建</b>。</p>
通过克隆创建角色	<p>a 选择角色，然后单击<b>克隆</b>。</p> <p>b 输入角色的名称。</p> <p>c 单击<b>确定</b>。</p> <p><b>注</b> 创建克隆的角色时，无法更改特权。要更改特权，请选择克隆的角色，然后单击<b>编辑</b>。</p>

#### 后续步骤

现在，您可以通过选择对象并将角色分配给该对象的用户或组来创建权限。

## 针对 vCenter Server 角色和权限的最佳做法

遵循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，请遵循以下最佳做法：

- 如果可能，请向组分配角色，而不要向单个用户分配角色。
- 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。使用最少权限数以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。
- 将对象分组到文件夹中，使权限分配变得更加轻松。例如，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。
- 考虑向对象分配权限时启用传播功能。传播可确保对象层次结构中的新对象继承权限。例如，您可以为虚拟机文件夹分配权限并启用传播，以确保该权限适用于该文件夹中的所有虚拟机。
- 使用“无权访问”角色屏蔽层次结构的特定区域。“无权访问”角色会限制具有该角色的用户或组的访问权限。
- 对许可证所做的更改将传播到同一 vCenter Single Sign-On 域中的所有链接 vCenter Server 系统。
- 即使用户并未对所有 vCenter Server 系统拥有特权，也会发生许可证传播。

## 常见任务的所需 vCenter Server 特权

许多任务需要对 vSphere 清单中多个对象的权限。如果尝试执行任务的用户仅具有一个对象的特权，则无法成功完成该任务。

下表列出了需要多个特权的常见任务。您可以通过将用户与某个预定义的角色或多个特权进行配对，为清单对象添加权限。如果您预计必须多次分配一组特权，请创建自定义角色。

请参阅《vSphere Web Services API 参考》，以了解 vSphere Client 用户界面中的操作如何映射到 API 调用，以及执行操作需要哪些特权。例如，AddHost\_Task (addHost) 方法对应的 API 文档规定，向集群添加主机需要拥有 Host.Inventory.AddHostToCluster 特权。

如果要执行的任务不在此表中，以下规则说明了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都需要目标数据存储的**数据存储.分配空间**特权以及用于执行该操作本身的特权。例如，当创建虚拟磁盘或创建快照时，必须具有这些特权。
- 在清单层次结构中移动对象需要对象自身、源父对象（如文件夹或集群）和目标父对象上的适当特权。
- 每个主机和集群有其自身的固有资源池，其中包含该主机或集群的所有资源。将虚拟机直接部署到主机或集群需要**资源.将虚拟机分配给资源池**特权。

表 2-6. 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"> <li>■ <b>虚拟机.编辑清单.新建</b></li> <li>■ <b>虚拟机.更改配置.添加新磁盘</b>（如果要创建新虚拟磁盘）</li> <li>■ <b>虚拟机.更改配置.添加现有磁盘</b>（如果使用现有虚拟磁盘）</li> <li>■ <b>虚拟机.配置.配置裸设备</b>（如果使用 RDM 或 SCSI 直通设备）</li> </ul>	管理员
	在目标主机、集群或资源池上： <b>资源.将虚拟机分配给资源池</b>	资源池管理员或管理员
	在目标数据存储或包含数据存储的文件夹上： <b>数据存储.分配空间</b>	数据存储用户或管理员
	在虚拟机将分配到的网络上： <b>网络.分配网络</b>	网络用户或管理员
打开虚拟机电源	在其中部署虚拟机的数据中心上： <b>虚拟机.交互.打开电源</b>	虚拟机超级用户或管理员
	在虚拟机或虚拟机的文件夹上： <b>虚拟机.交互.打开电源</b>	
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"> <li>■ <b>虚拟机.编辑清单.从现有清单创建</b></li> <li>■ <b>虚拟机.更改配置.添加新磁盘</b></li> </ul>	管理员
	在模板或模板的文件夹上： <b>虚拟机.置备.部署模板</b>	管理员

表 2-6. 常见任务的所需特权（续）

任务	所需特权	适用角色
	在目标主机、集群或资源池上： ■ 资源.将虚拟机分配给资源池 ■ vApp.导入	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： ■ 资源.将虚拟机分配给资源池 ■ 虚拟机.编辑清单.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： ■ 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 介质（如果从 CD 安装） ■ 虚拟机.交互.配置软盘介质（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
	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
	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
通过 vMotion 迁移虚拟机	在目标主机、集群或资源池上（如果与源主机、集群或资源池不同）： 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、集群或资源池上（如果与源主机、集群或资源池不同）： 资源.将虚拟机分配给资源池	资源池管理员或管理员

表 2-6. 常见任务的所需特权（续）

任务	所需特权	适用角色
	在目标数据存储上（如果与源数据存储不同）： <b>数据存储.分配空间</b>	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： <b>资源.迁移已打开电源的虚拟机</b>	资源池管理员或管理员
	在目标数据存储上： <b>数据存储.分配空间</b>	数据存储用户或管理员
将主机移动到集群	在主机上： <b>主机.清单.将主机添加到集群</b>	管理员
	在目标集群上： ■ <b>主机.清单.将主机添加到集群</b> ■ <b>主机.清单.修改集群</b>	管理员
使用 vSphere Client 将单个主机添加到数据中心，或者使用 PowerCLI 或 API（利用 addHost API）将单个主机添加到集群	在主机上： <b>主机.清单.将主机添加到集群</b>	管理员
	在集群上： ■ <b>主机.清单.修改集群</b> ■ <b>主机.清单.将主机添加到集群</b>	管理员
	在数据中心上： <b>主机.清单.添加独立主机</b>	管理员
将多个主机添加到集群	在集群上： ■ <b>主机.清单.修改集群</b> ■ <b>主机.清单.将主机添加到集群</b>	管理员
	在集群的父数据中心（具有传播权限）上： ■ <b>主机.清单.添加独立主机</b> ■ <b>主机.清单.移动主机</b> ■ <b>主机.清单.修改集群</b> ■ <b>主机.配置.维护</b>	管理员
加密虚拟机	只有在包含 vCenter Server 的环境中才能执行加密任务。此外，ESXi 主机必须为大多数加密任务启用加密模式。执行任务的用户必须拥有相应的特权。一组 <b>加密操作</b> 特权可实现精细控制。请参见 <a href="#">虚拟机加密任务的必备条件和必需特权</a> 。	管理员
保护虚拟机（如果使用 vSphere+ 保护虚拟机）	在其中部署虚拟机的数据中心上： ■ <b>vSphere 标记.分配或取消分配 vSphere 标记</b>	管理员

# 确保 ESXi 主机安全

## 3

ESXi Hypervisor 架构具有许多内置安全功能，包括 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，但通常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。ESXi 主机已加入证书基础架构。默认情况下，VMware Certificate Authority (VMCA) 使用以 VMCA 作为根证书颁发机构的签名证书置备新 ESXi 主机。

---

**注** ESXi 并非基于 Linux 内核或商用 Linux 发行版构建。它使用自己的 VMware 专用和专利内核及软件工具，作为独立单元提供，并且不包含 Linux 发行版中的应用程序和组件。

---

本章讨论了以下主题：

- 常规 ESXi 安全建议
- 管理 ESXi 主机的证书
- 自定义 ESXi 主机安全性
- 为 ESXi 主机分配特权
- 使用 Active Directory 管理 ESXi 用户
- 使用 vSphere Authentication Proxy
- 为 ESXi 配置和管理智能卡身份验证
- 使用 ESXi Shell
- ESXi 主机的 UEFI 安全引导
- 使用可信平台模块保护 ESXi 主机
- ESXi 日志文件
- 确保 Fault Tolerance 日志记录通信的安全
- 管理 ESXi 审核记录
- 确保 ESXi 配置安全
- 停用 execInstalledOnly 高级配置运行时选项

## 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。要满足配置需求，您可以放宽限制。如果放宽限制，确保在可信任的环境中使用并采取其他安全措施。

## 什么是 ESXi 内置安全功能

如下所示，ESXi 可降低主机的风险：

- 默认情况下，ESXi Shell 接口和 SSH 接口处于停用状态。除非要执行故障排除或支持活动，否则这些接口应保持停用状态。对于日常活动，请使用 vSphere Client，使活动受制于基于角色的访问控制和现代访问控制方法。
- 默认情况下，只有部分防火墙端口处于打开状态。您可以明确打开与特定服务关联的防火墙端口。
- 默认情况下，对主机进行管理访问时无需使用的所有端口均处于关闭状态。需要其他服务时，可以打开端口。
- 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，弱密码被停用，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 使用内部 Web 服务支持通过 Web Client 进行访问。该服务已修改为只运行 Web Client 进行系统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 Web 服务安全问题。
- VMware 监控可能影响 ESXi 安全的所有安全警示，并根据需要发布安全修补程序。您可以订阅 VMware 安全公告和安全警示邮件列表以接收安全警示。请参见网页，网址为 <http://lists.vmware.com/mailman/listinfo/security-announce>。
- 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。
- 为了防止主机加载未加密签名的驱动程序和应用程序，请使用 UEFI 安全引导。在系统 BIOS 中启用安全引导。不需要在 ESXi 主机上进行其他配置更改，例如，不需要对磁盘分区进行更改。请参见 [ESXi 主机的 UEFI 安全引导](#)。
- 如果 ESXi 主机具有 TPM 2.0 芯片，请在系统 BIOS 中启用并配置该芯片。通过与安全引导协同工作，TPM 2.0 提供增强的安全性和植根于硬件的信任保证。请参见 [使用可信平台模块保护 ESXi 主机](#)。

## 采取更多 ESXi 安全措施

评估主机安全和管理时请考虑以下建议。

### 对 ESXi 主机进行访问限制

如果激活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 ESXi 主机

使用 vSphere Client 来管理受 vCenter Server 管理的 ESXi 主机。切勿使用 VMware Host Client 直接访问受管主机，且不要从 DCUI 更改受管主机。

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。

### 仅将 DCUI 用于进行故障排除

以 root 用户身份从 DCUI 或 ESXi Shell 访问主机仅能进行故障排除。要管理 ESXi 主机，请使用 vSphere Client（或 VMware Host Client）或一个 VMware CLI 或 API。请参见《ESXCLI 概念和示例》，网址为 <https://code.vmware.com/>。如果使用 ESXi Shell 或 SSH，则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

主机运行多个第三方软件包来支持管理界面或必须执行的任务。VMware 仅支持升级到这些来自 VMware 源的软件包。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。查看第三方供应商站点和 VMware 知识库以了解安全警示。

**注** 请遵循 <http://www.vmware.com/security/> 上的 VMware 安全建议。

## ESXi 高级系统设置

高级系统设置控制 ESXi 行为的各个方面，例如日志记录、系统资源 and 安全性。

下表展示了安全性方面的一些重要 ESXi 高级系统设置。要查看所有高级系统设置，请查看 vSphere Client（主机 > 配置 > 系统 > 高级系统设置）或适用于给定版本的 API。

表 3-1. 安全性高级系统设置部分列表

高级系统设置	描述	默认值
Annotations.WelcomeMessage	在 Host Client 中登录之前显示欢迎消息，或者在 DCUI 中的默认屏幕上显示欢迎消息。在 DCUI 中，欢迎消息会替换某些文本，例如主机 IP 地址。	（空）
Config.Etc.issue	在 SSH 登录会话期间显示横幅。可使用尾随换行符呈现最佳效果。	（空）
Config.Etc.motd	在 SSH 登录时显示当天的消息。	（空）
Config.HostAgent.vmacore.soap.sessionTimeout	设置系统自动注销 VIM API 之前的空闲时间（以分钟为单位）。值为 0（零）表示取消激活空闲时间。此设置仅适用于新会话。	30（分钟）
Mem.MemEagerZero	在虚拟机退出后，激活 VMkernel 操作系统（包括 VMM 进程）中的用户环境和客户机内存页置零。默认值 (0) 使用延迟置零。值为 1 时使用快速置零。	0（已取消激活）



表 3-1. 安全性高级系统设置部分列表（续）

高级系统设置	描述	默认值
Security.AccountLockFailures	<p>设置系统锁定用户帐户之前的最大失败登录尝试次数。例如，要在第五次登录失败时锁定帐户，请将此值设置为 4。值为 0（零）表示取消激活帐户锁定。</p> <p>出于实施原因，某些登录机制会意外计数：</p> <ul style="list-style-type: none"> <li>■ VIM 登录（包括 VMware Host Client）和 ESXCLI 反映确切的登录失败次数。</li> <li>■ 在显示密码提示时，SSH 连接计为一次登录尝试，在成功登录时撤销该计数。此行为在质询和响应通信中正常。</li> <li>■ CGI 登录重复计算登录失败次数。</li> </ul> <p><b>小心</b> 由于此问题，使用 CGI 界面时，用户锁定的速度可能比失败登录次数更快。</p>	5
Security.AccountUnlockTime	设置锁定用户的秒数。指定锁定超时内的任何登录尝试将重新启动锁定超时。	900（15 分钟）
Security.PasswordHistory	设置要为每个用户记住的密码数。此设置可防止重复或类似的密码。	0
Security.PasswordMaxDays	设置两次更改密码之间的最大天数。	99999
Security.PasswordQualityControl	<p>在 Pam_passwdqc 配置中更改所需长度和字符类别要求，或允许使用密码短语。可以在密码中使用特殊字符。密码长度可以至少为 15 个字符。默认设置需要三类字符，且最小长度为七个字符。</p> <p>如果实施 DoD Annex，可以结合使用 similar=deny 选项与最小密码长度，以强制执行密码完全不同的要求。仅对通过 VIM LocalAccountManager.changePassword API 更改的密码强制执行密码历史记录设置。要更改密码，需要用户具有管理员权限。</p> <p>PasswordQualityControl 设置和 PasswordMaxDays 设置满足 DoD Annex 的要求：</p> <pre>min=disabled,disabled,d disabled,disabled,15 similar=deny</pre>	retry=3 min=disabled,disabled,disabled,7,7

表 3-1. 安全性高级系统设置部分列表（续）

高级系统设置	描述	默认值
UserVars.DcuiTimeOut	设置系统自动注销 DCUI 之前的空闲时间（以秒为单位）。值为 0（零）表示取消激活超时。	600（10 分钟）
UserVars.ESXiShellInteractiveTimeOut	设置系统自动注销交互式 shell 之前的空闲时间（以秒为单位）。此设置仅对新会话生效。值为 0（零）表示取消激活空闲时间。同时适用于 DCUI 和 SSH shell。	0
UserVars.ESXiShellTimeOut	设置登录 shell 等待登录的时间（以秒为单位）。值为 0（零）表示取消激活超时。同时适用于 DCUI 和 SSH shell。	0
UserVars.HostClientSessionTimeout	设置系统自动注销 Host Client 之前的空闲时间（以秒为单位）。值为 0（零）表示取消激活空闲时间。	900（15 分钟）
UserVars.HostClientWelcomeMessage	在 Host Client 中登录时显示欢迎消息。该消息在登录后以“提示”的方式进行显示。	（空）

## 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。

主机配置文件为主机配置和配置合规性提供自动化的集中管理机制。主机配置文件可以通过降低对重复手动任务的依赖来提高效率。主机配置文件捕获预配置和验证的引用主机的配置，以受管对象方式存储该配置，并使用其中包含的参数目录来配置网络连接、存储、安全性及其他主机级别的参数。

可以从 vSphere 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集群以将其应用于集群中的所有主机。

### 步骤

- 1 设置引用主机规范并创建主机配置文件。
- 2 将配置文件附加到主机或集群。
- 3 将引用主机的主机配置文件应用到其他主机或集群。

## 使用脚本管理 ESXi 主机配置设置

在包含许多 ESXi 主机的环境中，使用脚本管理主机比在 vSphere Client 中管理主机更快且不容易出错。

vSphere 包括用于 ESXi 主机管理的多种脚本编制语言。VMware PowerCLI 是 vSphere API 的 Windows PowerShell 接口，包含了用于管理 vSphere 组件的 PowerShell cmdlet。ESXCLI 包含用于管理 ESXi 主机和虚拟机的一组命令。有关参考信息和编程提示，请参见 <https://developer.vmware.com>。vSphere 管理员文档重点介绍了如何使用 vSphere Client 进行管理。

还可以使用 vSphere Automation SDK 的一个脚本接口，如 vSphere Automation SDK for Python。

### 步骤

- 1 创建具有有限特权的自定义角色。

请参见 [创建 vCenter Server 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 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
ESXCLI	<pre>esxcli &lt;conn_options&gt; 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>

- 4 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。
- 5 运行命令后，确认更改已生效。

## ESXi 密码和帐户锁定

对于 ESXi 主机，必须使用符合预定义要求的密码。可以使用 `Security.PasswordQualityControl` 高级系统设置更改所需长度和字符类别要求或允许密码短语。还可以使用 `Security.PasswordHistory` 高级系统设置来设置要为每个用户记住的密码数。

**注** ESXi 密码的默认要求因版本而异。可以使用 `Security.PasswordQualityControl` 高级系统设置检查并更改默认密码限制。

### ESXi 密码

ESXi 对从直接控制台用户界面、ESXi Shell、SSH 或 VMware Host Client 进行的访问强制执行密码要求。

- 默认情况下，在创建密码时，必须至少包括以下四类字符中三类字符的组合：小写字母、大写字母、数字和特殊字符（如下划线或短划线）。
- 默认情况下，密码长度至少为 7 个字符，且小于 40 个字符。
- 密码不得包含字典单词或部分字典单词。
- 密码不得包含用户名或部分用户名。

**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。密码内使用的字典词可降低整体密码强度。

### 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，如果新密码不够强或者两次未正确输入密码，则系统最多会提示用户输入三次 (`retry=3`)。不允许使用包含一种或两种类别字符的密码，也不允许使用密码短语，因为前三项已停用。使用三种和四种类别字符的密码需要 7 个字符。有关其他选项（例如，`max`、`passphrase` 等）的详细信息，请参见 `pam_passwdqc` 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`：以大写字母开头，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，密码短语默认处于停用状态。可以在 vSphere Client 中使用 `Security.PasswordQualityControl` 高级系统设置更改默认设置和其他设置。

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。

对于旧版主机，仍然支持更改 `/etc/pam.d/passwd` 文件，但在将来的版本中将不再支持更改此文件。而是使用 `Security.PasswordQualityControl` 高级系统设置。

## 更改默认密码限制

可以使用 ESXi 主机的 `Security.PasswordQualityControl` 高级系统设置更改密码或密码短语的默认限制。有关更改《vCenter Server 和主机管理》高级系统设置的信息，请参见 ESXi 文档。

例如，您可以更改默认设置，要求包含最少 15 个字符和最少 4 个词 (`passphrase=4`)，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** 并非所有可能的密码组合选项都已经过测试。更改默认密码设置后执行测试。

---

以下示例设置了密码复杂性要求，要求使用四类字符中的 8 个字符并实现显著的密码差异、记住五个密码的历史记录以及 90 天轮换策略：

```
min=disabled,disabled,disabled,disabled,8 similar=deny
```

将 `Security.PasswordHistory` 选项设置为 5，并将 `Security.PasswordMaxDays` 选项设置为 90。

## ESXi 帐户锁定行为

对于通过 SSH 和通过 vSphere Web Services SDK 进行的访问，支持帐户锁定。直接控制台界面 (DCUI) 和 ESXi Shell 不支持帐户锁定。默认情况下，最多允许 5 次尝试，当这些尝试均失败后，便会锁定帐户。默认情况下，帐户将在 15 分钟后解锁。

## 配置登录行为

可以使用以下高级系统设置配置 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。零表示取消激活帐户锁定。
- `Security.AccountUnlockTime`。用户被锁定的秒数。
- `Security.PasswordHistory`。要为每个用户记住的密码数。零表示取消激活密码历史记录。

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 加密密钥生成

ESXi 会生成多个非对称密钥，用于正常操作。传输层安全 (TLS) 密钥使用 TLS 协议保护与 ESXi 主机的通信。SSH 密钥使用 SSH 协议保护与 ESXi 主机的通信。

### 传输层安全密钥

传输层安全 (TLS) 密钥使用 TLS 协议保护与主机的通信。首次引导时，ESXi 主机将以 2048 位 RSA 密钥的形式生成 TLS 密钥。当前，ESXi 不为 TLS 自动生成 ECDSA 密钥。TLS 私钥不由管理员进行维护。

TLS 密钥位于以下非持久位置：

```
/etc/vmware/ssl/rui.key
```

TLS 公钥（包括中间证书颁发机构）作为 X.509 v3 证书位于以下非持久位置：

```
/etc/vmware/ssl/rui.crt
```

将 vCenter Server 与 ESXi 主机结合使用时，vCenter Server 会自动生成 CSR，使用 VMware Certificate Authority (VMCA) 对其进行签名，并生成证书。将 ESXi 主机添加到 vCenter Server 时，vCenter Server 会在该 ESXi 主机上安装该生成的证书。

默认 TLS 证书是自签名证书，且 `subjectAltName` 字段与安装时主机名匹配。可以安装不同的证书，以便使用不同的 `subjectAltName` 或在验证链中包含特定的证书颁发机构 (CA) 等。请参见[替换 ESXi SSL 证书和密钥](#)。

还可以使用 VMware Host Client 替换证书。请参见《vSphere 单台主机管理 - VMware Host Client》。

### SSH 密钥

SSH 密钥使用 SSH 协议保护与 ESXi 主机的通信。首次引导时，系统会生成 nistp256 ECDSA 密钥，并将 SSH 密钥作为 2048 位 RSA 密钥。默认情况下，SSH 服务器处于取消激活状态。SSH 访问主要用于故障排除目的。SSH 密钥不由管理员进行维护。通过 SSH 登录需要相当于完全主机控制的管理特权。要启用 SSH 访问，请参见[使用 vSphere Client 激活对 ESXi Shell 的访问](#)。

SSH 公钥位于以下位置：

```
/etc/ssh/ssh_host_rsa_key.pub
```

```
/etc/ssh/ssh_host_ecdsa_key.pub
```

SSH 私钥位于以下位置：

```
/etc/ssh/ssh_host_rsa_key
```

```
/etc/ssh/ssh_host_ecdsa_key
```

### TLS 加密密钥建立

TLS 加密密钥建立的配置由选择的 TLS 密码套件进行控制，这些套件选择基于 RSA 的密钥传输（如 NIST 特别出版物 800-56B 中所述）或使用临时 Ecliptic Curve Diffie Hellman (ECDH) 的基于 ECC 的密钥协议（如 NIST 特别出版物 800-56A 中所述）之一。

## SSH 加密密钥建立

SSH 加密密钥建立的配置由 SSHD 配置控制。ESXi 提供了一项默认配置，即允许基于 RSA 的密钥传输（如 NIST 特别出版物 800-56B 中所述）、临时 Diffie Hellman (DH)（如 NIST 特别出版物 800-56A 中所述）密钥协议和临时 Elliptic Curve Diffie Hellman (ECDH)（如 NIST 特别出版物 800-56A 中所述）。SSHD 配置不由管理员进行维护。

## ESXi 中的 SSH 安全性

默认情况下，ESXi Shell 接口和 SSH 接口处于停用状态。除非要执行故障排除或支持活动，否则这些接口应保持停用状态。对于日常活动，请使用 vSphere Client，使活动受制于基于角色的访问控制和现代访问控制方法。

### ESXi 中的 SSH 配置

ESXi 中的 SSH 配置使用以下设置。

#### 停用第 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。

### ESXi SSH 密钥

SSH 密钥可以限制、控制以及保护对 ESXi 主机的访问。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。

您可以使用 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，网址为 <http://kb.vmware.com/kb/1002866>。

启用 SSH 并将 SSH 密钥添加到主机具有内在的风险。请权衡暴露用户名和密码的潜在风险与具有可信密钥的用户实施入侵的风险。

### 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 密钥上载到主机：

- root 用户的授权密钥
- DSA 密钥

- DSA 公用密钥
- RSA 密钥
- RSA 公用密钥

**重要说明** 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>

## 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。在客户机操作系统中以特权模式运行错误代码或恶意代码（如设备驱动程序）时，可能会触发该漏洞。行业标准硬件和固件当前无法提供足够的容错支持，以防止 ESXi 主机出现漏洞。

仅当可信实体拥有和管理虚拟机时，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被直通的硬件设备中存在缺陷或不兼容。导致出现错误的其他原因还有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，此操作可导致 ESXi 主机上出现 IOMMU 页面故障。此操作可能是由于 DMA 操作指向虚拟机内存外部的地址。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。此致命错误会导致 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。虚假中断可能会导致 ESXi 主机崩溃。理论上可能存在利用这些虚假中断的其他方式。



## 停用 vSphere Managed Object Browser

Managed Object Browser (MOB) 是一个 vSphere 实用程序，可用于浏览 VMkernel 对象模型。但是，攻击者可以使用此界面执行恶意配置更改或操作，因为可以使用 MOB 更改主机配置。仅将 MOB 用于调试，并确保在生产系统中停用该功能。

MOB 默认处于停用状态。但是，对于某些任务（如从系统提取旧证书），必须使用 MOB。您可以按以下方式激活和停用 MOB。

### 步骤

- 1 在 vSphere Client 清单中，浏览到主机。
- 2 单击**配置**。
- 3 在“系统”下，单击**高级系统设置**。
- 4 检查 **Config.HostAgent.plugins.solo.enableMob** 的值，然后单击**编辑**以根据需要进行更改。

请勿从 ESXi Shell 使用 `vim-cmd`。

## 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 VMware 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，还建议使用独立的网络。

- vSphere 基础架构网络用于 vSphere vMotion、VMware vSphere Fault Tolerance、VMware vSAN 和存储等功能。隔离这些特定功能使用的网络。通常不必将这些网络中的流量路由到单个物理服务器机架外部。
- 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其他流量隔离开来。通常，管理网络只能由系统、网络和安全管理员访问。要保护对管理网络的访问，请使用堡垒主机或虚拟专用网络 (VPN)。严格控制该网络中的访问。
- 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。

## 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 连接激活 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 连接停用 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停用 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。停用 SSL 可以提高性能，因为您可以避免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

使用 vSphere Auto Deploy 时，要特别注意网络安全、引导映像安全以及通过主机配置文件导致的潜在密码暴露隐患，以保护您的环境。

### 网络安全

就像保护使用任何其他基于 PXE 的部署方法的网络一样保护您的网络。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（root 帐户）密码和用户密码使用 SHA-512 进行了哈希处理。
  - 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 Proxy 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。

## 基于 CIM 的硬件监控工具的控制访问

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 从远程应用程序监控硬件资源。为了确保 CIM 接口安全，请仅为这些远程应用程序提供必需的最小访问权限。使用 root 或管理员帐户置备远程应用程序时，如果应用程序受到影响，则虚拟环境可能也会受到影响。

CIM 是一种开放式标准，用于为 ESXi 主机硬件资源的无代理标准监控定义一个框架。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 提供程序支持对设备驱动程序和底层硬件进行管理访问。硬件供应商（包括服务器制造商和硬件设备供应商）可以编写提供程序，以便监控和管理其设备。VMware 可以编写提供程序，用于监控服务器硬件、ESXi 存储基础架构和虚拟化特定资源。这些提供程序属于轻量级程序，在 ESXi 主机内部运行，并专注于特定管理任务。CIM 代理程序从所有 CIM 提供程序获得信息，并使用标准 API 将这些信息提供给外部。最常用的 API 是 WS-MAN。

请不要为远程应用程序提供访问 CIM 接口的 root 凭据。请为这些应用程序创建低特权 vSphere 用户帐户，并使用 VIM API 票证功能向此低特权用户帐户发布一个 sessionId（称为“票证”）以向 CIM 进行身份验证。如果该帐户已获得获取 CIM 票证的权限，则 VIM API 可将票证提供给 CIM。然后，将这些票证作为用户 ID 和密码提供给任何 CIM-XML API 调用。有关详细信息，请参见 `AcquireCimServicesTicket()` 方法。

安装第三方 CIM VIB（例如，运行 `esxcli software vib install -n VIBname` 命令）时，CIM 服务启动。

如果必须手动激活 CIM 服务，请运行以下命令：

```
esxcli system wbem set -e true
```

如有必要，可以停用 wsman（WSManagement 服务），以便仅运行 CIM 服务：

```
esxcli system wbem set -W false
```

要确认 wsman 已停用，请运行以下命令：

```
esxcli system wbem get
...
WSManagement PID: 0
WSManagement Service: false
```

有关 ESXCLI 命令的详细信息，请参见 ESXCLI 文档。有关激活 CIM 服务的详细信息，请参见 VMware 知识库文章，网址为 <https://kb.vmware.com/kb/1025757>。

### 步骤

- 1 为 CIM 应用程序创建非 root vSphere 用户帐户。

请参见《vSphere 身份验证》中有关添加 vCenter Single Sign-On 用户的主题。此用户帐户所需的 vSphere 特权为 **Host.CIM.交互**。

- 2 使用所选 vSphere API SDK 针对 vCenter Server 对用户帐户进行身份验证。然后，调用 `AcquireCimServicesTicket()` 返回票证，以管理员级别帐户使用 CIM-XML 端口 5989 或 WS-Man 端口 433 API 通过 ESXi 进行身份验证。

有关详细信息，请参见《vSphere Web Services API 参考》。

- 3 根据需要每隔两分钟续订一次票证。

## vSphere Distributed Services Engine 安全性最佳做法

要最大限度提高 ESXi 环境的安全性，请遵循 vSphere Distributed Services Engine 的最佳做法。

从 vSphere 8.0 开始，vSphere Distributed Services Engine 支持将基础架构功能从主机或服务器的 CPU 卸载到数据处理单元（DPUS，也称为 SmartNIC），从而释放 CPU 周期来为应用程序提供服务。有关 vSphere Distributed Services Engine 的介绍，请参见《《VMware ESXi 安装和设置》》文档。有关 vSphere Distributed Services Engine 的详细信息，请参见《《管理主机和集群生命周期》》文档。

通常，请像保护 ESXi 环境那样处理 vSphere Distributed Services Engine 的安全方面。

- 默认情况下，vSphere Distributed Services Engine 的 ESXi Shell 接口和 SSH 接口处于停用状态。除非要执行故障排除或支持活动，否则这些接口应保持停用状态。
- 对于 vSphere Distributed Services Engine 的日常管理活动，请使用 vSphere Client，使活动受制于基于角色的访问控制和现代访问控制方法。

## 控制 ESXi 熵

从 vSphere 8.0 开始，ESXi 熵实施支持 FIPS 140-3 和 EAL4 认证。内核引导选项控制要在 ESXi 主机上激活哪些熵源。

在计算中，“熵”这个术语是指收集用于加密的随机字符和数据，例如生成加密密钥以保护通过网络传输的数据。在生成密钥并通过网络安全通信时，需要熵来确保安全。熵通常是从系统的各种源收集的。

如果满足以下条件，那么 FIPS 熵处理就是默认行为。

- 1 硬件支持 RDSEED。
- 2 `disableHwrng VMkernel` 引导选项不存在或为 FALSE。
- 3 `entropySources VMkernel` 引导选项不存在、为 0（零）或为 4。

可以使用以下 VMkernel 引导选项配置 ESXi Entropy 子系统：

表 3-2. ESXi Entropy VMkernel 引导选项

VMkernel 引导选项	选项类型	描述	默认值
disableHwrng（在 vSphere 8.0 之前可用）	布尔	设置为 TRUE（覆盖“entropySources”）时停用 RDRAND 和 RDSEED 熵源。	FALSE 激活硬件随机数生成器熵源（如果存在）。
entropySources（从 vSphere 8.0 开始可用）	整数，位掩码	指定要激活的熵源。 ■ 0=全部 ■ 1=中断 ■ 2=rdrand ■ 4=rdseed ■ 8=用户空间（激活 EAL4 熵处理） 指定 entropySources=9 会激活中断和用户空间熵源，并停用 rdrand 和 rdseed 熵源。	0（零） 激活所有可用的熵源。

**注** 在做出更改以便仅使用 RDRAND、RDSEED 或两个熵源之前，请查看供应商文档，确保 ESXi 主机支持这些配置。如果主机不支持这些配置，vCenter Server 会向您发送警示，并且主机重新使用中断和用户空间熵源。

#### 前提条件

您必须在 ESXi 主机上具有根访问权限。

#### 步骤

- 1 在 ESXi 主机上，使用 SSH 或其他远程控制台连接启动会话。
- 2 以 root 用户身份登录。
- 3 设置所需的熵 VMkernel 引导选项。
  - a 要为 disableHwrng 停用 RDRAND 和 RDSEED 熵源，请执行以下操作：

```
esxcli system settings kernel set -s disableHwrng -v TRUE
```

- b 要设置熵源，请执行以下操作：

```
esxcli system settings kernel set -s entropySources -v entropy_source_value
```

有关可为 entropySources 设置的值，请参见上表。

## 管理 ESXi 主机的证书

默认情况下，VMware Certificate Authority (VMCA) 使用以 VMCA 作为根证书颁发机构的签名证书置备新 ESXi 主机。在主机明确或作为安装或升级 ESXi 的一部分添加到 vCenter Server 时，便会进行置备。

您可以通过 vSphere Client 以及通过在 vSphere Web Services SDK 中使用 `vim.CertificateManager` API 来查看和管理 ESXi 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 中的证书

在 ESXi 与 vCenter Server 进行通信时，二者将使用 TLS 处理几乎所有管理流量。

vCenter Server 支持 ESXi 主机的以下证书模式。

表 3-3. 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 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或企业 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 Client 刷新和续订证书。</p> <p><b>注</b> 除非将证书模式更改为自定义证书颁发机构，否则在 vSphere Client 中选择<b>续订</b>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.x 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 Server 6.x 及更高版本服务在指纹模式下可能无法正常运行。</p>

## ESXi 证书过期

可以在 vSphere 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**不久即将过期**状态（少于八个月），则将发出黄色警报。如果证书处于**即将过期**状态（少于两个月），则将发出红色警报。

## ESXi 置备和证书

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。

您还可以将第三方或企业证书颁发机构签名的自定义证书用于 ESXi 主机。

## Auto Deploy 中的 ESXi 置备和证书

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 主机后续引导期间，将重新使用该证书。Auto Deploy 服务器是任何嵌入式部署或 vCenter Server 系统的一部分。

如果 Auto Deploy 主机首次引导时 VMCA 不可用，则主机将先尝试连接。如果主机无法连接，则它会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。

您可以将 Auto Deploy 设为第三方证书颁发机构的辅助证书颁发机构。在这种情况下，生成的证书使用 Auto Deploy SSL 密钥进行签名。请参见[将 Auto Deploy 设为辅助证书颁发机构](#)。

从 8.0 开始，您可以将自定义证书（证书颁发机构签名的证书）与 Auto Deploy 结合使用。主机启动时，Auto Deploy 会将自定义证书与 ESXi 主机的 MAC 地址或 BIOS UUID 相关联。请参见[在 Auto Deploy 中使用自定义证书](#)。

## ESXi 证书管理所需的特权

用户需要拥有 **证书.管理证书** 特权才能管理 ESXi 主机证书。

## ESXi 主机名称和 IP 地址更改

ESXi 主机名称或 IP 地址更改可能会影响 vCenter Server 是否将主机的证书视为有效。将 ESXi 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 3-4. 主机名称或 IP 地址更改时需要人工干预

将 ESXi 主机添加到 vCenter Server 所使用的方式...	ESXi 主机名称更改	ESXi 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 主机升级和证书

如果将 ESXi 主机升级到 ESXi 6.5 或更高版本，升级过程会将自签名（指纹）证书替换为 VMCA 签名证书。如果 ESXi 主机使用自定义证书，升级过程会保留这些证书，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。必须将这些主机升级到 ESXi 6.5 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，则这些证书在升级过程中将保留在原地。将证书模式更改为自定义，以确保稍后在证书刷新过程中不会意外替换证书。

**注** 如果环境处于 VMCA 模式下，且您在 vSphere 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 Client 中监控证书并显示有关证书到期等的信息。

## 使用 Auto Deploy 置备的主机

对于使用 Auto Deploy 置备的主机，在其首次使用 ESXi 6.5 或更高版本软件引导时，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。

请参见将 [Auto Deploy 设为辅助证书颁发机构](#) 和 [在 Auto Deploy 中使用自定义证书](#)。

## ESXi 证书模式切换工作流

默认情况下，VMware Certificate Authority (VMCA) 使用证书置备 ESXi。您可以改用自定义证书模式或用于调试的旧版指纹模式。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。

vCenter Server 支持 ESXi 主机的以下证书模式。

证书模式	描述
VMware Certificate Authority (默认值)	默认情况下，VMware Certificate Authority (VMCA) 被用作 ESXi 主机证书的证书颁发机构 (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 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 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于向后兼容。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 Server 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。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 的根证书添加到 VMware Endpoint Certificate Store (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 ESXi 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。工作流如下。

- 1 移除 vCenter Server 系统中的所有主机。
- 2 在 vCenter Server 系统上，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 ESXi 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 ESXi 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。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 ESXi 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 ESXi 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。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 ESXi 证书模式](#)。
- 5 将主机添加到 vCenter Server 系统。

## ESXi 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)。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。

可以使用 vSphere Client 更改许多默认设置。考虑更改组织和位置信息。请参见[更改 ESXi 证书默认设置](#)。

**表 3-5. ESXi 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.daysValid
证书过期的硬阈值。达到此阈值时，vCenter Server 将发出红色警报。	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

表 3-5. ESXi CSR 设置（续）

参数	默认值	高级选项
证书过期的软阈值。达到此阈值时，vCenter Server 将引发事件。	240 天	vpxd.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 <a href="#">ESXi 主机升级和证书</a> 。	vmca 您还可以指定指纹或自定义。请参见 <a href="#">更改 ESXi 证书模式</a> 。	vpxd.certmgmt.mode

## 更改 ESXi 证书默认设置

当 ESXi 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 Client 中的 vCenter Server “高级设置” 更改 CSR 中的某些默认设置。

请参见上一个表中的默认设置列表。某些默认设置不能更改。

### 步骤

- 1 在 vSphere Client 中，选择管理主机的 vCenter Server 系统。
- 2 单击**配置**，然后单击**高级配置**。
- 3 单击**编辑设置**。
- 4 单击“名称”列中的**筛选器**图标，然后在“筛选器”框中输入 **vpxd.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**保存**。

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，可以断开并重新连接该主机或续订证书。

## 查看 ESXi 主机的证书过期信息

对于处于 VMCA 模式或自定义模式的 ESXi 主机，可以从 vSphere Client 中查看证书详细信息。根据证书信息，您可以确定任何证书是否即将过期。您还可以使用此信息调试证书问题。

无法查看处于指纹模式中的 ESXi 主机的证书状态信息。您可以查看多个 ESXi 主机或单个 ESXi 主机的信息。多主机视图仅显示“证书有效期结束日期”信息。

### 步骤

- 1 使用 vSphere Client 登录 vCenter Server。
- 2 浏览清单列表，然后选择 vCenter Server 实例。

### 3 获取证书信息。

单个主机或多个主机	步骤
Single	a 浏览到 ESXi 主机。 b 单击 <b>配置</b> 。 c 在 <b>系统</b> 下，单击 <b>证书</b> 。
倍数	a 选择 <b>主机和集群 &gt; 主机</b> 。 默认情况下，主机显示不包含查证书状态。 b 要显示或隐藏列，请单击左下角的三栏 <b>列选择器</b> 。 c 选中 <b>证书有效期至</b> 复选框，然后根据需要滚动到右侧以查看添加的列。 证书信息将显示证书过期的时间。 d （可选）取消选择其他列可更方便地查看您所关注的内容。

### 4 查看证书信息。

以下信息仅在单主机视图中可用。

字段	描述
主体	在证书生成期间使用的主体。
颁发者	证书的颁发者。
有效期自	生成证书的日期。
有效期至	证书过期的日期。
状态	证书的状态，以下状态之一。  <b>正常</b> 正常操作。  <b>即将过期</b> 证书即将过期。  <b>不久即将过期</b> 证书最多还剩 8 个月就将过期（默认）。  <b>即将过期</b> 证书最多还剩 2 个月就将过期（默认）。  <b>已过期</b> 证书无效，因为已过期。

**注** 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。

## 后续步骤

续订即将过期的证书。请参见[续订或刷新 ESXi 证书](#)。

## 续订或刷新 ESXi 证书

在 ESXi 6.0 及更高版本中，如果 VMware Certificate Authority (VMCA) 向主机分配证书，您可以从 vSphere 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。如果在证书过期之前未续订证书，则断开主机连接后又将其重新连接时，会使 vCenter Server 续订证书。将主机重新添加到 vCenter Server 的行为将重新建立信任，并使 vCenter Server 无条件地颁发续订的证书。

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。

### 前提条件

确认以下情况：

- ESXi 主机已连接到 vCenter Server 系统。
- vCenter Server 系统与 ESXi 主机之间已正确同步时间。
- 可在 vCenter Server 系统和 ESXi 主机之间进行 DNS 解析。
- vCenter Server 系统的 MACHINE\_SSL\_CERT 和 Trusted\_Root 证书有效且未过期。请参见 VMware 知识库文章，网址为 <https://kb.vmware.com/s/article/2111411>。
- ESXi 主机不处于维护模式。

### 步骤

- 1 在 vSphere Client 清单中，浏览到主机。
- 2 单击**配置**。
- 3 在**系统**下，单击**证书**。

您可以查看有关所选主机的证书的详细信息。

- 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**。

## 更改 ESXi 证书模式

使用 VMware Certificate Authority (VMCA) 置备您环境中的 ESXi 主机，除非公司策略要求您使用自定义证书。要使用具有不同根 CA 的自定义证书，可以编辑 vCenter Server 高级设置 `vpzd.certmgmt.mode`。更改后，当您刷新证书时，将不再使用 VMCA 证书自动置备主机。您必须负责环境中的证书管理。

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 在 vSphere Client 中，选择管理主机的 vCenter Server 系统。
- 2 单击**配置**，然后在“设置”下，单击**高级设置**。
- 3 单击**编辑设置**。
- 4 单击“名称”列中的**筛选器**图标，然后在“筛选器”框中输入 `vpzd.certmgmt` 以仅显示证书管理参数。
- 5 如果要管理自己的证书，请将 `vpzd.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**保存**。
- 6 重新启动 vCenter Server 服务。

有关重新启动服务的信息，请参见《vCenter Server 配置》文档。

## 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。您可以通过各种方式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。

有关对 ESXi 主机使用 CA 签名证书的详细说明，请参见 [ESXi 证书模式切换 workflow](#)。

**注** 如果要替换属于 vSAN 集群的 ESXi 主机上的 SSL 证书，请按照 VMware 知识库文章 (<https://kb.vmware.com/s/article/56441>) 中的步骤进行操作。

#### ■ ESXi 证书签名请求的要求

如果要使用企业或第三方 CA 签名的证书或辅助 CA 签名的证书，必须向 CA 发送证书签名请求 (CSR)。

#### ■ 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 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

如果要使用企业或第三方 CA 签名的证书或辅助 CA 签名的证书，必须向 CA 发送证书签名请求 (CSR)。

使用具有以下特性的 CSR：

- 密钥大小：2048 位（最小值）到 16384 位（最大值）（PEM 编码）
- PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。密钥添加到 VECS 后，会转换为 PKCS8。
- x509 版本 3
- 对于根证书，CA 扩展必须设置为 true，并且 cert 签名必须在要求列表中。
- SubjectAltName 必须包含 DNS Name=<machine\_FQDN>。
- CRT 格式
- 包含以下密钥用法：数字签名、密钥加密。
- 比当前时间早一天的开始时间。
- CN（和 SubjectAltName）设置为 vCenter Server 清单中的 ESXi 主机的主机名（或 IP 地址）。

vSphere 不支持以下证书。

- 使用通配符的证书。
- 不支持算法 md2WithRSAEncryption、md5WithRSAEncryption、RSASSA-PSS、dsaWithSHA1、ecdsa\_with\_SHA1 和 sha1WithRSAEncryption。

有关生成 CSR 的信息，请参见相应的 VMware 知识库文章，网址为 <https://kb.vmware.com/s/article/2113926>。

## 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 Client 启用 ESXi Shell 或启用 SSH 流量。
- 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。

### 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 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 Client 启用 ESXi Shell 或启用 SSH 流量。
- 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。

### 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>

`/host/ssl_cert` 和 `host/ssl_key` 位置链接到 `/etc/vmware/ssl` 中的证书文件。

## 3 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）](#)。

## 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。

**注** 如果 vCenter Server 系统所使用的自定义证书的 CA 颁发方与 ESXi 主机上安装证书的相同，则不需要此步骤。

### 步骤

- 1 登录到管理 ESXi 主机的 vCenter Server 系统的 vCenter Server shell。
- 2 要将新证书添加到 TRUSTED\_ROOTS 存储，运行 `dir-cli`，例如：
 

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_RootCA
```
- 3 出现提示时，提供 Single Sign-On 管理员凭据。
- 4 如果您的自定义证书由中间 CA 颁发，您还必须将中间 CA 添加到 vCenter Server 上的 TRUSTED\_ROOTS 存储，例如：

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_intermediateCA
```

## 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，则执行证书刷新时，自定义证书将替换为 VMCA 签名的证书。请参见[更改 ESXi 证书模式](#)。

## 将 Auto Deploy 设为辅助证书颁发机构

默认情况下，Auto Deploy 服务器使用 VMware Certificate Authority (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证书颁发机构 (CA) 机构的辅助证书颁发机构。

### 前提条件

- 向您的 CA 请求证书。证书必须满足以下要求。
  - 密钥大小：2048 位（最小值）到 16384 位（最大值）（PEM 编码）
  - PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。密钥添加到 VECS 后，会转换为 PKCS8。
  - x509 版本 3
  - 对于根证书，CA 扩展必须设置为 true，并且 cert 签名必须在要求列表中。
  - SubjectAltName 必须包含 DNS Name=<machine\_FQDN>。
  - CRT 格式
  - 包含以下密钥用法：数字签名、密钥加密。
  - 比当前时间早一天的开始时间。
  - CN（和 SubjectAltName）设置为 vCenter Server 清单中的 ESXi 主机的主机名（或 IP 地址）。
- 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。

证书位于 /etc/vmware-rbd/ssl/ 目录中。

## 2 停止 vSphere Authentication Proxy 服务。

工具	步骤
vCenter Server 管理界面	<ol style="list-style-type: none"> <li>在 Web 浏览器中，输入 <code>https://vCenter Server vcenter-IP-address-or-FQDN:5480</code> 转至管理界面。</li> <li>以 root 用户身份登录。 默认 root 密码是您在部署 vCenter Server 时设置的密码。</li> <li>单击<b>服务</b>，然后单击 <b>VMware vSphere Authentication Proxy</b> 服务。</li> <li>单击<b>停止</b>。</li> </ol>
CLI	<code>service-control --stop vmcam</code>

- 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。

- 在运行 Auto Deploy 服务的系统上，运行以下命令以更新 VMware Endpoint Certificate Store (VECS) 内的 TRUSTED\_ROOTS 存储，以便使用新证书。

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert /etc/vmware-rbd/ssl/rbd-ca.crt
/usr/lib/vmware-vmafd/bin/vecs-cli force-refresh
```

- 创建包含 TRUSTED\_ROOTS 存储内容的 `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。

- 将 vCenter Server 系统的 ESXi 证书模式更改为**自定义**。

请参见更改 [ESXi 证书模式](#)。

- 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 服务器将生成证书。Auto Deploy 服务器将使用添加到 TRUSTED\_ROOTS 存储的根证书。

**注** 如果证书替换后遇到自动部署问题，请参见 VMware 知识库文章，网址为 <http://kb.vmware.com/kb/2000988>。

## 在 Auto Deploy 中使用自定义证书

从 vSphere 8.0 开始，您可以将 Auto Deploy 服务器设置为使用第三方证书颁发机构（CA）或您自己的内部 CA 签名的自定义证书置备 ESXi 主机。默认情况下，Auto Deploy 服务器使用 VMware Certificate Authority (VMCA) 签名的证书置备 ESXi 主机。

在 vSphere 8.0 之前，使用 Auto Deploy 管理证书的选项包括：

- 使用 vCenter Server 和内置 VMware Certificate Authority（默认）。

- 将 Auto Deploy 设为第三方 CA 的辅助 CA。在这种情况下，Auto Deploy SSL 密钥会对证书进行签名。

从 vSphere 8.0 开始，您可以将第三方 CA 或您自己的内部 CA 签名的自定义证书上载到 Auto Deploy。Auto Deploy 将自定义证书与 ESXi 主机的 MAC 地址或 BIOS UUID 相关联。每次 Auto Deploy 主机启动时，Auto Deploy 都会检查自定义证书。如果 Auto Deploy 找到自定义证书，它将使用该证书，而不是通过 VMCA 生成一个证书。

此任务的主要步骤包括：

- 1 为第三方 CA 或您自己的内部 CA 生成自定义证书请求。
- 2 获取签名的自定义证书（密钥和证书）并将其存储在本地。
- 3 如果使用的是第三方 CA，并且之前未曾使用，请确保将 CA 的根证书上载到 vCenter Server 上的 TRUSTED\_ROOTS 存储。
- 4 将自定义证书上载到 Auto Deploy 并将证书与 ESXi 主机的 MAC 地址或 BIOS UUID 相关联。
- 5 引导 ESXi 主机。

将自定义证书分配给 ESXi 主机时，Auto Deploy 会在下次从 Auto Deploy 引导时将该证书推送到主机。

使用自定义证书和 Auto Deploy 时，请注意以下注意事项。

- 您必须使用 PowerCLI `Add-CustomCertificate`、`Remove-CustomCertificate` 和 `List-CustomCertificate` cmdlet 来管理与 Auto Deploy 一起使用的自定义证书。管理自定义证书的功能在 vSphere Client 中不可用。
- 要刷新用于 Auto Deploy 的自定义证书，必须再次运行 `Add-CustomCertificate` cmdlet。
- 请务必检查自定义证书是否存在潜在错误。Auto Deploy 仅验证自定义证书是否符合 X.509 证书标准，以及证书的过期阈值是否设置为至少 240 天。Auto Deploy 不会执行任何其他证书验证或检查。要更改证书阈值，可以运行 `Set-DeployOption -Key certificate-refresh-threshold` cmdlet。
- 如果稍后使用 `Remove-CustomCertificate` cmdlet 从 ESXi 主机中移除自定义证书，必须重新启动该主机才能使更改生效。

有关自定义证书和 Auto Deploy 的详细信息，请参见《VMware ESXi 安装和设置》文档。

#### 前提条件

确保您具有以下内容：

- 从证书颁发机构请求证书。证书必须满足以下要求。
  - 密钥大小：2048 位（最小值）到 16384 位（最大值）（PEM 编码）
  - 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
  - CRT 格式

- CA 扩展设置为 true
- 证书签名的密钥用法
- 比当前时间早一天的开始时间
- ESXi 主机 MAC 地址或 BIOS UUID。评估哪种方法最适合您的环境。BIOS UUID 比 MAC 地址更稳定，更不受更改的影响。如果更改 ESXi 主机中的网络适配器，MAC 地址将发生变化。但是，MAC 地址可能更易于使用，并且比 BIOS UUID 更易于获取。
- 至少为 PowerCLI 版本 12.6.0。有关 Auto Deploy PowerCLI cmdlet 的详细信息，请参见《VMware ESXi 安装和设置》文档中的 Auto Deploy PowerCLI Cmdlet 概览主题。

确保您具有以下特权：

- 添加自定义证书：Autodeploy.规则.创建
- 获取自定义证书信息：系统.读取

## 步骤

### 1 生成证书请求。

- a 使用之前列出的证书请求要求，创建配置 (.cfg) 文件。
- b 要生成 CSR 文件和密钥文件，请运行 `openssl req` 命令文件，同时传入配置 (.cfg) 文件。

例如：

```
openssl req -new -config custom_cert.cfg -days 4200 -sha256 -keyout rui.key -out rui.csr
```

在该命令中：

- `-new` 生成新的证书请求。
  - `-config custom_cert.cfg` 指定自定义 .cfg 文件。
  - `-days 4200` 指定证书认证时间为 4200 天。
  - `-sha256` 指定签署请求所需的消息摘要。
  - `-keyout rui.key` 指定要将新创建的私钥写入到的文件。
  - `-out rui.csr` 指定要写入到的输出文件。
- 2 将证书请求发送给第三方 CA，或者，如果您给自己的证书签名，请运行 `openssl x509 -req` 命令，从 `rui.csr` 文件生成自定义证书。

例如：

```
openssl x509 -req -in rui.csr -CA "/etc/vmware-rbd/ssl/rbd-ca.crt" -CAkey \
"/etc/vmware-rbd/ssl/rbd-ca.key" -extfile \
openssl.cfg -extensions x509 -CAserial "/etc/vmware-rbd/ssl/rbd-ca.srl" -days \
4200 -sha256 -out signed_rui.crt
```

在该命令中：

- `-in rui.csr` 指定输入文件。
- `-CA "/etc/vmware-rbd/ssl/rbd-ca.crt"` 指定用于服务器证书验证的目录。
- `-CAkey "/etc/vmware-rbd/ssl/rbd-ca.key"` 设置用于签署证书的 CA 私钥。
- `-extfile openssl.cfg` 指定要从中读取证书扩展名的其他可选配置文件。
- `-extensions x509` 指定使用 x509 证书扩展。
- `-CAserial "/etc/vmware-rbd/ssl/rbd-ca.srl"` 使用 `rbd-ca.srl` 中的序列号对证书进行签名。
- `-days 4200` 指定证书认证时间为 4200 天。
- `-sha256` 指定签署请求所需的消息摘要。
- `-out signed_rui.crt` 指定要写入到的输出文件。

- 3 （可选）如果之前未将签名证书颁发机构的证书上载到 VMware 端点证书存储 (VECS) 内的 TRUSTED\_ROOTS 存储，请在运行 Auto Deploy 服务的 vCenter Server 上执行以下步骤。

- a 使用 WinSCP 等工具将证书复制到 vCenter Server。
- b 使用 SSH 登录到 vCenter Server 并运行以下命令。

```
/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --cert path_to_ca_certificate
```

- 4 获取 ESXi 主机 MAC 地址或 BIOS UUID。

- 5 执行以下步骤将自定义证书添加到 Auto Deploy。

- a 要连接到 vCenter Server，请运行 `Connect-VIServer cmdlet`。

```
Connect-VIServer -server VC_ip_address -User administrator_user -Password 'password'
```

- b （可选）要查看现有的自定义证书，请运行 `Get-CustomCertificates cmdlet`。

首次添加自定义证书时，将看不到此 cmdlet 返回的任何证书。

- c 要将自定义证书与 ESXi 主机关联，请运行 `Add-CustomCertificate cmdlet`。

```
Add-CustomCertificate -HostID [MAC_Address | BIOS_UUID] -Certificate
"path_to_custom_cert" -Key "path_to_custom_cert_key"
```

您可以指定主机的 MAC 地址或 BIOS UUID。Auto Deploy 将自定义证书上载到主机。

- d 要验证证书是否已上载，请运行 `Get-CustomCertificates cmdlet`。

您会看到类似以下内容的输出：

```
Name:      CustomHostCert-1
CertificateId:      1
HostId:      02:08:b0:8e:18:a2
ExpirationTime: 1  2/28/2033 10:45:50 AM
TimeCreated:      9/29/2022 7:40:28 AM
LastModified:      9/29/2022 7:40:28 AM
AssociatedHostName:
```

`AssociatedHostName` 目前为空。启动主机后，输出将反映与自定义证书关联的 ESXi 主机的名称。

- 6 启动 ESXi 主机。
- 7 要验证自定义证书是否与 vCenter Server 相关联，请再次运行 `Get-CustomCertificates cmdlet`。

您会看到输出包含以下内容。

```
Name:      CustomHostCert-1
CertificateId:      1
HostId:      02:08:b0:8e:18:a2
ExpirationTime: 1  2/28/2033 10:45:50 AM
TimeCreated:      9/29/2022 7:40:28 AM
LastModified:      9/29/2022 7:40:28 AM
AssociatedHostName: host1.example.com
```

现在，`AssociatedHostName` 包含 ESXi 主机的名称。

## 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** 如果使用 HTTP PUT 或者从 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 ESXi 主机。

或者，也可以将主机置于维护模式，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。

## 自定义 ESXi 主机安全性

通过 vSphere Client 中提供的“防火墙”、“服务”和“安全配置文件”面板自定义 ESXi 主机的许多基本安全设置。“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 VMware CLI 或 SDK 之一，并自动执行自定义。

## 配置 ESXi 防火墙

ESXi 包括默认启用的防火墙。安装时，会配置 ESXi 防火墙阻止入站和出站流量，但在主机安全配置文件中启用的服务的流量除外。您可以使用 vSphere Client、CLI 和 API 管理防火墙。

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 防火墙配置为仅从授权网络启用访问来降低该风险。

---

**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 Client 中，对每台主机使用 **配置 > 防火墙**。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[使用 ESXCLI 防火墙命令配置 ESXi 行为](#)。
- 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。

要安装自定义 VIB，必须将 ESXi 主机的接受程度改为 CommunitySupported。

---

**注** 如果您联系 VMware 技术支持来调查装有社区支持的 VIB 的 ESXi 主机上的问题，VMware 技术支持可能会要求您卸载该 VIB。此类请求是一个故障排除步骤，用于确定该 VIB 是否与调查的问题有关。

---

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 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。

此任务介绍了如何使用 vSphere Client 配置 ESXi 防火墙设置。可以使用 ESXi Shell 或 ESXCLI 命令在命令行处配置 ESXi 以自动执行防火墙配置。有关使用 ESXCLI 操作防火墙和防火墙规则的示例，请参见[使用 ESXCLI 防火墙命令配置 ESXi 行为](#)。

---

**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在不知不觉中激活其他服务。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 使用 vSphere Client 登录 vCenter Server。
- 2 在清单中，浏览到主机。
- 3 单击**配置**，然后单击**系统下的防火墙**。  
可以通过单击**入站**和**出站**，在入站和出站连接之间切换。
- 4 在“防火墙”部分中，单击**编辑**。
- 5 从以下三个服务组中选择一个：**未分组**、**安全 Shell** 和**简单网络管理协议**。
- 6 选择要激活的规则集，或取消选择要停用的规则集。
- 7 对于某些访问，还可以通过导航到**系统下的配置 > 服务**来管理服务详细信息。  
有关启动、停止和重新启动服务的详细信息，请参见[激活或停用 ESXi 服务](#)。
- 8 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](#)。
- 9 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。

要更新服务的允许的 IP 列表，可以使用 vSphere Client、ESXCLI 或 PowerCLI。此任务介绍了如何使用 vSphere Client。有关使用 ESXCLI 的说明，请参见 ESXCLI 概念和示例中的[管理 ESXi 防火墙](#)。

### 步骤

- 1 使用 vSphere Client 登录 vCenter Server。
- 2 浏览到 ESXi 主机。
- 3 单击**配置**，然后单击**系统下的防火墙**。  
可以通过单击**入站**和**出站**，在入站和出站连接之间切换。
- 4 在“防火墙”部分中，单击**编辑**。
- 5 从以下三个服务组中选择一个：**未分组**、**安全 Shell** 和**简单网络管理协议**。
- 6 要显示“允许的 IP 地址”部分，请展开一个服务。
- 7 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

- 8 确保选择服务本身。
- 9 单击**确定**。
- 10 验证服务的**允许的 IP 地址**列中的更改。

## ESXi 主机的入站和出站防火墙端口

通过 vSphere Client 和 VMware Host 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。

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。有关 ESXi 防火墙中受支持端口和协议的列表，请参见 <https://ports.vmware.com/> 中的 VMware Ports and Protocols Tool™。

VMware Ports and Protocols Tool 将列出默认安装的服务的端口信息。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。这些信息主要用于 vSphere Client 中显示的服务，但是 VMware Ports and Protocols Tool 还包括其他某些端口。

## 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。

- 如果停用了 nfsClient 规则集，则 ESXi 将激活规则集，并通过将 allowedAll 标记设置为 FALSE 来停用“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。
- 如果激活了 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** 如果手动激活 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，将停用 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 将停用 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 将激活 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，否则该端口将保持激活状态。

## 使用 ESXCLI 防火墙命令配置 ESXi 行为

如果环境包含多个 ESXi 主机，可使用 ESXCLI 命令或 vSphere Web Services SDK 自动执行防火墙配置。

### 防火墙命令参考

可以使用 ESXi Shell 或 ESXCLI 命令在命令行处配置 ESXi 以自动执行防火墙配置。要操作防火墙和防火墙规则，请参见《ESXCLI 入门》了解相关介绍，参见《ESXCLI 概念和示例》查看使用 ESXCLI 的示例。

在 ESXi 7.0 及更高版本中，已限制对用于创建自定义防火墙规则的 service.xml 文件进行访问。有关使用 /etc/rc.local.d/local.sh 文件创建自定义防火墙规则的信息，请参见 VMware 知识库文章 [2008226](#)。

表 3-6. 防火墙命令

命令	描述
<code>esxcli network firewall get</code>	返回防火墙的状态并列出默认操作。
<code>esxcli network firewall set --default-action</code>	设置为 <b>true</b> 可将默认操作设置为通过。设置为 <b>false</b> 可将默认操作设置为丢弃。
<code>esxcli network firewall set --enabled</code>	激活或停用 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 <b>true</b> 可允许所有人对所有 IP 地址具有访问权限。设置为 <b>false</b> 可使用允许的 IP 地址列表。
<code>esxcli network firewall ruleset set --enabled --ruleset-id=&lt;string&gt;</code>	将“已启用”设置为 <b>true</b> 可激活指定规则集。将“已启用”设置为 <b>false</b> 可停用指定规则集。
<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。

## 激活或停用 ESXi 服务

可以从 vSphere Client 启用或停用 ESXi 服务。

ESXi 主机包含默认情况下处于运行状态的多项服务。如果公司策略允许，可以从安全配置文件停用服务，或激活服务。

**注** 激活服务会影响主机的安全性。除非绝对必要，否则不要激活服务。

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。有时，需要先进行其他设置，然后才能在 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。

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 Client 中修改以下服务的状态。

表 3-7. 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激活对 ESXi Shell 的访问。可以激活对本地 ESXi Shell 的访问或对 ESXi Shell 和 SSH 的访问。
SSH	已停止	主机上允许通过 Secure Shell 进行远程连接的 SSH 客户端服务。
基于负载的绑定守护进程	正在运行	基于负载的绑定。
attestd	已停止	vSphere Trust Authority 证明服务。
kmxd	已停止	vSphere Trust Authority 密钥提供程序服务。
Active Directory 服务	已停止	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。
PC/SC 智能卡守护进程	已停止	当主机上激活智能卡身份验证时，该服务启动。请参见为 <a href="#">ESXi 配置和管理智能卡身份验证</a> 。
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》文档。
Syslog 服务器	已停止	Syslog 守护进程。可以在 vSphere Client 的“高级系统设置”中激活 syslog。请参见《vCenter Server 安装和设置》文档。
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。

### 前提条件

使用 vSphere Client 连接到 vCenter Server。

### 步骤

- 1 在清单中，浏览到 ESXi 主机。
- 2 单击**配置**，然后单击**系统下的服务**。

### 3 选择要更改的服务。

- a 选择**重新启动**、**启动**或**停止**，以对主机状态进行一次性更改。
- b 要在重新引导后更改主机的状态，请单击**编辑启动策略**，然后选择一个策略。
  - **与主机一起启动和停止**：主机启动后随即启动服务，主机关闭前不久关闭服务。与**根据端口使用情况启动和停止**极其相似，此选项意味着服务定期尝试完成其任务，例如连接指定的 **NTP** 服务器。如果端口先是处于关闭状态，但稍后又打开了，则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。用户启动 **NTP** 服务时，如果主机打开电源，该服务会一直运行。如果服务已启动，并且主机已关闭电源，则该服务将在关机过程中停止。主机打开电源时，服务将再次启动，从而保留用户指定的状态。
  - **根据端口使用情况启动和停止**：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。

---

**注** 这些设置仅适用于通过 UI 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。

---

### 4 单击**确定**。

## 在 ESXi 主机上配置和管理锁定模式

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。

可以选择正常锁定模式或严格锁定模式，这两种模式提供不同的锁定程度。还可以使用“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“异常用户”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。

### 锁定模式行为

在锁定模式下，一些服务会被停用，一些服务只允许特定用户访问。

#### 对不同用户可用的锁定模式服务

当主机正在运行时，可用服务取决于锁定模式是否激活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、通过 vSphere 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) 服务处于停用状态。
  - 在正常锁定模式下，“例外用户”列表中具有管理员特权的帐户可以访问 DCUI。此外，`DCUI.Access` 高级系统设置中指定的所有用户也可以访问 DCUI。
- 如果已激活 **ESXi Shell** 或 **SSH** 且将主机置于锁定模式，则“例外用户”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，将停用 **ESXi Shell** 或 **SSH** 访问。不具备管理员特权的用户的 **ESXi** 或 **SSH** 会话将关闭。

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 3-8. 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) Exception 用户，基于特权 vCloud Director (vsiauser，如果可用)	vCenter (vpxuser) Exception 用户， 基于特权 vCloud Director (vsiauser，如果可用)
直接控制台 UI (DCUI)	拥有主机管理员特权的用户 和 DCUI.Access 高级系统 设置中指定的用户	DCUI.Access 高级系统设置 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（如果已激活） 和 SSH（如果已激活）	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 高级系统设置中定义 的用户 具有主机管理员特权的异常用户

### 在激活锁定模式时登录到 ESXi Shell 的用户的锁定模式行为

在激活锁定模式之前，用户可以登录 ESXi Shell 或通过 SSH 访问主机。在这种情况下，“例外用户”列表中具有主机管理员特权的用户仍保持登录状态。所有其他用户的会话将关闭。终止在正常锁定模式和严格锁定模式下均适用。

### 如何停用锁定模式

您可以按以下方式停用锁定模式。

#### 从 vSphere Client 中

用户可以从 vSphere Client 中停用正常锁定模式和严格锁定模式。请参见[从 vSphere Client 停用锁定模式](#)。

#### 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停用正常锁定模式。在严格锁定模式下，直接控制台界面服务已停止。请参见[从直接控制台用户界面激活或停用正常锁定模式](#)。

### 从 vSphere Client 激活锁定模式

选择锁定模式以要求所有主机配置更改都通过 vCenter Server 进行。vSphere 支持正常锁定模式和严格锁定模式。

如果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。激活严格锁定模式后，如果 vCenter Server 不可用，并且 SSH 和 ESXi Shell 处于停用状态，用户将无法访问主机。请参见[锁定模式行为](#)。



**步骤**

- 1 在 vSphere Client 清单中，浏览到主机。
- 2 单击**配置**。
- 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。如果激活了 SSH 或 ESXi Shell，则可以访问。
严格	只能通过 vCenter Server 访问主机。如果激活了 SSH 或 ESXi Shell，DCUI.Access 高级系统设置中的帐户以及具有管理员特权的“例外用户”帐户的正在运行的会话仍处于启用状态。所有其他会话将关闭。

- 6 单击**确定**。

**从 vSphere Client 停用锁定模式**

停用锁定模式后配置更改可通过直接连接传递到 ESXi 主机。激活锁定模式可确保环境更安全。

用户可以从 vSphere Client 中停用正常锁定模式和严格锁定模式。

**步骤**

- 1 在 vSphere Client 清单中，浏览到主机。
- 2 单击**配置**。
- 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**已禁用**以停用锁定模式。
- 6 单击**确定**。

**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激活或停用正常锁定模式**

可以从直接控制台用户界面 (DCUI) 激活和停用正常锁定模式。只能从 vSphere Client 激活和停用严格锁定模式。

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 `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激活访问权限。

激活锁定模式时，将保留用户权限。用户权限在您从直接控制台界面停用锁定模式时还原。

---

**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 **ESXi6.0**，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 Client** 停用主机的锁定模式。

---

#### 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，可以指定能够访问 **ESXi** 主机的单个用户。

#### vSphere 处于锁定模式时帐户可以执行的操作

vSphere 版本决定激活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。

- 在 vSphere 5.0 和早期版本中，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，可以将用户添加到每个主机的 `DCUI.Access` 高级系统设置中。该设置在 **vCenter Server** 出现灾难性故障时使用。公司通常将拥有此访问权限的用户的密码锁入保险箱内。`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 Client** 指定异常用户。

---

**注** 例外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 高级系统设置

出现灾难性故障时，如果无法从 vCenter Server 访问主机，可以通过 DCUI.Access 高级系统设置退出锁定模式。可以通过从 vSphere 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。更改锁定模式的功能可能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“例外用户”列表中。例外用户只能执行自己有权执行的任务。请参见本主题后面的“指定锁定模式异常用户”。

---

- 1 在 vSphere Client 清单中，浏览到主机。
- 2 单击**配置**。
- 3 在“系统”下，单击**高级系统设置**，然后单击**编辑**。
- 4 筛选 DCUI。
- 5 在 **DCUI.Access** 文本框中，输入本地 ESXi 用户名，用逗号分隔。

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，并指定命名帐户以增强可审核性。

- 6 单击**确定**。

## 指定锁定模式异常用户

可以通过 vSphere Client 将用户添加到“例外用户”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，例外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“例外用户”列表违背了锁定模式的初衷。

---

例外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停用锁定模式。

- 1 在 vSphere Client 清单中，浏览到主机。
- 2 单击**配置**。
- 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**例外用户**，然后单击**添加用户**图标以添加例外用户。
- 6 单击**确定**。

## 使用 vSphere 安装包执行安全更新

使用 ESXCLI 升级 ESXi 需要了解 vSphere 安装包、映像配置文件和软件库。

ESXi 包含映像配置文件，该配置文件描述了一组包含实际软件的 vSphere 安装包 (VIB)。VIB 是表示系统组件的签名 ramdisk，大致类似于 Linux 系统上的 RPM 或 DEB。映像配置文件是 VIB 集合。软件库是 VIB 和映像配置文件的集合。ESXi 修补程序和库包含由一组常用 VIB 组成的更新映像配置文件。

可以使用 `esxcli software` 命令在独立主机上安装 ESXi 更新。有关详细信息，请参见《VMware ESXi 升级》文档。

---

**注** 通常，在 vSphere 7.0 及更高版本的环境中，可以使用 VMware vSphere® vSphere Lifecycle Manager 对 ESXi 主机进行生命周期管理。

---

要列出所有已安装的 VIB 及其当前版本或当前映像配置文件，您可以使用以下 ESXCLI 命令。

- `esxcli software vib list`
- `esxcli software profile get`

通常，可以使用以下简要步骤安全地升级 ESXi：

- 将 ESXi 主机置于维护模式
- 运行 `esxcli software profile update` 命令，该命令指向 URL 或通过 SSH 传输到主机的 ZIP 文件
- 重新启动 ESXi 主机

由于 VMware 会对 VIB 进行加密签名，因此不需要安全传输 VIB 或整个库，更新过程会验证这些签名。

## 管理 ESXi 主机和 vSphere 安装包的接受级别

vSphere 安装包 (VIB) 的接受级别由该 VIB 的证书数量决定。ESXi 主机的接受级别由最低 VIB 接受级别决定。如果您要允许使用较低级别的 VIB，则可以更改主机的接受级别。您可以移除由社区支持的 VIB，这样就可以更改主机的接受级别。

VIB 是包含 VMware 或 VMware 合作伙伴签名的软件包。为保护 ESXi 主机的完整性，请不要允许用户安装未签名的（由社区支持的）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。由社区支持的 VIB 没有数字签名。

ESXi 主机的接受级别限制必须与要添加到该主机的任何 VIB 的接受级别相同或更少。例如，如果主机的接受级别是由 VMware 接受，则您无法安装接受级别为由合作伙伴支持的 VIB。可以使用 ESXCLI 命令来设置主机的接受级别。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（社区支持的）VIB。

ESXi 主机的接受级别显示在 vSphere Client 的**安全配置文件**中。

支持以下接受级别。

### VMware 认证

“VMware 认证”接受级别具有最严格的要求。此级别的 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。当前，只有 I/O Vendor Program (IOVP) 程序驱动程序在此级别发布。VMware 受理此接受级别的 VIB 的支持致电。

## VMware 认可

此接受级别的 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，以此级别发布的 VIB 包括 CIM 提供程序和 PSA 插件。VMware 会引导 VIB 的支持致电为此接受级别的客户联系合作伙伴的支持部门。

## 合作伙伴支持

接受级别为“合作伙伴支持”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。合作伙伴要在 VMware 系统中启用的新的或非主流的技术将使用此级别。现在，驱动程序 VIB 技术（例如 Infiniband、ATAoE 和 SSD）处于此级别，且具有非标准的硬件驱动程序。VMware 会引导 VIB 的支持致电为此接受级别的客户联系合作伙伴的支持部门。

## 社区支持

“社区支持”接受级别用于由 VMware 合作伙伴程序外部的个人或公司创建的 VIB。此级别的 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 使用 SSH 连接至每个 ESXi 主机。
- 2 通过运行以下命令确认已将接受级别设置为由 VMware 认证、由 VMware 接受或由合作伙伴支持。

```
esxcli software acceptance get
```

- 3 如果该主机的接受级别为由社区支持，通过运行以下命令确认是否有任何 VIB 的接受级别为由社区支持。

```
esxcli software vib list
esxcli software vib get -n vibname
```

- 4 通过运行以下命令移除所有由社区支持的 VIB。

```
esxcli software vib remove --vibname vib
```

## 5 使用以下方法之一更改主机的接受级别。

选项	描述
CLI 命令	<pre>esxcli software acceptance set --level level</pre> <p>需要 level 参数，它指定了要设置的接受级别。应为 <b>VMwareCertified</b>、<b>VMwareAccepted</b>、<b>PartnerSupported</b> 或 <b>CommunitySupported</b> 之一。有关详细信息，请参见《ESXCLI 参考指南》。</p>
vSphere Client	<ol style="list-style-type: none"> <li>在清单中选择主机。</li> <li>单击<b>配置</b>。</li> <li>在“系统”下，选择<b>安全配置文件</b>。</li> <li>单击主机映像配置文件接受级别对应的<b>编辑</b>，然后选择接受级别。</li> </ol>

### 结果

新的接受级别生效。

**注** ESXi 会对接受级别监管的 VIB 执行完整性检查。您可以使用 `VMkernel.Boot.execInstalledOnly` 设置指示 ESXi 仅执行主机上安装的有效 VIB 中的二进制文件。该设置与安全引导结合使用，可确保 ESXi 主机上运行的每一个进程都是签名、允许和预期的进程。在 vSphere 7 中，默认为合作伙伴兼容性停用 `VMkernel.Boot.execInstalledOnly` 设置。尽可能激活此设置以提高安全性。有关配置 ESXi 高级选项的详细信息，请参见 VMware 知识库文章，网址为 <https://kb.vmware.com/kb/1038578>。

## 为 ESXi 主机分配特权

通常，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 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，并为有限数量的用户分配管理员角色。随后，这些用户可以对 ESXi 主机执行直接管理。请参见[使用 vCenter Server 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

可以在 VMware Host Client 的“管理”选项卡中添加本地用户及定义自定义角色。请参见《vSphere 单台主机管理 - VMware Host Client》文档。

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。此角色为默认角色。可以替代默认角色。

您可以使用直接连接到 ESXi 主机的 VMware Host 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。请参见《vSphere 单台主机管理 - VMware Host Client》文档。

在 vSphere 6.0 及更高版本中，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 ESXi 用户分配某个角色，则不会为 vCenter Server 用户分配同一角色。

---

## 预定义的 ESXi 用户和特权

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

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。

分配 root 用户权限可以更方便地访问 ESXi 主机，因为其名称已知。但是使用公共 root 帐户难以确定每个用户执行的操作。

为了更好地进行审核，可以创建具有管理员特权的各个帐户。为 root 帐户设置一个高度复杂的密码，并限制 root 帐户的使用，例如向 vCenter Server 添加主机时使用 root 帐户。不要移除 root 帐户。有关向 ESXi 主机的用户分配权限的详细信息，请参见《vSphere 单台主机管理 - VMware Host Client》文档。

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。使用 ESXi Active Directory 功能，以便管理 Active Directory 凭据。

---

**重要说明** 您可以移除 root 用户的访问特权。但是，必须首先在 root 级别创建可向另一个用户分配管理员角色的另一种权限。

---

### vpxuser 用户

管理主机的活动时，vCenter Server 使用 vpxuser 特权。

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。只有拥有管理员特权的用户才能直接在主机上执行这些任务。

无法使用 Active Directory 管理 vpxuser 用户。

---

**小心** 不要以任何方式更改 vpxuser 用户。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问题。

---

## dcui 用户

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。

## 停用非 ESXi 用户的 Shell 访问

从 vSphere 8.0 开始，可以使用 API 或 ESXCLI 停用 vpxuser 用户和 dcui 用户的 Shell 访问。您还可以使用 API 或 ESXCLI 防止 vpxuser 用户更改其他用户的密码。做出此类更改时，请确认它们不会破坏现有的第三方工作流。有关详细信息，请参见 API 或 ESXCLI 文档。

## 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。

## 配置 ESXi 主机以使用 Active Directory

可以对 ESXi 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**，则会向其分配对该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。

完全限定域名 = *host\_name.domain\_name*

#### 步骤

- 1 同步 ESXi 和目录服务系统的时间。

有关如何使用 Microsoft 域控制器同步 ESXi 时间的信息，请参见[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 Client 清单中，浏览到主机。
  - b 单击**配置**。
  - c 在“网络”下，单击 **TCP/IP 配置**。
  - d 在“TCP/IP 堆栈: 默认”下，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

将主机加入到目录服务域。请参见[将 ESXi 主机添加到目录服务域](#)。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](#)。您可以配置权限，以便已加入的 Active Directory 域中的用户和组配置可以访问 vCenter Server 组件。有关管理权限的信息，请参见[将权限添加到清单对象](#)。

## 将 ESXi 主机添加到目录服务域

要让 ESXi 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 Client 清单中，浏览到主机。
- 2 单击**配置**。
- 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。

#### 后续步骤

您可以配置权限，以便已加入的 Active Directory 域中的用户和组配置可以访问 vCenter Server 组件。有关管理权限的信息，请参见[将权限添加到清单对象](#)。

## 查看 ESXi 主机的目录服务设置

可以查看 ESXi 主机用于对用户进行身份验证的目录服务器的类型（如果有）和目录服务器设置。

#### 步骤

1 在 vSphere Client 清单中，浏览到主机。

2 单击**配置**。

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。

#### 后续步骤

您可以配置权限，以便已加入的 Active Directory 域中的用户和组配置可以访问 vCenter Server 组件。有关管理权限的信息，请参见[将权限添加到清单对象](#)。

## 使用 vSphere Authentication Proxy

您可以通过使用 vSphere Authentication Proxy 将 ESXi 主机添加到 Active Directory 域，而不是将主机明确添加到 Active Directory 域。

您只需设置主机，使其能够识别 Active Directory 服务器的域名和 vSphere Authentication Proxy 的 IP 地址。当启用了 vSphere Authentication Proxy 时，其会自动将使用 Auto Deploy 置备的主机添加到 Active Directory 域。您还可以对未使用 Auto Deploy 置备的主机使用 vSphere Authentication Proxy。

有关 vSphere Authentication Proxy 所用 TCP 端口的信息，请参见 [vCenter Server](#) 的所需端口。

#### Auto Deploy

如果使用 Auto Deploy 置备主机，可以设置指向 Authentication Proxy 的引用主机。随后可以设置一个规则，将引用主机的配置文件应用到使用 Auto Deploy 置备的所有 ESXi 主机。vSphere Authentication Proxy 会将 Auto Deploy 使用 PXE 置备的所有主机的 IP 地址存储在其访问控制列表中。主机在引导时会与 vSphere Authentication Proxy 联系，而 vSphere Authentication Proxy 会将其访问控制列表中已存在的主机加入到 Active Directory 域中。

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，即可无缝运行相关过程。

请参见将 [Auto Deploy](#) 设为辅助证书颁发机构。

## 其他 ESXi 主机

如果您希望其他主机能够在不使用 Active Directory 凭据的情况下加入域，可以将这些主机设置为使用 vSphere Authentication Proxy。这意味着，您无需将 Active Directory 凭据传输到主机，且无需在主机配置文件中保存 Active Directory 凭据。

在此情况下，需要将主机的 IP 地址添加到 vSphere Authentication Proxy 访问控制列表，而 vSphere Authentication Proxy 默认情况下会根据主机 IP 地址对主机进行授权。您可以通过启用客户端身份验证，让 vSphere Authentication Proxy 检查主机证书。

**注** 不能在仅支持 IPv6 的环境中使用 vSphere Authentication Proxy。

## 启动 vSphere Authentication Proxy 服务

每个 vCenter Server 系统都提供了 vSphere Authentication Proxy 服务。默认情况下，该服务没有运行。如果要在环境中使用 vSphere Authentication Proxy，可以通过 vCenter Server 管理界面或命令行启动该服务。

vSphere Authentication Proxy 服务绑定到 IPv4 地址以实现与 vCenter Server 通信，而不支持 IPv6。vCenter Server 实例可以存在于仅 IPv4 或 IPv4/IPv6 混合模式的网络环境中的主机上。但是，指定 vSphere Authentication Proxy 的地址时，必须指定 IPv4 地址。

### 前提条件

请验证您使用的是否是 vCenter Server 6.5 或更高版本。在 vSphere 早期版本中，单独安装 vSphere Authentication Proxy。有关产品早期版本的说明，请参见相关文档。

### 步骤

- 1 启动 VMware vSphere Authentication Proxy 服务。

选项	描述
vCenter Server 管理界面	<ol style="list-style-type: none"> <li>a 在 Web 浏览器中，输入 <code>https://vCenter Server vcenter-IP-address-or-FQDN:5480</code> 转至管理界面。</li> <li>b 以 root 用户身份登录。 默认 root 密码是您在部署 vCenter Server 时设置的密码。</li> <li>c 单击<b>服务</b>，然后单击 <b>VMware vSphere Authentication Proxy</b> 服务。</li> <li>d 单击<b>启动</b>。</li> <li>e （可选）启动该服务后，单击<b>设置启动类型</b>，然后单击<b>自动</b>以实现自动启动。</li> </ol>
CLI	<pre>service-control --start vmcam</pre>

- 2 确认服务已成功启动。

### 结果

您现在可以设置 vSphere Authentication Proxy 域。之后，vSphere Authentication Proxy 会处理所有使用 Auto Deploy 置备的主机，您可以明确地将主机添加到 vSphere Authentication Proxy。

## 使用 vSphere Client 将域添加到 vSphere Authentication Proxy

可以从 vSphere Client 向 vSphere Authentication Proxy 添加域。

只有在启用 vSphere Authentication Proxy 后，才能向其添加域。添加域后，vSphere Authentication Proxy 会将使用 Auto Deploy 置备的所有主机都添加到该域中。对于其他主机，如果您不希望向它们授予域特权，也可以使用 vSphere Authentication Proxy。

### 步骤

- 1 通过 vSphere Client 连接到 vCenter Server 系统。
- 2 选择 vCenter Server，并单击**配置**。
- 3 单击**身份验证代理**，然后单击**编辑**。
- 4 输入 vSphere Authentication Proxy 将向其添加主机的域的域名，以及拥有将主机添加到域的 Active Directory 特权的用户的用户名和密码。
- 5 单击**保存**。

## 使用 camconfig 命令向 vSphere Authentication Proxy 添加域

可以使用 camconfig 命令向 vSphere Authentication Proxy 添加域。

只有在启用 vSphere Authentication Proxy 后，才能向其添加域。添加域后，vSphere Authentication Proxy 会将使用 Auto Deploy 置备的所有主机都添加到该域中。对于其他主机，如果您不希望向它们授予域特权，也可以使用 vSphere Authentication Proxy。

### 步骤

- 1 以具有管理员特权的用户身份登录到 vCenter Server 系统。
- 2 运行以下命令以启用对 Bash shell 的访问。

```
shell
```

- 3 转到 **camconfig** 脚本所在的 `/usr/lib/vmware-vmcam/bin/` 目录。
- 4 要将域和用户 Active Directory 凭据添加到 Authentication Proxy 配置，请运行以下命令。

```
camconfig add-domain -d domain -u user
```

系统将提示您输入密码。

vSphere Authentication Proxy 会缓存该用户名和密码。您可以根据需要移除用户，然后重新创建用户。该域必须可以通过 DNS 访问，但不必是 vCenter Single Sign-On 标识源。

vSphere Authentication Proxy 使用用户指定的用户名，为 Active Directory 中的 ESXi 主机创建帐户。用户必须拥有在您向其中添加主机的 Active Directory 域中创建帐户的特权。撰写此信息时，Microsoft 知识库文章 932455 已经列出了帐户创建特权的背景信息。

- 5 如果您稍后要从 vSphere Authentication Proxy 中移除该域和用户信息，请运行以下命令。

```
camconfig remove-domain -d domain
```

## 使用 vSphere Authentication Proxy 将主机添加到域

Auto Deploy 服务器会将其置备的所有主机添加到 vSphere Authentication Proxy，而 vSphere Authentication Proxy 会将这些主机添加到域中。如果要使用 vSphere Authentication Proxy 将其他主机添加到域中，可以将这些主机明确添加到 vSphere Authentication Proxy。随后，vSphere Authentication Proxy 服务器会将这些主机添加到域中。因此，无需再将用户提供的凭据传输到 vCenter Server 系统。

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

- 如果 ESXi 主机使用的是 VMCA 签名证书，请确认是否已将该主机添加到 vCenter Server。否则，Authentication Proxy 服务无法信任 ESXi 主机。
- 如果 ESXi 主机使用的是根 CA 签名证书，请确认已将适当的根 CA 签名证书添加到 vCenter Server 系统。请参见管理 [ESXi 主机的证书](#)。

### 步骤

- 1 在 vSphere Client 清单中，浏览到主机。
- 2 单击**配置**。
- 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**（例如 **mydomain.com**）或 **name.tld/container/path** 形式（例如 **mydomain.com/organizational\_unit1/organizational\_unit2**）。

- 6 选择**使用代理服务器**。
- 7 输入 Authentication Proxy 服务器的 IP 地址，其应始终与 vCenter Server 系统的 IP 地址相同。
- 8 单击**确定**。

## 为 vSphere Authentication Proxy 激活客户端身份验证

默认情况下，如果 vSphere Authentication Proxy 的访问控制列表中有某个主机的 IP 地址，它就会添加该主机。为了增强安全性，您可以激活客户端身份验证。如果激活了客户端身份验证，vSphere Authentication Proxy 还会检查该主机的证书。

### 前提条件

- 请验证 vCenter Server 系统是否信任主机。默认情况下，当您将主机添加到 vCenter Server 时，该主机会分配到一个由 vCenter Server 受信任根 CA 签名的证书。vSphere Authentication Proxy 信任 vCenter Server 受信任根 CA。
- 如果您计划替换环境中的 ESXi 证书，请在激活 vSphere Authentication Proxy 之前替换。ESXi 主机上的证书必须与该主机注册的证书匹配。

### 步骤

- 1 以具有管理员特权的用户身份登录到 vCenter Server 系统。
- 2 要激活对 Bash shell 的访问，请运行 shell 命令。
- 3 转到 **camconfig** 脚本所在的 `/usr/lib/vmware-vmcam/bin/` 目录。
- 4 要激活客户端身份验证，请运行以下命令。

```
camconfig ssl-cliAuth -e
```

接下来，vSphere Authentication Proxy 会检查每个已添加主机的证书。

- 5 如果您稍后要再次停用客户端身份验证，请运行以下命令。

```
camconfig ssl-cliAuth -n
```

## 将 vSphere Authentication Proxy 证书导入到 ESXi 主机

默认情况下，ESXi 主机需要对 vSphere Authentication Proxy 证书进行明确验证。如果使用 vSphere Auto Deploy，可以借助 Auto Deploy 服务为它所置备的主机添加证书。对于其他主机，必须明确添加证书。

### 前提条件

- 将 vSphere Authentication Proxy 证书上载到 ESXi 主机可访问的数据存储。通过使用 WinSCP 等 SFTP 应用程序，可以从 vCenter Server 主机的以下位置下载证书。

```
/var/lib/vmware/vmcam/ssl/rui.crt
```

- 验证是否已将 `UserVars.ActiveDirectoryVerifyCAMCertificate` ESXi 高级设置设置为 1（默认）。

### 步骤

- 1 选择 ESXi 主机，然后单击**配置**。
- 2 在**系统**下，选择**身份验证服务**。
- 3 单击**导入证书**。
- 4 采用格式 `[datastore]/path/certname.crt` 输入证书文件路径，然后单击**确定**。

## 为 vSphere Authentication Proxy 生成新证书

可以生成 VMware 证书颁发机构 (VMCA) 置备的新证书，或将 VMCA 作为从属证书包括在内的新证书。

如果要使用第三方或企业 CA 签名的自定义证书，请参见[设置 vSphere Authentication Proxy 以使用自定义证书](#)。

### 前提条件

您必须对运行 vSphere Authentication Proxy 的系统拥有 root 或管理员特权。

### 步骤

- 1 创建 `certtool.cfg` 的副本。

```
cp /usr/lib/vmware-vmca/share/config/certtool.cfg /var/lib/vmware/vmcam/ssl/vmcam.cfg
```

- 2 使用您组织的一些相关信息编辑该副本，如以下示例所示。

```
Country = IE
Name = vmcam
Organization = VMware
OrgUnit = vTSU
State = Cork
Locality = Cork
Hostname = test-cam-1.test1.vmware.com
```

- 3 在 `/var/lib/vmware/vmcam/ssl/` 中生成新的专用密钥。

```
/usr/lib/vmware-vmca/bin/certtool --genkey --privkey=/var/lib/vmware/vmcam/ssl/rui.key --pubkey=/tmp/vmcam.pub --server=localhost
```

对于 `localhost`，请提供 vCenter Server 的 FQDN。

- 4 使用在步骤 1 和步骤 2 中创建的密钥和 `vmcam.cfg` 文件在 `/var/lib/vmware/vmcam/ssl/` 中生成新证书。

```
/usr/lib/vmware-vmca/bin/certtool --server=localhost --gencert --privkey=/var/lib/vmware/vmcam/ssl/rui.key --cert=/var/lib/vmware/vmcam/ssl/rui.crt --config=/var/lib/vmware/vmcam/ssl/vmcam.cfg
```

对于 `localhost`，请提供 vCenter Server 的 FQDN。

## 设置 vSphere Authentication Proxy 以使用自定义证书

使用具有 vSphere Authentication Proxy 的自定义证书包含多个步骤。首先，生成 CSR 并将其发送给 CA 进行签名。然后，将已签名证书和密钥文件放在 vSphere Authentication Proxy 能够访问的位置。

默认情况下，vSphere Authentication Proxy 会在首次引导期间生成 CSR 并要求 VMCA 签署此 CSR。vSphere Authentication Proxy 将使用此证书向 vCenter Server 进行注册。将自定义证书添加到 vCenter Server 后，即可在环境中使用这些证书。

## 步骤

### 1 为 vSphere Authentication Proxy 生成 CSR。

- a 创建配置文件 `/var/lib/vmware/vmcam/ssl/vmcam.cfg`，如下例所示。

```
[ req ]
distinguished_name = req_distinguished_name
encrypt_key = no
prompt = no
string_mask = nombstr
req_extensions = v3_req
[ v3_req ]
basicConstraints = CA:false
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = DNS:dns.static-1.csl.vmware.com
[ req_distinguished_name ]
countryName = IE
stateOrProvinceName = Cork
localityName = Cork
0.organizationName = VMware
organizationalUnitName = vTSU
commonName = test-cam-1.test1.vmware.com
```

- b 运行 `openssl` 以生成 CSR 文件和密钥文件，同时传入配置文件。

```
openssl req -new -nodes -out vmcam.csr -newkey rsa:2048 -keyout /var/lib/vmware/
vmcam/ssl/rui.key -config /var/lib/vmware/vmcam/ssl/vmcam.cfg
```

### 2 备份 `rui.crt` 证书和 `rui.key` 文件，它们存储在以下位置。

`/var/lib/vmware/vmcam/ssl/rui.crt`

### 3 取消注册 vSphere Authentication Proxy。

- a 转到 `camregister` 脚本所在的 `/usr/lib/vmware-vmcam/bin` 目录。
- b 运行下列命令。

```
camregister --unregister -a VC_address -u user
```

*user* 必须是对 vCenter Server 拥有管理员权限的 vCenter Single Sign-On 用户。

#### 4 停止 vSphere Authentication Proxy 服务。

工具	步骤
vCenter Server 配置管理界面	<ol style="list-style-type: none"> <li>在 Web 浏览器中，输入 <code>https://vcenter-ip-address-or-FQDN:5480</code>，转至 vCenter Server 配置管理界面。</li> <li>以 root 用户身份登录。 默认 root 密码是您在部署 vCenter Server 时设置的密码。</li> <li>单击<b>服务</b>，然后单击 <b>VMware vSphere Authentication Proxy</b> 服务。</li> <li>单击<b>停止</b>。</li> </ol>
CLI	<code>service-control --stop vmcam</code>

5 将现有 `rui.crt` 证书和 `rui.key` 文件替换为从 CA 收到的文件。

6 重新启动 vSphere Authentication Proxy 服务。

7 使用新证书和密钥向 vCenter Server 明确地重新注册 vSphere Authentication Proxy。

```
camregister --register -a VC_address -u user -c full_path_to_rui.crt -k
full_path_to_rui.key
```

## 为 ESXi 配置和管理智能卡身份验证

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，而不是指定用户名和密码。

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因素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 会显示登录 ID，并提示您输入 PIN。
- 3 输入 PIN 后，ESXi 主机会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。



## 激活智能卡身份验证

激活智能卡身份验证后，在登录到 ESXi DCUI 时，会提示您提供智能卡和 PIN。

### 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 Client 添加根证书。请参见 [管理 ESXi 主机的证书](#)。

### 步骤

- 1 在 vSphere Client 清单中，浏览到主机。
- 2 单击**配置**。
- 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。  
证书必须采用 PEM 格式。
- 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**。

## 停用智能卡身份验证

停用智能卡身份验证以恢复 ESXi DCUI 登录的默认用户名和密码身份验证。

### 步骤

- 1 在 vSphere Client 清单中，浏览到主机。
- 2 单击**配置**。
- 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，使用用户名和密码进行身份验证

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。在这种情况下，您可以使用本地 ESXi 管理员用户的凭据登录到 ESXi DCUI。登录后，您可以执行诊断或其他紧急操作。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

激活时，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。锁定模式可能会导致智能卡身份验证不再起作用。

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 Client 将用户添加到“例外用户”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。

## 使用 ESXi Shell

ESXi Shell 提供基本维护命令，且默认情况下，在 ESXi 主机上处于停用状态。如有必要，可以激活对 shell 的本地或远程访问。为了降低未经授权访问风险，请激活 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（如果已激活）。

适用服务如下所示。

### ESXi Shell

激活此服务以本地访问 ESXi Shell。

### SSH

激活此服务以使用 SSH 远程访问 ESXi Shell。

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 时才激活它。

---

- **使用 vSphere Client 设置 ESXi Shell 的闲置超时**

如果您在主机上启用了 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。可以通过为闲置会话设置超时来防止出现此问题。

- **使用 vSphere Client 设置 ESXi Shell 的可用性超时**

ESXi Shell 默认处于停用状态。您可设置 ESXi Shell 的可用性超时，提高激活 shell 时的安全性。

- **使用 DCUI 设置 ESXi Shell 的可用性超时或闲置超时**

ESXi Shell 默认处于停用状态。要提高激活 Shell 时的安全性，可以设置可用性超时或闲置超时，也可以同时设置两者。

- **使用 vSphere Client 激活对 ESXi Shell 的访问**

默认情况下，ESXi Shell 和 SSH 接口处于停用状态。除非要执行故障排除或支持活动，否则这些接口应保持停用状态。对于日常活动，请使用 vSphere Client，使活动受制于基于角色的访问控制和现代访问控制方法。

- **使用 DCUI 激活对 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。评估您的环境安全要求是否支持激活直接控制台用户界面。

- **登录 ESXi Shell 以进行故障排除**

使用 vSphere Client、ESXCLI 或 VMware 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 Client 设置 ESXi Shell 的闲置超时

如果您在主机上启用了 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。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 Client 中控制本地和远程 (SSH) 会话的时间量。

### 步骤

- 1 在 vSphere Client 清单中，浏览到主机。
- 2 单击**配置**。
- 3 在“系统”下，选择**高级系统设置**。
- 4 单击**编辑**，选择 `UserVars.ESXiShellInteractiveTimeout`，然后输入超时设置。

值为零 (0) 表示停用空闲时间。

5 重新启动 ESXi Shell 服务和 SSH 服务，以使此超时生效。

- a 转到**系统 > 服务**。
- b 依次选择 ESXi Shell 和 SSH，然后单击**重新启动**。

#### 结果

如果该会话闲置，则用户将在超时期限过后注销。

## 使用 vSphere Client 设置 ESXi Shell 的可用性超时

ESXi Shell 默认处于停用状态。您可设置 ESXi Shell 的可用性超时，提高激活 shell 时的安全性。

可用性超时设置是激活 ESXi Shell 后且必须登录前可以经过的时间量。超过超时期限之后，该服务会停用并且不允许用户登录。

#### 步骤

- 1 在 vSphere Client 清单中，浏览到主机。
- 2 单击**配置**。
- 3 在“系统”下，选择**高级系统设置**。
- 4 单击**编辑**，然后选择 `UserVars.ESXiShellTimeOut`。
- 5 输入闲置超时设置。
- 6 单击**确定**。
- 7 重新启动 ESXi Shell 服务和 SSH 服务，以使此超时生效。
  - a 转到**系统 > 服务**。
  - b 依次选择 ESXi Shell 和 SSH，然后单击**重新启动**。

#### 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。

## 使用 DCUI 设置 ESXi Shell 的可用性超时或闲置超时

ESXi Shell 默认处于停用状态。要提高激活 Shell 时的安全性，可以设置可用性超时或闲置超时，也可以同时设置两者。

这两种超时类型适用于不同的情况。

### ESXi Shell 闲置超时

如果用户在主机上激活了 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情况。

### ESXi Shell 可用性超时

可用性超时决定最初激活 Shell 之后到登录之前可经过的时间量。如果等待较长时间，则会停用服务，并且您无法登录到 ESXi Shell。

### 前提条件

激活 ESXi Shell。请参见[使用 DCUI 激活对 ESXi Shell 的访问](#)。

### 步骤

- 1 登录到 ESXi Shell。
- 2 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。
- 3 输入闲置超时（以秒为单位）或可用性超时。
- 4 按 Enter 并按 Esc 直到返回到直接控制台用户界面的主菜单。
- 5 单击**确定**。
- 6 重新启动 ESXi Shell 服务和 SSH 服务，以使此超时生效。
  - a 在 vSphere Client 中，选择主机，然后转到**配置 > 系统 > 服务**。
  - b 依次选择 ESXi Shell 和 SSH，然后单击**重新启动**。

### 结果

- 如果设置闲置超时，用户将在会话闲置了指定的时间后注销。
- 如果设置可用性超时，并且您未在该超时经过之前登录，则会再次停用登录。

## 使用 vSphere Client 激活对 ESXi Shell 的访问

默认情况下，ESXi Shell 和 SSH 接口处于停用状态。除非要执行故障排除或支持活动，否则这些接口应保持停用状态。对于日常活动，请使用 vSphere Client，使活动受制于基于角色的访问控制和现代访问控制方法。

---

**注** 使用 vSphere Client、远程命令行工具（ESXCLI 和 PowerCLI）和已发布的 API 来访问主机。不要激活使用 SSH 远程访问主机的功能，特殊要求除外。

---

### 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 在清单中，浏览到主机。
- 2 单击**配置**，然后单击“系统”下的**服务**。
- 3 管理 ESXi、SSH 或直接控制台 UI 服务。
  - a 在“服务”窗格中，选择服务。
  - b 单击**编辑启动策略**，然后选择**手动启动和停止**启动策略。
  - c 要激活服务，请单击**启动**。

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**。

## 后续步骤

设置 ESXi Shell 的可用性超时和闲置超时。请参见[使用 vSphere Client 设置 ESXi Shell 的可用性超时](#)和[使用 vSphere Client 设置 ESXi Shell 的闲置超时](#)。

## 使用 DCUI 激活对 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。评估您的环境安全要求是否支持激活直接控制台用户界面。

可以使用直接控制台用户界面 (DCUI) 激活对 ESXi Shell 的本地和远程访问。可以从连接到主机的物理控制台访问直接控制台用户界面。主机重新引导并加载 ESXi 后，按 F2 以登录到 DCUI。输入您在安装 ESXi 时创建的凭据。

---

**注** 使用直接控制台用户界面、vSphere 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，选择要激活的服务。
  - 启用 ESXi Shell
  - 启用 SSH
- 4 按 Enter 即可激活服务。
- 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 的可用性超时和闲置超时。请参见[使用 DCUI 设置 ESXi Shell 的可用性超时或闲置超时](#)。

## 登录 ESXi Shell 以进行故障排除

使用 vSphere Client、ESXCLI 或 VMware 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。

## ESXi 主机的 UEFI 安全引导

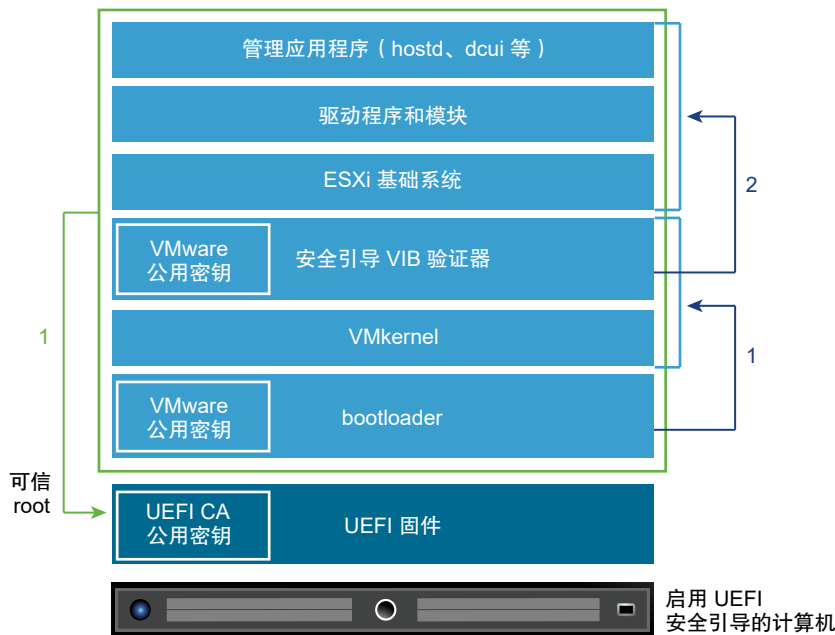
安全引导属于 UEFI 固件标准的一部分。使用安全引导后，计算机会拒绝加载任何 UEFI 驱动程序或应用程序，除非操作系统引导加载程序以加密形式进行签名。在 vSphere 6.5 及更高版本中，如果在硬件中启用了安全引导，则 ESXi 会支持安全引导。

### ESXi 如何使用 UEFI 安全引导

ESXi 版本 6.5 和更高版本在引导堆栈的各个级别上均支持 UEFI 安全引导。

**注** 在已升级的主机上使用 UEFI 安全引导之前，请按照在升级后的 ESXi 主机上运行安全引导验证脚本中的说明检查兼容性。

图 3-1. UEFI 安全引导



使用安全引导后，引导顺序如下所示。

- 1 在 vSphere 6.5 及更高版本中，ESXi 引导加载程序包含 VMware 公钥。该引导加载程序使用此密钥验证内核签名以及包含安全引导 VIB 验证器的小型系统子集。
- 2 VIB 验证器验证系统上安装的每个 VIB 软件包。

此时将引导整个系统以及属于 UEFI 固件的证书中的可信 root。

**注** 当您安装或者升级到 vSphere 7.0 Update 2 或更高版本，并且 ESXi 主机具有 TPM 时，TPM 会基于 UEFI 安全引导的 PCR 值使用 TPM 策略来封装敏感信息。如果符合策略，则后续重新引导期间将加载此值。要在 vSphere 7.0 Update 2 及更高版本中停用或激活 UEFI 安全引导，请参见[激活或停用安全引导实施](#)以获得安全的 ESXi 配置。

## UEFI 安全引导故障排除

如果安全引导在引导顺序的任何一级别上失败，则会出错。

错误消息取决于硬件供应商和验证失败的级别。

- 如果尝试使用未签名或已被篡改的引导加载程序进行引导，则会在执行引导顺序时出错。确切消息取决于硬件供应商。此消息可能类似以下错误，但可能有所不同。

```
UEFI0073: Unable to boot PXE Device...because of the Secure Boot policy
```

- 如果内核已被篡改，则会出现类似以下结果的错误。

```
Fatal error: 39 (Secure Boot Failed)
```

- 如果软件包（VIB 或驱动程序）已被篡改，则会显示紫色屏幕以及以下消息。

```
UEFI Secure Boot failed:
Failed to verify signatures of the following vibs (XX)
```

要使用安全引导解决问题，请执行以下步骤。

- 1 停用安全引导并重新引导主机。
- 2 运行安全引导验证脚本（请参见在升级后的 [ESXi 主机上运行安全引导验证脚本](#)）。
- 3 查看 `/var/log/esxupdate.log` 文件中的信息。

## 在升级后的 ESXi 主机上运行安全引导验证脚本

从不支持 UEFI 安全引导的 ESXi 旧版本升级 ESXi 主机之后，您或许能激活安全引导。能否激活安全引导取决于您执行升级的方式，以及升级是替换所有现有 VIB 还是保持某些 VIB 不变。您可以在执行升级后运行验证脚本以确定升级后的安装是否支持安全引导。

要使安全引导成功，每个已安装 VIB 的签名必须在系统上可用。在安装 VIB 时，ESXi 的旧版本不会保存签名。

- 如果使用 ESXCLI 命令升级，ESXi 的旧版本将安装新 VIB，因此不会保存其签名，并且无法实现安全引导。
- 如果使用 ISO 升级，新 VIB 则会保存其签名。这同样适用于使用 ISO 的 vSphere Lifecycle Manager 升级。
- 如果有旧版 VIB 保留在系统上，这些 VIB 的签名不可用，无法进行安全引导。
  - 如果系统使用第三方驱动程序，而 VMware 升级不包括新版本的驱动程序 VIB，则在升级后旧版本的 VIB 仍会保留在系统上。
  - 在极少数情况下，VMware 可能会停止持续开发特定 VIB，且不提供新版本的 VIB 来替换或弃用它，因此在升级后旧版本的 VIB 会保留在系统上。

---

**注** UEFI 安全引导还需要最新的引导加载程序。此脚本不会检查最新的引导加载程序。

---



### 前提条件

- 验证硬件是否支持 UEFI 安全引导。
- 验证是否所有 VIB 均已签名且接受级别至少为“合作伙伴支持”。如果 VIB 为“社区支持”级别，则无法使用安全引导。

### 步骤

- 1 升级 ESXi 并运行以下命令。

```
/usr/lib/vmware/secureboot/bin/secureBoot.py -c
```

- 2 检查输出结果。

输出包含 Secure boot can be enabled 或 Secure boot CANNOT be enabled。

## 使用可信平台模块保护 ESXi 主机

ESXi 主机可以使用可信平台模块 (Trusted Platform Module, TPM) 芯片，该模块是安全的密码处理器，通过提供植根于硬件（而不是软件）的信任保证来增强主机安全性。



(ESXi 和可信平台模块 2.0 功能演示)

### 什么是 TPM

TPM 是安全密码处理器的行业标准。如今的大多数计算机（从笔记本电脑到台式机、再到服务器）中都含 TPM 芯片。vSphere 6.7 及更高版本支持 TPM 2.0 版本。

TPM 2.0 芯片证明主机的 ESXi 身份。主机证明是在给定时间点对主机软件状态进行身份验证和证明的过程。UEFI 安全引导可确保在引导时只加载签名软件，这是成功证明的一项要求。TPM 2.0 芯片将记录并安全存储系统中引导的软件模块的测量数据，vCenter Server 将远程验证这些测量数据。

远程证明过程的概要步骤为：

- 1 建立远程 TPM 的可信赖度并在其上创建证明密钥 (Attestation Key, AK)。

将 ESXi 主机添加到 vCenter Server、从中重新引导 ESXi 主机或重新连接到 vCenter Server 时，vCenter Server 将从主机请求 AK。AK 创建过程的一部分还涉及到 TPM 硬件本身的验证，以确保已知（且可信）的供应商生成该 TPM 硬件。

- 2 从主机检索证明报告。

vCenter Server 请求主机发送证明报告，其中包含由 TPM 签名的平台配置寄存器 (Platform Configuration Register, PCR) 证言，以及其他签名的主机二进制元数据。通过检查与其认为可信的配置相对应的信息，vCenter Server 将在先前不可信的主机上标识平台。

- 3 验证主机的真实性。

vCenter Server 会验证签名证言的真实性，推断软件版本并确定所述软件版本的可信赖度。如果 vCenter Server 确定签名证言无效，则远程证明失败，该主机不可信。

## 使用 TPM 对 vSphere 有哪些要求

要使用 TPM 2.0 芯片，vCenter Server 环境必须满足以下要求：

- vCenter Server 6.7 或更高版本
- 在 UEFI 中安装有 TPM 2.0 芯片并启用的 ESXi 6.7 主机或更高版本
- 已启用 UEFI 安全引导

确保在 ESXi 主机的 BIOS 中配置了 TPM，以使用 SHA-256 哈希算法和 TIS/FIFO（先进先出）接口，而不是 CRB（命令响应缓冲区）。有关设置这些所需 BIOS 选项的信息，请参阅供应商文档。

在以下位置查看由 VMware 认证的 TPM 2.0 芯片：

<https://www.vmware.com/resources/compatibility/search.php>

## 使用 TPM 引导主机时会发生什么情况

引导安装有 TPM 2.0 芯片的 ESXi 主机时，vCenter Server 将监控主机的证明状态。要查看硬件信任状态，请在 vSphere Client 中选择 vCenter Server，然后选择**安全性**下的**摘要**选项卡。硬件信任状态有以下几种：

- 绿色：正常状态，指示完全信任。
- 红色：证明失败。

---

**注** 如果将 TPM 2.0 芯片添加到 vCenter Server 已管理的 ESXi 主机，则必须先将主机断开连接，然后再将其重新连接。有关断开连接并重新连接主机的信息，请参见《vCenter Server 和主机管理》文档。

---

对于 vSphere 7.0 及更高版本，VMware® vSphere Trust Authority™ 为 ESXi 主机使用远程证明功能。请参见什么是 [vSphere Trust Authority 证明服务](#)。

## 查看 ESXi 主机认证状态

将 ESXi 添加到主机时，可信任平台模块 2.0 兼容芯片将认证平台的完整性。可以在 vSphere Client 中查看主机的认证状态。还可以查看 Intel 可信执行技术 (TXT) 状态。

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 导航到数据中心，然后单击**监控**选项卡。
- 3 单击**安全**。
- 4 在“认证”列中查看主机的状态，并阅读**消息**列中的消息。
- 5 如果此主机是受信任主机，请参见[查看受信任集群证明状态](#)，了解详细信息。

### 后续步骤

有关“失败”或“警告”的认证状态，请参见[对 ESXi 主机认证问题进行故障排除](#)。有关受信任主机，请参见[对受信任主机认证问题进行故障排除](#)。

## 对 ESXi 主机认证问题进行故障排除

在 ESXi 主机上安装可信平台模块 (TPM) 设备时，主机可能无法通过认证。您可以对此问题的潜在原因进行故障排除。

### 步骤

- 1 查看 ESXi 主机警报状态以及随附的错误消息。请参见查看 [ESXi 主机认证状态](#)。
- 2 如果错误消息为主机安全引导已禁用，您必须重新启用安全引导才能解决该问题。
- 3 如果主机的证明状态为失败，请检查 vCenter Server vpxd.log 文件是否存在以下消息：

```
No cached identity key, loading from DB
```

此消息表明您要将 TPM 2.0 芯片添加到 vCenter Server 已管理的 ESXi 主机。您必须先将主机断开连接，然后再将其重新连接。有关断开连接并重新连接主机的信息，请参见《vCenter Server 和主机管理》文档。

有关 vCenter Server 日志文件的详细信息（包括位置和日志轮换），请参见 <https://kb.vmware.com/s/article/1021804> 中的 VMware 知识库文章。

- 4 有关所有其他错误消息，请联系“客户支持部门”。

## ESXi 日志文件

日志文件是对攻击进行故障排除以及获取有关违反情况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。

为了提高主机安全性，请采取下列措施。

- 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。启用持久日志记录时，您将拥有主机的专用活动记录。
- 远程日志记录到中央主机允许您在中央主机上收集日志文件。在该主机中，使用一个工具即可监控所有主机，并可以执行汇总分析和搜索日志数据。这种方法有助于监控和揭示多个主机上协调攻击的相关信息。
- 使用 ESXCLI 或 PowerCLI 或者使用 API 客户端在 ESXi 主机上配置远程安全 syslog。
- 查询 syslog 配置，确保 syslog 服务器和端口有效。

有关 syslog 设置的信息和 ESXi 日志文件的其他信息，请参见《vSphere 监控和性能》文档。

## 在 ESXi 主机上配置 Syslog

可以使用 vSphere Client、VMware Host Client 或 `esxcli system syslog` 命令配置 syslog 服务。

有关使用 `esxcli system syslog` 命令和其他 ESXCLI 命令的信息，请参见《ESXCLI 入门》。有关如何为每个远程主机规范中指定的端口打开 ESXi 防火墙的详细信息，请参见配置 [ESXi 防火墙](#)。

### 步骤

- 1 在 vSphere Client 清单中，浏览到主机。
- 2 单击**配置**。
- 3 在**系统**下，单击**高级系统设置**。
- 4 单击**编辑**。
- 5 筛选出 **syslog**。
- 6 要全局设置日志记录并配置各种高级设置，请参见 [ESXi Syslog 选项](#)。
- 7 （可选）要覆盖任何日志的默认日志大小和日志轮换，请执行以下操作：
  - a 单击要自定义的日志的名称。
  - b 输入所需的轮换数和日志大小。
- 8 单击**确定**。

### 结果

对 syslog 选项的更改生效。

---

**注** 使用 vSphere Client 或 VMware Host Client 定义的 Syslog 参数设置将立即生效。但是，使用 ESXCLI 定义的大多数设置都需要额外命令才能生效。有关更多详细信息，请参见 [ESXi Syslog 选项](#)。

---

## ESXi Syslog 选项

可以使用一组 syslog 选项定义 ESXi syslog 文件和传输的行为。

除了基本设置（如 `Syslog.global.logHost`）之外，从 ESXi 7.0 Update 1 开始，还提供了用于自定义和 NIAP 合规性的高级选项列表。

---

**注** 所有审核记录设置（以 `Syslog.global.auditRecord` 开头）会立即生效。但是，对于使用 ESXCLI 定义的其他设置，请确保运行 `esxcli system syslog reload` 命令以启用更改。

---

表 3-9. 旧版 Syslog 选项

选项	ESXCLI 命令	描述
Syslog.global.logHost	esxcli system syslog config set --loghost=<str>	定义有关消息传输的以逗号分隔的远程主机列表和规范。如果 loghost=<str> 字段为空，则不会转发任何日志。虽然对接收 syslog 消息的远程主机数量没有硬性限制，但最好将远程主机的数量保持在 5 个或 5 个以下。远程主机规范的格式为：protocol://hostname ipv4 ['ipv6'][:port]。该协议必须是 TCP、UDP 或 SSL 之一。端口值可以是介于 1 到 65535 之间的任何十进制数字。如果未提供端口，则 SSL 和 TCP 使用 1514。UDP 使用 514。例如：ssl://hostname1:1514。
Syslog.global.defaultRotate	esxcli system syslog config set --default-rotate=<long>	要保留的旧日志文件的最大数目。您可以在全局范围内设置该数字，也可以针对单个子记录器设置该数字（请参见 Syslog.global.defaultSize）。
Syslog.global.defaultSize	esxcli system syslog config set --default-size=<long>	日志文件的默认大小 (KiB)。文件达到默认大小后，syslog 服务会创建一个新文件。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	esxcli system syslog config set --logdir=<str>	日志所在的目录。该目录可以位于挂载的 NFS 或 VMFS 卷中。只有本地文件系统上的 /scratch 目录在重新引导后仍然存在。将目录指定为 [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 root 目录的路径。例如，路径 [storage1] /systemlogs 将映射为路径 /vmfs/volumes/storage1/systemlogs。
Syslog.global.logDirUnique	esxcli system syslog config set --logdir-unique=<bool>	指定要与 Syslog.global.logDir 值连接的 ESXi 主机名。当多个 ESXi 主机登录到共享文件系统时，启用此设置至关重要。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.certificate.checkSSLCerts	esxcli system syslog config set --check-ssl-certs=<bool>	将消息传输到远程主机时强制检查 SSL 证书。

表 3-10. 从 ESXi 7.0 Update 1 开始可用的 Syslog 选项

选项	ESXCLI 命令	描述
<code>Syslog.global.auditRecord.storageCapacity</code>	<code>esxcli system auditrecords local set --size=&lt;long&gt;</code>	指定位于 ESXi 主机上的审核记录存储目录的容量（以 MiB 为单位）。无法减少审核记录存储的容量。可以在启用审核记录存储之前或之后（请参见 <code>Syslog.global.auditRecord.storageEnable</code> ）增加容量。
<code>Syslog.global.auditRecord.remoteEnable</code>	<code>esxcli system auditrecords remote enable</code>	启用将审核记录发送到远程主机的功能。远程主机通过使用 <code>Syslog.global.logHost</code> 参数指定。
<code>Syslog.global.auditRecord.storageDirectory</code>	<code>esxcli system auditrecords local set --directory=&lt;dir&gt;</code>	指定审核记录存储目录的位置。启用审核记录存储（请参见 <code>Syslog.global.auditRecord.storageEnable</code> ）后，无法更改审核记录存储目录。
<code>Syslog.global.auditRecord.storageEnable</code>	<code>esxcli system auditrecords local enable</code>	在 ESXi 主机上启用审核记录存储。如果审核记录存储目录不存在，则使用 <code>Syslog.global.auditRecord.storageCapacity</code> 指定的容量创建该目录。
<code>Syslog.global.certificate.checkCRL</code>	<code>esxcli system syslog config set --crl-check=&lt;bool&gt;</code>	<p>启用检查 SSL 证书链中所有证书的吊销状态。</p> <p>启用 X.509 CRL 验证，默认情况下不会根据行业约定检查这些 CRL。经过 NIAP 验证的配置需要进行 CRL 检查。由于实施限制，如果启用了 CRL 检查，则证书链中的所有证书都必须提供 CRL 链接。</p> <p>不要为与认证无关的安装启用 <code>crl-check</code> 选项，因为很难正确配置使用 CRL 检查的环境。</p>
<code>Syslog.global.certificate.strictX509Compliance</code>	<code>esxcli system syslog config set --x509-strict=&lt;bool&gt;</code>	<p>启用严格遵守 X.509。在验证期间对 CA 根证书执行额外的有效性检查。通常不会执行这些检查，因为 CA 根本来就受信任，并且可能会导致与现有配置错误的 CA 根不兼容。经过 NIAP 验证的配置甚至需要 CA 根来通过验证。</p> <p>不要为与认证无关的安装启用 <code>x509-strict</code> 选项，因为很难正确配置使用 CRL 检查的环境。</p>
<code>Syslog.global.droppedMsgs.fileRotate</code>	<code>esxcli system syslog config set --drop-log-rotate=&lt;long&gt;</code>	指定要保留的旧的已丢弃消息日志文件数。
<code>Syslog.global.droppedMsgs.fileSize</code>	<code>esxcli system syslog config set --drop-log-size=&lt;long&gt;</code>	指定切换为新的日志文件之前每个已丢弃消息日志文件的大小 (KiB)。

表 3-10. 从 ESXi 7.0 Update 1 开始可用的 Syslog 选项（续）

选项	ESXCLI 命令	描述
Syslog.global.logCheckSSLCerts	esxcli system syslog config set --check-ssl-certs=<bool>	将消息传输到远程主机时强制检查 SSL 证书。  <b>注</b> 已弃用。在 ESXi 7.0 Update 1 及更高版本中使用 Syslog.global.certificate.checkSSLCerts。
Syslog.global.logFilters	esxcli system syslog logfile [add   remove   set] ...	指定一个或多个日志筛选规范。每个日志筛选器必须用双竖线“  ”分隔。日志筛选器的格式为：numLogs   ident   logRegex。numLogs 为指定的日志消息设置最大日志条目数。达到此数目之后，将会筛选并忽略指定日志消息。ident 指定一个或多个系统组件以将筛选器应用于这些组件生成的日志消息。logRegex 使用 Python 正则表达式语法指定区分大小写的短语，以按内容筛选日志消息。
Syslog.global.logFiltersEnable		允许使用日志筛选器。
Syslog.global.logLevel	esxcli system config set --log-level=<str>	指定日志筛选级别。仅当对 syslog 守护进程问题进行故障排除时，才必须更改此参数。可以使用值 debug 表示最详细级别，使用 info 表示默认详细级别，使用 warning 表示仅警告或错误，使用 error 表示仅错误。
Syslog.global.msgQueueDropMark	esxcli system syslog config --queue-drop-mark=<long>	指定占消息队列容量的百分比，达到此值后丢弃消息。
Syslog.global.remoteHost.connectRetryDelay	esxcli system syslog config set --default-timeout=<long>	指定连接尝试失败后重试连接到远程主机之前的延迟（以秒为单位）。
Syslog.global.remoteHost.maxMsgLen	esxcli system syslog config set --remote-host-max-msg-len=<long>	对于 TCP 和 SSL 协议，此参数指定截断发生之前 syslog 传输的最大长度（以字节为单位）。远程主机消息的默认最大长度为 1 KiB。可以将最大消息长度增加到多达 16 KiB。但是，将此值提高到 1 KiB 以上不能确保长传输到达 syslog 收集器时未被截断。例如，发出消息的 syslog 基础架构位于 ESXi 外部时。 RFC 5426 将 UDP 协议的最大消息传输长度设置为 480 字节 (IPv4) 和 1180 字节 (IPv6)。
Syslog.global.vsanBacking	esxcli system syslog config set --vsan-backing=<bool>	允许将日志文件和审核记录存储目录放置在 vSAN 集群上。但是，启用此参数可能会导致 ESXi 主机变得无响应。

## 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。

表 3-11. ESXi 日志文件地址

组件	位置	用途
身份验证	/var/log/auth.log	包含与本地系统身份验证相关的所有事件。
ESXi 主机代理日志	/var/log/hostd.log	包含管理和配置 ESXi 主机及其虚拟机的代理的有关信息。
Shell 日志	/var/log/shell.log	包含键入 ESXiShell 的所有命令以及 Shell 事件（例如启用 Shell）的记录。
系统消息	/var/log/syslog.log	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。
vCenter Server 代理日志	/var/log/vpxa.log	包含与 vCenter Server 通信的代理的相关信息（如果主机由 vCenter Server 管理）。
虚拟机	与受影响虚拟机的配置文件位于同一目录，名为 vmware.log 和 vmware*.log。例如，/vmfs/volumes/datastore/virtual machine/vmware.log	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。
VMkernel	/var/log/vmkernel.log	记录与虚拟机以及 ESXi 有关的活动。
VMkernel 摘要	/var/log/vmksummary.log	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）。
VMkernel 警告	/var/log/vmkwarning.log	记录与虚拟机有关的活动。
快速引导	/var/log/loadESX.log	包含与通过快速引导重新启动 ESXi 主机相关的所有事件。
可信基础架构代理	/var/run/log/kmxa.log	记录与 ESXi 受信任主机上的客户端服务相关的活动。
密钥提供程序服务	/var/run/log/kmxd.log	记录与 vSphere Trust Authority 密钥提供程序服务相关的活动。
证明服务	/var/run/log/attestd.log	记录与 vSphere Trust Authority 证明服务相关的活动。
ESX 令牌服务	/var/run/log/esxtokend.log	记录与 vSphere Trust AuthorityESX 令牌服务相关的活动。
ESX API 转发器	/var/run/log/esxapiadapter.log	记录与 vSphere Trust AuthorityAPI 转发器相关的活动。



## 确保 Fault Tolerance 日志记录通信的安全

VMware Fault Tolerance (FT) 可捕获主虚拟机上发生的输入和事件，然后将它们发送给在其他主机上运行的辅助虚拟机。

主虚拟机与辅助虚拟机之间的该日志记录通信是未加密的，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。此通信可能包含敏感数据，如纯文本格式的密码。为避免这些数据被泄漏，尤其是避免受到“中间人”攻击，请确保此网络是受保护的。例如，对 FT 日志记录通信使用专用网络。您还可以对 FT 日志记录流量进行加密。

### 激活 Fault Tolerance 加密

您可以加密 Fault Tolerance 日志流量。

vSphere Fault Tolerance 会在主虚拟机和辅助虚拟机之间执行频繁检查，以便辅助虚拟机可以从上次成功的检查点快速恢复。检查点包含自上一检查点之后已修改的虚拟机状态。您可以加密 Fault Tolerance 日志流量。

打开 Fault Tolerance 时，FT 加密默认设置为**视情况**，这意味着只有在首选主机和辅助主机均能加密时，才激活加密。如果需要手动更改 FT 加密模式，请执行以下过程。

---

**注** Fault Tolerance 支持 vSphere 7.0 Update 2 及更高版本的 vSphere 虚拟机加密。客户机内和基于阵列的加密不依赖或干扰虚拟机加密。具有多个加密层会使用其他计算资源，这可能会影响虚拟机性能。影响因硬件以及 I/O 的数量和类型而异，但对于大多数工作负载而言，整体性能影响可以忽略不计。去重、压缩和复制等后端存储功能的有效性和兼容性也可能会受到虚拟机加密的影响。

---

#### 前提条件

FT 加密需要 SMP-FT。不支持对旧版 FT（记录/重放 FT）进行加密。

#### 步骤

- 1 选择虚拟机，然后选择**编辑设置**。
- 2 在**虚拟机选项**下，选择**已加密 FT** 下拉菜单。

### 3 选择以下选项之一：

选项	描述
已禁用	不启用加密 Fault Tolerance 日志记录。
视情况	仅在双方均能加密时，才启用加密。允许 Fault Tolerance 虚拟机移动到不支持加密 Fault Tolerance 日志记录的 ESXi 主机。
必需	选择同时支持加密 FT 日志记录的 Fault Tolerance 首选主机和辅助主机。

**注** 激活虚拟机加密后，FT 加密模式默认设置为**必需**，且无法修改。

当 FT 加密模式设置为**必需**时：

- 启用 FT 后，将仅列出支持 FT 加密的主机以便放置 FT 辅助主机。
- 只能在支持 FT 加密的主机上进行 FT 故障切换。

### 4 单击**确定**。

## 管理 ESXi 审核记录

审核记录符合 RFC 5424，且包含与事项相关的事件的信息，例如针对 ESXi 主机上发生的事件记录的时间、状态、描述和用户信息。本地和远程审核记录保留均可用。默认情况下，审核记录保留处于取消激活状态。您必须手动激活本地和远程审核模式。

本地 ESXi 审核日志作为包含近期审核消息的固定大小缓冲区运行。消息填满缓冲区后，新记录将覆盖最早的记录。远程审核日志以标准 syslog 格式 (RFC 3164) 将相同的审核记录流转发到远程服务器，未加密或加密 (RFC 5425) 形式均可。审核消息符合 RFC 5424，但常规 syslog 消息仅符合 RFC 3164。系统将生成的审核消息同时发送到本地存储和远程存储。

在主机与远程存储之间连接中断期间，远程存储会丢弃生成的任何审核消息。重新连接后，系统会生成一条审核消息，指示可能存在消息丢失情况。

## 配置审核记录

可以使用 ESXCLI 配置本地审核记录保留。有关详细信息，请参见《ESXCLI 参考指南》，网址为 <https://code.vmware.com/>。

## 查看审核记录

您可以按如下方式查看审核记录。

- 本地：使用 ESXi /bin/viewAudit 应用程序。
- 远程：使用 ESXCLI 配置远程审核服务器。

您还可以使用 FetchAuditRecords API（在 DiagnosticsManager 受管对象中）查看审核记录。

## 确保 ESXi 配置安全

在 vSphere 7.0 Update 2 及更高版本中，ESXi 配置会受到加密保护。

### 什么是安全的 ESXi 配置

许多 ESXi 服务将密钥存储在其配置文件中。这些配置会作为存储文件存储在 ESXi 主机的引导槽中。在 vSphere 7.0 Update 2 之前，存档的 ESXi 配置文件未加密。在 vSphere 7.0 Update 2 及更高版本中，存档的配置文件已加密。这样，攻击者将无法直接读取或更改此文件，即使他们具有 ESXi 主机存储的物理访问权限。

除了防止攻击者访问密钥外，当 ESXi 安全配置与 TPM 一同使用时，还可以使保存的虚拟机加密密钥在重新引导后仍然存在。为 ESXi 主机配置 TPM，TPM 用于将配置“封装”到主机，从而提供强有力的安全保证。因此，当密钥服务器不可用或无法访问时，加密的工作负载可以继续运行。请参见 [ESXi 主机上的 vSphere 密钥持久性](#)。

您无需手动激活 ESXi 配置加密。安装或升级到 vSphere 7.0 Update 2 或更高版本时，存档的 ESXi 配置文件将被加密。

有关与安全的 ESXi 配置关联的任务，请参见 [管理 ESXi 安全配置](#)。

### vSphere 7.0 Update 2 之前的 ESXi 配置文件概览

ESXi 主机的配置包括主机上运行的每个服务的配置文件。配置文件通常位于 `/etc/` 目录中，但也可以驻留在其他命名空间中。配置文件包含有关服务状态的运行时信息。随着时间的推移，配置文件中的默认值可能会发生变化，例如，当您更改 ESXi 主机上的设置时。cron 作业会定期、在 ESXi 正常关闭时或按需备份 ESXi 配置文件，并在引导槽中创建存档的配置文件。ESXi 在重新引导时，会读取存档的配置文件，并重新创建 ESXi 在创建备份时所处的状态。在 vSphere 7.0 Update 2 之前，存档的配置文件未加密。因此，在系统处于脱机状态时，有权访问物理 ESXi 存储的攻击者可以读取并更改此文件。

### 如何实施安全的 ESXi 配置

在安装或将 ESXi 主机升级到 vSphere 7.0 Update 2 或更高版本后的首次引导过程中，将发生以下情况：

- 如果 ESXi 主机具有 TPM 并在固件中激活了 TPM，则存档的配置文件将通过存储在 TPM 中的加密密钥进行加密。从此时起，主机的配置由 TPM 封装。
- 如果 ESXi 主机不具有 TPM，ESXi 将使用密钥派生功能 (KDF) 为存档的配置文件生成安全配置加密密钥。KDF 的输入存储在磁盘上的 `encryption.info` 文件中。

---

**注** 如果 ESXi 主机具有已激活的 TPM 设备，您将获得额外的保护。

---

ESXi 主机在首次引导之后重新引导时，将发生以下情况：

- 如果 ESXi 主机具有 TPM，则主机必须从该特定主机的 TPM 获取加密密钥。如果 TPM 衡量指标满足创建加密密钥时使用的封装策略，则主机可从 TPM 中获取加密密钥。
- 如果 ESXi 主机不具有 TPM，则 ESXi 将从 `encryption.info` 文件读取信息以解锁安全配置。

## ESXi 安全配置的要求

- ESXi 7.0 Update 2 或更高版本
- 用于配置加密的 TPM 2.0 以及使用封装策略的功能

## ESXi 安全配置恢复密钥

ESXi 安全配置包括一个恢复密钥。如果必须恢复 ESXi 安全配置，请使用包含了您输入为命令行引导选项的内容的恢复密钥。您可以列出恢复密钥以创建恢复密钥备份。您也可以根据安全要求轮换恢复密钥。

备份恢复密钥是管理 ESXi 安全配置的重要部分。vCenter Server 会生成警报，以提醒您备份恢复密钥。

## 安全的 ESXi 配置恢复密钥警报

备份恢复密钥是管理 ESXi 安全配置的重要部分。每当处于 TPM 模式的 ESXi 主机连接或重新连接至 vCenter Server 时，vCenter Server 都会生成警报以提醒您备份恢复密钥。重置警报时，除非情况发生变化，否则不会再次触发警报。

## ESXi 安全配置的最佳做法

请遵循以下安全 ESXi 恢复密钥的最佳做法：

- 列出恢复密钥时，它会暂时显示在不受信任的环境中，并且驻留在内存中。请清除密钥的痕迹。
  - 重新引导主机可去除内存中的残留痕迹。
  - 为增强保护，您可以在主机上激活加密模式。请参见[明确激活主机加密模式](#)。
- 执行恢复时：
  - 要消除不受信任环境中的任何恢复密钥痕迹，请重新引导主机。
  - 为了增强安全性，请在恢复密钥一次后轮换恢复密钥以使用新密钥。

## 什么是 TPM 封装策略

TPM 可以使用平台配置寄存器 (PCR) 衡量指标实施用于限制对敏感数据的未授权访问的策略。安装具有 TPM 的 ESXi 主机或将其升级到 vSphere 7.0 Update 2 或更高版本时，TPM 会使用包含安全引导设置的策略来封装敏感信息。此策略会在首次使用 TPM 封装数据时检查是否已激活安全引导，然后，在后续引导中尝试解封数据时，安全引导必须仍然处于激活状态。

安全引导属于 UEFI 固件标准的一部分。激活 UEFI 安全引导后，主机会拒绝加载任何 UEFI 驱动程序或应用程序，除非操作系统引导加载程序具有有效的数字签名。

您可以选择停用或激活 UEFI 安全引导实施。请参见[激活或停用安全引导实施以获得安全的 ESXi 配置](#)。

**注** 如果在安装或升级到 vSphere 7.0 Update 2 或更高版本时未激活 TPM，可以稍后使用以下命令进行激活。

```
esxcli system settings encryption set --mode=TPM
```

激活 TPM 后，将无法撤消该设置。

即使为主机激活了 TPM，`esxcli system settings encryption set` 命令也会在某些 TPM 上失败。

- 在 vSphere 7.0 Update 2 中：NationZ (NTZ) 的 TPM、Infineon Technologies (IFX) 的 TPM 以及 Nuvoton Technologies Corporation (NTC) 的某些新型号（例如 NPCT75x）
- vSphere 7.0 Update 3 中：来自 NationZ (NTZ) 的 TPM

如果安装或升级 vSphere 7.0 Update 2 或更高版本在首次引导期间无法使用 TPM，则安装或升级将继续，并且模式默认为“无”（即，`--mode=NONE`）。由此引发的行为就像未激活 TPM 一样。

TPM 还可以在封装策略中强制执行 `execInstalledOnly` 引导选项的设置。`execInstalledOnly` 实施是 ESXi 高级引导选项，可保证 VMkernel 仅执行已作为 VIB 的一部分正确打包和签名的二进制文件。`execInstalledOnly` 引导选项依赖于安全引导选项。必须先激活安全引导实施，然后才能在封装策略中强制执行 `execInstalledOnly` 引导选项。请参见[激活或停用 execInstalledOnly 实施以获得安全的 ESXi 配置](#)。

## 管理 ESXi 安全配置

可以使用 ESXCLI 命令列出 ESXi 安全配置恢复密钥、轮换恢复密钥以及更改 TPM 策略（例如，强制执行 UEFI 安全引导）。

### 列出 ESXi 安全配置恢复密钥的内容

可以使用 ESXCLI 显示 ESXi 安全配置恢复密钥的内容。

此任务仅适用于具有 TPM 的 ESXi 主机。通常，您可以列出 ESXi 安全配置恢复密钥的内容以创建备份或轮换恢复密钥。

#### 前提条件

- 有权访问 ESXCLI 命令集。可以远程或在 ESXi Shell 中运行 ESXCLI 命令。
- 具有使用 ESXCLI 独立版本或 PowerCLI 所需的特权：**主机.配置.设置**

#### 步骤

- 1 在 ESXi 主机上运行以下命令。

```
esxcli system settings encryption recovery list
```

- 2 将输出保存在安全的远程位置作为备份，以防出现必须恢复安全配置的情况。

#### 结果

将显示恢复密钥 ID 和密钥。

**示例：列出 ESXi 安全配置恢复密钥**

```
[root@host1] esxcli system settings encryption recovery list
```

Recovery ID	Key
-----	---
{2DDD5424-7F3F-406A-8DA8-D62630F6C8BC}	
478269-039194-473926-430939-686855-231401-642208-184477-602511	
-225586-551660-586542-338394-092578-687140-267425	

**轮换 ESXi 安全配置恢复密钥**

可以使用 ESXCLI 轮换 ESXi 安全配置恢复密钥。

此任务仅适用于具有 TPM 的 ESXi 主机。可以作为安全最佳做法的一部分轮换 ESXi 安全配置恢复密钥。

**前提条件**

- 有权访问 ESXCLI 命令集。可以远程或在 ESXi Shell 中运行 ESXCLI 命令。
- 具有使用 ESXCLI 独立版本或 PowerCLI 所需的特权：**主机.配置.设置**

**步骤**

- 1 列出恢复密钥。

请参见列出 [ESXi 安全配置恢复密钥的内容](#)。

- 2 运行下列命令。

```
esxcli system settings encryption recovery rotate [-k keyID] -u uuid
```

在此命令中，可选的 *keyID* 是 VMkernel 密钥缓存中的密钥 ID，*uuid* 是恢复 ID（从 `esxcli system settings encryption recovery list` 命令获取）。如果不提供可选密钥 ID，ESXi 会将旧恢复密钥替换为随机生成的新恢复密钥。

**结果**

恢复密钥现在设置为密钥 ID 引用的密钥的内容（如果已提供）。否则，ESXi 提供新的密钥 ID。

**ESXi 安全配置的故障排除和恢复**

您可对可能遇到的 ESXi 安全配置问题进行故障排除和恢复。

如果清除了 TPM（即重置 TPM 中的种子值），或者 TPM 失败，则必须采取措施来恢复 ESXi 安全配置。必须具有恢复密钥，才能恢复配置。恢复配置之前，主机 ESXi 无法引导。请参见恢复 [ESXi 安全配置](#)。

ESXi 主机可能无法还原或解密安全配置，从而阻止主机引导，虽然这种情况并不常见。可能的情况包括：

- 更改为安全引导设置（或其他策略）
- 实际篡改
- 恢复密钥不可用

要对这些情况进行故障排除，请参见 VMware 知识库文章，网址：<https://kb.vmware.com/kb/81446>。

## 恢复 ESXi 安全配置

如果 TPM 失败或您清除了 TPM，必须恢复 ESXi 安全配置。恢复配置之前，主机 ESXi 无法引导。

涉及以下情况时，需要恢复 ESXi 安全配置：

- 您已清除 TPM（即，TPM 中的种子已重置）。
- TPM 失败。

要解决其他 ESXi 安全配置问题，请参见 VMware 知识库文章，网址：<https://kb.vmware.com/kb/81446>。

手动执行恢复。请勿在安装或升级脚本中执行恢复。

### 前提条件

获取恢复密钥。您之前应已列出并存储了恢复密钥。请参见[列出 ESXi 安全配置恢复密钥的内容](#)。

### 步骤

- 1 （可选） 如果 TPM 失败，请将磁盘（具有引导槽）移至另一个具有 TPM 的主机。
- 2 启动 ESXi 主机。
- 3 出现 ESXi 安装程序窗口时，按 Shift+O 编辑引导选项。
- 4 在命令提示符下，输入引导选项以恢复配置。

```
encryptionRecoveryKey=recovery_key
```

ESXi 安全配置将恢复，并且 ESXi 主机将引导。

- 5 要保留更改，请输入以下命令：

```
/sbin/auto-backup.sh
```

### 后续步骤

输入恢复密钥时，它会暂时显示在不受信任的环境中，并且驻留在内存中。尽管并非必要，但最佳做法是通过重新引导主机从内存中去除密钥的残留痕迹。或者，您可以轮换密钥。请参见[轮换 ESXi 安全配置恢复密钥](#)。

## 激活或停用安全引导实施以获得安全的 ESXi 配置

您可以选择激活 UEFI 安全引导实施，或停用先前激活的 UEFI 安全引导实施。必须使用 ESXCLI 在 ESXi 主机上的 TPM 中更改此设置。

此任务仅适用于具有 TPM 的 ESXi 主机。UEFI 安全引导是一种固件设置，可确保由固件启动的软件是可信的。每次引导时都可以使用 TPM 强制启用 UEFI 安全引导。

### 前提条件

- 有权访问 ESXCLI 命令集。可以远程或在 ESXi Shell 中运行 ESXCLI 命令。
- 具有使用 ESXCLI 独立版本或 PowerCLI 所需的特权：**主机.配置.设置**

## 步骤

- 1 列出 ESXi 主机的当前设置。

```
esxcli system settings encryption get
Mode: TPM
Require Executables Only From Installed VIBs: false
Require Secure Boot: true
```

如果已激活安全引导实施，“需要安全引导”将显示 **true**。如果已停用安全引导实施，“需要安全引导”将显示 **false**。

如果模式显示为 **NONE**，您必须在主机的固件中激活 **TPM**，并通过运行以下命令设置模式：

```
esxcli system settings encryption set --mode=TPM
```



## 2 激活或停用安全引导实施。

选项	描述
激活	<p>a 正常关闭主机。</p> <p>例如，右键单击 vSphere Client 中的 ESXi 主机，然后选择<b>电源 &gt; 关机</b>。</p> <p>b 在主机的固件中激活安全引导。</p> <p>请参见特定供应商硬件文档。</p> <p>c 重新启动主机。</p> <p>d 运行以下 ESXCLI 命令。</p> <pre>esxcli system settings encryption set --require-secure-boot=T</pre> <p>e 验证更改。</p> <pre>esxcli system settings encryption get Mode: TPM Require Executables Only From Installed VIBs: false Require Secure Boot: true</pre> <p>确认“需要安全引导”显示 <b>true</b>。</p> <p>f 要保存设置，请运行以下命令。</p> <pre>/sbin/auto-backup.sh</pre>
取消激活	<p>a 运行以下 ESXCLI 命令。</p> <pre>esxcli system settings encryption set --require-secure-boot=F</pre> <p>b 验证更改。</p> <pre>esxcli system settings encryption get Mode: TPM Require Executables Only From Installed VIBs: false Require Secure Boot: false</pre> <p>确认“需要安全引导”显示 <b>false</b>。</p> <p>c 要保存设置，请运行以下命令。</p> <pre>/sbin/auto-backup.sh</pre> <p>您可以选择在主机固件中停用安全引导，此时不再设置固件设置和 TPM 实施之间的依赖关系。</p>

## 结果

ESXi 主机以激活还是停用安全引导实施方式运行，取决于您的选择。

**注** 如果在安装或升级到 vSphere 7.0 Update 2 或更高版本时未激活 TPM，可以稍后使用以下命令进行激活。

```
esxcli system settings encryption set --mode=TPM
```

激活 TPM 后，将无法撤消该设置。

即使为主机激活了 TPM，esxcli system settings encryption set 命令也会在某些 TPM 上失败。

- 在 vSphere 7.0 Update 2 中：NationZ (NTZ) 的 TPM、Infineon Technologies (IFX) 的 TPM 以及 Nuvoton Technologies Corporation (NTC) 的某些新型号（例如 NPCT75x）
- vSphere 7.0 Update 3 中：来自 NationZ (NTZ) 的 TPM

如果安装或升级 vSphere 7.0 Update 2 或更高版本在首次引导期间无法使用 TPM，则安装或升级将继续，并且模式默认为“无”（即，--mode=NONE）。由此引发的行为就像未激活 TPM 一样。

## 激活或停用 execInstalledOnly 实施以获得安全的 ESXi 配置

您可以选择激活 execInstalledOnly 实施，或停用先前启用的 execInstalledOnly 实施。必须使用 ESXCLI 在 ESXi 主机上的 TPM 中更改此设置。必须先激活 UEFI 安全引导实施，然后才能激活 execInstalledOnly 实施。

此任务仅适用于具有 TPM 的 ESXi 主机。execInstalledOnly 高级 ESXi 引导选项（设置为 TRUE 时）可确保 VMkernel 仅执行已作为 VIB 的一部分进行打包和签名的二进制文件。每次引导时都可以使用 TPM 强制启用此引导选项。

### 前提条件

- 要激活 execInstalledOnly 实施，必须先激活 UEFI 安全引导实施。execInstalledOnly 实施建立在 UEFI 安全引导实施的基础上。请参见[激活或停用安全引导实施以获得安全的 ESXi 配置](#)。
- 有权访问 ESXCLI 命令集。可以远程或在 ESXi Shell 中运行 ESXCLI 命令。
- 具有使用 ESXCLI 独立版本或 PowerCLI 所需的特权：**主机.配置.设置**

### 步骤

- 1 列出 ESXi 主机的当前设置。

```
esxcli system settings encryption get
Mode: TPM
Require Executables Only From Installed VIBs: false
Require Secure Boot: true
```

如果已激活 execInstalledOnly 实施，则“需要仅来自自己安装 VIB 的可执行文件”会显示 true。如果已停用 execInstalledOnly 实施，则“需要仅来自自己安装 VIB 的可执行文件”会显示 false。要激活 execInstalledOnly 实施，必须激活安全引导实施，在这种情况下，“需要安全引导”显示 true。

如果模式显示为 **NONE**，您必须在主机的固件中启用 **TPM**，并通过运行以下命令设置模式：

```
esxcli system settings encryption set --mode=TPM
```

此外，如果“需要安全引导”显示为 **False**，请参见[激活或停用安全引导实施以获得安全的 ESXi 配置以激活实施](#)。

## 2 激活或停用 execInstalledOnly 实施。

选项	描述
激活	<p>a 确认已激活安全引导选项。</p> <pre>esxcli system settings encryption get Mode: TPM Require Executables Only From Installed VIBs: false Require Secure Boot: true</pre> <p>确认“需要安全引导”显示 true。否则，请参见<a href="#">激活或停用安全引导实施以获得安全的 ESXi 配置</a>。</p>
	<p>b 要将 execInstalledOnly 引导选项的运行时值配置为 TRUE，请运行以下 ESXCLI 命令。</p> <pre>esxcli system settings kernel set -s execInstalledOnly -v TRUE</pre>
	<p>c 正常关闭主机。</p> <p>例如，右键单击 vSphere Client 中的 ESXi 主机，然后选择<b>电源 &gt; 关机</b>。</p>
	<p>d 重新启动主机。</p>
	<p>e 要设置 execInstalledOnly 防护，请运行以下 ESXCLI 命令。</p> <pre>esxcli system settings encryption set --require-exec-installed-only=T</pre>
	<p>f 验证更改。</p> <pre>esxcli system settings encryption get Mode: TPM Require Executables Only From Installed VIBs: true Require Secure Boot: true</pre> <p>确认“需要仅来自已安装 VIB 的可执行文件”显示 true。</p>
取消激活	<p>g 要保存设置，请运行以下命令。</p> <pre>/sbin/auto-backup.sh</pre>
	<p>a 运行以下 ESXCLI 命令。</p> <pre>esxcli system settings encryption set --require-exec-installed-only=F</pre>
	<p>b 验证更改。</p> <pre>esxcli system settings encryption get Mode: TPM Require Executables Only From Installed VIBs: false Require Secure Boot: true</pre> <p>确认“需要仅来自已安装 VIB 的可执行文件”显示 false。</p>
	<p>c 要保存设置，请运行以下命令。</p> <pre>/sbin/auto-backup.sh</pre> <p>TPM 不再强制执行 execInstalledOnly 引导选项。</p>

## 结果

ESXi 主机以激活还是停用 `execInstalledOnly` 实施方式运行，取决于您的选择。

## 停用 `execInstalledOnly` 高级配置运行时选项

安装或升级到 ESXi 8.0 时，默认情况下会在主机上激活 `execInstalledOnly` 高级配置运行时选项。此选项有助于保护主机免受勒索软件攻击。如果 ESXi 8.0 主机仍运行来自外部源的非 VIB 二进制文件，则可以停用 `execInstalledOnly` 高级配置运行时选项。

`execInstalledOnly` 选项可确保 VMkernel 仅执行已作为有效 VIB 一部分正确打包和签名的二进制文件，从而帮助保护主机免受勒索软件攻击。

`execInstalledOnly` 选项既是引导选项，也是运行时选项。`execInstalledOnly` 引导选项（也称为内核选项）是在 ESXi 5.5 中引入的。默认情况下，`execInstalledOnly` 引导选项处于停用状态。从 vSphere 7.0 Update 2 开始，可以在每次使用 TPM 引导时强制执行 `execInstalledOnly` 引导选项。有关详细信息，请参见[激活或停用 `execInstalledOnly` 实施以获得安全的 ESXi 配置](#)。

默认情况下，ESXi 8.0 中添加的 `execInstalledOnly` 高级配置运行时选项在主机上处于激活状态。默认情况下，`execInstalledOnly` 引导选项将继续处于停用状态，但先前启用的 `execInstalledOnly` 引导选项会在您设置了这两个选项时覆盖运行时选项。

---

**注** `execInstalledOnly` 选项不受安全引导影响。安全引导会检查所有已安装的 VIB 是否已签名。有关详细信息，请参见[ESXi 主机的 UEFI 安全引导](#)。

---

停用 `execInstalledOnly` 运行时选项时，将针对主机显示 vCenter Server 警告。

### 前提条件

要停用 `execInstalledOnly` 选项，您必须对 ESXi 主机拥有 root 访问权限。可以使用 ESXCLI、PowerCLI 或 API。接下来的任务使用 ESXCLI。

---

**小心** 停用 `execInstalledOnly` 高级配置运行时选项会让您更容易受到攻击。

---

### 步骤

- 1 使用 SSH 连接至 ESXi 主机。
- 2 要停用 `execInstalledOnly` 引导选项，请输入以下 ESXCLI 命令。

```
esxcli system settings advanced set -o /User/execInstalledOnly -i 0
```

# 确保 vCenter Server 系统安全

# 4

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 访问控制的最佳做法
- 限制 vCenter Server 网络连接
- vCenter Server 安全性最佳做法
- vCenter 密码要求和锁定行为
- 验证旧版 ESXi 主机的指纹
- vCenter Server 的所需端口

## 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。

### 使用指定帐户访问 vCenter Server

- 请仅将管理员角色授予需要该角色的管理员。您可以为具有更多有限特权的管理员创建自定义角色或使用无加密管理员角色。请勿将该角色应用于成员资格未受到严格控制的任何组。
- 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。

### 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。

## 最大程度地减少对 vCenter Server Appliance 的访问

不允许用户直接登录 vCenter Server Appliance。登录到 vCenter Server Appliance 的用户可能会更改设置以及修改进程，从而有意或无意地造成危害。这些用户还可能访问 vCenter Server 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。

## 为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。

某些特权仅在安装和升级时需要。您可以在安装或升级 vCenter Server 之后，移除数据库管理员的这些特权。

## 限制数据存储浏览器访问

仅将**数据存储.浏览**和**数据存储.浏览.写入**特权分配给真正需要这些特权的用户或组。拥有特权的用户可以通过 Web 浏览器或 vSphere Client 在 vSphere 部署关联的数据存储上查看、上载或下载文件。

## 限制用户在虚拟机中运行命令

默认情况下，具有管理员角色的用户可以与虚拟机中客户机操作系统的文件和程序进行交互。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**虚拟机.客户机操作**特权的非客户机自定义访问角色。请参见[限制用户在虚拟机中运行命令](#)。

## 考虑修改 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。确保此设置符合公司策略，或配置 vCenter Server 密码策略。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。

---

## 重新启动 vCenter Server 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。如果重新启动时无法验证在根文件夹上拥有管理员角色的用户或组，则说明此角色已从相应用户或组中移除。取而代之，vCenter Server 将管理员角色授予 vCenter Single Sign-On 管理员，默认为 administrator@vsphere.local。然后，此帐户将充当 vCenter Server 管理员。

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，从而避免使用匿名 vCenter Single Sign-On 管理员帐户（默认为 administrator@vsphere.local）。

## 对远程桌面协议使用高加密级别

在基础架构中的每台 Windows 计算机上，请务必设置远程桌面协议 (RDP) 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 Client 证书

指示 vSphere Client 或其他客户端应用程序的用户注意证书验证警告。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 Client 中更改该值。

### 步骤

- 1 使用 vSphere Client 登录到 vCenter Server 系统。
- 2 在对象层次结构中选择 vCenter Server 系统。
- 3 单击**配置**。
- 4 单击**高级设置**，然后单击**编辑设置**。
- 5 单击**筛选器**图标，然后输入 **VimPasswordExpirationInDays**。
- 6 根据您的要求设置 `VirtualCenter.VimPasswordExpirationInDays`。

## 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 Client（您在其中使用 PowerCLI 的 Windows 系统）或任何其他基于 SDK 的客户端。
- 基础架构服务，例如 DNS、Active Directory 和 PTP 或 NTP。
- 运行对 vCenter Server 系统功能至关重要的组件的其他系统。

在 vCenter Server 上使用防火墙。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。

## 评估 Linux 客户端与 CLI 和 SDK 的结合使用

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。

为了提高安全性，您可以将 vCenter Server 系统和 ESXi 主机上的 VMCA 签名证书替换为由企业或第三方 CA 签名的证书。但是，与 Linux 客户端的某些通信仍然容易受到中间机器的攻击。以下组件在 Linux 操作系统上运行时易受攻击。

- ESXCLI 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。
- 使用堡垒主机（跳转盒系统）确保 Linux 客户端受“跳转”限制。

## 检查 vSphere Client 插件

vSphere 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，例如窃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安装。

vCenter Server 安装包含 vSphere Client 的可扩展性框架。可以使用此框架通过菜单选项或工具栏图标扩展客户端。扩展可提供对 vCenter Server 加载项组件或外部基于 Web 的功能的访问。

使用可扩展性框架存在引入意外功能的危险。例如，如果管理员在 vSphere 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运行任意命令。

为了保护 vSphere Client 免受潜在的危害，请定期检查所有已安装的插件并确保每个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 Client。

- 2 在主页上，选择**系统管理**，然后在**解决方案**下，选择**客户端插件**。
- 3 检查客户端插件列表。

## vCenter Server 安全性最佳做法

遵循确保 vCenter Server 系统安全的所有最佳做法。下述额外措施将有助于提高 vCenter Server 的安全性。

### 配置精确时间协议或网络时间协议

确保所有系统使用相同的相对时间源。此时间源必须与商定的时间标准（如协调世界时，UTC）同步。系统同步对于证书验证至关重要。精确时间协议 (PTP) 和网络时间协议 (NTP) 有助于更轻松地在日志文件中跟踪入侵者。错误的时间设置难以检查和关联日志文件以检测攻击，使得审核不准确。请参见[将 vCenter Server 中的时间与 NTP 服务器同步](#)。

### 限制 vCenter Server 网络访问

限制对与 vCenter Server 通信所需的组件进行访问。阻止不必要的系统访问可降低操作系统遭受攻击的可能性。

有关 VMware 产品（包括 vSphere 和 vSAN）中所有受支持的端口和协议的列表，请参见 <https://ports.vmware.com/> 中的 VMware Ports and Protocols Tool™。您可以按 VMware 产品搜索端口，创建自定义端口列表，以及打印或保存端口列表。

### 配置 Bastion 主机

为了帮助保护资产，请配置 bastion 主机（也称为跳转盒）以执行提升的管理任务。bastion 主机是一种专用计算机，可托管最低数量的管理应用程序。将移除所有其他不必要的服务。主机通常驻留在管理网络上。bastion 主机通过将登录限制为主要用户、要求防火墙规则登录以及使用审核工具添加监控来提高资产的保护。

## vCenter 密码要求和锁定行为

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

本部分将讨论 vCenter Single Sign-On 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](#)。

### vCenter Single Sign-On 管理员密码要求

vCenter Single Sign-On 管理员（默认为 administrator@vsphere.local）的密码由 vCenter Single Sign-On 密码策略指定。默认情况下，此密码必须满足以下要求：

- 至少八个字符
- 至少一个小写字母

- 至少一个数字字符
- 至少一个特殊字符

此用户的密码长度不得超过 20 个字符。允许使用非 ASCII 字符。管理员可以更改默认密码策略。请参见《vSphere 身份验证》文档。

## vCenter Server 密码要求

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 或 OpenLDAP。

## vCenter Single Sign-On 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。可以使用 vCenter Single Sign-On 锁定策略更改这些默认值。请参见《vSphere 身份验证》文档。

vCenter Single Sign-On 域管理员（默认为 administrator@vsphere.local）不受锁定策略影响。用户受密码策略影响。

## vCenter Server 密码更改

如果您知道密码，可以通过使用 `dir-cli password change` 命令更改密码。如果忘记了密码，vCenter Single Sign-On 管理员可以使用 `dir-cli password reset` 命令重置密码。

有关密码过期信息和不同 vSphere 版本中的相关主题，请搜索 VMware 知识库。

## 验证旧版 ESXi 主机的指纹

在 vSphere 6.0 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 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 Client 清单中，浏览到 vCenter Server。
- 2 单击**配置**。
- 3 在**设置**下，单击**常规**。
- 4 单击**编辑**。
- 5 单击 **SSL 设置**。

- 6 如果任何 ESXi 5.5 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。

- 7 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。

- 8 单击**保存**。

## vCenter Server 的所需端口

vCenter Server 系统必须能将数据发送到每个受管主机，并且能够从每个 vSphere Client 接收数据。要在受管主机间启用迁移和置备活动，源主机和目标主机必须能够通过预确定的 TCP 和 UDP 端口彼此接收数据。

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。有关 vSphere 中所有受支持端口和协议的列表，请参阅 <https://ports.vmware.com> 中的 VMware Ports and Protocols Tool™。

在安装过程中，如果端口正在使用中或被拒绝列表阻止，vCenter Server 安装程序将显示错误消息。您必须使用另一个端口号才能继续安装。存在一些仅用于进程间通信的内部端口。

VMware 使用指定的端口进行通信。此外，受管主机将在指定的端口上监控来自于 vCenter Server 的数据。如果这些元素中的任意两个之间存在内置防火墙，安装程序将在安装或升级过程中打开这些端口。对于自定义防火墙，必须手动打开所需端口。如果在两台受管主机之间有防火墙，并且您要在源主机或目标主机上执行活动，例如迁移或克隆，则必须配置一种方式，以便受管主机接收数据。

要将 vCenter Server 系统配置为使用不同的端口接收 vSphere Client 数据，请参见《vCenter Server 和主机管理》文档。

# 确保虚拟机安全

# 5

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。与物理机一样，需要确保虚拟机的安全，请按照本文档和安全性配置指南（以前称为强化指南）中所述的最佳做法确保安全。

可从以下网址获取《安全配置指南》：<https://core.vmware.com/security>。

本章讨论了以下主题：

- 为虚拟机激活或停用 UEFI 安全引导
- 限制信息性消息从虚拟机流向 VMX 文件
- 虚拟机安全性最佳做法
- 使用 Intel Software Guard Extensions 确保虚拟机安全
- 使用 AMD Secure Encrypted Virtualization-Encrypted State 保护虚拟机

## 为虚拟机激活或停用 UEFI 安全引导

UEFI 安全引导是一种安全标准，有助于确保您的 PC 仅使用该 PC 制造商信任的软件进行引导。对于某些虚拟机硬件版本和操作系统，您可以完全按照对物理计算机激活安全引导的方式来激活安全引导。

在支持 UEFI 安全引导的操作系统中，引导软件的每个部分都会进行签名，包括引导加载程序、操作系统内核以及操作系统驱动程序。虚拟机的默认配置包括多个代码签名证书。

- 一个仅用于引导 Windows 的 Microsoft 证书。
- 一个用于 Microsoft 签名的第三方代码（例如 Linux 引导加载程序）的 Microsoft 证书。
- 一个仅用于在虚拟机内部引导 ESXi 的 VMware 证书。

虚拟机的默认配置包括一个用于在虚拟机内部对修改安全引导配置（包括安全引导撤消列表）的请求进行身份验证的证书，该证书是一个 Microsoft KEK（密钥交换密钥）证书。

几乎在所有情况下，均不需要替换现有证书。如果要替换证书，请参见 VMware 知识库系统。

对于使用 UEFI 安全引导的虚拟机，需要 VMware Tools 10.1 或更高版本。在 VMware Tools 的更高版本推出后，可以将这些虚拟机升级到该版本。

对于 Linux 虚拟机，安全引导模式不支持 VMware 主机客户机文件系统。先将 VMware 主机客户机文件系统从 VMware Tools 中移除，然后再激活安全引导。

---

**注** 如果为某个虚拟机启用了安全引导，则只能在该虚拟机中加载经过签名的驱动程序。

---

此任务介绍了如何使用 vSphere Client 为虚拟机激活和停用安全引导。此外，还可以编写脚本来管理虚拟机设置。例如，可以使用以下 PowerCLI 代码自动将虚拟机固件由 BIOS 更改为 EFI：

```
$vm = Get-VM TestVM

$spec = New-Object VMware.Vim.VirtualMachineConfigSpec
$spec.Firmware = [VMware.Vim.GuestOsDescriptorFirmwareType]::efi
$vm.ExtensionData.ReconfigVM($spec)
```

有关详细信息，请参见《VMware PowerCLI 用户指南》。

### 前提条件

只有在满足所有必备条件的情况下，才能激活安全引导。如果不满足必备条件，则 vSphere Client 中将不显示该复选框。

- 验证虚拟机操作系统和固件是否支持 UEFI 引导。
  - EFI 固件
  - 虚拟硬件版本 13 或更高版本。
  - 支持 UEFI 安全引导的操作系统。

---

**注** 某些客户机操作系统不支持在不进行客户机操作系统修改的情况下从 BIOS 引导更改为 UEFI 引导。更改为 UEFI 引导之前，请查看客户机操作系统文档。如果将已使用 UEFI 引导的虚拟机升级到支持 UEFI 安全引导的操作系统，则可以对该虚拟机激活安全引导。

---

- 关闭虚拟机。如果虚拟机正在运行，则该复选框将灰显。

### 步骤

- 1 在 vSphere Client 清单中，浏览到虚拟机。
- 2 右键单击虚拟机，然后选择**编辑设置**。
- 3 单击**虚拟机选项**选项卡，然后展开**引导选项**。
- 4 在**引导选项**下，确保固件设置为 **EFI**。
- 5 选择任务。
  - 选中**安全引导**复选框以激活安全引导，
  - 取消选中**安全引导**复选框以停用安全引导。
- 6 单击**确定**。

### 结果

当虚拟机引导时，仅支持具有有效签名的组件。如果某个组件缺少签名或签名无效，则引导过程将停止。

## 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 VMX 文件的大小，当信息量超过数据存储容量时，会造成 DoS 问题。

虚拟机配置文件（VMX 文件）的限制默认为 1 MB。通常情况下，此容量足够使用，但如有必要，可以更改此值。例如，如果在该文件中存储大量自定义信息，则可以提高限制值。

---

**注** 请仔细考量所需要的信息量。如果信息量超过数据存储容量，则会发生 DoS 问题。

---

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 Client 清单中，浏览到虚拟机。
- 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。

## 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移除的设备连接控制。因此，控制台访问权限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）。

### ■ 停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。通过停用支持系统上运行的应用程序或服务非必需的系统组件，可以降低攻击风险。



## 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。有关其他信息，请参见 vSphere 安全配置指南，网址为 <https://core.vmware.com/security-configuration-guide>。

### 修补虚拟机

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，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。此外，还应确保您拥有足够的空间来存储虚拟机日志。

### 扫描虚拟机中的病毒

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均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。

### 停用虚拟机上的串行端口

串行端口是用于将外围设备连接到虚拟机的接口。管理员通常使用串行端口提供到服务器控制台的直接低级别连接。虚拟串行端口允许对虚拟机进行相同的访问。因为串行端口允许低级别访问，并且没有强大的控制功能（如日志记录或特权），所以请在虚拟机上将其停用。

## 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

有关模板的更多信息，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移除的设备连接控制。因此，控制台访问权限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 限制虚拟机控制台连接数。

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。

- a 在 vSphere Client 中，关闭虚拟机的电源。
- b 右键单击虚拟机，然后选择**编辑设置**。
- c 单击**虚拟机选项**选项卡，然后展开 **VMware 远程控制台选项**。
- d 输入会话数上限，例如，**2**。
- e 单击**确定**。

## 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。

在完全了解影响之前，请不要设置限制或使用资源池。

### 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

有关份额和限制的信息，请参见《vSphere 资源管理》文档。

## 停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。通过停用支持系统上运行的应用程序或服务非必需的系统组件，可以降低攻击风险。

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。

---

**注** 如果可能，请使用“最小”或“核心”安装模式安装客户机操作系统，以减少客户机操作系统的大小、复杂性和攻击面。

---

### 步骤

- ◆ 停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。
- ◆ 停用未使用的功能，例如未使用的显示功能或 VMware 共享文件夹，该功能允许与虚拟机（主机客户机文件系统）共享主机文件。
- ◆ 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。

## 从虚拟机中移除不必要的硬件设备

虚拟机中的任何激活或连接的设备都表示潜在的攻击渠道。虚拟机上具有特权的用户和进程可以连接硬件设备（如网络适配器和 CD-ROM 驱动器）或断开设备连接。攻击者可利用该能力破坏虚拟机安全性。移除不必要的硬件设备可帮助防止攻击。

具有虚拟机访问权限的攻击者可以连接已断开连接的硬件设备，并访问硬件设备中遗留的介质上的敏感信息。攻击者还可以断开网络适配器连接，将虚拟机与其网络隔离，这样将导致拒绝服务。

- 切勿将未授权设备连接到虚拟机。
- 移除不需要或不使用的硬件设备。
- 从虚拟机中停用不必要的虚拟设备。
- 确保只将需要的设备连接到虚拟机。虚拟机极少使用串行或并行端口。通常，只在软件安装期间暂时连接到 CD/DVD 驱动器。

### 步骤

- 1 在 vSphere Client 清单中，浏览到虚拟机。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 停用不需要的硬件设备。

包括检查以下设备：

- 串行端口

- 并行端口
- USB 控制器
- CD-ROM 驱动器

**注** 您必须使用 PowerCLI 命令管理 vSphere 7.0 及更高版本中的软盘驱动器设备。

## 停用虚拟机上未使用的显示功能

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。停用环境中未使用的功能。

### 前提条件

关闭虚拟机电源。

### 步骤

- 1 在 vSphere Client 清单中，浏览到虚拟机。
- 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 如果适用，请添加或编辑以下参数。

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。对于现代客户机操作系统，不要将此参数设置为 <code>TRUE</code> ，因为它们无法正常运行。当 <code>svga.vgaonly</code> 设置为 <code>TRUE</code> 时，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。  <b>注</b> 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> 。

## 停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停用状态。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 Client 将其激活。

将这些选项设置为默认值以保证安全环境。但是，如果要使审核工具能够检查设置是否正确，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 在 vSphere Client 清单中，浏览到虚拟机。
- 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 确保“名称”和“值”列中存在以下值，否则添加这些值。

名称	值
<code>isolation.tools.copy.disable</code>	<code>true</code>
<code>isolation.tools.paste.disable</code>	<code>true</code>
<code>isolation.tools.setGUIOptions.enable</code>	<code>false</code>

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**。
- 7 （可选）如果更改了配置参数，则要重新启动虚拟机。

## 限制公开复制到虚拟机控制台剪贴板中的敏感数据

默认情况下，已停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。

在运行 VMware Tools 的虚拟机上激活复制和粘贴时，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。当控制台窗口获得焦点时，虚拟机中运行的进程和非特权用户可以访问虚拟机控制台剪贴板。如果用户在使用控制台前将敏感信息复制到剪贴板中，则该使用可能会向虚拟机暴露敏感数据。为防止此问题，默认情况下已停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激活复制和粘贴操作。

## 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以与虚拟机客户机操作系统中的文件和应用程序交互。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**虚拟机.客户机操作**特权的非客户机访问角色。将该角色分配给不需要虚拟机文件访问权限的管理员。

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。将不包括**虚拟机.客户机操作**特权的自定义角色应用于需要管理员特权但无权与客户机操作系统文件和应用程序交互的用户。

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。

如果通过 vMotion 迁移等任务要求数据中心管理员访问虚拟机，请停用某些远程客户机操作系统操作，确保这些管理员无法访问敏感信息。

### 前提条件

验证您对其上创建该角色的 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 Client。
- 2 选择**系统管理**，然后单击**角色**。

- 3 单击管理员角色，然后单击**克隆**。
- 4 输入角色名称和描述，然后单击**确定**。  
例如，输入**无客户机访问权限的管理员**。
- 5 选择克隆的角色，然后单击**编辑**图标。
- 6 在**虚拟机**特权下，取消选择客户机操作。
- 7 单击**保存**。

#### 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

虚拟机中不具有 root 或管理员特权的用户和进程可以连接设备（如网络适配器和 CD-ROM 驱动器）或断开设备的连接，还可以修改设备设置。若要提高虚拟机安全性，请移除这些设备。

可以通过更改虚拟机高级设置，阻止客户机操作系统中的虚拟机用户以及在客户机操作系统中运行的进程对设备进行任何更改。

#### 前提条件

关闭虚拟机。

#### 步骤

- 1 在 vSphere Client 清单中，浏览到虚拟机。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 单击**高级参数**选项卡。
- 4 确认“名称”和“值”列中存在以下值，否则添加该值。

名称	值
<code>isolation.device.connectable.disable</code>	<code>true</code>

此设置不会影响 vSphere 管理员连接或断开连接到虚拟机的设备的能力。

- 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

为确保客户机操作系统不会修改配置设置，可以阻止这些进程将任何名称-值对写入配置文件。

#### 前提条件

关闭虚拟机。

**步骤**

- 1 在 vSphere Client 清单中，浏览到虚拟机。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 单击**高级参数**选项卡。
- 4 确认“名称”和“值”列中存在以下值，否则添加该值。

列	值
名称	<code>isolation.tools.setinfo.disable</code>
值	<code>true</code>

- 5 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。

**使用 Intel Software Guard Extensions 确保虚拟机安全**

vSphere 支持为虚拟机配置虚拟 Intel® Software Guard Extensions (vSGX)。通过使用 vSGX，可以为工作负载提供额外的安全保护。

一些现代 Intel CPU 实施了名为 Intel® Software Guard Extensions (Intel® SGX) 的安全扩展。Intel SGX 是一种特定于处理器的技术，适用于力图保护选择代码和数据免遭泄露或修改的应用程序开发人员。Intel SGX 允许用户级代码定义内存的专用区域，称为安全区。安全区内容受到保护，因此在安全区外部运行的代码无法访问安全区内容。

vSGX 使虚拟机能够使用 Intel SGX 技术（如果在硬件上可用）。要使用 vSGX，ESXi 主机必须安装在支持 SGX 的 CPU 上，并且必须在 ESXi 主机的 BIOS 中启用 SGX。可以使用 vSphere Client 为虚拟机启用 SGX。

从 vSphere 8.0 开始，可以对启用了 vSGX 的虚拟机使用远程证明。Intel SGX 远程证明是一种安全机制，允许您与受信任的远程实体建立经过身份验证的安全通信通道。要对使用 SGX 安全区的虚拟机使用远程证明，具有单个 CPU 插槽的主机不需要 Intel 注册。要在具有多个 CPU 插槽的主机中运行的虚拟机上启用远程证明，必须先向 Intel 注册服务器注册该主机。如果具有多个 CPU 插槽且支持 SGX 的主机未向 Intel 注册服务器注册，则只能打开不需要远程证明且已启用 vSGX 的虚拟机的电源。

有关向 Intel 注册服务器注册多插槽《vCenter Server 和主机管理》主机的详细信息，请参见《ESXi》文档。

## vSGX 入门

虚拟机可以使用 Intel SGX 技术（如果在硬件上可用）。

### vSGX 对 vSphere 的要求

要使用 vSGX，您的 vSphere 环境必须满足以下要求：

- 虚拟机要求：
  - EFI 固件
  - 硬件版本 17 或更高版本
  - 要启用远程证明，请使用硬件版本 20 或更高版本
- 组件要求：
  - vCenter Server 7.0 及更高版本
  - ESXi 7.0 及更高版本
  - ESXi 主机必须安装在支持 SGX 的 CPU 上，并且必须在 ESXi 主机的 BIOS 中启用 SGX。
  - 要为主机启用远程证明，请向 Intel 注册服务器注册主机。这样，在主机上运行的虚拟机就可以使用远程证明。有关如何注册多插槽 ESXi 的详细信息，请参见《vCenter Server 和主机管理》文档。
- 客户机操作系统支持：
  - Linux
  - Windows Server 2016（64 位）及更高版本
  - Windows 10（64 位）及更高版本

### vSGX 支持的 Intel 硬件

有关适用于 vSGX 的受支持的 Intel 硬件，请参见位于 <https://www.vmware.com/resources/compatibility/search.php> 的《vSphere 兼容性指南》。

可能需要关闭某些 CPU 上的超线程，才能在 ESXi 主机上启用 SGX。有关详细信息，请参见 VMware 知识库文章，网址为 <https://kb.vmware.com/s/article/71367>。

## vSGX 上不支持的 VMware 功能

启用 vSGX 时，以下功能在虚拟机中不受支持：

- vMotion/DRS 迁移
- 虚拟机挂起和恢复
- 虚拟机快照（如果未生成虚拟机内存快照，则支持虚拟机快照。）
- Fault Tolerance
- 客户机完整性（GI，VMware AppDefense™ 1.0 的平台基础）

**注** 鉴于 Intel SGX 架构的工作方式，这些 VMware 功能不受支持，并非 VMware 缺陷所致。

## 在虚拟机上启用 vSGX

可以在创建虚拟机的同时在虚拟机上启用 vSGX。

### 前提条件

请参见 [vSGX 对 vSphere 的要求](#)。

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 在清单中选择一个对象（虚拟机的有效父对象），如 ESXi 主机或集群。
- 3 右键单击对象，选择**新建虚拟机**，并按照提示创建虚拟机。
- 4 在**自定义硬件**页面上，单击**虚拟硬件**选项卡，然后展开 **安全设备**。
- 5 要启用 SGX，请选中**启用**复选框。
- 6 在**安全区页面缓存大小 (MB)** 文本框中，输入缓存大小（以 MB 为单位）。

**注** 安全区页面缓存大小必须为 2 MB 的倍数。

- 7 要防止虚拟机打开不支持 SGX 远程证明的主机（如未注册的多插槽 SGX 主机）的电源，请选中**远程证明**复选框。
- 8 从**启动控制配置**下拉菜单中，选择相应的模式。

选项	操作
已解锁	此选项可启用客户机操作系统的启动安全区配置。
已锁定	<p>此选项可用于配置启动安全区。</p> <ol style="list-style-type: none"> <li>a 选择<b>启动安全区公钥哈希</b>选项。</li> <li>b 要使用主机上配置的一个公钥，请选择<b>使用主机端</b>，然后从下拉菜单中选择一个公钥哈希。</li> <li>c 要手动输入公钥，请选择<b>手动输入</b>，然后输入有效的 SHA256 哈希 (64) 字符密钥。</li> </ol>

- 9 单击**确定**。



## 在现有虚拟机上启用 vSGX

可以在现有虚拟机上启用 vSGX。

### 前提条件

请参见 [vSGX 对 vSphere 的要求](#)。

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 在清单中右键单击您要修改的虚拟机，然后选择**编辑设置**。
- 3 在**虚拟硬件**选项卡中，展开**安全设备**。
- 4 要启用 SGX，请选中**启用**复选框。
- 5 在**安全区**页面**缓存大小 (MB)** 文本框中，输入缓存大小（以 MB 为单位）。

**注** 安全区页面缓存大小必须为 2 MB 的倍数。

- 6 要防止虚拟机打开不支持 SGX 远程证明的主机（如未注册的多插槽 SGX 主机）的电源，请选中**远程证明**复选框。
- 7 从**启动控制配置**下拉菜单中，选择相应的模式。

选项	操作
已解锁	此选项可启用客户机操作系统的启动安全区配置。
已锁定	<p>此选项可用于配置启动安全区。</p> <ol style="list-style-type: none"> <li>a 选择<b>启动安全区公钥哈希</b>选项。</li> <li>b 要使用主机上配置的一个公钥，请选择<b>使用主机端</b>，然后从下拉菜单中选择一个公钥哈希。</li> <li>c 要手动输入公钥，请选择<b>手动输入</b>，然后输入有效的 SHA256 哈希 (64) 字符密钥。</li> </ol>

- 8 单击**确定**。

## 从虚拟机中移除 vSGX

可以从虚拟机中移除 vSGX。

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 在清单中右键单击您要修改的虚拟机，然后选择**编辑设置**。
- 3 在**编辑设置**对话框中的**安全设备**下，取消选中 SGX 对应的**启用**复选框。
- 4 单击**确定**。

验证 vSGX 条目是否不再显示在**虚拟机硬件**窗格的虚拟机**摘要**选项卡中。

## 使用 AMD Secure Encrypted Virtualization-Encrypted State 保护虚拟机

Secure Encrypted Virtualization-Encrypted State (SEV-ES) 是在最新 AMD CPU 中启用的一项硬件功能，可确保客户机操作系统的内存和寄存器状态处于加密状态，从而防止从 Hypervisor 对其进行访问。

可以将 SEV-ES 添加到虚拟机，以进一步增强安全性。SEV-ES 可防止 CPU 寄存器将寄存器中的信息泄漏给 Hypervisor 等组件。SEV-ES 还可以检测对 CPU 寄存器状态的恶意修改。

### vSphere 和 AMD Secure Encrypted Virtualization-Encrypted State

在 vSphere 7.0 Update 1 及更高版本中，您可以在受支持的 AMD CPU 和客户机操作系统上激活 Secure Encrypted Virtualization-Encrypted State (SEV-ES)。

目前，SEV-ES 仅支持 AMD EPYC 7xx2 CPU（代码为“Rome”）和更高版本的 CPU，同时仅支持对 SEV-ES 提供特定支持的 Linux 内核版本。

#### SEV-ES 组件和架构

SEV-ES 架构中包含以下组件。

- AMD CPU，具体来说，是管理加密密钥和处理加密的平台安全处理器 (PSP)。
- 开明的操作系统，也就是对 Hypervisor 使用客户机启动的调用的操作系统。
- 虚拟机监控 (VMM) 和虚拟机可执行 (VMX)，用于在虚拟机打开电源时初始化加密的虚拟机状态，还可以处理来自客户机操作系统的调用。
- VMkernel 驱动程序，用于在 Hypervisor 和客户机操作系统之间传递未加密的数据。

#### 在 ESXi 上实施和管理 SEV-ES

您必须先要在系统的 BIOS 配置中激活 SEV-ES。有关访问 BIOS 配置的详细信息，请参见系统的文档。在系统的 BIOS 中激活 SEV-ES 后，可以将 SEV-ES 添加到虚拟机。

可以使用 vSphere Client（从 vSphere 7.0 Update 2 开始）或 PowerCLI 命令在虚拟机上激活和停用 SEV-ES。您可以使用 SEV-ES 创建新的虚拟机，也可以在现有虚拟机上激活 SEV-ES。管理已激活 SEV-ES 的虚拟机的特权与管理常规虚拟机的特权相同。

#### SEV-ES 上不支持的 VMware 功能

激活 SEV-ES 后，不支持以下功能。

- 系统管理模式
- vMotion
- 已打开电源的快照（但是支持无内存快照）
- 热添加或移除 CPU 或内存
- 挂起/恢复
- VMware Fault Tolerance

- 克隆和即时克隆
- 客户机完整性
- UEFI 安全引导

## 使用 vSphere Client 向虚拟机添加 AMD Secure Encrypted Virtualization-Encrypted State

在 vSphere 7.0 Update 2 及更高版本中，可以使用 vSphere Client 将 SEV-ES 添加到虚拟机，以便为客户机操作系统提供增强的安全性。

您可以将 SEV-ES 添加到在 ESXi 7.0 Update 1 或更高版本上运行的虚拟机。

### 前提条件

- 系统必须安装有 AMD EPYC 7xx2（代码为“Rome”）或更高版本的 CPU 以及支持的 BIOS。
- 必须在 BIOS 中启用 SEV-ES。
- 每个 ESXi 主机的 SEV-ES 虚拟机数量由 BIOS 控制。在 BIOS 中启用 SEV-ES 时，请为**最小 SEV 非 ES ASID** 设置输入一个等于 SEV-ES 虚拟机数加 1 的值。例如，如果您有 12 个要并发运行的虚拟机，请输入 13。

**注** vSphere 7.0 Update 1 支持每个 ESXi 主机拥有 16 个启用了 SEV-ES 的虚拟机。在 BIOS 中使用较高的设置不会阻止 SEV-ES 正常运行，但是，限制值 16 仍适用。vSphere 7.0 Update 2 支持每个 ESXi 主机拥有 480 个启用了 SEV-ES 的虚拟机。

- 在您的环境中运行的 ESXi 主机必须为 ESXi 7.0 Update 1 或更高版本。
- vCenter Server 必须为 vSphere 7.0 Update 2 或更高版本。
- 客户机操作系统必须支持 SEV-ES。

目前，仅支持为 SEV-ES 提供特定支持的 Linux 内核。

- 虚拟机必须使用硬件版本 18 或更高版本。
- 虚拟机必须启用**预留所有客户机内存**选项，否则打开电源将失败。

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 在清单中选择一个对象（虚拟机的有效父对象），如 ESXi 主机或集群。
- 3 右键单击对象，选择**新建虚拟机**，并按照提示创建虚拟机。

选项	操作
选择创建类型	创建虚拟机。
选择名称和文件夹	指定名称和目标位置。
选择计算资源	指定您有权为其创建虚拟机的对象。
选择存储	在虚拟机存储策略中，选择存储策略。选择兼容的数据存储。

选项	操作
选择兼容性	确保选择 <b>ESXi 7.0 及更高版本</b> 。
选择客户机操作系统	选择“Linux”，然后选择对 SEV-ES 具有特定支持的 Linux 版本。
自定义硬件	在 <b>虚拟机选项 &gt; 引导选项 &gt; 固件</b> 下，确保已选择 EFI。在 <b>虚拟机选项 &gt; 加密</b> 下，选中 AMD SEV-ES 对应的 <b>启用</b> 复选框。
即将完成	检查信息，然后单击 <b>完成</b> 。

## 结果

将创建具有 SEV-ES 的虚拟机。

## 向虚拟机添加 AMD Secure Encrypted Virtualization-Encrypted State

可以将 SEV-ES 添加到虚拟机，以便为客户机操作系统提供增强的安全性。

您可以将 SEV-ES 添加到在 ESXi 7.0 Update 1 或更高版本上运行的虚拟机。

### 前提条件

- 系统必须安装有 AMD EPYC 7xx2（代码为“Rome”）或更高版本的 CPU 以及支持的 BIOS。
- 必须在 BIOS 中启用 SEV-ES。
- 每个 ESXi 主机的 SEV-ES 虚拟机数量由 BIOS 控制。在 BIOS 中启用 SEV-ES 时，请为**最小 SEV 非 ES ASID** 设置输入一个等于 SEV-ES 虚拟机数加 1 的值。例如，如果您有 12 个要并发运行的虚拟机，请输入 **13**。

**注** vSphere 7.0 Update 1 支持每个 ESXi 主机拥有 16 个启用了 SEV-ES 的虚拟机。在 BIOS 中使用较高的设置不会阻止 SEV-ES 正常运行，但是，限制值 16 仍适用。vSphere 7.0 Update 2 支持每个 ESXi 主机拥有 480 个启用了 SEV-ES 的虚拟机。

- 在您的环境中运行的 ESXi 主机必须为 ESXi 7.0 Update 1 或更高版本。
- 客户机操作系统必须支持 SEV-ES。

目前，仅支持为 SEV-ES 提供特定支持的 Linux 内核。

- 虚拟机必须使用硬件版本 18 或更高版本。
- 虚拟机必须启用**预留所有客户机内存**选项，否则打开电源将失败。
- 必须在能够访问您环境的系统上安装 PowerCLI 12.1.0 或更高版本。

### 步骤

- 1 在 PowerCLI 会话中，运行 `Connect-VIServer cmdlet`，以管理员身份连接到管理（要在其中添加具有 SEV-ES 的虚拟机的）ESXi 主机的 vCenter Server。

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

## 2 使用 New-VM cmdlet 创建虚拟机，并指定 -SEVEnabled \$true。

例如，先将主机信息分配给变量，然后再创建虚拟机。

```
$vmhost = Get-VMHost -Name 10.193.25.83
New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
```

如果必须指定虚拟硬件版本，请使用 -HardwareVersion vmx-18 参数运行 New-VM cmdlet。例如：

```
New-VM -Name MyVM1 $vmhost -NumCPU 2 -MemoryMB 4 -DiskMB 4 -SEVEnabled $true
-HardwareVersion vmx-18
```

### 结果

将创建具有 SEV-ES 的虚拟机。

## 使用 vSphere Client 在现有虚拟机上激活 AMD Secure Encrypted Virtualization-Encrypted State

在 vSphere 7.0 Update 2 及更高版本中，可以使用 vSphere Client 将 SEV-ES 添加到现有虚拟机，以便为客户机操作系统提供增强的安全性。

您可以将 SEV-ES 添加到在 ESXi 7.0 Update 1 或更高版本上运行的虚拟机。

### 前提条件

- 系统必须安装有 AMD EPYC 7xx2（代码为“Rome”）或更高版本的 CPU 以及支持的 BIOS。
- 必须在 BIOS 中激活 SEV-ES。
- 每个 ESXi 主机的 SEV-ES 虚拟机数量由 BIOS 控制。在 BIOS 中激活 SEV-ES 时，请为 **Minimum SEV non-ES ASID** 设置输入一个等于 SEV-ES 虚拟机数加 1 的值。例如，如果您有 12 个要并发运行的虚拟机，请输入 **13**。

---

**注** vSphere 7.0 Update 1 支持每个 ESXi 主机拥有 16 个激活 SEV-ES 的虚拟机。在 BIOS 中使用较高的设置不会阻止 SEV-ES 正常运行，但是，限制值 16 仍适用。vSphere 7.0 Update 2 支持每个 ESXi 主机拥有 480 个激活 SEV-ES 的虚拟机。

---

- 在您的环境中运行的 ESXi 主机必须为 ESXi 7.0 Update 1 或更高版本。
- vCenter Server 必须为 vSphere 7.0 Update 2 或更高版本。
- 客户机操作系统必须支持 SEV-ES。  
目前，仅支持为 SEV-ES 提供特定支持的 Linux 内核。
- 虚拟机必须使用硬件版本 18 或更高版本。
- 虚拟机必须选中**预留所有客户机内存**选项，否则打开电源将失败。
- 确保已关闭虚拟机电源。

## 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 在清单中右键单击您要修改的虚拟机，然后选择**编辑设置**。
- 3 在**虚拟机选项** > **引导选项** > **固件**下，确保已选择 EFI。
- 4 在**编辑设置**对话框中的**虚拟机选项** > **加密**下，选中 AMD SEV-ES 对应的**启用**复选框。
- 5 单击**确定**。

## 结果

SEV-ES 添加到了虚拟机。

## 在现有虚拟机上激活 AMD Secure Encrypted Virtualization-Encrypted State

可以将 SEV-ES 添加到现有虚拟机，以增强客户机操作系统的安全性。

您可以将 SEV-ES 添加到在 ESXi 7.0 Update 1 或更高版本上运行的虚拟机。

### 前提条件

- 系统必须安装有 AMD EPYC 7xx2（代码为“Rome”）或更高版本的 CPU 以及支持的 BIOS。
- 必须在 BIOS 中激活 SEV-ES。
- 每个 ESXi 主机的 SEV-ES 虚拟机数量由 BIOS 控制。在 BIOS 中激活 SEV-ES 时，请为 **Minimum SEV non-ES ASID** 设置输入一个等于 SEV-ES 虚拟机数加 1 的值。例如，如果您有 12 个要并发运行的虚拟机，请输入 **13**。

---

**注** vSphere 7.0 Update 1 支持每个 ESXi 主机拥有 16 个激活 SEV-ES 的虚拟机。在 BIOS 中使用较高的设置不会阻止 SEV-ES 正常运行，但是，限制值 16 仍适用。vSphere 7.0 Update 2 支持每个 ESXi 主机拥有 480 个激活 SEV-ES 的虚拟机。

---

- 您环境中运行的 ESXi 主机必须为 ESXi 7.0 Update 1 或更高版本。
- 客户机操作系统必须支持 SEV-ES。  
目前，仅支持为 SEV-ES 提供特定支持的 Linux 内核。
- 虚拟机必须使用硬件版本 18 或更高版本。
- 虚拟机必须选中**预留所有客户机内存**选项，否则打开电源将失败。
- 必须在能够访问您环境的系统上安装 PowerCLI 12.1.0 或更高版本。
- 确保已关闭虚拟机电源。

## 步骤

- 1 在 PowerCLI 会话中，运行 `Connect-VIServer cmdlet`，以管理员身份连接到 vCenter Server，该服务器负责管理要在其中添加 SEV-ES 的虚拟机所在的 ESXi 主机。

例如：

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

- 2 使用 `Set-VM cmdlet`，指定 `-SEVEnabled $true` 以在虚拟机中添加 SEV-ES。

例如：

```
$vmhost = Get-VMHost -Name 10.193.25.83
Set-VM -Name MyVM2 $vmhost -SEVEnabled $true
```

如果必须指定虚拟硬件版本，请使用 `-HardwareVersion vmx-18` 参数运行 `Set-VM cmdlet`。例如：

```
Set-VM -Name MyVM2 $vmhost -SEVEnabled $true -HardwareVersion vmx-18
```

## 结果

SEV-ES 添加到了虚拟机。

## 使用 vSphere Client 在虚拟机上停用 AMD Secure Encrypted Virtualization-Encrypted State

在 vSphere 7.0 Update 2 及更高版本中，可以使用 vSphere Client 在虚拟机上停用 SEV-ES。

### 前提条件

- 确保已关闭虚拟机电源。

## 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 在清单中右键单击您要修改的虚拟机，然后选择**编辑设置**。
- 3 在**编辑设置**对话框中的**虚拟机选项 > 加密**下，取消选中 AMD SEV-ES 对应的**启用**复选框。
- 4 单击**确定**。

## 结果

在虚拟机上停用了 SEV-ES。

## 在虚拟机上停用 AMD Secure Encrypted Virtualization-Encrypted State

您可以在虚拟机上停用 SEV-ES。

### 前提条件

- 确保已关闭虚拟机电源。
- 必须在有权访问您环境的系统上安装 PowerCLI 12.1.0 或更高版本。

### 步骤

- 1 在 PowerCLI 会话中，运行 `Connect-VIServer cmdlet`，以管理员身份连接到 vCenter Server，该服务器负责管理要从中移除 SEV-ES 的虚拟机所在的 ESXi 主机。

例如：

```
Connect-VIServer -server vCenter_Server_ip_address -User admin_user -Password 'password'
```

- 2 使用 `Set-VM cmdlet`，指定 `-SEVEnabled $false` 以在虚拟机上停用 SEV-ES。

例如，先将主机信息分配给变量，然后再对虚拟机停用 SEV-ES。

```
$vmhost = Get-VMHost -Name 10.193.25.83  
Set-VM -Name MyVM2 $vmhost -SEVEnabled $false
```

### 结果

在虚拟机上停用了 SEV-ES。



利用 vSphere 虚拟机加密，能够以更安全的方式对敏感工作负载进行加密。可以将对加密密钥的访问设为以 ESXi 主机处于受信任状态为条件。

必须先设置密钥提供程序，之后才能开始执行虚拟机加密任务。可以使用以下密钥提供程序类型。

表 6-1. vSphere 密钥提供程序

密钥提供程序	描述	如需详细信息
标准密钥提供程序	标准密钥提供程序在 vSphere 6.5 及更高版本中可用，它使用 vCenter Server 从外部密钥服务器请求密钥。密钥服务器将生成并存储密钥，然后将密钥传递给 vCenter Server 以进行分发。	请参见第 7 章 配置和管理标准密钥提供程序。
可信密钥提供程序	vSphere Trust Authority 可信密钥提供程序在 vSphere 7.0 及更高版本中可用，它可以工作负载集群的证明状态为条件来访问加密密钥。vSphere Trust Authority 需要外部密钥服务器。	请参见第 9 章 vSphere Trust Authority。
VMware vSphere® Native Key Provider™	在 vSphere 7.0 Update 2 及更高版本中，所有 vSphere 版本均包含 vSphere Native Key Provider，它不需要外部密钥服务器。	请参见第 8 章 配置和管理 vSphere Native Key Provider。

本章讨论了以下主题：

- [vSphere 密钥提供程序比较](#)
- [vSphere 虚拟机加密如何保护您的环境](#)
- [vSphere 虚拟机加密组件](#)
- [加密过程流](#)
- [虚拟磁盘加密](#)
- [虚拟机加密错误](#)
- [虚拟机加密任务的必备条件和必需特权](#)
- [加密 vSphere vMotion](#)
- [虚拟机加密最佳做法](#)

- [虚拟机加密限制](#)
- [虚拟机加密互操作性](#)
- [ESXi 主机上的 vSphere 密钥持久性](#)

## vSphere 密钥提供程序比较

简要地概述了能够帮助您规划加密策略，因此需要您加以关注的 vSphere 密钥提供程序。

通常，密钥提供程序日常操作之间的功能或产品支持几乎没有差异。尽管密钥提供程序的外观和行为相似，但您在选择密钥提供程序时可能要考虑一些要求和法规，如下表所示。

**表 6-2. 密钥提供程序注意事项**

密钥提供程序	需要外部密钥服务器?	快速设置?	只能与 vSphere 配合使用?
标准密钥提供程序	是	否	否
可信密钥提供程序	是	否	否
vSphere Native Key Provider	否	是	是

## 加密功能

每种密钥提供程序类型都支持以下加密功能。

- 使用同一密钥提供程序或其他密钥提供程序重新加密
- 轮换密钥
- 虚拟可信平台模块 (vTPM)
- 磁盘加密
- vSphere 虚拟机加密
- 与其他密钥提供程序共存
- 升级到其他密钥提供程序

## vSphere 功能

下面介绍了一些重要 vSphere 功能的密钥提供程序支持。

- 加密的 vSphere vMotion：受所有密钥提供程序类型的支持。同一密钥提供程序必须在目标主机上可用。请参见[加密 vSphere vMotion](#)。
- vCenter Server 基于文件的备份和还原：标准密钥提供程序和 vSphere Native Key Provider 支持 vCenter Server 基于文件的备份和还原。由于大多数 vSphere Trust Authority 配置信息存储在 ESXi 主机上，因此 vCenter Server 基于文件的备份机制不会备份此信息。要确保保存 vSphere Trust Authority 部署的配置信息，请参见[备份 vSphere Trust Authority 配置](#)。

## VMware 产品

下表对比了部分 VMware 产品的密钥提供程序支持。

表 6-3. VMware 产品支持比较

密钥提供程序	vSAN	Site Recovery Manager	vSphere Replication
标准密钥提供程序	是	是	是
可信密钥提供程序	是	是 如果相同的 vSphere Trust Authority 服务配置在恢复端上可用，则支持使用基于阵列的复制的 SRM。	否
vSphere Native Key Provider	是	是	是

## 所需的硬件

下表对比了一些密钥提供程序最低硬件要求。

表 6-4. 所需硬件比较

密钥提供程序	ESXi 主机上的 TPM
标准密钥提供程序	不需要
可信密钥提供程序	受信任主机（受信任集群中的主机）需要此密钥提供程序。  <b>注</b> 目前，Trust Authority 集群中的 ESXi 主机不需要 TPM。但是，作为最佳做法，请考虑安装配有 TPM 的新 ESXi 主机。
vSphere Native Key Provider	不需要  可以选择将 vSphere Native Key Provider 的可用性限制到具有 TPM 的主机。

## 密钥提供程序命名

vSphere 使用密钥提供程序名称查找密钥标识符。如果两个密钥提供程序具有相同的名称，vSphere 会假定它们是等效的并且有权访问相同的密钥。每个逻辑密钥提供程序（无论其类型如何：标准、可信和本机密钥提供程序），都必须在所有 vCenter Server 系统中具有唯一的名称。

在几个实例中，您可以跨多个 vCenter Server 系统配置同一个密钥提供程序，例如：

- 在 vCenter Server 系统之间迁移加密虚拟机
- 将 vCenter Server 设置为灾难恢复站点

## vSphere 虚拟机加密如何保护您的环境

无论您使用哪种密钥提供程序，通过 vSphere 虚拟机加密，都可以创建加密虚拟机并加密现有虚拟机。由于所有包含敏感信息的虚拟机文件都会加密，因此虚拟机受保护。只有具备加密特权的管理员才能执行加密和解密任务。

### vSphere 虚拟机加密支持哪些存储

vSphere 虚拟机加密适用于任何支持的存储类型（NFS、iSCSI、光纤通道、直接连接的存储等），包括 VMware vSAN。有关在 vSAN 集群上使用加密的详细信息，请参见《管理 VMware vSAN》文档。

vSphere 虚拟机加密和 vSAN 使用相同的加密库，但具有不同的配置文件。虚拟机加密是虚拟机级加密，vSAN 是数据存储级加密。

### vSphere 加密密钥和密钥提供程序

vSphere 以密钥加密密钥 (KEK) 和数据加密密钥 (DEK) 的形式使用两级加密。简单来说，ESXi 主机生成 DEK，用于加密虚拟机和磁盘。KEK 由密钥服务器提供，对 DEK 进行加密（或“封装”）。KEK 使用 AES256 算法进行加密，DEK 使用 XTS-AES-256 算法进行加密。根据密钥提供程序的类型，使用不同的方法创建和管理 DEK 和 KEK。

标准密钥提供程序的运行方式如下。

- 1 ESXi 主机会生成内部密钥并使用这些密钥加密虚拟机和磁盘。这些密钥用作 DEK。
- 2 vCenter Server 从密钥服务器 (KMS) 请求密钥。这些密钥用作 KEK。vCenter Server 仅存储每个 KEK 的 ID，但不存储密钥本身。
- 3 ESXi 使用 KEK 加密内部密钥，并将已加密的内部密钥存储在磁盘上。ESXi 不会将 KEK 存储在磁盘上。如果主机重新引导，vCenter Server 会从密钥服务器请求具有相应 ID 的 KEK，并将其提供给 ESXi。然后，ESXi 可以根据需要解密内部密钥。

vSphere Trust Authority 可信密钥提供程序的运行方式如下。

- 1 受信任集群的 vCenter Server 检查要在其中创建加密虚拟机的 ESXi 主机是否可以访问默认可信密钥提供程序。
- 2 受信任集群的 vCenter Server 将可信密钥提供程序添加到虚拟机 ConfigSpec。
- 3 虚拟机创建请求发送到 ESXi 主机。
- 4 如果 ESXi 主机尚无可用的证明令牌，则会从证明服务请求一个证明令牌。
- 5 密钥提供程序服务验证证明令牌，并创建要发送到 ESXi 主机的 KEK。使用在密钥提供程序上配置的主要密钥对 KEK 进行封装（加密）。KEK 密码文本和 KEK 纯文本都返回到受信任主机。
- 6 ESXi 主机生成 DEK，对虚拟机磁盘进行加密。
- 7 KEK 用于封装 ESXi 主机生成的 DEK，且密钥提供程序中的密码文本与加密数据一起存储。

## 8 虚拟机会进行加密并写入存储。

**注** 如果删除或取消注册已加密的虚拟机，ESXi 主机和集群将从缓存中移除 KEK。ESXi 主机将无法再使用 KEK。对于标准密钥提供程序和可信密钥提供程序，此行为是一样的。

vSphere Native Key Provider 的运行方式如下。

- 1 创建密钥提供程序时，vCenter Server 会生成主密钥，并将其推送到集群中的 ESXi 主机。（不涉及外部密钥服务器。）
- 2 ESXi 主机按需生成 DEK。
- 3 执行加密活动时，数据会通过 DEK 进行加密。  
加密的 DEK 与加密数据存储在一起。
- 4 解密数据时，主密钥用于解密 DEK，然后解密数据。

## vSphere 虚拟机加密可以对哪些组件加密

vSphere 虚拟机加密功能支持加密虚拟机文件、虚拟磁盘文件以及核心转储文件。

### 虚拟机文件

大多数虚拟机文件（特别是未存储在 VMDK 文件中的客户机数据）都会加密。这组文件包括但不限于 NVRAM、VSWP 和 VMSN 文件。密钥提供程序中的密钥会解锁 VMX 文件中包含内部密钥和其他密钥的加密包。密钥检索的工作方式如下，具体取决于密钥提供程序：

- 标准密钥提供程序：vCenter Server 管理来自密钥服务器的密钥，ESXi 主机无法直接访问密钥提供程序。主机等待 vCenter Server 推送密钥。
- 可信密钥提供程序和 vSphere Native Key Provider：ESXi 主机直接访问密钥提供程序，因此可以直接从 vSphere Trust Authority 服务或 vSphere Native Key Provider 获取请求的密钥。

使用 vSphere Client 创建加密虚拟机时，可以独立于虚拟机文件加密和解密虚拟磁盘。默认情况下，将加密所有虚拟磁盘。对于其他加密任务（例如，加密现有虚拟机），您可以独立于虚拟机文件加密和解密虚拟磁盘。

**注** 不能将已加密的虚拟磁盘与未加密的虚拟机相关联。

### 虚拟磁盘文件

加密虚拟磁盘 (VMDK) 文件中的数据不会以明文形式写入存储或物理磁盘，也不会以明文形式通过网络传输。VMDK 描述符文件主要是明文，但将 KEK 和内部密钥 (DEK) 的密钥 ID 包含在加密包中。

您可以使用 vSphere Client 或 vSphere API 通过新的 KEK 执行浅层重新加密操作，或者使用 vSphere API 通过新的内部密钥执行深层重新加密操作。

### 核心转储

启用了加密模式的 ESXi 主机上的核心转储始终都会加密。请参见 [vSphere 虚拟机加密和核心转储](#)。vCenter Server 系统上的核心转储未加密。可保护对 vCenter Server 系统的访问。

**注** 如需了解有关 vSphere 虚拟机加密可与之交互的设备和功能的限制信息，请参见[虚拟机加密互操作性](#)。

## vSphere 虚拟机加密不对哪些组件加密

与虚拟机关联的某些文件未加密或部分加密。

### 日志文件

日志文件未加密，因为它们不包含敏感数据。

### 虚拟机配置文件

存储在 VMX 和 VMDS 文件中的大多数虚拟机配置信息未加密。

### 虚拟磁盘描述符文件

为了支持在不使用密钥的情况下管理磁盘，大多数虚拟磁盘描述符文件都不会加密。

## 如何执行加密操作

只有分配了**加密操作**特权的用户可以执行加密操作。特权组非常精细。默认管理员系统角色包括**加密操作**特权。无加密管理员角色支持**加密操作**特权除外的所有管理员特权。

除了使用 **Cryptographer.\*** 权限，vSphere Native Key Provider 还可以使用特定于 vSphere Native Key Provider 的 **Cryptographer.ReadKeyServersInfo** 特权。

有关详细信息，请参见[加密操作特权](#)。

您可以创建其他自定义角色，例如，允许一组用户加密虚拟机、但是禁止其解密虚拟机。

## 如何执行加密操作

vSphere Client 支持许多加密操作。对于其他任务，您可以使用 PowerCLI 或 vSphere API。

表 6-5. 用于执行加密操作的界面

接口	操作	信息
vSphere Client	创建加密虚拟机	本书
	加密和解密虚拟机	
	执行虚拟机的浅层重新加密（使用不同的 KEK）	
PowerCLI	创建加密虚拟机	VMware PowerCLI Cmdlets 参考
	加密和解密虚拟机	
	配置 vSphere Trust Authority	

表 6-5. 用于执行加密操作的界面（续）

接口	操作	信息
vSphere Web Services SDK	创建加密虚拟机	《vSphere Web Services SDK 编程指南》
	加密和解密虚拟机	
	执行虚拟机的深层重新加密（使用不同的 DEK）	《vSphere Web Services API 参考》
	执行虚拟机的浅层重新加密（使用不同的 KEK）	
crypto-util	解密已加密的核心转储	命令行帮助
	检查文件是否已加密	vSphere 虚拟机加密和核心转储
	直接在 ESXi 主机上执行其他管理任务	

## 如何重新加密虚拟机

您可以使用新密钥重新加密虚拟机，以防密钥过期或已泄漏等情况。可用选项如下：

- 深层重新加密，将更换磁盘加密密钥 (DEK) 和密钥加密密钥 (KEK)
- 浅层重新加密，仅更换 KEK

可以使用 vSphere Client 或 API 重新加密虚拟机。请参见[使用 vSphere Client 对加密虚拟机进行重新加密](#)和《vSphere Web Services SDK 编程指南》。

深层重新加密要求虚拟机已关闭电源且不包含任何快照。虚拟机打开电源时，如果虚拟机中存在快照，可以执行浅层重新加密操作。仅允许在单个快照分支（磁盘链）上对具有快照的加密虚拟机执行浅层重新加密。不支持多个快照分支。此外，在虚拟机或磁盘的链接克隆上不支持浅层重新加密。如果浅层重新加密在使用新 KEK 更新链中的所有链接之前失败，则仍然可以访问加密虚拟机（如果具有新旧 KEK）。但是，最好在执行任何快照操作之前重新发出浅层重新加密操作。

## vSphere 虚拟机加密组件

根据您使用的密钥提供程序、外部密钥服务器、vCenter Server 系统和 ESXi 主机可能会影响加密解决方案。

以下组件包括 vSphere 虚拟机加密：

- 外部密钥服务器，也称为 KMS（vSphere Native Key Provider 不需要 KMS）
- vCenter Server
- ESXi 主机

## 密钥服务器在 vSphere 虚拟机加密中是什么角色

密钥服务器是与密钥提供程序相关联的密钥管理互操作性协议 (Key Management Interoperability) 管理服务。标准密钥提供程序和可信密钥提供程序需要密钥服务器。vSphere Native Key Provider 不需要密钥服务器。下表介绍了密钥提供程序和密钥服务器交互之间的差异。

表 6-6. 密钥提供程序和密钥服务器交互

密钥提供程序	与密钥服务器的交互
标准密钥提供程序	标准密钥提供程序使用 vCenter Server 从密钥服务器请求密钥。密钥服务器将生成并存储密钥，然后将密钥传递给 vCenter Server 以分发到 ESXi 主机。
可信密钥提供程序	可信密钥提供程序使用密钥提供程序服务，该服务允许可信 ESXi 主机直接获取密钥。请参见 <a href="#">什么是 vSphere Trust Authority 密钥提供程序服务</a> 。
vSphere Native Key Provider	vSphere Native Key Provider 不需要密钥服务器。vCenter Server 生成主密钥，并将其推送到 ESXi 主机。然后，ESXi 主机生成数据加密密钥（即使未连接到 vCenter Server）。请参见 <a href="#">vSphere Native Key Provider 概览</a> 。

可以使用 vSphere Client 或 vSphere API 将密钥提供程序实例添加到 vCenter Server 系统。如果使用多个密钥提供程序实例，所有实例必须来自同一家供应商，并且必须复制密钥。

如果您的环境在不同的环境中使用不同的密钥服务器供应商，您可以为每个密钥服务器添加密钥提供程序并指定默认密钥提供程序。所添加的第一个密钥提供程序将成为默认密钥提供程序。您可以在以后指定默认集群。

作为 KMIP 客户端，vCenter Server 利用密钥管理互操作协议 (Key Management Interoperability Protocol, KMIP)，以便轻松使用您选择的密钥服务器。

## vCenter Server 在 vSphere 虚拟机加密中是什么角色

下表介绍了 vCenter Server 在加密过程中的角色。

表 6-7. 密钥提供程序和 vCenter Server

密钥提供程序	vCenter Server 的角色	如何检查特权
标准密钥提供程序	仅 vCenter Server 拥有登录密钥服务器的凭据。ESXi 主机不具有这些凭据。 vCenter Server 将从密钥服务器获取密钥，并将其推送给 ESXi 主机。vCenter Server 不会存储密钥服务器密钥，只会保留密钥 ID 的列表。	vCenter Server 将检查执行加密操作的用户特权。
可信密钥提供程序	通过 vSphere Trust Authority，vCenter Server 不再需要从密钥服务器请求密钥，它可以工作负载集群的证明状态为条件来访问加密密钥。必须对受信任集群和 Trust Authority 集群使用单独的 vCenter Server 系统。	vCenter Server 将检查执行加密操作的用户特权。只有 TrustedAdmins SSO 组的成员用户才能执行管理操作。
vSphere Native Key Provider	vCenter Server 生成密钥。	vCenter Server 将检查执行加密操作的用户特权。

您可以使用 vSphere Client 来分配加密操作特权，也可以将[无加密管理员](#)自定义角色分配给用户组。请参见[虚拟机加密任务的必备条件和必需特权](#)。



vCenter Server 会将加密事件添加到事件列表中，您可以通过 vSphere Client 事件控制台查看和导出该列表。每个事件都包括用户、时间、密钥 ID 和加密操作。

来自密钥服务器的密钥用作密钥加密密钥 (Key Encryption Key, KEK)。

## ESXi 主机在 vSphere 虚拟机加密中是什么角色

ESXi 主机负责处理加密工作流的几个方面。

表 6-8. 密钥提供程序和 ESXi 主机

密钥提供程序	ESXi 主机方面
标准密钥提供程序	<ul style="list-style-type: none"> <li>■ vCenter Server 会在 ESXi 主机需要密钥时将密钥推送给该主机。该主机必须已启用加密模式。</li> <li>■ 确保在将已加密虚拟机的客户机数据存储在磁盘时对其进行加密。</li> <li>■ 确保已加密虚拟机的客户机数据不会在未加密的情况下通过网络发送。</li> </ul>
可信密钥提供程序	ESXi 主机运行 vSphere Trust Authority 服务，具体取决于它们是受信任主机还是 Trust Authority 主机。可信 ESXi 主机运行工作负载虚拟机，这些虚拟机可以使用 Trust Authority 主机发布的密钥提供程序进行加密。请参见 <a href="#">可信基础架构概述</a> 。
vSphere Native Key Provider	ESXi 主机直接从 vSphere Native Key Provider 获取密钥。

ESXi 主机生成的密钥在本文档中称为内部密钥。这些密钥通常用作数据加密密钥 (Data Encryption Key, DEK)。

## 加密过程流

设置密钥提供程序后，具有所需特权的用户可以创建加密虚拟机和磁盘。这些用户还可以加密现有虚拟机和解密已加密的虚拟机，以及将虚拟可信平台模块 (vTPM) 添加到虚拟机。

根据密钥提供程序类型，过程流可能涉及密钥服务器、vCenter Server 和 ESXi 主机。

### 标准密钥提供程序加密流程

在加密过程中，不同 vSphere 组件的交互方式如下所示。

- 1 用户执行加密任务（例如，创建加密虚拟机）时，vCenter Server 会从默认的密钥服务器请求一个新密钥。该密钥用作 KEK。
- 2 vCenter Server 存储该密钥 ID，并将该密钥传递给 ESXi 主机。如果 ESXi 主机是某个集群的一部分，则 vCenter Server 会将该 KEK 发送至该集群中的每一个主机。  
密钥本身不存储在 vCenter Server 系统上。只有密钥 ID 是已知的。
- 3 ESXi 主机为虚拟机及其磁盘生成内部密钥 (DEK)。它将内部密钥仅保存在内存中，并使用 KEK 加密该内部密钥。

解密的内部密钥决不会存储在磁盘上。仅将加密的数据存储在磁盘上。由于 KEK 来自密钥服务器，所以主机会继续使用相同的 KEK。

#### 4 ESXi 主机使用加密的内部密钥加密虚拟机。

任何具有 KEK 并可以访问加密密钥文件的主机可以在加密虚拟机或磁盘上执行操作。

### 可信密钥提供程序加密过程流

vSphere Trust Authority 加密过程流包括 vSphere Trust Authority 服务、可信密钥提供程序、vCenter Server 和 ESXi 主机。

使用可信密钥提供程序对虚拟机进行加密与使用标准密钥提供程序时的虚拟机加密用户体验看起来一样。vSphere Trust Authority 下的虚拟机加密继续依赖于虚拟机加密存储策略或是否存在 vTPM 设备来决定何时加密虚拟机。从 vSphere Client 加密虚拟机时，仍使用配置的默认密钥提供程序（在 vSphere 6.5 和 6.7 中称为 KMS 集群）。此外，仍然可以通过与手动指定密钥提供程序类似的方式使用 API。为 vSphere 6.5 添加的现有加密特权在 vSphere 7.0 中仍与 vSphere Trust Authority 相关。

可信密钥提供程序与标准密钥提供程序的加密过程具有重要差异：

- 在为 vCenter Server 实例设置密钥服务器时，Trust Authority 管理员不会直接指定信息，并且不会建立密钥服务器信任。而是，vSphere Trust Authority 发布受信任主机可以使用的可信密钥提供程序。
- vCenter Server 不再向 ESXi 主机推送密钥，而是将每个可信密钥提供程序视为单个顶级密钥。
- 只有受信任主机可以从 Trust Authority 主机请求加密操作。

### vSphere Native Key Provider 加密过程流

从 vSphere 7.0 Update 2 开始，vSphere 中包含了 vSphere Native Key Provider。配置 vSphere Native Key Provider 时，vCenter Server 会将主密钥推送到集群中的所有 ESXi 主机。同样，如果更新或删除 vSphere Native Key Provider，更改将推送到集群中的主机。加密过程流程类似于可信密钥提供程序的工作方式。区别在于，vSphere Native Key Provider 会生成密钥，并使用主密钥对其进行封装，然后归还密钥以执行加密。

### 密钥服务器的自定义属性

密钥管理互操作协议 (KMIP) 支持添加用于供应商特定用途的自定义属性。自定义属性使您能够更具体地识别密钥服务器中存储的密钥。vCenter Server 为虚拟机密钥和主机密钥添加以下自定义属性。

表 6-9. 虚拟机加密自定义属性

自定义属性	值
x-Vendor	VMware, Inc.
x-Product	VMware vSphere
x-Product_Version	vCenter Server 版本
x-Component	虚拟机
x-Name	虚拟机名称（从 ConfigInfo 或 ConfigSpec 收集）
x-Identifier	虚拟机的实例 UUID（从 ConfigInfo 或 ConfigSpec 收集）

表 6-10. 主机加密自定义属性

自定义属性	值
x-Vendor	VMware, Inc.
x-Product	VMware vSphere
x-Product_Version	vCenter Server 版本
x-Component	ESXi 服务器
x-Name	主机名称
x-Identifier	主机的硬件 UUID

密钥服务器创建密钥时，vCenter Server 将添加 x-Vendor、x-Product 和 x-Product\_Version 属性。使用密钥对虚拟机或主机进行加密时，vCenter Server 将设置 x-Component、x-Identifier 和 x-Name 属性。您或许能够在密钥服务器用户界面中查看这些自定义属性。请咨询密钥服务器供应商。

主机密钥和虚拟机密钥都具有六个自定义属性。这两种密钥的 x-Vendor、x-Product 和 x-Product\_Version 可能相同。这些属性在生成密钥时进行设置。根据密钥是否用于虚拟机或主机，可能会附加 x-Component、x-Identifier 和 x-Name 属性。

## 密钥错误

如果将密钥从密钥服务器发送到 ESXi 主机时出错，vCenter Server 会在事件日志中针对以下事件生成一条消息：

- 由于主机连接或主机支持问题，向 ESXi 主机添加密钥失败。
- 由于密钥服务器中缺少密钥，从密钥服务器获取密钥失败。
- 由于密钥服务器连接，从密钥服务器获取密钥失败。

## 解密加密的虚拟机

如果稍后要解密加密的虚拟机，请更改其存储策略。您可以更改虚拟机及所有磁盘的存储策略。如果要解密单独的组件，先解密选定的磁盘，然后通过更改虚拟机主页的存储策略解密虚拟机。解密每个组件都需要两种密钥。请参见[解密加密虚拟机或虚拟磁盘](#)。

## 虚拟磁盘加密

从 vSphere Client 创建加密虚拟机时，可以决定哪些磁盘不需要进行加密。您可以稍后添加磁盘并设置其加密策略。不能将加密磁盘添加到未加密的虚拟机；如果虚拟机未加密，无法加密磁盘。

可以通过存储策略控制虚拟机及其磁盘的加密。虚拟机主页的存储策略可以控制虚拟机本身，每个虚拟磁盘都具有关联的存储策略。

- 将虚拟机主页的存储策略设置为加密策略时，将仅加密虚拟机本身。
- 将虚拟机主页及所有磁盘的存储策略设置为加密策略时，将加密所有组件。

请考虑以下用例。

**表 6-11. 虚拟磁盘加密用例**

用例	详细信息
创建加密的虚拟机。	如果在创建加密的虚拟机时添加磁盘，将默认加密这些磁盘。可以将策略更改为不加密一个或多个磁盘。 创建虚拟机之后，可以明确更改每个磁盘的存储策略。请参见 <a href="#">更改虚拟磁盘的加密策略</a> 。
加密虚拟机。	要加密现有虚拟机，可以更改其存储策略。可以更改虚拟机及所有虚拟磁盘的存储策略。要仅加密虚拟机，可以为虚拟机主页指定加密策略，并为每个虚拟磁盘选择不同的存储策略（例如数据存储默认值）。请参见 <a href="#">创建加密虚拟机</a> 。
将现有未加密磁盘添加到加密虚拟机（加密存储策略）。	失败并显示错误。必须通过默认存储策略添加磁盘，但可以稍后更改存储策略。请参见 <a href="#">更改虚拟磁盘的加密策略</a> 。
通过不包括加密的存储策略（例如数据存储默认值）将现有未加密磁盘添加到加密的虚拟机。	磁盘使用默认存储策略。如果需要加密磁盘，可以在添加磁盘后明确更改存储策略。请参见 <a href="#">更改虚拟磁盘的加密策略</a> 。
将加密磁盘添加到加密虚拟机。虚拟机主页存储策略为加密策略。	添加磁盘时，其将保持加密状态。 <b>vSphere Client</b> 显示大小和其他属性，包括加密状态。
将现有加密磁盘添加到未加密的虚拟机。	不支持此用例。
注册加密虚拟机。	<p>如果从 <b>vCenter Server</b> 中移除加密虚拟机，但不将其从磁盘删除，则可以通过注册虚拟机的虚拟机配置 (.vmx) 文件将其返回到 <b>vCenter Server</b> 清单。要注册加密虚拟机，用户必须具有 <b>加密操作.注册虚拟机</b> 特权。</p> <p>如果使用标准密钥提供程序对虚拟机进行了加密，则在注册加密虚拟机时，<b>vCenter Server</b> 会将所需密钥推送到 ESXi 主机。如果注册虚拟机的用户没有 <b>加密操作.注册虚拟机</b> 特权，<b>vCenter Server</b> 会在注册时锁定虚拟机，并且在解锁之前无法使用虚拟机。</p> <p>如果使用可信密钥提供程序或 <b>vSphere Native Key Provider</b> 对虚拟机进行了加密，则在注册加密虚拟机时，<b>vCenter Server</b> 不再向 ESXi 主机推送密钥。而是在注册虚拟机时从主机中获取密钥。如果注册虚拟机的用户没有 <b>加密操作.注册虚拟机</b> 特权，则 <b>vCenter Server</b> 不允许执行该操作。</p>

## 虚拟机加密错误

如果 **vCenter Server** 检测到虚拟机加密存在严重错误，则会创建事件。可以查看这些事件，以帮助进行故障排除并解决加密错误。

**vCenter Server** 会为以下虚拟机加密严重错误创建事件。

- 无法生成 KEK。
- 数据存储上的磁盘空间不足，无法创建加密虚拟机。
- 用户特权不足，无法启动加密操作。
- 密钥提供程序上缺少指定的密钥，因此使用新密钥续订 ESXi 主机密钥。

- 具有指定密钥的密钥提供程序出现错误，因此使用新密钥续订 ESXi 主机密钥。

## 虚拟机加密任务的必备条件和必需特权

只有在包含 vCenter Server 的环境中才能执行虚拟机加密任务。此外，ESXi 主机必须为大多数加密任务激活加密模式。执行任务的用户必须拥有相应的特权。一组**加密操作**特权可实现精细控制。如果虚拟机加密任务要求更改为主机加密模式，则需要额外的特权。

**注** vSphere Trust Authority 具有其他必备条件和所需特权。请参见 [vSphere Trust Authority 的必备条件和所需特权](#)。

## 使用加密特权和角色

默认情况下，具有 vCenter Server 管理员角色的用户拥有所有特权，包括加密操作特权。**无加密管理员**角色不具有加密操作所需的以下权限。

- 添加**加密操作**特权。
- **全局.诊断**
- **主机.清单.将主机添加到集群**
- **主机.清单.添加独立主机**
- **主机.本地操作.管理用户组**

您可以为不需要**加密操作**特权的 vCenter Server 管理员分配**无加密管理员**角色。

要对用户可执行的操作施加更多的限制，可以克隆**无加密管理员**角色，然后创建仅具有部分**加密操作**特权的自定义角色。例如，您可以创建这样一个角色：它允许用户加密但不能解密虚拟机。请参见[使用 vCenter Server 角色分配特权](#)。

## 什么是主机加密模式

主机加密模式确定 ESXi 主机是否已准备好接受加密材料以加密虚拟机和虚拟磁盘。在主机上执行任何加密操作之前，必须先激活加密模式。主机加密模式通常在需要时自动设置，但可以明确设置此模式。可从 vSphere Client 或通过 vSphere API 检查和明确设置当前主机加密模式。

激活主机加密模式时，vCenter Server 会在主机上安装主机密钥，这样可确保主机通过加密保障安全。安装主机密钥后，可以继续执行其他加密操作，包括 vCenter Server 从密钥提供程序获取密钥并将其推送到 ESXi 主机。

在“安全”模式下，用户环境（即，hostd）和加密虚拟机会加密其核心转储。未加密虚拟机不会加密其核心转储。

有关加密核心转储以及 VMware 技术支持如何使用它们的详细信息，请参见位于 <http://kb.vmware.com/kb/2147388> 的 VMware 知识库文章。

有关说明，请参见 [明确激活主机加密模式](#)。

设置主机加密模式后，无法轻易停用。请参见[使用 API 停用主机加密模式](#)。

当加密操作尝试设置主机加密模式时，会自动进行更改。例如，假定您将加密虚拟机添加到独立主机。未设置主机加密模式。如果在主机上具有所需特权，则会自动设置加密模式。

假设一个集群有三个 ESXi 主机，即主机 A、B 和 C。在主机 A 上创建一个加密虚拟机。发生的具体情况取决于几个要素。

- 如果主机 A、B 和 C 已经设置主机加密模式，您只需**加密操作.加密新项**特权即可创建虚拟机。
- 如果主机 A 和 B 已设置主机加密，而主机 C 未设置主机加密，则系统按照下面所述继续运行。
  - 假定您对每台主机都拥有**加密操作.加密新项**和**加密操作.注册主机**特权。在这种情况下，加密过程会在主机 C 上设置主机加密模式，并将密钥推送到集群中的每个主机。  
对于这种情况，您还可以在主机 C 上明确设置主机加密模式。
  - 假定您对虚拟机或虚拟机文件夹仅拥有**加密操作.加密新项**特权。在这种情况下，虚拟机将成功创建，密钥在主机 A 和主机 B 上将变为可用。主机 C 仍然停用加密且没有虚拟机密钥。
- 如果所有主机均未设置主机加密模式，并且您对主机 A 拥有**加密操作.注册主机**特权，则虚拟机创建过程会在该主机上设置主机加密。否则，主机 B 和 C 会出现错误。
- 还可以使用 vSphere API 将集群的加密模式设置为“强制启用”。强制启用会使集群中的所有主机都加密“安全”，即 vCenter Server 在主机上安装了主机密钥。请参见《vSphere Web Services SDK 编程指南》。

## 加密虚拟机时的磁盘空间要求

您对现有虚拟机进行加密时，至少需要虚拟机目前占用空间的两倍。

## 加密 vSphere vMotion

vSphere vMotion 在迁移加密虚拟机时始终使用加密。对于未加密虚拟机，您可以选择加密 vSphere vMotion 选项之一。

加密 vSphere vMotion 可保证使用 vSphere vMotion 传输的数据的保密性、完整性和真实性。vSphere 支持在 vCenter Server 实例之间对未加密的虚拟机和加密虚拟机执行加密 vMotion。

## 哪些内容加密

对于加密磁盘，在所有情况下，数据都进行加密传输。对于未加密磁盘，将具有以下情况：

- 如果在主机内传输磁盘数据，即不更改主机，仅更改数据存储，则传输未加密。
- 如果在主机之间传输磁盘数据并使用加密 vMotion，则传输将加密。如果未使用加密 vMotion，则传输未加密。

对于加密的虚拟机，使用 vSphere vMotion 迁移时始终使用加密 vSphere vMotion。您无法为加密虚拟机关闭加密 vSphere vMotion。

## 加密的 vSphere vMotion 状态

对于未加密的虚拟机，您可以将加密 vSphere vMotion 设置为以下状态之一。默认状态为“视情况”。

### 已禁用

不使用加密 vSphere vMotion。

### 视情况

如果源主机和目标主机都支持，则可以使用加密 vSphere vMotion。仅 ESXi 6.5 及更高版本使用加密 vSphere vMotion。

### 必需

仅允许加密 vSphere vMotion。如果源主机或目标主机不支持加密 vSphere vMotion，则不允许使用 vSphere vMotion 进行迁移。

加密虚拟机时，虚拟机会记录加密 vSphere vMotion 的当前设置。如果您稍后停用虚拟机加密，则在您明确更改设置之前，加密 vMotion 设置将保持为“必需”。您可以使用[编辑设置](#)进行设置更改。

有关激活和停用未加密虚拟机的加密 vSphere vMotion 的信息，请参见《vCenter Server 和主机管理》文档。

---

**注** 目前，必须使用 vSphere API 在 vCenter Server 实例之间迁移或克隆加密虚拟机。请参见《vSphere Web Services SDK 编程指南》和《vSphere Web Services API 参考》。

---

## 在 vCenter Server 实例之间迁移或克隆加密虚拟机

vSphere vMotion 支持在 vCenter Server 实例之间迁移和克隆加密虚拟机。

在 vCenter Server 实例之间迁移或克隆加密虚拟机时，必须将源和目标 vCenter Server 实例配置为共享用于对虚拟机进行加密的密钥提供程序。此外，源和目标 vCenter Server 实例上的密钥提供程序名称也必须相同，它们具有以下特征。

- 标准密钥提供程序：该密钥提供程序中的密钥服务器必须相同。
- 可信密钥提供程序：目标主机上必须配置相同的 vSphere Trust Authority 服务。
- vSphere Native Key Provider：必须具有相同的 KDK。

---

**注** 无论源主机是否位于集群中，都无法将使用 vSphere Native Key Provider 加密的虚拟机克隆或迁移到独立主机。

---

目标 vCenter Server 确保目标 ESXi 主机已设置加密模式，从而确保主机可通过加密保障安全。

使用 vSphere vMotion 在 vCenter Server 实例之间迁移或克隆加密虚拟机时，需要具备以下特权。

- 迁移：[加密操作.迁移](#)（在虚拟机上）
- 克隆：[加密操作.克隆](#)（在虚拟机上）

此外，目标 vCenter Server 还必须具有[加密操作.加密新项](#)特权。如果目标 ESXi 主机未处于“安全”模式，则目标 vCenter Server 也必须具有[加密操作.注册主机](#)特权。



在同一 vCenter Server 或跨 vCenter Server 实例迁移虚拟机（未加密或加密）时，不允许执行某些任务。

- 不能更改虚拟机存储策略。
- 不能执行密钥更改。

---

**注** 可以在克隆虚拟机时更改虚拟机存储策略。

---

## 在 vCenter Server 实例之间迁移或克隆加密虚拟机的最低要求

使用 vSphere vMotion 在 vCenter Server 实例之间迁移或克隆标准密钥提供程序加密虚拟机的最低版本要求：

- 源和目标 vCenter Server 实例都必须为 7.0 或更高版本。
- 源和目标 ESXi 主机都必须为 6.7 或更高版本。

使用 vSphere vMotion 在 vCenter Server 实例之间迁移或克隆可信密钥提供程序加密虚拟机的最低版本要求：

- 必须为目标主机配置 vSphere Trust Authority 服务，且目标主机必须已证明。
- 迁移时无法更改加密。例如，将虚拟机迁移到新存储时，无法加密未加密的磁盘。
- 可以将标准加密虚拟机迁移到受信任主机。源和目标 vCenter Server 实例上的密钥提供程序名称必须相同。
- 无法将 vSphere Trust Authority 加密虚拟机迁移到非受信任主机。

## 可信密钥提供程序 vMotion 和跨 vCenter Server vMotion

可信密钥提供程序完全支持跨 ESXi 主机 vMotion

支持跨 vCenter Server vMotion，但具有以下限制。

- 1 必须在目标主机上配置所需的可信服务，且目标主机必须已证明。
- 2 迁移时无法更改加密。例如，将虚拟机迁移到新存储时，无法加密磁盘。

执行跨 vCenter Server vMotion 时，vCenter Server 会检查可信密钥提供程序在目标主机上是否可用，以及主机是否有权访问该密钥提供程序。

## vSphere Native Key Provider vMotion 和跨 vCenter Server vMotion

vSphere Native Key Provider 支持跨 ESXi 主机 vMotion 和加密 vMotion 如果在目标主机上配置了 vSphere Native Key Provider，则支持跨 vCenter Server vMotion。



## 虚拟机加密最佳做法

请遵循虚拟机加密最佳做法，以避免以后（例如，在生成 `vm-support` 包时）遇到问题。

### 入门最佳做法

要避免在使用虚拟机加密时出现问题，请遵循以下常规最佳做法。

- 不要加密任何 vCenter Server Appliance 虚拟机。
- 如果 ESXi 主机发生故障，请尽快检索支持包。要生成使用密码的支持包或解密核心转储，主机密钥必须可用。如果重新引导主机，主机密钥可能会更改。如果发生这种情况，则无法再生成包含密码的支持包，或使用主机密钥解密支持包中的核心转储。
- 精心管理密钥提供程序名称。如果已在使用的密钥服务器的密钥提供程序名称发生更改，则使用此密钥服务器中的密钥加密的虚拟机在打开电源或进行注册时将进入锁定状态。在这种情况下，请从 vCenter Server 中移除该密钥服务器，然后使用最初所用的密钥提供程序名称重新添加。
- 不要编辑 VMX 文件和 VMDK 描述符文件。这些文件包含加密包。所做更改可能会使虚拟机不可恢复，并且可能无法修复恢复问题。
- vSphere 虚拟机加密过程先对主机上的数据进行加密，然后再将数据写入存储。以这种方式加密虚拟机时，后端存储功能（如去重、压缩、复制等）的有效性可能会受到影响。
- 如果使用多层加密，例如，vSphere 虚拟机加密和客户机内加密（BitLocker、dm-crypt 等），则虚拟机的整体性能可能会受到影响，因为加密过程会使用额外的 CPU 和内存资源。
- 确保使用 vSphere 虚拟机加密进行加密的虚拟机的复制副本有权在恢复站点访问加密密钥。对于标准密钥提供程序，在 vSphere 外部作为密钥管理系统设计的一部分进行处理。对于 vSphere Native Key Provider，请确保存在 Native Key Provider 密钥的备份副本，并受到保护以防丢失。有关详细信息，请参见[备份 vSphere Native Key Provider](#)。
- 加密会占用大量 CPU。AES-NI 可以大幅提高加密性能。在您的 BIOS 中启用 AES-NI。

### 加密核心转储的最佳做法

请遵循以下最佳做法以避免在想要检查核心转储以诊断问题时遇到问题。

- 建立有关核心转储的策略。核心转储会进行加密，因为它们可能包含敏感信息（例如密钥）。解密核心转储时，将其视为敏感信息进行处理。ESXi 核心转储可能包含用于 ESXi 主机以及该主机上的虚拟机的密钥。考虑在解密核心转储后更改主机密钥并重新加密已加密的虚拟机。您可以使用 vSphere API 执行这两项任务。

有关详细信息，请参见[vSphere 虚拟机加密和核心转储](#)。

- 在收集 `vm-support` 包时，始终应使用密码。通过 vSphere Client 或使用 `vm-support` 命令生成支持包时，您可以指定密码。

密码会重新加密使用内部密钥的核心转储，以便使用基于该密码的密钥。您可以在以后使用该密码来解密支持包中可能包含的任何加密核心转储。使用密码选项不会影响未加密的核心转储和日志。

- 在创建 vm-support 包期间指定的密码不会保留在 vSphere 组件中。您需要负责跟踪支持包的密码。
- 在更改主机密钥前，生成包含密码的 vm-support 包。稍后可以使用该密码访问可能已使用旧主机密钥进行加密的任何核心转储。

## 密钥生命周期管理最佳做法

请实施可保证密钥服务器可用性并监控密钥服务器上的密钥的最佳做法。

- 您负责实施可为密钥服务器的可用性提供保障的策略。

如果密钥服务器不可用，则要求 vCenter Server 从密钥服务器请求密钥的虚拟机操作将无法进行。这意味着正在运行的虚拟机将继续运行，您可以打开和关闭这些虚拟机的电源，还可以重新配置这些虚拟机。但是，无法将虚拟机重定位到不具有密钥信息的主机。

大多数关键服务器解决方案都包括高可用性功能。可以使用 vSphere Client 或 API 指定密钥提供程序和关联的密钥服务器。

---

**注** 从版本 7.0 Update 2 开始，即使密钥服务器暂时脱机或不可用，加密的虚拟机和虚拟 TPM 也可以继续运行。ESXi 主机可以保留加密密钥，以继续执行加密和 vTPM 操作。请参见 [ESXi 主机上的 vSphere 密钥持久性](#)。

---

- 您需要负责跟踪密钥，以及在现有虚拟机的密钥不处于“活动”状态时执行修复。

KMIP 标准定义了以下密钥状态。

- 活动前
- 活动
- 已取消激活
- 已泄漏
- 已破坏
- 已破坏且已泄漏

“vSphere 虚拟机加密”仅使用活动密钥进行加密。如果密钥处于“活动前”状态，“vSphere 虚拟机加密”会激活该密钥。如果密钥处于“已取消激活”、“已泄漏”、“已破坏”或“已破坏且已泄漏”状态，则无法使用该密钥对虚拟机或虚拟磁盘进行加密。

如果密钥处于其他状态，使用这些密钥的虚拟机将继续工作。克隆或迁移操作能否成功取决于密钥是否已存在于主机上。

- 如果密钥位于目标主机上，则即使该密钥在密钥服务器上不处于“活动”状态，操作也会成功。
- 如果所需的虚拟机密钥和虚拟磁盘密钥不位于目标主机上，则 vCenter Server 必须从密钥服务器获取密钥。如果密钥处于“已取消激活”、“已泄漏”、“已破坏”或“已破坏且已泄漏”状态，则 vCenter Server 会显示错误，并且操作将不成功。

如果密钥已存在于主机上，则克隆或迁移操作将成功。如果 vCenter Server 必须从密钥服务器提取密钥，则操作将失败。

如果不处于“活动”状态，请使用 API 执行重新生成密钥操作。请参见《vSphere Web Services SDK 编程指南》。

- 制定密钥轮换策略，使密钥在特定时间后停用并滚动。
  - 可信密钥提供程序：更改可信密钥提供程序的主密钥。
  - vSphere Native Key Provider：更改 vSphere Native Key Provider 的 `key_id`。

## 备份和还原最佳做法

请设置有关备份和还原操作的策略。

- 并非所有备份架构均受支持。请参见[虚拟机加密互操作性](#)。
- 请为还原操作设置策略。由于备份始终以明文方式进行，因此请计划在还原完成后立即对虚拟机进行加密。您可以指定在还原操作的过程中对虚拟机进行加密。如果可能，请在还原过程中对虚拟机进行加密，以避免暴露敏感信息。要更改与虚拟机关联的任何磁盘的加密策略，请更改该磁盘的存储策略。
- 由于虚拟机主页文件已加密，请确保加密密钥在还原时可用。

## 提高性能的最佳做法

- 加密性能取决于 CPU 和存储速度。
- 对现有虚拟机进行加密所需的时间比在创建虚拟机期间对其进行加密更多。请尽可能在创建虚拟机期间对其进行加密。

## 样本存储策略的最佳做法

不要修改捆绑的虚拟机加密示例存储策略。相反，应克隆该策略并对克隆进行编辑。

---

**注** 没有任何自动方法可用于将虚拟机加密策略恢复为其原始设置。

---

有关自定义存储策略的详细信息，请参见《vSphere 存储》文档。

## 移除加密密钥的最佳做法

要确保从集群中移除加密密钥，请在删除、取消注册加密虚拟机或将加密虚拟机移至另一个 vCenter Server 后，重新引导集群中的 ESXi 主机。

## 虚拟机加密限制

请查看以下虚拟机加密限制以避免以后遇到问题。

要了解哪些设备和功能不能与虚拟机加密结合使用，请参见[虚拟机加密互操作性](#)。

## 加密虚拟机限制

规划虚拟机加密策略时，请考虑以下限制。

- 克隆已加密虚拟机或执行 **Storage vMotion** 操作时，您可以尝试更改磁盘格式。此类转换不一定成功。例如，如果您克隆一个虚拟机并尝试将磁盘格式从延迟置零厚格式更改为精简置备格式，虚拟机磁盘将保持延迟置零厚格式。
- 从虚拟机分离磁盘时，该虚拟磁盘的存储策略信息不会保留。
  - 如果虚拟磁盘已加密，则您必须将存储策略显式设置为虚拟机加密策略，或显式设置为包含加密的存储策略。
  - 如果虚拟磁盘未加密，则您可以在将该磁盘添加到虚拟机时更改存储策略。

有关详细信息，请参见[虚拟磁盘加密](#)。

- 将虚拟机移动到其他集群之前，请解密核心转储。

vCenter Server 不会存储密钥服务器密钥，只会跟踪密钥 ID。因此，vCenter Server 不会持久存储 ESXi 主机密钥。但是，在 vSphere 7.0 Update 2 及更高版本中，即使对密钥服务器的访问中断，加密设备也可以正常工作。请参见 [ESXi 主机上的 vSphere 密钥持久性](#)。

在某些情况下，例如当您将 ESXi 主机移动到其他集群并重新引导该主机时，vCenter Server 会为该主机分配新的主机密钥。您无法使用新的主机密钥解密任何现有的核心转储。

- 已加密虚拟机不支持 OVF 导出。
- 不支持使用 VMware Host Client 注册加密的虚拟机。

## 虚拟机锁定状态

如果虚拟机密钥或一个或多个虚拟磁盘密钥缺失，虚拟机将进入锁定状态。在锁定状态下，您无法执行虚拟机操作。

- 通过 vSphere Client 对虚拟机及其磁盘进行加密时，同一个密钥用于两者。
- 使用 API 执行加密时，您可以对虚拟机和磁盘使用不同的加密密钥。在这种情况下，如果您尝试打开虚拟机的电源，并且其中一个磁盘密钥缺失，则打开电源操作将失败。如果移除该虚拟磁盘，则您可以打开虚拟机的电源。

有关故障排除建议，请参见[解决缺失加密密钥问题](#)。

## 虚拟机加密互操作性

vSphere 虚拟机加密在可与之进行交互的设备和功能方面具有一些限制。

以下限制和备注适用于使用 vSphere 虚拟机加密的情况。有关使用 vSAN 加密的类似信息，请参见《管理 VMware vSAN》文档。

## 某些加密任务的限制

在加密虚拟机上执行某些任务时，存在一些限制。

- 无法在已打开电源的虚拟机上执行大多数加密操作。必须关闭虚拟机电源。您可以克隆已加密虚拟机，还可以在虚拟机已打开电源时执行浅层重新加密。
- 无法在具有快照的虚拟机上执行深层重新加密。可以在具有快照的虚拟机上执行浅层重新加密。

## 虚拟可信平台模块设备和 vSphere 虚拟机加密

虚拟可信平台模块 (vTPM) 是物理可信平台模块 2.0 芯片的基于软件的表示形式。可以将 vTPM 添加到新虚拟机，也可以添加到现有虚拟机。要将 vTPM 添加到虚拟机，必须在 vSphere 环境中配置密钥提供程序。配置 vTPM 时，将对虚拟机的“主”文件（内存交换、NVRAM 文件等）进行加密。磁盘文件或 VMDK 文件不会自动加密。可以选择为虚拟机磁盘明确添加加密。

**小心** 克隆虚拟机将复制整个虚拟机，包括 vTPM 等虚拟设备。存储在 vTPM 中的信息（包括软件可用于确定系统身份的 vTPM 属性）也会进行复制。

从 vSphere 8.0 开始，克隆包含 vTPM 的虚拟机时，可以选择从新的空白 vTPM 开始，该 vTPM 会获取自己的密钥和身份。

## vSphere 虚拟机加密以及挂起状态和快照

可以从加密虚拟机的挂起状态恢复，也可以恢复到加密虚拟机的内存快照。可以在 ESXi 主机之间迁移具有内存快照且处于挂起状态的加密虚拟机。

## vSphere 虚拟机加密和 IPv6

可以将 vSphere 虚拟机加密与纯 IPv6 模式或混合模式结合使用。可以为密钥服务器配置 IPv6 地址。可以为 vCenter Server 和密钥服务器仅配置 IPv6 地址。

## vSphere 虚拟机加密中的克隆限制

对于所有密钥提供程序类型，支持克隆需要满足一定的条件。您可以在克隆时更改加密密钥。某些克隆功能无法与 vSphere 虚拟机加密配合工作。

- 支持完整克隆。克隆将继承父加密状态，包括密钥。可以加密完整克隆，重新加密完整克隆以使用新密钥，或解密完整克隆。

支持链接克隆。克隆将继承父加密状态，包括密钥。无法解密链接克隆或使用其他密钥重新加密链接克隆。

**注** 验证其他应用程序是否支持链接克隆。例如，VMware Horizon<sup>®</sup> 7 支持完整克隆和即时克隆，但不支持链接克隆。

- 所有密钥提供程序类型均支持即时克隆，但您无法更改克隆上的加密密钥。
- 您可以从加密的虚拟机创建链接的克隆虚拟机。链接的克隆虚拟机包含相同的密钥。您可以对链接克隆的加密虚拟机“主页”文件重新加密，但无法对磁盘重新加密。

## vSphere Native Key Provider 的限制

vSphere Native Key Provider 不支持某些操作。

- 无法使用 vSphere Native Key Provider 加密独立主机上的虚拟机。主机必须位于集群中才能使用 vSphere Native Key Provider。
- 无法将包含使用 vSphere Native Key Provider 加密的虚拟机的主机移至其他集群，除非目标集群包含相同的 vSphere Native Key Provider。（当加密密钥不存在且目标集群不具有相同的 vSphere Native Key Provider 时，已移动主机上的加密虚拟机将被锁定。）
- 由于不支持 vSphere Native Key Provider，无法将 vSphere Native Key Provider 加密的虚拟机注册到旧版主机。
- 由于要求独立主机位于集群中，无法将 vSphere Native Key Provider 加密的虚拟机注册到独立主机。

## vSphere 虚拟机加密不支持的磁盘配置

某些类型的虚拟机磁盘配置不支持 vSphere 虚拟机加密。

- RDM（裸设备映射）。但是，支持 vSphere Virtual Volumes (vVols)。
- 多写入程序或共享磁盘（MSCS、WSFC 或 Oracle RAC）。多写入器磁盘支持加密虚拟机的“主”文件。多写入器磁盘不支持加密虚拟磁盘。如果尝试在具有加密虚拟磁盘的虚拟机的[编辑设置](#)页面中选择“多写入器”，则会取消激活**确定**按钮。

## vSphere 虚拟机加密中的其他限制

无法与 vSphere 虚拟机加密配合使用的其他功能包括。

- vSphere ESXi Dump Collector
- 内容库
  - 内容库支持两种类型的模板，即 OVF 模板类型和虚拟机模板类型。无法将加密虚拟机导出为 OVF 模板类型。OVF Tool 不支持加密虚拟机。可以使用虚拟机模板类型创建加密虚拟机模板。从 vSphere 8.0 开始，ovftool 命令包含将 vTPM 占位符添加到 OVF 描述符文件的选项。从此类模板部署虚拟机时，vCenter Server 在目标虚拟机上创建具有唯一密钥的 vTPM。请参见《vSphere 虚拟机管理》文档。
- 用于备份加密虚拟磁盘的软件必须使用 VMware vSphere Storage API - Data Protection (VADP) 在热添加模式或启用了 SSL 的 NBD 模式下备份磁盘。但是，并非所有使用 VADP 进行虚拟磁盘备份的备份解决方案都受支持。有关详细信息，请咨询您的备份供应商。
  - 不支持使用 VADP SAN 传输模式解决方案备份加密虚拟磁盘。
  - 加密虚拟磁盘支持 VADP 热添加解决方案。备份软件必须支持对在热添加备份工作流程中使用的代理虚拟机进行加密。供应商必须具有**加密操作.加密虚拟机**特权。
  - 备份加密虚拟磁盘时，支持使用 NBD-SSL 传输模式的备份解决方案。供应商应用程序必须具有**加密操作.直接访问**特权。



- 无法将已加密虚拟机的输出发送到串行端口或并行端口。即使配置看起来成功，输出也会发送到文件。
- VMware Cloud on AWS 不支持 vSphere 虚拟机加密。请参见《管理 VMware Cloud on AWS 数据中心》文档。

## ESXi 主机上的 vSphere 密钥持久性

在 vSphere 7.0 Update 2 及更高版本中，即使密钥服务器暂时脱机或不可用，加密的虚拟机和虚拟 TPM 也可以继续运行（可选）。ESXi 主机可以保留加密密钥，以继续执行加密和 vTPM 操作。

在 vSphere 7.0 Update 2 之前，密钥服务器必须始终可用加密虚拟机和 vTPM 才能正常工作。在 vSphere 7.0 Update 2 及更高版本中，即使对密钥服务器的访问中断，加密设备也可以正常运行。

从 vSphere 7.0 Update 3 开始，即使对密钥提供程序的访问中断，加密 vSAN 集群也可以正常运行。

---

**注** 使用 vSphere Native Key Provider 时，不需要密钥持久性。vSphere Native Key Provider 设计为即时可用，无需访问密钥服务器即可运行。请参见以下部分：“密钥持久性和 vSphere Native Key Provider”。

---

## ESXi 主机上的密钥持久性的工作原理

使用标准密钥提供程序时，ESXi 主机依靠 vCenter Server 来管理加密密钥。使用可信密钥提供程序时，ESXi 主机直接依靠 Trust Authority 主机获取密钥，并不涉及 vCenter Server。vSphere Native Key Provider 处理密钥的方式不同。有关更多信息，请参见下一部分。

无论密钥提供程序是何种类型，ESXi 主机最初都会获取密钥，并将其保留在其密钥缓存中。如果 ESXi 主机重新引导，它将丢失其密钥缓存。然后，ESXi 主机再次向密钥服务器（标准密钥提供程序）或 Trust Authority 主机（可信密钥提供程序）请求密钥。当 ESXi 主机尝试获取密钥时，如果密钥服务器处于脱机状态或无法访问，则 vTPMs 和工作负载加密将无法正常运行。对于 Edge 式部署（通常站点上未部署密钥服务器），与密钥服务器的连接中断可能会导致加密工作负载不必要地停止。

在 vSphere 7.0 Update 2 及更高版本中，即使密钥服务器处于脱机状态或无法访问，加密工作负载也可以继续工作。如果 ESXi 主机具有 TPM，即使重新引导，加密密钥也会保留在 TPM 中。因此，即使 ESXi 主机重新引导，主机也无需请求加密密钥。此外，当密钥服务器不可用时，仍然可以继续加密和解密操作，因为密钥保留在 TPM 中。从本质上说，当密钥服务器或 Trust Authority 主机不可用时，您可以继续“无密钥服务器”运行加密工作负载，具体取决于密钥提供程序。此外，即使密钥服务器无法访问，vTPM 也可以继续运行。

## 密钥持久性和 vSphere Native Key Provider

使用 vSphere Native Key Provider 时，vSphere 会生成加密密钥，而无需使用密钥服务器。ESXi 主机获取密钥派生密钥 (KDK)，该密钥用于派生其他密钥。收到 KDK 并生成其他密钥后，ESXi 主机无需访问 vCenter Server，即可执行加密操作。从本质上说，vSphere Native Key Provider 始终“无密钥服务器”运行。

默认情况下，即使 ESXi 主机重新引导，甚至 vCenter Server 在主机重新引导后不可用时，KDK 仍会保留在主机上。

您可以使用 vSphere Native Key Provider 激活密钥持久性，但通常无需执行此操作。ESXi 主机可完全访问 vSphere Native Key Provider，因此额外的密钥持久性是冗余的。使用 vSphere Native Key Provider 激活密钥持久性的一个用例是，当您还配置了标准密钥提供程序（外部 KMIP 服务器）时。

## 如何设置密钥持久性

要激活或停用密钥持久性，请参见 [在 ESXi 主机上激活和停用密钥持久性](#)。



# 配置和管理标准密钥提供程序

# 7

要在 vSphere 环境中使用标准密钥提供程序，需要进行一些准备工作。设置环境之后，您可以创建已加密虚拟机和虚拟磁盘，还可以对现有的虚拟机和虚拟磁盘进行加密。

针对标准密钥提供程序设置环境后，可以使用 vSphere Client 创建加密虚拟机和虚拟磁盘，还可以对现有的虚拟机和磁盘进行加密。请参见第 10 章 [在 vSphere 环境中使用加密](#)。

可以使用 API 和 crypto-util CLI 执行附加任务。请参见《vSphere Web Services SDK 编程指南》，获取 API 文档；参见 crypto-util 命令行帮助，了解有关该工具的详细信息。

本章讨论了以下主题：

- [标准密钥提供程序概览](#)
- [设置标准密钥提供程序](#)
- [为不同用户设置不同的密钥提供程序](#)

## 标准密钥提供程序概览

您可以使用标准密钥提供程序执行虚拟机加密任务。

### 什么是标准密钥提供程序？

在 vSphere 中，标准密钥提供程序可直接从密钥服务器获取加密密钥，vCenter Server 则将密钥分发给数据中心内所需的 ESXi 主机。

可以为不同用户添加单独的标准密钥提供程序，并设置默认的标准密钥提供程序。

### vSphere 标准密钥提供程序要求

- vSphere 6.5 或更高版本
- 外部密钥服务器 (KMS)

密钥服务器必须支持密钥管理互操作协议 (KMIP) 1.1 标准。请参见《vSphere 兼容性列表》获取详细信息。

您可以在“平台和计算资源”下的《[VMware 兼容性指南](#)》中找到有关 VMware 认证密钥服务器 (KMS) 供应商的信息。如果您选择的是兼容性指南，则可以打开密钥管理服务器 (KMS) 兼容性文档。本文档时常更新。

## 标准密钥提供程序特权

标准密钥提供程序使用 **Cryptographer.\*** 特权。请参见[加密操作特权](#)。

## 设置标准密钥提供程序

必须先设置标准密钥提供程序，之后才能开始执行虚拟机加密任务。

设置标准密钥提供程序的过程包括添加密钥提供程序及与密钥服务器建立信任。添加密钥提供程序时，系统会提示您将其设为默认密钥提供程序。可以明确更改默认密钥提供程序。vCenter Server 从默认密钥提供程序置备密钥。

---

**注** 以前，在 vSphere 6.5 和 6.7 中称为密钥管理服务器集群，现在称为密钥提供程序。

---

## 使用 vSphere Client 添加标准密钥提供程序

可以通过 vSphere Client 或使用公用 API 将标准密钥提供程序添加到 vCenter Server 系统。

通过 vSphere Client，可以将标准密钥提供程序添加到 vCenter Server 系统，并在密钥服务器与 vCenter Server 之间建立信任关系。

- 可以添加来自同一供应商的多个密钥服务器。
- 如果您的环境支持不同供应商提供的解决方案，则可以添加多个密钥提供程序。
- 如果您的环境包含多个密钥提供程序，且您删除了默认密钥提供程序，则必须明确设置另一个默认密钥提供程序。
- 可以为密钥服务器配置 IPv6 地址。
  - vCenter Server 系统和密钥服务器都可以仅配置 IPv6 地址。

### 前提条件

- 验证密钥服务器 (KMS) 是否在《密钥管理服务器 (KMS) 的 VMware 兼容性指南》中列出，是否符合 KMIP 1.1，以及是否可以成为对称密钥 Foundry 和服务器。
- 验证您是否拥有所需特权：**加密操作.管理密钥服务器**。
- 确保密钥服务器具有高可用性。在发生停电或灾难恢复等事件期间与密钥服务器断开连接会致使加密虚拟机无法访问。

---

**注** 从 vSphere 7.0 Update 2 开始，即使密钥服务器暂时脱机或不可用，加密的虚拟机和虚拟 TPM 也可以继续运行。请参见 [ESXi 主机上的 vSphere 密钥持久性](#)。

---

- 仔细考虑您的基础架构对密钥服务器的依赖关系。某些 KMS 解决方案以虚拟设备的形式交付，因此可能会产生依赖关系循环或其他与 KMS 设备放置位置不佳相关的可用性问题。

### 步骤

- 1 使用 vSphere Client 登录到 vCenter Server 系统。
- 2 浏览清单列表，然后选择 vCenter Server 实例。

- 3 单击**配置**，然后在**安全**下单击**密钥提供程序**。
- 4 单击**添加标准密钥提供程序**，然后输入密钥提供程序信息。

选项	值
名称	密钥提供程序的名称。 每个逻辑密钥提供程序（无论其类型如何：标准、可信和本机密钥提供程序），都必须在所有 vCenter Server 系统中具有唯一的名称。 有关详细信息，请参见 <a href="#">密钥提供程序命名</a> 。
KMS	密钥服务器 (KMS) 的别名。
地址	密钥服务器的 IP 地址或 FQDN。
端口	vCenter Server 连接到密钥服务器的端口。
代理服务器	用于连接到密钥服务器的可选代理服务器地址。
代理端口	用于连接到密钥服务器的可选代理端口。
用户名	一些密钥服务器供应商允许用户通过指定用户名和密码来隔离不同用户或组使用的加密密钥。仅当您的密钥服务器支持此功能且您准备使用时指定用户名。
密码	一些密钥服务器供应商允许用户通过指定用户名和密码来隔离不同用户或组使用的加密密钥。仅当您的密钥服务器支持此功能且您准备使用时指定密码。

可以通过单击**添加 KMS** 添加更多密钥服务器。

- 5 单击**添加密钥提供程序**。
- 6 单击**信任**。

vCenter Server 将添加密钥提供程序，并将状态显示为“已连接”。

#### 后续步骤

请参见[通过交换证书建立标准密钥提供程序可信连接](#)。

## 通过交换证书建立标准密钥提供程序可信连接

将标准密钥提供程序添加到 vCenter Server 系统后，可以建立可信连接。具体过程取决于密钥提供程序接受的证书和公司策略。

#### 前提条件

添加标准密钥提供程序。

#### 步骤

- 1 导航到 vCenter Server。
- 2 单击**配置**，然后选择**安全**下的**密钥提供程序**。
- 3 选择密钥提供程序。  
此时将显示该密钥提供程序的 KMS。
- 4 选择 KMS。

- 5 从**建立信任**下拉菜单中，选择**使 KMS 信任 vCenter**。
- 6 选择适用于服务器的选项，然后执行各个步骤。

选项	请参见
vCenter Server 根 CA 证书	使用“根 CA 证书”选项建立标准密钥提供程序可信连接。
vCenter Server 证书	使用“证书”选项建立标准密钥提供程序可信连接。
上载证书和私有密钥	使用“上载证书和私钥”选项建立标准密钥提供程序可信连接。
新建证书签名请求	使用“新建证书签名请求”选项建立标准密钥提供程序可信连接。

## 使用“根 CA 证书”选项建立标准密钥提供程序可信连接

某些密钥管理服务器 (KMS) 供应商要求将根 CA 证书上载到 KMS。随后，此 KMS 即会信任根 CA 签名的所有证书。

vSphere 虚拟机加密使用的根 CA 证书为自签名证书，它存储在 vCenter Server 系统上 VMware Endpoint 证书存储 (VECS) 的独立库中。

**注** 仅当要替换现有证书时才生成根 CA 证书。如果执行此操作，根 CA 签名的其他证书将变为无效。可以在此工作流程中生成新的根 CA 证书。

### 步骤

- 1 导航到 vCenter Server。
- 2 单击**配置**，然后选择**安全**下的**密钥提供程序**。
- 3 选择要与之建立可信连接的密钥提供程序。  
此时将显示该密钥提供程序的密钥服务器 (KMS)。
- 4 从**建立信任**下拉菜单中，选择**使 KMS 信任 vCenter**。
- 5 选择 **vCenter 根 CA 证书**，然后单击**下一步**。

“下载根 CA 证书”对话框将填充 vCenter Server 用于加密的根证书。此证书存储在 VECS 中。

- 6 将证书复制到剪贴板，或将证书作为文件下载。
- 7 按照您的 KMS 供应商的说明，将证书上载到其系统中。

**注** 某些 KMS 供应商要求 KMS 供应商重新启动 KMS 以发现上载的根证书。

### 后续步骤

完成证书交换。请参见[完成标准密钥提供程序的信任设置](#)。

## 使用“证书”选项建立标准密钥提供程序可信连接

某些密钥管理服务器 (KMS) 供应商要求将 vCenter Server 证书上载到 KMS。上载后，KMS 便会接受来自具有该证书的系统的流量。

vCenter Server 将生成证书以保护与 KMS 的连接。证书存储在 vCenter Server 系统上 VMware Endpoint 证书存储 (VECS) 的独立密钥库中。

### 步骤

- 1 导航到 vCenter Server。
- 2 单击**配置**，然后选择**安全**下的**密钥提供程序**。
- 3 选择要与之建立可信连接的密钥提供程序。  
此时将显示该密钥提供程序的密钥服务器 (KMS)。
- 4 从**建立信任**下拉菜单中，选择**使 KMS 信任 vCenter**。
- 5 选择 **vCenter 证书**，然后单击**下一步**。

“下载证书”对话框将填充 vCenter Server 用于加密的根证书。此证书存储在 VECS 中。

---

**注** 除非您要替换现有证书，否则请勿生成新证书。

---

- 6 将证书复制到剪贴板，或将其作为文件下载。
- 7 按照您的 KMS 供应商的说明，将证书上载到 KMS。

### 后续步骤

完成信任关系。请参见[完成标准密钥提供程序的信任设置](#)。

## 使用“上载证书和私钥”选项建立标准密钥提供程序可信连接

某些密钥管理服务器 (KMS) 供应商要求将 KMS 服务器证书和私钥上载到 vCenter Server 系统。

某些 KMS 供应商会针对连接生成证书和私有密钥，并为您提供这些内容。上载这些文件之后，KMS 将信任您的 vCenter Server 实例。

### 前提条件

- 向 KMS 供应商请求证书和私有密钥。这些文件为 PEM 格式的 X509 文件。

### 步骤

- 1 导航到 vCenter Server。
- 2 单击**配置**，然后选择**安全**下的**密钥提供程序**。
- 3 选择要与之建立可信连接的密钥提供程序。  
此时将显示该密钥提供程序的密钥服务器 (KMS)。
- 4 从**建立信任**下拉菜单中，选择**使 KMS 信任 vCenter**。
- 5 选择 **KMS 证书和私钥**，然后单击**下一步**。

- 6 将从 KMS 供应商收到的证书粘贴到顶部文本框中，或单击**上载文件**上载证书文件。
- 7 将密钥文件粘贴到底部文本框中，或单击**上载文件**上载密钥文件。
- 8 单击**建立信任**。

#### 后续步骤

完成信任关系。请参见[完成标准密钥提供程序的信任设置](#)。

### 使用“新建证书签名请求”选项建立标准密钥提供程序可信连接

某些密钥管理服务器 (KMS) 供应商要求 vCenter Server 生成证书签名请求 (Certificate Signing Request, CSR) 并将该 CSR 发送到 KMS。KMS 将签署 CSR 并返回已签名证书。可以将已签名证书上载到 vCenter Server。

使用**新建证书签名请求**选项的过程分为两步。首先，生成 CSR 并将其发送给 KMS 供应商。然后，将从 KMS 供应商收到的已签名证书上载到 vCenter Server。

#### 步骤

- 1 导航到 vCenter Server。
- 2 单击**配置**，然后选择**安全**下的**密钥提供程序**。
- 3 选择要与之建立可信连接的密钥提供程序。  
此时将显示该密钥提供程序的密钥服务器 (KMS)。
- 4 从**建立信任**下拉菜单中，选择**使 KMS 信任 vCenter**。
- 5 选择**新建证书签名请求 (CSR)**，然后单击**下一步**。
- 6 在对话框中，将文本框中的完整证书复制到剪贴板，或将其作为文件下载。  
仅当您明确生成 CSR 时才使用该对话框中的**生成新的 CSR** 按钮。
- 7 按照 KMS 供应商的说明提交 CSR。
- 8 从 KMS 供应商收到签名证书时，再次单击**密钥提供程序**，选择密钥提供程序，然后从**建立信任**下拉菜单中，选择**上载已签名 CSR 证书**。
- 9 将签名证书粘贴到底部文本框中，或单击**上载文件**并上载文件，然后单击**上载**。

#### 后续步骤

完成信任关系。请参见[完成标准密钥提供程序的信任设置](#)。

### 完成标准密钥提供程序的信任设置

除非**添加密钥提供程序**对话框提示您信任 KMS，否则必须在完成证书交换后明确建立信任。

您可以完成信任设置，即：通过信任 KMS 或上载 KMS 证书使 vCenter Server 信任 KMS。您有两个选项：

- 通过使用**上载 KMS 证书**选项明确信任证书。

- 通过使用**使 vCenter 信任 KMS** 选项，将 KMS 叶证书或 KMS CA 证书上载到 vCenter Server。

**注** 如果上载根 CA 证书或中间 CA 证书，则 vCenter Server 将信任 CA 签发的所有证书。出于强安全性，请上载叶证书或 KMS 供应商控制的中间 CA 证书。

#### 步骤

- 1 导航到 vCenter Server。
- 2 单击**配置**，然后选择**安全**下的**密钥提供程序**。
- 3 选择要与之建立可信连接的密钥提供程序。  
此时将显示该密钥提供程序的密钥服务器 (KMS)。
- 4 选择 KMS。
- 5 从**建立信任**下拉菜单中选择以下选项之一。

选项	操作
使 vCenter 信任 KMS	在显示的对话框中，单击 <b>信任</b> 。
上载 KMS 证书	<ol style="list-style-type: none"> <li>a 在显示的对话框中，粘贴证书，或者单击<b>上载文件</b>并浏览到证书文件。</li> <li>b 单击<b>上载</b>。</li> </ol>

## 为不同用户设置不同的密钥提供程序

可以设置同一 KMS 实例的不同用户使用不同密钥提供程序的环境。具有多个密钥提供程序非常有用，例如，希望向公司的不同部门授予不同加密密钥集的访问权限的情况。

可以对同一 KMS 使用多个密钥提供程序以分隔密钥。对于不同 BU 或不同客户等用例，具有不同的密钥集非常重要。

**注** 并非所有 KMS 供应商都支持多个用户。

#### 前提条件

建立与 KMS 的连接。

#### 步骤

- 1 在 KMS 上使用相应的用户名和密码创建两个用户，例如 C1 和 C2。
- 2 登录到 vCenter Server 并创建密钥提供程序。
- 3 提示输入用户名和密码时，提供第一个用户专用的信息。
- 4 创建第二个密钥提供程序并添加相同的 KMS，但使用第二个用户名和密码 (C2)。

#### 结果

这两个密钥提供程序与 KMS 建立相互独立的连接，并使用不同的密钥集。

# 配置和管理 vSphere Native Key Provider

## 8

要在 vSphere 环境中使用 VMware vSphere® Native Key Provider™，需要进行一些准备工作。配置 vSphere Native Key Provider 后，可以在虚拟机上创建虚拟可信平台模块 (vTPM)。

针对 vSphere Native Key Provider 设置环境后，可以使用 vSphere Client 和 API 创建 vTPM。如果购买 VMware vSphere® Enterprise Plus Edition™，还可以加密虚拟机和虚拟磁盘，并加密现有虚拟机和磁盘。



(配置 vSphere Native Key Provider )

本章讨论了以下主题：

- vSphere Native Key Provider 概览
- vSphere Native Key Provider 过程流
- 配置 vSphere Native Key Provider
- 备份 vSphere Native Key Provider
- 在增强型链接模式配置中导入 vSphere Native Key Provider
- 恢复 vSphere Native Key Provider
- 更新 vSphere Native Key Provider
- 删除 vSphere Native Key Provider

## vSphere Native Key Provider 概览

在 vSphere 7.0 Update 2 及更高版本中，您可以使用内置 vSphere Native Key Provider 启用加密技术，例如虚拟 TPM (vTPM)。

所有 vSphere 版本均包含 vSphere Native Key Provider，它不需要外部密钥服务器（业内也称为密钥管理服务 (KMS)）。您还可以将 vSphere Native Key Provider 用于 vSphere 虚拟机加密，但必须购买 VMware vSphere® Enterprise Plus Edition™。



## 什么是 vSphere Native Key Provider

对于标准密钥提供程序或可信密钥提供程序，您必须配置外部密钥服务器。在标准密钥提供程序设置中，vCenter Server 从外部密钥服务器获取密钥并将它们分发给 ESXi 主机。在可信密钥提供程序 (vSphere Trust Authority) 设置中，可信 ESXi 主机直接获取密钥。

通过 vSphere Native Key Provider，不再需要外部密钥服务器。vCenter Server 会生成一个称为密钥派生密钥 (KDK) 的主密钥，并将其推送到集群中的所有 ESXi 主机。然后，ESXi 主机生成数据加密密钥（即使未连接到 vCenter Server），以启用 vTPM 等安全性功能。所有 vSphere 版本均包含 vTPM 功能。要将 vSphere Native Key Provider 用于 vSphere 虚拟机加密，您必须已购买 vSphere Enterprise Plus Edition。vSphere Native Key Provider 可与现有密钥服务器基础架构共存。

vSphere Native Key Provider:

- 允许使用 vTPM、vSphere 虚拟机加密和 vSAN 静态数据加密（如果不需要或不想使用外部密钥服务器）。
- 仅适用于 VMware 基础架构产品。
- 不提供外部互操作性、KMIP 支持、硬件安全模块或传统的第三方外部密钥服务器为实现互操作性或法规遵从性而提供的其他功能。如果您的组织需要将此功能用于非 VMware 产品和组件，请安装传统的第三方密钥服务器。
- 帮助满足无法使用或不想使用外部密钥服务器的组织的需求。
- 改进了数据清理和系统重用实践，允许在难以清理的介质（如闪存和 SSD）上早些使用加密技术。
- 提供密钥提供程序之间的转换路径。vSphere Native Key Provider 与 VMware 标准密钥提供程序和 vSphere Trust Authority 可信密钥提供程序兼容。
- 可用于使用增强型链接模式配置或 vCenter Server 高可用性配置的多个 vCenter Server 系统。
- 可用于在所有版本的 vSphere 中启用 vTPM，以及对虚拟机进行加密（但需要购买包含 vSphere 虚拟机加密的 vSphere Enterprise Plus Edition）。vSphere 虚拟机加密与 vSphere Native Key Provider 配合使用，就像与 VMware 标准和可信密钥提供程序一起使用一样。
- 可用于通过使用适当的 vSAN 许可证启用 vSAN 静态数据加密。
- 可使用可信平台模块 (TPM) 2.0 提高安全性（如果 ESXi 主机中安装了 TPM）。还可以将 vSphere Native Key Provider 配置为仅对安装了 TPM 2.0 的主机可用。

---

**注** ESXi 主机无需 TPM 2.0 即可使用 vSphere Native Key Provider。但是，TPM 2.0 确实会提高安全性。

---

与所有安全解决方案一样，请考虑系统设计、实施注意事项和使用 Native Key Provider 的利弊。例如，ESXi 密钥持久性避免了要求密钥服务器始终可用的依赖。但是，由于密钥持久性将 Native Key Provider 加密信息存储在集群主机上，因此，如果恶意操作者盗用 ESXi 主机本身，您仍会面临风险。由于环境各不相同，因此请根据您所在组织的法规和安全需求、运维要求以及风险承受能力来评估和实施安全控制。

有关 vSphere Native Key Provider 的更多概览信息，请参见 <https://core.vmware.com/native-key-provider>。

## vSphere Native Key Provider 要求

要使用 vSphere Native Key Provider，您必须：

- 确保 vCenter Server 系统和 ESXi 主机均运行 vSphere 7.0 Update 2 或更高版本。
- 在集群中配置 ESXi 主机。尽管不是必需要求，但最好使用尽可能相同的 ESXi 主机，包括 TPM。集群主机相同时，集群管理和功能启用要容易得多。
- 配置基于 vCenter Server 文件的备份和还原，并安全地存储备份，因为它们包含密钥派生密钥。请参见《vCenter Server 安装和设置》文档中有关 vCenter Server 备份和还原的主题。

要使用 vSphere Native Key Provider 执行 vSphere 虚拟机加密或 vSAN 加密，必须购买包含适当许可证的产品版本。

## vSphere Native Key Provider 和增强型链接模式

可以配置一个 vSphere Native Key Provider，并使其可在增强型链接模式下配置的 vCenter Server 系统之间共享。此场景中的简要步骤包括：

- 1 在一个 vCenter Server 系统上创建 vSphere Native Key Provider
- 2 在创建 Native Key Provider 的 vCenter Server 上备份 Native Key Provider
- 3 导出 Native Key Provider
- 4 将 Native Key Provider 导入到增强型链路模式配置中的其他 vCenter Server 系统

请参见在[增强型链接模式配置中导入 vSphere Native Key Provider](#)。

## vSphere Native Key Provider 特权

与标准和可信密钥提供程序一样，vSphere Native Key Provider 使用 **Cryptographer.\*** 特权。此外，vSphere Native Key Provider 使用 vSphere Native Key Provider 专用的 **Cryptographer.ReadKeyServersInfo** 特权列出 vSphere Native Key Provider。请参见[加密操作特权](#)。

## vSphere Native Key Provider 警报

您必须备份 vSphere Native Key Provider。如果未备份 vSphere Native Key Provider，vCenter Server 将生成警报。备份已为其生成警报的 vSphere Native Key Provider 时，vCenter Server 将重置警报。默认情况下，vCenter Server 每天检查一次备份的 vSphere Native Key Provider。可以通过修改 `vpdx.KMS.backupCheckInterval` 选项来更改检查时间间隔。

## vSphere Native Key Provider 定期修复检查

vCenter Server 定期检查 vCenter Server 和 ESXi 主机上的 vSphere Native Key Provider 配置是否匹配。当主机状态更改时（例如，当您将主机添加到集群时），集群上的密钥提供程序配置会与主机上的配置产生差异。如果主机上的配置 (keyID) 不同，vCenter Server 将自动更新主机的配置。无需任何人工干预。

默认情况下，vCenter Server 每五分钟检查一次配置。可以使用 `vpzd.KMS.remediationInterval` 选项修改时间间隔。

## 将 vSphere Native Key Provider 用于灾难恢复站点

可以将 vSphere Native Key Provider 用于备份灾难恢复站点。通过将 vSphere Native Key Provider 备份从主站点的 vCenter Server 导入到备份灾难恢复站点的 vCenter Server，该集群能够解密并运行加密的虚拟机。

始终测试 DR 解决方案。不要以为您的解决方案可正常运行，无需尝试恢复。确保 DR 站点也可以使用 vSphere Native Key Provider 备份的副本。

## vSphere Native Key Provider 过程流

了解 vSphere Native Key Provider 过程流对于配置和管理 vSphere Native Key Provider 至关重要。

您可以使用内置 vSphere Native Key Provider 为基于加密的虚拟 TPM (vTPM) 供电。所有 vSphere 版本均包含 vSphere Native Key Provider，它不需要外部密钥服务器 (KMS)。要将 vSphere Native Key Provider 用于 vSphere 虚拟机加密，您必须购买 vSphere Enterprise+ 版本。

## 配置 vSphere Native Key Provider

配置 vSphere Native Key Provider 的过程涉及以下基本操作：

- 1 具有相应管理特权的用户使用 vSphere Client 在 vCenter Server 上创建 vSphere Native Key Provider。
- 2 然后，vCenter Server 为 ESXi 主机的所有集群配置 vSphere Native Key Provider。  
在此步骤中，vCenter Server 将主密钥推送到集群中的所有 ESXi 主机。同样，如果更新或删除 vSphere Native Key Provider，更改将推送到集群中的主机。
- 3 具有相应加密特权的用户创建 vTPMs 和加密虚拟机（前提是您已购买 vSphere Enterprise+ 版本）。  
请参见第 11 章 使用虚拟可信平台模块保护虚拟机和第 10 章 在 vSphere 环境中使用加密。

## vSphere Native Key Provider 加密过程流

要了解不同组件如何交互以使用 vSphere Native Key Provider 执行加密任务，请参见 [vSphere Native Key Provider 加密过程流](#)。

## 配置 vSphere Native Key Provider

执行加密任务需要密钥提供程序。您可以使用 vSphere Client 在 vCenter Server 上配置 vSphere Native Key Provider。

vSphere 7.0 Update 2 及更高版本包含名为 vSphere Native Key Provider 的密钥提供程序。vSphere Native Key Provider 无需外部密钥服务器 (KMS)，即可启用加密相关的功能。vCenter Server 最初并未配置 vSphere Native Key Provider。因此，您必须手动配置 vSphere Native Key Provider。

ESXi 主机无需 TPM 2.0 即可使用 vSphere Native Key Provider。但是，TPM 2.0 确实会提高安全性。

**注** 配置 vSphere Native Key Provider 时，密钥提供程序在配置了它们的 vCenter Server 的所有集群上均可用。因此，连接到 vCenter Server 的所有主机均可访问您配置的所有 vSphere Native Key Provider。

#### 前提条件

所需特权：[加密操作](#)、[管理密钥服务器](#)

#### 步骤

- 1 使用 vSphere Client 登录到 vCenter Server 系统。
- 2 浏览清单列表，然后选择 vCenter Server 实例。
- 3 单击**配置**，然后在**安全**下单击**密钥提供程序**。
- 4 单击**添加**，然后单击**添加本机密钥提供程序**。
- 5 输入 vSphere Native Key Provider 的名称。

每个逻辑密钥提供程序（无论其类型如何：标准、可信和本机密钥提供程序），都必须在所有 vCenter Server 系统中具有唯一的名称。

有关详细信息，请参见[密钥提供程序命名](#)。

- 6 如果希望此 vSphere Native Key Provider 仅由具有 TPM 2.0 的主机使用，请选中**仅对受 TPM 保护的 ESXi 主机使用密钥提供程序**复选框。

启用此复选框后，vSphere Native Key Provider 仅在具有 TPM 2.0 的主机上可用。

- 7 单击**添加密钥提供程序**。

**注** 数据中心内的所有集群 ESXi 主机获取密钥提供程序和 vCenter Server 更新缓存大约需要五分钟。由于信息传播的方式，您可能需要等待几分钟后，才能使用密钥提供程序在某些主机上执行密钥操作。

#### 结果

vSphere Native Key Provider 已添加，并显示在**密钥提供程序**窗格中。此时尚未备份 vSphere Native Key Provider。您必须先备份 vSphere Native Key Provider，然后才能使用它。

#### 后续步骤

请参见[备份 vSphere Native Key Provider](#)。

## 备份 vSphere Native Key Provider

为了应对必须还原密钥提供程序配置的情景，必须备份 vSphere Native Key Provider，这是灾难恢复方案的一部分。您可以使用 vSphere Client、PowerCLI 或 API 备份 vSphere Native Key Provider。

vSphere Native Key Provider 在基于 vCenter Server 文件的备份过程中进行备份。但是，您必须至少先备份 vSphere Native Key Provider 一次，然后才能使用它。创建 vSphere Native Key Provider 时，不会对其进行备份。

为了应对必须还原配置的情况，需要进行备份。要还原 vSphere Native Key Provider，请参见[使用 vSphere Client 还原 vSphere Native Key Provider](#)。

将备份文件保持在一个安全的位置。您可以在创建备份时对备份进行密码保护。备份文件采用 PKCS#12 格式。

如果尚未备份 vSphere Native Key Provider，vCenter Server 将创建警报。您可以确认该警报，但警报每 24 小时便会重新显示一次，直到您备份 vSphere Native Key Provider 为止。

### 前提条件

所需特权：[加密操作.管理密钥服务器](#)

---

**注** 在增强型链路模式配置中，您必须在密钥提供程序所属的 vCenter Server 上执行备份。

---

### 步骤

- 1 使用 vSphere Client 登录到 vCenter Server 系统。
- 2 浏览清单列表，然后选择 vCenter Server 实例。
- 3 单击**配置**，然后在**安全**下单击**密钥提供程序**。
- 4 选择要备份的 vSphere Native Key Provider。  
对于尚未备份的密钥提供程序，将显示“未备份”状态。
- 5 单击**备份**。
- 6 要对备份进行密码保护，请选中**使用密码保护 Native Key Provider 数据**复选框。
  - a 输入密码并将其保存在一个安全的位置。
  - b 选中**我已将密码保存到一个安全的位置**复选框，表明已将密码保存到安全位置。
- 7 单击**备份密钥提供程序**。  
备份文件采用 PKCS#12 格式。
- 8 将备份文件保存在一个安全的位置。

### 结果

vSphere Native Key Provider 的状态从“未备份”变为“警告”，再变为“活动”。“警告”表示 vCenter Server 仍在向数据中心内的所有 ESXi 主机推送信息。“活动”表示信息已推送到所有主机。

## 后续步骤

要向您的 ESXi 主机添加 vTPM，请参见第 11 章 [使用虚拟可信平台模块保护虚拟机](#)。要加密虚拟机，请参见第 10 章 [在 vSphere 环境中使用加密](#)。

# 在增强型链接模式配置中导入 vSphere Native Key Provider

在增强型链接模式配置中的一个 vCenter Server 上创建 vSphere Native Key Provider 后，可以使用 vSphere Client 将其导入到配置中的另一个 vCenter Server。

可以配置一个 vSphere Native Key Provider，并使其可在增强型链接模式下配置的 vCenter Server 系统之间共享。可以在增强型链接模式配置中的一个 vCenter Server 系统上创建 vSphere Native Key Provider，然后使用[还原](#)功能将加密密钥文件导入到其他 ELM 连接的 vCenter Server 系统。

## 前提条件

- 所需特权：[加密操作.管理密钥服务器](#)
- 在增强型链接模式配置中的一个 vCenter Server 系统上创建 vSphere Native Key Provider。请参见[配置 vSphere Native Key Provider](#)。
- 备份 vSphere Native Key Provider 并下载备份加密密钥文件。请参见[备份 vSphere Native Key Provider](#)。将备份加密密钥文件放置在导入时可以访问的安全位置。

## 步骤

- 1 使用 vSphere Client，登录到增强型链接模式配置中要导入 vSphere Native Key Provider 的一个 vCenter Server。
- 2 浏览清单列表，然后选择 vCenter Server 实例。
- 3 单击[配置](#)，然后在[安全](#)下单击[密钥提供程序](#)。
- 4 单击[还原](#)。
- 5 浏览到存储 vSphere Native Key Provider 备份加密密钥文件的文件位置。  
文件已保存为 PKCS#12 格式。
- 6 选择文件。
- 7 （可选）如果该文件受密码保护，请输入密码。
- 8 单击[下一步](#)。
- 9 （可选）如果决定仅在受 TPM 保护的 ESXi 主机中使用此密钥提供程序，请选中该复选框。
- 10 单击[完成](#)。

## 结果

vSphere Native Key Provider 导入到 vCenter Server。要使用 vSphere Native Key Provider 执行加密任务，请确保先在[密钥提供程序](#)窗格中选择它，然后单击[设置为默认值](#)。

## 后续步骤

对增强型链接模式配置中要添加 vSphere Native Key Provider 的其他 vCenter Server 系统重复这些步骤。

## 恢复 vSphere Native Key Provider

您可以通过 vSphere Client 或从 vCenter Server Appliance 备份恢复 vSphere Native Key Provider。

必要时，您可以按照以下方式恢复 vSphere Native Key Provider。

- 1 如果不需要重新构建 vCenter Server Appliance，请使用 vSphere Client 还原密钥提供程序。请参见 [使用 vSphere Client 还原 vSphere Native Key Provider](#)。
- 2 如果必须重新构建 vCenter Server Appliance，则必须从 vCenter Server Appliance 备份还原密钥提供程序。执行 vCenter Server Appliance 备份时，它会保存本机密钥提供程序。有关从备份还原 vCenter Server Appliance 的信息，请参见 <https://blogs.vmware.com/vsphere/2018/05/vcenter-server-appliance-6-7-file-based-backup-and-restore-walkthroughs.html>。

## 使用 vSphere Client 还原 vSphere Native Key Provider

您可以使用 vSphere Client 还原 vSphere Native Key Provider。

您可以还原本机密钥提供程序，以防它被意外删除或必须执行灾难恢复。

还原 vSphere Native Key Provider 时，无需再次备份密钥提供程序。初始备份就够用了。继续将备份文件维护在一个安全的位置。

### 前提条件

- 所需特权：**加密操作.管理密钥服务器**
- 密钥提供程序备份文件。
- 密钥提供程序文件的密码（如果您在备份密钥提供程序时输入了密码）。

### 步骤

- 1 使用 vSphere Client 登录到 vCenter Server 系统。
- 2 浏览清单列表，然后选择 vCenter Server 实例。
- 3 单击**配置**，然后在**安全**下单击**密钥提供程序**。
- 4 选择 vSphere Native Key Provider，然后单击**还原**。
- 5 浏览到文件位置，然后选择备份的加密密钥文件。  
文件已保存为 PKCS#12 格式。
- 6 （可选）如果该文件受密码保护，请输入密码。
- 7 单击**下一步**。
- 8 （可选）如果决定仅在受 TPM 保护的 ESXi 主机中使用此密钥提供程序，请选中该复选框。



9 单击**完成**。

## 结果

vSphere Native Key Provider 已还原。

# 更新 vSphere Native Key Provider

作为定期密钥轮换计划的一部分，可以使用 PowerCLI 更新 vSphere Native Key Provider。

如果您有密钥轮换策略，则可以更新 vSphere Native Key Provider，并为使用该密钥提供程序加密的虚拟机重新加密。必须使用 PowerCLI 更新 vSphere Native Key Provider。此外，也可以在不更新密钥提供程序的情况下重新加密已经加密的虚拟机。在这种情况下，仅更改虚拟机密钥。要为虚拟机重新加密，请参见 [使用 vSphere Client 对加密虚拟机进行重新加密](#)。

## 前提条件

- 所需特权：**加密操作.管理密钥服务器**
- PowerCLI 12.3.0

## 步骤

- 1 在 PowerCLI 会话中，运行 `Connect-VIServer cmdlet`，以管理员用户身份连接到配置了要更新的 vSphere Native Key Provider 的 vCenter Server。

```
Connect-VIServer -server VC_ip_address -User admin_user -Password 'password'
```

- 2 要获取 vSphere Native Key Provider 名称，请使用可选的 `Get-KeyProvider` 参数运行 `Type` cmdlet。

```
Get-KeyProvider -Type NativeKeyProvider
```

- 3 要更新密钥提供程序，请在指定密钥提供程序名称和 GUID 的情况下运行 `Set-KeyProvider` cmdlet。

可以通过运行 `New-Guid cmdlet` 生成要使用的 GUID。

```
Set-KeyProvider -KeyProvider KeyProvider_name -KeyId Guid
```

此时将显示有关备份配置的警告。

- 4 要备份密钥提供程序，请运行 `Export-KeyProvider` cmdlet。

```
Export-KeyProvider -KeyProvider KeyProvider_name -FilePath path_file_name
```

还可以使用 vSphere Client 备份密钥提供程序。请参见[备份 vSphere Native Key Provider](#)。

## 结果

更新密钥提供程序后，其状态将更改为“未备份”。备份密钥提供程序后，其状态将更改为“活动”。



## 删除 vSphere Native Key Provider

您可以使用 vSphere Client 从 vCenter Server 中删除 vSphere Native Key Provider。

删除 vSphere Native Key Provider 后，具有 vTPM 或加密的虚拟机会继续运行。如果重新引导 ESXi 主机，它的加密虚拟机将进入锁定状态。取消注册这些虚拟机后，它们将在您尝试重新注册它们时进入锁定状态。解锁虚拟机的唯一方法就是还原先前的 vSphere Native Key Provider。

### 前提条件

所需特权：[加密操作.管理密钥服务器](#)

在删除 vSphere Native Key Provider 之前，请将通过该密钥提供程序加密的任何加密虚拟机和数据存储重新加密到另一个密钥提供程序。请参见[使用 vSphere Client 对加密虚拟机进行重新加密](#)。

此外，保留 vSphere Native Key Provider 的备份，以防在删除密钥提供程序后必须重新加密已加密的虚拟机。

### 步骤

- 1 使用 vSphere Client 登录到 vCenter Server 系统。
- 2 浏览清单列表，然后选择 vCenter Server 实例。
- 3 单击**配置**，然后在**安全**下单击**密钥提供程序**。
- 4 选择要删除的密钥提供程序。
- 5 单击**删除**。
- 6 阅读警告消息，将滑块滑动到右侧。
- 7 单击**删除**。

### 结果

vSphere Native Key Provider 从 vCenter Server 中移除。

# vSphere Trust Authority

# 9

在 vSphere 7.0 及更高版本中，可以利用 VMware® vSphere Trust Authority™。vSphere Trust Authority 是增强工作负载安全性的基础技术。vSphere Trust Authority 可将 ESXi 主机的硬件信任根与工作负载本身相关联，从而在您的组织中建立更高的信任级别。

本章讨论了以下主题：

- [vSphere Trust Authority 概念和功能](#)
- [配置 vSphere Trust Authority](#)
- [管理 vSphere 环境中的 vSphere Trust Authority](#)

## vSphere Trust Authority 概念和功能

vSphere Trust Authority 可将可信计算基础的可信赖度扩展到组织的整个计算基础架构，从而保护 SDDC 免受恶意攻击。vSphere Trust Authority 使用远程证明和受控访问高级加密功能。

vSphere Trust Authority 是一组满足高安全性要求的服务。通过 vSphere Trust Authority，可以设置和维护一个安全基础架构。可以确保敏感工作负载仅在已证明安装有真实引导软件的 ESXi 主机上运行。

## vSphere Trust Authority 如何保护您的环境

可以配置 vSphere Trust Authority 服务以证明您的 ESXi 主机，然后这些主机能够执行受信任的加密操作。

vSphere Trust Authority 对 ESXi 主机使用远程证明，以证明其引导软件的真实性和完整性。证明会验证 ESXi 主机是否运行的是真实的 VMware 软件或 VMware 签名的合作伙伴软件。证明依赖植根于 ESXi 主机中安装的可信平台模块 (TPM) 2.0 芯片的衡量指标。在 vSphere Trust Authority 中，ESXi 只有在经过证明后，才能访问加密密钥并执行加密操作。

## vSphere Trust Authority 术语表

vSphere Trust Authority 引入了一些必须了解的特定术语和定义。

表 9-1. vSphere Trust Authority 术语表

术语	定义
VMware vSphere® Trust Authority™	指定一组启用可信基础架构的服务。负责确保 ESXi 主机运行的是可信软件，并负责仅将加密密钥发布到受信任的 ESXi 主机。
vSphere Trust Authority 组件	vSphere Trust Authority 组件包括： <ul style="list-style-type: none"> <li>■ 证明服务</li> <li>■ 密钥提供程序服务</li> </ul>
证明服务	证明远程 ESXi 主机的状态。使用 TPM 2.0 建立硬件信任根，并根据管理员批准的 ESXi 版本列表验证软件衡量指标。
密钥提供程序服务	封装一个或多个密钥服务器，并公开可在加密虚拟机时指定的可信密钥提供程序。目前，密钥服务器仅限于使用 KMIP 协议。
可信基础架构	可信基础架构包括： <ul style="list-style-type: none"> <li>■ Trust Authority vCenter Server</li> <li>■ 工作负载 vCenter Server</li> <li>■ 至少一个 vSphere Trust Authority 集群（配置为 Trust Authority vCenter Server 的一部分）</li> <li>■ 至少一个受信任集群（配置为工作负载 vCenter Server 的一部分）</li> <li>■ 受信任集群中运行的加密工作负载虚拟机</li> <li>■ 至少一个符合 KMIP 的密钥管理服务器</li> </ul> <p><b>注</b> 必须对 Trust Authority 集群和受信任集群使用单独的 vCenter Server 系统。</p>
Trust Authority 集群	包括运行 vSphere Trust Authority 组件（证明服务和密钥提供程序服务）的 ESXi 主机的 vCenter Server 集群。
Trust Authority 主机	运行 vSphere Trust Authority 组件（证明服务和密钥提供程序服务）的 ESXi 主机。
受信任集群	包括由 Trust Authority 集群远程证明的受信任 ESXi 主机的 vCenter Server 集群。尽管未严格要求，但配置的密钥提供程序服务确实大大提升了受信任集群提供的价值。
受信任主机	其软件已经 Trust Authority 集群证明服务验证的 ESXi 主机。此主机运行的工作负载虚拟机可以使用由 Trust Authority 集群密钥提供程序服务发布的密钥提供程序进行加密。
vSphere 虚拟机加密	利用 vSphere 虚拟机加密功能，可以创建加密虚拟机并加密现有虚拟机。vSphere 6.5 中引入了 vSphere 虚拟机加密。关于密钥提供程序处理加密密钥的方式上的差异，请参见 <a href="#">vSphere 加密密钥和密钥提供程序</a> 。
可信密钥提供程序	在密钥服务器上封装单个加密密钥的密钥提供程序。访问加密密钥需要证明服务确认已在受信任主机上验证 ESXi 软件。
标准密钥提供程序	直接从密钥服务器获取加密密钥并将密钥分发给数据中心内所需主机的密钥提供程序。之前在 vSphere 中称为 KMS 集群。
密钥服务器	与密钥提供程序关联的 KMIP 密钥管理服务器 (KMS)。
工作负载 vCenter Server	管理并用于配置一个或多个受信任集群的 vCenter Server。

## vSphere Trust Authority 基础知识

利用 vSphere Trust Authority，您可以：

- 提供具有硬件信任根和远程证明功能的 ESXi 主机

- 通过仅将密钥发布到经过证明的 ESXi 主机来限制加密密钥管理
- 创建更安全的管理环境以管理信任
- 集中管理多个密钥服务器
- 继续在虚拟机上执行加密操作，但增强了加密密钥管理级别

在 vSphere 6.5 和 6.7 中，虚拟机加密依赖 vCenter Server 从密钥服务器获取加密密钥，然后根据需要 将密钥推送到 ESXi 主机。vCenter Server 使用客户端证书和服务器证书对密钥服务器进行身份验证，这些证书存储在 VMware 端点证书存储 (VECS) 中。从密钥服务器发出的加密密钥通过 vCenter Server 内存传递到所需的 ESXi 主机（使用 TLS 通过线路提供数据加密）。此外，vSphere 还依赖 vCenter Server 中的特权检查验证用户权限并强制执行密钥服务器访问限制。尽管这种架构很安全，但并未解决 vCenter Server 受到破坏、恶意 vCenter Server 管理员的潜在问题，或者可能会导致密钥泄漏或被盗的管理或配置错误。

从 vSphere 7.0 开始，vSphere Trust Authority 解决了这些问题。可以创建一个可信计算基础，它由一组安全、可管理的 ESXi 主机组成。vSphere Trust Authority 对要信任的 ESXi 主机实施远程证明服务。此外，vSphere Trust Authority 还改进了 TPM 2.0 证明支持（从 6.7 版本开始添加到 vSphere），可对加密密钥实施访问限制，从而更好地保护虚拟机工作负载密钥。另外，vSphere Trust Authority 仅允许经授权的 Trust Authority 管理员配置 vSphere Trust Authority 服务和配置 Trust Authority 主机。Trust Authority 管理员可以与 vSphere 管理员用户是同一个用户，也可以是单独的用户。

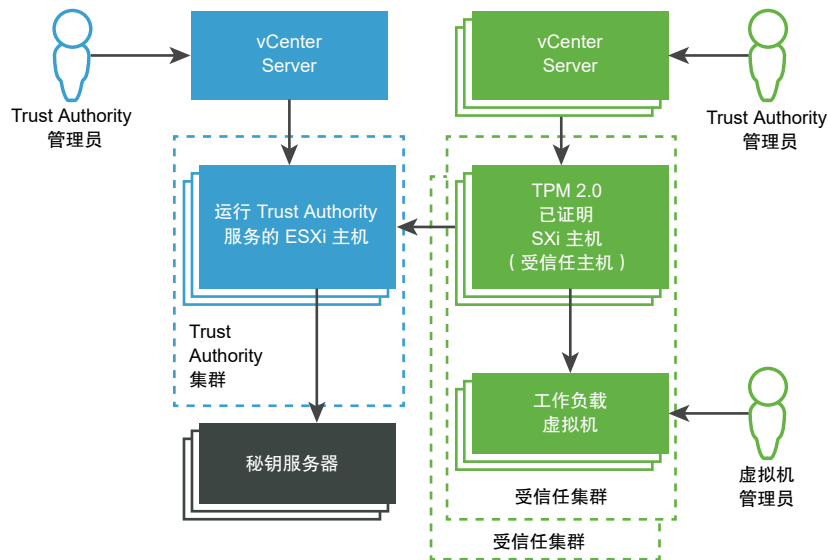
最后，vSphere Trust Authority 支持执行以下操作，从而使您能够在更安全的环境中运行工作负载：

- 检测篡改
- 禁止未经授权的更改
- 防止恶意软件和修改
- 将敏感工作负载限制为仅在经过验证的安全硬件和软件堆栈上运行

## vSphere Trust Authority 架构

下图显示了 vSphere Trust Authority 架构的简化视图。

图 9-1. vSphere Trust Authority 架构



在此图中：

#### 1 vCenter Server 系统

单独的 vCenter Server 系统管理 Trust Authority 集群和受信任集群。

#### 2 Trust Authority 集群

包括运行 vSphere Trust Authority 组件的 ESXi 主机。

#### 3 密钥服务器

存储执行加密操作时密钥提供程序服务使用的加密密钥。密钥服务器位于 vSphere Trust Authority 外部。

#### 4 受信任集群

包括已使用 TPM 远程证明并运行加密工作负载的 ESXi 受信任主机。

#### 5 Trust Authority 管理员

属于 vCenter Server TrustedAdmins 组成员并负责配置可信基础架构的管理员。

vSphere Trust Authority 在 Trust Authority 管理员指定方式上实现了灵活性。图中的 Trust Authority 管理员可以是单独的用户。此外，Trust Authority 管理员也可以是同一个用户，使用的凭据跨 vCenter Server 系统链接。在此情况下，为同一个用户和同一个 TrustedAdmins 组。

#### 6 虚拟机管理员

已授予管理受信任主机上加密工作负载虚拟机特权的管理员。

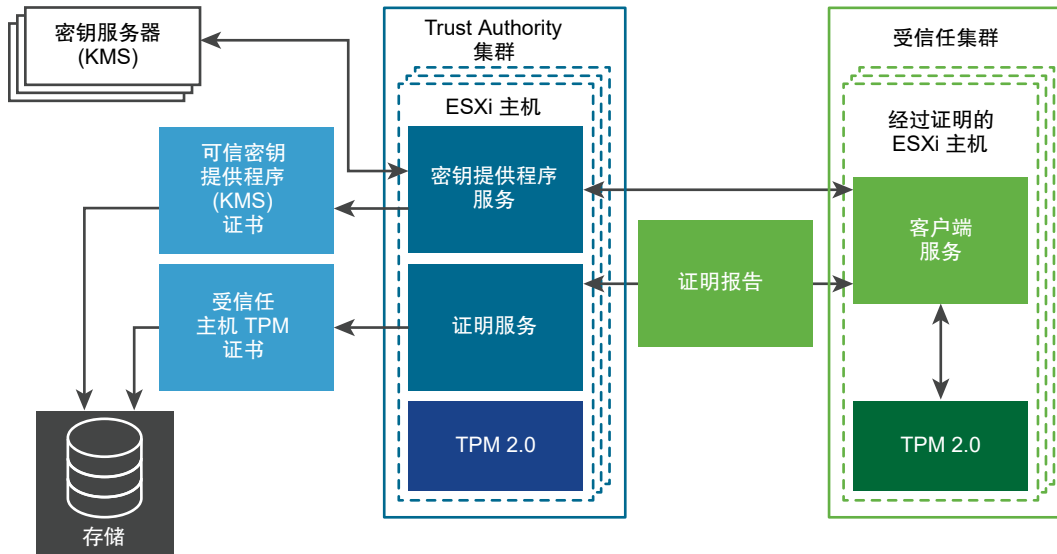
## 可信基础架构概述

可信基础架构包括 vSphere Trust Authority 服务、至少一个符合 KMIP 的外部密钥服务器、vCenter Server 系统和 ESXi 主机。

### 什么是可信基础架构

可信基础架构包含至少一个 vSphere Trust Authority 集群、至少一个受信任集群以及至少一个符合 KMIP 的外部密钥服务器。每个集群都包含运行特定 vSphere Trust Authority 服务的 ESXi 主机，如下图所示。

图 9-2. vSphere Trust Authority 服务



配置 Trust Authority 集群会启用两种服务：

- 证明服务
- 密钥提供程序服务

配置 vSphere Trust Authority 时，受信任集群中的 ESXi 主机将与证明服务进行通信。密钥提供程序服务介于受信任主机与一个或多个可信密钥提供程序之间。

**注** 目前，Trust Authority 集群中的 ESXi 主机不需要 TPM。但是，作为最佳做法，请考虑安装配有 TPM 的新 ESXi 主机。

### 什么是 vSphere Trust Authority 证明服务

证明服务会生成一个签名文档，其中包含描述受信任集群中远程 ESXi 主机的二进制文件和配置状态的断言。证明服务使用可信平台模块 (TPM) 2.0 芯片作为软件衡量和报告的基础来证明 ESXi 主机的状态。远程 ESXi 主机上的 TPM 衡量软件堆栈，并将配置数据发送到证明服务。证明服务验证软件衡量签名是否可以归因于以前配置的可信 TPM 认可密钥 (EK)。证明服务还确保软件衡量指标与一组以前保存的 ESXi 映像中的一个相匹配。证明服务对向 ESXi 主机发出的 JSON Web 令牌 (JWT) 进行签名，从而提供有关 ESXi 主机的标识、有效性和配置的断言。

## 什么是 vSphere Trust Authority 密钥提供程序服务

利用密钥提供程序服务，vCenter Server 和 ESXi 主机不再需要直接密钥服务器凭据。在 vSphere Trust Authority 中，要使 ESXi 主机能够访问加密密钥，必须使用密钥提供程序服务进行身份验证。

要使密钥提供程序服务连接到密钥服务器，Trust Authority 管理员必须配置信任设置。对于大多数符合 KMIP 的服务器，配置信任设置包含配置客户端证书和服务器证书。

要确保仅将密钥发布到 ESXi 受信任主机，密钥提供程序服务将充当密钥服务器的网关守卫。密钥提供程序服务使用可信密钥提供程序的概念，对数据中心软件堆栈的其余部分隐藏密钥服务器详细信息。每个可信密钥提供程序具有一个配置的主加密密钥，并引用一个或多个密钥服务器。密钥提供程序服务可以具有多个已配置的可信密钥提供程序。例如，您可能希望为组织中的每个部门提供一个单独的可信密钥提供程序。每个可信密钥提供程序使用一个不同的主要密钥，但可以引用同一个支持密钥服务器。

创建可信密钥提供程序后，密钥提供程序服务可以接受来自 ESXi 受信任主机的请求，以便对该可信密钥提供程序运行加密操作。

当 ESXi 受信任主机请求对可信密钥提供程序执行操作时，密钥提供程序服务会确保尝试获取加密密钥的 ESXi 主机已经过证明。通过所有检查后，ESXi 受信任主机从密钥提供程序服务收到加密密钥。

## vSphere Trust Authority 使用哪些端口

vSphere Trust Authority 服务侦听通过 ESXi 主机反向代理的连接。所有通信都在端口 443 上通过 HTTPS 进行。

## 什么是 vSphere Trust Authority 受信任主机

ESXi 受信任主机配置为使用可信密钥提供程序执行加密操作。ESXi 受信任主机通过与密钥提供程序服务和证明服务进行通信来执行密钥操作。对于身份验证和授权，ESXi 受信任主机使用从证明服务获取的令牌。要获取有效令牌，ESXi 受信任主机必须成功地向证明服务进行证明。令牌包含某些声明，用于确定 ESXi 受信任主机是否有权访问可信密钥提供程序。

## vSphere Trust Authority 和密钥服务器要求

vSphere Trust Authority 要求至少使用一个密钥服务器。在以前的 vSphere 版本中，密钥服务器称为密钥管理服务器或 KMS。目前，vSphere 虚拟机加密支持符合 KMIP 1.1 的密钥服务器。

## vSphere Trust Authority 如何存储配置和状态信息

vCenter Server 主要是用于 vSphere Trust Authority 配置和状态信息的直通服务。大多数 vSphere Trust Authority 配置和状态信息存储在 ESXi 主机上的 ConfigStore 数据库中。一些状态信息也存储在 vCenter Server 数据库中。

---

**注** 由于大多数 vSphere Trust Authority 配置信息存储在 ESXi 主机上，因此，vCenter Server 基于文件的备份机制不会备份这些信息。要确保保存 vSphere Trust Authority 部署的配置信息，请参见[备份 vSphere Trust Authority 配置](#)。

---

## vSphere Trust Authority 如何与 vCenter Server 集成

需要配置单独的 vCenter Server 实例来管理 Trust Authority 集群和受信任集群。请参见[配置 vSphere Trust Authority](#)。

在受信任集群上，vCenter Server 管理 Trust Authority API 调用，并将这些调用传递到 ESXi 主机。vCenter Server 会在受信任集群中的所有 ESXi 主机之间复制 API 调用。

在最初配置 vSphere Trust Authority 后，可以在 Trust Authority 集群或受信任集群中添加或移除 ESXi 主机。请参见[添加和移除 vSphere Trust Authority 主机](#)。

## vSphere Trust Authority 过程流

了解 vSphere Trust Authority 过程流对于了解如何配置和管理可信基础架构至关重要。

### 如何配置 vSphere Trust Authority

默认情况下不会激活 vSphere Trust Authority。必须在您的环境中手动配置 vSphere Trust Authority。请参见[配置 vSphere Trust Authority](#)。

配置 vSphere Trust Authority 时，必须指定证明服务接受的 ESXi 软件版本，以及可信赖的可信平台模块 (TPM)。

### TPM 和证明

本指南在讨论 TPM 和证明时使用以下定义。

表 9-2. TPM 和证明术语表

术语	定义
认可密钥 (EK)	TPM 使用内置于硬件中的 RSA 公钥/私钥对（称为认可密钥 (EK)）制造而成。EK 对于特定的 TPM 是唯一的。
EK 公钥	EK 密钥对的公钥部分。
EK 私钥	EK 密钥对的私钥部分。
EK 证书	用签名封装的 EK 公钥。EK 证书由使用其证书颁发机构私钥对 EK 公钥进行签名的 TPM 制造商创建。并非所有 TPM 都包含 EK 证书。在这种情况下，EK 公钥未签名。
TPM 证明	证明服务能够验证在远程主机上所运行的软件。TPM 证明通过 TPM 在远程主机启动时执行的加密度量完成，并根据请求中继续到证明服务。证明服务通过 EK 公钥或 EK 证书在 TPM 中建立信任。

### 在受信任主机上配置 TPM 信任

ESXi 受信任主机必须包含 TPM。TPM 使用内置于硬件中的公钥/私钥对（称为认可密钥 (EK)）制造而成。尽管 TPM 2.0 允许许多密钥/证书对，但最常用的是 RSA-2048 密钥对。当 TPM EK 公钥由 CA 签名时，会生成 EK 证书。TPM 制造商通常至少预先生成一个 EK，使用证书颁发机构对公钥进行签名，并将签名证书嵌入到 TPM 的非易失性内存中。

可以将证明服务配置为信任 TPM，如下所示：

- 信任制造商签名 TPM 所用的所有 CA 证书（EK 公钥）。证明服务的默认设置是信任 CA 证书。在此方法中，同一 CA 证书涵盖许多 ESXi 主机，因此减少了管理开销。



- 信任 ESXi 主机的 TPM CA 证书和 EK 公钥。后者可以是 EK 证书或 EK 公钥。尽管此方法提供更高的安全性，但要求配置每个受信任主机的相关信息。
- 某些 TPM 不包含 EK 证书。在这种情况下，信任 EK 公钥。

决定信任所有 TPM CA 证书在操作上方便实现。仅当向数据中心添加新型硬件时，才需要配置新证书。通过信任单个 EK 证书，可以限制对特定 ESXi 主机的访问。

也可以决定不信任 TPM CA 证书。尽管这种情况并不常见，但 EK 未由 CA 签名时可以使用此配置。目前，此功能未完全实现。

---

**注** 某些 TPM 不包含 EK 证书。如果要信任单个 ESXi 主机，TPM 必须包含一个 EK 证书。

---

## 证明 TPM

要开始证明过程，受信任集群中的 ESXi 受信任主机将预配置的 EK 公钥和 EK 证书发送到 Trust Authority 集群上的证明服务。当证明服务收到请求时，将查找其配置中的 EK，EK 可以是 EK 公钥或 EK 证书，也可以是这两者，具体取决于配置。如果任何情况都无效，则证明服务将拒绝证明请求。

EK 不直接用于签名，因此会协商证明密钥（AK 或 AIK）。协商协议可确保将新创建的 AK 绑定到之前验证的 EK，从而防止出现中间人或冒充者的情况。协商 AK 后，将在未来的证明请求中重用，而不是每次生成一个新 AK。

ESXi 受信任主机从 TPM 读取引用和 PCR 值。引用由 AK 签名。ESXi 受信任主机还会读取 TCG 事件日志，其中包括导致当前 PCR 状态的所有事件。此 TPM 信息将发送到证明服务进行验证。证明服务使用事件日志验证 PCR 值。

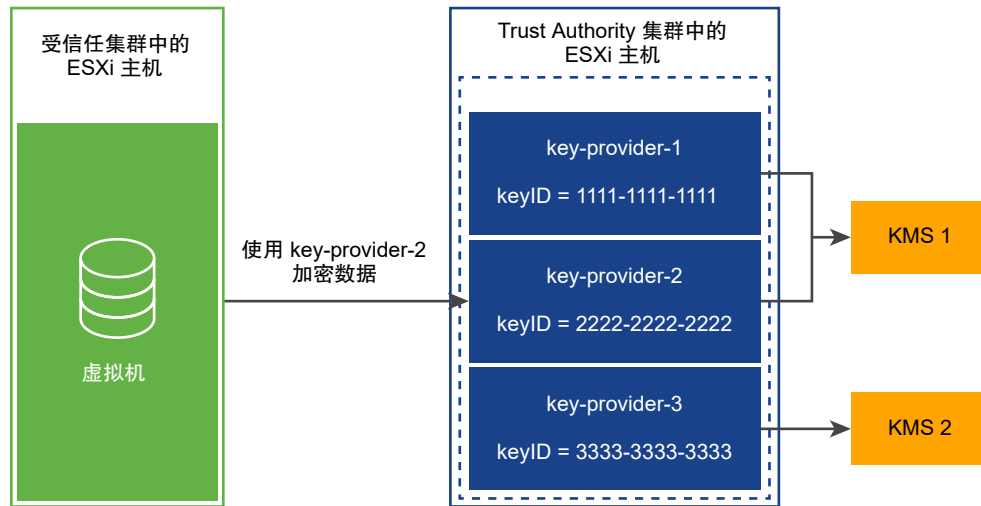
## 密钥提供程序如何与密钥服务器配合使用

密钥提供程序服务使用可信密钥提供程序的概念，对其余数据中心软件隐藏密钥服务器的详细信息。每个可信密钥提供程序具有一个配置的主加密密钥，并引用一个或多个密钥服务器。主要加密密钥存在于密钥服务器中。在配置 vSphere Trust Authority 的过程中，必须将主密钥置备为单独的活动并将其激活。密钥提供程序服务可以具有多个已配置的可信密钥提供程序。每个可信密钥提供程序使用一个不同的主要密钥，但可以引用同一个支持密钥服务器。

添加新的可信密钥提供程序时，Trust Authority 管理员必须指定密钥服务器和该密钥服务器上的现有密钥标识符。

下图显示了密钥提供程序服务与密钥服务器之间的关系。

图 9-3. 密钥提供程序和密钥服务器



为受信任集群配置可信密钥提供程序后，密钥提供程序服务可以接受对该可信密钥提供程序运行加密操作的请求。例如，在此图中，配置了三个可信密钥提供程序，两个用于 KMS-1，一个用于 KMS-2。受信任主机针对 key-provider-2 发出加密操作请求。受信任主机请求生成并返回加密密钥，并使用此加密密钥执行加密操作。

密钥提供程序服务使用 key-provider-2 引用的主要密钥对指定的纯文本数据进行加密并返回相应的密码文本。稍后，受信任主机可以为解密操作提供相同的密码文本，并恢复原始纯文本。

## vSphere Trust Authority 身份验证和授权

vSphere Trust Authority 管理操作要求用户是 TrustedAdmins 组的成员。仅具有 Trust Authority 管理员特权不足以执行涉及 ESXi 主机的所有管理操作。有关详细信息，请参见 [vSphere Trust Authority 的必备条件和所需特权](#)。

## 将受信任主机添加到受信任集群

有关最初将 ESXi 主机添加到受信任集群的步骤，请参见[配置 vSphere Trust Authority](#)。

稍后，如果要将 ESXi 主机添加到受信任集群，工作流会有所不同。请参见[添加和移除 vSphere Trust Authority 主机](#)。

最初将 ESXi 主机添加到受信任集群时，必须收集以下信息：

- 集群中每种硬件的 TPM 证书
- 集群中每个 ESXi 版本的 ESXi 映像
- vCenter Server 主体信息

如果稍后将 ESXi 主机添加到受信任集群，可能需要收集一些其他信息。也就是说，如果新 ESXi 主机的硬件或 ESXi 版本与原始主机不同，则必须收集新的 ESXi 主机信息并将其导入到 Trust Authority 集群中。每个 vCenter Server 系统只需收集一次 vCenter Server 主体信息。

## vSphere Trust Authority 拓扑

vSphere Trust Authority 要求对 Trust Authority 集群和受信任集群使用单独的 vCenter Server 系统。

Trust Authority 集群在独立、隔离的 vCenter Server 上进行配置和管理。Trust Authority 集群的 vCenter Server 也不能是受信任集群的 vCenter Server。受信任集群必须具有自己的单独 vCenter Server。单个 vCenter Server 可以管理多个受信任集群。受信任集群的多个 vCenter Server 系统可以加入增强型链接模式。Trust Authority 集群的 vCenter Server 不能与其他 Trust Authority 集群 vCenter Server 系统或受信任集群 vCenter Server 系统一起加入增强型链接模式。

Trust Authority 管理员独立于其他 vCenter Server 实例管理 Trust Authority 集群及其关联的 vCenter Server，因为这种方法提供最佳安全隔离。

Trust Authority 管理员记录或发布受信任集群管理员用于配置其集群的主机名和 SSL 证书。Trust Authority 管理员还为组织及其部门，甚至管理员个人置备可信密钥提供程序。

无法直接在由工作负载 vCenter Server 管理的受信任集群上部署 vSphere Trust Authority 服务，因为工作负载管理员对 ESXi 主机具有高特权访问权限。此类型的部署不能实现满足 vSphere Trust Authority 安全目标所要求的必要角色隔离。

## vSphere Trust Authority 的必备条件和所需特权

配置 vSphere Trust Authority 时，必须考虑硬件和软件要求。必须设置加密特权和角色才能使用加密。执行 vSphere Trust Authority 任务的用户必须拥有相应的特权。

### vSphere Trust Authority 的要求

要使用 vSphere Trust Authority，您的 vSphere 环境必须满足以下要求：

- ESXi 受信任主机的硬件要求：
  - TPM 2.0
  - 必须启用安全引导
  - EFI 固件
- 组件要求：
  - vCenter Server 7.0 或更高版本
  - 一个专用 vCenter Server 系统用于 vSphere Trust Authority 集群和 ESXi 主机
  - 一个单独的 vCenter Server 系统用于受信任集群和 ESXi 受信任主机
  - 密钥服务器（在以前的 vSphere 版本中，称为密钥管理服务器或 KMS）
- 虚拟机要求：
  - EFI 固件
  - 已启用安全引导

---

**注** 在开始配置 vSphere Trust Authority 之前，请确保已为 Trust Authority 集群和受信任集群设置了 vCenter Server 系统，并将 ESXi 主机添加到了每个集群。

---

## vSphere Trust Authority 和加密特权

vSphere Trust Authority 不会引入任何新的加密特权。[使用加密特权和角色](#)中所述的相同加密特权适用于 vSphere Trust Authority。

## vSphere Trust Authority 和主机加密模式

vSphere Trust Authority 不会引入在 ESXi 受信任主机上启用主机加密模式的任何新要求。有关主机加密模式的详细信息，请参见[虚拟机加密任务的必备条件和必需特权](#)。

## 使用 vSphere Trust Authority 角色和 TrustedAdmins 组

vSphere Trust Authority 操作要求用户是 TrustedAdmins 组的成员。此用户称为 Trust Authority 管理员。vSphere 管理员必须将自己添加到 TrustedAdmins 组，或者将其他用户添加到该组，才能获得可信基础架构管理员角色。可信基础架构管理员角色是 vCenter Server 授权的必要条件。要在属于可信基础架构的 ESXi 主机上进行身份验证，TrustedAdmins 组是必需的。具有 ESXi 主机的[加密操作.注册主机](#)特权的用户可以管理受信任集群。vCenter Server 权限不会传播到 Trust Authority 主机，只会传播到受信任主机。Trust Authority 主机上的特权只能授予 TrustedAdmins 组的成员。组成员资格在 ESXi 主机本身上进行验证。

---

**注** vSphere 管理员和管理员组中的成员会分配有可信基础架构管理员角色，但此角色本身不允许用户执行 vSphere Trust Authority 操作。还要求具备 TrustedAdmins 组中的成员资格。

---

启用 vSphere Trust Authority 后，Trust Authority 管理员可以将可信密钥提供程序分配给受信任主机。然后，这些受信任主机可以使用可信密钥提供程序执行加密任务。

除了可信基础架构管理员角色外，vSphere Trust Authority 还提供无可信基础架构管理员角色，该角色包含 vCenter Server 中除调用 vSphere Trust Authority API 的特权之外的所有特权。

vSphere Trust Authority 组、角色和用户按如下方式运作：

- 首次引导时，vSphere 授予 TrustedAdmins 组具有全局权限的可信基础架构管理员角色。
- 可信基础架构管理员角色是一个系统角色，具有调用 vSphere Trust Authority API (`TrustedAdmin.*`) 所需的特权以及用于查看清单对象的系统特权 **System.Read**、**System.View** 和 **System.Anonymous**。
- 无可信基础架构管理员角色是一个系统角色，包含 vCenter Server 中除调用 vSphere Trust Authority API 的特权之外的所有特权。将新特权添加到 vCenter Server 也会将这些特权添加到无可信基础架构管理员角色。（无可信基础架构管理员角色类似于无加密管理员角色。）
- vSphere Trust Authority 特权 (`TrustedAdmin.*` API) 不包括在无加密管理员角色中，从而可阻止具有此角色的用户设置可信基础架构或执行加密操作。

下表显示了这些用户、组和角色的用例。

表 9-3. vSphere Trust Authority 用户、组和角色

用户、组或角色	是否可以调用 vSphere Trust Authority vCenter Server API (包括对 vSphere Trust Authority ESXi API 的调用)	是否可以调用 vSphere Trust Authority vCenter Server API (不包括对 vSphere Trust Authority ESXi API 的调用)	是否可以在与 vSphere Trust Authority 无关的集群中执行主机操作	备注
Administrators@system.domain 组和 TrustedAdmins@system.domain 组中的用户	是	是	是	不适用
仅 TrustedAdmins@system.domain 组中的用户	是	是	否	此类用户无法执行常规的集群管理操作。
仅 Administrators@system.domain 组中的用户	是	否	是	不适用
具有可信基础架构管理员角色但不属于 TrustedAdmins@system.domain 组的用户	是	否	否	ESXi 主机检查用户的组成员资格以授予权限。
仅具有无可信基础架构管理员角色的用户	否	否	是	此类用户与无法执行 vSphere Trust Authority 操作的管理员类似。

## vSphere Trust Authority 最佳做法、局限性和互操作性

鉴于 vSphere Trust Authority 架构的特点，我们额外提出一些建议。在计划 vSphere Trust Authority 策略时，请注意互操作性方面的限制。

### 可信基础架构互操作性

对于 ESXi 版本，证明服务向后和向前兼容。例如，您可以在 vSphere Trust Authority 集群中具有运行 ESXi 7.0 的 ESXi 主机集群，而将受信任集群中的 ESXi 主机升级或修补到较新的 ESXi 版本。同样，可以升级或修补 Trust Authority 集群中的 ESXi 主机，而将受信任集群的 ESXi 主机保留为当前版本。

无法将集群功能同时设置为 Trust Authority 集群和受信任集群。此配置不受支持。

### 受信任集群配置限制

只能为每个工作负载 vCenter Server 配置一个受信任集群。不能将一个受信任集群配置为引用多个 Trust Authority 集群。

## 支持的功能

vSphere Trust Authority 支持以下组件：

- vCenter High Availability (vCenter HA)
- VMware vSphere High Availability
- DRS
- DPM
- SRM，但需注意：
  - 如果恢复端提供相同的 vSphere Trust Authority 服务配置，则支持具有基于阵列的复制的 SRM。
  - SPPG
- VADP
  - 支持与标准加密相同。支持热添加和 NFC 模式，但不支持 SAN 模式。备份已解密。VADP 合作伙伴可以选择使用与原始虚拟机相同的加密密钥恢复备份的虚拟机。
- vSAN
  - vSAN 完全支持虚拟机加密。
- OVF
  - 无法将加密虚拟机导出到 OVF。但是，在从 OVF 导入虚拟机时，可以对虚拟机进行加密。
- vVol

## 不支持的功能

当前，vSphere Trust Authority 不支持以下项：

- vSAN 加密
- 第一类磁盘 (FCD) 加密
- vSphere Replication
- 《vSphere 主机配置文件》

## vSphere Trust Authority 生命周期

vSphere Trust Authority 服务作为基础 ESXi 映像的一部分进行打包和安装。

### 启动和停止 vSphere Trust Authority 服务

在 vSphere Client 中，可以启动、停止和重新启动 ESXi 主机上运行的 vSphere Trust Authority 服务。可以在配置更改或者怀疑出现功能或性能问题时重新启动服务。要重新启动 ESXi 受信任主机上的服务，必须登录到主机本身才能重新启动服务。请参见[启动、停止和重新启动 vSphere Trust Authority 服务](#)。

## 升级和修补 vSphere Trust Authority

每次升级或修补 ESXi 受信任主机时，必须使用新的 ESXi 版本信息更新 vSphere Trust Authority 集群。实现此目的的一种方法是升级或修补测试 ESXi 主机，导出 ESXi 基础映像信息，将映像文件导入 Trust Authority 集群，然后升级或修补 ESXi 受信任主机。

### vSphere Trust Authority 升级的最佳做法

升级 vSphere Trust Authority 基础架构的最佳做法是先升级 Trust Authority vCenter Server 和 Trust Authority 主机。这样，可以最大程度地从最新的 vSphere Trust Authority 功能中获益。但是，可以对 vCenter Server 和 ESXi 主机执行单独的独立升级，以满足特定的业务要求。

一般情况下，按照以下顺序升级 vSphere Trust Authority 基础架构：

- 1 升级 Trust Authority 集群 vCenter Server。
- 2 升级 Trust Authority 主机。
- 3 升级受信任集群 vCenter Server。
- 4 升级受信任主机。

为确保顺利执行该过程，请逐步升级 Trust Authority 主机和受信任主机，一次一个。

### 对 vSphere Trust Authority 升级问题进行故障排除

如果 Trust Authority 主机升级失败，请执行以下步骤。

- 1 从受信任集群中移除 Trust Authority 主机。
- 2 恢复到以前版本的 ESXi。
- 3 按照 VMware 知识库文章 (<https://kb.vmware.com/s/article/77234>) 中所述，将 Trust Authority 主机重新添加到集群。
- 4 验证 Trust Authority 主机的配置是否与 Trust Authority 集群中的其他 Trust Authority 主机一致。请参见[检查受信任集群的运行状况](#)。

当受信任主机上的 ESXi 升级到新版本时，在使用新的 ESXi 基础映像信息更新 Trust Authority 集群之前，证明将失败。这是预期行为。修复该问题之前，无法再对虚拟机进行加密，也无法使用在升级之前加密的现有虚拟机。vSphere Client **近期任务**窗格以及 attestd.log、kmtx.log 和 vpxd.log 文件中将显示证明错误消息。

要更正该问题，请执行以下步骤。

- 1 运行 `Export-VMHostImageDb cmdlet` 以重新导出 ESXi 基础映像。请参见[收集有关要信任的 ESXi 主机和 vCenter Server 的信息](#)中的步骤 5。
- 2 运行 `New-TrustAuthorityVMHostBaseImage cmdlet`，以将新基础映像重新导入到 Trust Authority 集群的 vCenter Server。请参见[将受信任主机信息导入到 Trust Authority 集群](#)中的步骤 8。



- 3 如果不再必须证明旧版本的 ESXi（已升级所有受信任主机），请运行 `Remove-TrustAuthorityVMHostBaseImage` cmdlet 以移除这些版本。例如：

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
$baseImages = Get-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
Remove-TrustAuthorityVMHostBaseImage -VMHostBaseImage $baseImages
```

## 备份 vSphere Trust Authority 配置

由于大多数 vSphere Trust Authority 配置信息存储在 ESXi 主机上，因此 vCenter Server 备份不会备份此 vSphere Trust Authority 信息。请参见[备份 vSphere Trust Authority 配置](#)。

## 配置 vSphere Trust Authority

默认情况下，不启用 vSphere Trust Authority。必须在环境中配置 vSphere Trust Authority，然后才能开始使用。

在称为 vSphere Trust Authority 集群的专用 vCenter Server 集群上启用 vSphere Trust Authority 服务。Trust Authority 集群用作集中式安全管理平台。然后，使工作负载 vCenter Server 集群用作受信任集群。受信任集群包含 ESXi 受信任主机。

Trust Authority 集群会远程证明受信任集群中的 ESXi 主机。Trust Authority 集群仅将加密密钥释放给受信任集群中经过证明的 ESXi 主机，以便使用可信密钥提供程序对虚拟机和虚拟磁盘进行加密。

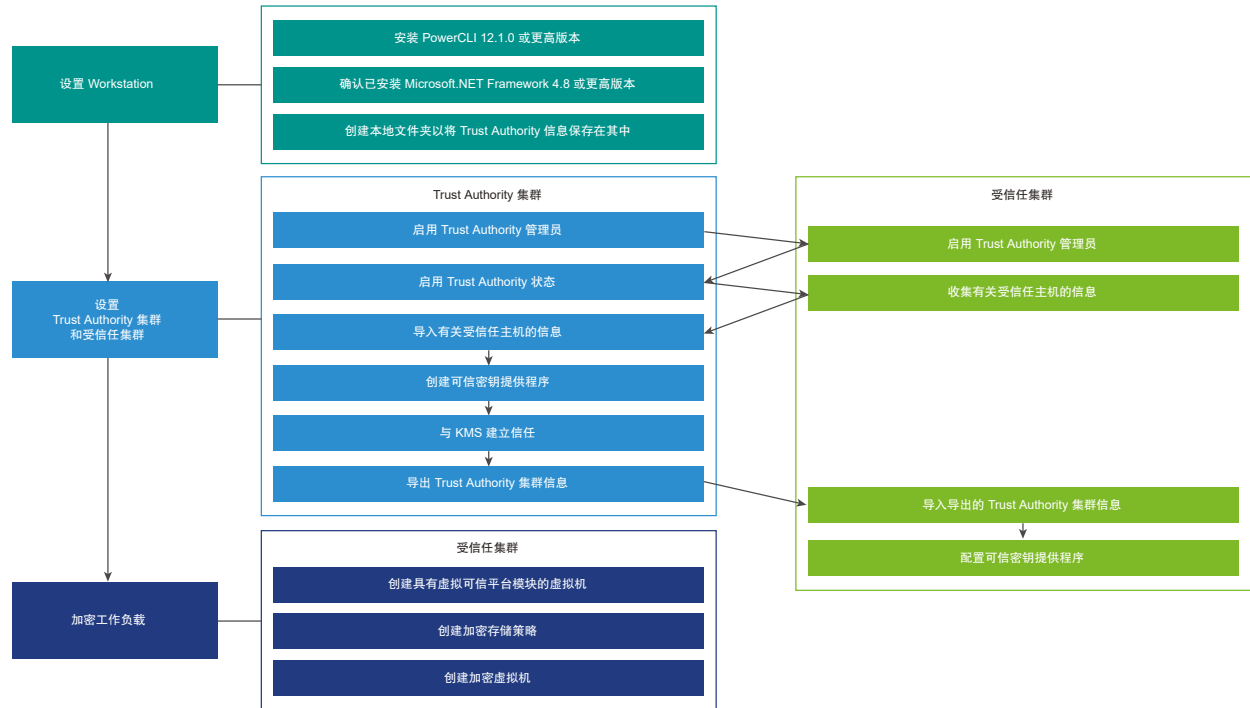
在开始配置 vSphere Trust Authority 之前，请参见[vSphere Trust Authority 的必备条件和所需特权](#)，了解有关 vCenter Server 系统和 ESXi 主机所需设置的信息。

可以通过以下方式管理 vSphere Trust Authority 的不同方面。

- 使用 PowerCLI cmdlet 或 vSphere API 配置 vSphere Trust Authority 服务和可信连接。请参见《VMware PowerCLI Cmdlet 参考》和《vSphere Automation SDK 编程指南》。
- 使用 PowerCLI cmdlet 或通过 vSphere Client 管理可信密钥提供程序的配置。
- 使用 vSphere Client 和 API 执行加密工作流，就像先前 vSphere 版本中那样。



图 9-4. vSphere Trust Authority workflow



要配置和管理 vSphere Trust Authority，可以使用 VMware PowerCLI，但是可以在 vSphere Client 中获得某些功能。

配置 vSphere Trust Authority 时，必须在 Trust Authority 集群和受信任集群上完成设置任务。其中一些任务需按照特定的顺序执行。使用本指南中列出的任务顺序。

**注** 完成初始 vSphere Trust Authority 设置后将更多 ESXi 主机添加到受信任集群时，可能需要再次导出和导入受信任主机信息。也就是说，如果新 ESXi 主机与原始主机不同，则必须收集新的 ESXi 主机信息并将其导入到 Trust Authority 集群中。请参见[添加和移除 vSphere Trust Authority 主机](#)。

## 步骤

### 1 设置工作站以配置 vSphere Trust Authority

要配置 vSphere Trust Authority 部署，必须先准备具有必要软件和设置的工作站。

### 2 启用 Trust Authority 管理员

要启用 vSphere Trust Authority，必须将用户添加到 vSphere TrustedAdmins 组。此用户将成为 Trust Authority 管理员。对于大多数 vSphere Trust Authority 配置任务，将使用 Trust Authority 管理员。

### 3 启用 Trust Authority 状态

将 vCenter Server 集群转变为 vSphere Trust Authority 集群（也称为启用 Trust Authority 状态）时，会在集群中的 ESXi 主机上启动所需的 Trust Authority 服务。

#### 4 收集有关要信任的 ESXi 主机和 vCenter Server 的信息

要建立信任，vSphere Trust Authority 集群需要有关受信任集群的 ESXi 主机和 vCenter Server 的信息。可以将此信息导出为文件，以便导入到 Trust Authority 集群中。您必须保证这些文件的机密性，并安全地进行传输。

#### 5 将受信任主机信息导入到 Trust Authority 集群

可以将导出的 ESXi 主机和 vCenter Server 信息导入到 vSphere Trust Authority 集群中，以便 Trust Authority 集群了解可以证明哪些主机。

#### 6 在 Trust Authority 集群上创建密钥提供程序

要使密钥提供程序服务能够连接到密钥提供程序，必须创建可信密钥提供程序，然后在 vSphere Trust Authority 集群和密钥服务器 (KMS) 之间配置信任设置。对于大多数符合 KMIP 的密钥服务器，此配置需要设置客户端和服务端证书。

#### 7 导出 Trust Authority 集群信息

要使受信任集群能够连接到 vSphere Trust Authority 集群，必须以文件的形式导出 Trust Authority 集群的服务信息，然后将该文件导入到受信任集群。必须保证此文件的机密性，并安全地进行传输。

#### 8 将 Trust Authority 集群信息导入到受信任主机

将 vSphere Trust Authority 集群信息导入到受信任集群后，受信任主机将开始使用 Trust Authority 集群执行证明过程。

#### 9 使用 vSphere Client 为受信任主机配置可信密钥提供程序

可以使用 vSphere Client 配置可信密钥提供程序。

#### 10 使用命令行行为受信任主机配置可信密钥提供程序

可以使用命令行配置可信密钥提供程序。可以为 vCenter Server 或在 vCenter 对象层次结构中的集群级别或集群文件夹级别配置默认可信密钥提供程序。

## 设置工作站以配置 vSphere Trust Authority

要配置 vSphere Trust Authority 部署，必须先准备具有必要软件和设置的工作站。

在有权访问 vSphere Trust Authority 环境的工作站上执行以下步骤。

### 步骤

- 1 安装 PowerCLI 12.1.0 或更高版本：请参见《PowerCLI 用户指南》。
- 2 确认已安装 Microsoft .NET Framework 4.8 或更高版本。
- 3 创建一个本地文件夹，用于保存导出为文件的 Trust Authority 信息。

### 后续步骤

继续启用 Trust Authority 管理员。

## 启用 Trust Authority 管理员

要启用 vSphere Trust Authority，必须将用户添加到 vSphere TrustedAdmins 组。此用户将成为 Trust Authority 管理员。对于大多数 vSphere Trust Authority 配置任务，将使用 Trust Authority 管理员。

使用不同于 vCenter Server 管理员的用户作为 Trust Authority 管理员。使用单独的用户可增强环境的安全性。必须为 Trust Authority 集群和受信任集群启用 Trust Authority 管理员。

### 前提条件

创建用户或标识现有用户，使其成为 Trust Authority 管理员。

### 步骤

- 1 使用 vSphere Client 连接到 Trust Authority 集群的 vCenter Server。
- 2 以管理员身份登录。
- 3 在主页菜单中，选择**系统管理**。
- 4 在 **Single Sign On** 下，单击**用户和组**。
- 5 单击**组**，然后单击 **TrustedAdmins** 组。

如果 TrustedAdmins 组最初未显示，请使用**筛选器**图标对其进行筛选，或者通过单击窗格底部的向右箭头在组之间进行导航。

- 6 在**组成员**区域中，单击**添加成员**。

确保选择了本地标识源（vsphere.local 是默认值，但您可能在安装过程中选择了不同的域），然后搜索要添加到组中作为 Trust Authority 管理员的成员（用户）。

- 7 选择成员。
- 8 单击**保存**。
- 9 对受信任集群的 vCenter Server 重复步骤 1 至 8。

### 后续步骤

继续[启用 Trust Authority 状态](#)。

## 启用 Trust Authority 状态

将 vCenter Server 集群转变为 vSphere Trust Authority 集群（也称为启用 Trust Authority 状态）时，会在集群中的 ESXi 主机上启动所需的 Trust Authority 服务。

### 前提条件

- [启用 Trust Authority 管理员](#)。

## 步骤

- 1 在 PowerCLI 会话中，运行 `Connect-VIServer cmdlet`，以 Trust Authority 管理员用户身份连接到 Trust Authority 集群的 vCenter Server。

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 2 要检查集群的当前状态，请运行 `Get-TrustAuthorityCluster cmdlet`。

例如，以下命令显示集群 vTA Cluster，并显示其状态为“已禁用”。

```
Get-TrustAuthorityCluster

Name                State                Id
----                -
vTA Cluster         Disabled            TrustAuthorityCluster-domain-c8
```

输出将在找到的每个集群对应的“State”列中显示“Disabled”或“Enabled”。“Disabled”表示 Trust Authority 服务未运行。

- 3 要启用 Trust Authority 集群，请运行 `Set-TrustAuthorityCluster cmdlet`。

例如，以下命令启用集群 vTA Cluster。

```
Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA Cluster' -State Enabled
```

系统将显示确认提示响应。

```
Confirmation
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to
proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

- 4 在确认提示处，按 **Enter**。（默认值为 **y**。）

输出将显示集群的状态。例如，以下输出显示集群 vTA Cluster 已启用：

```
Name                State                Id
----                -
vTA Cluster         Enabled            TrustAuthorityCluster-domain-c8
```

## 结果

以下两个服务在 Trust Authority 集群中的 ESXi 主机上启动：证明服务和密钥提供程序服务。

## 示例：在 Trust Authority 集群上启用受信任状态

此示例显示了如何使用 PowerCLI 在 Trust Authority 集群上启用服务。下表显示了所使用的示例组件和值。

表 9-4. vSphere Trust Authority 设置示例

组件	值
Trust Authority 集群的 vCenter Server	192.168.210.22
Trust Authority 集群名称	vTA Cluster
Trust Authority 管理员	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'
```

Name	Port	User
----	----	----
192.168.210.22	443	VSPHERE.LOCAL\trustedadmin

```
PS C:\Users\Administrator.CORP> Get-TrustAuthorityCluster
```

Name	State	Id
----	-----	--
vTA Cluster	Disabled	TrustAuthorityCluster-domain-c8

```
PS C:\Users\Administrator.CORP> Set-TrustAuthorityCluster -TrustAuthorityCluster 'vTA
Cluster' -State Enabled
```

Confirmation  
Setting TrustAuthorityCluster 'vTA Cluster' with new State 'Enabled'. Do you want to proceed?  
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y

Name	State	Id
----	-----	--
vTA Cluster	Enabled	TrustAuthorityCluster-domain-c8

### 后续步骤

继续收集有关要信任的 ESXi 主机和 vCenter Server 的信息。

## 收集有关要信任的 ESXi 主机和 vCenter Server 的信息

要建立信任，vSphere Trust Authority 集群需要有关受信任集群的 ESXi 主机和 vCenter Server 的信息。可以将此信息导出为文件，以便导入到 Trust Authority 集群中。您必须保证这些文件的机密性，并安全地进行传输。

可以使用 vSphere Trust Authority PowerCLI cmdlet 将受信任集群中 ESXi 主机的以下信息导出为文件，以便 Trust Authority 集群了解要信任的软件和硬件。

- ESXi 版本
- TPM 制造商（CA 证书）

- （可选）单个 TPM （EK 证书）

**注** 请将这些导出的文件存储在安全位置，以防必须还原 vSphere Trust Authority 配置。

如果您的主机具有相同的类型和供应商，并且制造时间和地点也相同，则能够通过仅获取其中一个 TPM 的 CA 证书来信任所有 TPM。要信任单个 TPM，需要获取该 TPM 的 EK 证书。

还必须从受信任集群的 vCenter Server 中获取主体信息。主体信息包含 vpxd 解决方案用户及其证书链。通过主体信息，受信任集群的 vCenter Server 能够发现 Trust Authority 集群上配置的可用可信密钥提供程序。

要最初配置 vSphere Trust Authority，必须收集 ESXi 版本和 TPM 信息。此外，每次部署新版本的 ESXi 后（包括升级或应用修补程序时），也都必须收集 ESXi 版本。

每个 vCenter Server 系统仅收集一次 vCenter Server 主体信息。

#### 前提条件

- 确定受信任集群中的 ESXi 版本和 TPM 硬件类型，以及是要信任所有 TPM 硬件类型、仅某些 TPM 硬件类型还是单个主机。
- 在运行 PowerCLI cmdlet 的计算机上，创建一个本地文件夹，用于保存导出为文件的信息。
- 启用 Trust Authority 管理员。
- 启用 Trust Authority 状态。

#### 步骤

- 1 在 PowerCLI 会话中，运行以下命令，断开任何当前连接，并以 root 用户身份连接到受信任集群中的某个 ESXi 主机。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

- 2 运行 Get-VMHost cmdlet 以确认 ESXi 主机。

```
Get-VMHost
```

此时将显示主机信息。

- 3 将 Get-VMHost 分配给变量。

例如：

```
$vmhost = Get-VMHost
```

#### 4 运行 Export-Tpm2CACertificate cmdlet 以导出给定 TPM 制造商的 CA 证书。

- a 将 Get-Tpm2EndorsementKey -VMHost \$vmhost 分配给变量。

例如，以下命令将 Get-Tpm2EndorsementKey -VMHost \$vmhost 分配给变量 \$tpm2。

```
$tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
```

- b 运行 Export-Tpm2CACertificate cmdlet。

例如，以下命令将 TPM 证书导出到 cacert.zip 文件。运行以下命令之前，请确保目标目录已存在。

```
Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip
```

将创建此文件。

- c 对要信任集群中的每个 TPM 硬件类型重复此操作。请对每个 TMP 硬件类型使用不同的文件名，以便不会覆盖以前导出的文件。

#### 5 运行 Export-VMHostImageDb cmdlet 以导出软件（ESXi 映像）的 ESXi 主机描述。

例如，以下命令将信息导出到 image.tgz 文件。运行以下命令之前，请确保目标目录已存在。

```
Export-VMHostImageDb -VMHost $vmhost -FilePath C:\vta\image.tgz
```

---

**注** 如果希望登录到受信任集群的 vCenter Server，Export-VMHostImageDb cmdlet 也会起作用。

---

将创建此文件。

对要信任集群中的每个 ESXi 版本重复此操作。请对每个版本使用不同的文件名，以便不会覆盖以前导出的文件。

## 6 导出受信任集群的 vCenter Server 主体信息。

- a 与 ESXi 主机断开连接。

```
Disconnect-VIServer -server * -Confirm:$false
```

- b 使用 Trust Authority 管理员用户连接到受信任集群的 vCenter Server。（或者，也可以使用具有管理员特权的用户。）

```
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'
```

- c 要导出受信任集群的 vCenter Server 主体信息，请运行 Export-TrustedPrincipal cmdlet。

例如，以下命令将信息导出到 principal.json 文件。运行以下命令之前，请确保目标目录已存在。

```
Export-TrustedPrincipal -FilePath C:\vta\principal.json
```

将创建此文件。

## 7 （可选）如果要信任单个主机，必须导出 TPM EK 公钥证书。

请参见[导出和导入 TPM 认可密钥证书](#)。

### 结果

将创建以下文件：

- TPM CA 证书文件（.zip 文件扩展名）
- ESXi 映像文件（.tgz 文件扩展名）
- vCenter Server 主体文件（.json 文件扩展名）

### 示例：收集有关要信任的 ESXi 主机和 vCenter Server 的信息

以下示例显示了如何使用 PowerCLI 导出 ESXi 主机信息和 vCenter Server 主体。下表显示了所使用的示例组件和值。

**表 9-5. vSphere Trust Authority 设置示例**

组件	值
受信任集群中的 ESXi 主机	192.168.110.51
受信任集群的 vCenter Server	192.168.110.22
变量 \$vmhost	Get-VMHost
变量 \$tpm2	Get-Tpm2EndorsementKey -VMHost \$vmhost



表 9-5. vSphere Trust Authority 设置示例（续）

组件	值
Trust Authority 管理员	trustedadmin@vsphere.local
包含输出文件的本地目录	C:\vta

```

PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.51 -User root -Password 'VMware1!'

Name                                     Port  User
----
192.168.110.51                         443   root

PS C:\Users\Administrator.CORP> Get-VMHost

Name                                     ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz MemoryUsageGB
MemoryTotalGB Version
-----
192.168.110.51 Connected          PoweredOn      4      200      9576
1.614          7.999  7.0.0

PS C:\Users\Administrator.CORP> $vmhost = Get-VMHost
PS C:\Users\Administrator.CORP> $tpm2 = Get-Tpm2EndorsementKey -VMHost $vmhost
PS C:\> Export-Tpm2CACertificate -Tpm2EndorsementKey $tpm2 -FilePath C:\vta\cacert.zip

Mode                LastWriteTime         Length Name
----
-a-----      10/8/2019   6:55 PM          1004 cacert.zip

PS C:\Users\Administrator.CORP> Export-VMHostImageDb -VMHost $vmhost -FilePath
C:\vta\image.tgz

Mode                LastWriteTime         Length Name
----
-a-----      10/8/2019  11:02 PM          2391 image.tgz

PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                                     Port  User
----
192.168.110.22                         443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Export-TrustedPrincipal -FilePath C:\vta\principal.json

Mode                LastWriteTime         Length Name
----
-a-----      10/8/2019  11:14 PM          1873 principal.json

```

## 后续步骤

继续将受信任主机信息导入到 [Trust Authority](#) 集群。

## 导出和导入 TPM 认可密钥证书

可以从 ESXi 主机中导出 TPM 认可密钥 (EK) 证书，然后将其导入 vSphere Trust Authority 集群。如果要信任受信任集群中的单个 ESXi 主机，需要执行此操作。

要将 TPM EK 证书导入到 Trust Authority 集群，必须将 Trust Authority 集群的默认证明类型更改为接受 EK 证书。默认证明类型接受 TPM 证书颁发机构 (CA) 证书。某些 TPM 不包含 EK 证书。如果要信任单个 ESXi 主机，TPM 必须包含一个 EK 证书。

---

**注** 请将导出的 EK 证书文件存储在安全的位置，以防必须还原 vSphere Trust Authority 配置。

---

### 前提条件

- 启用 [Trust Authority](#) 管理员。
- 启用 [Trust Authority](#) 状态。

### 步骤

- 1 确保您已经以 Trust Authority 管理员身份连接到 Trust Authority 集群的 vCenter Server。  
例如，可以输入 `$global:defaultviservers`，显示所有连接的服务器。
- 2 (可选) 如有必要，可以运行以下命令确保您已连接到 Trust Authority 集群的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 3 要更改 Trust Authority 集群的证明类型，请执行以下操作：
  - a 运行 `Get-TrustAuthorityCluster cmdlet` 以显示由此 vCenter Server 管理的集群。

```
Get-TrustAuthorityCluster
```

此时将显示这些集群。

- b 将 `Get-TrustAuthorityCluster` 信息分配给变量。  
例如，以下命令将名为 `vTA Cluster` 的集群分配给变量 `$vTA`。

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

- c 将 `Get-TrustAuthorityTpm2AttestationSettings` 信息分配给变量。  
例如，以下命令将信息分配给变量 `$tpm2Settings`。

```
$tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster $vTA
```

- d 运行 `Set-TrustAuthorityTpm2AttestationSettings cmdlet`，并指定 `RequireEndorsementKey` 和/或 `RequireCertificateValidation`。

例如，以下命令指定 `RequireEndorsementKey`。

```
Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings $tpm2Settings
-RequireEndorsementKey
```

系统将显示如下类似的确认提示响应。

```
Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-
c8' with the following parameters:
  RequireCertificateValidation: False
  RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"):
```

- e 在确认提示处，按 **Enter**。（默认值为 **Y**。）

输出显示指定设置的状态为 **True**。例如，在以下输出中，需要认可密钥的状态显示为 **True**，需要证书验证的状态显示为 **False**。

```
Name                                     RequireEndorsementKey
-----
RequireCertificateValidation  Health
-----
TrustAuthorityTpm2AttestationSettings... True
False                         Ok
```

#### 4 要导出 TPM EK 证书，请执行以下操作：

- a 与 Trust Authority 集群的 vCenter Server 断开连接。

```
Disconnect-VIServer -server * -Confirm:$false
```

- b 运行 `Connect-VIServer cmdlet`，以 `root` 用户身份连接到受信任集群中的某个 ESXi 主机。

```
Connect-VIServer -server host_ip_address -User root -Password 'password'
```

- c 运行 `Get-VMHost cmdlet` 以确认 ESXi 主机。

```
Get-VMHost
```

此时将显示主机信息。

- d 将 Get-VMHost 分配给变量。

例如：

```
$vmhost = Get-VMHost
```

- e 运行 Export-Tpm2EndorsementKey cmdlet，导出 ESXi 主机的 EK 证书。

例如，以下命令将 EK 证书导出到 tpm2ek.json 文件。

```
Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath C:\vta\tpm2ek.json
```

将创建此文件。

## 5 要导入 TPM EK，请执行以下操作：

- a 与受信任集群中的 ESXi 主机断开连接。

```
Disconnect-VIServer -server * -Confirm:$false
```

- b 使用 Trust Authority 管理员用户连接到 Trust Authority 集群的 vCenter Server。

```
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user  
-Password 'password'
```

- c 运行 Get-TrustAuthorityCluster cmdlet。

```
Get-TrustAuthorityCluster
```

此时将显示 Trust Authority 集群中的集群。

- d 将 Get-TrustAuthorityCluster '*cluster*' 信息分配给变量。

例如，以下命令将集群 vTA Cluster 的信息分配给变量 \$vTA。

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

- e 运行 New-TrustAuthorityTpm2EndorsementKey cmdlet。

例如，以下命令使用之前在步骤 4 中导出的 tpm2ek.json 文件。

```
New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA -FilePath  
C:\vta\tpm2ek.json
```

此时将显示导入的认可密钥信息。

## 结果

Trust Authority 集群的证明类型更改为接受 EK 证书。EK 证书从受信任集群中导出并导入到 Trust Authority 集群。

### 示例：导出和导入 TPM EK 证书

以下示例显示了如何使用 PowerCLI 将 Trust Authority 集群的默认证明类型更改为接受 EK 证书，从受信任集群中的 ESXi 主机导出 TPM EK 证书，然后将其导入到 Trust Authority 集群。下表显示了所使用的示例组件和值。

**表 9-6. vSphere Trust Authority 设置示例**

组件	值
Trust Authority 集群的 vCenter Server	192.168.210.22
变量 \$vTA	Get-TrustAuthorityCluster 'vTA Cluster'
变量 \$tpm2Settings	Get-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster \$vTA
变量 \$vmhost	Get-VMHost
受信任集群中的 ESXi 主机	192.168.110.51
Trust Authority 管理员	trustedadmin@vsphere.local
包含输出文件的本地目录	C:\vta

```
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                                Port  User
----                                -
192.168.210.22                     443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                State           Id
----                -
vTA Cluster         Enabled         TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster'

PS C:\Users\Administrator> $tpm2Settings = Get-TrustAuthorityTpm2AttestationSettings
-TrustAuthorityCluster $vTA

PS C:\Users\Administrator> Set-TrustAuthorityTpm2AttestationSettings -Tpm2AttestationSettings
$tpm2Settings -RequireEndorsementKey

Confirmation
Configure the Tpm2AttestationSettings 'TrustAuthorityTpm2AttestationSettings-domain-c8' with
the following parameters:
  RequireCertificateValidation: False
  RequireEndorsementKey: True
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

Name                                RequireEndorsementKey
RequireCertificateValidation  Health
----                                -
```

```

-----
TrustAuthorityTpm2AttestationSettings... True
False                               Ok

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.110.51 -User root -Password
'VMware1!'

Name                               Port  User
----                               -
192.168.110.51                     443   root

PS C:\Users\Administrator> Get-VMHost

Name                               ConnectionState PowerState NumCpu CpuUsageMhz CpuTotalMhz
MemoryUsageGB MemoryTotalGB Version
-----
-----
192.168.110.51 Connected      PoweredOn    4      55      9576
1.230          7.999    7.0.0

PS C:\Users\Administrator> $vmhost = Get-VMHost
PS C:\Users\Administrator> Export-Tpm2EndorsementKey -VMHost $vmhost -FilePath
C:\vta\tpm2ek.json

Mode                               LastWriteTime           Length Name
----                               -
-a----          12/3/2019  10:16 PM           2391 tpm2ek.json

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                               Port  User
----                               -
192.168.210.22                     443   VSPHERE.LOCAL\TrustedAdmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                               State           Id
----                               -
vTA Cluster                       Enabled         TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster'
PS C:\Users\Administrator> New-TrustAuthorityTpm2EndorsementKey -TrustAuthorityCluster $vTA
-FilePath C:\vta\tpm2ek.json

TrustAuthorityClusterId           Name                               Health
-----
TrustAuthorityCluster-domain-c8   1a520e42-4db8-1cbb-6dd7-f493fd921ccb  Ok

```

## 后续步骤

继续将受信任主机信息导入到 [Trust Authority 集群](#)。

## 将受信任主机信息导入到 Trust Authority 集群

可以将导出的 ESXi 主机和 vCenter Server 信息导入到 vSphere Trust Authority 集群中，以便 Trust Authority 集群了解可以证明哪些主机。

如果按顺序执行这些任务，您仍会连接到 Trust Authority 集群的 vCenter Server。

### 前提条件

- 启用 Trust Authority 管理员。
- 启用 Trust Authority 状态。
- 收集有关要信任的 ESXi 主机和 vCenter Server 的信息。

### 步骤

- 1 确保您已经以 Trust Authority 管理员身份连接到 Trust Authority 集群的 vCenter Server。  
例如，可以输入 `$global:defaultviservers`，显示所有连接的服务器。
- 2 （可选）如有必要，可以运行以下命令确保您已连接到 Trust Authority 集群的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 3 要显示此 vCenter Server 管理的集群，请运行 `Get-TrustAuthorityCluster` cmdlet。

```
Get-TrustAuthorityCluster
```

此时将显示这些集群。

- 4 将 `Get-TrustAuthorityCluster 'cluster'` 信息分配给变量。

例如，以下命令将集群 vTA Cluster 的信息分配给变量 `$vTA`。

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

- 5 要将受信任集群的 vCenter Server 主体信息导入到 Trust Authority 集群中，请运行 `New-TrustAuthorityPrincipal` cmdlet。

例如，以下命令导入之前在收集有关要信任的 ESXi 主机和 vCenter Server 的信息中导出的 `principal.json` 文件。

```
New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA -FilePath C:\vta\principal.json
```

此时将显示 `TrustAuthorityPrincipal` 信息。

- 6 要验证导入，请运行 `Get-TrustAuthorityPrincipal` cmdlet。

例如：

```
Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
```

此时将显示导入的 `TrustAuthorityPrincipal` 信息。

- 7 要导入可信平台模块 (TPM) CA 证书信息，请运行 `New-TrustAuthorityTpm2CACertificate` cmdlet。

例如，以下命令将从之前在收集有关要信任的 ESXi 主机和 vCenter Server 的信息中导出的 `cacert.zip` 文件导入 TPM CA 证书信息。

```
New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster $vTA -FilePath C:\vta\cacert.zip
```

此时将显示导入的证书信息。

- 8 要导入 ESXi 主机基础映像信息，请运行 `New-TrustAuthorityVMHostBaseImage` cmdlet。

例如，以下命令将从之前在收集有关要信任的 ESXi 主机和 vCenter Server 的信息中导出的 `image.tgz` 文件导入映像信息。

```
New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA -FilePath C:\vta\image.tgz
```

此时将显示导入的映像信息。

## 结果

Trust Authority 集群了解可以远程证明哪些 ESXi 主机，由此了解可以信任哪些主机。

## 示例：将受信任主机信息导入到 Trust Authority 集群

以下示例显示了如何使用 PowerCLI 将受信任集群的 vCenter Server 主体信息和受信任主机信息文件导入到 Trust Authority 集群。该示例假设您已经以 Trust Authority 管理员身份连接到 Trust Authority 集群的 vCenter Server。下表显示了所使用的示例组件和值。

表 9-7. vSphere Trust Authority 设置示例

组件	值
变量 <code>\$vTA</code>	<code>Get-TrustAuthorityCluster 'vTA Cluster1'</code>
Trust Authority 集群的 vCenter Server	192.168.210.22
Trust Authority 集群名称	vTA Cluster1 (Enabled) vTA Cluster2 (Disabled)
主体信息文件	C:\vta\principal.json
TPM 证书文件	C:\vta\cacert.cer



表 9-7. vSphere Trust Authority 设置示例（续）

组件	值
ESXi 主机基础映像文件	C:\vta\image.tgz
Trust Authority 管理员	trustedadmin@vsphere.local

```

PS C:\Users\Administrator> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                                Port  User
----                                -
192.168.210.22                      443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator> Get-TrustAuthorityCluster

Name                State          Id
----                -
vTA Cluster1        Enabled        TrustAuthorityCluster-domain-c8
vTA Cluster2        Disabled       TrustAuthorityCluster-domain-c26

PS C:\Users\Administrator> $vTA = Get-TrustAuthorityCluster 'vTA Cluster1'

PS C:\Users\Administrator.CORP> New-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA
-FilePath C:\vta\principal.json

Name                                Domain          Type
TrustAuthorityClusterId
----                                -
-----
vpxd-de207929-0601-43ef-9616-47d0cee0302f    vsphere.local  STS_USER
TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> Get-TrustAuthorityPrincipal -TrustAuthorityCluster $vTA

Name                                Domain          Type
TrustAuthorityClusterId
----                                -
-----
vpxd-de207929-0601-43ef-9616-47d0cee0302f    vsphere.local  STS_USER
TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityTpm2CACertificate -TrustAuthorityCluster
$vTA -FilePath C:\vta\cacert.cer

TrustAuthorityClusterId              Name                                Health
-----
TrustAuthorityCluster-domain-c8      52BDB7B4B2F55C925C047257DED4588A7767D961 Ok

PS C:\Users\Administrator.CORP> New-TrustAuthorityVMHostBaseImage -TrustAuthorityCluster $vTA
-FilePath C:\vta\image.tgz

TrustAuthorityClusterId              VMHostVersion              Health
-----

```

-----  
TrustAuthorityCluster-domain-c8-----  
ESXi 7.0.0-0.0.14828939-----  
Ok

## 后续步骤

继续在 [Trust Authority](#) 集群上创建密钥提供程序。

## 在 Trust Authority 集群上创建密钥提供程序

要使密钥提供程序服务能够连接到密钥提供程序，必须创建可信密钥提供程序，然后在 vSphere Trust Authority 集群和密钥服务器 (KMS) 之间配置信任设置。对于大多数符合 KMIP 的密钥服务器，此配置需要设置客户端和服务端证书。

以前在 vSphere 6.7 中称为 KMS 集群，现在，在 vSphere 7.0 中称为密钥提供程序。有关密钥提供程序的详细信息，请参见[什么是 vSphere Trust Authority 密钥提供程序服务](#)。

在生产环境中，您可以创建多个密钥提供程序。通过创建多个密钥提供程序，可以解决如何根据公司组织、不同的业务单位或客户等管理部署的问题。

如果按顺序执行这些任务，您仍会连接到 vSphere Trust Authority 集群的 vCenter Server。

### 前提条件

- 启用 [Trust Authority](#) 管理员。
- 启用 [Trust Authority](#) 状态。
- 收集有关要信任的 [ESXi](#) 主机和 [vCenter Server](#) 的信息。
- 将受信任主机信息导入到 [Trust Authority](#) 集群。
- 在密钥服务器上创建并激活密钥，使其成为可信密钥提供程序的主密钥。此密钥可封装此可信密钥提供程序使用的其他密钥。有关创建密钥的详细信息，请参见密钥服务器供应商文档。

### 步骤

- 1 确保您已连接到 Trust Authority 集群的 vCenter Server。例如，可以输入 `$global:defaultviservers`，显示所有连接的服务器。
- 2 （可选）如有必要，可以运行以下命令确保您已连接到 Trust Authority 集群的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 3 要创建可信密钥提供程序，请运行 `New-TrustAuthorityKeyProvider` cmdlet。

例如，此命令使用 1 作为 `PrimaryKeyId`，并使用名称 `clkp`。如果按顺序执行这些任务，则之前已将 `Get-TrustAuthorityCluster` 信息分配给了变量（例如，`$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`）。

```
New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA -PrimaryKeyId 1 -Name clkp
-KmipServerAddress ip_address
```

PrimaryKeyID 通常是来自密钥服务器的密钥 ID，采用 UUID 形式。请勿将密钥名称用于 PrimaryKeyID。PrimaryKeyID 值与供应商有关。请参见您的密钥服务器文档。New-TrustAuthorityKeyProvider cmdlet 可以采用其他选项，如 KmipServerPort、ProxyAddress 和 ProxyPort。有关详细信息，请参见 New-TrustAuthorityKeyProvider 帮助系统。

每个逻辑密钥提供程序（无论其类型如何：标准、可信和本机密钥提供程序），都必须在所有 vCenter Server 系统中具有唯一的名称。

有关详细信息，请参见[密钥提供程序命名](#)。

---

**注** 要将多个密钥服务器添加到密钥提供程序，请使用 Add-TrustAuthorityKeyProviderServer cmdlet。

---

此时将显示密钥提供程序信息。

- 4 建立可信连接，以便密钥服务器信任可信密钥提供程序。具体过程取决于密钥服务器接受的证书以及您的公司策略。选择适用于服务器的选项，然后完成各个步骤。

选项	请参见
上载客户端证书	<a href="#">上载客户端证书以建立可信密钥提供程序可信连接.</a>
上载 KMS 证书和私钥	<a href="#">上载证书和私钥以建立可信密钥提供程序可信连接.</a>
新建证书签名请求	<a href="#">创建证书签名请求以建立可信密钥提供程序可信连接.</a>

## 5 通过上载密钥服务器证书完成信任设置，以使可信密钥提供程序信任密钥服务器。

- a 将 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 信息分配给变量。

例如：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

此变量获取给定 **Trust Authority** 集群（在本例中为 `$vTA`）中的可信密钥提供程序。

**注** 如果您有多个可信密钥提供程序，请使用如下类似命令选择一个所需的可信密钥提供程序：

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

使用 `Select-Object -Last 1` 选择列表中的最后一个可信密钥提供程序。

- b 要获取密钥服务器服务器证书，请运行 `Get-TrustAuthorityKeyProviderServerCertificate` 命令。

例如：

```
Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers
```

此时将显示服务器证书信息。最初，证书不可信，因此“受信任”状态为 **False**。如果您配置了多个密钥服务器，则会返回证书列表。按照以下说明验证并添加每个证书。

- c 信任证书之前，请将 `Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer $kp.KeyProviderServers` 信息分配给变量（例如 `cert`），然后运行 `$cert.Certificate.ToString()` 命令并验证输出。

例如：

```
$cert = Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer
$kp.KeyProviderServers
$cert.Certificate.ToString()
```

此时将显示证书信息，包括主体、颁发者和其他信息。

- d 要将 **KMIP** 服务器证书添加到可信密钥提供程序，请运行 `Add-TrustAuthorityKeyProviderServerCertificate`。

例如：

```
Add-TrustAuthorityKeyProviderServerCertificate -ServerCertificate $cert
```

此时将显示证书信息，“受信任”状态现在为 **True**。

## 6 验证密钥提供程序的状态。

- a 要刷新密钥提供程序状态，请重新分配 \$kp 变量。

例如：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

**注** 如果您有多个可信密钥提供程序，请使用如下类似命令选择一个所需的可信密钥提供程序：

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

使用 `Select-Object -Last 1` 选择列表中的最后一个可信密钥提供程序。

- b 运行 `$kp.Status` 命令，获取密钥提供程序状态。

例如：

```
$kp.Status
```

**注** 状态可能需要几分钟才会刷新。要查看状态，请重新分配 \$kp 变量，然后重新运行 `$kp.Status` 命令。

运行状况为“Ok”表示密钥提供程序正常运行。

### 结果

可信密钥提供程序已创建，并与密钥服务器建立了信任。

### 示例：在 Trust Authority 集群上创建密钥提供程序

此示例显示了如何使用 PowerCLI 在 Trust Authority 集群上创建可信密钥提供程序。该示例假设您已经以 Trust Authority 管理员身份连接到 Trust Authority 集群的 vCenter Server。在向供应商提交 CSR 后，它还使用密钥服务器供应商签名的证书。

下表显示了所使用的示例组件和值。

**表 9-8. vSphere Trust Authority 设置示例**

组件	值
变量 \$vTA	Get-TrustAuthorityCluster 'vTA Cluster'
变量 \$kp	Get-TrustAuthorityKeyProvider -TrustAuthorityCluster \$vTA
变量 \$cert	Get-TrustAuthorityKeyProviderServerCertificate -KeyProviderServer \$kp.KeyProviderServers
Trust Authority 集群的 vCenter Server	192.168.210.22
符合 KMIP 的密钥服务器	192.168.110.91

表 9-8. vSphere Trust Authority 设置示例（续）

组件	值
符合 KMIP 的密钥服务器用户	vcqekmip
Trust Authority 集群名称	vTA Cluster
Trust Authority 管理员	trustedadmin@vsphere.local

```

PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
-PrimaryKeyId 8 -Name clkp -KmipServerAddress 192.168.110.91
Name                PrimaryKeyId      Type            TrustAuthorityClusterId
----                -
clkp                8                KMIP            TrustAuthorityCluster-domain-c8

PS C:\Users\Administrator.CORP> New-TrustAuthorityKeyProviderClientCertificate -KeyProvider
$kp
<Export the client certificate when you need to use it.>
PS C:\Users\Administrator.CORP> Export-TrustAuthorityKeyProviderClientCertificate
-KeyProvider $kp -FilePath clientcert.pem

PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$vTA
PS C:\Users\Administrator.CORP> Get-TrustAuthorityKeyProviderServerCertificate
-KeyProviderServer $kp.KeyProviderServers

Certificate                Trusted    KeyProviderServerId    KeyProviderId
-----                -
[Subject]...                False    domain-c8-clkp:192.16.... domain-c8-clkp

PS C:\WINDOWS\system32> $cert.Certificate.ToString()
[Subject]
    E=<domain>, CN=<IP address>, OU=VMware Engineering, O=VMware, L=Palo Alto, S=California,
    C=US

[Issuer]
    O=<host>.eng.vmware.com, C=US, DC=local, DC=vsphere, CN=CA

[Serial Number]
    00CEF192BBF9D80C9F

[Not Before]
    8/10/2015 4:16:12 PM

[Not After]
    8/9/2020 4:16:12 PM

[Thumbprint]
    C44068C124C057A3D07F51DCF18720E963604B70

```

```
PS C:\Users\Administrator.CORP> $cert = Get-TrustAuthorityKeyProviderServerCertificate
-KeyProviderServer $kp.KeyProviderServers
PS C:\Users\Administrator.CORP> Add-TrustAuthorityKeyProviderServerCertificate
-ServerCertificate $cert
```

Certificate	Trusted	KeyProviderServerId	KeyProviderId
[Subject]...	True		domain-c8-clkp

```
PS C:\Users\Administrator.CORP> $kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster
$vTA
PS C:\Users\Administrator.CORP> $kp.Status
```

KeyProviderId	Health	HealthDetails	ServerStatus
domain-c8-kp4	Ok	{}	{192.168.210.22}

### 后续步骤

继续导出 [Trust Authority](#) 集群信息。

## 上载客户端证书以建立可信密钥提供程序可信连接

某些密钥服务器 (KMS) 供应商要求将可信密钥提供程序的客户端证书上载到密钥服务器。上载后，密钥服务器便会接受来自可信密钥提供程序的流量。

### 前提条件

- 启用 [Trust Authority](#) 管理员。
- 启用 [Trust Authority](#) 状态。
- 收集有关要信任的 [ESXi](#) 主机和 [vCenter Server](#) 的信息。
- 将受信任主机信息导入到 [Trust Authority](#) 集群。
- 在 [Trust Authority](#) 集群上创建密钥提供程序。

### 步骤

- 1 确保您已连接到 [Trust Authority](#) 集群的 [vCenter Server](#)。例如，可以输入 `$global:defaultviservers`，显示所有连接的服务器。
- 2 （可选）如有必要，可以运行以下命令确保您已连接到 [Trust Authority](#) 集群的 [vCenter Server](#)。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 3 将 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 信息分配给变量。

例如：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

如果按顺序执行这些任务，则之前已将 `Get-TrustAuthorityCluster` 信息分配给了变量（例如，`$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`）。

此变量获取给定 **Trust Authority** 集群（在本例中为 `$vTA`）中的可信密钥提供程序。

**注** 如果您有多个可信密钥提供程序，请使用如下类似命令选择一个所需的可信密钥提供程序：

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

使用 `Select-Object -Last 1` 选择列表中的最后一个可信密钥提供程序。

- 4 要创建可信密钥提供程序客户端证书，请运行 `New-TrustAuthorityKeyProviderClientCertificate cmdlet`。

例如：

```
New-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp
```

此时将显示指纹。

- 5 要导出密钥提供程序客户端证书，请运行 `Export-TrustAuthorityKeyProviderClientCertificate cmdlet`。

例如：

```
Export-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -FilePath clientcert.pem
```

证书将导出到文件。

- 6 将证书文件上载到密钥服务器。  
有关详细信息，请参见密钥服务器文档。

## 结果

可信密钥提供程序与密钥服务器建立了信任。

## 上载证书和私钥以建立可信密钥提供程序可信连接

某些密钥服务器 (KMS) 供应商要求使用密钥服务器提供的客户端证书和私钥配置可信密钥提供程序。配置可信密钥提供程序后，密钥服务器将接受来自可信密钥提供程序的流量。

### 前提条件

- 启用 **Trust Authority** 管理员。
- 启用 **Trust Authority** 状态。
- 收集有关要信任的 **ESXi** 主机和 **vCenter Server** 的信息。
- 将受信任主机信息导入到 **Trust Authority** 集群。
- 在 **Trust Authority** 集群上创建密钥提供程序。



- 向密钥服务器供应商请求 PEM 格式的证书和私钥。如果证书以非 PEM 的格式返回，请将其转换为 PEM。如果私钥受密码保护，请创建移除了密码的 PEM 文件。可以使用 openssl 命令执行这两项操作。例如：

- 要将证书从 CRT 转换为 PEM 格式，请执行以下命令：

```
openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
```

- 要将证书从 DER 转换为 PEM 格式，请执行以下命令：

```
openssl x509 -inform DER -in clientcert.der -out clientcert.pem
```

- 要从私钥中移除密码，请执行以下命令：

```
openssl rsa -in key.pem -out keynopassword.pem
Enter pass phrase for key.pem:
writing RSA key
```

## 步骤

- 1 确保您已连接到 Trust Authority 集群的 vCenter Server。例如，可以输入 `$global:defaultviservers`，显示所有连接的服务器。
- 2 （可选）如有必要，可以运行以下命令确保您已连接到 Trust Authority 集群的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 3 将 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 信息分配给变量。

例如：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

如果按顺序执行这些任务，则之前已将 `Get-TrustAuthorityCluster` 信息分配给了变量（例如，`$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`）。

`$kp` 变量获取给定 Trust Authority 集群（在本例中为 `$vTA`）中的可信密钥提供程序。

**注** 如果您有多个可信密钥提供程序，请使用如下类似命令选择一个所需的可信密钥提供程序：

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

使用 `Select-Object -Last 1` 选择列表中的最后一个可信密钥提供程序。

#### 4 使用 Set-TrustAuthorityKeyProviderClientCertificate 命令上载证书和私钥。

例如：

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath
<path/to/certfile.pem> -PrivateKeyFilePath <path/to/privatekey.pem>
```

#### 结果

可信密钥提供程序与密钥服务器建立了信任。

### 创建证书签名请求以建立可信密钥提供程序可信连接

某些密钥服务器 (KMS) 供应商要求生成证书签名请求 (CSR) 并将该 CSR 发送到密钥服务器供应商。密钥服务器供应商将对 CSR 进行签名并返回签名证书。将此签名证书配置为可信密钥提供程序的客户端证书后，密钥服务器将接受来自可信密钥提供程序的流量。

此任务分为两步。首先，生成 CSR 并将其发送给密钥服务器供应商。然后，上载从密钥服务器供应商收到的签名证书。

#### 前提条件

- 启用 Trust Authority 管理员。
- 启用 Trust Authority 状态。
- 收集有关要信任的 ESXi 主机和 vCenter Server 的信息。
- 将受信任主机信息导入到 Trust Authority 集群。
- 在 Trust Authority 集群上创建密钥提供程序。

#### 步骤

- 1 确保您已连接到 Trust Authority 集群的 vCenter Server。例如，可以输入 `$global:defaultviservers`，显示所有连接的服务器。
- 2 （可选）如有必要，可以运行以下命令确保您已连接到 Trust Authority 集群的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 3 将 `Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA` 信息分配给变量。

例如：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

如果按顺序执行这些任务，则之前已将 `Get-TrustAuthorityCluster` 信息分配给了变量（例如，`$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`）。

此变量获取给定 Trust Authority 集群（在本例中为 \$vTA）中的可信密钥提供程序。

**注** 如果您有多个可信密钥提供程序，请使用如下类似命令选择一个所需的可信密钥提供程序：

```
Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
<The trusted key providers listing is displayed.>
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA | Select-Object -Last 1
```

使用 `Select-Object -Last 1` 选择列表中的最后一个可信密钥提供程序。

- 4 要生成 CSR，请使用 `New-TrustAuthorityKeyProviderClientCertificateCSR cmdlet`。

例如：

```
New-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp
```

此时将显示 CSR。您还可以使用 `Get-TrustAuthorityKeyProviderClientCertificateCSR -KeyProvider $kp cmdlet` 获取 CSR。

- 5 要获取签名证书，请将 CSR 提交给密钥服务器供应商。

证书必须采用 PEM 格式。如果证书以非 PEM 的格式返回，请使用 `openssl` 命令将其转换为 PEM。例如：

- 要将证书从 CRT 转换为 PEM 格式，请执行以下命令：

```
openssl x509 -in clientcert.crt -out clientcert.pem -outform PEM
```

- 要将证书从 DER 转换为 PEM 格式，请执行以下命令：

```
openssl x509 -inform DER -in clientcert.der -out clientcert.pem
```

- 6 从密钥服务器供应商收到签名证书后，使用 `Set-TrustAuthorityKeyProviderClientCertificate cmdlet` 将证书上载到密钥服务器。

例如：

```
Set-TrustAuthorityKeyProviderClientCertificate -KeyProvider $kp -CertificateFilePath
<path/tp/certfile.pem>
```

## 结果

可信密钥提供程序与密钥服务器建立了信任。

## 导出 Trust Authority 集群信息

要使受信任集群能够连接到 vSphere Trust Authority 集群，必须以文件的形式导出 Trust Authority 集群的服务信息，然后将该文件导入到受信任集群。必须保证此文件的机密性，并安全地进行传输。

如果按顺序执行这些任务，您仍会连接到 Trust Authority 集群的 vCenter Server。

**注** 请将导出的服务信息文件存储在安全的位置，以防必须还原 vSphere Trust Authority 配置。

## 前提条件

- 启用 Trust Authority 管理员。
- 启用 Trust Authority 状态。
- 收集有关要信任的 ESXi 主机和 vCenter Server 的信息。
- 将受信任主机信息导入到 Trust Authority 集群。
- 在 Trust Authority 集群上创建密钥提供程序。

## 步骤

- 1 确保您已连接到 Trust Authority 集群的 vCenter Server。例如，可以输入 `$global:defaultviservers`，显示所有连接的服务器。
- 2 （可选）如有必要，可以运行以下命令确保您已连接到 Trust Authority 集群的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustAuthorityCluster_VC_ip_address -User trust_admin_user
-Password 'password'
```

- 3 要导出 Trust Authority 集群的证明服务和密钥提供程序服务信息，请运行 `Export-TrustAuthorityServicesInfo` cmdlet。

例如，以下命令将服务信息导出到 `clsettings.json` 文件。如果按顺序执行这些任务，则之前已将 `Get-TrustAuthorityCluster` 信息分配给了变量（例如，`$vTA = Get-TrustAuthorityCluster 'vTA Cluster'`）。

```
Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA -FilePath
C:\vta\clsettings.json
```

将创建此文件。

## 结果

将创建包含 Trust Authority 集群信息的文件。

## 示例：导出 Trust Authority 集群信息

此示例显示了如何使用 PowerCLI 导出 Trust Authority 集群服务信息。下表显示了所使用的示例组件和值。

表 9-9. vSphere Trust Authority 设置示例

组件	值
变量 \$vTA	Get-TrustAuthorityCluster 'vTA Cluster'
Trust Authority 集群的 vCenter Server	192.168.210.22
Trust Authority 管理员	trustedadmin@vsphere.local

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.210.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

PS C:\Users\Administrator.CORP> Export-TrustAuthorityServicesInfo -TrustAuthorityCluster $vTA
-FilePath C:\vta\clsettings.json

Mode                LastWriteTime         Length Name
----                -
-a----          10/16/2019   9:59 PM           8177 clsettings.json
```

#### 后续步骤

继续将 [Trust Authority](#) 集群信息导入到受信任主机。

## 将 Trust Authority 集群信息导入到受信任主机

将 vSphere Trust Authority 集群信息导入到受信任集群后，受信任主机将开始使用 Trust Authority 集群执行证明过程。

#### 前提条件

- 启用 [Trust Authority](#) 管理员。
- 启用 [Trust Authority](#) 状态。
- 收集有关要信任的 [ESXi](#) 主机和 [vCenter Server](#) 的信息。
- 将受信任主机信息导入到 [Trust Authority](#) 集群。
- 在 [Trust Authority](#) 集群上创建密钥提供程序。
- 导出 [Trust Authority](#) 集群信息。

#### 步骤

- 1 确保您已经以 [Trust Authority](#) 管理员身份连接到受信任集群的 [vCenter Server](#)。

例如，可以输入 `$global:defaultviservers`，显示所有连接的服务器。

- 2 (可选) 如有必要, 可以运行以下命令确保您已连接到受信任集群的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password
'password'
```

**注** 或者, 也可以启动另一个 PowerCLI 会话以连接到受信任集群的 vCenter Server。

- 3 验证受信任集群的状态是否为已禁用。

```
Get-TrustedCluster
```

“State” 显示为 “Disabled”。

- 4 将 Get-TrustedCluster 信息分配给变量。

例如, 以下命令将集群 Trusted Cluster 的信息分配给变量 \$TC。

```
$TC = Get-TrustedCluster -Name 'Trusted Cluster'
```

- 5 通过回显变量验证变量的值。

例如:

```
$TC
```

此时将显示 Get-TrustedCluster 信息。

- 6 要将 Trust Authority 集群信息导入到 vCenter Server, 请运行 Import-TrustAuthorityServicesInfo cmdlet。

例如, 以下命令从之前在导出 Trust Authority 集群信息中导出的 clsettings.json 文件导入服务信息。

```
Import-TrustAuthorityServicesInfo -FilePath C:\vta\clsettings.json
```

系统将显示确认提示予以响应。

```
Confirmation
Importing the TrustAuthorityServicesInfo into Server 'ip_address'. Do you want to proceed?

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):
```

- 7 在确认提示处, 按 Enter。(默认值为 **y**。)

此时将显示 Trust Authority 集群中主机的服务信息。

- 8 要启用受信任集群, 请运行 Set-TrustedCluster cmdlet。

例如:

```
Set-TrustedCluster -TrustedCluster $TC -State Enabled
```

系统将显示确认提示响应。

```
Confirmation
Setting TrustedCluster 'cluster' with new TrustedState 'Enabled'. Do you want to proceed?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"):
```

如果受信任集群未处于正常状态，则在确认消息之前会显示以下警告消息：

```
WARNING: The TrustedCluster 'cluster' is not healthy in its TrustedClusterAppliedStatus.
This cmdlet will automatically remediate the TrustedCluster.
```

## 9 在确认提示处，按 Enter。（默认值为 **y**。）

受信任集群已启用。

**注** 也可以通过分别启用证明服务和密钥提供程序服务来启用受信任集群。使用 `Add-TrustedClusterAttestationServiceInfo` 和 `Add-TrustedClusterKeyProviderServiceInfo` 命令。例如，以下命令为包含两个可信密钥提供程序服务和两个证明服务的集群 `Trusted Cluster` 启用这些服务，一次启用一个。

```
Add-TrustedClusterAttestationServiceInfo -TrustedCluster 'Trusted Cluster'
-AttestationServiceInfo (Get-AttestationServiceInfo | Select-Object -index 0,1)
Add-TrustedClusterKeyProviderServiceInfo -TrustedCluster 'Trusted Cluster'
-KeyProviderServiceInfo (Get-KeyProviderServiceInfo | Select-Object -index 0,1)
```

## 10 验证是否已在受信任集群中配置证明服务和密钥提供程序服务。

### a 将 `Get-TrustedCluster` 信息分配给变量。

例如，以下命令将集群 `Trusted Cluster` 的信息分配给变量 `$TC`。

```
$TC = Get-TrustedCluster -Name 'Trusted Cluster'
```

### b 验证是否已配置证明服务。

```
$tc.AttestationServiceInfo
```

此时将显示证明服务信息。

### c 验证是否已配置密钥提供程序服务。

```
$tc.KeyProviderServiceInfo
```

此时将显示密钥提供程序服务信息。

## 结果

受信任集群中的 ESXi 受信任主机开始使用 `Trust Authority` 集群执行证明过程。

## 示例：将 Trust Authority 集群信息导入到受信任主机

此示例显示了如何将 Trust Authority 集群服务信息导入到受信任集群。下表显示了所使用的示例组件和值。

**表 9-10. vSphere Trust Authority 设置示例**

组件	值
受信任集群的 vCenter Server	192.168.110.22
Trust Authority 管理员	trustedadmin@vsphere.local
受信任集群名称	受信任集群
Trust Authority 集群中的 ESXi 主机	192.168.210.51 和 192.168.210.52
变量 \$TC	Get-TrustedCluster -Name 'Trusted Cluster'

```
PS C:\Users\Administrator.CORP> Disconnect-VIServer -server * -Confirm:$false
PS C:\Users\Administrator.CORP> Connect-VIServer -server 192.168.110.22 -User
trustedadmin@vsphere.local -Password 'VMware1!'

Name                               Port  User
----                               -
192.168.110.22                    443   VSPHERE.LOCAL\trustedadmin

PS C:\Users\Administrator.CORP> Get-TrustedCluster

Name          State      Id
----          -
Trusted Cluster Disabled   TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $TC

Name          State      Id
----          -
Trusted Cluster Disabled   TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> Import-TrustAuthorityServicesInfo -FilePath
C:\vta\clsettings.json

Confirmation
Importing the TrustAuthorityServicesInfo into Server '192.168.110.22'. Do you want to proceed?
[Y] Yes  [A] Yes to All  [N] No  [L] No to All  [S] Suspend  [?] Help (default is "Y"): y

ServiceAddress      ServicePort      ServiceGroup
-----
192.168.210.51      443              host-13:86f7ab6c-ad6f-4606-...
192.168.210.52      443              host-16:86f7ab6c-ad6f-4606-...
192.168.210.51      443              host-13:86f7ab6c-ad6f-4606-...
192.168.210.52      443              host-16:86f7ab6c-ad6f-4606-...

PS C:\Users\Administrator.CORP> Set-TrustedCluster -TrustedCluster $TC -State Enabled
```



```

Confirmation
Setting TrustedCluster 'Trusted Cluster' with new TrustedState 'Enabled'. Do you want to
proceed?
[Y] Yes   [A] Yes to All   [N] No   [L] No to All   [S] Suspend   [?] Help (default is "Y"):

Name                      State                Id
----                      -
Trusted Cluster           Enabled              TrustedCluster-domain-c8

PS C:\Users\Administrator.CORP> $TC = Get-TrustedCluster -Name 'Trusted Cluster'
PS C:\Users\Administrator.CORP> $tc.AttestationServiceInfo

ServiceAddress            ServicePort          ServiceGroup
-----
192.168.210.51            443                  host-13:dc825986-73d2-463c-...
192.168.210.52            443                  host-16:dc825986-73d2-463c-...

PS C:\Users\Administrator.CORP> $tc.KeyProviderServiceInfo

ServiceAddress            ServicePort          ServiceGroup
-----
192.168.210.51            443                  host-13:dc825986-73d2-463c-...
192.168.210.52            443                  host-16:dc825986-73d2-463c-...

```

## 后续步骤

继续使用 [vSphere Client](#) 为受信任主机配置可信密钥提供程序或使用命令行为受信任主机配置可信密钥提供程序。

## 使用 vSphere Client 为受信任主机配置可信密钥提供程序

可以使用 vSphere Client 配置可信密钥提供程序。

### 前提条件

- 启用 [Trust Authority](#) 管理员。
- 启用 [Trust Authority](#) 状态。
- 收集有关要信任的 [ESXi](#) 主机和 [vCenter Server](#) 的信息。
- 将受信任主机信息导入到 [Trust Authority](#) 集群。
- 在 [Trust Authority](#) 集群上创建密钥提供程序。
- 导出 [Trust Authority](#) 集群信息。
- 将 [Trust Authority](#) 集群信息导入到受信任主机。

### 步骤

- 1 使用 vSphere Client 连接到受信任集群的 vCenter Server。
- 2 以 vCenter Server 管理员身份登录，或以具 [加密操作.管理密钥服务器](#) 特权的 [管理员身份](#) 登录。

- 3 选择 vCenter Server，然后选择**配置**。
- 4 在**安全**下，选择**密钥提供程序**。
- 5 选择**添加可信密钥提供程序**。

可用的可信密钥提供程序显示为“已连接”状态。

- 6 选择可信密钥提供程序，然后单击**添加密钥提供程序**。

该可信密钥提供程序显示为“受信任”和“已连接”。如果这是您添加的第一个可信密钥提供程序，则会将其标记为默认提供程序。

---

**注** 过一会儿后，所有主机才能获取密钥提供程序，vCenter Server 才会更新缓存。由于信息传播的方式，您可能需要等待几分钟后，才能使用密钥提供程序在某些主机上执行密钥操作。

---

## 结果

ESXi 受信任主机现在可以执行加密操作，例如，创建加密虚拟机。

## 后续步骤

使用可信密钥提供程序对虚拟机进行加密与在 vSphere 6.5 中首次提供的虚拟机加密用户体验看起来一样。请参见第 10 章在 [vSphere 环境中使用加密](#)。

## 使用命令行为受信任主机配置可信密钥提供程序

可以使用命令行配置可信密钥提供程序。可以为 vCenter Server 或在 vCenter 对象层次结构中的集群级别或集群文件夹级别配置默认可信密钥提供程序。

### 前提条件

- 启用 Trust Authority 管理员。
- 启用 Trust Authority 状态。
- 收集有关要信任的 ESXi 主机和 vCenter Server 的信息。
- 将受信任主机信息导入到 Trust Authority 集群。
- 在 Trust Authority 集群上创建密钥提供程序。
- 导出 Trust Authority 集群信息。
- 将 Trust Authority 集群信息导入到受信任主机。

在受信任集群上，您必须具有包含**加密操作.管理 KMS** 特权的角色。

### 步骤

- 1 确保您已经以管理员身份连接到受信任集群的 vCenter Server。

例如，可以输入 `$global:defaultviservers`，显示所有连接的服务器。

- 2 （可选）如有必要，可以运行以下命令确保您已连接到受信任集群的 vCenter Server。

```
Disconnect-VIServer -server * -Confirm:$false
Connect-VIServer -server TrustedCluster_VC_ip_address -User admin_user -Password 'password'
```

- 3 获取可信密钥提供程序。

```
Get-KeyProvider
```

可以使用 `-Name` *keyprovider* 选项指定单个可信密钥提供程序。

- 4 将 `Get-KeyProvider` 可信密钥提供程序信息分配给变量。

例如，以下命令将信息分配给变量 `$workload_kp`。

```
$workload_kp = Get-KeyProvider
```

如果您有多个可信密钥提供程序，则可以使用 `Select-Object` 选择其中一个密钥提供程序。

```
$workload_kp = Get-KeyProvider | Select-Object -Index 0
```

- 5 注册可信密钥提供程序。

```
Register-KeyProvider -KeyProvider $workload_kp
```

要注册其他可信密钥提供程序，请重复步骤 4 和 5。

---

**注** 过一会儿后，所有主机才能获取密钥提供程序，vCenter Server 才会更新缓存。由于信息传播的方式，您可能需要等待几分钟后，才能使用密钥提供程序在某些主机上执行密钥操作。

---

- 6 设置要使用的默认可信密钥提供程序。

- a 要在 vCenter Server 级别设置默认密钥提供程序，请运行以下命令。

```
Set-KeyProvider -KeyProvider $workload_kp -DefaultForSystem
```

- b 要在集群级别设置密钥提供程序，请运行以下命令。

例如，以下命令为集群 `Trusted Cluster` 设置密钥提供程序。

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'Trusted Cluster'
```

- c 要在集群文件夹级别设置密钥提供程序，请运行以下命令。

例如，以下命令为在 `workLoad` 数据中心创建的集群文件夹 `TC Folder` 设置密钥提供程序。

```
Add-EntityDefaultKeyProvider -KeyProvider $workload_kp -Entity 'TC Folder'
```

## 后续步骤

使用可信密钥提供程序对虚拟机进行加密与在 vSphere 6.5 中首次提供的虚拟机加密用户体验看起来一样。请参见第 10 章 在 vSphere 环境中使用加密。

## 管理 vSphere 环境中的 vSphere Trust Authority

配置 vSphere Trust Authority 后，可以执行其他操作，例如，停止和启动服务、将主机添加到集群以及查看 Trust Authority 集群的状态。

可以使用 vSphere Client、API 和 PowerCLI cmdlet 执行任务。请参见《vSphere Web Services SDK 编程指南》、VMware PowerCLI 文档和 VMware PowerCLI Cmdlet 参考文档。

### 启动、停止和重新启动 vSphere Trust Authority 服务

可以通过使用 vSphere Client 启动、停止和重新启动 vSphere Trust Authority 服务。

构成 vSphere Trust Authority 的服务包括证明服务 (attestd) 和密钥提供程序服务 (kmsd)。

#### 步骤

- 1 使用 vSphere Client 连接到 vSphere Trust Authority 集群的 vCenter Server。
- 2 以管理员身份登录。
- 3 浏览到 Trust Authority 集群中的 ESXi 主机。
- 4 选择**配置**，然后选择**系统**下的**服务**。
- 5 找到 attestd 服务和 kmsd 服务。
- 6 根据需要选择**重新启动**、**启动**或**停止**操作。

### 查看 Trust Authority 主机

可以使用 vSphere Client 查看为受信任集群配置的 vSphere Trust Authority 主机。

#### 步骤

- 1 使用 vSphere Client 连接到受信任集群的 vCenter Server。
- 2 以管理员身份登录。
- 3 选择 vCenter Server 实例。
- 4 单击**配置**选项卡，然后选择**安全**下的 **Trust Authority**。

此时将显示为受信任集群配置的 Trust Authority 集群中的 ESXi 主机。

### 查看 vSphere Trust Authority 集群状态

可以使用 vSphere Client 查看 vSphere Trust Authority 集群的状态。状态为“已启用”或“已禁用”。

启用 Trust Authority 集群状态后，受信任集群中的受信任主机可以与证明服务和密钥提供程序服务进行通信。

#### 步骤

- 1 使用 vSphere Client 连接到 Trust Authority 集群的 vCenter Server。
- 2 以管理员身份登录。

- 3 在对象层次结构中选择 Trust Authority 集群。
- 4 单击**配置**选项卡，然后选择 **Trust Authority** 下的 **Trust Authority 集群**。  
状态显示为“已启用”或“已禁用”。

## 重新启动受信任主机服务

可以重新启动在受信任主机上运行的服务。

服务 kmxa 在 ESXi 受信任主机上运行。

### 前提条件

必须启用对 ESXi shell 的访问。请参见[使用 vSphere Client 激活对 ESXi Shell 的访问](#)。

### 步骤

- 1 使用 SSH 或其他远程控制台连接在 ESXi 受信任主机上启动会话。
- 2 以 root 用户身份登录。
- 3 运行下列命令。

```
/etc/init.d/kmxa restart
```

## 添加和移除 vSphere Trust Authority 主机

可以使用 VMware 提供的脚本在 vSphere Trust Authority 集群中添加和移除 ESXi 主机。

在 vSphere 7.0 中，可以使用 VMware 提供的脚本在现有的 vSphere Trust Authority 集群或受信任集群中添加和移除 ESXi 主机。在 vSphere 7.0 Update 1 及更高版本中，可以使用修复功能将 ESXi 主机添加到现有的受信任集群。请参见[使用 vSphere Client 将主机添加到受信任集群](#)和[使用 CLI 将主机添加到受信任集群](#)。

在 vSphere 7.0 Update 1 及更高版本中，仍然需要使用脚本将 ESXi 主机添加到现有的 Trust Authority 集群。请参见 VMware 知识库文章，网址为 <https://kb.vmware.com/s/article/77234> 和 <https://kb.vmware.com/s/article/77146>。

## 使用 vSphere Client 将主机添加到受信任集群

您可以使用 vSphere Client 将 ESXi 主机添加到现有的受信任集群。

在最初配置了受信任集群后，您可能需要添加更多 ESXi 主机。但是，将主机添加到受信任集群时，必须执行额外的修复步骤。修复受信任集群时，请确保其所需的配置状态与其应用的配置相匹配。

在 vSphere 7.0 所发布的第一版 vSphere Trust Authority 中，您可以运行脚本以将主机添加到现有的受信任集群。在 vSphere 7.0 Update 1 及更高版本中，您可以使用修复功能将主机添加到受信任集群。在 vSphere 7.0 Update 1 及更高版本中，仍必须使用脚本将主机添加到现有的 Trust Authority 集群。请参见[添加和移除 vSphere Trust Authority 主机](#)。

### 前提条件

受信任集群的 vCenter Server 必须运行 vSphere 7.0 Update 1 或更高版本。

如果要添加的 ESXi 主机的 ESXi 版本或 TPM 硬件类型不同于您最初为受信任集群配置的版本或类型，则需要执行额外的步骤。您必须导出此信息并将其导入到 vSphere Trust Authority 集群中。请参见[收集有关信任的 ESXi 主机和 vCenter Server 的信息](#)和将受信任主机信息导入到 Trust Authority 集群。

所需特权：请参见[常见任务的所需 vCenter Server 特权](#)中的“添加主机任务”。

#### 步骤

- 1 使用 vSphere Client 连接到受信任集群的 vCenter Server。
- 2 以 Trust Authority 管理员的身份登录。
- 3 导航到一个受信任集群。
- 4 在配置选项卡上，选择配置 > 快速入门。
- 5 在添加主机卡片中，单击添加。
- 6 按照提示操作。
- 7 在 Trust Authority 选项卡上，单击修复。
- 8 要验证受信任集群是否处于正常状态，请单击检查运行状况。

## 使用 CLI 将主机添加到受信任集群

您可以使用命令行将 ESXi 主机添加到现有的受信任集群。

在最初配置了受信任集群后，您可能需要添加更多 ESXi 主机。但是，将主机添加到受信任集群时，必须执行额外的修复步骤。修复受信任集群时，请确保其所需的配置状态与其应用的配置相匹配。

在 vSphere 7.0 所发布的第一版 vSphere Trust Authority 中，您可以运行脚本以将主机添加到现有的受信任集群。在 vSphere 7.0 Update 1 及更高版本中，可以使用修复功能添加受信任主机。在 vSphere 7.0 Update 1 及更高版本中，仍必须使用脚本将主机添加到现有的 Trust Authority 集群。请参见[添加和移除 vSphere Trust Authority 主机](#)。

#### 前提条件

- 受信任集群的 vCenter Server 必须运行 vSphere 7.0 Update 1 或更高版本。
- 需要 PowerCLI 12.1.0 或更高版本。
- 所需特权：请参见[常见任务的所需 vCenter Server 特权](#)中的“添加主机任务”。

#### 步骤

- 1 使用常规步骤将 ESXi 主机添加到受信任集群。
- 2 在 PowerCLI 会话中，运行 Connect-VIServer cmdlet，以 Trust Authority 管理员身份连接到受信任集群的 vCenter Server。

```
Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'
```

- 3 要检查受信任集群的状态，请运行 `Get-TrustedClusterAppliedStatus` PowerCLI cmdlet。

```
Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
```

- 4 如果受信任集群处于不正常状态，请使用 `-Remediate` 参数运行 `Set-TrustedCluster` cmdlet。

```
Set-TrustedCluster -TrustedCluster 'TrustedCluster' -Remediate
```

- 5 要验证受信任集群是否处于正常状态，请重新运行 `Get-TrustedClusterAppliedStatus` cmdlet。

```
Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'
```

## 取消配置受信任集群中的受信任主机

您可以从受信任集群中移除或取消配置受信任主机。您可以从受信任集群中取消配置一个或全部受信任主机，具体取决于具体情况。

取消配置受信任主机时，修复功能会将受信任主机的所需状态设置为它移动到的非受信任集群的所需状态。取消配置的受信任主机将成为普通主机。受信任集群（从中移出了受信任主机）继续具有所需的状态配置，并且仍然作为受信任集群运行。

如果从受信任集群中移除所有受信任主机，将取消配置受信任集群。您可以从受信任主机和受信任集群中移除所需的状态配置和应用的配置，然后将所有受信任主机移至非受信任集群。

您可以在您的环境中重用已取消配置的受信任主机。例如，您可以在非受信任基础架构容量中重用主机，或将主机重用为 vSphere Trust Authority 主机。您可以在同一 vCenter Server 中或不同 vCenter Server 中使用已取消配置的主机。

有关受信任集群配置和运行状况的详细信息，请参见[检查和修复受信任集群的运行状况](#)。

### 前提条件

- 受信任集群的 vCenter Server 必须运行 vSphere 7.0 Update 1 或更高版本。
- 如果使用 PowerCLI，则需要 12.1.0 或更高版本。

### 步骤

- 1 使用 vSphere Client 连接到受信任集群的 vCenter Server。
- 2 以 Trust Authority 管理员的身份登录。
- 3 导航到一个受信任集群。

#### 4 确定如何取消配置受信任集群中的受信任主机。

任务	步骤
保留受信任集群和剩余受信任主机的所需配置状态	<p>a 将主机置于维护模式，并将其移至新的空集群（即，集群中不包含任何主机）。</p> <p>b 退出主机上的维护模式。</p> <p>c 对于新的空集群（而不是受信任集群），请在 <b>Trust Authority</b> 选项卡上，单击 <b>修复</b>。</p> <p>修复将从移动的主机中移除受信任配置。受信任集群将保留其所需的状态配置。</p>
移除所有受信任主机的所需配置状态和已应用配置状态	<p>a 在 PowerCLI 会话中，运行 Connect-VIServer cmdlet，以 Trust Authority 管理员身份连接到受信任集群的 vCenter Server。</p> <pre>Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'</pre> <p>b 运行 Set-TrustedCluster cmdlet，例如：</p> <pre>Set-TrustedCluster -TrustedCluster 'TrustedCluster' -State Disabled</pre> <p>将从所有受信任主机中移除可信基础架构配置，受信任集群将移除它的所需状态配置。</p> <p>c 将所有主机置于维护模式并将它们移动到其他集群。</p> <p>d 退出主机上的维护模式。</p>

#### 5 要验证受信任集群是否处于正常状态，请单击受信任集群的 **Trust Authority** 选项卡上的 **检查运行状况**。

##### 后续步骤

如果不再打算证明 ESXi 主机或已取消配置的 ESXi 主机中的 TPM 硬件的特定版本，请更新 Trust Authority 集群的配置，以获得最佳安全性。请参见 VMware 知识库文章，网址为 <https://kb.vmware.com/s/article/77146>。

## 备份 vSphere Trust Authority 配置

使用配置 vSphere Trust Authority 时导出的文件作为 Trust Authority 备份。可以使用这些文件还原 Trust Authority 部署。请保证这些配置文件的机密性，并安全地进行传输。

大多数 vSphere Trust Authority 配置和状态信息存储在 ESXi 主机上的 ConfigStore 数据库中。用于备份 vCenter Server 实例的 vCenter Server 管理界面不会备份 vSphere Trust Authority 的配置信息。如果您保存并安全地存储在设置 vSphere Trust Authority 环境时导出的配置文件，则您将拥有还原 vSphere Trust Authority 配置所需的信息。如果必须生成这些信息，请参见 [收集有关要信任的 ESXi 主机和 vCenter Server 的信息](#)。

## 更改可信密钥提供程序的主要密钥

可以更改可信密钥提供程序的主密钥，例如，当您要轮换使用的主密钥时。

有关密钥生命周期的指导，请参见 [虚拟机加密最佳做法](#)。



## 前提条件

在要用作可信密钥提供程序的新主密钥的密钥服务器 (KMS) 上创建并激活密钥。此密钥可封装此可信密钥提供程序使用的其他密钥。有关创建密钥的详细信息，请参见 KMS 供应商文档。

## 步骤

- 1 运行 Set-TrustAuthorityKeyProvider 命令。

例如：

```
Set-TrustAuthorityKeyProvider -MasterKeyId Key-ID
```

- 2 验证密钥提供程序的状态。

- a 将 Get-TrustAuthorityCluster 信息分配给变量。

例如：

```
$vTA = Get-TrustAuthorityCluster 'vTA Cluster'
```

- b 将 Get-TrustAuthorityKeyProvider -TrustAuthorityCluster \$vTA 信息分配给变量。

例如：

```
$kp = Get-TrustAuthorityKeyProvider -TrustAuthorityCluster $vTA
```

- c 通过运行 \$kp.Status 验证密钥提供程序的状态。

例如：

```
$kp.Status

KeyProviderId Health HealthDetails ServerStatus
-----
domain-c8-kp4    Ok {} {IP_address}
```

运行状况为“Ok”表示密钥提供程序正常运行。

## 结果

新的主要密钥用于任何新的加密操作。使用旧主要密钥加密的数据仍使用旧密钥进行解密。

## 受信任主机证明报告

在 vSphere Trust Authority 中，vCenter Server 会验证和报告受信任主机的证明状态。可以使用 vSphere Client 查看受信任主机的证明状态。

### 什么是 vSphere Trust Authority 证明报告

vSphere Trust Authority 对受信任主机使用远程证明，以证明其引导软件的真实性和完整性。证明会验证受信任主机是否运行的是真实的 VMware 软件或 VMware 签名的合作伙伴软件。受信任集群的 vCenter Server 与受信任主机进行通信，以获取内部证明报告。证明报告指定受信任主机是否经过了在 Trust Authority 集群上所运行认证服务的证明。如果受信任主机未经过证明，则证明报告也会指定一条错误消息。vSphere Client 显示受信任主机的证明状态，以及 vSphere Trust Authority 或 vCenter Server 是否证明了主机。

### 已通过证明状态

已通过证明状态表示受信任主机已经过 vSphere Trust Authority 证明服务的证明，并为 vCenter Server 提供内部证明报告。

### 未通过证明状态

未通过证明状态表示受信任主机无法使用任何 vSphere Trust Authority 证明服务证明。vCenter Server 内部证明报告包含受信任主机尝试经过其证明的证明服务报告的错误。

### 处理未证明的受信任主机

如果受信任主机未经证明，受信任主机上运行的虚拟机（包括加密虚拟机）仍可访问。无法打开未经证明的受信任主机上的虚拟机电源。但是，仍可以添加未加密的虚拟机。如果受信任主机未经证明，请采取措施解决证明问题。请参见[对受信任主机认证问题进行故障排除](#)。

### 多个 Trust Authority 主机和证明报告

如果配置了多个 Trust Authority 主机，则每个主机可能有多个可用的证明报告。报告状态时，vSphere Client 将显示所找到的第一个“已经证明”报告中的状态。如果不存在任何“已经证明”报告，则 vSphere Client 将显示所找到的第一个“未经证明”报告中的错误。

即使配置了多个 Trust Authority 主机，vSphere Client 也会仅显示一个证明报告中的状态以及可能的错误消息。

### 查看受信任集群证明状态

可以使用 vSphere Client 查看受信任主机的证明状态。

#### 前提条件

- 受信任主机和 vSphere Trust Authority 主机都必须运行 ESXi 7.0 Update 1 或更高版本。
- 相应集群的 vCenter Server 主机必须运行 vSphere 7.0 Update 1 或更高版本。

#### 步骤

- 1 使用 vSphere Client 连接到受信任集群的 vCenter Server。

## 2 以管理员身份登录。

可以 Trust Authority 管理员或 vSphere 管理员身份登录。

## 3 导航到数据中心，然后单击[监控](#)选项卡。

## 4 单击[安全](#)。

## 5 在“认证”列中查看受信任主机的状态，并在“消息”列中阅读相应的消息。

### 后续步骤

如果出现错误，请参见[对受信任主机认证问题进行故障排除](#)。

## 对受信任主机认证问题进行故障排除

vSphere Trust Authority 证明报告为对受信任主机证明错误进行故障排除提供了起点。

### 步骤

#### 1 查看受信任集群证明状态。

#### 2 使用下表对错误进行故障排除和解决错误。

错误	原因和解决方案
未配置证明服务。	尚未配置证明服务。通过使用修复操作，将受信任主机配置为使用证明服务。请参见 <a href="#">修复受信任集群</a> 。
没有可用的 TPM2 设备。	安装受信任主机并将其配置为使用可信平台模块 (TPM)。请参见供应商文档。
无法检索 TPM2 认可的公钥或证书。	检查 TPM 是否受支持，以及是否具有有效的认可密钥。您可能需要联系 VMware 技术支持。
证明报告不可用。	受信任主机可能尚未完成证明。请等待几分钟，然后重新检查证明状态。
证明服务版本与请求不兼容。	将运行证明服务的 Trust Authority 主机更新为 vSphere 7.0 Update 1 或更高版本。
由于未启用安全引导，证明失败。	检查受信任主机是否配置为使用安全引导。请参见 <a href="#">ESXi 主机的 UEFI 安全引导</a> 。
证明无法识别远程软件版本。	将受信任主机的基础映像信息导入到证明服务。请参见 <a href="#">将受信任主机信息导入到 Trust Authority 集群</a> 。
由于需要 TPM 证书，证明失败。	检查 TPM 是否受支持。或者，运行以下 PowerCLI cmdlet，修改 <code>com.vmware.esx.attestation.tpm2.settings</code> ，将 <code>requireCertificateValidation</code> 设置为 <code>false</code> 。 <pre>Set-TrustAuthorityTpm2AttestationSettings -TrustAuthorityCluster TrustedCluster -RequireCertificateValidation:\$false -RequireEndorsementKey:\$true</pre>
由于 TPM 未知，证明失败。	将 TPM 认可密钥导入到证明服务。请参见 <a href="#">将受信任主机信息导入到 Trust Authority 集群</a> 。
错误: <code>vapi.send.failed</code> 。	<code>kmxa</code> 服务可能未在受信任主机上运行，或者 <code>kmxa</code> 服务无法联系证明服务。确保 <code>kmxa</code> 服务已启动。此外，还请检查证明服务是否正在运行。请参见 <a href="#">重新启动受信任主机服务</a> 。

## 检查和修复受信任集群的运行状况

您可以检查和验证受信任集群的运行状况。如果受信任集群的配置不正常，则必须解决配置不一致问题。可以通过修复受信任集群进行解决。修复受信任集群时，请确保受信任集群中的所有受信任主机都具有相同的受信任配置。

受信任集群包括由 Trust Authority 集群远程证明的受信任 ESXi 主机的 vCenter Server 集群。最初配置 vSphere Trust Authority 时，必须将 Trust Authority 服务信息从 Trust Authority 集群导入到受信任集群。受信任集群使用该组件配置连接在 Trust Authority 集群上运行的密钥提供程序服务和证明服务。有关配置受信任集群这方面的详细信息，请参见[将 Trust Authority 集群信息导入到受信任主机](#)。配置受信任集群后，可以检查并修复其运行状况。

### 检查受信任集群的运行状况

检查受信任集群的运行状况依赖于以下要素。

#### 所需状态配置

所需状态配置基于导入到受信任集群的 Trust Authority 服务信息。所需状态配置是受信任集群的“可信来源”。可将所需状态配置视为设置受信任集群时最初创建的配置。

#### 已应用配置

已应用配置是指为受信任集群配置了特定证明服务和密钥提供程序服务的注册。已应用配置是受信任集群当前正在运行的配置。可以将已应用配置视为“运行时”配置。所需状态配置应与已应用配置相匹配。但是，如果已应用配置与所需状态配置不一致，则受信任集群将视为“不正常”。处于非正常状态的受信任集群可能会出现性能下降或根本无法正常运行的情况。

此运行状况检查并不指示受信任集群或 vSphere Trust Authority 基础架构的整体运行状况。此运行状况检查仅将受信任集群的所需状态配置与已应用配置进行比较。

### 修复受信任集群

修复是 vSphere Trust Authority 解决受信任集群不一致配置所实施的过程。受信任集群的配置可能会在一段时间内或由于其他操作错误而变得不一致。

修复按以下方式执行：

- 检查受信任集群的运行状况。
- 如果受信任集群不正常，则进行修复。

可以使用 vSphere Client 或 CLI 检查受信任集群的运行状况。请参见[检查受信任集群的运行状况](#)。此外，也可以使用 vSphere Client 或 CLI 修复受信任集群。请参见[修复受信任集群](#)。

---

**注** 将主机添加到现有受信任集群时，修复也是要使用的相应过程。请参见[使用 vSphere Client 将主机添加到受信任集群](#)和[使用 CLI 将主机添加到受信任集群](#)。

---

## 检查受信任集群的运行状况

您可以使用 vSphere Client 或命令行检查受信任集群的运行状况。

### 前提条件

- 受信任集群的 vCenter Server 必须运行 vSphere 7.0 Update 1 或更高版本。
- 如果使用 PowerCLI，则需要 12.1.0 或更高版本。

### 步骤

- 1 检查受信任集群的运行状况。

工具	步骤
vSphere Client	<ol style="list-style-type: none"> <li>a 使用 vSphere Client 连接到受信任集群的 vCenter Server。</li> <li>b 以 Trust Authority 管理员的身份登录。</li> <li>c 导航到一个受信任集群，选择<b>配置</b>，然后选择 <b>Trust Authority</b>。</li> <li>d 单击<b>检查运行状况</b>。</li> </ol>
CLI	<ol style="list-style-type: none"> <li>a 在 PowerCLI 会话中，运行 Connect-VIServer cmdlet，以 Trust Authority 管理员身份连接到受信任集群的 vCenter Server。 <div data-bbox="679 900 1377 953" data-label="Text"> <pre>Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'</pre> </div> </li> <li>b 运行 Get-TrustedClusterAppliedStatus cmdlet，例如： <div data-bbox="679 1041 1297 1092" data-label="Text"> <pre>Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'</pre> </div> </li> </ol>

- 2 如果出现错误，请参见[修复受信任集群](#)。

## 修复受信任集群

可以使用 vSphere Client 或命令行修复受信任集群的配置。

### 前提条件

受信任集群的 vCenter Server 必须运行 vSphere 7.0 Update 1 或更高版本。

### 步骤

- 1 连接到受信任集群的 vCenter Server。

工具	步骤
vSphere Client	<ol style="list-style-type: none"> <li>a 使用 vSphere Client 连接到受信任集群的 vCenter Server。</li> <li>b 以 Trust Authority 管理员的身份登录。</li> </ol>
CLI	<p>在 PowerCLI 会话中，运行 Connect-VIServer cmdlet，以 Trust Authority 管理员身份连接到受信任集群的 vCenter Server。</p> <div data-bbox="639 1810 1339 1862" data-label="Text"> <pre>Connect-VIServer -server TrustedCluster_VC_ip_address -User trust_admin_user -Password 'password'</pre> </div>

## 2 修复受信任集群，然后重新检查受信任集群运行状况。

工具	步骤
vSphere Client	<ol style="list-style-type: none"><li>导航到一个受信任集群。</li><li>选择<b>配置</b>，然后选择 <b>Trust Authority</b>。</li><li>单击<b>修复</b>。</li><li>单击<b>检查运行状况</b>。</li></ol>
CLI	<ol style="list-style-type: none"><li>运行带 -Remediate 参数的 Set-TrustedCluster cmdlet，例如：<pre>Set-TrustedCluster -TrustedCluster 'TrustedCluster' -Remediate</pre></li><li>运行 Get-TrustedClusterAppliedStatus cmdlet，例如：<pre>Get-TrustedClusterAppliedStatus -TrustedCluster 'TrustedCluster'</pre></li></ol>

# 在 vSphere 环境中使用加密

# 10

无论使用标准密钥提供程序、可信密钥提供程序还是 vSphere Native Key Provider，在 vSphere 环境中使用加密都需要一些准备工作。

请参见以下信息将您的环境设置为使用密钥提供程序：

- 第 7 章 配置和管理标准密钥提供程序
- 第 8 章 配置和管理 vSphere Native Key Provider
- 配置 vSphere Trust Authority

设置环境后，可以使用 vSphere Client 创建加密虚拟机和虚拟磁盘，还可以对现有的虚拟机和磁盘进行加密。

可以使用 API 和 `crypto-utilCLI` 执行附加任务。请参见《vSphere Web Services SDK 编程指南》，获取 API 文档；参见 `crypto-util` 命令行帮助，了解有关该工具的详细信息。

本章讨论了以下主题：

- 创建加密存储策略
- 明确激活主机加密模式
- 使用 API 停用主机加密模式
- 创建加密虚拟机
- 克隆加密虚拟机
- 加密现有虚拟机或虚拟磁盘
- 解密加密虚拟机或虚拟磁盘
- 更改虚拟磁盘的加密策略
- 解决缺失加密密钥问题
- 解锁锁定的虚拟机
- 解决 ESXi 主机加密模式问题
- 重新激活 ESXi 主机加密模式
- 设置密钥服务器证书过期阈值
- vSphere 虚拟机加密和核心转储

- 在 ESXi 主机上激活和停用密钥持久性
- 使用 vSphere Client 对加密虚拟机进行重新加密
- 使用 vSphere Client 设置默认密钥提供程序
- 使用 CLI 设置默认密钥提供程序

## 创建加密存储策略

必须先创建加密存储策略，然后才能创建加密虚拟机。只要创建存储策略一次，即可在每次加密虚拟机或虚拟磁盘时分配该策略。

如果要将虚拟机加密与其他 I/O 筛选器配合使用，或在 vSphere Client 中使用[创建虚拟机存储策略](#)向导，请参见《vSphere 存储》文档，了解详细信息。

### 前提条件

- 建立与密钥提供程序的连接。

尽管您可以在未建立密钥提供程序连接的情况下创建虚拟机加密存储策略，但是只有建立与密钥提供程序的可信连接才能执行加密任务。

- 所需特权：[加密操作](#)、[管理加密策略](#)。

### 步骤

- 1 使用 vSphere Client 登录 vCenter Server。
- 2 选择主页，单击[策略和配置文件](#)，然后单击[虚拟机存储策略](#)。
- 3 单击[创建](#)。
- 4 选择 vCenter Server，输入策略名称，（可选）输入描述，然后单击[下一步](#)。
- 5 在[策略结构](#)页面上，选中[启用基于主机的角色](#)，然后单击[下一步](#)。
- 6 在[基于主机的服务](#)页面上，选择[使用存储策略组件](#)，从下拉菜单中选择[默认加密属性](#)，然后单击[下一步](#)。
- 7 在[存储兼容性](#)页面上，将[兼容保留](#)为选中状态，选择一个数据存储，然后单击[下一步](#)。
- 8 检查信息，然后单击[完成](#)。

### 结果

虚拟机加密存储策略将添加到列表中，并可在加密虚拟机时使用。

## 明确激活主机加密模式

如果要执行加密任务，例如，在 ESXi 主机上创建加密虚拟机，必须设置主机加密模式。大多数情况下，在执行加密任务时会自动激活主机加密模式。

有时，必须以显式方式开启加密模式。请参见[虚拟机加密任务的必备条件和必需特权](#)。



## 前提条件

所需特权：**加密操作.注册主机**

## 步骤

- 1 使用 vSphere Client 登录 vCenter Server。
- 2 浏览到 ESXi 主机，然后单击**配置**。
- 3 在“系统”下，单击**安全配置文件**。
- 4 在“主机加密模式”面板中，单击**编辑**。
- 5 选择已启用，然后单击**确定**。

## 使用 API 停用主机加密模式

如果用户拥有足够的特权，在用户执行加密任务时，将自动激活主机加密模式。激活主机加密模式之后，为了避免向技术支持人员发布敏感信息，会对所有核心转储进行加密。如果不再将虚拟机加密用于 ESXi 主机，则可停用加密模式。

为 ESXi 主机激活加密模式后，您可能需要将其停用。例如，您可能需要停用加密模式才能生成 ESXi 支持包（使用 `vm-support` 命令）。当主机上存在密钥材料时，无法使用主机加密模式切换（**主机 > 配置 > 安全配置文件 > 编辑主机加密模式**）。

通过调用 `CryptoManagerHostDisable` API 方法，可以使用 API 停用主机加密模式。

为 ESXi 主机定义的加密模式或状态包括：

- **pendingIncapable**：停用主机加密，即主机无法执行 vSphere 虚拟机加密操作。
- **incapable**：主机无法安全地接收敏感材料。
- **prepared**：主机已准备好接收敏感材料，但尚未设置主机密钥。
- **Safe**：主机经过安全加密（已激活），并设置主机密钥，即，可以执行 vSphere 虚拟机加密操作。

在主机关调用 `CryptoManagerHostDisable` 后，主机的加密状态将发生如下变化：

- 如果原始主机加密状态为 **incapable** 或 **prepared**，则主机加密状态将更改为 **incapable**。
- 如果原始主机加密状态为 **safe**，则主机加密状态将更改为 **pendingIncapable**。
- 如果主机加密状态为 **pendingIncapable**，则主机加密状态仍为 **pendingIncapable**。

此任务显示如何使用 vCenter Server Managed Object Browser（MOB）停用主机加密模式。有关使用 API 的详细信息，请参见 vSphere Web Services API 文档，网址为 <https://developer.vmware.com/apis/968/vsphere>。

## 步骤

- 1 以管理员身份登录到 vCenter Server。
- 2 从要停用其加密模式的 ESXi 主机取消注册所有已加密的虚拟机。

### 3 访问 vCenter Server 上的 MOB。

```
https://vcenter_server/mob
```

### 4 在主机上调用 CryptoManagerHostDisable 方法。

- a 在内容名称下，单击**内容**。
- b 在 rootFolder 下，单击 **group-D1 (Datacenters)**。
- c 在 childEntity 下，单击相应的数据中心。
- d 在 hostFolder 下，单击相应的主机。
- e 在 childEntity 下，单击相应的集群。
- f 在主机下，单击相应的主机。
- g 在 configManager 下，单击 **configManager**。
- h 在 cryptoManager 下，单击 **CryptoManagerHost-*number***。
- i 单击 **CryptoManagerHostDisable**。

主机加密状态将更改为 pendingIncapable 或 incapable，具体取决于其原始加密状态。

### 5 对要停用加密模式的其他主机重复步骤 4。

### 6 重新引导主机。

#### 结果

停用主机加密模式后，除非重新激活主机加密模式，否则无法执行加密操作，例如添加已加密虚拟机。

---

**注** 重新引导已停用加密模式的 ESXi 主机后，如果主机加密状态最初为 pendingIncapable，则主机加密状态仍为 pendingIncapable。要重新激活主机加密模式，请重新访问 vCenter Server MOB 并调用 ConfigureCryptoKey API 方法。重新激活主机加密模式时，如果主机加密状态为 pendingIncapable，请使用原始主机密钥 ID。

---

## 创建加密虚拟机

您可以使用 vSphere Client 创建加密虚拟机。

vSphere Client 按虚拟机加密存储策略筛选，从而简化了加密虚拟机的创建。

---

**注** 相比加密现有虚拟机，创建加密虚拟机速度更快，使用的存储资源更少。如果可能，请在创建过程中对虚拟机进行加密。

---

#### 前提条件

- 配置密钥提供程序并将其设置为默认值。
- 创建加密存储策略，或使用捆绑的示例，虚拟机加密策略。
- 确保已关闭虚拟机电源。

- 确认您拥有所需特权：
  - 加密操作.加密新项
  - 如果未启用主机加密模式，您还需要加密操作.注册主机。

#### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 在清单中选择一个对象（虚拟机的有效父对象），如 ESXi 主机或集群。
- 3 右键单击该对象，然后选择**新建虚拟机**。
- 4 按照提示创建加密虚拟机。

选项	操作
选择创建类型	创建新虚拟机。
选择名称和文件夹	指定虚拟机的唯一名称和目标位置。
选择计算资源	指定您拥有创建加密虚拟机特权的对象。请参见 <a href="#">虚拟机加密任务的必备条件和必需特权</a> 。
选择存储	选中 <b>加密此虚拟机</b> 复选框。将显示包括加密的虚拟机存储策略。选择一个虚拟机存储策略（捆绑的示例是虚拟机加密策略），然后选择兼容的数据存储。
选择兼容性	选择兼容性。只能将加密虚拟机迁移到兼容 ESXi 6.5 及更高版本的主机上。
选择客户机操作系统	选择您计划稍后安装在虚拟机上的客户机操作系统。
自定义硬件	自定义硬件，例如，通过更改磁盘大小或 CPU。 （可选）选择 <b>虚拟机选项</b> 选项卡，然后展开 <b>加密</b> 。选择要从加密中排除的磁盘。取消选择某个磁盘后，仅对虚拟机主目录以及任何选定的磁盘进行加密。 添加的任何新硬盘都会进行加密。您可以稍后更改各个硬盘的存储策略。
即将完成	检查信息，然后单击 <b>完成</b> 。

## 克隆加密虚拟机

克隆的加密虚拟机使用相同的密钥进行加密，除非您更改密钥。要更改密钥，可以使用 vSphere Client、PowerCLI 或 API。如果使用 PowerCLI 或 API，则可以在一个步骤中克隆加密的虚拟机并更改密钥。

可以在克隆期间执行以下操作。

- 从未加密的虚拟机或模板虚拟机创建加密虚拟机。
- 从加密虚拟机或模板虚拟机创建解密虚拟机。
- 使用不同于源虚拟机的密钥重新加密目标虚拟机。
- 从 vSphere 8.0 开始，对具有 vTPM 的虚拟机选择**替换**选项时，会以新的空白 vTPM 开始，该 vTPM 将获得自己的密钥和身份。

**注** vSphere 8.0 包含 `vpdx.clone.tpmProvisionPolicy` 高级设置，可将 vTPM 的默认克隆行为设置为“替换”。

可以从加密虚拟机创建即时克隆虚拟机，但需注意，即时克隆与源虚拟机共享相同的密钥。无法重新加密源虚拟机或即时克隆虚拟机上的密钥。

要使用 API 克隆加密计算机，请参见《vSphere Web Services SDK 编程指南》。

#### 前提条件

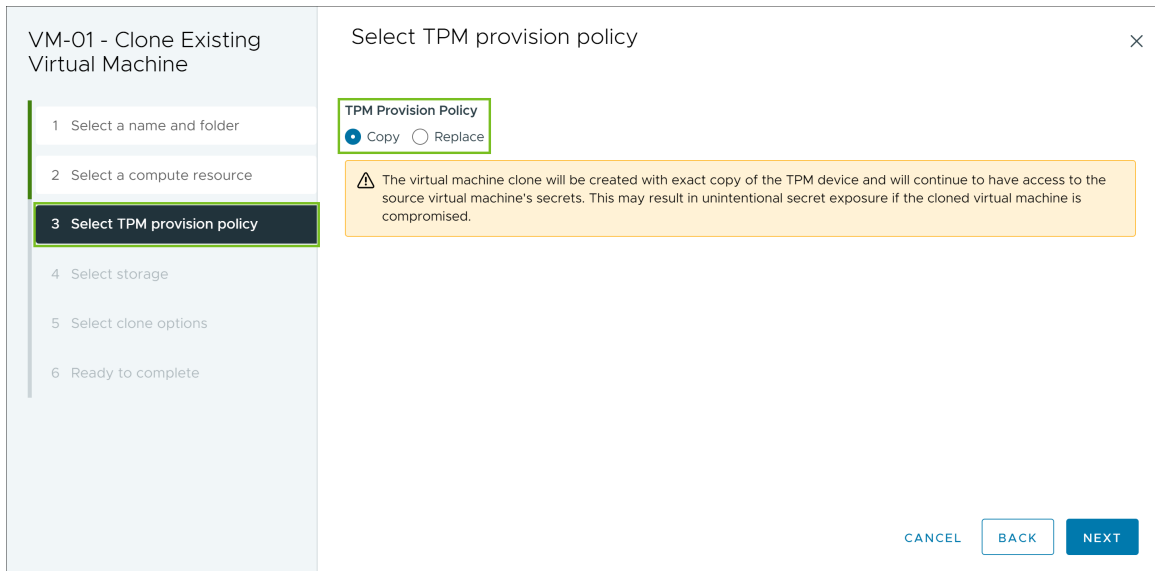
- 必须配置并启用密钥提供程序。
- 创建加密存储策略，或使用捆绑的示例，虚拟机加密策略。
- 所需特权（适用于所有密钥提供程序）：
  - 加密操作.克隆
  - 加密操作.加密
  - 加密操作.解密
  - 加密操作.重新加密
  - 如果未启用主机加密模式，还必须拥有 加密操作.注册主机 特权。

#### 步骤

- 1 在 vSphere Client 清单中，浏览到虚拟机。
- 2 要创建加密虚拟机的克隆，请右键单击虚拟机，选择**克隆 > 克隆到虚拟机**，并按照提示操作。
  - a 在**选择名称和文件夹**页面中，指定一个名称，然后选择克隆的目标位置。
  - b 在**选择计算资源**页面上，指定您拥有特权的对象。

- c （可选）更改克隆的 vTPM 的密钥。

图 10-1. 选择 TPM 置备策略



克隆虚拟机会复制整个虚拟机，包括 vTPM 及其密钥，可用于确定系统的身份。要更改 vTPM 上的密钥，请对 **TPM 置备策略** 选择替换。

**注** 替换 vTPM 的密钥时，将替换所有密钥，包括工作负载相关密钥。最佳做法是，在替换密钥之前，确保工作负载不再使用 vTPM。否则，克隆的虚拟机中的工作负载可能无法正常运行。

- d 在**选择存储**页面中，选择一个数据存储。可以在克隆操作过程中更改存储策略。例如，从使用加密策略更改为使用非加密策略会对磁盘进行解密。
- e 在**选择克隆选项**页面上，选择克隆选项，如《vSphere 虚拟机管理》文档中所述。
- f 在**即将完成**页面上，检查信息并单击**完成**。
- 3 （可选）更改克隆虚拟机的密钥。

默认情况下，使用与父虚拟机相同的密钥来创建克隆虚拟机。最佳做法是更改克隆虚拟机的密钥，以确保多个虚拟机没有相同的密钥。

- a 确定执行浅层重新加密还是深层重新加密。

要使用不同的 DEK 和 KEK，请对克隆虚拟机执行深层重新加密。要使用不同的 KEK，请对克隆虚拟机执行浅层重新加密。要执行深层重新加密，必须关闭虚拟机电源。虚拟机打开电源时，如果虚拟机中存在快照，可以执行浅层重新加密操作。仅允许在单个快照分支（磁盘链）上对具有快照的加密虚拟机执行浅层重新加密。不支持多个快照分支。如果浅层重新加密在使用新 KEK 更新链中的所有链接之前失败，则仍然可以访问加密虚拟机（如果具有新旧 KEK）。

- b 使用 API 对克隆执行重新加密。请参见《vSphere Web Services SDK 编程指南》。

## 加密现有虚拟机或虚拟磁盘

您可以通过更改现有虚拟机或虚拟磁盘的存储策略对其进行加密。您只能对加密虚拟机的虚拟磁盘进行加密。

### 前提条件

- 配置密钥提供程序并将其设置为默认值。
- 创建加密存储策略，或使用捆绑的示例，虚拟机加密策略。
- 确保已关闭虚拟机电源。
- 确认您拥有所需特权：
  - **加密操作.加密新项**
  - 如果未启用主机加密模式，您还需要**加密操作.注册主机**。

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 右键单击您要更改的虚拟机，并选择**虚拟机策略 > 编辑虚拟机存储策略**。  
您可以针对虚拟机文件（由虚拟机主页表示）设置存储策略，同时针对虚拟磁盘设置存储策略。
- 3 选择存储策略。
  - 要对虚拟机及其硬盘进行加密，请选择加密存储策略并单击**确定**。
  - 要对虚拟磁盘进行加密但不对虚拟机进行加密，请打开**按磁盘配置**，为虚拟机主目录选择加密存储策略并为虚拟磁盘选择其他存储策略，然后单击**确定**。  
您无法对未加密虚拟机的虚拟磁盘进行加密。
- 4 您可以根据自己的偏好从 vSphere Client 中的**编辑设置**菜单对虚拟机进行解密，也可以同时对虚拟机和磁盘进行加密。
  - a 右键单击虚拟机，然后选择**编辑设置**。
  - b 选择**虚拟机选项**选项卡，然后打开**加密**。选择加密策略。如果取消选择所有磁盘，则仅对虚拟机主目录进行加密。
  - c 单击**确定**。

## 解密加密虚拟机或虚拟磁盘

可以通过更改存储策略对虚拟机或其磁盘（或两者）进行解密。

此任务介绍了如何使用 vSphere Client 解密加密的虚拟机。

所有加密虚拟机都需要加密 vMotion。在虚拟机解密过程中，加密 vMotion 设置保持不变。要更改此设置以停止使用 Encrypted vMotion，请明确更改此设置。

该任务说明如何使用存储策略执行解密。对于虚拟磁盘，您也可以使用**编辑设置**菜单执行解密。

### 前提条件

- 虚拟机必须加密。
- 虚拟机必须处于电源关闭状态或处于维护模式。
- 所需特权：**加密操作.解密**

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 右键单击您要更改的虚拟机，并选择**虚拟机策略 > 编辑虚拟机存储策略**。  
您可以针对虚拟机文件（由虚拟机主页表示）设置存储策略，同时针对虚拟磁盘设置存储策略。
- 3 选择存储策略。
  - 要对虚拟机及其硬盘进行解密，请关闭**按磁盘配置**，从下拉菜单中选择存储策略，然后单击**确定**。
  - 要对虚拟磁盘进行解密但不对虚拟机进行解密，请打开**按磁盘配置**，为虚拟机主目录选择加密存储策略并为虚拟磁盘选择其他存储策略，然后单击**确定**。  
您无法解密虚拟机而让磁盘保持加密状态。
- 4 您可以根据自己的偏好使用 vSphere Client 从**编辑设置**菜单中对虚拟机和磁盘进行解密。
  - a 右键单击虚拟机，然后选择**编辑设置**。
  - b 选择**虚拟机选项**选项卡，然后展开**加密**。
  - c 要对虚拟机及其硬盘进行解密，请从**虚拟机加密**下拉菜单中选择**无**。
  - d 要对虚拟磁盘进行解密但不对虚拟机进行解密，请取消选择磁盘。
  - e 单击**确定**。
- 5 （可选）现在可以更改 Encrypted vMotion 设置。
  - a 右键单击虚拟机，然后单击**编辑设置**。
  - b 单击**虚拟机选项**，然后打开**加密**。
  - c 设置**加密 vMotion** 值。

## 更改虚拟磁盘的加密策略

通过 vSphere Client 创建加密虚拟机时，可以选择加密在创建虚拟机过程中添加的哪些虚拟磁盘。您可以使用**编辑虚拟机存储策略**选项解密加密的虚拟磁盘。

---

**注** 加密虚拟机中可以包含未加密的虚拟磁盘。但未加密的虚拟机无法包含已加密的虚拟磁盘。

---

请参见[虚拟磁盘加密](#)。

此任务介绍了如何使用存储策略更改加密策略。您也可以使用**编辑设置**菜单更改加密策略。

### 前提条件

- 您必须具有**加密操作.管理加密策略**特权。
- 确保已关闭虚拟机电源。

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 右键单击虚拟机，然后选择**虚拟机策略 > 编辑虚拟机存储策略**。
- 3 更改存储策略。
  - 要更改虚拟机及其硬盘的存储策略，请选择加密存储策略，然后单击**确定**。
  - 要对虚拟磁盘进行加密但不对虚拟磁盘进行加密，请打开**按磁盘配置**，为虚拟机主目录选择加密存储策略并为虚拟磁盘选择其他存储策略，然后单击**确定**。

您无法对未加密虚拟机的虚拟磁盘进行加密。
- 4 您可以根据自己的偏好从**编辑设置**菜单中更改存储策略。
  - a 右键单击虚拟机，然后选择**编辑设置**。
  - b 选择**虚拟硬件**选项卡，展开硬盘，然后从下拉菜单中选择加密策略。
  - c 单击**确定**。

## 解决缺失加密密钥问题

如果 ESXi 主机无法从 vCenter Server 获取加密虚拟机或加密虚拟磁盘的密钥 (KEK)，则加密虚拟机将锁定。使密钥在密钥服务器 (KMS) 上可用后，您可以解锁锁定的加密虚拟机。

在某些情况下，使用标准密钥提供程序时，ESXi 主机无法从 vCenter Server 获取加密虚拟机或加密虚拟磁盘的密钥加密密钥 (KEK)。在这种情况下，您仍然可以取消注册或重新加载虚拟机。但是，无法执行其他虚拟机操作，例如打开虚拟机电源。在采取必要的步骤使所需密钥在密钥服务器上可用后，可以使用 vSphere Client 解锁锁定的加密虚拟机。

如果虚拟机密钥不可用，vCenter Server 警报会向您发出通知，并且虚拟机的状态将显示为无效。虚拟机无法打开电源。如果虚拟机密钥可用，但是加密磁盘的密钥不可用，则虚拟机状态不会显示为无效。但是，虚拟机无法打开电源，并且会出现以下错误：

```
The disk [/path/to/the/disk.vmdk] is encrypted and a required key was not found.
```

**注** 以下过程说明了会导致虚拟机进入锁定状态的情况、显示的相应警报和事件日志以及在每种情况下应执行的操作。



## 步骤

- 1 如果 vCenter Server 系统和密钥服务器之间的连接有问题，vCenter Server 将生成虚拟机警报。此外，还会在事件日志中显示一条错误消息。

还原与密钥服务器的连接。当密钥服务器和密钥可用时，解锁锁定的虚拟机。请参见[解锁锁定的虚拟机](#)。您也可以重新引导主机并重新注册虚拟机，以便在还原连接后解锁该虚拟机。

与密钥服务器的连接断开不会自动锁定虚拟机。如果满足以下条件，虚拟机只会进入锁定状态：

- 密钥在 ESXi 主机上不可用。
- vCenter Server 无法从密钥服务器检索密钥。

每次重新引导后，ESXi 主机必须能够访问 vCenter Server。vCenter Server 会从密钥服务器请求具有相应 ID 的密钥，并将其提供给 ESXi。

---

**注** 在 vSphere 7.0 Update 2 及更高版本中，可以在 ESXi 重新引导后持久保留加密密钥。请参见[ESXi 主机上的 vSphere 密钥持久性](#)。

---

如果还原与密钥提供程序的连接后虚拟机仍锁定，请参见[解锁锁定的虚拟机](#)。

- 2 如果连接已还原，请注册虚拟机。如果出现错误，或者虽然操作成功但虚拟机处于锁定状态，请验证您是否具有 vCenter Server 系统的 **Cryptographic operations.RegisterVM** 特权。

如果密钥可用，则不需要此特权即可打开加密虚拟机的电源。如果必须检索密钥，则需要此特权才能注册虚拟机。

- 3 如果密钥在密钥服务器上不再可用，vCenter Server 将生成虚拟机警报。此外，还会在事件日志中显示一条错误消息。

请求密钥服务器管理员还原密钥。如果要打开已从清单中移除且已很长时间未注册的虚拟机的电源，您可能会遇到非活动的密钥。如果您重新引导 ESXi 主机且密钥服务器不可用，也会发生这种情况。

- a 使用 Managed Object Browser (MOB) 或 vSphere API 检索密钥 ID。

从 `VirtualMachine.config.keyId.keyId` 中检索 `keyId`。

- b 请求密钥服务器管理员重新激活与该密钥 ID 关联的密钥。

- c 还原密钥后，参见[解锁锁定的虚拟机](#)。

如果可在密钥服务器上还原此密钥，vCenter Server 则会在下次需要时对其进行检索并推送到 ESXi 主机。

- 4 如果密钥服务器可供访问且 ESXi 主机已开机，但 vCenter Server 系统不可用，请按照以下步骤解锁虚拟机。

- a 还原 vCenter Server 系统，或者设置不同的 vCenter Server 系统，然后与密钥服务器建立信任。

您必须使用相同的密钥提供程序名称，但密钥服务器 IP 地址可以不同。

- b 重新注册所有已锁定的虚拟机。

新 vCenter Server 实例将从密钥服务器中检索密钥，并且虚拟机将解锁。

- 5 如果仅在 ESXi 主机上缺少密钥，则 vCenter Server 会生成虚拟机警报，并且会在事件日志中显示以下消息：

虚拟机已锁定，因为主机上缺少密钥。

vCenter Server 系统可以从密钥提供程序检索缺少的密钥。不需要手动恢复密钥。请参见[解锁锁定的虚拟机](#)。

## 解锁锁定的虚拟机

当加密虚拟机处于锁定状态时，vCenter Server 警报会通知您。执行必要步骤以使所需的密钥在密钥服务器上可用后，您可以使用 vSphere Client 来解锁已锁定的加密虚拟机。

### 前提条件

- 验证您是否拥有所需特权：[加密操作.注册虚拟机](#)
- 诸如启用主机加密等可选任务可能需要其他特权。
- 解锁已锁定的虚拟机之前，请查明锁定原因并尝试手动解决问题。请参见[解决缺失加密密钥问题](#)。

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 导航到虚拟机的[摘要](#)选项卡。  
虚拟机锁定时，将显示“虚拟机已锁定”警报。
- 3 确定您要确认警报，还是要将警报重置为绿色而不立即解锁虚拟机。  
单击[确认](#)或[重置为绿色](#)后，警报会消失，但在解锁之前，虚拟机会保持处于锁定状态。
- 4 导航到虚拟机的[监控](#)选项卡并单击[事件](#)，以获取有关锁定虚拟机的原因的更多信息。
- 5 解锁虚拟机之前，请执行建议的故障排除。
- 6 导航到虚拟机的[摘要](#)选项卡，然后单击虚拟机控制台下的[解锁虚拟机](#)。  
将显示一条消息，警告加密密钥数据将传输到主机。
- 7 单击[是](#)。

## 解决 ESXi 主机加密模式问题

在某些情况下，ESXi 主机的加密模式可能会被停用。

如果 ESXi 主机包含任何加密虚拟机，则它需要激活主机加密模式。如果主机检测到缺少主机密钥，或者密钥提供程序不可用，该主机可能无法激活加密模式。无法激活主机加密模式时，vCenter Server 会生成警报。

## 步骤

- 1 如果 vCenter Server 系统和密钥提供程序之间的连接有问题，则会生成警报，并且事件日志中会显示错误消息。

您必须还原与包含相关加密密钥的密钥提供程序的连接。

- 2 如果缺少密钥，则会生成警报，并且事件日志中会显示错误消息。

必须确保密钥存在于密钥提供程序中。有关从备份还原的信息，请参阅密钥管理供应商文档。

## 后续步骤

还原与密钥提供程序的连接或为密钥提供程序手动恢复密钥后，如果主机的加密模式仍然处于停用状态，请重新激活主机加密模式。请参见[重新激活 ESXi 主机加密模式](#)。

# 重新激活 ESXi 主机加密模式

从 vSphere 6.7 开始，ESXi 主机加密模式停用后，vCenter Server 警报会通知您。如果主机加密模式已停用，您可以重新激活该模式。

## 前提条件

- 验证您是否拥有所需特权：**加密操作.注册主机**。
- 重新激活加密模式之前，请对原因进行故障排除并尝试手动修复该问题。

## 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。

- 2 导航到 ESXi 主机的**摘要**选项卡。

加密模式停用后，将显示“主机需要启用加密模式”警报。

- 3 确定您要确认警报，还是要将警报重置为绿色而不立即重新激活主机加密模式。

单击**确认**或**重置为绿色**后，警报会消失，但在重新激活之前，主机的加密模式会保持停用状态。

- 4 导航到 ESXi 主机的**监控**选项卡，然后单击**事件**。

随即显示有关停用加密模式的原因的更多信息。在重新激活加密模式之前，请执行建议的故障排除。

- 5 在**摘要**选项卡上，单击**启用主机加密模式**，以重新激活主机加密。

将显示一条消息，警告加密密钥数据将传输到主机。

- 6 单击**是**。

# 设置密钥服务器证书过期阈值

默认情况下，vCenter Server 会在密钥服务器 (KMS) 证书过期前 30 天向您发出通知。您可以对此默认值进行更改。

密钥服务器证书有一个过期日期。达到过期日期的阈值时，将显示一条警报来通知您。

vCenter Server 和密钥服务器交换两种证书：服务器和客户端。vCenter Server 系统上的 VMware 端点证书存储 (VECS) 可存储每个密钥提供程序的多个服务器证书和一个客户端证书。由于有两种证书类型，因此每种证书类型有两条警报（一条针对客户端，一条针对服务器）。

#### 步骤

- 1 使用 vSphere Client 登录到 vCenter Server 系统。
- 2 在对象层次结构中选择 vCenter Server 系统。
- 3 单击配置。
- 4 在设置下，单击高级设置，然后单击编辑设置。
- 5 单击筛选器图标，然后输入 `vpzd.kmscert.threshold`，或滚动到配置参数本身。
- 6 以天为单位输入值，然后单击保存。

## vSphere 虚拟机加密和核心转储

如果您的环境使用 vSphere 虚拟机加密，且 ESXi 主机发生错误，则将对生成的核心转储进行加密，以便保护客户数据。还会对 vm-support 软件包中包含的核心转储进行加密。

**注** 核心转储可以包含敏感信息。处理核心转储时，请遵循您组织的数据安全和隐私策略。

### ESXi 主机上的核心转储

当 ESXi 主机、用户环境或虚拟机出现故障时，将生成核心转储，并且主机会重新引导。如果 ESXi 主机已启用加密模式，则会使用 ESXi 密钥缓存中的密钥对核心转储进行加密。（根据使用的密钥提供程序，密钥来自外部密钥服务器、密钥提供程序服务或 vCenter Server）。有关背景信息，请参见 [vSphere 虚拟机加密如何保护您的环境](#)。

当 ESXi 主机加密“安全”并生成核心转储时，会创建一个事件。该事件指明执行了核心转储并提供以下信息：环境名称、执行时间、用于加密核心转储的密钥的 keyID 以及核心转储文件名。可以在 vCenter Server 的**任务和事件**下的“事件”查看器中查看该事件。

下表按 vSphere 版本显示了用于每种核心转储类型的加密密钥。

表 10-1. 核心转储加密密钥

核心转储类型	加密密钥 (ESXi6.5)	加密密钥 (ESXi6.7 及更高版本)
ESXi 内核	主机密钥	主机密钥
用户环境 (hostd)	主机密钥	主机密钥
加密虚拟机 (VM)	主机密钥	虚拟机密钥

ESXi 主机重新引导后可执行的操作取决于多个因素。

- 在大多数情况下，密钥提供程序会在重新引导后尝试将密钥推送到 ESXi 主机。如果此操作成功，您可以生成 vm-support 软件包，并对核心转储进行解密或重新加密。请参见[解密或重新加密已加密核心转储](#)。

- 如果 vCenter Server 无法连接到 ESXi 主机，您也许可以检索密钥。请参见[解决缺失加密密钥问题](#)。
- 如果主机使用自定义密钥，且该密钥不同于 vCenter Server 推送到主机的密钥，您将无法处理核心转储。请避免使用自定义密钥。

## 核心转储和 vm-support 软件包

当您遇到严重错误而联系 VMware 技术支持时，您的支持代表通常会要求您生成 vm-support 软件包。该软件包包含日志文件和其他信息，包括核心转储。如果您的支持代表无法通过查看日志文件和其他信息解决问题，他们可能会要求您解密核心转储并提供相关信息。为保护诸如密钥等敏感信息，请遵循您所在组织的安全和隐私权政策。请参见[为使用加密的 ESXi 主机收集 vm-support 软件包](#)。

## vCenter Server 系统上的核心转储

vCenter Server 系统上的核心转储未加密。vCenter Server 已包含可能的敏感信息。至少确保 vCenter Server 受到保护。请参见第 4 章 [确保 vCenter Server 系统安全](#)。您还可以考虑关闭 vCenter Server 系统的核心转储。日志文件中的其他信息可以帮助确定问题所在。

## 为使用加密的 ESXi 主机收集 vm-support 软件包

如果为 ESXi 主机启用了主机加密模式，则会加密 vm-support 软件包中的所有核心转储。您可以从 vSphere Client 收集该软件包，如果随后希望解密核心转储，可以指定一个密码。

vm-support 软件包中包含日志文件、核心转储文件等。

### 前提条件

通知您的支持代表已针对 ESXi 主机启用主机加密模式。支持代表可能会要求您解密核心转储并提取相关信息。

---

**注** 核心转储可以包含敏感信息。请遵循您组织的安全和隐私权政策，以保护主机密钥等敏感信息。

---

### 步骤

- 1 使用 vSphere Client 登录到 vCenter Server 系统。
- 2 单击**主机和集群**，然后右键单击 ESXi 主机。
- 3 选择**导出系统日志**。
- 4 在对话框中，选择**已加密核心转储的密码**，然后指定并确认密码。
- 5 其他选项保留默认值，或者根据 VMware 技术支持要求进行更改，然后单击**导出日志**。
- 6 指定该文件的位置。

- 7 如果支持代表要求您解密 `vm-support` 软件包中的核心转储，请登录任一 ESXi 主机，然后按照以下步骤操作。

- a 登录 ESXi 并连接到 `vm-support` 软件包所在的目录。

文件名采用 `esx.date_and_time.tgz` 模式。

- b 确保该目录具有足够的空间来存储该软件包、未压缩的软件包和重新压缩的软件包，或者移动该软件包。
- c 将该软件包解压缩到本地目录中。

```
vm-support -x *.tgz .
```

生成的文件层次结构可能包含 ESXi 主机的核心转储文件（通常位于 `/var/core` 中），并且可能包含虚拟机的多个核心转储文件。

- d 单独解密每个加密核心转储文件。

```
crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
--password encryptedZdump decryptedZdump
```

`vm-support-incident-key-file` 是位于该目录顶层的事件密钥文件。

`encryptedZdump` 是加密核心转储文件的名称。

`decryptedZdump` 是该命令生成的文件名。请确保该名称类似于 `encryptedZdump` 名称。

- e 提供在创建 `vm-support` 软件包时指定的密码。
- f 移除加密核心转储，然后重新压缩该软件包。

```
vm-support --reconstruct
```

- 8 移除任何包含保密信息的文件。

## 解密或重新加密已加密核心转储

您可以使用 `crypto-util` CLI 解密或重新加密 ESXi 主机上的已加密核心转储。

您可以自行解密并检查 `vm-support` 软件包中的核心转储。核心转储可能包含敏感信息。请遵循您所在组织的安全和隐私权政策以保护密钥等敏感信息。

有关重新加密核心转储的详细信息以及 `crypto-util` 的其他功能，请参见命令行帮助。

---

**注** `crypto-util` 面向高级用户。

---

### 前提条件

用于对核心转储进行加密的密钥在生成核心转储的 ESXi 主机上必须可用。

## 步骤

- 1 直接登录到发生核心转储的 ESXi 主机。

如果 ESXi 主机处于锁定模式或 SSH 访问已停用，您可能需要先激活访问。

- 2 确定核心转储是否已加密。

选项	描述
监控程序核心转储	<code>crypto-util envelope describe vmmcores.ve</code>
zdump 文件	<code>crypto-util envelope describe --offset 4096 zdumpFile</code>

- 3 根据相应的类型解密核心转储。

选项	描述
监控程序核心转储	<code>crypto-util envelope extract vmmcores.ve vmmcores</code>
zdump 文件	<code>crypto-util envelope extract --offset 4096 zdumpEncrypted zdumpUnencrypted</code>

## 在 ESXi 主机上激活和停用密钥持久性

必须在 ESXi 主机上激活密钥持久性。默认情况下，未激活此功能。

有关密钥持久性的概念信息，请参见 [ESXi 主机上的 vSphere 密钥持久性](#)。

### 前提条件

激活密钥持久性的要求：

- ESXi 7.0 Update 2 或更高版本
- ESXi 主机安装了 TPM 2.0
- 有权访问 ESXCLI 命令集。可以远程或在 ESXi Shell 上运行 ESXCLI 命令。

**注** 使用 vSphere Native Key Provider 时，不需要密钥持久性。vSphere Native Key Provider 设计为即时可用，无需访问密钥服务器即可运行。

为了进一步提高安全性，TPM 还可以使用封装策略防止在 ESXi 主机引导期间发生篡改。请参见[什么是 TPM 封装策略](#)。

## 步骤

- 1 在 ESXi 主机上，使用 SSH 或其他远程控制台连接启动会话。

- 2 以 root 用户身份登录。

### 3 激活或停用密钥持久性。

- a 要激活密钥持久性，请执行以下操作：

```
esxcli system security keypersistence enable
```

- b 要停用持久性，请执行以下操作：

```
esxcli system security keypersistence disable --remove-all-stored-keys
```

## 使用 vSphere Client 对加密虚拟机进行重新加密

可以使用 vSphere Client 对加密虚拟机执行浅层重新加密。您可能会出于业务或合规性原因对加密虚拟机执行重新加密。

浅层重新加密或重新加密（也称为 **shallow recrypt**（浅层重新加密））支持在加密虚拟机上使用新的（和不同的）密钥加密密钥 (KEK)。可以在虚拟机打开电源时执行重新加密操作。如果虚拟机存在快照，也可以执行重新加密。仅允许在单个快照分支（磁盘链）上对具有快照的加密虚拟机执行重新加密。不支持多个快照分支。如果重新加密在使用新 KEK 更新链中的所有链接之前失败，则仍然可以访问加密虚拟机（如果具有新旧 KEK）。

#### 前提条件

所需特权：**加密操作.管理密钥服务器**

#### 步骤

- 1 使用 vSphere Client 登录到 vCenter Server 系统。
- 2 浏览清单列表并选择加密虚拟机。
- 3 右键单击加密虚拟机，然后选择**虚拟机策略**。
- 4 选择**重新加密**。
- 5 单击**是**。

加密虚拟机将使用新 KEK 重新加密。

---

**注** 如果重新加密失败，事件子系统将发布以下事件：

```
com.vmware.vc.vm.crypto.RekeyFail
```

---



## 使用 vSphere Client 设置默认密钥提供程序

如果您未将第一个密钥提供程序设置为默认密钥提供程序，或者您的环境使用多个密钥提供程序且您移除了默认密钥提供程序，则必须设置默认密钥提供程序。您可以使用 vSphere Client 在 vCenter Server 级别设置默认密钥提供程序。

### 前提条件

最佳做法是，确认“密钥提供程序”选项卡中的“连接状态”显示“活动”和一个绿色复选标记。

### 步骤

- 1 使用 vSphere Client 登录。
- 2 导航到 vCenter Server。
- 3 单击**配置**，然后选择**安全**下的**密钥提供程序**。
- 4 选择密钥提供程序。
- 5 单击**设置为默认值**。  
此时将显示确认对话框。
- 6 单击**设置为默认值**。  
该密钥提供程序显示为当前默认值。

## 使用 CLI 设置默认密钥提供程序

如果您未将第一个密钥提供程序设置为默认密钥提供程序，或者您的环境使用多个密钥提供程序且您移除了默认密钥提供程序，则必须设置默认密钥提供程序。您可以使用 PowerCLI 在 vCenter Server 级别、集群级别或集群文件夹级别设置默认密钥提供程序。

### 前提条件

最佳做法是，确认“密钥提供程序”选项卡中的“连接状态”显示“活动”和一个绿色复选标记。

您必须具有包含**加密操作.管理 KMS** 特权的角色。在 vSphere Trust Authority 中，该角色必须应用于受信任集群。

### 步骤

- 1 确保您已经以管理员身份连接到您创建密钥提供程序的 vCenter Server。

---

**注** 在 vSphere Trust Authority 中，连接到受信任集群的 vCenter Server。

---

```
Connect-VIServer -server VC_ip_address -User admin_user -Password 'password'
```

- 2 获取密钥提供程序。

```
Get-KeyProvider
```

可以使用 `-Name` *keyprovider* 选项指定单个密钥提供程序。

### 3 将 Get-KeyProvider 密钥提供程序信息分配给变量。

例如，以下命令将信息分配给变量 `$kp`。

```
$kp = Get-KeyProvider
```

如果您有多个密钥提供程序，则可以使用 `Select-Object` 选择其中一个密钥提供程序。

```
$kp = Get-KeyProvider | Select-Object -Index 0
```

### 4 使用以下 PowerCLI 命令之一。

设置默认值的位置	命令
<b>vCenter Server 级别</b>	<code>Set-KeyProvider -KeyProvider \$kp -DefaultForSystem</code>
<b>集群级别</b>	<p>以下示例命令为集群 CL-01 设置密钥提供程序。</p> <pre>Add-EntityDefaultKeyProvider -KeyProvider \$kp -Entity 'CL-01'</pre>
<b>集群文件夹级别</b>	<p>以下示例命令为集群文件夹 Cluster-Folder-01 设置密钥提供程序。</p> <pre>Add-EntityDefaultKeyProvider -KeyProvider \$kp -Entity 'Cluster-Folder-01'</pre>

# 使用虚拟可信平台模块保护虚拟机

# 11

使用虚拟可信平台模块 (Virtual Trusted Platform Module, vTPM) 功能，可以向虚拟机添加 TPM 2.0 虚拟加密处理器。

vTPM 是物理可信平台模块 2.0 芯片的基于软件的表示形式。vTPM 的作用与任何其他虚拟设备一样。可以使用与添加虚拟 CPU、内存、磁盘控制器或网络控制器相同的方式将 vTPM 添加到虚拟机。vTPM 不需要硬件可信平台模块芯片。

本章讨论了以下主题：

- 什么是虚拟可信平台模块
- 创建具有虚拟可信平台模块的虚拟机
- 将虚拟可信平台模块添加到现有虚拟机
- 从虚拟机中移除虚拟可信平台模块
- 确定已启用虚拟可信平台模块的虚拟机
- 查看虚拟可信平台模块设备证书
- 导出和替换虚拟可信平台模块设备证书

## 什么是虚拟可信平台模块

虚拟可信平台模块 (vTPM) 是物理可信平台模块 2.0 芯片的基于软件的表示形式。vTPM 的作用与任何其他虚拟设备一样。

vTPMs 提供基于硬件的安全相关功能，如随机数生成、证明、密钥生成等。添加到虚拟机后，vTPM 使客户机操作系统能够创建并存储私钥。这些密钥不向客户机操作系统本身公开。因此，虚拟机攻击面会缩小。通常，对于安全受到危害的客户机操作系统，其密钥的安全也会受到危害，但启用 vTPM 可在很大程度上降低此风险。只有客户机操作系统可以使用这些密钥进行加密或签名。通过连接的 vTPM，客户端可以远程证明虚拟机的身份，并验证它正在运行的软件。

vTPM 不要求 ESXi 主机上存在可信平台模块 (TPM) 2.0 物理芯片。但是，如果要执行主机证明，则需要外部实体，例如 TPM 2.0 物理芯片。请参见[使用可信平台模块保护 ESXi 主机](#)。

---

**注** 默认情况下，没有任何存储策略与已启用 vTPM 的虚拟机关联。仅对虚拟机文件（虚拟机主目录）进行加密。您可以选择为虚拟机及其磁盘明确添加加密，但虚拟机文件已加密。

---

## 如何为虚拟机配置 vTPM

从虚拟机的角度来看，vTPM 是一个虚拟设备。可以将 vTPM 添加到新虚拟机，也可以添加到现有虚拟机。vTPM 依赖虚拟机加密来保护重要的 TPM 数据，因此需要您配置密钥提供程序。配置 vTPM 时，虚拟机文件会进行加密，而不是磁盘加密。您可以选择为虚拟机及其磁盘明确添加加密。

备份启用了 vTPM 的虚拟机时，备份必须包含所有虚拟机数据，包括 \*.nvram 文件。如果备份不包含 \*.nvram 文件，则无法还原已启用 vTPM 的虚拟机。此外，由于已启用 vTPM 的虚拟机的虚拟机主目录文件已加密，因此请确保加密密钥在还原时可用。

从 vSphere 8.0 开始，在克隆具有 vTPM 的虚拟机时，为具有 vTPM 的虚拟机选择 **替换** 选项，会创建一个新的空白 vTPM，它将获取自己的密钥和身份。替换 vTPM 的密钥时，将替换所有密钥，包括工作负载相关密钥。最佳做法是，在替换密钥之前，确保工作负载不再使用 vTPM。否则，克隆的虚拟机中的工作负载可能无法正常运行。

## vTPM 对 vSphere 的要求

要使用 vTPM，您的 vSphere 环境必须满足以下要求：

- 虚拟机要求：
  - EFI 固件
  - 硬件版本 14 及更高版本
- 组件要求：
  - 适用于 Windows 虚拟机的 vCenter Server 6.7 及更高版本，适用于 Linux 虚拟机的 vCenter Server 7.0 Update 2。
  - 虚拟机加密（用于对虚拟机主目录文件进行加密）。
  - 为 vCenter Server 配置的密钥提供程序。请参见 [vSphere 密钥提供程序比较](#)。
- 客户机操作系统支持：
  - Linux
  - Windows Server 2008 及更高版本
  - Windows 7 及更高版本

## 硬件 TPM 和虚拟 TPM 之间的差别

您可以使用硬件可信平台模块 (TPM) 为凭据或密钥提供安全存储。vTPM 可起到与 TPM 相同的作用，但它在软件中执行加密协处理器功能。vTPM 使用 .nvram 文件作为自己的安全存储，该文件使用虚拟机加密进行加密。

硬件 TPM 包含预加载的密钥，称为认可密钥 (Endorsement Key, EK)。EK 包含私钥和公钥。EK 可为 TPM 提供唯一标识。对于 vTPM，该密钥由 VMware Certificate Authority (VMCA) 或第三方证书颁发机构 (Certificate Authority, CA) 提供。vTPM 使用某个密钥后，该密钥通常不会更改，因为更改后会使用 vTPM 中存储的敏感信息失效。vTPM 在任何时候都不会与第三方 CA 联系。

## 创建具有虚拟可信平台模块的虚拟机

可以在创建虚拟机时添加虚拟可信平台模块 (vTPM)，以便为客户机操作系统提供增强的安全性。必须先创建密钥提供程序，然后才能添加 vTPM。

VMware 虚拟 TPM 与 TPM 2.0 兼容，可创建启用了 TPM 的虚拟芯片，以供虚拟机及其托管的客户机操作系统使用。

### 前提条件

- 确保您的 vSphere 环境配置了密钥提供程序。有关详细信息，请参见以下链接：
  - [配置 vSphere Trust Authority](#)
  - [第 7 章 配置和管理标准密钥提供程序](#)
  - [第 8 章 配置和管理 vSphere Native Key Provider](#)
- 您使用的客户机操作系统可以是 Windows Server 2008 及更高版本、Windows 7 及更高版本或 Linux。
- 在您的环境中运行的 ESXi 主机必须为 ESXi 6.7 或更高版本（Windows 客户机操作系统）或者 7.0 Update 2（Linux 客户机操作系统）。
- 虚拟机必须使用 EFI 固件。
- 确认您拥有所需特权：
  - 加密操作.克隆
  - 加密操作.加密
  - 加密操作.加密新项
  - 加密操作.迁移
  - 加密操作.注册虚拟机

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 在清单中选择一个对象（虚拟机的有效父对象），如 ESXi 主机或集群。
- 3 右键单击对象，选择**新建虚拟机**，并按照提示创建虚拟机。

选项	操作
选择创建类型	创建新虚拟机。
选择名称和文件夹	指定名称和目标位置。
选择计算资源	指定一个您有权为其创建虚拟机的对象。请参见 <a href="#">虚拟机加密任务的必备条件和必需特权</a> 。
选择存储	选择兼容的数据存储。
选择兼容性	必须选择 <b>ESXi 6.7 及更高版本</b> （对于 Windows 客户机操作系统）或者 <b>ESXi 7.0 U2 及更高版本</b> （对于 Linux 客户机操作系统）。

选项	操作
选择客户机操作系统	选择 Windows 或 Linux 以用作客户机操作系统。
自定义硬件	单击 <b>添加新设备</b> ，然后选择 <b>可信平台模块</b> 。 可以进一步自定义硬件，例如通过更改磁盘大小或 CPU 进行自定义。
即将完成	检查信息，然后单击 <b>完成</b> 。

## 结果

清单中将显示所指定的启用了 vTPM 的虚拟机。

## 将虚拟可信平台模块添加到现有虚拟机

可以将虚拟可信平台模块 (vTPM) 添加到现有虚拟机，以便为客户机操作系统提供增强的安全性。必须先创建密钥提供程序，然后才能添加 vTPM。

VMware 虚拟 TPM 与 TPM 2.0 兼容，可创建已启用 TPM 的虚拟芯片以供虚拟机及其托管的客户机操作系统使用。

### 前提条件

- 确保您的 vSphere 环境配置了密钥提供程序。有关详细信息，请参见以下链接：
  - [配置 vSphere Trust Authority](#)
  - [第 7 章 配置和管理标准密钥提供程序](#)
  - [第 8 章 配置和管理 vSphere Native Key Provider](#)
- 您使用的客户机操作系统可以是 Windows Server 2008 及更高版本、Windows 7 及更高版本或 Linux。
- 验证是否已关闭虚拟机。
- 在您的环境中运行的 ESXi 主机必须为 ESXi 6.7 或更高版本（Windows 客户机操作系统）或者 7.0 Update 2（Linux 客户机操作系统）。
- 虚拟机必须使用 EFI 固件。
- 确认您拥有所需特权：
  - 加密操作.克隆
  - 加密操作.加密
  - 加密操作.加密新项
  - 加密操作.迁移
  - 加密操作.注册虚拟机

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。

- 2 在清单中右键单击您要修改的虚拟机，然后选择**编辑设置**。
- 3 在**编辑设置**对话框中，单击**添加新设备**，然后选择**可信平台模块**。
- 4 单击**确定**。

现在，虚拟机**摘要**选项卡在**虚拟机硬件**窗格中包括虚拟可信平台模块。

## 从虚拟机中移除虚拟可信平台模块

可以从虚拟机中移除虚拟可信平台模块 (vTPM) 安全性。

移除 vTPM 设备可导致虚拟机上的所有加密信息变得不可恢复。从虚拟机中移除 vTPM 之前，请先停用客户机操作系统中使用 vTPM 设备的任何应用程序，例如 BitLocker。否则，可能会导致虚拟机无法引导。此外，无法从包含快照的虚拟机中移除 vTPM。

### 前提条件

- 确保已关闭虚拟机电源。
- 确认您拥有所需特权：**加密操作.解密**

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 在清单中右键单击您要修改的虚拟机，然后选择**编辑设置**。
- 3 在**编辑设置**对话框的**虚拟硬件**选项卡中找到“可信平台模块”条目。
- 4 将指针移到该设备上，然后单击**移除**图标。

该图标仅针对可以安全移除的虚拟硬件显示。

- 5 单击**删除**以确认要移除设备。

vTPM 设备将标记为移除。

- 6 单击**确定**。

确认虚拟机**摘要**选项卡的**虚拟机硬件**窗格中不再显示虚拟可信平台模块条目。

## 确定已启用虚拟可信平台模块的虚拟机

可以确定已启用虚拟可信平台模块 (vTPM) 的虚拟机。

可生成清单中所有虚拟机的列表，以显示虚拟机名称、操作系统和 vTPM 状态。还可以将此列表导出为 CSV 文件以用于合规性审核。

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 选择 vCenter Server 实例、主机或集群。
- 3 单击**虚拟机**选项卡，然后单击**虚拟机**。

- 4 要查看已启用 TPM 的所有虚拟机，请单击左下角的三栏**列选择器**，然后选择 **TPM**。

对于已启用 TPM 的虚拟机，“TPM”列会显示“存在”。未启用 TPM 的虚拟机将列为“不存在”。

- 5 可以将清单列表视图的内容导出到 CSV 文件。

- a 单击列表视图右下角的**导出**。

将打开“导出列表内容”对话框，其列出了要在 CSV 文件中包含的可用选项。

- b 选择是要在 CSV 文件中列出所有行，还是列出当前选定行。
  - c 从可用选项中，选择要在 CSV 文件中列出的列。
  - d 单击**导出**。

将生成 CSV 文件，并且可供下载。

## 查看虚拟可信平台模块设备证书

虚拟可信平台模块 (vTPM) 设备已预先配置了默认证书，您可以查看这些证书。

### 前提条件

您的环境中必须具有启用了 vTPM 的虚拟机。

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 在清单中选择一个对象（虚拟机的有效父对象），如 ESXi 主机或集群。
- 3 单击**虚拟机**，然后单击**虚拟机**。
- 4 选择要查看其证书信息的已启用 vTPM 的虚拟机。  
如有必要，请单击左下角的三栏**列选择器**，然后选择 **TPM** 以显示 TPM 为“存在”的虚拟机。
- 5 单击**配置**选项卡。
- 6 在 **TPM** 下，选择**证书**。
- 7 选择证书并查看其信息。
- 8 （可选）要导出证书信息，请单击**导出**。  
证书即保存到磁盘。

### 后续步骤

可以使用第三方证书颁发机构 (CA) 颁发的证书替换默认证书。请参见[导出和替换虚拟可信平台模块设备证书](#)。



## 导出和替换虚拟可信平台模块设备证书

可以替换虚拟可信平台模块 (vTPM) 设备附带的默认证书。

### 前提条件

您的环境中必须具有启用了 vTPM 的虚拟机。

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 在清单中选择一个对象（虚拟机的有效父对象），如 ESXi 主机或集群。
- 3 在清单中选择要替换其证书信息的已启用 vTPM 的虚拟机。
- 4 单击**配置**选项卡。
- 5 在 **TPM** 下，选择**签名请求**。
- 6 选择证书。
- 7 要导出证书信息，请单击**导出**。  
证书即保存到磁盘。
- 8 根据导出的证书签名请求 (CSR) 获取由第三方证书颁发机构 (CA) 颁发的证书。  
可以使用您的 IT 环境中可能具有的任何 CA。
- 9 当有新证书时，替换现有证书。
  - a 右键单击清单中要替换其证书的虚拟机，然后选择**编辑设置**。
  - b 在**编辑设置**对话框中，展开**安全设备**，然后展开**可信平台模块**。  
系统将显示证书。
  - c 针对要替换的证书单击**替换**。  
此时将显示**文件上载**对话框。
  - d 在本地计算机中找到并上载新证书。  
新证书将替换 vTPM 设备附带的默认证书。
  - e 虚拟机**摘要**选项卡中的**虚拟可信平台模块**列表下的证书名称将更新。

# 使用基于虚拟化的安全保护 Windows 客户机操作系统

# 12

在 vSphere 6.7 及更高版本中，可以在受支持的 Windows 客户机操作系统上启用 Microsoft 基于虚拟化的安全 (VBS)。

Microsoft VBS 是 Windows 10 和 Windows Server 2016 操作系统引入的一个功能，它使用硬件虚拟化和软件虚拟化通过创建独立的、受 Hypervisor 限制的专用子系统来增强系统安全性。

借助 VBS，您可以使用以下 Windows 安全功能来强化系统并隔离关键系统密钥和用户密钥以避免其安全受到危害：

- **Credential Guard**：旨在隔离并强化关键系统密钥和用户密钥以防其安全受到危害。
- **Device Guard**：提供一套设计为协同工作的功能，以防止恶意软件在 Windows 系统上运行并将其消除。
- **可配置的代码完整性**：确保以后只有可信代码可以从引导加载程序运行。

有关更多信息，请参见 Microsoft 文档中有关基于虚拟化的安全的主题。

通过 vCenter Server 为虚拟机启用 VBS 后，可以在 Windows 客户机操作系统中启用 VBS。

本章讨论了以下主题：

- [vSphere 基于虚拟化的安全最佳做法](#)
- [在虚拟机上激活基于虚拟化的安全](#)
- [在现有虚拟机上激活基于虚拟化的安全](#)
- [在客户机操作系统上激活基于虚拟化的安全](#)
- [停用基于虚拟化的安全](#)
- [标识已启用 VBS 的虚拟机](#)

## vSphere 基于虚拟化的安全最佳做法

要最大程度提高 Windows 客户机操作系统环境的安全性和可管理性，请遵循基于虚拟化的安全 (VBS) 的最佳做法。

通过遵循以下最佳做法来避免出现问题。

## VBS 硬件要求

要实现 VBS，请使用以下硬件：

- Intel
  - Haswell CPU 或更高版本为获得最佳性能，请使用 Skylake-EP CPU 或更高版本。
  - 可接受 Ivy Bridge CPU。
  - Sandy Bridge CPU 可能会导致性能较低。
- AMD
  - Zen 2 系列 CPU (Rome) 或更高版本。
  - 较早版本的 CPU 可能会导致性能降低。

针对“页大小更改时出现计算机检查异常”Intel CPU 漏洞的缓解措施可能会在 VBS 使用时对客户机操作系统性能产生负面影响。有关详细信息，请参见 VMware 知识库文章，网址为 <https://kb.vmware.com/kb/76050>。

## VBS 和 Windows 客户机操作系统兼容性

在 Intel 上，Windows 10 和 Windows Server 2016 及更高版本的虚拟机支持 VBS，尽管 Windows Server 2016 版本 1607 和 1703 需要修补程序。有关 ESXi 主机硬件兼容性，请参见 Microsoft 文档。要使用 Intel CPU 实现 VBS，需要使用 vSphere 6.7 或更高版本以及硬件版本 14 或更高版本。

在 AMD 上，Windows 10 版本 1809 和 Windows 2019 及更高版本的虚拟机支持 VBS。要使用 AMD CPU 实现 VBS，需要使用 vSphere 7.0 Update 2 或更高版本及硬件版本 19 或更高版本。

Windows 10 最初要求启用 Hyper-V 后才能实现 VBS。现在，Windows 10 不要求启用 Hyper-V。Windows Server 2016 及更高版本也同样适用。有关详细信息，请参见当前的 Microsoft 文档和 VMware vSphere 发行说明。

## VBS 上不支持的 VMware 功能

启用 VBS 时，以下功能在虚拟机中不受支持：

- Fault Tolerance
- PCI 直通
- 热添加 CPU 或内存

## VBS 的安装和升级限制

配置 VBS 之前，请了解以下安装和升级限制：

- 默认情况下，为低于版本 14 的虚拟硬件版本上的 Windows 10 和 Windows Server 2016 及更高版本配置的新虚拟机是使用旧版 BIOS 创建的。将虚拟机的固件类型从旧版 BIOS 更改为 UEFI 后，必须重新安装客户机操作系统。
- 如果计划将虚拟机从以前的 vSphere 版本迁移到 vSphere 6.7 或更高版本，并在虚拟机上启用 VBS，请使用 UEFI 以避免重新安装操作系统。

## 在虚拟机上激活基于虚拟化的安全

可以在创建虚拟机时为受支持的 Windows 客户机操作系统激活 Microsoft 基于虚拟化的安全 (VBS)。

激活 VBS 的过程包括两个步骤，第一个步骤是在虚拟机中激活 VBS，第二个步骤是在 Windows 客户机操作系统中激活 VBS。

### 前提条件

有关可接受的 CPU，请参见 [vSphere 基于虚拟化的安全最佳做法](#)。

要使用 Intel CPU 实现 VBS，需要使用 vSphere 6.7 或更高版本。创建使用硬件版本 14 或更高版本和以下受支持的客户机操作系统之一的虚拟机：

- Windows 10（64 位）或更高版本
- Windows Server 2016（64 位）或更高版本

要使用 AMD CPU 实现 VBS，需要使用 vSphere 7.0 Update 2 或更高版本。创建使用硬件版本 19 或更高版本和以下受支持的客户机操作系统之一的虚拟机：

- Windows 10（64 位）版本 1809 或更高版本
- Windows Server 2019（64 位）或更高版本

在激活 VBS 之前，请确保已安装 Windows 10 版本 1809 和 Windows Server 2019 的最新修补程序。

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 在清单中选择一个对象（虚拟机的有效父对象），如 ESXi 主机或集群。
- 3 右键单击对象，选择**新建虚拟机**，并按照提示创建虚拟机。

选项	操作
选择创建类型	创建虚拟机。
选择名称和文件夹	指定名称和目标位置。
选择计算资源	指定您有权为其创建虚拟机的对象。
选择存储	在虚拟机存储策略中，选择存储策略。选择兼容的数据存储。
选择兼容性	Intel CPU：确保选择 <b>ESXi 6.7 及更高版本</b> 。 AMD CPU：确保选择 <b>ESXi 7.0 U2 及更高版本</b> 。
选择客户机操作系统	选择与操作系统版本最匹配的 Windows 客户机操作系统选项。 选中 <b>启用 Windows 基于虚拟化的安全</b> 复选框。
自定义硬件	自定义硬件，例如，通过更改磁盘大小或 CPU。
即将完成	检查信息，然后单击 <b>完成</b> 。

### 结果

**摘要**选项卡下的“虚拟机详细信息”磁贴显示“基于虚拟化的安全性 - 启用”。

## 后续步骤

请参见在客户机操作系统上激活基于虚拟化的安全。

# 在现有虚拟机上激活基于虚拟化的安全

可以在受支持的 Windows 客户机操作系统的现有虚拟机上激活 Microsoft 基于虚拟化的安全 (VBS)。

激活 VBS 的过程包括两个步骤，第一个步骤是在虚拟机中激活 VBS，第二个步骤是在客户机操作系统中激活 VBS。

---

**注** 默认情况下，为低于版本 14 的硬件版本上的 Windows 10、Windows Server 2016 和 Windows Server 2019 配置的新虚拟机是使用旧版 BIOS 创建的。如果将虚拟机的固件类型从旧版 BIOS 更改为 UEFI，您必须重新安装客户机操作系统。

---

## 前提条件

有关可接受的 CPU，请参见 [vSphere 基于虚拟化的安全最佳做法](#)。

要使用 Intel CPU 实现 VBS，需要使用 vSphere 6.7 或更高版本。必须已使用硬件版本 14 或更高版本和以下受支持的客户机操作系统之一创建了虚拟机：

- Windows 10（64 位）或更高版本
- Windows Server 2016（64 位）或更高版本

要使用 AMD CPU 实现 VBS，需要使用 vSphere 7.0 Update 2 或更高版本。必须已使用硬件版本 19 或更高版本和以下受支持的客户机操作系统之一创建了虚拟机：

- Windows 10（64 位）版本 1809 或更高版本
- Windows Server 2019（64 位）或更高版本

在激活 VBS 之前，请确保已安装 Windows 10 版本 1809 和 Windows Server 2019 的最新修补程序。

## 步骤

- 1 在 vSphere Client 中，浏览到虚拟机。
- 2 右键单击虚拟机，然后选择**编辑设置**。
- 3 单击**虚拟机选项**选项卡。
- 4 选中基于虚拟化的安全性的**启用**复选框。
- 5 单击**确定**。

## 结果

**摘要**选项卡下的“虚拟机详细信息”磁贴显示“基于虚拟化的安全性 - 启用”。

## 后续步骤

请参见在客户机操作系统上激活基于虚拟化的安全。

## 在客户机操作系统上激活基于虚拟化的安全

可以为受支持的 Windows 客户机操作系统激活 Microsoft 基于虚拟化的安全 (VBS)。

可以从 Windows 客户机操作系统中激活 VBS。Windows 通过组策略对象 (Group Policy Object, GPO) 配置并强制启用 VBS。使用 GPO，您可以打开和关闭 VBS 提供的各个服务，例如 Secure Boot、Device Guard 和 Credential Guard。某些 Windows 版本还要求执行附加步骤，即启用 Hyper-V 平台。

有关部署 Device Guard 以激活基于虚拟化的安全的详细信息，请参见 [Microsoft 文档](#)。

### 前提条件

- 确保已在虚拟机上激活基于虚拟化的安全。

### 步骤

- 1 在 Microsoft Windows 中，编辑组策略以打开 VBS 并选择其他与 VBS 相关的安全选项。
- 2 （可选）对于低于 Redstone 4 的 Microsoft Windows 版本，可在 Windows 功能控制面板中启用 Hyper-V 平台。
- 3 重新引导客户机操作系统。

## 停用基于虚拟化的安全

如果您不再对虚拟机使用基于虚拟化的安全 (VBS)，则可以停用 VBS。停用虚拟机的 VBS 时，Windows VBS 选项保持不变，但可能会引发性能问题。在虚拟机上停用 VBS 之前，请在 Windows 中停用 VBS 选项。

### 前提条件

确保已关闭虚拟机电源。

### 步骤

- 1 在 vSphere Client 中，浏览到使用 VBS 的虚拟机。  
有关查找使用 VBS 的虚拟机的帮助，请参见[标识已启用 VBS 的虚拟机](#)。
- 2 右键单击虚拟机，然后选择**编辑设置**。
- 3 单击**虚拟机选项**。
- 4 取消选中基于虚拟化的安全的**启用**复选框。  
将显示一条消息，提醒您在客户机操作系统中停用 VBS。
- 5 单击**确定**。
- 6 确认虚拟机**摘要**选项卡的客户机操作系统描述中不再显示“VBS true”。

## 标识已启用 VBS 的虚拟机

可以确定哪些虚拟机已启用 VBS，以便用于报告和合规性目的。

### 步骤

- 1 使用 vSphere Client 连接到 vCenter Server。
- 2 在清单中选择 vCenter Server 实例、数据中心或主机。
- 3 单击**虚拟机**选项卡，然后单击**虚拟机**。
- 4 要显示 **VBS** 列，请单击左下角的三栏**列选择器**，然后选中 **VBS** 复选框。
- 5 在 **VBS** 列中扫描“存在”。

# 确保 vSphere 网络安全

# 13

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。

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。

## 使用防火墙

通过在部分或所有虚拟机上安装和配置基于主机的防火墙，为虚拟网络添加防火墙保护。

为提高效率，可设置专用虚拟机以太网或虚拟网络。使用虚拟网络，您可以在虚拟网络主节点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。

基于主机的防火墙会降低性能。因此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](#)。

## 使用网络分段

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，可以最大限度降低区域间泄露数据的风险。分段可防止多种威胁，包括地址解析协议 (ARP) 欺骗。通过 ARP 欺骗，攻击者操作 ARP 表格以重新映射 MAC 和 IP 地址，并得以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。因此，分段可防止嗅探攻击（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。

- 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。在初次创建段之后，这种方法更不容易出现配置错误。
- 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。VLAN 可为您节省部署和维护附加设备、线缆等硬件的成本。请参见[通过 VLAN 确保虚拟机安全](#)。



## 防止对虚拟机进行未经授权的访问

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。

- 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。
- 即使您不将某个虚拟机连接到物理网络，该虚拟机也会受到其他虚拟机的攻击。

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经授权的访问。保护虚拟机不遭受此类未经授权的访问。

有关保护虚拟机的其他信息，请参见标题为“用于保护虚拟机 (VM) 的安全虚拟网络配置”的 NIST 文档，网址为：

<https://csrc.nist.gov/publications/detail/sp/800-125b/final>

本章讨论了以下主题：

- 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
- 标准交换机保护和 VLAN
- 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 主机中创建多个网络
- 在 ESXi 主机上使用 Internet 协议安全
- 确保 SNMP 配置正确
- vSphere 网络连接安全性最佳做法

## 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。

---

**重要说明** 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 VMware 产品（包括 vSphere 和 vSAN）中所有受支持的端口和协议的列表，请参见 <https://ports.vmware.com/> 中的 VMware Ports and Protocols Tool™。您可以按 VMware 产品搜索端口，创建自定义端口列表，以及打印或保存端口列表。

## 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。

入口点上必须设置防火墙。防火墙可以位于客户端与 vCenter Server 之间，vCenter Server 与客户端都可以受到防火墙保护。

有关 VMware 产品（包括 vSphere 和 vSAN）中所有受支持的端口和协议的列表，请参见 <https://ports.vmware.com/> 中的 VMware Ports and Protocols Tool™。您可以按 VMware 产品搜索端口，创建自定义端口列表，以及打印或保存端口列表。

配置了 vCenter Server 的网络可以通过 vSphere Client、其他 UI 客户端或使用 vSphere API 的客户端接收通信。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。

您还可以在网络中的其他接入点上包括防火墙，具体取决于网络使用情况和客户端要求的安全级别。根据您的网络配置对应的安全风险选择防火墙位置。下面是常用的防火墙位置。

- vSphere 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 Client 与 ESXi 主机之间（如果用户通过 vSphere Client 访问虚拟机）。此连接是 vSphere 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 主机之间添加防火墙并计划在这些主机间迁移虚拟机，请在将源主机与目标主机隔开的防火墙中打开端口。

- ESXi 主机和网络存储（例如 NFS 或 iSCSI 存储）之间。这些端口并非专用于 VMware。根据网络规范进行配置。

## 通过防火墙连接到 vCenter Server

在防火墙中打开 TCP 端口 443 以允许 vCenter Server 接收数据。

默认情况下，vCenter Server 使用 TCP 端口 443 侦听来自其客户端的数据。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。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。

## 通过防火墙连接 ESXi 主机

如果在 ESXi 主机与 vCenter Server 之间配置了防火墙，请确保受管主机可以接收数据。

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 Client 访问权限以及防火墙命令的讨论，请参见配置 ESXi 防火墙。有关端口列表，请参见 VMware Ports and Protocols Tool™，网址为 <https://ports.vmware.com>。

## 针对没有 vCenter Server 的配置设立防火墙

如果您的环境中不包含 vCenter Server，客户端可以直接连接到 ESXi 网络。

您可以通过多种方式连接到独立 ESXi 主机。

- VMware Host Client
- ESXCLI 接口
- vSphere Web Services SDK 或 vSphere Automation SDK
- 第三方客户端

独立主机的防火墙要求类似于包含 vCenter Server 时的要求。

- 使用防火墙保护 ESXi 层，或者保护客户端和 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 ESXi 上，因此不需要设有防火墙的单独 License Server。

您可以使用 ESXCLI 或使用 VMware Host Client 配置防火墙端口。请参见《vSphere 单台主机管理 - VMware Host Client》。

## 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，以及是通过 vCenter Server 使用 vSphere Client 进行连接还是通过 VMware Host Client 直接连接到 ESXi 主机。

有关端口、用途和分类（入站、出站或双向）的详细信息，请参见 VMware Ports and Protocols Tool™，网址为 <https://ports.vmware.com>。

## 通过 vSphere Client 连接到基于浏览器的虚拟机控制台

使用 vSphere 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 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 Client 访问端口 443 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 Client 连接到 VMware Remote Console

如果使用 vSphere Client 并连接到 VMware Remote Console (VMRC)，则必须允许进行以下访问：

- 防火墙必须允许 vSphere Client 访问端口 443 上的 vCenter Server。
- 防火墙必须允许 VMRC 访问端口 443 上的 vCenter Server，以及访问端口 902（对于 11.0 之前的 VMRC 版本）和端口 443（对于 VMRC 版本 11.0 及更高版本）上的 ESXi 主机。有关 VMRC 版本 11.0 和 ESXi 端口要求的详细信息，请参见 VMware 知识库文章，网址为 <https://kb.vmware.com/s/article/76672>。

## 使用 VMware Host Client 直接连接到 ESXi 主机

如果直接连接到 ESXi 主机，则可以使用 VMware Host Client 虚拟机控制台。

---

**注** 请勿使用 VMware Host Client 直接连接到 vCenter Server 系统管理的主机。如果从 VMware Host Client 更改这些主机，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。

VMware Host 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。

为了让主机得到最好的保护，请确保物理交换机端口已配置为停用生成树，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停用了生成树协议，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停用 BPDU Guard 和 Port Fast，但激活生成树协议。

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激活动态中继协议 (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

标准交换机上的 VMkernel 端口组或虚拟机端口组具有可配置的安全策略。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。

就像物理网络适配器一样，虚拟机网络适配器也可以模拟另一个虚拟机。模拟是一种安全风险。

- 虚拟机可以发送似乎来自不同计算机的帧，以便其可以接收针对该计算机的网络帧。
- 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。

在为标准交换机添加 VMkernel 端口组或虚拟机端口组时，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。可能会尝试实施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。要正确使用安全配置文件中的设置，请参见《《vSphere 网络连接》》出版物中的“安全策略”部分。此部分介绍：

- 虚拟机网络适配器如何控制传输。
- 在此级别上如何实施攻击

## 确保 vSphere 标准交换机的安全

可以通过限制虚拟机网络适配器的一些 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 地址的入站网络流量。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。

### 创建虚拟机网络适配器时会发生什么

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。因此，操作系统可以模拟接收端网络授权的网络适配器，并在网络中的设备上实施恶意攻击。

## 使用安全策略保护端口和组

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：

- MAC 地址更改（请参见 [MAC 地址更改](#)）
- 混杂模式（请参见[混杂模式运行](#)）
- 伪信号（请参见[伪传输](#)）

您可以通过从 vSphere 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。此选项让虚拟机能够接收 Mac 地址不同于 VMX 中所配置地址的帧。

当 **Mac 地址更改** 选项设置为 **接受** 时，ESXi 接受将虚拟机的有效 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 不接受将虚拟机有效 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停用，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获取 MAC 地址更改。如果将 ESXi iSCSI 与 iSCSI 存储一起使用，则将 **MAC 地址更改** 选项设置为 **接受**。

---

有时，可能确实需要多个适配器在一个网络中使用同一 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。

---

**注** 从 vSphere 7.0 开始，**伪信号** 和 **MAC 地址更改** 的默认值已从“接受”更改为“拒绝”。请联系存储供应商进行验证。

---

## 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。

---

**注** 从 vSphere 7.0 开始，**伪传输**和 **MAC 地址更改**的默认值更改为了“拒绝”，而不是“接受”。

---

## 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。

有关为混杂模式配置虚拟机适配器的信息，请参见《vSphere 网络连接》文档中有关为 vSphere 标准交换机或标准端口组配置安全策略的主题。

---

**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）。

---

## 标准交换机保护和 VLAN

通过 VMware 标准交换机可阻止某些威胁 VLAN 安全的行为。标准交换机的设计方式使其可以保护 VLAN 防御各种攻击，其中多种攻击均涉及 VLAN 跳转。

有了这层保护并不能保证您的虚拟机配置不会遭受其他类型的攻击。例如，标准交换机只能保护虚拟网络免遭这些攻击，但不能保护物理网络。

标准交换机和 VLAN 可以抵御以下类型的攻击。

由于将来还会不断出现新的安全威胁，因此请勿将此视作有关攻击的详尽列表。请定期查看网站上的 VMware 安全资源，了解安全警示、近期安全警示及 VMware 安全策略。

### MAC 泛洪攻击

MAC 泛洪攻击会使交换机充满大量数据包，其中包含标记为来自不同源的 MAC 地址。许多交换机使用内容可寻址内存表了解和存储每个数据包的源地址。当此表填满时，交换机会进入完全开放状态，此时将在所有端口广播每个入站数据包，致使攻击者看到交换机上的所有流量。此状况可能导致 VLAN 间的数据包泄漏。

尽管 VMware 标准交换机存储 MAC 地址表，但不会获取来自可观测流量的 MAC 地址，因此不容易受到此类攻击。

### 802.1q 和 ISL 标记攻击

802.1q 和 ISL 标记攻击强制交换机将帧从一个 VLAN 重定向至另一个 VLAN，方法是通过欺骗手段致使交换机充当中继并向其他 VLAN 广播流量。

VMware 标准交换机不执行此类攻击所需的动态中继，因此不会遭到攻击。

## 双重封装攻击

当攻击者创建一个双重封装数据包，其内部标记中的 VLAN 标识符与外部标记中的 VLAN 标识符不同时，双重封装攻击发生。为实现向后兼容性，本机 VLAN 将去除传输数据包的外部标记，除非进行其他配置。当本机 VLAN 交换机去除外部标记后，只剩下内部标记，它将把数据包路由到与所去除外部标记中标识的 VLAN 不同的 VLAN。

VMware 标准交换机会丢弃虚拟机尝试通过为特定 VLAN 配置的端口发送的任何双重封装帧。因此，它们不容易遭到此类攻击。

## 多播暴力攻击

涉及到将大量多播帧几乎同时发送到已知 VLAN，使交换机过载，从而错误地允许向其他 VLAN 广播一些帧。

VMware 标准交换机不允许帧离开其正确的广播域 (VLAN)，因此不容易遭到此类攻击。

## 生成树攻击

生成树攻击针对的是生成树协议 (STP)，此协议用于控制 LAN 组件间的桥接。攻击者发送网桥协议数据单元 (BPDU) 数据包，尝试更改网络拓扑，将攻击者自己建立成为根网桥。作为根网桥，攻击者可以嗅探传输帧的内容。

VMware 标准交换机不支持 STP，因此不容易遭到此类攻击。

## 随机帧攻击

随机帧攻击涉及发送大量数据包，这些数据包的源地址和目标地址保持不变，但字段的长度、类型或内容会随机变化。此类攻击的目标是强制交换机错误地将数据包重新路由到不同 VLAN。

VMware 标准交换机不容易遭到此类攻击。

## 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。

标准交换机中的 VLAN 规则同样适用于 vSphere Distributed Switch 中的 VLAN。有关详细信息，请参见[标准交换机保护和 VLAN](#)。

### 步骤

- 1 对于具有静态绑定的分布式端口组，停用自动扩展功能。

默认情况下，自动扩展处于激活状态。

要停用自动扩展，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。如果未正确跟踪 VLAN ID，错误地重用 ID 可能会允许意外流量。同样，VLAN ID 错误或丢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 需要交换机名称文本框。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上的内部网络连接。没有流量会经过物理网络适配器。

- 6 如果当前未使用 vSphere Distributed Switch 的网络运行状况检查功能，请停用该功能。

默认情况下，网络运行状况检查功能处于停用状态。激活后，运行状况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。网络运行状况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：

- MAC 地址更改（请参见 [MAC 地址更改](#)）
- 混杂模式（请参见[混杂模式运行](#)）
- 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。

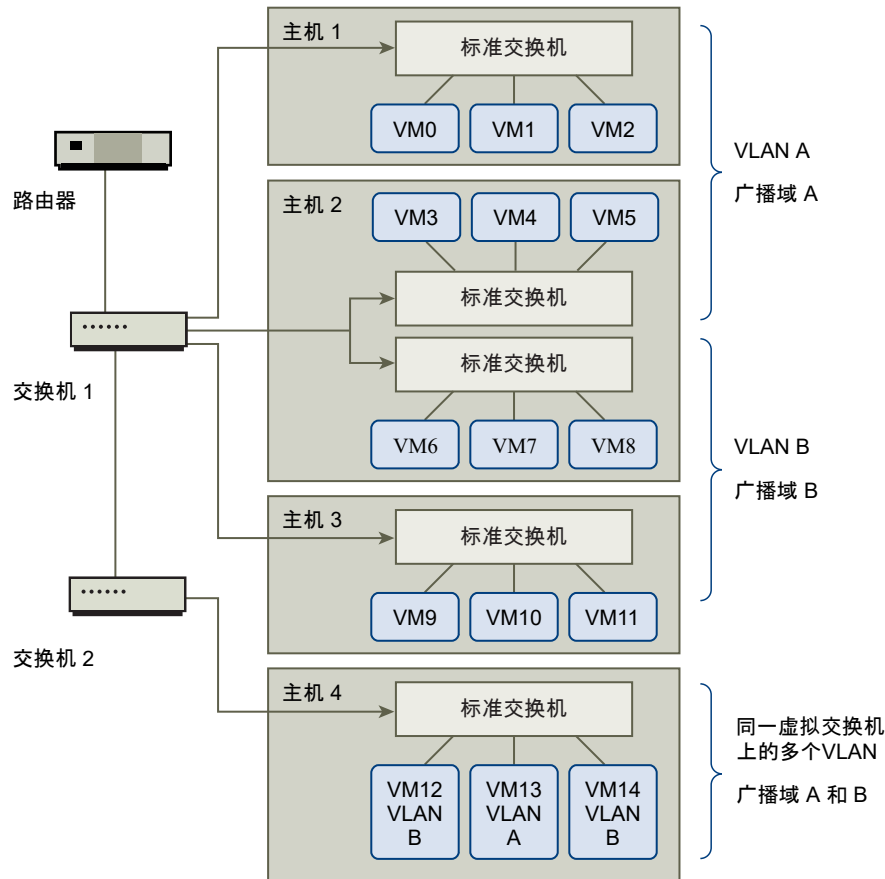
## 通过 VLAN 确保虚拟机安全

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 13-1. 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 4094 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。

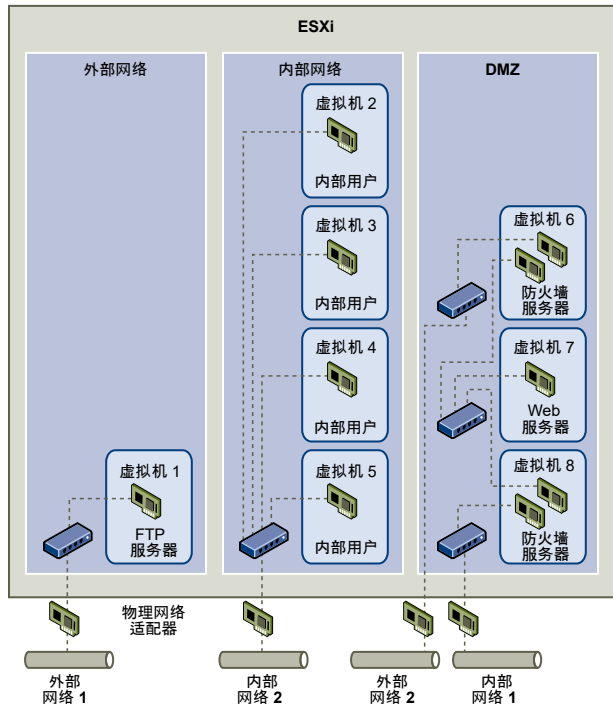
在标准交换机上，可以在交换机或端口组级别上配置 VLAN 网络连接模式，而在 Distributed Switch 上，则在分布式端口组或端口级别。

- 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 13-2. 单台 ESXi 主机上配置的外部网络、内部网络和 DMZ



在该图中，系统管理员将一台主机配置到三个不同的虚拟机区域：FTP 服务器、内部虚拟机和 DMZ。每个区域均提供唯一功能。

### FTP 服务器区域

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。

## 内部网络区域

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 区域

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。

此虚拟机组与外部网络 2 和内部网络 1 相关联。公司使用外部网络 2 支持营销部门和财务部门用来托管公司网站的 Web 服务器，以及公司面向外部用户的其他 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。

## 使用虚拟机区域的优势

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，您可在同一 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分离，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，因此您可以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。如果要确认不存在公用虚拟交换路径，可通过在 vSphere 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。

要保护虚拟机的资源，请为每个虚拟机配置资源预留和限制，以降低 DoS 和 DDoS 攻击的风险。通过在 DMZ 的前端和后端安装软件防火墙，可以进一步保护 ESXi 主机和虚拟机。最后，确保主机位于物理防火墙后面，并配置网络存储资源，以便每个主机都有自己的虚拟交换机。

## 在 ESXi 主机上使用 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 ESXi 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` 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` 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 = 源地址</code>	必需。指定源地址。
<code>--sa-destination = 目标地址</code>	必需。指定目标地址。
<code>--sa-mode = 模式</code>	必需。指定模式 transport 或 tunnel。
<code>--sa-spi = 安全参数索引</code>	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 0x 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 = 加密算法</code>	必需。使用以下参数之一指定加密算法。 <ul style="list-style-type: none"> <li>■ 3des-cbc</li> <li>■ aes128-cbc</li> <li>■ null（不提供任何加密）</li> </ul>
<code>--encryption-key = 加密密钥</code>	在指定加密算法时为必填项。指定加密密钥。可以使用 0x 前缀输入 ASCII 文本或十六进制形式的密钥。
<code>--integrity-algorithm = 身份验证算法</code>	必需。指定身份验证算法 hmac-sha1 或 hmac-sha2-256。

选项	描述
<code>--integrity-key = 身份验证密钥</code>	必需。指定身份验证密钥。可以使用 0x 前缀输入 ASCII 文本或十六进制形式的密钥。
<code>--sa-name = 名称</code>	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 0x6970763672656164796c6f676f3364657363626366f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x6970763672656164796c6f67736861316f757432
--sa-name sal
```

## 移除 IPsec 安全关联

可以使用 ESXCLI 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 security_association_name`。

## 列出可用的 IPsec 安全策略

可以使用 ESXCLI 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** 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
<b>--sp-source = 源地址</b>	必需。指定源 IP 地址和前缀长度。
<b>--sp-destination = 目标地址</b>	必需。指定目标地址和前缀长度。
<b>--source-port = 端口</b>	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。
<b>--destination-port = 端口</b>	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。
<b>--upper-layer-protocol = 协议</b>	使用以下参数之一指定上层协议。 <ul style="list-style-type: none"> <li>■ tcp</li> <li>■ udp</li> <li>■ icmp6</li> <li>■ any</li> </ul>
<b>--flow-direction = 方向</b>	使用 in 或 out 指定要监控流量的方向。
<b>--action = 操作</b>	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"> <li>■ none: 不采取任何操作。</li> <li>■ discard: 不允许数据进出。</li> <li>■ 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。</li> </ul>
<b>--sp-mode = 模式</b>	指定模式 tunnel 或 transport。
<b>--sa-name = 安全关联名称</b>	必需。为要使用的安全策略提供安全关联名称。
<b>--sp-name = 名称</b>	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 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。

ESXi 包括一个可发送通知（陷阱和通知）并接收 GET、GETBULK 和 GETNEXT 请求的 SNMP 代理。默认情况下，未激活 SNMP。必须在每台 ESXi 主机上配置 SNMP。可以使用 ESXCLI、PowerCLI 或 vSphere Web Services SDK 进行配置。

有关配置 SNMP（包括 SNMP v3）的详细信息，请参见《vSphere 监控和性能》文档。SNMP v3 提供比 SNMP v1 或 SNMP v2c 更高的安全性，包括密钥身份验证和加密。有关 `esxcli system snmp` 命令选项的详细信息，请参见《ESXCLI 参考指南》。

### 步骤

- 1 要确定是否使用 SNMP，请运行以下命令。

```
esxcli system snmp get
```

- 2 要激活 SNMP，请运行以下命令。

```
esxcli system snmp set --enable true
```

- 3 要停用 SNMP，请运行以下命令。

```
esxcli system snmp set --enable false
```

## 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 vSphere 网络安全建议

遵循常规网络连接安全建议是确保 vSphere 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。

### 保护 vSphere 网络连接环境的建议

- 生成树协议 (STP) 检测并防止在网络拓扑中形成循环。VMware 虚拟交换机通过其他方式防止形成循环，但不直接支持 STP。网络拓扑发生更改时，网络重新发现拓扑需要一些时间（30 到 50 秒）。在这段时间内，不允许任何流量通过。为避免出现这些问题，网络供应商创建了一些功能，使交换机端口能够继续转发流量。有关详细信息，请参见相应的 VMware 知识库文章，网址为 <https://kb.vmware.com/kb/1003804>。有关正确的网络和网络硬件配置，请参阅您的网络供应商文档。
- 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，可以包含有关虚拟网络的信息。这些信息增加了敏感信息在传输过程中被攻击者查看和捕获的可能性。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，虚拟机管理员只能访问其虚拟机驻留的端口组。网络管理员可以访问所有虚拟网络连接组件，但不能访问虚拟机。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。物理交换机通常配置一个本机 VLAN，默认情况下，该本机 VLAN 通常为 VLAN 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停用状态。如果激活了替代，则可以为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 vSphere 网络组件

标识 vSphere 网络架构的不同组件非常关键，有助于确保网络扩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。

## 在 vSphere 中采用网络隔离做法

网络隔离做法可增强 vSphere 环境的网络安全性。

### 隔离 vSphere 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。

通过按照 ESXi 主机或集群上运行的最安全虚拟机的安全级别来保护管理网络，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标准交换机上的专用 VLAN 中。如果生产虚拟机未使用 vSphere 管理端口组的 VLAN，则生产（虚拟机）流量可以共享标准交换机。

检查网络段是否未路由，其他管理相关的实体所在的网络除外。路由网络段可能对 vSphere Replication 有意义。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。

使用以下方法之一严格控制对管理功能的访问。

- 要在特别敏感环境中访问管理网络，请配置受控网关或其他受控方法。例如，要求管理员通过 VPN 连接到管理网络。仅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堡垒主机。

### 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。有权访问此网络的任何人都可以查看基于 IP 的存储流量。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。攻击者还可能筹划中间人攻击 (MITM) 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。

将通用标准交换机上的专用 VLAN 用于 vMotion 端口组。如果生产虚拟机未使用 vMotion 端口组的 VLAN，则生产（虚拟机）流量可以使用相同的标准交换机。

### 隔离 vSAN 流量

配置 vSAN 网络时，将 vSAN 流量隔离在其自己的第 2 层网络段上。可以通过使用专用交换机或端口或者使用 VLAN 执行此隔离。

## 仅在需要时才在 vSphere Network Appliance API 中使用虚拟交换机

请勿将主机配置为向虚拟机发送网络信息，除非您使用的产品在使用 vSphere Network Appliance API (DvFilter)。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，文档网址为：<https://developer.vmware.com/docs/6518/developing-and-deploying-vsphere-solutions--vservices--and-esx-agents>。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 在 vSphere Client 清单中，浏览到主机。
- 2 单击**配置**。
- 3 在“系统”下，单击**高级系统设置**。
- 4 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”文本框中输入 **DVFilter** 以显示所有相关参数。

- 5 确认设置。
  - 如果未使用 DvFilter 设置，请确保值为空。
  - 如果正使用 DvFilter 设置，请确保参数值正确。该值必须与使用 DvFilter 的产品正在使用的值匹配。

# 涉及多个 vSphere 组件的最佳做法

# 14

一些安全性最佳做法（如在环境中设置 PTP 或 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 3 章 确保 ESXi 主机安全和第 5 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
- 验证是否已停用向客户机发送主机性能数据
- 为 ESXi Shell 和 vSphere Client 设置超时

## 同步 vSphere 网络连接上的时钟

验证 vSphere 网络上所有组件的时钟是否均已同步。如果 vSphere 网络中的物理机时钟不同步，则可能无法在网络计算机之间的通信中将时间敏感的 SSL 证书和 SAML 令牌识别为有效。

时钟不同步可能会引起身份验证问题，从而导致安装失败或 vCenter Server `vmware-vpxd` 服务无法启动。

vSphere 中的时间不一致可能会导致首次引导环境中的组件在不同的服务处失败，具体取决于哪段环境时间不准确以及时间何时同步。目标 vCenter Server 的目标 ESXi 主机与 NTP 或 PTP 不同步时，通常会出现问题。同样，如果目标 vCenter Server 迁移到因 DRS 完全自动化而设置为不同时间的 ESXi 主机，也会出现问题。

要避免时间同步问题，请在安装、迁移或升级 vCenter Server 实例之前，确保以下项正确。

- 要部署目标 vCenter Server 的目标 ESXi 主机同步到 NTP 或 PTP。
- 运行源 vCenter Server 的 ESXi 主机同步到 NTP 或 PTP。
- 从 vSphere 6.7 升级或迁移到 vSphere 8.0 时，如果 vCenter Server Appliance 连接到外部 Platform Services Controller，请确保运行外部 Platform Services Controller 的 ESXi 主机同步到 NTP 或 PTP。
- 如果从 vSphere 6.7 升级或迁移到 vSphere 8.0，请确认源 vCenter Server 或 vCenter Server Appliance 以及外部 Platform Services Controller 的时间正确。

验证运行 vCenter Server 的任何 Windows 主机是否与网络时间协议 (Network Time Protocol, NTP) 服务器同步。请参见 VMware 知识库文章，网址为 <https://kb.vmware.com/s/article/1318>。

要将 ESXi 时钟与 NTP 或 PTP 服务器同步，可以使用 VMware Host Client。有关编辑 ESXi 主机时间配置的信息，请参见《vSphere 单台主机管理 - VMware Host Client》文档中的“在 VMware Host Client 中编辑 ESXi 主机的时间配置”主题。

要了解如何更改 vCenter Server 的时间同步设置，请参见《vCenter Server 配置》文档中的“配置系统时区和时间同步设置”主题。

要了解如何使用 vSphere Client 编辑主机的时间配置，请参见《vCenter Server 和主机管理》文档中的“编辑主机的时间配置设置”主题。

- **使 ESXi 时钟与网络时间服务器同步**

安装 vCenter Server 之前，请确保 vSphere 网络中所有计算机的时钟均已同步。

- **配置 vCenter Server 中的时间同步设置**

可以在部署后更改 vCenter Server 中的时间同步设置。

## 使 ESXi 时钟与网络时间服务器同步

安装 vCenter Server 之前，请确保 vSphere 网络中所有计算机的时钟均已同步。

此任务将介绍如何从 VMware Host Client 设置 NTP。

### 步骤

- 1 启动 VMware Host Client，然后连接到 ESXi 主机。
- 2 单击**管理**。
- 3 在**系统**下，单击**时间和日期**，然后单击**编辑设置**。
- 4 选择**使用网络时间协议 (启用 NTP 客户端)**。
- 5 在“NTP 服务器”文本框中，输入要与其同步的一个或多个 NTP 服务器的 IP 地址或完全限定域名。
- 6 从 **NTP 服务启动策略** 下拉菜单中，选择**随主机启动和停止**。
- 7 单击**保存**。

此时，主机将与 NTP 服务器同步。

## 配置 vCenter Server 中的时间同步设置

可以在部署后更改 vCenter Server 中的时间同步设置。

部署 vCenter Server 时，可以选择时间同步方法：使用 NTP 服务器或使用 VMware Tools。如果 vSphere 网络连接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 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。只能在 vCenter Server 中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，则会停用 vCenter Server VMware Tools 周期性时间同步。

## 使用 VMware Tools 时间同步

可以将 vCenter Server 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 配置中添加或替换 NTP 服务器

要设置 vCenter Server 以使用基于 NTP 的时间同步，必须将 NTP 服务器添加到 vCenter Server 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 通过运行以下 `ntp.set` 命令将 NTP 服务器添加到 vCenter Server 配置中。

```
ntp.set --servers IP-addresses-or-host-names
```

在此命令中，*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。此命令将移除当前 NTP 服务器（如果有），并将新的 NTP 服务器添加到配置。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，此命令会将 NTP 配置中的当前 NTP 服务器替换为您指定的新 NTP 服务器。



- 3 （可选）要验证是否已成功应用新的 NTP 配置设置，请运行以下命令。

```
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。如果已激活 NTP 同步，此命令返回 NTP 配置处于启用状态。如果已停用 NTP 同步，此命令返回 NTP 配置处于禁用状态。

- 4 （可选）要验证 NTP 服务器是否可访问，请运行以下命令。

```
ntp.test --servers IP-addresses-or-host-names
```

该命令将返回 NTP 服务器的状态。

### 后续步骤

如果已停用 NTP 同步，您可以将 vCenter Server 中的时间同步设置配置为基于 NTP 服务器。请参见[将 vCenter Server 中的时间与 NTP 服务器同步](#)。

## 将 vCenter Server 中的时间与 NTP 服务器同步

您可以将 vCenter Server 中的时间同步设置配置为基于 NTP 服务器。

### 前提条件

在 vCenter Server 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 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 vSAN》文档。

## 确保 iSCSI 存储安全

为主机配置的存储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，可采取措施最小化安全风险。

iSCSI 支持使用 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。iSCSI 事务会在 iSCSI 记录中封装原始 SCSI 数据块，并将数据传输到请求设备或用户。

iSCSI SAN 支持高效使用现有以太网基础架构，以便为主机提供对其可动态共享的存储资源的访问权限。iSCSI SAN 是适用于依赖公用存储池服务许多用户的环境的经济型存储解决方案。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，以及与主机关联的 iSCSI 硬件适配器和通过主机直接配置的 iSCSI 的要求和过程，两者类似。

---

### 确保 iSCSI 设备安全

为确保 iSCSI 设备安全，每当 ESXi 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。

身份验证可确保启动器具有访问目标的权利。您在为 iSCSI 设备配置身份验证时授予设备此权利。

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。为每台主机设置不同的双向身份验证密钥。如果可能，也为 ESXi 主机的每个客户端设置不同的密钥。唯一密钥可确保即使一台主机受到影响，攻击者也无法创建其他任意主机并向存储设备进行身份验证。使用共享密钥时，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

使用 NFS 版本 4.1 时，ESXi 支持 Kerberos 身份验证机制。

RPCSEC\_GSS Kerberos 机制是一种身份验证服务。它允许 ESXi 上安装 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 安全在不安全的网络连接中使用加密进行工作。

ESXi 针对 NFS 4.1 实施 Kerberos 可提供两种安全模型：krb5 和 krb5i，分别提供不同的安全级别。

- 仅用于身份验证的 Kerberos (krb5) 支持身份认证。
- 用于身份验证和数据完整性的 Kerberos (krb5i) 除了提供身份认证，还提供数据完整性服务。这些服务通过检查潜在的数据包修改操作，帮助保护 NFS 流量免受篡改。

Kerberos 支持加密算法，可防止未经授权的用户访问 NFS 流量。ESXi 上的 NFS 4.1 客户端尝试使用 AES256-CTS-HMAC-SHA1-96 或 AES128-CTS-HMAC-SHA1-96 算法访问 NAS 服务器上的共享。使用 NFS 4.1 数据存储之前，确保在 NAS 服务器上启用 AES256-CTS-HMAC-SHA1-96 或 AES128-CTS-HMAC-SHA1-96。

下表比较了 ESXi 支持的 Kerberos 安全级别。

表 14-1. Kerberos 安全类型

		ESXi6.0	ESXi6.5 及更高版本
仅用于身份验证的 Kerberos (krb5)	RPC 标头的完整性校验和	是，使用 DES	是，使用 AES
	RPC 数据的完整性校验和	否	否
用于身份验证和数据完整性的 Kerberos (krb5i)	RPC 标头的完整性校验和	无 krb5i	是，使用 AES
	RPC 数据的完整性校验和		是，使用 AES

使用 Kerberos 身份验证时，需要考虑以下注意事项：

- ESXi 使用 Kerberos 与 Active Directory 域。
- 作为 vSphere 管理员，您可以指定 Active Directory 凭据以向 NFS 用户提供 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 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。要自动执行分配过程，请在主机配置文件中设置用户并将配置文件应用于所有 ESXi 主机。
- 不能对多个主机共享的同一个 NFS 4.1 数据存储使用两个安全机制：AUTH\_SYS 和 Kerberos。

有关分步说明，请参见《《vSphere 存储》》文档。

## 验证是否已停用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，向虚拟机发送主机性能数据的功能处于停用状态。此默认设置将阻止虚拟机获取有关物理主机的详细信息。如果出现违反虚拟机安全的行为，此设置不会向攻击者提供主机数据。

**注** 以下步骤说明了基本过程。请考虑使用 ESXCLI 或 VMware PowerCLI 命令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 Client 设置超时

要防止入侵者使用闲置会话，请为 ESXi Shell 和 vSphere Client 设置超时。

## ESXi Shell 超时

对于 ESXi Shell，您可以在 vSphere 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

可用性超时设置是激活 ESXi Shell 后且必须登录前可以经过的时间量。超过超时期限之后，该服务会停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 ESXi Shell 时应用。更改不影响现有会话。

## 更改 vSphere Client 超时

默认情况下，vSphere Client 会话会在 120 分钟后终止。更改默认值，请执行以下操作：

- 1 在 vSphere Client 中，导航到 vCenter Server 实例。
- 2 选择**配置**选项卡，然后选择**设置**下的**常规**。
- 3 单击**编辑**。
- 4 选择**超时设置**。
- 5 输入您的选择，然后单击**保存**。

# 使用 TLS Configurator 实用程序管理 vSphere TLS 协议配置

# 15

vSphere 默认仅激活 TLS。默认已停用 TLS 1.0 和 TLS 1.1。无论是执行全新安装、升级还是迁移，vSphere 都会停用 TLS 1.0 和 TLS 1.1。可以使用 TLS Configurator 实用程序在 vCenter Server 系统上临时激活协议的旧版本。在所有连接都使用 TLS 1.2 后，可以停用安全性较低的旧版本。

从 ESXi 8.0 开始，仅支持 TLS 1.2。ESXi 8.0 不再支持 TLS 1.0 和 1.1，您也无法激活这些较旧的协议版本。在 ESXi 8.0 上运行 TLS Configurator 实用程序失败，但不报告错误。

在 vCenter Server 上重新配置旧协议版本之前，请考虑您的环境。根据环境要求和软件版本，除了启用 TLS 1.2 之外，您可能还需要重新激活 TLS 1.0 和 TLS 1.1 以保持互操作性。请参见 VMware 知识库文章 (<https://kb.vmware.com/s/article/2145796>) 以了解支持 TLS 1.2 的 VMware 产品。对于第三方集成，请参见供应商的文档。TLS Configurator 实用程序适用于 vSphere 8.0 和早期版本，包括 7.0、6.7、6.5 和 6.0。

vCenter Server 使用可为 TLS 协议激活或停用的端口。TLS 配置实用程序的 scan 选项可显示为每个服务激活的 TLS 版本。请参见[扫描 vCenter Server 上的 TLS 协议](#)。

有关 VMware 产品（包括 vSphere 和 vSAN）中所有受支持的端口和协议的列表，请参见 <https://ports.vmware.com/> 中的 VMware Ports and Protocols Tool™。您可以按 VMware 产品搜索端口，创建自定义端口列表，以及打印或保存端口列表。

## vCenter Server 和 Envoy

在 vSphere 7.0 及更高版本中，vCenter Server 运行两个反向代理服务：

- VMware 反向代理服务 rhttpproxy
- Envoy

Envoy 是一个开源 Edge 和服务代理。Envoy 拥有端口 443，所有入站 vCenter Server 请求都通过 Envoy 进行路由。在 vSphere 7.0 及更高版本中，rhttpproxy 用作 Envoy 的配置管理服务器。因此，TLS 配置将应用于 rhttpproxy，而后者又会将配置发送到 Envoy。

## 有关 vSphere 和 TLS 的注意和警告

- vSphere 6.7 版本是适用于 Windows 的 vCenter Server 的最终版本。有关为适用于 Windows 的 vCenter Server 上的 Update Manager 端口重新配置 TLS 的信息，请参见产品 6.7 版本对应的《vSphere 安全性》文档。

- 可以使用 TLS 1.2 对 vCenter Server 和外部 Microsoft SQL Server 之间的连接进行加密。不能使用仅 TLS 1.2 连接来连接到外部 Oracle 数据库。请参见 VMware 知识库文章，网址为 <https://kb.vmware.com/kb/2149745>。
- 对于 vSphere 6.7 及更低版本，请勿对 Windows Server 2008 上运行的 vCenter Server 或 Platform Services Controller 实例停用 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。

本章讨论了以下主题：

- 执行可选的 vCenter Server TLS 手动备份
- 在 vCenter Server 系统上激活或停用 TLS 版本
- 扫描 vCenter Server 上的 TLS 协议
- 恢复 vCenter Server TLS 配置更改

## 执行可选的 vCenter Server TLS 手动备份

每次脚本修改 vCenter Server 时，TLS 配置实用程序都会执行 TLS 配置的备份。如果必须将备份保存到特定目录，则可以执行手动备份。

对于 vCenter Server，默认目录为 `/tmp/yearmonthdayTtime`。

### 步骤

- 1 使用 SSH 连接到 vCenter Server。
- 2 将目录更改为 `/usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator`。
- 3 要备份到特定目录，请运行以下命令：

```
directory_path/VcTlsReconfigurator> ./reconfigureVc backup -d backup_directory_path
```

- 4 确认备份成功完成。

成功的备份类似于以下示例。由于 `reconfigureVc backup` 命令运行的方式不同，每次运行该命令时显示的服务顺序可能会有所不同。

```
vCenter Transport Layer Security reconfigurator, version=8.0.0, build=10068142
For more information refer to the following article: https://kb.vmware.com/kb/2147469
Log file: "/var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log".
===== Backing up vCenter Server TLS configuration =====
Using backup directory: /tmp/20220714T225653
Backing up: vmcam
Backing up: vmdird
Backing up: vmware-rhttpproxy
Backing up: vmware-stds
Backing up: vami-lighttp
Backing up: vmware-rbd-watchdog
```

```
Backing up: rsyslog
Backing up: vmware-updatemgr
Backing up: vmware-sps
Backing up: vmware-vpxd
```

- 5 （可选） 如果稍后必须执行还原，可以运行以下命令。

```
reconfigureVc restore -d optional_custom_backup_directory_path
```

## 在 vCenter Server 系统上激活或停用 TLS 版本

可以使用 TLS 配置实用程序在 vCenter Server 系统上激活或停用 TLS 版本。在此过程中，您可以停用 TLS 1.0 并激活 TLS 1.1 和 TLS 1.2。或者，您可以停用 TLS 1.0 和 TLS 1.1，并且仅激活 TLS 1.2。

### 前提条件

确保 vCenter Server 管理的主机和服务可以使用仍处于激活状态的 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 使用 administrator@vsphere.local 的用户名和密码登录到 vCenter Server 系统，或者以可以运行脚本的其他 vCenter Single Sign-On 管理员组成员的身份登录。
- 2 转到脚本所在的目录。

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

- 3 根据要使用的 TLS 版本，运行以下命令。

- 要停用 TLS 1.0 并同时激活 TLS 1.1 和 TLS 1.2，请运行以下命令。

```
directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.1 TLSv1.2
```

- 要停用 TLS 1.0 和 TLS 1.1 并仅激活 TLS 1.2，请运行以下命令。

```
directory_path/VcTlsReconfigurator> ./reconfigureVc update -p TLSv1.2
```

- 4 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。

## 扫描 vCenter Server 上的 TLS 协议

在 vCenter Server 上激活或停用 TLS 版本后，可以使用 TLS 配置实用程序查看所做更改。

TLS 配置实用程序的 scan 选项可显示为每个服务激活的 TLS 版本。



**步骤**

- 1 登录到 vCenter Server 系统。
  - a 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。
  - b 如果当前未启用 Bash Shell，请运行以下命令。

```
shell.set --enabled true
shell
```

- 2 转到 VcTlsReconfigurator 目录。

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

- 3 要显示哪些服务已激活 TLS 及使用哪些端口，请运行以下命令。

```
reconfigureVc scan
```

## 恢复 vCenter Server 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，系统会激活您使用 TLS Configurator 实用程序停用的协议。

**前提条件**

恢复更改之前，请使用 vCenter Server 管理界面备份 vCenter Server。

**步骤**

- 1 以具有脚本运行特权的用户身份连接到要恢复更改的 vCenter Server。
- 2 如果当前未启用 Bash shell，请运行以下命令。

```
shell.set --enabled true
shell
```

- 3 转到 VcTlsReconfigurator 目录。

```
cd /usr/lib/vmware-TlsReconfigurator/VcTlsReconfigurator
```

- 4 查看以前的备份。

```
grep "backup directory" /var/log/vmware/vSphere-TlsReconfigurator/VcTlsReconfigurator.log
```

输出类似于以下示例。

```
2022-07-14T22:56:53.706Z INFO Using backup directory: /tmp/20220714T225653
2022-07-14T22:58:08.594Z INFO Using backup directory: /tmp/20220714T225808
```

- 5 运行以下命令以执行还原。

```
reconfigureVc restore -d Directory_path_from_previous_step
```

将还原 TLS 配置。在该过程中，会重新启动 vCenter Server。

- 6 对任何其他 vCenter Server 实例重复此过程。

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。

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  
的访问权限之外，有些操作还需要对根文件夹或父文件夹的访问权限。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
- 证书颁发机构特权
- 证书管理特权
- Cns 特权
- 计算策略特权
- 内容库特权
- 加密操作特权
- dvPort 组特权
- Distributed Switch 特权
- 数据中心特权
- 数据存储特权
- 数据存储集群特权
- ESX Agent Manager 特权
- 扩展特权
- 外部统计信息提供程序特权
- 文件夹特权
- 全局特权

- 混合链接模式特权
- 运行状况更新提供程序特权
- 主机 CIM 特权
- 主机配置特权
- 主机熵池特权
- 主机 Intel Software Guard Extensions 特权
- 主机清单特权
- 主机本地操作特权
- 主机统计信息特权
- 托管可信平台模块特权
- 主机 vSphere Replication 特权
- 主机配置文件特权
- vCenter Server 配置文件特权
- vSphere with Tanzu 特权
- 网络特权
- NSX 特权
- VMware 可观察性特权
- OvfManager 特权
- 与合作伙伴 Rest 守护进程交互特权
- 性能特权
- 插件特权
- 权限特权
- 资源特权
- 已调度任务特权
- 会话特权
- 虚拟机存储策略特权
- 存储视图特权
- 主管服务特权
- 任务特权
- 租户管理特权
- Transfer Service 特权

- VcTrusts/VcIdentity 特权
- 可信基础架构管理员特权
- vApp 特权
- VcIdentityProviders 特权
- VMware vSphere Lifecycle Manager 配置特权
- VMware vSphere Lifecycle Manager ESXi 运行状况视图特权
- VMware vSphere Lifecycle Manager 常规特权
- VMware vSphere Lifecycle Manager 硬件兼容性特权
- VMware vSphere Lifecycle Manager 映像特权
- VMware vSphere Lifecycle Manager 映像修复特权
- VMware vSphere Lifecycle Manager 设置特权
- VMware vSphere Lifecycle Manager 管理基准特权
- VMware vSphere Lifecycle Manager 管理修补程序和升级特权
- VMware vSphere Lifecycle Manager 上载文件特权
- 虚拟机更改配置特权
- 虚拟机客户机操作特权
- 虚拟机交互特权
- 虚拟机编辑清单特权
- 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
- 虚拟机类特权
- vSAN 特权
- vSphere 区域特权
- vService 特权
- vSphere 标记特权
- vSphere Client 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 16-1. 警报特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
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	Alarm.Acknowledge
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	Alarm.Create
禁用警报操作	允许阻止警报操作在触发警报后发生。警报本身未停用。	对其定义了警报的对象	Alarm.DisableActions
在实体上禁用或启用警报	允许激活或停用特定目标类型的特定警报。	警报可触发的对象	Alarm.ToggleEnableOnEntity
修改警报	允许更改警报的属性。	对其定义了警报的对象	Alarm.Edit
移除警报	允许删除警报。	对其定义了警报的对象	Alarm.Delete
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 <b>正常</b> 、 <b>警告</b> 或 <b>警示</b> 。	对其定义了警报的对象	Alarm.SetStatus

## 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。有关 Auto Deploy 的详细信息，请参见《VMware ESXi 安装和设置》文档。

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 16-2. Auto Deploy 特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>主机           <ul style="list-style-type: none"> <li>管理计算机</li> </ul> </li> </ul>	允许用户关联主机与计算机。	vCenter Server	AutoDeploy.Host.AssociateMachine
<ul style="list-style-type: none"> <li>映像配置文件           <ul style="list-style-type: none"> <li>创建</li> <li>编辑</li> </ul> </li> </ul>	<b>创建</b> 允许创建映像配置文件。 <b>编辑</b> 允许编辑映像配置文件。	vCenter Server	AutoDeploy.Profile.Create AutoDeploy.Profile.Edit
<ul style="list-style-type: none"> <li>规则           <ul style="list-style-type: none"> <li>创建</li> <li>编辑</li> <li>删除</li> </ul> </li> </ul>	<b>创建</b> 允许创建 Auto Deploy 规则。 <b>编辑</b> 允许编辑 Auto Deploy 规则。 <b>删除</b> 允许删除 Auto Deploy 规则。	vCenter Server	AutoDeploy.Rule.Create AutoDeploy.Rule.Edit AutoDeploy.Rule.Delete
<ul style="list-style-type: none"> <li>规则集           <ul style="list-style-type: none"> <li>激活</li> <li>编辑</li> </ul> </li> </ul>	<b>激活</b> 允许激活 Auto Deploy 规则集。 <b>编辑</b> 允许编辑 Auto Deploy 规则集。	vCenter Server	AutoDeploy.RuleSet.Activate AutoDeploy.RuleSet.Edit

## 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。有关 vCenter Server 证书管理的信息，请参见《vSphere 身份验证》文档中的“证书管理操作所需的特权”。

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 16-3. 主机证书特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
管理证书	允许对 ESXi 主机进行证书管理。	vCenter Server	Certificate.Manage

## 证书颁发机构特权

证书颁发机构特权控制 VMware Certificate Authority (VMCA) 证书的各个方面。

表 16-4. 证书颁发机构特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
创建/删除 (管理员特权)。	允许对 vCenter Server 证书的管理进行完全管理级访问。	vCenter Server	CertificateAuthority.Administer
创建/删除 (低于管理员特权)。	允许在 vSphere Client 的“证书管理”页面中查看 VMCA 根证书。	vCenter Server	CertificateAuthority.Manage

## 证书管理特权

证书管理特权控制哪些用户可以管理 vCenter Server 证书。

表 16-5. 证书管理特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
创建/删除 (管理员特权)。	允许对 vCenter Server 证书相关操作的各种内部 API 和功能进行完全管理级访问。	vCenter Server	CertificateManagement.Administer
创建/删除 (低于管理员特权)。	<p>允许减少对各种内部 API 和功能的管理访问。此特权限制证书相关操作，这样用户便无法升级非管理员特权。允许的操作有：</p> <ul style="list-style-type: none"> <li>■ 生成证书签名请求</li> <li>■ 创建和检索受信任的根链</li> <li>■ 删除具有 <b>证书管理.创建/删除 (低于管理员特权)</b> 的特权的用户创建的受信任的根链</li> <li>■ 正在检索计算机 SSL 证书</li> <li>■ 检索用于验证 vCenter Server 颁发的令牌的签名证书链</li> </ul>	vCenter Server	CertificateManagement.Manage



## Cns 特权

云原生存储 (Cns) 特权控制哪些用户可以访问云原生存储 UI。

表 16-6. Cns 特权

vSphere Client 中的 特权名称	描述	要求	API 中的特权名称
可搜索	允许存储管理员查看云原生存储 UI。	根 vCenter Server	Cns.Searchable

## 计算策略特权

计算策略特权控制管理计算策略的能力。

表 16-7. 计算策略特权

vSphere Client 中的 特权名称	描述	要求	API 中的特权名称
创建和删除计算策略	允许创建和删除计算策略。	根 vCenter Server	ComputePolicy.Manage

## 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。

**注** 内容库权限的继承可在单个 vCenter Server 实例的上下文中进行。但是在清单中，内容库并非 vCenter Server 系统的直接子级。内容库的直接父级是全局根对象。这种关系意味着如果在 vCenter Server 级别设置权限并将其传播到子对象，该权限将应用于数据中心、文件夹、集群、主机、虚拟机等，但不会应用于该 vCenter Server 实例中显示和操作的内容库。要分配内容库的权限，管理员必须将该权限作为全局权限授予用户。全局权限支持从全局根对象跨多个解决方案分配特权。

表 16-8. 内容库特权

vSphere Client 中的 特权名称	描述	要求	API 中的特权名称
添加库项目	允许在库中添加项目。	库	ContentLibrary.AddLibraryItem
将根证书添加到信任存储	允许将根证书添加到可信根证书存储。	vCenter Server	ContentLibrary.AddCertToTrustStore
签入模板	允许签入模板。	库	ContentLibrary.CheckInTemplate
签出模板	允许签出模板。	库	ContentLibrary.CheckOutTemplate
为已发布库创建订阅	允许创建库订阅。	库	ContentLibrary.AddSubscription

表 16-8. 内容库特权（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
创建本地库	允许在指定的 vCenter Server 系统上创建本地库。	vCenter Server	ContentLibrary.CreateLocalLibrary
创建或删除 Harbor 注册表	允许创建或删除 VMware Tanzu Harbor 注册表服务。	在其上进行创建的 vCenter Server。要删除的注册表。	ContentLibrary.ManageRegistry
创建已订阅库	允许创建已订阅库。	vCenter Server	ContentLibrary.CreateSubscribedLibrary
创建、删除或清除 Harbor 注册表项目	允许创建、删除或清除 VMware Tanzu Harbor 注册表项目。	注册表	ContentLibrary.ManageRegistryProject
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。	ContentLibrary.DeleteLibraryItem
删除本地库	允许删除本地库。	库	ContentLibrary.DeleteLocalLibrary
从信任存储中删除根证书	允许从可信根证书存储中删除根证书。	vCenter Server	ContentLibrary.DeleteCertFromTrustStore
删除已订阅库	允许删除已订阅库。	库	ContentLibrary.DeleteSubscribedLibrary
删除已发布库的订阅	允许删除库订阅。	库	ContentLibrary.DeleteSubscription
下载文件	允许从内容库下载文件。	库	ContentLibrary.DownloadSession
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。	ContentLibrary.EvictLibraryItem
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	ContentLibrary.EvictSubscribedLibrary

表 16-8. 内容库特权（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
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，将停用内容库管理员的此特权。由于从存储 URL 导入意味着导入内容，因此只有在需要时以及在执行导入的用户不存在安全问题时，才激活此特权。	库	ContentLibrary.ImportStorage
在指定计算资源上管理 Harbor 注册表资源	允许管理 VMware Tanzu Harbor 注册表资源。	计算集群	ContentLibrary.ManageClusterRegistryResource
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	ContentLibrary.ProbeSubscription
将库项目发布到其订阅者	允许将库项目发布到订阅者。	库。将此权限设置为传播到所有库项目。	ContentLibrary.PublishLibraryItem
将库发布到其订阅者	允许将库发布到订阅者。	库	ContentLibrary.PublishLibrary
读取存储	允许读取内容库存储。	库	ContentLibrary.ReadStorage
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。	ContentLibrary.SyncLibraryItem
同步已订阅库	允许同步已订阅库。	库	ContentLibrary.SyncLibrary
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	ContentLibrary.TypeIntrospection
更新配置设置	允许更新配置设置。没有与此特权关联的 vSphere Client 用户界面元素。	库	ContentLibrary.UpdateConfiguration
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	ContentLibrary.UpdateSession

表 16-8. 内容库特权（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
更新库	允许更新内容库。	库	ContentLibrary.UpdateLibrary
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。	ContentLibrary.UpdateLibraryItem
更新本地库	允许更新本地库。	库	ContentLibrary.UpdateLocalLibrary
更新已订阅库	允许更新已订阅库的属性。	库	ContentLibrary.UpdateSubscribedLibrary
更新已发布库的订阅	允许更新订阅参数。用户可以更新已订阅库的 vCenter Server 实例规范及其虚拟机模板项的放置等参数。	库	ContentLibrary.UpdateSubscription
查看配置设置	允许查看配置设置。没有与此特权关联的 vSphere Client 用户界面元素。	库	ContentLibrary.GetConfiguration

## 加密操作特权

加密操作特权控制哪些人可以在哪些对象类型上执行哪些类型的加密操作。

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 16-9. 加密操作特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
直接访问	允许用户访问加密资源。用户可以导出虚拟机，对虚拟机进行 NFC 访问以及打开与加密虚拟机的控制台会话。	虚拟机、主机或数据存储	Cryptographer.Access
添加磁盘	允许用户向加密虚拟机添加磁盘。	虚拟机	Cryptographer.AddDisk
克隆	允许用户克隆加密虚拟机。	虚拟机	Cryptographer.Clone
解密	允许用户解密虚拟机或磁盘。	虚拟机	Cryptographer.Decrypt

表 16-9. 加密操作特权（续）

vSphere Client 中的			
特权名称	描述	要求	API 中的特权名称
加密	允许用户加密虚拟机或虚拟机磁盘。	虚拟机	Cryptographer.Encrypt
加密新项	允许用户在创建虚拟机时加密虚拟机或在创建磁盘时加密磁盘。	虚拟机文件夹	Cryptographer.EncryptNew
管理加密策略	允许用户使用加密 IO 筛选器管理虚拟机存储策略。默认情况下，使用加密存储策略的虚拟机不使用其他存储策略。	vCenter Server root 文件夹	Cryptographer.ManageEncryptionPolicy
管理 KMS	允许用户管理 vCenter Server 系统的密钥管理服务。管理任务包括添加和移除 KMS 实例以及与 KMS 建立信任关系。	vCenter Server 系统	Cryptographer.ManageKeyServers
管理密钥	允许用户执行密钥管理操作。不支持通过 vSphere Client 执行这些操作，但可以通过使用 crypto-util 或 API 执行。	vCenter Server root 文件夹	Cryptographer.ManageKeys
迁移	允许用户将加密虚拟机迁移到其他 ESXi 主机。支持使用或不使用 vMotion 和 Storage vMotion 进行迁移。支持迁移到不同的 vCenter Server 实例。	虚拟机	Cryptographer.Migrate
重新加密	允许用户使用其他密钥重新加密虚拟机或磁盘。深层和浅层重新加密操作均需要此特权。	虚拟机	Cryptographer.Recrypt

表 16-9. 加密操作特权（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
注册虚拟机	允许用户向 ESXi 主机注册加密虚拟机。	虚拟机文件夹	Cryptographer.RegisterVM
注册主机	允许用户在主机上启用加密。可以在主机上明确启用加密，或者在虚拟机创建过程中启用加密。	主机文件夹（对于独立主机），集群（对于集群中的主机）	Cryptographer.RegisterHost
读取 KMS 信息	允许用户列出 vCenter Server 和主机上的 vSphere Native Key Provider。还允许用户获取 vSphere Native Key Provider 信息。	vCenter Server 或主机	Cryptographer.ReadKeyServersInfo

## 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 16-10. 分布式虚拟端口组特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
创建	允许创建分布式虚拟端口组。	虚拟端口组	DVPortgroup.Create
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	DVPortgroup.Delete
修改	允许修改分布式虚拟端口组的配置。	虚拟端口组	DVPortgroup.Modify
策略操作	允许设置分布式虚拟端口组的策略。	虚拟端口组	DVPortgroup.PolicyOp
范围操作	允许设置分布式虚拟端口组的范围。	虚拟端口组	DVPortgroup.ScopeOp

## 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 16-11. vSphere Distributed Switch 特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
创建	允许创建 Distributed Switch。	数据中心、网络文件夹	DVSwitch.Create
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	DVSwitch.Delete
主机操作	允许更改 Distributed Switch 的主机成员。	Distributed Switch	DVSwitch.HostOp
修改	允许更改 Distributed Switch 的配置。	Distributed Switch	DVSwitch.Modify
移动	允许将 vSphere Distributed Switch 移动到其他文件夹。	Distributed Switch	DVSwitch.Move
Network I/O Control 操作	允许更改 vSphere Distributed Switch 的资源设置。	Distributed Switch	DVSwitch.ResourceManagement
策略操作	允许更改 vSphere Distributed Switch 的策略。	Distributed Switch	DVSwitch.PolicyOp
端口配置操作	允许更改 vSphere Distributed Switch 中端口的配置。	Distributed Switch	DVSwitch.PortConfig
端口设置操作	允许更改 vSphere Distributed Switch 中端口的设置。	Distributed Switch	DVSwitch.PortSetting
VSPAN 操作	允许更改 vSphere Distributed Switch 的 VSPAN 配置。	Distributed Switch	DVSwitch.Vspan

## 数据中心特权

数据中心特权控制在 vSphere 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 16-12. 数据中心特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
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	Datacenter.Create
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	Datacenter.Move
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	Datacenter.IpPoolConfig
查询 IP 池分配	允许 IP 地址池的配置。	数据中心	Datacenter.IpPoolQueryAllocations
重新配置数据中心	允许重新配置数据中心。	数据中心	Datacenter.Reconfigure
释放 IP 分配	允许为数据中心发布分配的 IP 分配。	数据中心	Datacenter.IpPoolReleaseIp
移除数据中心	允许移除数据中心。 要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	Datacenter.Delete
重命名数据中心	允许更改数据中心的名称。	数据中心	Datacenter.Rename
更新数据中心碳信息	允许收集与能量和碳测量相关的衡量指标。	数据中心	Datacenter.UpdateCarbonInfo

## 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 16-13. 数据存储特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
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	Datastore.AllocateSpace
浏览数据存储	允许浏览数据存储上的文件。	数据存储	Datastore.Browse
配置数据存储 IO 管理	允许配置 Storage I/O Control。	数据存储	Datastore.ConfigIOManagement
配置数据存储	允许配置数据存储。	数据存储	Datastore.Config



表 16-13. 数据存储特权（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
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	Datastore.FileManagement
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	Datastore.Move
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	Datastore.Delete
移除文件	允许在数据存储中删除文件。 此特权已弃用。 分配 <b>低级别文件操作</b> 特权。	数据存储	Datastore.DeleteFile
重命名数据存储	允许重命名数据存储。	数据存储	Datastore.Rename
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	Datastore.UpdateVirtualMachineFiles
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	Datastore.UpdateVirtualMachineMetadata

## 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 16-14. 数据存储集群特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
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	StoragePod.Config

## 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 16-15. ESX Agent Manager

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
配置	允许在主机或集群上部署代理虚拟机。	虚拟机	EAM.Config
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	EAM.Modify
查看	允许查看代理虚拟机。	虚拟机	EAM.View

## 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 16-16. 扩展特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
注册扩展	允许注册扩展（插件）。	根 vCenter Server	Extension.Register
取消注册扩展	允许取消注册扩展（插件）。	根 vCenter Server	Extension.Unregister
更新扩展	允许更新扩展（插件）。	根 vCenter Server	Extension.Update

## 外部统计信息提供程序特权

外部统计信息提供程序特权控制是否能够向 vCenter Server 通知主动式 Distributed Resource Scheduler (DRS) 统计信息。

这些特权仅适用于 VMware 内部 API。

## 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 16-17. 文件夹特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
创建文件夹	允许创建新文件夹。	文件夹	Folder.Create
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	Folder.Delete
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	Folder.Move
重命名文件夹	允许更改文件夹的名称。	文件夹	Folder.Rename

## 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 16-18. 全局特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
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	Global.VCServer
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	Global.CancelTask
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	Global.CapacityPlanning

表 16-18. 全局特权（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
诊断	允许检索诊断文件、日志头、二进制文件或诊断包的列表。 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	Global.Diagnostics
禁用方法	允许 vCenter Server 扩展的服务器对 vCenter Server 管理的对象停用某些操作。	根 vCenter Server	Global.DisableMethods
启用方法	允许 vCenter Server 扩展的服务器对 vCenter Server 管理的对象激活某些操作。	根 vCenter Server	Global.EnableMethods
全局标记	允许添加或移除全局标记。	根主机或 vCenter Server	Global.GlobalTag
运行状况	允许查看 vCenter Server 组件的健康状况。	根 vCenter Server	Global.Health
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	Global.Licenses
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	Global.LogEvent
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	Global.ManageCustomFields
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	Global.Proxy
脚本操作	允许调度脚本操作和警报。	任何对象	Global.ScriptAction
服务管理器	允许在 ESXCLI 中使用 <code>resxstop</code> 命令。	根主机或 vCenter Server	Global.ServiceManagers
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	Global.SetCustomField
设置	允许读取并修改运行时 vCenter Server 配置设置。	根 vCenter Server	Global.Settings
系统标记	允许添加或移除系统标记。	根 vCenter Server	Global.SystemTag

## 混合链接模式特权

混合链接模式特权控制将云 vCenter Server 实例与内部部署 vCenter Single Sign-On 域链接的各个方面。（适用于 VMware Cloud on AWS。）

表 16-19. 混合链接模式特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
创建	允许创建和删除社区所需的完整管理级别访问权限。	SDDC	HLM.Create
管理	允许为源创建信任和访问社区（读取级别）。	SDDC	HLM.Manage

## 运行状况更新提供程序特权

运行状况更新提供程序特权控制硬件供应商是否能够向 vCenter Server 通知 Proactive HA 事件。

这些特权仅适用于 VMware 内部 API。

## 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 16-20. 主机 CIM 特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
■ CIM	允许客户端获取用于 CIM 服务的票证。	主机	Host.Cim.CimInteraction
■ CIM 交互			

## 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 16-21. 主机配置特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
■ 配置 ■ 高级设置	允许设置高级主机配置选项。	主机	Host.Config.AdvancedConfig
■ 配置 ■ 身份验证存储	允许配置 Active Directory 身份验证存储。	主机	Host.Config.AuthenticationStore
■ 配置 ■ 更改 PciPassthru 设置	允许更改主机的 PciPassthru 设置。	主机	Host.Config.PciPassthru
■ 配置 ■ 更改 SNMP 设置	允许更改主机的 SNMP 设置。	主机	Host.Config.Snmp
■ 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	Host.Config.DateTime
■ 配置 ■ 更改设置	允许在 ESXi 主机上设置锁定模式。	主机	Host.Config.Settings
■ 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	Host.Config.Connection
■ 配置 ■ 固件	允许更新 ESXi 主机的固件。	主机	Host.Config.Firmware
■ 配置 ■ GuestStore 设置	允许对 GuestStore 进行更改。	GuestStore 存储库	Host.Config.GuestStore
■ 配置 ■ 超线程	允许激活和停用主机 CPU 调度程序中的超线程。	主机	Host.Config.HyperThreading
■ 配置 ■ 映像配置	允许更改与主机关联的映像。		Host.Config.Image
■ 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	Host.Config.Maintenance
■ 配置 ■ 内存配置	允许修改主机配置。	主机	Host.Config.Memory
■ 配置 ■ NVDIMM	允许读取和配置非易失性 DIMM。	主机	Host.Config.Nvdimmm
■ 配置 ■ 网络配置	允许配置网络、防火墙和 vMotion 网络。	主机	Host.Config.Network
■ 配置 ■ 电源	允许配置主机电源管理设置。	主机	Host.Config.Power
■ 配置 ■ ProductLocker 设置	允许配置 ESXi productlocker 文件夹。	主机	Host.Config.ProductLocker
■ 配置 ■ 隔离	允许将主机置于隔离模式。	主机	Host.Config.Quarantine

表 16-21. 主机配置特权（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>配置           <ul style="list-style-type: none"> <li>查询修补程序</li> </ul> </li> </ul>	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	Host.Config.Patch
<ul style="list-style-type: none"> <li>配置           <ul style="list-style-type: none"> <li>安全配置文件和防火墙</li> </ul> </li> </ul>	允许配置 Internet 服务，如 SSH、Telnet、SNMP 和主机防火墙。	主机	Host.Config.NetService
<ul style="list-style-type: none"> <li>配置           <ul style="list-style-type: none"> <li>存储分区配置</li> </ul> </li> </ul>	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	Host.Config.Storage
<ul style="list-style-type: none"> <li>配置           <ul style="list-style-type: none"> <li>系统管理</li> </ul> </li> </ul>	允许扩展以便操作主机上的文件系统。	主机	Host.Config.SystemManagement
<ul style="list-style-type: none"> <li>配置           <ul style="list-style-type: none"> <li>系统资源</li> </ul> </li> </ul>	允许更新系统资源层次结构的配置。	主机	Host.Config.Resources
<ul style="list-style-type: none"> <li>配置           <ul style="list-style-type: none"> <li>虚拟机自动启动配置</li> </ul> </li> </ul>	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	Host.Config.AutoStart

## 主机熵池特权

主机熵池特权控制查看和添加 ESXi 主机熵的能力。

表 16-22. 主机熵池特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>熵池           <ul style="list-style-type: none"> <li>读取</li> </ul> </li> </ul>	允许读取主机熵池信息。	主机	Host.Entropy.Read
<ul style="list-style-type: none"> <li>熵池           <ul style="list-style-type: none"> <li>写入</li> </ul> </li> </ul>	允许向主机熵池添加熵。	主机	Host.Entropy.Write

## 主机 Intel Software Guard Extensions 特权

主机 Intel Software Guard Extensions 特权控制多插槽 ESXi 主机上远程证明的各个方面。

表 16-23. 主机 Intel Software Guard Extensions (SGX) 特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>Intel Software Guard Extensions (SGX)</li> <li>Intel Software Guard Extensions (SGX) 注册主机</li> </ul>	允许向 Intel SGX 注册服务注册主机（使 SGX 工作负载能够在支持多插槽 SGX 的主机上运行时执行 SGX 远程证明）。	主机	Host.Sgx.Register

## 主机清单特权

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 16-24. 主机清单特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>清单               <ul style="list-style-type: none"> <li>将主机添加到集群</li> </ul> </li> </ul>	允许将主机添加到现有集群。	集群	Host.Inventory.AddHostToCluster
<ul style="list-style-type: none"> <li>清单               <ul style="list-style-type: none"> <li>添加独立主机</li> </ul> </li> </ul>	允许添加独立主机。	主机文件夹	Host.Inventory.AddStandaloneHost
<ul style="list-style-type: none"> <li>清单               <ul style="list-style-type: none"> <li>创建集群</li> </ul> </li> </ul>	允许创建新集群。	主机文件夹	Host.Inventory.CreateCluster
<ul style="list-style-type: none"> <li>清单               <ul style="list-style-type: none"> <li>管理集群生命周期</li> </ul> </li> </ul>	允许管理集群。	集群	Host.Inventory.ManageClusterLifecycle
<ul style="list-style-type: none"> <li>清单               <ul style="list-style-type: none"> <li>修改集群</li> </ul> </li> </ul>	允许更改集群的属性。	集群	Host.Inventory.EditCluster
<ul style="list-style-type: none"> <li>清单               <ul style="list-style-type: none"> <li>移动集群或独立主机</li> </ul> </li> </ul>	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。	集群	Host.Inventory.MoveCluster
<ul style="list-style-type: none"> <li>清单               <ul style="list-style-type: none"> <li>移动主机</li> </ul> </li> </ul>	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。	集群	Host.Inventory.MoveHost



表 16-24. 主机清单特权（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>■ 清单 <ul style="list-style-type: none"> <li>■ 移除集群</li> </ul> </li> </ul>	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	Host.Inventory.DeleteCluster
<ul style="list-style-type: none"> <li>■ 清单 <ul style="list-style-type: none"> <li>■ 移除主机</li> </ul> </li> </ul>	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	Host.Inventory.RemoveHostFromCluster
<ul style="list-style-type: none"> <li>■ 清单 <ul style="list-style-type: none"> <li>■ 重命名集群</li> </ul> </li> </ul>	允许重命名集群。	集群	Host.Inventory.RenameCluster

## 主机本地操作特权

主机本地操作特权控制当 VMware Host 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 16-25. 主机本地操作特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>■ 本地操作 <ul style="list-style-type: none"> <li>■ 将主机添加到 vCenter</li> </ul> </li> </ul>	允许安装和卸载主机上的 vCenter Agent，如 vpxa 和 aam。	根主机	Host.Local.InstallAgent
<ul style="list-style-type: none"> <li>■ 本地操作 <ul style="list-style-type: none"> <li>■ 创建虚拟机</li> </ul> </li> </ul>	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	Host.Local.CreateVM
<ul style="list-style-type: none"> <li>■ 本地操作 <ul style="list-style-type: none"> <li>■ 删除虚拟机</li> </ul> </li> </ul>	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	Host.Local.DeleteVM
<ul style="list-style-type: none"> <li>■ 本地操作 <ul style="list-style-type: none"> <li>■ 管理用户组</li> </ul> </li> </ul>	允许在主机上管理本地帐户。	根主机	Host.Local.ManageUserGroups
<ul style="list-style-type: none"> <li>■ 本地操作 <ul style="list-style-type: none"> <li>■ 重新配置虚拟机</li> </ul> </li> </ul>	允许对虚拟机进行重新配置。	根主机	Host.Local.ReconfigVM

## 主机统计信息特权

主机统计信息特权控制从数据处理单元 (DPU) 访问统计信息的能力。

这些特权仅适用于 VMware 内部 API。

## 托管可信平台模块特权

主机可信平台模块特权控制与管理可信平台模块 (TPM) 芯片相关的操作。

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 16-26. 托管可信平台模块特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>可信平台模块           <ul style="list-style-type: none"> <li>读取</li> <li>解封</li> </ul> </li> </ul>	<p><b>读取</b> 允许读取有关 ESXi 主机中安装的 TPM 状态的详细信息。</p> <p><b>解封</b> 允许请求 ESXi 主机解密质询以证明其状态。</p>	主机	<p>Host.Tpm.Read</p> <p>Host.Tpm.Unsel</p>

## 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 16-27. 主机 vSphere Replication 特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>vSphere Replication           <ul style="list-style-type: none"> <li>管理复制</li> </ul> </li> </ul>	允许管理此主机上的虚拟机复制。	主机	Host.Hbr.HbrManagement

## 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 16-28. 主机配置文件特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
清除	允许清除配置文件相关信息。	根 vCenter Server	Profile.Clear
创建	允许创建主机配置文件。	根 vCenter Server	Profile.Create

表 16-28. 主机配置文件特权（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
删除	允许删除主机配置文件。	根 vCenter Server	Profile.Delete
编辑	允许编辑主机配置文件。	根 vCenter Server	Profile.Edit
导出	允许导出主机配置文件。	根 vCenter Server	Profile.Export
查看	允许查看主机配置文件。	根 vCenter Server	Profile.View

## vCenter Server 配置文件特权

vCenter Server 配置文件特权控制列出配置文件以及将配置从一个 vCenter Server 导出和导入到另一个的方方面面。

表 16-29. vCenter Server 配置文件特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
vCenter Server 配置文件读取特权	允许列出和导出 vCenter Server 配置文件	vCenter Server	Infraprofile.Read
vCenter Server 配置文件写入特权	允许将配置文件导入到另一个 vCenter Server 并对其进行验证。	vCenter Server	Infraprofile.Write

## vSphere with Tanzu 特权

命名空间特权控制哪些用户可以创建和管理 VMware vSphere® with VMware Tanzu™ 命名空间。

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 16-30. 命名空间特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
允许磁盘取消配置操作	允许对数据存储执行取消配置操作。	数据存储	Namespaces.ManageDisks
备份工作负载组件文件	允许备份 etcd 集群的内容（仅在 VMware Cloud on AWS 中使用）。	集群	Namespaces.Backup
列出可访问的命名空间	允许列出可访问的命名空间。	集群	Namespaces.ListAccess
修改集群范围的配置	允许修改集群范围的配置，以及激活和停用集群命名空间。	集群	Namespaces.ManageCapabilities

表 16-30. 命名空间特权（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
修改集群范围的命名空间自助服务配置	允许修改命名空间自助服务配置。	集群 （用于激活和取消激活） 模板 （用于修改配置） vCenter Server （用于创建模板）	Namespaces.SelfServiceManage
修改命名空间配置	允许修改命名空间配置选项，如资源分配和用户权限。	集群	Namespaces.Manage
切换集群功能	允许操作集群功能的状态（仅在 VMware Cloud on AWS 内部使用）。	集群	不适用
将集群升级到较新版本	允许启动集群升级。	集群	Namespaces.Upgrade

## 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 16-31. 网络特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
分配网络	允许将网络分配到虚拟机。	网络、虚拟机	Network.Assign
配置	允许配置网络。	网络、虚拟机	Network.Config
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	Network.Move
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	Network.Delete

## NSX 特权

NSX 特权控制与 NSX 管理相关的任务。

表 16-32. NSX 特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
读取 NSX 配置	允许读取 NSX 对象。	NSX	Nsx.Read
管理 NSX 配置	允许从 vSphere 管理员的角度管理 NSX 对象。	NSX	Nsx.Manage
修改 NSX 配置	允许从企业管理员的角度管理 NSX 对象。	NSX	Nsx.ModifyAll

## VMware 可观察性特权

VMware 可观察性特权控制代理访问 vCenter Server 上可观察性 API 的能力。

这些特权仅适用于 VMware 内部 API。

## OvfManager 特权

OvfManager 特权控制访问 vService Manager 的能力。

这些特权仅适用于 VMware 内部 API。

## 与合作伙伴 Rest 守护进程交互特权

与合作伙伴 Rest 守护进程交互特权控制对读取和写入操作的访问。

表 16-33. 与合作伙伴 Rest 守护进程交互特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
从合作伙伴 Rest 守护进程执行 GET 操作	允许合作伙伴置备的 REST 客户端执行 GET 操作。	执行 GET 操作的合作伙伴用户。	PartnerRestDaemon.Read
对合作伙伴 Rest 守护进程执行修改操作	允许合作伙伴置备的 REST 客户端执行 POST、PUT 和 DELETE 操作。	执行 POST、PUT 或 DELETE 操作的合作伙伴用户。	PartnerRestDaemon.Write

## 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 16-34. 性能特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
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	Performance.ModifyIntervals

## 插件特权

插件特权控制 vSphere Client 插件的管理。

表 16-35. 插件特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
管理插件	允许管理 vSphere Client 插件。	vCenter Server	Plugin.Management

## 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 16-36. 权限特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
修改权限	<p>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。</p> <p>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。</p>	任何对象加父对象	Authorization.ModifyPermissions
修改特权	<p>允许修改特权的组或描述。</p> <p>没有与此特权关联的 vSphere Client 用户界面元素。</p>	任何对象	Authorization.ModifyPrivileges

表 16-36. 权限特权（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
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	Authorization.ModifyRoles
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	Authorization.ReassignRolePermissions

## 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 16-37. 资源特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
应用建议	允许接受服务器提供的建议以通过 vMotion 执行迁移。	集群	Resource.ApplyRecommendation
将 vApp 分配给资源池	允许将 vApp 分配到资源池。	资源池	Resource.AssignVAppToPool
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	Resource.AssignVMToPool
创建资源池	允许创建资源池。	资源池、集群	Resource.CreatePool
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	Resource.ColdMigrate
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。		Resource.HotMigrate
修改资源池	允许更改资源池的分配。	资源池	Resource.EditPool
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	Resource.MovePool
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	Resource.QueryVMotion
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	Resource.DeletePool
重命名资源池	允许重命名资源池。	资源池	Resource.RenamePool

## 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 16-38. 已调度任务特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
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	ScheduledTask.Create
修改任务	允许重新配置已调度任务的属性。	任何对象	ScheduledTask.Edit
移除任务	允许移除队列中的已调度任务。	任何对象	ScheduledTask.Delete
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	ScheduledTask.Run

## 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 16-39. 会话特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
模拟用户	允许模拟其他用户。该功能由扩展使用。	根 vCenter Server	Sessions.ImpersonateUser
消息	允许设置全局登录消息。	根 vCenter Server	Sessions.GlobalMessage
验证会话	允许验证会话有效性。	根 vCenter Server	Sessions.ValidateSession
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	Sessions.TerminateSession
privilege.StorageProfile.ViewPermissions.label	允许收集会话。	根 vCenter Server	Sessions.CollectPrivilegeChecks



## 虚拟机存储策略特权

虚拟机存储策略特权控制为虚拟机创建和管理存储策略的能力。

表 16-40. 虚拟机存储策略特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
应用虚拟机存储策略	允许使用虚拟机存储策略。	根 vCenter Server	StorageProfile.Apply
更新虚拟机存储策略	允许创建和更新虚拟机存储配置文件。	根 vCenter Server	StorageProfile.Update
虚拟机存储策略编辑权限	允许编辑分配的虚拟机存储策略。	根 vCenter Server	StorageProfile.EditPermissions
虚拟机存储策略查看权限	允许查看虚拟机存储策略的可用权限。	根 vCenter Server	StorageProfile.ViewPermissions
查看虚拟机存储策略	允许查看定义的虚拟机存储策略。	根 vCenter Server	StorageProfile.View

## 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 16-41. 存储视图特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
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 <a href="#">存储视图.查看</a> 。	根 vCenter Server	StorageViews.ConfigureService
查看	允许特权用户使用只读存储监控服务 API。	根 vCenter Server	StorageViews.View

## 主管服务特权

主管服务特权控制哪些用户可以在 vSphere with Tanzu 环境中创建和管理主管服务。

表 16-42. 主管服务特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
管理主管服务	允许创建、更新或删除主管服务。还允许在集群上安装主管服务，以及创建或删除主管服务版本。	集群	SupervisorServices.Manage

## 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 16-43. 任务特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
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 Client 用户界面元素。	根 vCenter Server	Task.Create
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 Client 用户界面元素。	根 vCenter Server	Task.Update

## 租户管理特权

租户管理特权控制定义和检索租户管理实体的各个方面。（适用于 VMware Cloud on AWS。）

表 16-44. 租户管理特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
租户置备操作	允许定义一组用于租户管理的资源。	根文件夹和当前标记为服务提供程序的每个实体。	TenantManager.Update
租户查询操作	允许检索租户管理资源列表。	根文件夹和当前标记为服务提供程序的每个实体。	TenantManager.Query

## Transfer Service 特权

Transfer Service 特权是 VMware 的内部特权。请勿使用这些特权。

## VcTrusts/VcIdentity 特权

VcTrusts/VcIdentity 特权控制对与在 vCenter Server 系统之间设置信任关系相关的各种内部 API 和功能的访问。

表 16-45. VcTrusts/VcIdentity 特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
创建/更新/删除 (管理员特权)	允许对在 vCenter Server 系统之间设置信任关系相关的各种内部 API 和功能进行完全管理级访问。	不适用	Trust.Administer
创建/更新/删除 (低于管理员特权)	允许对在 vCenter Server 系统之间设置信任关系相关的各种内部 API 和功能进行精简管理访问。此特权限制创建/更新/删除 VcTrusts/VcIdentity，这样用户便无法升级非管理员特权。	不适用	Trust.Manage

## 可信基础架构管理员特权

可信基础架构管理员特权配置和管理 vSphere Trust Authority 部署。

这些特权确定哪些用户可以为 vSphere Trust Authority 部署执行配置和管理任务。有关 Trust Authority 角色和 TrustedAdmins 组的详细信息，请参见 [vSphere Trust Authority 的必备条件和所需特权](#)。

表 16-46. 可信基础架构管理员特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
配置密钥服务器信任	允许管理密钥提供程序服务的密钥提供程序。	根 vCenter Server	TrustedAdmin.ManageKMSTrust
配置 Trust Authority 主机 TPM 证书	允许创建和修改证明服务设置。	根 vCenter Server	TrustedAdmin.ConfigureHostCertificates
配置 Trust Authority 主机元数据	允许编辑要由证明服务证明的基础映像。	根 vCenter Server	TrustedAdmin.ConfigureHostMetadata
配置证明 SSO	允许编辑可受 Trust Authority 主机信任的主机。	根 vCenter Server	TrustedAdmin.ManageAttestingSSO
配置令牌转换策略	允许配置令牌转换策略。	根 vCenter Server	TrustedAdmin.ConfigureTokenConversionPolicy
列出可信基础架构主机	允许读取有关受信任主机和 Trust Authority 主机的信息。	根 vCenter Server	TrustedAdmin.ReadTrustedHosts
列出有关 STS 的信息	允许导出受信任主机的详细信息，以便可以将其导入到 Trust Authority 集群中。	根 vCenter Server	TrustedAdmin.ReadStsInfo
管理可信基础架构主机	允许编辑有关受信任主机和 Trust Authority 主机的信息。	根 vCenter Server	TrustedAdmin.ManageTrustedHosts
读取密钥服务器信任	允许读取密钥提供程序服务的密钥提供程序。	根 vCenter Server	TrustedAdmin.ReadKMSTrust
读取证明 SSO	允许读取可受 Trust Authority 主机信任的主机。	根 vCenter Server	TrustedAdmin.ReadAttestingSSO
检索 TPM Trust Authority 主机证书	允许读取证明服务的设置。	根 vCenter Server	TrustedAdmin.RetrieveTPMHostCertificates
检索 Trust Authority 主机元数据	允许读取可由证明服务证明的基础映像。	根 vCenter Server	TrustedAdmin.RetrieveHostMetadata

## 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 16-47. vApp 特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
添加虚拟机	允许将虚拟机添加到 vApp。	vApp	VApp.AssignVM
分配资源池	允许将资源池分配到 vApp。	vApp	VApp.AssignResourcePool
分配 vApp	允许将一个 vApp 分配给另一个 vApp	vApp	VApp.AssignVApp
克隆	允许克隆 vApp。	vApp	VApp.Clone
创建	允许创建 vApp。	vApp	VApp.Create
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.Delete
导出	允许从 vSphere 导出 vApp。	vApp	VApp.Export
导入	允许将 vApp 导入 vSphere。	vApp	VApp.Import
移动	允许将 vApp 移动到新清单位置。	vApp	VApp.Move
关闭电源	允许对 vApp 执行关闭电源操作。	vApp	VApp.PowerOff
打开电源	允许对 vApp 执行打开电源操作。	vApp	VApp.PowerOn
从 URL 拉取	允许列出远程源文件描述符。	vApp	VApp.PullFromUrls
重命名	允许重命名 vApp。	vApp	VApp.Rename
挂起	允许暂停 vApp。	vApp	VApp.Suspend
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.Unregister
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.ExtractOvfEnvironment
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.ApplicationConfig
vApp 实例配置	允许修改 vApp 的实例配置，例如策略。	vApp	VApp.InstanceConfig

表 16-47. vApp 特权（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<b>vApp 托管主体配置</b>	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 Client 用户界面元素。	vApp	VApp.ManagedByConfig
<b>vApp 资源配置</b>	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	VApp.ResourceConfig

## VcIdentityProviders 特权

VcIdentityProviders 特权控制对 VcIdentityProviders API 的访问。

表 16-48. VcIdentityProviders 特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<b>创建</b>	允许对 VcIdentityProviders API（vCenter Server 身份提供程序）进行只创建访问。	不适用	VcIdentityProviders.Create
<b>管理</b>	允许对 VcIdentityProviders API（vCenter Server 身份提供程序）进行管理级别的写入访问（创建、读取、更新、删除）。	不适用	VcIdentityProviders.Manage
<b>读取</b>	允许对 VcIdentityProviders API（vCenter Server 身份提供程序）进行读取访问。	不适用	VcIdentityProviders.Read

## VMware vSphere Lifecycle Manager 配置特权

VMware vSphere Lifecycle Manager 配置特权控制配置 vSphere Lifecycle Manager 服务的能力。

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。

**注** 仅向管理员或受信任的用户分配允许用户调用 VMware vSphere Lifecycle Manager API（接受 URL）的特权。

表 16-49. VMware vSphere Lifecycle Manager 配置特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>配置           <ul style="list-style-type: none"> <li>配置服务</li> </ul> </li> </ul>	允许配置 vSphere Lifecycle Manager 服务和已调度修补程序下载任务。	根 vCenter Server	VcIntegrity.General.com.vmware.vcIntegrity.Configure

## VMware vSphere Lifecycle Manager ESXi 运行状况视图特权

VMware vSphere Lifecycle Manager ESXi 运行状况视图特权控制检查 ESXi 主机和集群运行状况的能力。

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 16-50. VMware vSphere Lifecycle Manager ESXi 运行状况视图特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>ESXi 运行状况视图           <ul style="list-style-type: none"> <li>读取</li> <li>写入</li> </ul> </li> </ul>	<b>读取</b> 允许查询 ESXi 主机和集群的运行状况。当前未使用。 <b>写入。</b>	主机 集群	VcIntegrity.lifecycleHealth.Read VcIntegrity.lifecycleHealth.Write

## VMware vSphere Lifecycle Manager 常规特权

VMware vSphere Lifecycle Manager 常规特权控制读取和写入 Lifecycle Manager 资源的能力。

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 16-51. VMware vSphere Lifecycle Manager 常规特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>Lifecycle Manager: 常规特权           <ul style="list-style-type: none"> <li>读取</li> <li>写入</li> </ul> </li> </ul>	<b>读取</b> 允许读取 vSphere Lifecycle Manager 资源。需要此特权才能获取任务信息。 <b>写入</b> 允许写入 vSphere Lifecycle Manager 资源。需要此特权才能取消 vSphere Lifecycle Manager 任务。	根 vCenter Server	VcIntegrity.lifecycleGeneral.Read VcIntegrity.lifecycleGeneral.Write

## VMware vSphere Lifecycle Manager 硬件兼容性特权

VMware vSphere Lifecycle Manager 硬件兼容性特权控制发现和解决潜在硬件兼容性问题的能力。

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 16-52. VMware vSphere Lifecycle Manager 硬件兼容性特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>■ Lifecycle Manager: 硬件兼容性特权           <ul style="list-style-type: none"> <li>■ 访问硬件兼容性</li> <li>■ 写入</li> </ul> </li> </ul>	访问硬件兼容性和写入允许访问硬件兼容性数据并解决潜在的硬件兼容性问题。	主机	VcIntegrity.HardwareCompatibility.Read VcIntegrity.HardwareCompatibility.Write

## VMware vSphere Lifecycle Manager 映像特权

VMware vSphere Lifecycle Manager 映像特权控制管理映像的能力。

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。

**注** 仅向管理员或受信任的用户分配允许用户调用 VMware vSphere Lifecycle Manager API（接受 URL）的特权。



表 16-53. VMware vSphere Lifecycle Manager 映像特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>■ Lifecycle Manager: 映像特权 <ul style="list-style-type: none"> <li>■ 读取</li> <li>■ 写入</li> </ul> </li> </ul>	<p><b>读取</b>允许读取 vSphere Lifecycle Manager 映像。需要此特权才能执行以下操作：</p> <ul style="list-style-type: none"> <li>■ 列出集群的所有草稿</li> <li>■ 获取有关草稿的更多信息</li> <li>■ 对草稿执行扫描</li> <li>■ 验证草稿</li> <li>■ 检索草稿内容</li> <li>■ 计算有效的组件列表</li> <li>■ 获取当前所需状态文档的内容</li> <li>■ 在集群上启动扫描</li> <li>■ 获取合规性结果</li> <li>■ 获取建议</li> <li>■ 将当前所需状态导出为库、JSON 文件或 ISO</li> </ul> <p><b>写入</b>允许管理 vSphere Lifecycle Manager 映像。需要此特权才能执行以下操作：</p> <ul style="list-style-type: none"> <li>■ 创建、删除或提交草稿</li> <li>■ 导入所需状态</li> <li>■ 生成建议</li> <li>■ 设置或删除草稿的不同部分</li> </ul>	根 vCenter Server	VcIntegrity.lifecycleSettings.Read VcIntegrity.lifecycleSettings.Write

## VMware vSphere Lifecycle Manager 映像修复特权

VMware vSphere Lifecycle Manager 映像特权控制修复映像的能力。

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 16-54. VMware vSphere Lifecycle Manager 映像修复特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>■ Lifecycle Manager: 映像修复特权 <ul style="list-style-type: none"> <li>■ 读取</li> <li>■ 写入</li> </ul> </li> </ul>	<p><b>读取</b>允许执行修复预检查。<b>写入</b>允许执行修复。</p>	集群	VcIntegrity.lifecycleSoftwareRemediation.Read VcIntegrity.lifecycleSoftwareRemediation.Write

## VMware vSphere Lifecycle Manager 设置特权

VMware vSphere Lifecycle Manager 设置特权控制管理库和修复策略的能力。

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。

**注** 仅向管理员或受信任的用户分配允许用户调用 VMware vSphere Lifecycle Manager API（接受 URL）的特权。

表 16-55. VMware vSphere Lifecycle Manager 设置特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
■ Lifecycle Manager: 设置特权	读取允许读取 vSphere Lifecycle Manager 库和修复策略。写入允许写入 vSphere Lifecycle Manager 库和修复策略。	根 vCenter Server	VcIntegrity.lifecycleSoftwareSpecification.Read
■ 读取			VcIntegrity.lifecycleSoftwareSpecification.Read
■ 写入			VcIntegrity.lifecycleSoftwareSpecification.Write

## VMware vSphere Lifecycle Manager 管理基准特权

VMware vSphere Lifecycle Manager 管理基准特权控制管理基准和基准组的能力。

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 16-56. VMware vSphere Lifecycle Manager 管理基准特权

中的特权名称	描述	要求	API 中的特权名称
■ 管理基准	附加基准允许将基准和基准组附加到 vSphere 清单中的对象。	根 vCenter Server	VcIntegrity.Baseline.com.vmware.vcIntegrity.AssignBaselines
■ 附加基准			VcIntegrity.Baseline.com.vmware.vcIntegrity.ManageBaselines
■ 管理基准	管理基准允许创建、编辑或删除基准和基准组。		

## VMware vSphere Lifecycle Manager 管理修补程序和升级特权

VMware vSphere Lifecycle Manager 管理修补程序和升级特权控制查看、扫描和修复适用修补程序、扩展或升级的能力。

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 16-57. VMware vSphere Lifecycle Manager 管理修补程序和升级特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>■ 管理修补程序和升级           <ul style="list-style-type: none"> <li>■ 修复以应用修补程序、扩展和升级</li> <li>■ 扫描适用的修补程序、扩展和升级</li> <li>■ 转储修补程序和扩展</li> <li>■ 查看合规性状态</li> </ul> </li> </ul>	<p><b>修复以应用修补程序、扩展和升级</b> 允许在使用基准时修复虚拟机和主机以应用修补程序、扩展或升级。此外，此特权还允许查看合规性状态。</p> <p><b>扫描适用的修补程序、扩展和升级</b> 允许在使用基准时扫描虚拟机和主机以搜索适用的修补程序、扩展或升级。</p> <p><b>转储修补程序和扩展</b> 允许在使用基准时将修补程序或扩展转储到 ESXi 主机。此外，此特权还允许查看 ESXi 主机的合规性状态。</p> <p><b>查看合规性状态</b> 允许查看 vSphere 清单中对象的基准合规性信息。</p>	根 vCenter Server	<p>VcIntegrity.Updates.com.vmware.vcIntegrity.Remediate</p> <p>VcIntegrity.Updates.com.vmware.vcIntegrity.Scan</p> <p>VcIntegrity.Updates.com.vmware.vcIntegrity.Stage</p> <p>VcIntegrity.Updates.com.vmware.vcIntegrity.ViewStatus</p>

## VMware vSphere Lifecycle Manager 上传文件特权

VMware vSphere Lifecycle Manager 上传文件特权控制将更新导入 vSphere Lifecycle Manager 库的能力。

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。

**注** 仅向管理员或受信任的用户分配允许用户调用 VMware vSphere Lifecycle Manager API（接受 URL）的特权。

表 16-58. VMware vSphere Lifecycle Manager 上传文件特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>■ 上传文件           <ul style="list-style-type: none"> <li>■ 上传文件</li> </ul> </li> </ul>	允许上传升级 ISO 和脱机修补程序包。	根 vCenter Server	VcLifecycle.Upgrade

## 虚拟机更改配置特权

虚拟机更改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 16-59. 虚拟机更改配置特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>获取磁盘租约</li> </ul> </li> </ul>	允许磁盘为虚拟机租用操作。	虚拟机	VirtualMachine.Config.DiskLease
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>添加现有磁盘</li> </ul> </li> </ul>	允许将现有虚拟磁盘添加到虚拟机。	虚拟机	VirtualMachine.Config.AddExistingDisk
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>添加新磁盘</li> </ul> </li> </ul>	允许创建新虚拟磁盘以添加到虚拟机。	虚拟机	VirtualMachine.Config.AddNewDisk
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>添加或移除设备</li> </ul> </li> </ul>	允许添加或移除任何非磁盘设备。	虚拟机	VirtualMachine.Config.AddRemoveDevice
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>高级配置</li> </ul> </li> </ul>	允许在虚拟机的配置文件中添加或修改高级参数。	虚拟机	VirtualMachine.Config.AdvancedConfig
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>更改 CPU 数目</li> </ul> </li> </ul>	允许更改虚拟 CPU 的数目。	虚拟机	VirtualMachine.Config.CPUCount
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>更改内存</li> </ul> </li> </ul>	允许更改分配给虚拟机的内存量。	虚拟机	VirtualMachine.Config.Memory
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>更改设置</li> </ul> </li> </ul>	允许更改常规虚拟机设置。	虚拟机	VirtualMachine.Config.Settings
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>更改交换文件位置</li> </ul> </li> </ul>	允许更改虚拟机的交换文件放置策略。	虚拟机	VirtualMachine.Config.SwapPlacement
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>更改资源</li> </ul> </li> </ul>	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	VirtualMachine.Config.Resource
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>配置主机 USB 设备</li> </ul> </li> </ul>	允许将基于主机的 USB 设备连接到虚拟机。	虚拟机	VirtualMachine.Config.HostUSBDevice
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>配置裸设备</li> </ul> </li> </ul>	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	VirtualMachine.Config.RawDevice
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>配置托管主体</li> </ul> </li> </ul>	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	VirtualMachine.Config.ManagedBy
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>显示连接设置</li> </ul> </li> </ul>	允许配置虚拟机远程控制台选项。	虚拟机	VirtualMachine.Config.MksControl
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>扩展虚拟磁盘</li> </ul> </li> </ul>	允许扩展虚拟磁盘的大小。	虚拟机	VirtualMachine.Config.DiskExtend

表 16-59. 虚拟机更改配置特权（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>修改设备设置</li> </ul> </li> </ul>	允许更改现有设备的属性。	虚拟机	VirtualMachine.Config.EditDevice
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>查询 Fault Tolerance 兼容性</li> </ul> </li> </ul>	允许检查虚拟机的兼容性是否符合 Fault Tolerance 的要求。	虚拟机	VirtualMachine.Config.QueryFTCompatibility
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>查询无主文件</li> </ul> </li> </ul>	允许查询无所有者的文件。	虚拟机	VirtualMachine.Config.QueryUnownedFiles
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>从路径重新加载</li> </ul> </li> </ul>	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	VirtualMachine.Config.ReloadFromPath
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>移除磁盘</li> </ul> </li> </ul>	允许移除虚拟磁盘设备。	虚拟机	VirtualMachine.Config.RemoveDisk
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>重命名</li> </ul> </li> </ul>	允许重命名虚拟机或修改虚拟机的相关注释。	虚拟机	VirtualMachine.Config.Rename
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>重置客户机信息</li> </ul> </li> </ul>	允许编辑虚拟机的客户机操作系统信息。	虚拟机	VirtualMachine.Config.ResetGuestInfo
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>设置注释</li> </ul> </li> </ul>	允许添加或编辑虚拟机注释。	虚拟机	VirtualMachine.Config.Annotation
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>切换磁盘更改跟踪</li> </ul> </li> </ul>	允许激活或停用虚拟机的磁盘更改跟踪。	虚拟机	VirtualMachine.Config.ChangeTracking
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>切换派生父项</li> </ul> </li> </ul>	允许激活或停用 vmfork 父项。	虚拟机	VirtualMachine.Config.ToggleForkParent
<ul style="list-style-type: none"> <li>更改配置 <ul style="list-style-type: none"> <li>升级虚拟机兼容性</li> </ul> </li> </ul>	允许升级虚拟机的虚拟机兼容性版本。	虚拟机	VirtualMachine.Config.UpgradeVirtualHardware

## 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 与虚拟机客户机操作系统中的文件和应用程序进行交互的能力。

有关这些操作的详细信息，请参见《vSphere Web Services 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 16-60. 虚拟机客户机操作

vSphere Client 中的特权名称	描述	生效对象	API 中的特权名称
<ul style="list-style-type: none"> <li>客户机操作               <ul style="list-style-type: none"> <li>客户机操作别名修改</li> </ul> </li> </ul>	允许对虚拟机别名进行修改的虚拟机客户机操作。	虚拟机	VirtualMachine.GuestOperations.ModifyAliases
<ul style="list-style-type: none"> <li>客户机操作               <ul style="list-style-type: none"> <li>客户机操作别名查询</li> </ul> </li> </ul>	允许对虚拟机别名进行查询的虚拟机客户机操作。	虚拟机	VirtualMachine.GuestOperations.QueryAliases
<ul style="list-style-type: none"> <li>客户机操作               <ul style="list-style-type: none"> <li>客户机操作修改</li> </ul> </li> </ul>	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 Client 用户界面元素。	虚拟机	VirtualMachine.GuestOperations.Modify
<ul style="list-style-type: none"> <li>客户机操作               <ul style="list-style-type: none"> <li>客户机操作程序执行</li> </ul> </li> </ul>	允许涉及在虚拟机中运行应用程序的虚拟机客户机操作。 没有与此特权关联的 vSphere Client 用户界面元素。	虚拟机	VirtualMachine.GuestOperations.Execute
<ul style="list-style-type: none"> <li>客户机操作               <ul style="list-style-type: none"> <li>客户机操作查询</li> </ul> </li> </ul>	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 Client 用户界面元素。	虚拟机	VirtualMachine.GuestOperations.Query

## 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 16-61. 虚拟机交互

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>交互               <ul style="list-style-type: none"> <li>回答问题</li> </ul> </li> </ul>	允许解决虚拟机状态转换的问题或运行时错误。	虚拟机	VirtualMachine.Interact.AnswerQuestion
<ul style="list-style-type: none"> <li>交互               <ul style="list-style-type: none"> <li>虚拟机上的备份操作</li> </ul> </li> </ul>	允许对虚拟机执行备份操作。	虚拟机	VirtualMachine.Interact.Backup

表 16-61. 虚拟机交互（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
■ 交互 ■ 配置 CD 介质	允许配置虚拟 DVD 或 CD-ROM 设备。	虚拟机	VirtualMachine.Interact.SetCDMedia
■ 交互 ■ 配置软盘介质	允许配置虚拟软盘设备。	虚拟机	VirtualMachine.Interact.SetFloppyMedia
■ 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	VirtualMachine.Interact.ConsoleInteract
■ 交互 ■ 创建屏幕截图	允许创建虚拟机屏幕截图。	虚拟机	VirtualMachine.Interact.CreateScreenshot
■ 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	VirtualMachine.Interact.DefragmentAllDisks
■ 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	VirtualMachine.Interact.DeviceConnection
■ 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	VirtualMachine.Interact.DnD
■ 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	VirtualMachine.Interact.GuestControl
■ 交互 ■ 插入 USB HID 扫描代码	允许插入 USB HID 扫描代码。	虚拟机	VirtualMachine.Interact.PutUsbScanCodes
■ 交互 ■ 暂停或取消暂停	允许暂停或取消暂停虚拟机。	虚拟机	VirtualMachine.Interact.Pause
■ 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	VirtualMachine.Interact.SESparseMaintenance
■ 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	VirtualMachine.Interact.PowerOff
■ 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	VirtualMachine.Interact.PowerOn
■ 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	VirtualMachine.Interact.Record
■ 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	VirtualMachine.Interact.Replay

表 16-61. 虚拟机交互（续）

vSphere Client 中的 特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>■ 交互</li> <li>■ 重置</li> </ul>	允许重置虚拟机并重新引导客户机操作系统。	虚拟机	VirtualMachine.Interact.Reset
<ul style="list-style-type: none"> <li>■ 交互</li> <li>■ 恢复 Fault Tolerance</li> </ul>	允许恢复虚拟机的 Fault Tolerance 功能。	虚拟机	VirtualMachine.Interact.EnableSecondary
<ul style="list-style-type: none"> <li>■ 交互</li> <li>■ 挂起</li> </ul>	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	VirtualMachine.Interact.Suspend
<ul style="list-style-type: none"> <li>■ 交互</li> <li>■ 挂起 Fault Tolerance</li> </ul>	允许暂停虚拟机的 Fault Tolerance 功能。	虚拟机	VirtualMachine.Interact.DisableSecondary
<ul style="list-style-type: none"> <li>■ 交互</li> <li>■ 挂起到内存</li> </ul>	允许暂停虚拟机的内存。	虚拟机	VirtualMachine.Interact.SuspendToMemory
<ul style="list-style-type: none"> <li>■ 交互</li> <li>■ 测试故障切换</li> </ul>	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	VirtualMachine.Interact.MakePrimary
<ul style="list-style-type: none"> <li>■ 交互</li> <li>■ 测试重新启动辅助虚拟机</li> </ul>	允许使用 Fault Tolerance 终止虚拟机的辅助虚拟机。	虚拟机	VirtualMachine.Interact.DisableSecondary
<ul style="list-style-type: none"> <li>■ 交互</li> <li>■ 关闭 Fault Tolerance</li> </ul>	允许关闭虚拟机的 Fault Tolerance 功能。	虚拟机	VirtualMachine.Interact.TurnOffFaultTolerance
<ul style="list-style-type: none"> <li>■ 交互</li> <li>■ 打开 Fault Tolerance</li> </ul>	允许打开虚拟机的 Fault Tolerance 功能。	虚拟机	VirtualMachine.Interact.CreateSecondary
<ul style="list-style-type: none"> <li>■ 交互</li> <li>■ VMware Tools 安装</li> </ul>	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	VirtualMachine.Interact.ToolsInstall

## 虚拟机编辑清单特权

虚拟机编辑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 16-62. 虚拟机编辑清单特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>■ 编辑清单 <ul style="list-style-type: none"> <li>■ 从现有清单创建</li> </ul> </li> </ul>	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。	集群、主机、虚拟机文件夹	VirtualMachine.Inventory.CreateFromExisting
<ul style="list-style-type: none"> <li>■ 编辑清单 <ul style="list-style-type: none"> <li>■ 新建</li> </ul> </li> </ul>	允许创建虚拟机并为其执行分配资源。	集群、主机、虚拟机文件夹	VirtualMachine.Inventory.Create
<ul style="list-style-type: none"> <li>■ 编辑清单 <ul style="list-style-type: none"> <li>■ 移动</li> </ul> </li> </ul>	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	VirtualMachine.Inventory.Move
<ul style="list-style-type: none"> <li>■ 编辑清单 <ul style="list-style-type: none"> <li>■ 注册</li> </ul> </li> </ul>	允许将现有虚拟机添加到 vCenter Server 或主机清单。	集群、主机、虚拟机文件夹	VirtualMachine.Inventory.Register
<ul style="list-style-type: none"> <li>■ 编辑清单 <ul style="list-style-type: none"> <li>■ 移除</li> </ul> </li> </ul>	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	VirtualMachine.Inventory.Delete
<ul style="list-style-type: none"> <li>■ 编辑清单 <ul style="list-style-type: none"> <li>■ 取消注册</li> </ul> </li> </ul>	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	VirtualMachine.Inventory.Unregister

## 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 16-63. 虚拟机置备特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 允许访问磁盘</li> </ul> </li> </ul>	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	VirtualMachine.Provisioning.DiskRandomAccess
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 允许访问文件</li> </ul> </li> </ul>	允许对与虚拟机关联的文件执行操作，包括 vmx、磁盘文件、日志和 nvram。	虚拟机	VirtualMachine.Provisioning.FileRandomAccess
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 允许对磁盘进行只读访问</li> </ul> </li> </ul>	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	VirtualMachine.Provisioning.DiskRandomRead
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 允许下载虚拟机</li> </ul> </li> </ul>	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	VirtualMachine.Provisioning.GetVmFiles
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 允许上传虚拟机文件</li> </ul> </li> </ul>	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	VirtualMachine.Provisioning.PutVmFiles
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 克隆模板</li> </ul> </li> </ul>	允许克隆模板。	模板	VirtualMachine.Provisioning.CloneTemplate
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 克隆虚拟机</li> </ul> </li> </ul>	允许克隆现有虚拟机和资源分配。	虚拟机	VirtualMachine.Provisioning.Clone
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 从虚拟机创建模板</li> </ul> </li> </ul>	允许从虚拟机创建新模板。	虚拟机	VirtualMachine.Provisioning.CreateTemplateFromVM
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 自定义客户机</li> </ul> </li> </ul>	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	VirtualMachine.Provisioning.Customize
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 部署模板</li> </ul> </li> </ul>	允许从模板部署虚拟机。	模板	VirtualMachine.Provisioning.DeployTemplate
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 标记为模板</li> </ul> </li> </ul>	允许将现有已关闭电源的虚拟机标记为模板。	虚拟机	VirtualMachine.Provisioning.MarkAsTemplate
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 标记为虚拟机</li> </ul> </li> </ul>	允许将现有模板标记为虚拟机。	模板	VirtualMachine.Provisioning.MarkAsVM
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 修改自定义规范</li> </ul> </li> </ul>	允许创建、修改或删除自定义规范。	根 vCenter Server	VirtualMachine.Provisioning.ModifyCustSpecs

表 16-63. 虚拟机置备特权（续）

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 升级磁盘</li> </ul> </li> </ul>	允许升级虚拟机的磁盘。	虚拟机	VirtualMachine.Provisioning.PromoteDisks
<ul style="list-style-type: none"> <li>■ 置备 <ul style="list-style-type: none"> <li>■ 读取自定义规范</li> </ul> </li> </ul>	允许读取自定义规范。	虚拟机	VirtualMachine.Provisioning.ReadCustSpecs

## 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对服务配置执行监控和管理任务。

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。

表 16-64. 虚拟机服务配置特权

vSphere Client 中的特权名称	描述	API 中的特权名称
<ul style="list-style-type: none"> <li>■ 服务配置 <ul style="list-style-type: none"> <li>■ 允许通知</li> </ul> </li> </ul>	允许生成和使用有关服务状态的通知。	VirtualMachine.Namespace.Event
<ul style="list-style-type: none"> <li>■ 服务配置 <ul style="list-style-type: none"> <li>■ 允许轮询全局事件通知</li> </ul> </li> </ul>	允许查询是否存在任何通知。	VirtualMachine.Namespace.EventNotify
<ul style="list-style-type: none"> <li>■ 服务配置 <ul style="list-style-type: none"> <li>■ 管理服务配置</li> </ul> </li> </ul>	允许创建、修改和删除虚拟机服务。	VirtualMachine.Namespace.Management
<ul style="list-style-type: none"> <li>■ 服务配置 <ul style="list-style-type: none"> <li>■ 修改服务配置</li> </ul> </li> </ul>	允许修改现有的虚拟机服务配置。	VirtualMachine.Namespace.ModifyContent
<ul style="list-style-type: none"> <li>■ 服务配置 <ul style="list-style-type: none"> <li>■ 查询服务配置</li> </ul> </li> </ul>	允许检索虚拟机服务的列表。	VirtualMachine.Namespace.Query
<ul style="list-style-type: none"> <li>■ 服务配置 <ul style="list-style-type: none"> <li>■ 读取服务配置</li> </ul> </li> </ul>	允许检索现有的虚拟机服务配置。	VirtualMachine.Namespace.ReadContent

## 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 16-65. 虚拟机快照管理特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>快照管理</li> <li>创建快照</li> </ul>	允许按照虚拟机的当前状况创建快照。	虚拟机	VirtualMachine.State.CreateSnapshot
<ul style="list-style-type: none"> <li>快照管理</li> <li>移除快照</li> </ul>	允许从快照历史记录移除快照。	虚拟机	VirtualMachine.State.RemoveSnapshot
<ul style="list-style-type: none"> <li>快照管理</li> <li>重命名快照</li> </ul>	允许使用新名称和/或新描述重命名快照。	虚拟机	VirtualMachine.State.RenameSnapshot
<ul style="list-style-type: none"> <li>快照管理</li> <li>恢复到快照</li> </ul>	允许将虚拟机设置为在给定快照中所处的状况。	虚拟机	VirtualMachine.State.RevertToSnapshot

## 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 16-66. 虚拟机 vSphere Replication 特权

中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>vSphere Replication</li> <li>配置复制</li> </ul>	允许对虚拟机进行复制配置。	虚拟机	VirtualMachine.Hbr.ConfigureReplication
<ul style="list-style-type: none"> <li>vSphere Replication</li> <li>管理复制</li> </ul>	允许在复制时触发完全同步、联机同步或脱机同步。	虚拟机	VirtualMachine.Hbr.ReplicaManagement
<ul style="list-style-type: none"> <li>vSphere Replication</li> <li>监控复制</li> </ul>	允许监控复制。	虚拟机	VirtualMachine.Hbr.MonitorReplication

## 虚拟机类特权

虚拟机类特权控制哪些用户可以在 Kubernetes 命名空间上添加和移除虚拟机类。

表 16-67. 虚拟机类特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
管理虚拟机类	允许管理主管集群中 Kubernetes 命名空间上的虚拟机类。	集群	VirtualMachineClasses.Manage

## vSAN 特权

vSAN 特权控制哪些用户可以执行浅层重新加密操作。

表 16-68. vSAN 特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
<ul style="list-style-type: none"> <li>■ 集群</li> <li>■ ShallowRekey</li> </ul>	允许对集群执行浅层重新加密。	集群	Vsan.Cluster.ShallowRekey

## vSphere 区域特权

vSphere 区域特权控制哪些用户可以在 vSphere with Tanzu 上创建和管理 vSphere 区域。

表 16-69. vSphere 区域特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
附加和分离 vSphere 区域的 vSphere 对象	允许将对象与 vSphere 区域相关联。	集群	Zone.ObjectAttachable
创建、更新和删除 vSphere 区域及其关联	允许创建和删除 vSphere 区域。	集群	Zone.Manage

## vService 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 16-70. vService 特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
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.CreateDependency
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.DestroyDependency
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.ReconfigureDependency
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	vService.UpdateDependency

## vSphere 标记特权

vSphere 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 vCenter Server 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 16-71. vSphere 标记特权

vSphere Client 中的特权名称	描述	要求	API 中的特权名称
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	InventoryService.Tagging.AttachTag
在对象上分配或取消分配 vSphere 标记	允许对象分配或取消分配标记。使用此特权限制用户可以分配或取消分配标记的对象。	任何对象	InventoryService.Tagging.ObjectAttachable
创建 vSphere 标记	允许创建标记。	任何对象	InventoryService.Tagging.CreateTag
创建 vSphere 标记类别	允许创建标记类别。	任何对象	InventoryService.Tagging.CreateCategory
删除 vSphere 标记	允许删除标记。	任何对象	InventoryService.Tagging.DeleteTag
删除 vSphere 标记类别	允许删除标记类别。	任何对象	InventoryService.Tagging.DeleteCategory
编辑 vSphere 标记	允许编辑标记。	任何对象	InventoryService.Tagging.EditTag
编辑 vSphere 标记类别	允许编辑标记类别。	任何对象	InventoryService.Tagging.EditCategory
修改类别的 UsedBy 字段	允许更改标记类别的 UsedBy 字段。	任何对象	InventoryService.Tagging.ModifyUsedByForCategory
修改标记的 UsedBy 字段	允许更改标记的 UsedBy 字段。	任何对象	InventoryService.Tagging.ModifyUsedByForTag

## vSphere Client 特权

vSphere Client 特权可控制对 vCenter Server 的脱机访问。

这些特权仅适用于 VMware Cloud。

# 了解 vSphere 强化与合规性

# 17

组织希望通过降低数据被盗、计算机攻击或未经授权的访问的风险来保持其数据的安全性。一般来讲，组织还必须遵守从政府标准到专用标准的一个或多个法规，如国家标准技术局 (NIST) 以及国防信息系统局安全技术实施指南 (DISA STIG)。确保您的 vSphere 环境符合这些标准需要了解各种注意事项，包括人员、流程和技术。

您可以关注安全与合规的高级别概述，这有助于规划安全策略。也可以从 VMware 网站的其他合规性相关资源中获取帮助。

本章讨论了以下主题：

- [vSphere 环境中的安全与合规性](#)
- [了解《vSphere 安全性配置指南》](#)
- [关于美国国家标准与技术研究院](#)
- [关于 DISA STIG](#)
- [关于 VMware 安全开发生命周期](#)
- [vSphere 中的审核日志记录](#)
- [了解安全与合规的后续步骤](#)
- [vCenter Server 和 FIPS](#)

## vSphere 环境中的安全与合规性

安全与合规这两个术语通常可以互换。但它们又是完全不同的概念。

安全性，通常被理解为信息安全，一般定义为用于实现保密性、完整性和可用性的一套技术、物理和管理控件。例如，通过锁定可登录的帐户及规定其登录方式（SSH、直接控制台等）保证主机的安全。相比之下，合规性是为满足不同监管框架建立的最小控件所需的一组要求，该框架对任何特定类型的技术、供应商或配置提供有限的指导。例如，支付卡行业 (PCI) 建立了安全准则，帮助组织主动地保护客户帐户数据。

安全性可减少数据被盗、计算机攻击或未经授权访问的风险，而合规性通常在定义的时间表内证明安全控件已就位。安全性主要在设计决策中概述，在技术配置中突显。合规性专注于映射安全控件和特定要求之间的关联。合规性映射提供了集中视图，以列出多个所需的安全控件。通过包括每个安全控件各自的合规性引文（按 NIST、PCI、FedRAMP、HIPAA 等域显示）进一步细化这些控件。

有效的网络安全和合规程序都使用三个支柱构建：人、流程和技术。一种普遍的误解是仅凭技术可以解决所有网络安全需求。技术在信息安全程序的开发和执行中发挥了巨大的重要作用。但是，如果技术脱离了过程和步骤、认知和培训，则会造成组织中的漏洞。

在定义安全和合规策略时，请记住以下信息：

- 用户需要常规认知和培训，而 IT 人员则需要专业培训。
- 流程定义了如何使用组织内的活动、角色和文档来降低风险。只有在人们正确遵循过程时，过程才能有效发挥作用。
- 可以使用技术防止或减少对您组织网络安全风险造成的影响。使用哪种技术取决于组织内的风险接受程度。

VMware 提供的合规性工具包同时包含《审核指南》和《产品适用性指南》，有助于消除合规性与法规要求与实施指南之间的差距。有关详细信息，请参见 <https://core.vmware.com/compliance>。

## 合规性术语表

合规性引入了一些必须了解的特定术语和定义。

表 17-1. 合规性术语

术语	定义
CJIS	刑事司法信息服务。在合规性环境中，CJIS 制定安全策略，规范当地、州和联邦刑事司法和法律实施机构必须采取安全措施来保护敏感信息，例如指纹和犯罪背景。
DISA STIG	美国国防信息系统局安全技术实施指南。美国国防信息系统局 (Defense Information Systems Agency, DISA) 是负责维护美国国防部 (DoD) IT 基础架构安全的实体。DISA 通过制定和使用《安全技术实施指南》（即 STIG）来完成这一任务。
FedRAMP	联邦风险和授权管理计划。FedRAMP 是为云产品和服务提供安全评估、授权和持续监控的标准化方法的政府级计划。
HIPAA	健康保险携带和责任法案。由国会在 1996 年通过，HIPAA 具有以下作用： <ul style="list-style-type: none"> <li>■ 使数百万个美国员工及其家庭能够在其工作变动或失业时转移和继续享受健康保险</li> <li>■ 减少了医疗保险欺诈和滥用</li> <li>■ 强制执行电子计费和其他过程有关医疗保险信息的行业标准</li> <li>■ 需要对受保护的健康信息进行保护和保密处理</li> </ul> 后者对于 vSphere 安全性文档最重要。
NCCoE	国家网络安全卓越中心。NCCoE 是一个美国政府组织，负责制定和公开共享美国公司遇到的网络安全问题的解决方案。该中心由来自网络安全技术公司、其他联邦机构和学术机构的人员组成，可以解决各种问题。
NIST	国家标准技术局。NIST 成立于 1901 年，是美国商业部的非监管联邦机构。NIST 的使命是通过推进测量科学、标准和技术，提高经济安全性并提升我们生活的质量，以支持美国的创新和行业竞争力。



表 17-1. 合规性术语（续）

术语	定义
PAG	产品适用性指南。本文档为正在考虑公司解决方案的组织提供一般准则，帮助他们解决合规性要求。
PCI DSS	支付卡行业数据安全标准。一组安全标准，旨在确保接受、处理、存储或传输信用卡信息的所有公司都能保有安全的环境。
VVD/VCF 合规性解决方案	VMware Validated Design/VMware Cloud Foundation。 VMware Validated Design 提供全面和广泛的测试蓝图来创建和运行软件定义的数据中心。VVD/VCF 合规性解决方案使客户能够满足适用于多个政府和行业法规的合规性要求。

## 了解《vSphere 安全性配置指南》

VMware 制定了《安全强化指南》，提供有关以安全方式部署和操作 VMware 产品的说明性指导。对于 vSphere，本指南称为《vSphere 安全性配置指南》（以前称为《强化指南》）。

《vSphere 安全性配置指南》（请访问 <https://core.vmware.com/security-configuration-guide>）包含 vSphere 的安全性最佳做法。《vSphere 安全性配置指南》并未直接映射到监管准则或框架，因此不是合规性指南。此外，《vSphere 安全性配置指南》不能用作安全性检查表。安全性始终有利也有弊。实施安全控制措施时，可能会对可用性、性能或其他操作任务产生负面影响。无论建议来自 VMware 还是其他行业来源，在进行安全性更改之前，都要仔细考虑您的工作负载、使用模式、组织结构等。如果您的组织需遵守法规要求，请参阅 [vSphere 环境中的安全与合规性](#) 或访问 <https://core.vmware.com/compliance>。该站点提供合规性工具包和产品审核指南，可帮助 vSphere 管理员和监管审核员根据监管框架保护和验证虚拟基础架构，如 NIST 800-53v4、NIST 800-171、PCI DSS、HIPAA、CJIS、ISO 27001 等。

《vSphere 安全性配置指南》不讨论保护以下各项：

- 虚拟机中运行的软件，例如客户机操作系统和应用程序
- 流经虚拟机网络的流量
- 加载项产品的安全性

《vSphere 安全性配置指南》不应被用作“合规性”工具。《vSphere 安全性配置指南》可以初步帮您实现合规性，但是如果单独使用，则无法确保您部署的合规性。有关合规性的详细信息，请参见 [vSphere 环境中的安全与合规性](#)。

## 阅读《vSphere 安全性配置指南》

《vSphere 安全性配置指南》是包含安全相关准则的电子表格，它可以帮助您修改 vSphere 安全配置。这些准则根据受影响的组件分组到选项卡中。

请勿盲目地将《vSphere 安全配置指南》中的准则应用到您的环境。请花时间评估每个设置，并针对是否应用做出明智的决定。至少，您可以使用评估列中的说明来验证您部署的安全性。

《vSphere 安全配置指南》可辅助您在部署中开始实现合规性。使用美国国防信息系统局 (DISA) 和其他合规性准则时，《vSphere 安全配置指南》能够让您根据各个准则将 vSphere 安全控制映射到合规性偏好。

## 关于美国国家标准与技术研究院

美国国家标准与技术研究院 (National Institute of Standards and Technology, NIST) 是美国非监管型政府机构，负责推进技术、衡量指标、标准和准则。符合 NIST 标准及准则已然成为许多行业的当务之急。

美国国家标准与技术研究院 (NIST) 成立于 1901 年，现隶属于美国商务部。NIST 是美国最早成立的物理科学实验室。目前，NIST 计量既支持最小的工艺，也支持最大、最复杂的人类创造，适用范围下至纳米级设备，上至能够抗震的摩天大楼和全球通信网络。

联邦信息安全管理法案 (Federal Information Security Management Act, FISMA) 是美国于 2002 年通过的联邦法律，联邦机构在制定、记录和实施信息安全与保护计划时必须遵守此法律。NIST 制定了重要的安全标准和准则（例如，FIPS 199、FIPS 200 和 SP 800 系列），在 FISMA 实施中具有重要作用。

政府组织和许多民间组织都使用 NIST 800-53 安全信息系统。网络安全和隐私控制至关重要，因为它能够保护组织运营（包括任务、职能、形象和信誉）、组织资产和个人免遭各种威胁的危害。这些威胁包括但不限于恶意网络攻击、自然灾害、结构性问题和人为错误。VMware 已雇用第三方审核合作伙伴，由他们根据 NIST 800-53 安全控制评估 VMware 的产品和解决方案。有关详细信息，请访问 NIST 网页，网址：<https://www.nist.gov/cyberframework>。

## 关于 DISA STIG

美国国防信息系统局 (DISA) 制定并发布了《安全技术实施指南》(STIG)。DISA STIG 为强化系统和降低威胁提供了技术指导。

美国国防信息系统局 (DISA) 是美国国防部 (DoD) 的直属作战支援局，负责维护 DOD 信息网络 (DODIN) 安全。为完成这一任务，DISA 制定、传播并强制实施《安全技术实施指南》(STIG)。简言之，STIG 是基于标准的可移植系统强化指南。STIG 是美国国防部 IT 系统必须实施的指南，可为非 DoD 实体提供经审查的安全基准作为衡量安全态势的依据。

VMware 等供应商根据 DISA 协议和反馈向 DISA 提交建议的安全强化指导以进行评估。此过程完成后，将在 DISA 组织网站上发布官方 STIG，网址为 <https://public.cyber.mil/stigs/>。VMware 在《vSphere 安全性配置指南》中提供了针对 vSphere 的安全基准和强化指导。请参见 <https://core.vmware.com/security>。

## 关于 VMware 安全开发生命周期

VMware 安全开发生命周期 (Security Development Lifecycle, SDL) 计划可在 VMware 软件产品开发阶段找出并降低安全风险。VMware 的 VMware 安全响应中心 (VMware Security Response Center, VSRC) 可对 VMware 产品中的软件安全问题进行分析和修复。

SDL 是一种软件开发方法，VMware 安全工程、通信和响应 (VMware Security Engineering, Communication, and Response, vSECR) 小组与 VMware 产品开发组用它来帮助确定和解决安全问题。有关 VMware 安全开发生命周期的更多信息，请参见 <https://www.vmware.com/security/sdl.html> 中的网页。

VSRC 用于客户和安全研究社区，能够实现解决安全问题和及时向客户提供可付诸实践的安全信息这两项目标。有关 VMware 安全响应中心的详细信息，请参见 <https://www.vmware.com/security/vsrc.html> 中的网页。

## vSphere 中的审核日志记录

对于任何 IT 环境，网络流量、合规性警示、防火墙活动、操作系统更改和置备活动的审核日志记录都被视为维护其安全性的最佳做法。此外，日志记录是许多法规和标准的特定要求。

为确保您知晓基础架构发生的更改，首先要执行的步骤之一是审核环境。默认情况下，vSphere 包含用于查看和跟踪更改的工具。例如，您可以对 vSphere 层次结构中的任何对象使用 vSphere Client 中的“任务和事件”选项卡来查看发生的更改。您还可以使用 PowerCLI 检索事件和任务。此外，vRealize Log Insight 还提供审核日志记录，以支持收集和保留重要系统事件。最后，还有许多提供 vCenter Server 审核的第三方工具可用。

日志文件可以提供审核记录，以帮助确定主机、虚拟机等的访问者。有关详细信息，请参见 [ESXi 日志文件地址](#)。

### 单点登录审核事件

Single Sign-On (SSO) 审核事件是访问 SSO 服务的用户或系统操作的记录。

vCenter Server 6.7 Update 2 及更高版本通过为以下操作添加事件来改进 VMware vCenter Single Sign-On 审核：

- 用户管理
- 登录
- 组创建
- 标识源
- 策略更新

支持的标识源为 vsphere.local、集成 Windows 身份验证 (IWA) 和基于 LDAP 的 Active Directory。

当用户通过 Single Sign-On 登录到 vCenter Server 时，或执行影响 SSO 的更改时，下面的审核事件写入到 SSO 审核日志文件：

- **登录和注销的尝试次数：**所有成功和失败登录和注销操作的事件。
- **特权更改：**更改用户角色或权限的事件。
- **帐户更改：**更改用户帐户信息的事件，例如用户名、密码或任何其他帐户信息。
- **安全性更改：**安全性配置、参数或策略更改的事件。
- **启用或禁用帐户：**激活或停用帐户的事件。
- **标识源：**添加、删除或编辑标识源的事件。

在 vSphere Client 中，事件数据显示在 [监控](#) 选项卡中。请参见《vSphere 监控和性能》文档。

SSO 审核事件数据包括以下详细信息：

- 事件发生时的时间戳。
- 执行该操作的用户。
- 事件的描述。
- 事件的严重性。
- 用于连接到 vCenter Server（如果可用）的客户端 IP 地址。

## SSO 审核事件日志概述

vSphere Single-Sign On 过程将审核事件写入到 `/var/log/audit/sso-events/` 目录中的 `audit_events.log` 文件。

---

**小心** 永远不要手动编辑 `audit_events.log` 文件，因为这样做可能会导致审核日志记录失败。

---

使用 `audit_events.log` 文件时，请牢记以下信息：

- 日志文件在达到 50 MB 时存档一次。
- 最多将保留 10 个存档文件。如果达到限制，创建新的存档时将清除最早的文件。
- 存档文件将命名为 `audit_events-<index>.log.gz`，其中索引是从 1 到 10 的数字。创建的第一个存档是索引 1，且每个后续存档的索引编号将依次加 1。
- 最早的事件位于存档索引 1 中。索引编号最大的文件是最近的存档。

## 了解安全与合规的后续步骤

进行安全评估是了解您的基础架构中的任何漏洞的第一步。安全评估是安全审核的一部分，用于查看系统和实践，其中包括安全合规性。

安全评估通常指扫描您组织的物理基础架构（防火墙、网络、硬件等）来识别漏洞与缺陷。安全评估与安全审核不同。安全审核不仅包括审查物理基础架构，还涉及策略和标准操作过程等其他领域，包括安全合规性。审核后，您可以决定解决系统中问题的步骤。

准备进行安全审核时，您可能会询问以下常规问题：

- 1 我们的组织必须要遵守合规性法规吗？如果是，必须遵守哪些法规？
- 2 我们多长时间进行一次审核？
- 3 我们内部自我评估的时间间隔是什么？
- 4 我们是否有权访问先前的审核结果，我们是否已查看它们？
- 5 我们是否使用第三方审核公司帮助我们准备审核？如果是，他们对虚拟化的熟悉程度是什么？
- 6 我们是否针对系统和应用程序运行安全漏洞扫描？运行的时间和频率是什么？
- 7 我们的内部网络安全策略是什么？
- 8 您是否根据需求进行了审核日志记录配置？请参见 [vSphere 中的审核日志记录](#)。

在入门时缺少具体指导或说明时，您可以使用快速入门服务，通过以下方式保护您的 vSphere 环境：

- 使用最新的软件和固件修补程序保持您的环境处于最新状态
- 为所有帐户维护良好的密码管理和安全机制
- 查看供应商批准的安全建议
- 参考 VMware 安全配置指南（请参见了解《[vSphere 安全性配置指南](#)》）
- 使用策略框架中随时可用且经验证的指南，例如 NIST 和 ISO 等
- 按照法规遵从性框架的指导进行操作，如 PCI、DISA 和 FedRAMP 等的

## vCenter Server 和 FIPS

在 vSphere 7.0 Update 2 及更高版本中，可以在 vCenter Server Appliance 上启用通过 FIPS 验证的加密。

FIPS 140-2 是一项美国和加拿大政府标准，指定了加密模块的安全要求。vSphere 使用通过 FIPS 验证的加密模块与 FIPS 140-2 标准指定的加密模块相匹配。FIPS vSphere 支持的目标是简化各种监管环境的合规性和安全性活动。

在 vSphere 6.7 及更高版本中，ESXi 和 vCenter Server 使用通过 FIPS 验证的加密保护管理接口和 VMware Certificate Authority (VMCA)。

vSphere 7.0 Update 2 及更高版本可将其他通过 FIPS 验证的加密添加到 vCenter Server Appliance 中。

**注** vSphere 的兼容性优于 FIPS，因此需要考虑有些组件的注意事项。请参见[使用 FIPS 时的注意事项](#)。

## FIPS 模块

加密模块是一组实现安全功能的硬件、软件或固件。ESXi 使用多个经过 FIPS 140-2 验证的加密模块。

下表显示了 ESXi 使用的经 FIPS 140-2 验证的加密模块集。

**表 17-2. FIPS 模块**

加密模块	安全策略版本	算法 (CAVP)	加密模块验证计划
Vmkernel 加密模块	1.0	AES、SHS、DRBG、HMAC (C 1182)	证书 #3073
Vmkernel 加密模块加载程序	不适用	HMAC、SHS (C 1181)	证书 #3073
Vmkernel DRBG 加密模块	不适用	AES、DRBG (C 499)	不适用
VMware OpenSSL FIPS 对象模块	2.0.20-vmw	DRBG、AES、SHS、HMAC、DSA、RSA、ECDSA、KAS-FFC、KAS-ECC (C 470)	证书 #3550 和 #3857

## 在 vCenter Server Appliance 上激活和停用 FIPS

您可以使用 HTTP 请求在 vCenter Server Appliance 上启用或停用通过 FIPS 验证的加密。FIPS 验证的加密默认情况下处于停用状态。

您可以通过多种方式执行 HTTP 请求。此任务说明了如何使用 vSphere Client 中的开发人员中心在 vCenter Server Appliance 上激活和停用 FIPS 验证的加密。有关通过 API 使用 vCenter Server Appliance 的详细信息，请参见《VMware vCenter Server 管理编程指南》。

### 步骤

- 1 使用 vSphere Client 登录到 vCenter Server 系统。
- 2 从菜单中，选择开发人员中心。
- 3 单击 **API 资源管理器**。
- 4 从**选择 API** 下拉菜单中，选择**设备**。
- 5 向下滚动浏览类别，展开 **system/security/global\_fips**。
- 6 展开 **GET**，并单击**尝试使用下的执行**。

您可以在**响应**下查看当前设置。

- 7 更改设置。

- a 要激活 FIPS，请展开 **PUT**，在 `request_body` 中输入以下内容，然后单击**执行**。

```
{
  "enabled":true
}
```

- b 要停用 FIPS，请展开 **PUT**，在 `request_body` 中输入以下内容，然后单击**执行**。

```
{
  "enabled":false
}
```

### 结果

激活或停用 FIPS 验证的加密后，将重新引导 vCenter Server Appliance。

## 使用 FIPS 时的注意事项

在 vCenter Server Appliance 上激活 FIPS 后，某些组件当前存在功能限制。

在 vCenter Server 上激活 FIPS 后，应该看不到任何差异，但需要考虑一些注意事项。

表 17-3. FIPS 注意事项

产品或组件	注意事项	解决办法
vSphere Single Sign-On	激活 FIPS 后，vCenter Server 仅支持用于联合身份验证的加密模块。因此，RSA SecureID 和某些 CAC 卡视图不再正常工作。	使用联合身份验证。有关详细信息，请参见《vSphere 身份验证》文档。
非 VMware 和合作伙伴 vSphere Client UI 插件	在启用 FIPS 后，这些插件可能不起作用。	升级插件以使用合规的加密库。请参见“准备本地插件以实现 FIPS 合规性”，网址为 <a href="https://code.vmware.com/docs/13385/preparing-local-plug-ins-for-fips-compliance">https://code.vmware.com/docs/13385/preparing-local-plug-ins-for-fips-compliance</a> 。