

vSphere 安全性

ESXi 6.5

vCenter Server 6.5

在本文档被更新的版本替代之前，本文档支持列出的每个产品的版本和所有后续版本。要查看本文档的更新版本，请访问 <http://www.vmware.com/cn/support/pubs>。

ZH_CN-002011-00

vmware®

最新的技术文档可以从 VMware 网站下载：

<http://www.vmware.com/cn/support/>

VMware 网站还提供最近的产品更新信息。

您如果对本文档有任何意见或建议，请把反馈信息提交至：

docfeedback@vmware.com

版权所有 © 2009 – 2016 VMware, Inc. 保留所有权利。 [版权和商标信息](#)。

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

北京办公室
北京市海淀区科学院南路 2 号
融科资讯中心 C 座南 8 层
www.vmware.com/cn

上海办公室
上海市浦东新区浦东南路 999 号
新梅联合广场 23 楼
www.vmware.com/cn

广州办公室
广州市天河北路 233 号
中信广场 7401 室
www.vmware.com/cn

目录

关于 vSphere 安全性 7

- 1 vSphere 环境中的安全性 9
 - 确保 ESXi 虚拟化管理程序安全 9
 - 确保 vCenter Server 系统及关联服务安全 11
 - 确保虚拟机安全 11
 - 确保虚拟网络连接层安全 12
 - vSphere 环境中的密码 13
 - 安全性最佳做法与资源 14

- 2 vSphere 权限和用户管理任务 15
 - 了解 vSphere 中的授权 16
 - 管理 vCenter 组件的权限 21
 - 全局权限 23
 - 使用角色分配特权 25
 - 角色和权限的最佳做法 28
 - 常见任务的所需特权 29

- 3 确保 ESXi 主机安全 31
 - 使用主机配置文件配置 ESXi 主机 31
 - 常规 ESXi 安全建议 32
 - ESXi 主机的证书管理 39
 - 使用安全配置文件自定义主机 52
 - 为 ESXi 主机分配特权 64
 - 使用 Active Directory 管理 ESXi 用户 66
 - 使用 vSphere Authentication Proxy 68
 - 配置 ESXi 的智能卡身份验证 74
 - 使用 ESXi Shell 75
 - ESXi 主机的 UEFI 安全引导 79
 - ESXi 日志文件 81

- 4 确保 vCenter Server 系统安全 83
 - vCenter Server 安全性最佳做法 83
 - 验证旧版 ESXi 主机的指纹 88
 - 验证“对网络文件复制的 SSL 证书验证”是否已启用 88
 - vCenter Server 和 Platform Services Controller 所需的端口 89
 - 其他 vCenter Server TCP 和 UDP 端口 92

- 5 确保虚拟机安全 95
 - 为虚拟机启用或禁用 UEFI 安全引导 95
 - 限制信息性消息从虚拟机流向 VMX 文件 96
 - 防止虚拟磁盘压缩 97
 - 虚拟机安全性最佳做法 97
- 6 虚拟机加密 105
 - vSphere 虚拟机加密 如何保护您的环境 105
 - vSphere 虚拟机加密 组件 107
 - 加密过程流 108
 - 虚拟磁盘加密 109
 - 加密任务的必备条件和必需特权 110
 - 加密 vSphere vMotion 111
 - 加密最佳做法、局限性和互操作性 111
- 7 在 vSphere 环境中使用加密 117
 - 设置密钥管理服务器群集 117
 - 创建加密存储策略 122
 - 以显式方式启用主机加密模式 122
 - 禁用主机加密模式 123
 - 创建加密虚拟机 123
 - 克隆加密虚拟机 124
 - 加密现有虚拟机或虚拟磁盘 124
 - 解密加密虚拟机或虚拟磁盘 125
 - 更改虚拟磁盘的加密策略 126
 - 解决缺少密钥问题 126
 - vSphere 虚拟机加密和核心转储 127
- 8 确保 vSphere 网络安全 131
 - vSphere 网络安全简介 131
 - 使用防火墙确保网络安全 132
 - 确保物理交换机安全 134
 - 使用安全策略确保标准交换机端口安全 135
 - 确保 vSphere 标准交换机的安全 135
 - 确保 vSphere Distributed Switch 和分布式端口组的安全 136
 - 通过 VLAN 确保虚拟机安全 137
 - 在单台 ESXi 主机中创建多个网络 139
 - Internet 协议安全 140
 - 确保 SNMP 配置正确 143
 - vSphere 网络连接安全性最佳做法 144
- 9 涉及多个 vSphere 组件的最佳做法 147
 - 同步 vSphere 网络连接上的时钟 147
 - 存储安全性最佳做法 150
 - 验证是否已禁止向客户机发送主机性能数据 152

为 ESXi Shell 和 vSphere Web Client 设置超时 152

10 定义的特权 153

- 警报特权 154
- Auto Deploy 和镜像配置文件特权 155
- 证书特权 155
- 内容库特权 155
- 加密操作特权 156
- 数据中心特权 157
- 数据存储特权 158
- 数据存储群集特权 159
- Distributed Switch 特权 159
- ESX Agent Manager 特权 159
- 扩展特权 160
- 文件夹特权 160
- 全局特权 160
- 主机 CIM 特权 161
- 主机配置特权 161
- 主机清单 162
- 主机本地操作特权 163
- 主机 vSphere Replication 特权 163
- 主机配置文件特权 163
- 网络特权 164
- 性能特权 164
- 权限特权 164
- 配置文件驱动的存储特权 165
- 资源特权 165
- 已调度任务特权 166
- 会话特权 166
- 存储视图特权 166
- 任务特权 167
- Transfer Service 特权 167
- 虚拟机配置特权 167
- 虚拟机客户机操作特权 168
- 虚拟机交互特权 169
- 虚拟机清单特权 173
- 虚拟机置备特权 173
- 虚拟机服务配置特权 174
- 虚拟机快照管理特权 174
- 虚拟机 vSphere Replication 特权 174
- dvPort 组特权 175
- vApp 特权 175
- vServices 特权 176
- vSphere 标记特权 176

索引 179

关于 vSphere 安全性

*vSphere 安全性*提供了有关确保 VMware® vCenter® Server 和 VMware ESXi 的 vSphere® 环境安全的信息。为了帮助保护 vSphere 环境，本文档介绍了可用的安全功能，以及可采取的保护该环境免受攻击的措施。

相关文档

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

目标读者

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

vSphere Web Client 和 vSphere Client（HTML 5 客户端）

本指南中的任务说明基于 vSphere Web Client。您也可以使用新的 vSphere Client 执行本指南中的大部分任务。新的 vSphere Client 用户界面术语、拓扑及工作流与 vSphere Web Client 用户界面的相同方面和元素保持高度一致。可以将 vSphere Web Client 说明应用到新的 vSphere Client，除非另有指示。

注意 在 vSphere 6.5 版本中，并未针对 vSphere Client 实现 vSphere Web Client 中的所有功能。有关不受支持的功能的最新列表，请参见《*vSphere Client 功能更新指南*》，网址为 <http://www.vmware.com/info?id=1413>。

vSphere 环境中的安全性

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，可以在 vCenter 对象上设置权限、打开防火墙端口或更改默认证书。可以针对 vCenter 对象层次结构中的不同对象采取安全措施，例如，vCenter Server 系统、ESXi 主机、虚拟机以及网络和存储对象。

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：

- 第 9 页，“确保 ESXi 虚拟化管理程序安全”
- 第 11 页，“确保 vCenter Server 系统及关联服务安全”
- 第 11 页，“确保虚拟机安全”
- 第 12 页，“确保虚拟网络连接层安全”
- 第 13 页，“vSphere 环境中的密码”
- 第 14 页，“安全性最佳做法与资源”

确保 ESXi 虚拟化管理程序安全

ESXi 虚拟化管理程序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。

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

限制 ESXi 访问

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

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

使用指定用户和最小特权

默认情况下，root 用户可以执行许多任务。您可以从 vCenter Server 权限管理界面将不同的主机配置特权应用于不同的指定用户，而不是允许管理员使用 root 用户帐户登录到 ESXi 主机。您可以在 vSphere Web Client 中创建自定义角色、将特权分配给该角色，并将该角色与指定用户或指定用户组以及 ESXi 主机对象关联。

	<p>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 <i>vSphere 单台主机管理 - VMware Host Client</i> 文档。</p>
尽可能减少打开的 ESXi 防火墙端口数	<p>默认情况下，只有启动相应的服务时，才会打开 ESXi 主机上的防火墙端口。可以使用 vSphere Web Client 或 ESXCLI 或 PowerCLI 命令检查和管理防火墙端口状态。</p> <p>请参见第 52 页，“ESXi 防火墙配置”。</p>
自动化 ESXi 主机管理	<p>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。</p> <p>有关 vSphere Auto Deploy 的信息，请参见第 33 页，“使用脚本管理主机配置设置”和 <i>vSphere 安装和设置</i> 文档。</p>
使用锁定模式	<p>在锁定模式下，默认只能通过 vCenter Server 访问 ESXi 主机。从 vSphere 6.0 开始，您可以选择严格锁定模式或正常锁定模式。可以定义异常用户以允许直接访问服务帐户（如备份代理）。</p> <p>请参见第 58 页，“锁定模式”。</p>
检查 VIB 软件包完整性	<p>每个 VIB 软件包均有关联的接受级别。只有在接受级别与主机的接受级别相同或更高时，才能将 VIB 添加到 ESXi 主机。除非明确更改主机的接受级别，否则无法将由社区支持或合作伙伴支持的 VIB 添加到主机。</p> <p>请参见第 63 页，“管理主机和 VIB 的接受级别”。</p>
管理 ESXi 证书	<p>在 vSphere 6.0 及更高版本中，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 CA 签名的证书。</p> <p>请参见第 39 页，“ESXi 主机的证书管理”。</p>
智能卡身份验证	<p>从 vSphere 6.0 开始，ESXi 提供了智能卡身份验证选项，而不是用户名和密码身份验证。</p> <p>请参见第 74 页，“配置 ESXi 的智能卡身份验证”。</p>
ESXi 帐户锁定	<p>从 vSphere 6.0 开始，系统将支持对通过 SSH 和通过 vSphere Web Services SDK 进行的访问进行帐户锁定。默认情况下，允许最多 10 次尝试，当这些尝试均失败后，才会锁定帐户。默认情况下，帐户将在两分钟后解锁。直接控制台界面 (DCUI) 和 ESXi Shell 不支持帐户锁定。</p> <p>请参见第 34 页，“ESXi 密码和帐户锁定”。</p>
<p>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。请参见和 <i>vSphere 单台主机管理 - VMware Host Client</i> 文档。</p>	

确保 vCenter Server 系统及关联服务安全

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

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，您可以保护多个 vCenter Server 实例及一个或多个 Platform Services Controller 实例。

强化对所有 vCenter 主机的保护

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

了解 vCenter 证书模型

默认情况下，VMware Certificate Authority 将为每个 ESXi 主机、环境中的每台计算机以及每个解决方案用户置备 VMCA 签名的证书。环境可以即装即用，但如果公司策略需要，则可以更改默认行为。有关详细信息，请参见 *Platform Services Controller 管理文档*。

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。您可以添加其他标识源（Active Directory 或 LDAP），并设置默认标识源。此后，能够向任一标识源进行身份验证的用户均可以查看对象并执行任务（如果拥有相关权限）。有关详细信息，请参见 *Platform Services Controller 管理文档*。

向指定用户或组分配角色

为了实现更好的日志记录，请将授予给对象的每个权限与指定用户或组以及预定义角色或自定义角色相关联。vSphere 6.0 权限模型提供了较大的灵活性，允许通过多种方式授权用户或组。请参见第 16 页，“了解 vSphere 中的授权”和第 29 页，“常见任务的所需特权”。

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 NTP

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

请参见第 147 页，“同步 vSphere 网络连接上的时钟”。

确保虚拟机安全

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

保护客户机操作系统

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

禁用不必要的功能

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

请参见第 99 页，“禁用虚拟机中不必要的功能”。

使用模板和脚本式管理

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

如果要在初始部署后更改设置，请考虑使用脚本（如 PowerCLI）。本文档使用 vSphere Web Client 对许多任务进行了说明，以阐述该过程。使用脚本（而不是 vSphere Web Client）有助于保持环境的一致性。在大型环境中，您可以将虚拟机分组到文件夹以优化脚本。

请参见第 98 页，“使用模板来部署虚拟机”。有关详细信息，请参见《vSphere 虚拟机管理》。

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。此访问可能造成对虚拟机的恶意攻击。

考虑 UEFI 安全引导

从 vSphere 6.5 开始，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。请参见第 95 页，“为虚拟机启用或禁用 UEFI 安全引导”。

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 131 页，第 8 章“确保 vSphere 网络安全”中进行更详细的介绍。

隔离网络流量

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

请参见第 37 页，“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。请参见第 52 页，“ESXi 防火墙配置”。

您也可以明确打开 Platform Services Controller 和 vCenter Server 实例上的端口。请参见第 89 页，“vCenter Server 和 Platform Services Controller 所需的端口”和第 92 页，“其他 vCenter Server TCP 和 UDP 端口”。

考虑网络安全策略

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

有关说明，请参见《vSphere 网络连接》文档。

确保虚拟机网络安全

可确保虚拟机网络安全的方法取决于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以及其他因素。与其他常见安全措施（例如，安装防火墙）结合使用时，虚拟交换机和分布式虚拟交换机提供的保护作用非常显著。

请参见第 131 页，第 8 章“确保 vSphere 网络安全”。

考虑使用 VLAN 保护您的环境

ESXi 支持可用于为虚拟机网络或存储配置提供进一步保护的 IEEE 802.1q VLAN。通过 VLAN，可对物理网络进行分段。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。

请参见第 137 页，“通过 VLAN 确保虚拟机安全”。

确保虚拟化存储连接的安全

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

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

请参见第 150 页，“存储安全性最佳做法”。

评估 IPSec 的使用

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

请参见第 140 页，“Internet 协议安全”。

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

vSphere 环境中的密码

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

ESXi 密码

ESXi 密码限制由 Linux PAM 模块 `pam_passwdqc` 确定。请参见 Linux 手册页了解 `pam_passwdqc` 并参见第 34 页，“ESXi 密码和帐户锁定”。

vCenter Server 及其他 vCenter 服务的密码

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

vCenter Single Sign-On 管理员

默认情况下，vCenter Single Sign-On 管理员密码为 `administrator@vsphere.local`，如果您在安装期间指定了其他域，则为 `administrator@mydomain`。此密码不会过期。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《Platform Services Controller 管理》。

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 域的其他用户

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《Platform Services Controller 管理》。默认情况下，这些密码将在 90 天后过期，但是根据密码策略管理员可以更改过期时间。

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

其他用户

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

vCenter Single Sign-On 支持一个默认标识源，用户只能使用其用户名登录到具有 vSphere Web Client 的相应域。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 Appliance 直接控制台用户界面用户的密码

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

部署 vCenter Server Appliance 时，指定这些密码。

- 设备 Linux 操作系统的 root 用户的密码。
- vCenter Single Sign-On 域管理员（默认为 administrator@vsphere.local）的密码。

可以从设备控制台更改 root 用户密码并执行其他 vCenter Server Appliance 本地用户管理任务。请参见 *vCenter Server Appliance 配置*。

安全性最佳做法与资源

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

本手册包括 vSphere 基础架构的不同组件的最佳做法。

表 1-1 安全性最佳做法

vSphere 组件	资源
ESXi 主机	第 31 页，第 3 章“确保 ESXi 主机安全”
vCenter Server 系统	第 83 页，“vCenter Server 安全性最佳做法”
虚拟机	第 97 页，“虚拟机安全性最佳做法”
vSphere 网络连接	第 144 页，“vSphere 网络连接安全性最佳做法”

本手册只是确保环境安全所需的其中一种资源。

VMware 安全资源（包括安全警示和下载）通过 Web 提供。

表 1-2 Web 上的 VMware 安全资源

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

vSphere 权限和用户管理任务

身份验证和授权可以控制访问权限。vCenter Single Sign-On 支持身份验证，这表明它可以确定用户究竟是否可以访问 vSphere 组件。每个用户还必须获得授权，才能查看或操作 vSphere 对象。

vSphere 支持多种不同的授权机制，如第 16 页，“了解 vSphere 中的授权”中所述。本部分中的信息重点关注 vCenter Server 权限模型的工作原理以及如何执行用户管理任务。

vCenter Server 允许通过权限和角色对授权进行精细控制。向 vCenter Server 对象层次结构中的对象分配权限时，请指定哪个用户或组对该对象具有哪些特权。要指定特权，请使用角色（即特权集）。

最初，仅 vCenter Single Sign-On 域的管理员用户（默认为 administrator@vsphere.local）有权登录到 vCenter Server 系统。授权后，该用户可以执行如下操作：

- 1 将在其中定义了用户和组的标识源添加到 vCenter Single Sign-On 中。请参见 *Platform Services Controller 管理文档*。
- 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。



角色、特权和权限 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_roles_privileges_permissions_vsphere_web_client)

本章讨论了以下主题：

- 第 16 页，“了解 vSphere 中的授权”
- 第 21 页，“管理 vCenter 组件的权限”
- 第 23 页，“全局权限”
- 第 25 页，“使用角色分配特权”
- 第 28 页，“角色和权限的最佳做法”
- 第 29 页，“常见任务的所需特权”

了解 vSphere 中的授权

您授权用户或组使用对象上的权限在 vCenter 对象上执行任务。

vSphere 6.0 及更高版本允许有特权的用户以下列方式授予其他用户执行任务的权限。在大多数情况下，这些方法相互排斥。但是，您可以分配全局权限以授权特定用户执行所有解决方案，分配本地 vCenter Server 权限以授权其他用户处理各个 vCenter Server 实例。

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。每种权限都会向一个用户或组授予一组特权，即选定对象的角色。例如，您可以选择对象层次结构中的一个 ESXi 主机并向一组用户分配角色，以授予这些用户对该主机的相应特权。

全局权限

全局权限应用到跨多个解决方案的全局 root 对象。例如，如果安装了 vCenter Server 和 vRealize Orchestrator，则可以使用全局权限向一组用户授予对这两个对象层次结构中所有对象的读取权限。

系统会在整个 vsphere.local 域中复制全局权限。全局权限不会为通过 vsphere.local 组管理的服务提供授权。请参见第 23 页，“全局权限”。

vsphere.local 组中的组成员资格

vCenter Single Sign-On 域的用户（默认 administrator@vsphere.local）可以执行与 Platform Services Controller 附带的服务相关联的任务。vsphere.local 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 *Platform Services Controller 管理* 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 vCenter Server 权限模型

vCenter Server 系统的权限模型需要向 vSphere 对象层次结构中的对象分配权限。每种权限都会向一个用户或组授予一组特权，即选定对象的角色。

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。

用户和组

在 vCenter Server 系统中，可以仅向经过身份验证的用户或经过身份验证的用户组分配特权。用户通过 vCenter Single Sign-On 进行身份验证。必须在 vCenter Single Sign-On 正用于进行身份验证的标识源中定义用户和组。使用您的标识源（例如 Active Directory）中的工具定义用户和组。

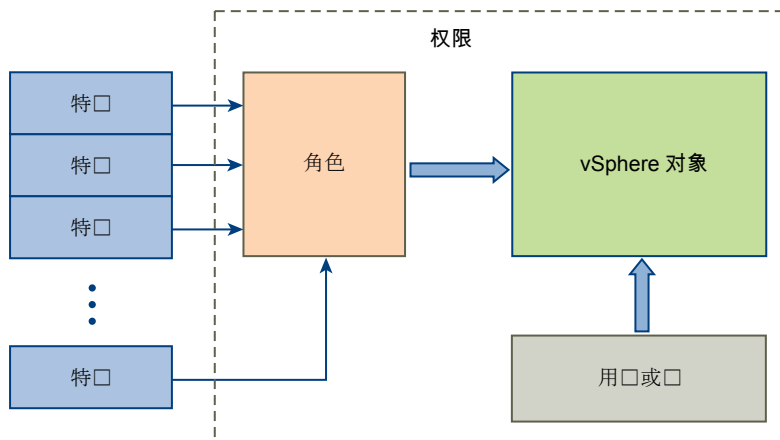
特权

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。默认角色（例如管理员）已在 vCenter Server 中预定义，不能更改。其他角色（例如资源池管理员）是预定义的样本角色。可以从头开始或者通过克隆和修改样本角色创建自定义角色。请参见第 27 页，“创建自定义角色”和第 27 页，“克隆角色”。

图 2-1 vSphere 权限



要向对象分配权限，请执行以下步骤：

- 1 在 vCenter 对象层次结构中选择要应用权限的对象。
- 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，权限会传播，即组或用户对选定对象及其子对象具有选定角色。

借助权限模型，您可以通过提供预定义的角色轻松完成操作。也可通过合并创建自定义角色。有关所有特权以及可对其应用特权的对象的参考信息，请参见第 153 页，第 10 章“定义的特权”。有关执行常见任务所需的特权集的示例，请参见第 29 页，“常见任务的所需特权”。

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。

独立 ESXi 主机的权限模型比较简单。请参见第 64 页，“为 ESXi 主机分配特权”。

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。

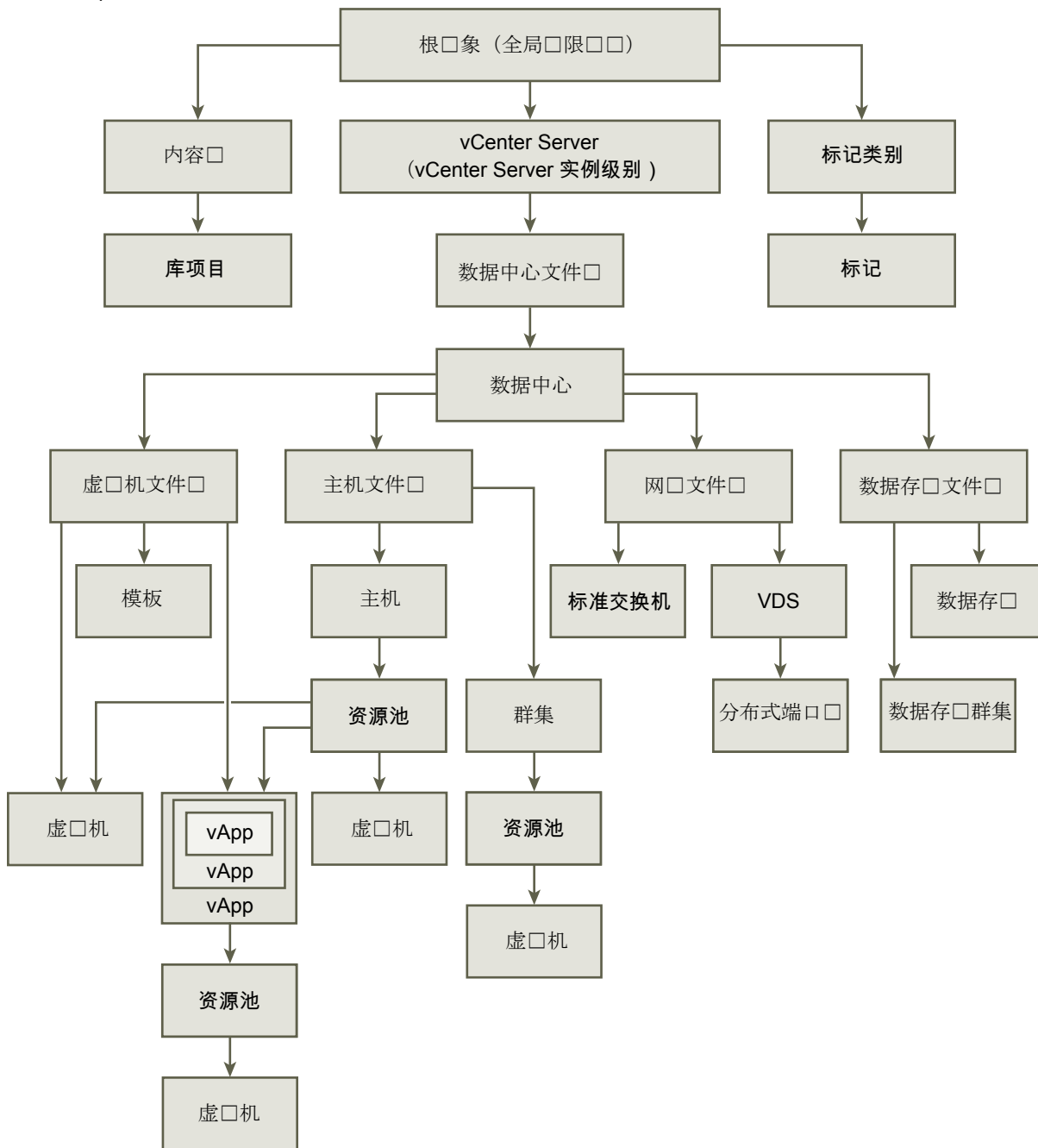
权限的层次结构继承

当向对象授予权限时，可以选择是否允许其沿对象层次结构向下传播。为每个权限设置传播。传播并非普遍适用。为子对象定义的权限将总是替代从父对象中传播的权限。

该图说明了清单层次结构和权限传播的路径。

注意 全局权限支持从全局根对象跨多个解决方案分配特权。请参见第 23 页，“全局权限”。

图 2-2 vSphere 清单层次结构



大多数清单对象在层次结构中从单一父对象继承权限。例如，数据存储从其父数据存储文件夹或父数据中心继承权限。虚拟机同时从父虚拟机文件夹和父主机、群集或资源池继承权限。

例如，可为 **Distributed Switch** 及其关联的分布式端口组设置权限，方法是设置对父对象（例如文件夹或数据中心）的权限。此外，还必须选择将这些权限传播给子对象的选项。

权限在层次结构中有多种形式：

受管实体

特权用户可以对受管实体定义权限。

- 群集
- 数据中心

- 数据存储
- 数据存储群集
- 文件夹
- 主机
- 网络（vSphere Distributed Switch 除外）
- 分布式端口组
- 资源池
- 模板
- 虚拟机
- vSphere vApp

全局实体

不能修改从根 vCenter Server 系统中派生权限的实体的权限。

- 自定义字段
- 许可证
- 角色
- 统计间隔
- 会话

多项权限设置

对象可能拥有多种权限，但每个用户或组只拥有一种权限。例如，一种权限可能会指定组 B 对某个对象具有管理员特权，另一种权限可能会指定组 B 可能对同一对象具有虚拟机管理员特权。

如果某个对象从两个父对象继承了权限，则对一个对象的权限将添加到对另一个对象的权限中。例如，如果某个虚拟机位于虚拟机文件夹中，同时还属于资源池，该虚拟机将同时从虚拟机文件夹和资源池继承所有权限设置。

在子对象上应用的权限始终会替代在父对象上应用的权限。请参见第 20 页，“示例 2：子权限替代父权限”。

如果对同一对象定义了多个组权限，且用户属于这些组中的两个或多个组，则可能出现以下两种情况：

- 如果没有为用户定义对该对象的权限，则用户将获得分配给该对象的组的一系列特权。
- 如果为用户定义了对该对象的权限，则该用户权限将优先于所有组权限。

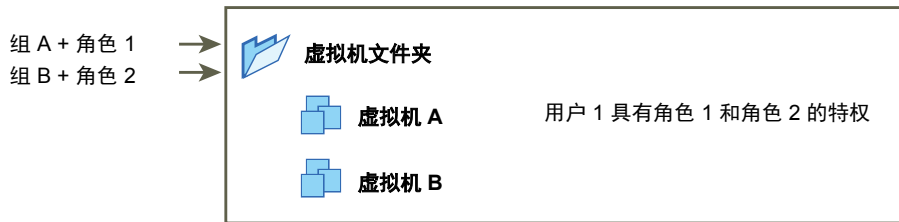
示例 1：继承多个权限

此示例说明了对象如何从组（在父对象上授予了权限）中继承多个权限。

在此示例中，为两个不同组中的同一对象分配两种权限。

- 角色 1 可启动虚拟机。
- 角色 2 可对虚拟机执行快照。
- 在虚拟机文件夹上为组 A 授予角色 1，并将权限设置为传播到子对象。
- 在虚拟机文件夹上为组 B 授予角色 2，并将权限设置为传播到子对象。
- 用户 1 未获得特定特权。

属于组 A 和组 B 的用户 1 登录。用户 1 可以同时启动虚拟机 A 和虚拟机 B 并对其执行快照。

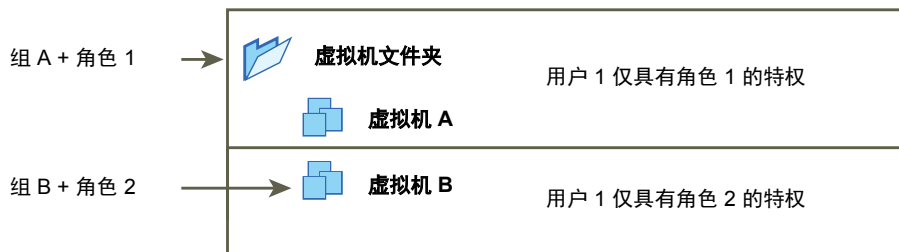
图 2-3 示例 1：继承多个权限**示例 2：子权限替代父权限**

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

在此示例中，权限在两个不同组的两个不同对象上定义。

- 角色 1 可启动虚拟机。
- 角色 2 可对虚拟机执行快照。
- 在虚拟机文件夹上为组 A 授予角色 1，并将权限设置为传播到子对象。
- 在虚拟机 B 上为组 B 授予角色 2。

属于组 A 和组 B 的用户 1 登录。因为在层次结构中，角色 2 被分配在角色 1 之下，所以它将在虚拟机 B 上替代角色 1。用户 1 可以启动虚拟机 A，但不能执行快照。用户 1 可对虚拟机 B 执行快照但无法将其启动。

图 2-4 示例 2：子权限替代父权限**示例 3：用户角色替代组角色**

下例说明了直接分配给单个用户的角色如何替代与分配给组的角色关联的特权。

在此示例中，权限在相同的对象上定义。一种权限与包含某个角色的组相关联，另一种权限与包含某个角色的单个用户相关联。用户属于组成员。

- 角色 1 可启动虚拟机。
- 在虚拟机文件夹上为组 A 授予角色 1。
- 在虚拟机文件夹上为用户 1 授予无权访问角色。

属于组 A 的用户 1 登录。在虚拟机文件夹上为用户 1 授予的无权访问角色替代分配给组的角色。用户 1 无权访问虚拟机文件夹或虚拟机 A 和 B。

图 2-5 示例 3：用户权限替代组权限



管理 vCenter 组件的权限

权限在 vCenter 对象层次结构中的对象上设置。每种权限与包含用户或组的对象以及该组或用户的访问角色相关联。例如，您可以选择一个虚拟机对象，添加一种权限用于向组 1 授予 **ReadOnly** 角色，然后添加另一种权限用于将管理员角色授予用户 2。

通过将不同角色分配给不同对象的用户组，您可控制这些用户能够在 vSphere 环境中执行的任务。例如，要允许组配置主机内存，请选择该主机并添加用于向该组授予角色的权限，包括**主机.配置.内存配置**特权。

要从 vSphere Web Client 管理权限，需要了解以下概念：

权限	vCenter Server 对象层次结构中的每个对象都具有关联的权限。每个权限为一个组或用户指定该组或用户具有对象的哪些特权。
用户和组	在 vCenter Server 系统中，可以仅向经过身份验证的用户或经过身份验证的用户组分配特权。用户通过 vCenter Single Sign-On 进行身份验证。必须在 vCenter Single Sign-On 正用于进行身份验证的标识源中定义用户和组。使用您的标识源（例如 Active Directory）中的工具定义用户和组。
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。默认角色（例如管理员）已在 vCenter Server 中预定义，不能更改。其他角色（例如资源池管理员）是预定义的样本角色。可以从头开始或者通过克隆和修改样本角色创建自定义角色。请参见第 27 页，“创建自定义角色”和第 27 页，“克隆角色”。

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。请参见第 17 页，“**权限的层次结构继承**”。还可以向全局根对象分配权限，以将权限应用于所有解决方案中的所有对象。请参见第 23 页，“**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，可以同时为相同的权限分配给多个对象。

从 vSphere Web Client 分配权限时，用户和组名称必须与 Active Directory 精确匹配，包括大小写。如果从 vSphere 的早期版本进行升级，则在遇到组问题时，请检查大小写是否不一致。

前提条件

在要修改其权限的对象上，必须具有包含**权限.修改权限**特权的角色。

步骤

- 1 在 vSphere Web Client 对象导航器中，浏览到要为其分配权限的对象。
- 2 单击**权限**选项卡。

- 3 单击“添加”图标，然后单击**添加**。
- 4 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”框中键入名称，或者从列表中选择名称。
系统会搜索用户名、组名称和相关描述。
 - c 选择用户或组，然后单击**添加**。
名称将添加到**用户或组**列表中。
 - d （可选）单击**检查名称**验证标识源中是否存在该用户或该组。
 - e 单击**确定**。
- 5 在**分配的角色**下拉菜单中选择角色。
分配给该对象的角色会显示在菜单中。该角色中包含的特权将在角色标题下面的区域中列出。
- 6 （可选）要限制传播，取消选中**传播到子对象**复选框。
角色只应用于选定对象，而不会传播给子对象。
- 7 单击**确定**以添加权限。

更改权限

在为清单对象设置用户或组和角色对后，可以更改与用户或组配对的角色或更改**传播**复选框的设置。还可移除权限设置。

步骤

- 1 在 vSphere Web Client 对象导航器中，浏览到对象。
- 2 单击**权限**选项卡。
- 3 单击某行以选择权限。
- 4 单击**针对权限更改角色**图标。
- 5 在**分配的角色**下拉菜单中为用户或组选择角色。
- 6 启用**传播到子对象**复选框，以便使权限更改得到继承，然后单击**确定**。

移除权限

您可以从对象层次结构的对象中移除各个用户或组的权限。执行此操作后，用户或组将不再拥有与对象上的角色关联的特权。

注意 无法移除系统预定义的权限。

步骤

- 1 在 vSphere Web Client 对象导航器中，浏览到对象。
- 2 单击**配置**选项卡，然后选择**权限**。
- 3 单击某行以选择权限。
- 4 单击**移除权限**图标。

更改用户验证设置

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。可以禁用验证或更改两次验证之间的时间间隔。如果域中有数千个用户或组，或者如果完成搜索需要很长时间，则可以考虑调整搜索设置。

对于早于 vCenter Server 5.0 的 vCenter Server 版本，这些设置适用于与 vCenter Server 关联的 Active Directory。对于 vCenter Server 5.0 及更高版本，这些设置适用于 vCenter Single Sign-On 标识源。

注意 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 Web 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**下的**常规**。
- 3 单击**编辑**，然后选择**用户目录**。
- 4 根据需要更改值。

选项	描述
用户目录超时	连接到 Active Directory 服务器的超时时间间隔（以秒为单位）。该值指定 vCenter Server 允许搜索在所选域上运行的最大时间。搜索大型域需要很长时间。
查询限制	选中此复选框以设置 vCenter Server 显示的用户和组的最大数目。
查询限制大小	在 选择用户或组 对话框中 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。
验证	取消选中复选框以禁用验证
验证周期	指定 vCenter Server 验证权限的频率（以分钟为单位）。

- 5 单击**确定**。

全局权限

全局权限应用到跨多个解决方案的全局 root 对象，例如，vCenter Server 和 vRealize Orchestrator。使用全局权限可为用户或组提供所有对象层次结构中所有对象的特权。

每个解决方案自身的对象层次结构中都有一个 root 对象。全局 root 对象充当所有解决方案的 root 对象的父对象。您可以向用户或组分配全局权限，确定每个用户或组的角色。角色确定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。请参见第 25 页，“[使用角色分配特权](#)”。重要的是对 vCenter Server 权限与全局权限加以区分。

vCenter Server 权限

您通常将权限应用到 vCenter Server 清单对象，如 ESXi 主机或虚拟机。操作时，指定拥有一组对象特权的用户或组（叫做角色）。

全局权限

全局权限向用户和组提供查看或管理部署的每个清单层次结构中所有对象的特权。

如果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。

重要事项 使用全局权限时要小心谨慎。确认您确实希望分配对所有清单层次结构中所有对象的权限。

添加全局权限

可以使用全局权限向用户或组授予对您的部署中所有清单层次结构中的所有对象的特权。

重要事项 使用全局权限时要小心谨慎。确认您确实希望分配对所有清单层次结构中所有对象的权限。

前提条件

您必须对所有清单层次结构的 **root** 对象具有**权限.修改权限**特权，才能执行此任务。

步骤

- 1 单击**系统管理**，然后在“访问控制”区域中选择**全局权限**。
- 2 单击**管理**，然后单击“添加权限”图标。
- 3 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”框中键入名称，或者从列表中选择名称。
系统会搜索用户名、组名称和相关描述。
 - c 选择用户或组，然后单击**添加**。
名称将添加到**用户或组**列表中。
 - d （可选）单击**检查名称**验证标识源中是否存在该用户或该组。
 - e 单击**确定**。
- 4 在**分配的角色**下拉菜单中选择角色。
分配给该对象的角色会显示在菜单中。该角色中包含的特权将在角色标题下面的区域中列出。
- 5 在大多数情况下，请选中**传播到子对象**复选框。
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。
- 6 单击**确定**。

标记对象的权限

在 vCenter Server 对象层次结构中，标记对象不是 vCenter Server 的子项，而是在 vCenter Server root 级别创建的。在具有多个 vCenter Server 实例的环境中，标记对象在 vCenter Server 实例间共享。标记对象权限的工作方式不同于 vCenter Server 对象层次结构中其他对象的权限。

只有全局权限或分配给标记对象的权限适用

如果将权限授予 vCenter Server 清单对象（例如 ESXi 主机或虚拟机）上的某个用户，那么该用户无法对该对象执行标记操作。

例如，如果将**分配 vSphere 标记**特权授予主机 TPA 上的用户 Dana，该权限对 Dana 能否在主机 TPA 上分配标记没有影响。Dana 必须拥有 root 级别的**分配 vSphere 标记**特权（即全局权限）或者必须拥有针对该标记对象的特权。

表 2-1 全局权限和标记对象权限如何影响用户可以执行的操作

全局权限	标记级别的权限	vCenter Server 对象级别的权限	有效权限
未分配标记特权	Dana 拥有标记的分配或取消分配 vSphere 标记特权。	Dana 在 ESXi 主机 TPA 上拥有删除 vSphere 标记特权	Dana 拥有标记的分配或取消分配 vSphere 标记特权。
Dana 拥有分配或取消分配 vSphere 标记特权。	未分配标记特权。	Dana 在 ESXi 主机 TPA 上拥有删除 vSphere 标记特权	Dana 拥有分配或取消分配 vSphere 标记全局特权。这包括标记级别的特权。
未分配标记特权	未分配标记特权。	Dana 在 ESXi 主机 TPA 上拥有分配或取消分配 vSphere 标记特权	Dana 在任何对象（包括主机 TPA）上均没有标记特权。

全局权限是标记对象权限的补充

全局权限，即在 root 对象上分配的权限，可在标记对象权限更为严格时作为标记对象权限的补充。vCenter Server 权限不会影响标记对象。

例如，假设您在 root 级别（也就是使用全局权限）向用户 Robin 分配了删除 vSphere 标记权限。对于标记“生产”，您未向 Robin 分配删除 vSphere 标记特权。这种情况下，Robin 对标记“生产”仍拥有特权，因为 Robin 拥有全局权限。除非修改全局权限，否则您无法限制特权。

表 2-2 全局权限是标记级别权限的补充

全局权限	标记级别的权限	有效权限
Robin 拥有删除 vSphere 标记特权	Robin 没有标记的删除 vSphere 标记特权。	Robin 拥有删除 vSphere 标记特权。
未分配标记特权	Robin 没有针对标记分配的删除 vSphere 标记特权。	Robin 没有删除 vSphere 标记特权

标记级别权限可以扩展全局权限

您可以使用标记级别权限扩展全局权限。这意味着用户可以同时对标记拥有全局权限和标记级别权限。

表 2-3 全局权限可以扩展标记级别权限

全局权限	标记级别的权限	有效权限
Lee 拥有分配或取消分配 vSphere 标记特权。	Lee 拥有删除 vSphere 标记特权。	Lee 拥有标记的分配 vSphere 标记特权和删除 vSphere 标记特权。
未分配标记特权。	Lee 拥有针对标记分配的删除 vSphere 标记特权。	Lee 拥有标记的删除 vSphere 标记特权。

使用角色分配特权

角色是一组预定义的特权。特权定义了执行操作和读取属性所需的权限。例如，虚拟机管理员角色允许用户读取和更改虚拟机属性。

分配权限时，可将用户或组与角色配对，并将该配对与清单对象关联。对于清单中的不同对象，单个用户或组可能有不同角色。

例如，假设清单中有两个资源池（池 A 和池 B）。可以为组 Sales 在池 A 上分配虚拟机用户角色，而在池 B 上分配只读角色。执行上述分配后，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。

默认情况下，vCenter Server 可提供系统角色和样本角色。

系统角色

系统角色是永久的。不能编辑与这些角色关联的特权。

样本角色

VMware 可为某些频繁执行的任务组合提供样本角色。您可以克隆、修改或删除这些角色。

注意 为避免丢失样本角色中的预定义设置，请先克隆角色，然后再对克隆进行修改。无法将样本重置为其默认设置。

用户只有在创建任务时其角色包含执行该任务所需的特权的情况下，才能调度任务。

注意 即使所涉及的用户已登录，对角色和特权的更改也会立即生效。但搜索除外，更改会在用户注销再重新登录之后才生效。

vCenter Server 和 ESXi 中的自定义角色

可以为 vCenter Server 及其管理的所有对象或者为各个主机创建自定义角色。

vCenter Server 自定义角色 (推荐)

可使用 vSphere Web Client 中的角色编辑功能创建自定义角色，以创建符合用户需求的特权组。

ESXi 自定义角色

可以使用 CLI 或 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。

注意 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**。



在 vSphere Web Client 中创建角色

(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_creating_role_in_vsphere_webclient)

vCenter Server 系统角色

角色是一组预定义的特权。向对象添加权限时，请将用户或组与角色配对。vCenter Server 包括多种无法更改的系统角色。

vCenter Server 系统角色

vCenter Server 提供一些默认角色。不能更改与默认角色关联的特权。默认角色以层次结构方式进行组织。每个角色将继承前一个角色的特权。例如，管理员角色继承只读角色的特权。您创建的角色不继承任何系统角色的特权。

管理员角色

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固有的所有特权。如果您使用管理员角色对对象执行操作，可以将特权分配给各个用户和组。如果您使用管理员角色在 vCenter Server 中进行操作，可以将特权分配给默认 vCenter Single Sign-On 标识源中的用户和组。支持的身份服务包括 Windows Active Directory 和 OpenLDAP 2.4。

默认情况下，安装后，`administrator@vsphere.local` 用户将对 vCenter Single Sign-On 和 vCenter Server 具有管理员角色。该用户之后可以将其他用户与 vCenter Server 上的管理员角色相关联。

无加密管理员角色

具有无加密管理员角色的对象用户与具有管理员角色的用户拥有相同的特权，**加密操作**特权除外。此角色允许管理员指定其他管理员，他们无法加密或解密虚拟机或访问加密数据，但可以执行所有其他管理任务。

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。

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。

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”。

创建自定义角色

您可以创建 vCenter Server 自定义角色，以满足环境的访问控制需求。

如果在与其他 vCenter Server 系统属于同一个 vCenter Single Sign-On 域的 vCenter Server 系统上创建或编辑一个角色，VMware Directory Service (vmdir) 会将您所做的更改传播到该组中的所有其他 vCenter Server 系统。对特定用户和对象的角色分配不会在 vCenter Server 系统上共享。

前提条件

验证您是否以具有管理员特权的用户身份登录。

步骤

- 1 通过 vSphere Web Client 登录到 vCenter Server。
- 2 选择“主页”，然后依次单击**管理**和**角色**。
- 3 单击**创建角色操作 (+)**按钮。
- 4 键入新角色的名称。
- 5 为该角色选择特权，然后单击**确定**。

克隆角色

可复制现有角色、重命名该角色，以及编辑该角色。在复制时，新角色不会应用到任何用户或组以及对象中。必须向用户或组以及对象分配该角色。

如果在与其他 vCenter Server 系统属于同一个 vCenter Single Sign-On 域的 vCenter Server 系统上创建或编辑一个角色，VMware Directory Service (vmdir) 会将您所做的更改传播到该组中的所有其他 vCenter Server 系统。对特定用户和对象的角色分配不会在 vCenter Server 系统上共享。

前提条件

验证您是否以具有管理员特权的用户身份登录。

步骤

- 1 通过 vSphere Web Client 登录到 vCenter Server。

- 2 选择“主页”，然后依次单击**管理**和**角色**。
- 3 选择某个角色，然后单击**克隆角色操作**图标。
- 4 键入克隆角色的名称。
- 5 为该角色选择或取消选择特权，然后单击**确定**。

编辑角色

编辑角色时，可更改为该角色选择的特权。完成后，这些特权将应用于分配了编辑后角色的所有用户或组。

如果在与其他 vCenter Server 系统属于同一个 vCenter Single Sign-On 域的 vCenter Server 系统上创建或编辑一个角色，VMware Directory Service (vmdir) 会将您所做的更改传播到该组中的所有其他 vCenter Server 系统。对特定用户和对象的角色分配不会在 vCenter Server 系统上共享。

前提条件

验证您是否以具有管理员特权的用户身份登录。

步骤

- 1 通过 vSphere Web Client 登录到 vCenter Server。
- 2 选择“主页”，然后依次单击**管理**和**角色**。
- 3 选择某一角色，然后单击**编辑角色操作**按钮。
- 4 为该角色选择或取消选择特权，然后单击**确定**。

角色和权限的最佳做法

使用角色和权限的最佳做法可充分提高 vCenter Server 环境的安全性和易管理性。

在 vCenter Server 环境中配置角色和权限时，VMware 建议采用以下最佳做法：

- 如果可能，请向组分配角色，而不要向单个用户分配角色，以便向该组授予特权。
- 仅授予对被需要对象的权限，仅向必须拥有特权的用户或组分配特权。使用最少权限数使得了解和管理权限结构变得更容易。
- 如果要为组分配限制性角色，请检查该组是否不包括管理员用户或其他具有管理特权的用户。否则，您可能无意识地限制了部分清单层次结构（已从中向该组分配了限制性角色）中管理员的特权。
- 使用文件夹对对象进行分组。例如，如果要授予对一组主机的修改权限并授予对另一组主机的查看权限，请将各组主机置于一个文件夹中。
- 向根 vCenter Server 对象添加权限时要小心。具有根级别特权的用户有权访问 vCenter Server 上的全局数据，例如，角色、自定义属性、vCenter Server 设置。
- 在大多数情况下，向对象分配权限时启用传播功能。这可确保当向清单层次结构中插入新对象时，它们会继承权限并且用户可以对其进行访问。
- 使用“无权访问”角色可屏蔽您希望特定用户或组无权访问的对象层次结构中的特定区域。
- 对许可证所做的更改会传播到链接到同一 Platform Services Controller 或同一 vCenter Single Sign-On 域中 Platform Services Controller 的所有 vCenter Server 系统，即使用户并未对所有 vCenter Server 系统拥有特权也会传播。

常见任务的所需特权

许多任务需要清单中多个对象的权限。您可查看执行任务所需的适用的特权以及适合的样本角色。

下表列出了需要多个特权的常见任务。可以通过将用户与其中一个预定义的角色配对来添加对清单对象的权限，或者可以创建具有所需特权集的自定义角色以多次使用。

如果要执行的任务不在此表中，以下规则可帮助您确定必须将权限分配到的位置以允许执行特定操作：

- 消耗存储空间的任何操作（例如创建虚拟磁盘或生成快照）都需要目标数据存储上的**数据存储.分配空间**特权，以及自我执行的特权。
- 在清单层次结构中移动对象需要对象自身、源父对象（如文件夹或群集）和目标父对象上的适当特权。
- 每个主机和群集有其自身的固有资源池，其中包含该主机或群集的所有资源。将虚拟机直接部署到主机或群集需要**资源.将虚拟机分配给资源池**特权。

表 2-4 常见任务的所需特权

任务	所需特权	适用角色
创建虚拟机	在目标文件夹或数据中心上： <ul style="list-style-type: none"> ■ 虚拟机.清单.新建 ■ 虚拟机.配置.添加新磁盘（如果要创建新虚拟磁盘） ■ 虚拟机.配置.添加现有磁盘（如果使用现有虚拟磁盘） ■ 虚拟机.配置.裸设备（如果使用 RDM 或 SCSI 直通设备） 	管理员
	在目标主机、群集或资源池上： 资源.将虚拟机分配给资源池	资源池管理员或管理员
	在包含数据存储的目标数据存储或文件夹上： 数据存储.分配空间	数据存储用户或管理员
	在虚拟机将分配到的网络上： 网络.分配网络	网络用户或管理员
从模板部署虚拟机	在目标文件夹或数据中心上： <ul style="list-style-type: none"> ■ 虚拟机.清单.从现有项创建 ■ 虚拟机.配置.添加新磁盘 	管理员
	在模板或模板的文件夹上： 虚拟机.置备.部署模板	管理员
	在目标主机、群集或资源池上： 资源.将虚拟机分配给资源池	管理员
	在目标数据存储或数据存储的文件夹上： 数据存储.分配空间	数据存储用户或管理员
	在虚拟机将分配到的网络上： 网络.分配网络	网络用户或管理员
生成虚拟机快照	在虚拟机或虚拟机的文件夹上： 虚拟机.快照管理.创建快照	虚拟机超级用户或管理员
将虚拟机移动到资源池中	在虚拟机或虚拟机的文件夹上： <ul style="list-style-type: none"> ■ 资源.将虚拟机分配给资源池 ■ 虚拟机.清单.移动 	管理员
	在目标资源池上： 资源.将虚拟机分配给资源池	管理员

表 2-4 常见任务的所需特权（续）

任务	所需特权	适用角色
在虚拟机上安装客户机操作系统	在虚拟机或虚拟机的文件夹上： <ul style="list-style-type: none"> ■ 虚拟机.交互.回答问题 ■ 虚拟机.交互.控制台交互 ■ 虚拟机.交互.设备连接 ■ 虚拟机.交互.关闭电源 ■ 虚拟机.交互.打开电源 ■ 虚拟机.交互.重置 ■ 虚拟机.交互.配置 CD 媒体（如果从 CD 安装） ■ 虚拟机.交互.配置软盘媒体（如果从软盘安装） ■ 虚拟机.交互.VMware Tools 安装 	虚拟机超级用户或管理员
	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： <ul style="list-style-type: none"> ■ 数据存储.浏览数据存储 ■ 数据存储.低级别文件操作 	虚拟机超级用户或管理员
通过 vMotion 迁移虚拟机	在虚拟机或虚拟机的文件夹上： <ul style="list-style-type: none"> ■ 资源.迁移已打开电源的虚拟机 ■ 资源.将虚拟机分配给资源池（如果目标资源池与源资源池不同） 	资源池管理员或管理员
	在目标主机、群集或资源池上（如果与源主机、群集或资源池不同）： 资源.将虚拟机分配给资源池	资源池管理员或管理员
冷迁移（重定位）虚拟机	在虚拟机或虚拟机的文件夹上： <ul style="list-style-type: none"> ■ 资源.迁移已关闭电源的虚拟机 ■ 资源.将虚拟机分配给资源池（如果目标资源池与源资源池不同） 	资源池管理员或管理员
	在目标主机、群集或资源池上（如果与源主机、群集或资源池不同）： 资源.将虚拟机分配给资源池	资源池管理员或管理员
	在目标数据存储上（如果与源数据存储不同）： 数据存储.分配空间	数据存储用户或管理员
通过 Storage vMotion 迁移虚拟机	在虚拟机或虚拟机的文件夹上： 资源.迁移已打开电源的虚拟机	资源池管理员或管理员
	在目标数据存储上： 数据存储.分配空间	数据存储用户或管理员
将主机移动到群集	在主机上： 主机.清单.将主机添加到群集	管理员
	在目标群集上： 主机.清单.将主机添加到群集	管理员

确保 ESXi 主机安全

ESXi 虚拟化管理程序架构具有许多内置安全功能，如 CPU 隔离、内存隔离和设备隔离。您可以配置锁定模式、证书替换和智能卡身份验证等其他功能以增强安全性。

ESXi 主机还受防火墙保护。您可以根据需要打开入站和出站流量的端口，但应限制对服务和端口的访问。使用 ESXi 锁定模式并限制对 ESXi Shell 的访问有助于进一步构建更加安全的环境。从 vSphere 6.0 开始，ESXi 主机将加入证书基础架构。默认情况下，主机将使用 VMware 证书颁发机构 (VMCA) 签名的证书进行置备。

有关 ESXi 安全性的其他信息，请参见 VMware 白皮书《*VMware vSphere Hypervisor 的安全性*》。

本章讨论了以下主题：

- [第 31 页](#)，“使用主机配置文件配置 ESXi 主机”
- [第 32 页](#)，“常规 ESXi 安全建议”
- [第 39 页](#)，“ESXi 主机的证书管理”
- [第 52 页](#)，“使用安全配置文件自定义主机”
- [第 64 页](#)，“为 ESXi 主机分配特权”
- [第 66 页](#)，“使用 Active Directory 管理 ESXi 用户”
- [第 68 页](#)，“使用 vSphere Authentication Proxy”
- [第 74 页](#)，“配置 ESXi 的智能卡身份验证”
- [第 75 页](#)，“使用 ESXi Shell”
- [第 79 页](#)，“ESXi 主机的 UEFI 安全引导”
- [第 81 页](#)，“ESXi 日志文件”

使用主机配置文件配置 ESXi 主机

使用主机配置文件，您可以设置 ESXi 主机的标准配置和自动化这些配置设置的合规性。使用主机配置文件，您可以控制主机配置的许多方面，其中包括内存、存储、网络等。

可以从 vSphere Web Client 中配置引用主机的主机配置文件，并将该主机配置文件应用到共享引用主机的特性的所有主机。还可以使用主机配置文件监控主机是否存在主机配置更改。请参见 *vSphere 主机配置文件* 文档。

可以将主机配置文件附加到群集以将其应用于群集中的所有主机。

步骤

- 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群集。

- 3 将引用主机的主机配置文件应用到其他主机或群集。

常规 ESXi 安全建议

为了避免 ESXi 主机遭到未经授权的入侵和误用，VMware 对几个参数、设置和活动施加了一些限制。可以根据配置需求而放宽这些限制。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。

内置的安全功能

可如下降低主机的风险：

- 默认情况下，ESXi Shell 和 SSH 处于禁用状态。
- 默认情况下，只会打开有限的防火墙端口数目。您可以明确打开与特定服务关联的额外防火墙端口。
- ESXi 仅运行管理其功能所不可或缺的服务。分发仅限于运行 ESXi 所需的功能。
- 默认情况下，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。
- 默认情况下，弱密码被禁用，来自客户端的通信将通过 SSL 进行保护。用于保护通道安全的确切算法取决于 SSL 握手。在 ESXi 上创建的默认证书会使用带有 RSA 加密的 PKCS#1 SHA-256 作为签名算法。
- ESXi 在内部使用 Tomcat 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 Tomcat 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。
- 未安装诸如 FTP 和 Telnet 之类的不安全服务，且这些服务的端口在默认情况下是关闭的。由于可以轻松使用 SSH 和 SFTP 等更为安全的服务，请避免使用这些不安全的服务，而使用更安全的替代方案。例如，如果 SSH 不可用，请避免使用带有 SSL 的 Telnet 访问虚拟串行端口，而必须使用 Telnet。

如果必须使用不安全的服务，且已为主机实施了充分的保护措施，则可以明确打开相应端口以支持这些服务。

- 考虑为 ESXi 系统使用 UEFI 安全引导。请参见第 79 页，“ESXi 主机的 UEFI 安全引导”。

其他安全措施

评估主机安全和管理时请考虑以下建议。

限制访问

如果启用对直接控制台用户界面 (DCUI)、ESXi Shell 或 SSH 的访问，请实施严格的访问安全策略。

ESXi Shell 具有访问主机的某些部分的特权。只向信任的用户提供 ESXi Shell 登录访问权限。

请勿直接访问受管主机

使用 vSphere Web Client 来管理受 vCenter Server 管理的 ESXi 主机。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。使用任一 GUI 客户端或任一 VMware CLI 或 API 管理 ESXi 主机。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。

注意 请遵循以下位置的 VMware 安全建议：<http://www.vmware.com/security/>。

使用脚本管理主机配置设置

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

vSphere 包括用于主机管理的多种脚本编制语言。有关参考信息和编程提示，请参见《vSphere 命令行文档》和《vSphere API/SDK 文档》；有关脚本式管理的其他提示，请参见 VMware 社区。vSphere 管理员文档重点介绍了如何使用 vSphere Web Client 进行管理。

vSphere PowerCLI	VMware vSphere PowerCLI 是 vSphere API 的 Windows PowerShell 接口。vSphere PowerCLI 包括用于管理 vSphere 组件的 PowerShell cmdlet。 vSphere PowerCLI 包含超过 200 个 cmdlet、一组示例脚本和用于管理和自动化的函数库。请参见《vSphere PowerCLI 文档》。
vSphere Command-Line Interface (vCLI)	vCLI 包含用于管理 ESXi 主机和虚拟机的一组命令。此安装程序还会安装 vSphere SDK for Perl，它会运行 Windows 或 Linux 系统，并将安装 ESXCLI 命令、vicfg- 命令以及一组其他 vCLI 命令。请参见《vSphere Command-Line Interface 文档》。

从 vSphere 6.0 开始，还可以对 vCloud Suite SDK（如 vCloud Suite SDK for Python）使用其中一个脚本界面。

步骤

- 1 创建具有有限特权的自定义角色。

例如，考虑创建一个角色，该角色具有一组管理主机的特权但没有管理虚拟机、存储或网络的特权。如果只要使用脚本提取信息，则可为主机创建具有只读特权的角色。
- 2 在 vSphere Web Client 中，创建服务帐户并为其分配自定义角色。

如果要严格限制对特定主机的访问权限，则可以创建具有不同访问权限级别的多个自定义角色。
- 3 编写脚本以执行参数检查或修改，然后运行脚本。

例如，您可以检查或设置主机的 shell 交互式超时，如下所示：

语言	命令
vCLI (ESXCLI)	<pre>esxcli <conn_options> system settings advanced get /UserVars/ESXiShellTimeout esxcli --formatter=csv --format-param=fields="Path,Int Value" system settings advanced list grep /UserVars/ESXiShellTimeout</pre>
PowerCLI	<pre>#List UserVars.ESXiShellInteractiveTimeout for each host Get-VMHost Select Name, @{N="UserVars.ESXiShellInteractiveTimeout";E={\$\$_ Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeout Select -ExpandProperty Value}} # Set UserVars.ESXiShellTimeout to 900 on all hosts Get-VMHost Foreach { Get-AdvancedSetting -Entity \$_ -Name UserVars.ESXiShellInteractiveTimeout Set-AdvancedSetting - Value 900 }</pre>

- 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，您需要使用符合预定义要求的密码。您可以使用 `Security.PasswordQualityControl` 高级选项更改所需长度和字符类别要求或允许密码短语。

ESXi 使用 Linux PAM 模块 `pam_passwdqc` 进行密码管理和控制。有关详细信息，请参见 `pam_passwdqc` 的手册页。

注意 ESXi 密码的默认要求因版本而异。您可以使用 `Security.PasswordQualityControl` 高级选项检查并更改默认的密码限制。

ESXi 密码

ESXi 对从直接控制台用户界面、ESXi Shell、SSH 或 VMware Host Client 进行的访问强制执行密码要求。默认情况下，创建密码时必须包括四类字符：小写字母、大写字母、数字和特殊字符（如下划线或短划线）。

注意 密码开头的大写字母不算入使用的字符类别数。密码结尾的数字不算入使用的字符类别数。

密码不能包含字典单词或部分字典单词。

ESXi 密码示例

以下候选密码说明选项设置如下时可以使用的密码。

```
retry=3 min=disabled,disabled,disabled,7,7
```

使用此设置时，不允许使用包含一种或两种类别字符的密码或不允许使用密码短语，因为前三项已禁用。使用三种和四种类别字符的密码需要 7 个字符。有关详细信息，请参见 `pam_passwdqc` 的手册页。

使用这些设置时，允许使用以下密码。

- `xQaTEhb!`：包含由三类字符组成的八个字符。
- `xQaT3#A`：包含由四类字符组成的七个字符。

下列候选密码不符合要求。

- `Xqat3hi`：以大写字母开头，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，默认情况下，密码短语处于禁用状态。您可以在 vSphere Web Client 中使用 `Security.PasswordQualityControl` 高级选项更改此默认值或其他设置。

例如，您可以将该选项更改为以下值。

```
retry=3 min=disabled,disabled,16,7,7
```

此示例允许密码短语的长度至少为 16 个字符，且至少包含 3 个单词，以空格分隔。

对于旧版主机，仍然支持更改 `/etc/pamd/passwd` 文件，但在将来的版本中将不再支持更改此文件。将来的版本将改用 `Security.PasswordQualityControl` 高级选项。

更改默认密码限制

您可以使用 ESXi 主机的 `Security.PasswordQualityControl` 高级选项更改密码或密码短语的默认限制。有关设置 ESXi 高级选项的信息，请参见 *vCenter Server 和主机管理* 文档。

例如，您可以将默认值更改为要求包含最少 15 个字符和最少 4 个字，如下所示：

```
retry=3 min=disabled,disabled,15,7,7 passphrase=4
```

有关详细信息，请参见 `pam_passwdqc` 的手册页。

注意 并非 `pam_passwdqc` 选项的所有可能的组合均已经过测试。请在更改默认密码设置后执行额外的测试。

ESXi 帐户锁定行为

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

配置登录行为

可以使用以下高级选项配置 ESXi 主机的登录行为：

- **Security.AccountLockFailures.** 在锁定用户帐户之前允许的最多失败登录尝试次数。“零”将禁用帐户锁定。
- **Security.AccountUnlockTime.** 用户被锁定的秒数。

有关设置 ESXi 高级选项的信息，请参见 *vCenter Server 和主机管理文档*。

SSH 安全

可以使用 SSH 远程登录到 ESXi Shell 并执行针对主机的故障排除任务。

ESXi 中的 SSH 配置得到了增强，能够提供较高的安全级别。

禁用第 1 版 SSH 协议 VMware 不再支持第 1 版 SSH 协议，而是以独占方式使用第 2 版协议。第 2 版消除了第 1 版中存在的某些安全问题，且提供了一个安全的方式与管理接口进行通信。

提高了密码强度 SSH 对连接仅支持 256 位和 128 位 AES 密码。

这些设置旨在为通过 SSH 传输到管理接口的数据提供可靠保护。不能更改这些设置。

ESXi SSH 密钥

可以使用 SSH 密钥限制、控制以及保护 ESXi 主机的访问权限。可以利用 SSH 密钥允许受信任的用户或脚本在不指定密码的情况下即可登录主机。

可以使用 `vifs vSphere CLI` 命令将 SSH 密钥复制到主机。有关安装和使用 vSphere CLI 命令集的信息，请参见《*vSphere Command-Line Interface 入门*》。也可以使用 `HTTPS PUT` 将 SSH 密钥复制到主机。

您无需在外部生成密钥并进行上载，而是可以在 ESXi 主机上创建密钥，然后进行下载。请参见 VMware 知识库文章 [1002866](#)。

启用 SSH 并将 SSH 密钥添加到主机具有内在的风险。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。

注意 对于 ESXi 5.0 及更早版本，即使主机处于锁定模式，具有 SSH 密钥的用户也可以访问主机。从 ESXi 5.1 开始，具有 SSH 密钥的用户无法再访问锁定模式下的主机。

使用 vifs 命令上载 SSH 密钥

如果您决定要使用授权密钥通过 SSH 登录到主机，则可以使用 `vifs` 命令上载授权密钥。

注意 由于授权密钥允许 SSH 访问而无需用户身份验证，请认真考虑是否要在环境中使用 SSH 密钥。

授权密钥允许您对主机的远程访问进行身份验证。当用户或脚本尝试通过 SSH 访问主机时，密钥提供身份验证，并且不需要密码。使用授权密钥，可以自动进行身份验证，这在编写脚本以执行例程任务时非常有用。

可以将以下类型的 SSH 密钥上传到主机。

- root 用户的授权密钥
- RSA 密钥
- RSA 公用密钥

从 vSphere 6.0 Update 2 版本开始，不再支持 DSS/DSA 密钥。

重要事项 请不要修改 `/etc/ssh/sshd_config` 文件。

步骤

- ◆ 在命令行或管理服务器中，使用 `vifs` 命令将 SSH 密钥上传到 ESXi 主机上合适的位置。

```
vifs --server hostname --username username --put filename /host/ssh_host_dsa_key_pub
```

密钥类型	位置
root 用户的授权密钥文件	/host/ssh_root_authorized_keys 您必须具有完全管理员特权才可上传此文件。
RSA 密钥	/host/ssh_host_rsa_key
RSA 公用密钥	/host/ssh_host_rsa_key_pub

使用 HTTPS PUT 上传 SSH 密钥

可以使用授权密钥通过 SSH 登录主机。可以使用 HTTPS PUT 上传授权密钥。

授权密钥允许您对主机的远程访问进行身份验证。当用户或脚本尝试通过 SSH 访问主机时，密钥提供身份验证，并且不需要密码。使用授权密钥，可以自动进行身份验证，这在编写脚本以执行例程任务时非常有用。

可以使用 HTTPS PUT 将以下类型的 SSH 密钥上传到主机：

- root 用户的授权密钥
- DSA 密钥
- DSA 公用密钥
- RSA 密钥
- RSA 公用密钥

重要事项 请不要修改 `/etc/ssh/sshd_config` 文件。

步骤

- 1 在上载应用程序中，打开密钥文件。
- 2 将文件发布到以下位置。

密钥类型	位置
root 用户的授权密钥文件	https://hostname_or_IP_address/host/ssh_root_authorized_keys 您必须对主机具有完全管理员特权才可上传此文件。
DSA 密钥	https://hostname_or_IP_address/host/ssh_host_dsa_key
DSA 公用密钥	https://hostname_or_IP_address/host/ssh_host_dsa_key_pub
RSA 密钥	https://hostname_or_IP_address/host/ssh_host_rsa_key
RSA 公用密钥	https://hostname_or_IP_address/host/ssh_host_rsa_key_pub

PCI 和 PCIe 设备和 ESXi

使用 VMware DirectPath I/O 功能将 PCI 或 PCIe 设备直通到虚拟机会导致潜在的安全漏洞。该漏洞可能会由错误代码或恶意代码触发，如客户机操作系统中以特权模式运行的设备驱动程序。行业标准硬件和固件当前无法提供足够的错误控制支持，导致 ESXi 无法完全关闭漏洞。

VMware 建议仅在虚拟机由可信实体所有和管理时，才使用 PCI 或 PCIe 直通到此虚拟机。必须确保此实体不会尝试通过虚拟机破坏或利用主机。

主机可能会因以下原因受到威胁。

- 客户机操作系统可能生成了不可恢复的 PCI 或 PCIe 错误。此类错误不会损坏数据，但是可能会导致 ESXi 主机崩溃。出现此类错误可能是由于正在直通的硬件设备中存在缺陷或不兼容，或者客户机操作系统的驱动程序存在问题。
- 客户机操作系统可能会生成直接内存访问 (DMA) 操作，此操作导致 ESXi 主机上出现 IOMMU 页面故障，例如，当 DMA 操作指向虚拟机内存的外部地址时。在一些计算机上，主机固件将 IOMMU 故障配置为通过不可屏蔽的中断 (NMI) 报告致命错误，这会导致 ESXi 主机崩溃。发生此问题可能是由于客户机操作系统的驱动程序存在问题。
- 如果 ESXi 主机上的操作系统未使用中断重新映射，客户机操作系统可能会在任意向量上向 ESXi 主机插入一个虚假中断。当前，ESXi 在可以使用中断重新映射的 Intel 平台上使用中断重新映射；中断映射是 Intel VT-d 功能集的一部分。ESXi 在 AMD 平台上不使用中断映射。虚假中断很可能会导致 ESXi 主机崩溃；但是，理论上可能存在利用这些中断的其他方式。

禁用 Managed Object Browser

Managed Object Browser (MOB) 提供了一个浏览 VMkernel 对象模型的方法。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。请仅在进行调试时使用 MOB，并确保在生产系统中禁用该功能。

从 vSphere 6.0 开始，默认情况下禁用 MOB。但是，对于某些任务（如从系统提取旧证书），必须使用 MOB。可以执行下列操作以启用和禁用 MOB。

步骤

- 1 在 vSphere Web Client 中选择主机，然后转至**高级系统设置**。
- 2 检查 `Config.HostAgent.plugins.solo.enableMob` 的值，并根据需要进行更改。

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 和存储等功能。隔离开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。此网络应仅供系统、网络和安全管理员访问。使用跳转盒或虚拟专用网络 (VPN) 安全访问管理网络。严格控制该网络中的访问。

- 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。

注意 对主机目录或身份验证机制做出任何更改之后重新启动主机进程。

- 不要设置使用密码或密码短语的证书。ESXi 不支持使用密码或密码短语（也称为加密密钥）的 Web 代理。如果设置需要密码或密码短语的 Web 代理，则 ESXi 进程将无法启动。
- 为了支持对用户名、密码和数据包进行加密，将在默认情况下针对 vSphere Web Services SDK 连接启用 SSL。如果要配置这些连接以使它们不对传输进行加密，请对 vSphere Web Services SDK 连接禁用 SSL，方法是将连接从 HTTPS 切换至 HTTP。

仅当为这些客户端创建了完全可信的环境时才可考虑禁用 SSL，在这样的环境中，安装有防火墙，而且与主机之间的传输是完全隔离的。禁用 SSL 可提高性能，因为省却了执行加密所需的开销。

- 为了防止误用 ESXi 服务，大多数内部 ESXi 服务只能通过端口 443（用于 HTTPS 传输的端口）来访问。端口 443 用作 ESXi 的反向代理。通过 HTTP 欢迎使用页面可看到 ESXi 上的服务列表，但如果未经适当授权，则不能直接访问存储适配器服务。

可对此配置进行更改，以便可通过 HTTP 连接直接访问各个服务。除非是在完全可信的环境中使用 ESXi，否则不要进行此更改。

- 在升级您的环境时，证书会保留在原地。

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）密码和用户密码进行了 MD5 加密。
 - 与配置文件关联的其他任何密码均采用明文形式。如果使用主机配置文件设置 Active Directory，则密码不受保护。

使用 vSphere Authentication 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 从远程应用程序进行硬件级别管理。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服务帐户。向在 ESXi 系统中定义的所有本地帐户以及在 vCenter Server 中定义的所有角色授予 CIM 信息的只读访问权限。

步骤

- 1 为 CIM 应用程序创建服务帐户。
- 2 向收集 CIM 信息的 ESXi 主机授予服务帐户只读权限。
- 3 （可选）如果应用程序需要写入访问权限，请创建只有两个特权的角色。
 - 主机.配置.系统管理
 - 主机.CIM.CIM 交互
- 4 针对所监控的每个 ESXi 主机，创建一个权限，将自定义角色与服务帐户配对。

请参见第 25 页，“使用角色分配特权”。

ESXi 主机的证书管理

在 vSphere 6.0 及更高版本中，默认情况下，VMware Certificate Authority (VMCA) 将使用将 VMware 作为 root 证书颁发机构的签名证书置备每个新 ESXi 主机。在主机明确或作为安装或升级到 ESXi 6.0 或更高版本的一部分添加到 vCenter Server 时，便会进行置备。

您可以通过 vSphere Web Client 以及通过在 vSphere Web Services SDK 中使用 `vim.CertificateManager` API 来查看和管理 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 5.5 和 vSphere 6.x 中的证书

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

在 vSphere 5.5 及更早版本中，只能通过组合使用用户名、密码和指纹确保 TLS/SSL 端点的安全。用户可以将对应的自签名证书替换为其自己的证书。请参见 vSphere 5.5 文档中心。

在 vSphere 6.0 及更高版本中，vCenter Server 支持 ESXi 主机的以下证书模式。

表 3-1 ESXi 主机的证书模式

证书模式	描述
VMware Certificate Authority (默认值)	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。 默认情况下，VMCA 将使用证书置备 ESXi 主机。 在此模式中，您可以从 vSphere Web Client 刷新和续订证书。
自定义证书颁发机构	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。 在此模式中，您必须管理证书。您无法从 vSphere Web Client 刷新和续订证书。 注意 除非将证书模式更改为自定义证书颁发机构，否则在 vSphere Web Client 中选择 续订 等情况下，VMCA 可能会替换自定义证书。
指纹模式	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。 除非使用其他两种模式之一时遇到无法解决的问题，否则不要使用此模式。某些 vCenter 6.x 及更高版本服务在指纹模式下可能无法正常运行。

证书过期

从 vSphere 6.0 开始，您可以在 vSphere Web Client 中查看有关由 VMCA 或第三方 CA 签名的证书的证书过期信息。您可以查看由 vCenter Server 管理的所有主机或单个主机的信息。如果证书处于**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 VMCA

从安装介质引导 ESXi 主机时，主机最初使用自动生成的证书。当主机添加到 vCenter Server 系统时，将使用 VMCA 作为 root CA 签名的证书置备主机。

该过程与使用 Auto Deploy 置备主机类似。但是，这些主机不会存储任何状态，因此签名证书将由 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。

ESXi 证书管理所需的特权

对于 ESXi 主机的证书管理，您必须具有 **证书.管理证书** 特权。可以从 vSphere Web Client 中设置该特权。

主机名称和 IP 地址更改

在 vSphere 6.0 及更高版本中，主机名称或 IP 地址更改会影响 vCenter Server 是否会将主机的证书视为有效。将主机添加到 vCenter Server 的方式将影响是否需要人工干预。人工干预是指重新连接主机或从 vCenter Server 中移除主机，然后再重新添加该主机。

表 3-2 主机名称或 IP 地址更改时需要人工干预

将主机添加到 vCenter Server 所使用的方式...	主机名称更改	IP 地址更改
主机名称	vCenter Server 连接问题。需要人工干预。	无需干预。
IP 地址	无需干预。	vCenter Server 连接问题。需要人工干预。



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

主机升级和证书

如果将 ESXi 主机升级到 ESXi 6.0 或更高版本，升级过程会将自签名（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。

如果决定不将主机升级到 ESXi 6.0 或更高版本，则主机会保留其当前使用的证书，即使主机由使用 VMCA 证书的 vCenter Server 系统管理亦如此。

建议的升级工作流程取决于当前证书。

使用指纹证书置备的主机 如果主机当前使用指纹证书，则在升级过程中会自动为其分配 VMCA 证书。

注意 无法使用 VMCA 证书置备旧版主机。必须将这些主机升级到 ESXi 6.0 或更高版本。

使用自定义证书置备的主机 如果主机使用自定义证书（通常是第三方 CA 签名的证书）置备，则这些证书在升级过程中将保留在原位。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。

注意 如果环境处于 VMCA 模式下，且您在 vSphere Web Client 中刷新证书，则任何现有证书将替换为 VMCA 签名的证书。

从今往后，vCenter Server 将在 vSphere Web Client 中监控证书并显示有关证书到期等的信息。

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 6.0 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。

请参见第 50 页，“在 Auto Deploy 中使用自定义证书”。

证书模式切换 workflow

从 vSphere 6.0 开始，默认情况下，ESXi 主机将由 VMCA 使用证书进行置备。您可以改用自定义证书模式或用于调试的旧版指纹模式。在大多数情况下，模式切换会造成破坏且没有必要。如果需要模式切换，请在开始之前检查潜在的影响。

在 vSphere 6.0 及更高版本中，vCenter Server 支持 ESXi 主机的以下证书模式。

证书模式	描述
VMware Certificate Authority (默认值)	默认情况下, VMware Certificate Authority 将作为 ESXi 主机证书的 CA。默认情况下, VMCA 为 root CA, 但可将其设置为其他 CA 的中间 CA。在此模式中, 用户可以从 vSphere Web Client 中管理证书。如果 VMCA 是辅助证书, 也将使用 VMCA。
自定义证书颁发机构	某些客户可能更愿意管理其自己的外部证书颁发机构。在此模式中, 客户负责管理证书且无法在 vSphere Web Client 中管理证书。
指纹模式	vSphere 5.5 使用指纹模式, 且此模式在 vSphere 6.0 中作为后备选项仍然可用。除非使用其他两种模式之一时遇到无法解决的问题, 否则不要使用此模式。某些 vCenter 6.0 及更高版本服务在指纹模式下可能无法正常运行。

使用自定义 ESXi 证书

如果公司策略要求使用 VMCA 以外的 root CA, 则可以在仔细规划后在您的环境中切换证书模式。建议的工作流如下:

- 1 获取要使用的证书。
- 2 移除 vCenter Server 中的所有主机。
- 3 将自定义 CA root 证书添加到 VECS (VMware Endpoint 证书存储)。
- 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。请参见第 46 页, “更改证书模式”。
- 6 将主机添加到 vCenter Server 系统。

从自定义 CA 模式切换到 VMCA 模式

如果要使用自定义 CA 模式, 且确定在您的环境中使用 VMCA 后会具有更优的性能, 则可以在仔细规划后执行模式切换。建议的工作流如下:

- 1 移除 vCenter Server 系统中的所有主机。
- 2 在 vCenter Server 系统中, 从 VECS 中移除第三方 CA 的 root 证书。
- 3 切换到 VMCA 模式。请参见第 46 页, “更改证书模式”。
- 4 将主机添加到 vCenter Server 系统。

注意 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, 请参见第 46 页, “更改证书模式”。

从指纹模式切换到 VMCA 模式

如果使用指纹模式且要开始使用 VMCA 签名证书, 则切换需要进行一些规划。建议的工作流如下:

- 1 移除 vCenter Server 系统中的所有主机。
- 2 切换到 VMCA 证书模式。请参见第 46 页, “更改证书模式”。
- 3 将主机添加到 vCenter Server 系统。

注意 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，请按照第 46 页，“更改证书模式”中的说明进行操作。模式切换之后，vCenter Server 系统将只检查证书的格式，不再检查证书本身是否有效。

从指纹模式切换到自定义 CA 模式

如果在故障排除期间将环境设置为指纹模式，且希望开始使用自定义 CA 模式，则必须首先生成所需的证书。建议的工作流如下：

- 1 移除 vCenter Server 系统中的所有主机。
- 2 将自定义 CA root 证书添加到 vCenter Server 系统上 VECS 中的 TRUSTED_ROOTS 存储区。请参见第 49 页，“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。请参见第 46 页，“更改证书模式”。
- 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 Web Client 更改许多默认设置。考虑更改组织和位置信息。请参见第 44 页，“更改证书默认设置”。

表 3-3 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.cn.daysValid

表 3-3 ESXi CSR 设置（续）

参数	默认值	高级选项
证书到期的硬阈值。达到此阈值时，vCenter Server 会发出红色警报。	30 天	vpzd.certmgmt.certs.cn.hardThreshold
vCenter Server 证书有效性检查的轮询间隔。	5 天	vpzd.certmgmt.certs.cn.pollIntervalDays
证书到期的软阈值。达到此阈值时，vCenter Server 会引发事件。	240 天	vpzd.certmgmt.certs.cn.softThreshold
vCenter Server 用户确定是否替换现有证书的模式。更改此模式以在升级过程中保留自定义证书。请参见第 41 页，“主机升级和证书”。	默认值为 vmca 您还可以指定指纹或自定义。请参见第 46 页，“更改证书模式”。	vpzd.certmgmt.mode

更改证书默认设置

当主机添加到 vCenter Server 系统时，vCenter Server 将向 VMCA 发送主机的证书签名请求 (CSR)。您可以使用 vSphere Web Client 中的 vCenter Server “高级设置” 更改 CSR 中的某些默认设置。

更改特定于公司的默认证书设置。有关默认设置的完整列表，请参见第 43 页，“ESXi 证书默认设置”。某些默认设置不能更改。

步骤

- 1 在 vSphere Web Client 中，选择管理主机的 vCenter Server 系统。
- 2 单击**配置**，然后单击**高级配置**。
- 3 在“筛选器”方框中，输入 **certmgmt** 以仅显示证书管理参数。
- 4 根据公司策略更改现有参数的值，然后单击**确定**。

下次将主机添加到 vCenter Server 时，新的设置将用于 vCenter Server 发送到 VMCA 的 CSR 以及分配给主机的证书。

下一步

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。

查看多个 ESXi 主机的证书过期信息

如果使用的是 ESXi 6.0 及更高版本，则可以查看由 vCenter Server 系统管理的所有主机的证书状态。通过该显示，您可以确定任何证书是否即将过期。

可以在 vSphere Web Client 中查看正在使用 VMCA 模式的主机和正在使用自定义模式的主机的证书状态信息。无法查看处于指纹模式中的主机的证书状态信息。

步骤

- 1 浏览到 vSphere Web Client 清单层次结构中的主机。
默认情况下，主机显示不包含查证书状态。
- 2 右键单击“名称”字段，然后选择**显示/隐藏列**。

- 3 选择**证书有效期至**，单击**确定**，并根据需要滚动到右侧。

证书信息将显示证书过期的时间。

如果将主机添加到 vCenter Server 或主机在断开连接后重新连接，则 vCenter Server 会续订状态为“已过期”、“即将过期”、“马上过期”或“快要过期”的证书。如果证书有效期少于八个月，则状态为即将过期；如果证书有效期少于两个月，则状态为马上过期；如果证书有效期少于一个月，则状态为快要过期。

- 4 （可选）取消选择其他列可更方便地查看您所关注的内容。

下一步

续订即将过期的证书。请参见第 45 页，“续订或刷新 ESXi 证书”。

查看单个 ESXi 主机的证书详细信息

对于处于 VMCA 模式或自定义模式的 ESXi 6.0 及更高版本的主机，可以从 vSphere Web Client 中查看证书详细信息。有关证书的信息对调试很有帮助。

步骤

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

您可以检查以下信息。此信息仅在单主机视图中可用。

字段	描述
主体	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。 正常 正常操作。 即将过期 证书即将过期。 不久即将过期 证书最多还剩 8 个月就将过期（默认）。 即将过期 证书最多还剩 2 个月就将过期（默认）。 已过期 证书无效，因为已过期。

续订或刷新 ESXi 证书

如果 VMCA 将证书分配给 ESXi 主机（6.0 及更高版本），则可以从 vSphere Web Client 续订这些证书。您还可以刷新与 vCenter Server 关联的 TRUSTED_ROOTS 存储中的所有证书。

如果您的证书即将过期，或者如果由于其他原因要使用新证书置备主机，则可以续订证书。如果证书已过期，则必须与主机断开连接，然后重新进行连接。

默认情况下，每次将主机添加到清单或重新连接主机时，vCenter Server 都会续订状态为“已过期”、“立即过期”或“即将过期”的主机证书。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
2 选择**配置**。

- 3 在**系统**下，单击**证书**。
可以查看有关所选主机证书的详细信息。
- 4 单击**续订**或**刷新 CA 证书**。

选项	描述
续订	从 VMCA 检索主机的全新签名证书。
刷新 CA 证书	将 vCenter Server VECS 存储的 TRUSTED_ROOTS 存储中的所有证书推送到主机。

- 5 单击**是**确认。

更改证书模式

在大多数情况下，使用 VMCA 在环境中置备 ESXi 主机是最佳解决方案。如果公司策略要求使用具有不同根 CA 的自定义证书，则可以编辑 vCenter Server 高级选项，以便在刷新证书时，不会使用 VMCA 证书自动置备主机。然后，您必须负责环境中的证书管理。

您可以使用 vCenter Server 高级设置更改为指纹模式或自定义 CA 模式。只能将指纹模式用作后备选项。

步骤

- 1 选择管理主机的 vCenter Server，然后单击**配置**。
- 2 单击**高级设置**，然后单击**编辑**。
- 3 在“筛选器”框中，输入 **certmgmt** 以仅显示证书管理密钥。
- 4 如果要管理自己的证书，请将 **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**确定**。
- 5 重新启动 vCenter Server 服务。

替换 ESXi SSL 证书和密钥

您的安全策略可能要求您在每台主机上将默认的 ESXi SSL 证书替换为第三方 CA 签名的证书。

默认情况下，vSphere 组件使用在安装过程中创建的 VMCA 签名证书和密钥。如果意外删除 VMCA 签名证书，请从其 vCenter Server 系统中移除该主机，然后再重新添加该主机。在添加主机时，vCenter Server 会请求由 VMCA 颁发的新证书，并使用该证书置备主机。

如果公司策略有相关要求，则可以将 VMCA 签名证书替换为由受信任的 CA（商业 CA 或组织 CA）颁发的证书。

默认证书位于与 vSphere 5.5 证书相同的位置。您可以通过多种方式来将默认证书替换为受信任的证书。

注意 您也可以使用 vSphere Web Services SDK 中的 **vim.CertificateManager** 和 **vim.host.CertificateManager** 受管对象。请参见 vSphere Web Services SDK 文档。

替换证书后，您必须在管理主机的 vCenter Server 系统上更新 VECS 中的 TRUSTED_ROOTS 存储，以确保 vCenter Server 和 ESXi 主机建立信任关系。

- [ESXi 证书签名请求的要求](#) 第 47 页，
如果要使用企业或第三方 CA 签名证书，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](#) 第 47 页，
可以从 ESXi Shell 替换默认的 VMCA 签名的 ESXi 证书。

- [通过 vifs 命令替换默认证书和密钥](#)第 48 页，
可以通过 `vifs` 命令替换默认的 VMCA 签名的 ESXi 证书。
- [通过 HTTPS PUT 替换默认证书](#)第 48 页，
可以使用第三方应用程序上传证书和密钥。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）](#)第 49 页，
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 位或更大（PEM 编码）
- PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。密钥添加到 VECS 后，会转换为 PKCS8
- x509 版本 3
- 对于 root 证书，CA 扩展必须设置为 `true`，并且 `cert` 签名必须在要求列表中。
- SubjectAltName 必须包含 `DNS Name=<machine_FQDN>`
- CRT 格式
- 包含以下密钥使用：数字签名、不可否认性、密钥加密
- 比当前时间早一天的开始时间
- CN（和 SubjectAltName）设置为 vCenter Server 清单中的 ESXi 主机的主机名（或 IP 地址）。

从 ESXi Shell 替换默认证书和密钥

可以从 ESXi Shell 替换默认的 VMCA 签名的 ESXi 证书。

前提条件

- 如果要使用第三方 CA 签名证书，请生成证书请求、将其发送至证书颁发机构，并将证书存储在每个 ESXi 主机上。
- 如果需要，从 vSphere Web Client 启用 ESXi Shell 或启用 SSH 流量。请参见 *vSphere 安全性* 出版物，了解有关启用对 ESXi Shell 访问的信息。
- 所有的文件传输和其他通信均通过安全 HTTPS 会话进行。用于验证会话的用户必须在主机上拥有**主机配置高级配置**特权。请参见 *vSphere 安全性* 出版物，了解有关通过角色分配特权的信息。

步骤

- 1 以管理员权限用户的身份登录 ESXi Shell，可直接从 DCUI 登录，也可从 SSH 客户端登录。
- 2 在 `/etc/vmware/ssl` 目录中，使用以下命令重命名现有证书。


```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```
- 3 将要使用的证书复制到 `/etc/vmware/ssl`。
- 4 将新证书和密钥重命名为 `rui.crt` 和 `rui.key`。

- 5 安装新证书之后重新启动主机。

或者也可以将主机置于维护模式，安装新证书，使用直接控制台用户界面 (DCUI) 重新启动管理代理，并将主机设置为退出维护模式。

下一步

更新 vCenter Server TRUSTED_ROOTS 存储。请参见 *vSphere 安全性* 出版物。

通过 vifs 命令替换默认证书和密钥

可以通过 `vifs` 命令替换默认的 VMCA 签名的 ESXi 证书。

您可以将 `vifs` 作为 vCLI 命令运行。请参见 *vSphere Command-Line Interface 入门*。

.

前提条件

- 如果要使用第三方 CA 签名证书，请生成证书请求、将其发送至证书颁发机构，并将证书存储在每个 ESXi 主机上。
- 如果需要，从 vSphere Web Client 启用 ESXi Shell 或启用 SSH 流量。请参见 *vSphere 安全性* 出版物，了解有关启用对 ESXi Shell 访问的信息。
- 所有的文件传输和其他通信均通过安全 HTTPS 会话进行。用于验证会话的用户必须在主机上拥有**主机配置.高级配置**特权。请参见 *vSphere 安全性* 出版物，了解有关通过角色分配特权的信息。

步骤

- 1 备份现有证书。
- 2 按照证书颁发机构的说明生成证书请求。
请参见第 47 页，“[ESXi 证书签名请求的要求](#)”。
- 3 如果拥有证书，请使用 `vifs` 命令通过与主机的 SSH 连接将证书上载到主机上合适的位置。

```
vifs --server hostname --username username --put rui.crt /host/ssl_cert
```

```
vifs --server hostname --username username --put rui.key /host/ssl_key
```

- 4 重新启动主机。

下一步

更新 vCenter Server TRUSTED_ROOTS 存储。请参见第 49 页，“[更新 vCenter Server TRUSTED_ROOTS 存储（自定义证书）](#)”。

通过 HTTPS PUT 替换默认证书

可以使用第三方应用程序上载证书和密钥。支持 HTTPS PUT 操作的应用程序可以与 ESXi 包含的 HTTPS 接口配合使用。

前提条件

- 如果要使用第三方 CA 签名证书，请生成证书请求、将其发送至证书颁发机构，并将证书存储在每个 ESXi 主机上。
- 如果需要，从 vSphere Web Client 启用 ESXi Shell 或启用 SSH 流量。请参见 *vSphere 安全性* 出版物，了解有关启用对 ESXi Shell 访问的信息。
- 所有的文件传输和其他通信均通过安全 HTTPS 会话进行。用于验证会话的用户必须在主机上拥有**主机配置.高级配置**特权。请参见 *vSphere 安全性* 出版物，了解有关通过角色分配特权的信息。

步骤

- 1 备份现有证书。
- 2 在上载应用程序中，如下处理每个文件：
 - a 打开文件。
 - b 将文件发布到以下位置之一。

选项	描述
证书	https://hostname/host/ssl_cert
密钥	https://hostname/host/ssl_key

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

- 3 重新启动主机。

下一步

更新 vCenter Server TRUSTED_ROOTS 存储。请参见第 49 页，“更新 vCenter Server TRUSTED_ROOTS 存储（自定义证书）”。

更新 vCenter Server TRUSTED_ROOTS 存储（自定义证书）

如果将 ESXi 主机设置为使用自定义证书，则必须在管理主机的 vCenter Server 系统上更新 TRUSTED_ROOTS 存储。

前提条件

将每台主机上的证书替换为自定义证书。

步骤

- 1 登录到管理 ESXi 主机的 vCenter Server 系统。
登录到已安装该软件的 Windows 系统，或登录到 vCenter Server Appliance shell。

- 2 运行 vecs-cli 以将新证书添加到 TRUSTED_ROOTS 存储，例如：

```
/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert /etc/vmware/ssl/custom1.crt
```

选项	描述
Linux	/usr/lib/vmware-vmafd/bin/vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert /etc/vmware/ssl/custom1.crt
Windows	C:\Program Files\VMware\vCenter Server\vmafdd\vecs-cli entry create --store TRUSTED_ROOTS --alias custom1.crt --cert c:\ssl\custom1.crt

下一步

将证书模式设置为“自定义”。如果证书模式是默认值 VMCA，且您刷新证书，则自定义证书将替换为 VMCA 签名的证书。请参见第 46 页，“更改证书模式”。

在 Auto Deploy 中使用自定义证书

默认情况下，Auto Deploy 服务器使用 VMCA 签名的证书置备每个主机。您可以将 Auto Deploy 服务器设置为使用未经 VMCA 签名的自定义证书置备所有主机。在这种情况下，Auto Deploy 服务器将成为第三方 CA 的辅助证书颁发机构。

前提条件

- 向您的 CA 请求证书。证书必须满足以下要求。
 - 密钥大小：2048 位或更大（PEM 编码）
 - PEM 格式。VMware 支持 PKCS8 和 PKCS1（RSA 密钥）。密钥添加到 VECS 后，会转换为 PKCS8
 - x509 版本 3
 - 对于 root 证书，CA 扩展必须设置为 true，并且 cert 签名必须在要求列表中。
 - SubjectAltName 必须包含 DNS Name=<machine_FQDN>
 - CRT 格式
 - 包含以下密钥使用：数字签名、不可否认性、密钥加密
 - 比当前时间早一天的开始时间
 - CN（和 SubjectAltName）设置为 vCenter Server 清单中的 ESXi 主机的主机名（或 IP 地址）。
- 将证书和密钥文件分别命名为 `rbd-ca.crt` 和 `rbd-ca.key`。

步骤

- 1 备份默认的 ESXi 证书。
该证书位于 `/etc/vmware-rbd/ssl/` 中。
- 2 在 vSphere Web Client 中，停止 Auto Deploy 服务。
 - a 选择**系统管理**，然后在**部署**下单击**系统配置**。
 - b 单击**服务**。
 - c 右键单击要停止的服务，然后选择**停止**。
- 3 在运行 Auto Deploy 服务的系统上，将 `/etc/vmware-rbd/ssl/` 中的 `rbd-ca.crt` 和 `rbd-ca.key` 替换为您的自定义证书和密钥文件。
- 4 在运行 Auto Deploy 服务的系统上，更新 VECS 中的 TRUSTED_ROOTS 存储以使用您的新证书。

选项	描述
Windows	<pre>cd C:\Program Files\VMware\vCenter Server\vmafdd\vecs- cli.exe vecs-cli entry delete --store TRUSTED_ROOTS --alias rbd_cert vecs-cli entry create --store TRUSTED_ROOTS --alias rbd_cert --cert /etc/vmware-rbd/ssl/rbd-ca.crt</pre>
Linux	<pre>cd /usr/lib/vmware-vmafd/bin/vecs-cli vecs-cli entry delete --store TRUSTED_ROOTS --alias rbd_cert vecs-cli entry create --store TRUSTED_ROOTS --alias rbd_cert --cert /etc/vmware-rbd/ssl/rbd-ca.crt</pre>

- 5 创建包含 TRUSTED_ROOTS 中内容的 `castore.pem` 文件，并将该文件放入 `/etc/vmware-rbd/ssl/` 目录中。
在自定义模式中，您必须维护此文件。
- 6 将 vCenter Server 系统的 ESXi 证书模式更改为自定义。
请参见第 46 页，“更改证书模式”。
- 7 重新启动 vCenter Server 服务，然后启动 Auto Deploy 服务。

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 服务器将使用刚刚添加到 TRUSTED_ROOTS 存储的 root 证书。

还原 ESXi 证书和密钥文件

使用 vSphere Web Services SDK 替换 ESXi 主机上的证书时，之前的证书和密钥将附加到 `.bak` 文件。通过将 `.bak` 文件中的信息移动到当前证书和密钥文件中，可以还原之前的证书。

主机证书和密钥位于 `/etc/vmware/ssl/rui.crt` 和 `/etc/vmware/ssl/rui.key` 中。使用 vSphere Web Services SDK `vim.CertificateManager` 受管对象替换主机证书和密钥时，之前的密钥和证书将附加到 `/etc/vmware/ssl/rui.bak` 文件。

注意 如果通过 HTTP PUT、vifs 或 ESXi Shell 替换证书，则现有证书不会附加到 `.bak` 文件。

步骤

- 1 在 ESXi 主机上，找到 `/etc/vmware/ssl/rui.bak` 文件。

该文件具有以下格式：

```
#
# Host private key and certificate backup from 2014-06-20 08:02:49.961
#
```

```
-----BEGIN PRIVATE KEY-----
previous key
-----END PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
previous cert
-----END CERTIFICATE-----
```

- 2 将开头为 `-----BEGIN PRIVATE KEY-----` 且结尾为 `-----END PRIVATE KEY-----` 的文本复制到 `/etc/vmware/ssl/rui.key` 文件中。
包括 `-----BEGIN PRIVATE KEY-----` 和 `-----END PRIVATE KEY-----`。
- 3 将 `-----BEGIN CERTIFICATE-----` 与 `-----END CERTIFICATE-----` 之间的文本复制到 `/etc/vmware/ssl/rui.crt` 文件中。
包括 `-----BEGIN CERTIFICATE-----` 和 `-----END CERTIFICATE-----`。
- 4 重新启动主机或将 `ssl_reset` 事件发送至使用密钥的所有服务。

```
for s in /etc/init.d/*; do $s | grep ssl_reset > /dev/null; if [ $?== 0 ]; then $s ssl_reset; fi; done
```

使用安全配置文件自定义主机

可以通过 vSphere Web Client 中提供的“安全配置文件”面板自定义大多数基本安全设置。“安全配置文件”对单台主机管理特别有用。如果要管理多台主机，请考虑使用 CLI 或 SDK 之一，并自动执行自定义。

ESXi 防火墙配置

ESXi 包括默认启用的防火墙。

安装时，ESXi 防火墙配置为阻止除主机的安全配置文件中启用的服务的流量之外的输入和输出流量。

打开防火墙端口时，应考虑不限制访问 ESXi 主机上运行的服务可能使主机遭受外部攻击及未经授权的访问。通过将 ESXi 防火墙配置为仅允许从授权网络访问来降低该风险。

注意 此防火墙还允许 Internet 控制消息协议 (ICMP) ping 及与 DHCP 和 DNS（仅 UDP）客户端的通信。

可以如下所示管理 ESXi 防火墙端口：

- 在 vSphere Web Client 中使用每个主机的安全配置文件。请参见第 52 页，“管理 ESXi 防火墙设置”
- 从命令行或在脚本中使用 ESXCLI 命令。请参见第 56 页，“ESXi ESXCLI 防火墙命令”。
- 如果安全配置文件中不包括要打开的端口，则使用自定义 VIB。

可以使用 VMware Lab 提供的 vibauthor 工具创建自定义 VIB。要安装自定义 VIB，必须将 ESXi 主机的接受程度改为 CommunitySupported。请参见 VMware 知识库文章 [2007381](#)。

注意 如果请求 VMware 技术支持调查安装了 CommunitySupported VIB 的 ESXi 主机上的问题，VMware 支持可能会在故障排除过程中请求卸载此 CommunitySupported VIB 作为故障排除步骤，以确定该 VIB 是否与调查的问题相关。



ESXi 防火墙概念 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_esxi_firewall_concepts)

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，请参见第 55 页，“NFS 客户端防火墙行为”。

管理 ESXi 防火墙设置

可以通过 vSphere Web Client 或在命令行中为服务或管理代理配置入站和出站防火墙连接。

注意 如果不同的服务具有重叠的端口规则，则启用一项服务可能会隐式启用其他服务。为了避免此问题，可以指定允许哪些 IP 地址访问主机上的各个服务。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 单击**配置**。
- 3 在“系统”下，单击**安全配置文件**。

vSphere Web Client 将显示相应防火墙端口的活动入站和出站连接列表。

- 4 在“防火墙”部分中，单击**编辑**。

屏幕将显示防火墙规则集，其中包括规则的名称和相关信息。

- 5 选择要启用的规则集，或取消选择要禁用的规则集。

列	描述
入站端口和出站端口	vSphere Web Client 为服务打开的端口
协议	服务使用的协议。
守护进程	与服务关联的守护进程的状态

- 6 对于某些服务，可以管理服务详细信息。
- 使用**启动**、**停止**或**重新启动**按钮可临时更改服务的状态。
 - 更改“启动策略”让服务根据主机或端口使用情况启动。
- 7 对于某些服务，可以明确指定允许连接的 IP 地址。
- 请参见第 53 页，“为 ESXi 主机添加允许的 IP 地址”。
- 8 单击**确定**。

为 ESXi 主机添加允许的 IP 地址

默认情况下，可以通过每个服务的防火墙访问所有 IP 地址。要限制流量，请更改每个服务，以便仅允许来自管理子网的流量。如果您的环境不使用某些服务，也可以取消选择这些服务。

可以使用 vSphere Web Client、vCLI 或 PowerCLI 更新服务的允许的 IP 列表。默认情况下，服务允许所有 IP 地址。



将允许的 IP 地址添加到 ESXi 防火墙
(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_adding_allowed_IP_to_esxi_firewall)

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 单击**配置**。
- 3 在“系统”下，单击**安全配置文件**。
- 4 在“防火墙”部分中，单击**编辑**，然后从列表中选择服务。
- 5 在“允许的 IP 地址”部分中，取消选择**允许从任何 IP 地址连接**，然后输入允许连接到主机的网络的 IP 地址。

使用逗号分隔 IP 地址。可以使用以下地址格式：

- 192.168.0.0/24
- 192.168.1.2, 2001::1/64
- fd3e:29a6:0a81:e478::/64

- 6 单击**确定**。

ESXi 主机的入站和出站防火墙端口

通过 vSphere Web Client 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。

下表列出了为通常所安装的服务配置的防火墙。如果在主机上安装其他 VIB，则可能还会配置其他服务和防火墙端口。这些信息主要用于 vSphere Web Client 中显示的服务，但是该表还包括其他某些端口。

表 3-4 入站防火墙连接

端口	协议	服务	描述
5988	TCP	CIM 服务器	适用于 CIM（公用信息模型）的服务器。
5989	TCP	CIM 安全服务器	适用于 CIM 的安全服务器。
427	TCP、UDP	CIM SLP	CIM 客户端使用服务位置协议版本 2 (SLPv2) 查找 CIM 服务器。
546		DHCPv6	IPv6 的 DHCP 客户端。
8301, 8302	UDP	DVSSync	DVSSync 端口可用于同步已启用 VMware FT 记录/重放的主机之间的分布式虚拟端口的状况。只有运行主虚拟机或备份虚拟机的主机才须打开这些端口。未使用 VMware FT 的主机无需打开这些端口。
902	TCP	NFC	网络文件复制 (NFC) 可为 vSphere 组件提供文件类型感知 FTP 服务。默认情况下，ESXi 将 NFC 用于在数据存储之间复制和移动数据等操作。
12345, 23451	UDP	Virtual SAN 群集服务	Virtual SAN 群集监控和成员资格目录服务。使用基于 UDP 的 IP 多播可建立群集成员并向所有群集成员分发 Virtual SAN 元数据。如果禁用，则 Virtual SAN 无法工作。
68	UDP	DHCP 客户端	IPv4 的 DHCP 客户端。
53	UDP	DNS 客户端	DNS 客户端。
8200, 8100, 8300	TCP、UDP	Fault Tolerance	主机之间的流量，用于 vSphere Fault Tolerance (FT)。
6999	UDP	NSX 分布式逻辑路由器服务	NSX 虚拟分布式路由器服务。如果已安装 NSX VIB 且已创建 VDR 模块，则与此服务关联的防火墙端口将打开。如果没有 VDR 实例与主机关联，则该端口无需打开。此服务在此产品的早期版本中称为“NSX 分布式逻辑路由器”。
2233	TCP	Virtual SAN 传输	Virtual SAN 可靠数据报传输。使用 TCP，并用于 Virtual SAN 存储 IO。如果禁用，则 Virtual SAN 无法工作。
161	UDP	SNMP 服务器	允许主机连接到 SNMP 服务器。
22	TCP	SSH 服务器	SSH 访问时为必需项。
8000	TCP	vMotion	使用 vMotion 迁移虚拟机时为必需项。ESXi 主机在端口 8000 上侦听远程 ESXi 主机中用于 vMotion 流量的 TCP 连接。
902, 443	TCP	vSphere Web Client	客户端连接
8080	TCP	vsanvp	VSAN VASA 供应商提供程序。由 vCenter 中的存储管理服务 (SMS) 使用，以访问有关 Virtual SAN 存储配置文件、功能和合规性的信息。如果禁用，则 Virtual SAN 基于存储配置文件的管理 (SPBM) 无法工作。
80	TCP	vSphere Web Access	“欢迎使用”页面，包含不同界面的下载链接。
5900-5964	TCP	RFB 协议	
80, 9000	TCP	vSphere Update Manager	

表 3-5 出站防火墙连接

端口	协议	服务	描述
427	TCP、UDP	CIM SLP	CIM 客户端使用服务位置协议版本 2 (SLPv2) 查找 CIM 服务器。
547	TCP、UDP	DHCPv6	IPv6 的 DHCP 客户端。

表 3-5 出站防火墙连接（续）

端口	协议	服务	描述
8301, 8302	UDP	DVSSync	DVSSync 端口可用于同步已启用 VMware FT 记录/重放的主机之间的分布式虚拟端口的状况。只有运行主虚拟机或备份虚拟机的主机才须打开这些端口。未使用 VMware FT 的主机无需打开这些端口。
44046, 31031	TCP	HBR	用于 vSphere Replication 和 VMware Site Recovery Manager 的持续复制流量。
902	TCP	NFC	网络文件复制 (NFC) 可为 vSphere 组件提供文件类型感知 FTP 服务。默认情况下，ESXi 将 NFC 用于在数据存储之间复制和移动数据等操作。
9	UDP	WOL	由 Wake on LAN 使用。
12345 23451	UDP	Virtual SAN 群集服务	由 Virtual SAN 使用的群集监控、成员资格和目录服务。
68	UDP	DHCP 客户端	DHCP 客户端。
53	TCP、UDP	DNS 客户端	DNS 客户端。
80, 8200, 8100, 8300	TCP、UDP	Fault Tolerance	支持 VMware Fault Tolerance。
3260	TCP	软件 iSCSI 客户端	支持软件 iSCSI。
6999	UDP	NSX 分布式逻辑路由器服务	如果已安装 NSX VIB 且已创建 VDR 模块，则与此服务关联的防火墙端口将打开。如果没有 VDR 实例与主机关联，则该端口无需打开。
5671	TCP	rabbitmqproxy	在 ESXi 主机上运行的代理，允许虚拟机内部运行的应用程序与 vCenter 网络域中运行的 AMQP 代理进行通信。虚拟机不必位于网络中，即无需网卡。代理将连接到 vCenter 网络域中的代理。因此，出站连接 IP 地址应至少包括当前正在使用的代理或未来的代理。如果客户要扩展，则可以添加代理。
2233	TCP	Virtual SAN 传输	用于 Virtual SAN 节点之间的 RDT 流量（单播点对点通信）。
8000	TCP	vMotion	使用 vMotion 迁移虚拟机时为必需项。
902	UDP	VMware vCenter Agent	vCenter Server 代理。
8080	TCP	vsanvp	用于 Virtual SAN 供应商提供程序流量。
9080	TCP	I/O 筛选器服务	用于 I/O 筛选器存储功能

表 3-6 默认情况下 UI 中不显示的服务的防火墙端口

端口	协议	服务	备注
5900-5964	TCP	RFB 协议	RFB 协议是一种用于远程访问图形用户界面的简单协议。
8889	TCP	OpenWSMAN 守护进程	Web 服务管理（WS 管理）是一种用于管理服务器、设备、应用程序和 Web 服务的 DMTF 开放式标准。

NFS 客户端防火墙行为

NFS 客户端防火墙规则集的行为方式与其他 ESXi 防火墙规则集不同。挂载或卸载 NFS 数据存储时，ESXi 将配置 NFS 客户端设置。对于不同版本的 NFS，行为有所不同。

添加、挂载或卸载 NFS 数据存储时，产生的行为取决于 NFS 版本。

NFS v3 防火墙行为

添加或挂载 NFS v3 数据存储时，ESXi 将检查 NFS 客户端 (nfsClient) 防火墙规则集的状态。

- 如果禁用了 nfsClient 规则集，则 ESXi 将启用规则集，并通过将 allowedAll 标记设置为 FALSE 来禁用“允许所有 IP 地址”策略。NFS 服务器的 IP 地址将会添加到允许的出站 IP 地址的列表中。
- 如果启用了 nfsClient 规则集，则规则集状态和允许的 IP 地址策略将不会更改。NFS 服务器的 IP 地址将会添加到允许的出站 IP 地址的列表中。

注意 如果手动启用 nfsClient 规则集或手动设置“允许所有 IP 地址”策略，则将 NFS v3 数据存储添加到系统之前或之后，卸载最新 NFS v3 数据存储时将替代您的设置。卸载所有 NFS v3 数据存储时，将禁用 nfsClient 规则集。

移除或卸载 NFS v3 数据存储时，ESXi 会执行以下操作之一。

- 如果未从已卸载数据存储的服务器挂载任何剩余的 NFS v3 数据存储，则 ESXi 将从出站 IP 地址列表中移除该服务器的 IP 地址。
- 如果执行卸载操作后没有剩余任何挂载的 NFS v3 数据存储，则 ESXi 将禁用 nfsClient 防火墙规则集。

NFS v4.1 防火墙行为

挂载第一个 NFS v4.1 数据存储时，ESXi 将启用 nfs41client 规则集并将其 allowedAll 标记设置为 TRUE。此操作将打开所有 IP 地址的端口 2049。卸载 NFS v4.1 数据存储不会影响防火墙状态。也就是说，第一个 NFS v4.1 挂载将打开端口 2049，除非明确关闭该端口，否则该端口将保持启用状态。

ESXi ESXCLI 防火墙命令

如果环境包含多个 ESXi 主机，则建议使用 ESXCLI 命令或 vSphere Web Services SDK 自动化防火墙配置。

可以使用 ESXi Shell 或 vSphere CLI 命令在命令行处配置 ESXi 以自动化防火墙配置。有关介绍，请参见 *vSphere Command-Line Interface 入门*；有关使用 ESXCLI 操作防火墙和防火墙规则的示例，请参见《*vSphere 命令行界面概念和示例*》。

表 3-7 防火墙命令

命令	描述
esxcli network firewall get	返回防火墙的启用或禁用状态，并列出默认操作。
esxcli network firewall set --default-action	设置为 true 可设置要传递的默认操作；设置为 false 可设置要丢弃的默认操作。
esxcli network firewall set --enabled	启用或禁用 ESXi 防火墙。
esxcli network firewall load	加载防火墙模块和规则集配置文件。
esxcli network firewall refresh	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。
esxcli network firewall unload	破坏过滤器并卸载防火墙模块。
esxcli network firewall ruleset list	列出规则集信息。
esxcli network firewall ruleset set --allowed-all	设置为 true 可允许对所有 IP 具有完全访问权限；设置为 false 可使用允许的 IP 地址的列表。
esxcli network firewall ruleset set --enabled --ruleset-id=<string>	将 enabled 设置为 true 或 false 可启用或禁用指定的规则集。
esxcli network firewall ruleset allowedip list	列出指定规则集允许的 IP 地址。
esxcli network firewall ruleset allowedip add	允许从指定的 IP 地址或 IP 地址范围访问规则集。

表 3-7 防火墙命令（续）

命令	描述
<code>esxcli network firewall ruleset allowedip remove</code>	从指定的 IP 地址或 IP 地址范围移除对规则集的访问。
<code>esxcli network firewall ruleset rule list</code>	列出防火墙中的每个规则集的规则。

从安全配置文件自定义 ESXi 服务

ESXi 主机包含默认情况下处于运行状态的多项服务。您可以通过安全配置文件禁用或启用服务（如果公司策略允许）。

第 76 页，“使用 vSphere Web Client 启用对 ESXi Shell 的访问”是如何启用某项服务的示例。

注意 启用服务会影响主机的安全性。除非绝对必要，否则不要启用服务。

可用服务取决于 ESXi 主机上安装的 VIB。如果未安装 VIB，则无法添加服务。某些 VMware 产品（例如 vSphere HA）会在主机上安装 VIB，并使服务和相应的防火墙端口可用。

在默认安装中，可以在 vSphere Web Client 中修改以下服务的状态。

表 3-8 安全配置文件中的 ESXi 服务

服务	默认	描述
直接控制台 UI	正在运行	通过直接控制台用户界面 (DCUI) 服务，您可以使用基于文本的菜单从本地控制台主机与 ESXi 主机进行交互。
ESXi Shell	已停止	ESXi Shell 可在直接控制台用户界面中使用，并包含一组完全受支持的命令和一组用于故障排除和修复的命令。必须从每个系统的直接控制台启用对 ESXi Shell 的访问。可以启用对本地 ESXi Shell 的访问或对 ESXi Shell 和 SSH 的访问。
SSH	已停止	允许通过安全 Shell 进行远程连接的主机的 SSH 客户端服务。
基于负载的绑定守护进程	正在运行	基于负载的绑定。
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	当主机上启用智能卡身份验证时，该服务启动。请参见第 74 页，“配置 ESXi 的智能卡身份验证”。
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 <i>vSphere 监控和性能</i> 。
Syslog 服务器	已停止	Syslog 守护进程。可以在 vSphere Web Client 的“高级系统设置”中启用 syslog。请参见 <i>vSphere 安装和设置</i> 。
VMware vCenter Agent	正在运行	vCenter Server 代理。允许 vCenter Server 连接到 ESXi 主机。具体来说，vpxa 是与 ESXi 内核通信的主机守护进程的通信媒介。
X.Org 服务器	已停止	X.Org 服务器。此可选功能在内部用于虚拟机的 3D 图形。

在安全配置文件中启用或禁用服务

您可以从 vSphere Web Client 启用和禁用“安全配置文件”中列出的服务之一。

安装完成后，默认情况下某些服务处于运行状态，而其他服务为停止状态。在某些情况下，需要先进行其他设置，然后才能在 vSphere Web Client UI 中使用某项服务。例如，NTP 服务是获取准确时间信息的一种方式，但此服务只能在防火墙中打开所需端口的情况下运作。

前提条件

使用 vSphere Web Client 连接到 vCenter Server。

步骤

- 1 在 vSphere Web Client 清单中浏览到某个主机，然后选择该主机。
- 2 单击**配置**。
- 3 在“系统”下，选择**安全配置文件**，然后单击**编辑**。
- 4 滚动到要更改的服务。
- 5 在“服务详细信息”窗格中，选择**启动**、**停止**或**重新启动**以对主机状态进行一次性更改，或从**启动策略**菜单中进行选择，以更改重新引导过程中主机的状态。
 - **如果任何端口打开则自动启动，如果所有端口关闭则停止：**这些服务的默认设置。如果任何端口打开，则客户端会尝试联系服务的网络资源。如果某些端口已打开，但特定服务的端口已关闭，则该尝试将失败。当适用的出站端口打开时，此服务将开始完成其启动。
 - **与主机一起启动和停止：**主机启动后随即启动服务，主机关闭前不久关闭服务。此选项与**如果任何端口打开则自动启动，如果所有端口关闭则停止**非常相似，都意味着此服务定期尝试完成其任务（例如尝试连接指定的 NTP 服务器）。如果端口先是处于关闭状态，但随后又打开了，客户端将在此后不久开始完成其任务。
 - **手动启动和停止：**无论端口打开与否，主机都会保留用户指定的服务设置。当用户启动 NTP 服务后，只要主机仍然开启，该服务会一直运行。如果服务已启动且主机已关闭，该服务将在关机过程中停止，但是，主机一启动，该服务将再次启动，保留用户确定的状况。

注意 这些设置仅适用于通过 vSphere Web Client 配置的服务设置或使用 vSphere Web Services SDK 创建的应用程序。通过其他方式（例如通过 ESXi Shell 或配置文件）进行的配置不会受这些设置的影响。

锁定模式

要提高 ESXi 主机的安全性，可以将其置于锁定模式。在锁定模式下，默认情况下，操作必须通过 vCenter Server 执行。

从 vSphere 6.0 开始，您可以选择正常锁定模式或严格锁定模式，这两种模式可提供不同的锁定程度。vSphere 6.0 还引入了“例外用户”列表。主机进入锁定模式时，例外用户不会丢失其特权。使用“例外用户”列表可添加在主机处于锁定模式时需要直接访问主机的第三方解决方案和外部应用程序帐户。请参见第 63 页，“指定锁定模式异常用户”。



vSphere 6 中的锁定模式 (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_lockdown_mode_vsphere)

正常锁定模式和严格锁定模式

从 vSphere 6.0 开始，您可以选择正常锁定模式或严格锁定模式，这两种模式可提供不同的锁定程度。

正常锁定模式

在正常锁定模式下，DCUI 服务未停止。如果与 vCenter Server 系统的连接断开且无法再通过 vSphere Web Client 进行访问，则特权帐户可以登录到 ESXi 主机的直接控制台界面并退出锁定模式。只有以下帐户可以访问直接控制台用户界面：

- 锁定模式下“例外用户”列表中对主机具有管理员特权的帐户。“例外用户”列表针对用于执行非常特殊的任务的服务帐户提供。将 ESXi 管理员添加到此列表违背了锁定模式的初衷。
- 在主机的 DCUI.Access 高级选项中定义的用户。此选项用于在与 vCenter Server 的连接断开时紧急访问直接控制台界面。这些用户不需要拥有对主机的管理特权。

严格的锁定模式

在严格锁定模式（该模式是 vSphere 6.0 中的新功能）下，DCUI 服务已停止。如果与 vCenter Server 的连接断开且 vSphere Web Client 不再可用，则 ESXi 主机将变为不可用，除非启用 ESXi Shell 和 SSH 服务并定义例外用户。如果无法恢复与 vCenter Server 系统的连接，则必须重新安装主机。

锁定模式及 ESXi Shell 和 SSH 服务

严格锁定模式会停止 DCUI 服务。但是，ESXi Shell 和 SSH 服务不受锁定模式影响。要使锁定模式成为有效的安全措施，请确保 ESXi Shell 和 SSH 服务也处于禁用状态。默认情况下，这些服务处于禁用状态。

在主机处于锁定模式下时，如果“例外用户”列表中的用户拥有对主机的管理员角色，则可以从 ESXi Shell 及通过 SSH 访问主机。即使在严格锁定模式下也可以进行此访问。保留 ESXi Shell 服务和 SSH 服务禁用状态是最安全的选项。

注意 “例外用户”列表针对用于执行特定任务（例如主机备份）的服务帐户提供，而非针对管理员提供。将管理员用户添加到“例外用户”列表违背了锁定模式的初衷。

启用和禁用锁定模式

特权用户可以通过多种方式启用锁定模式：

- 使用添加主机向导将主机添加到 vCenter Server 系统时。
- 使用 vSphere Web Client。请参见第 61 页，“使用 vSphere Web Client 启用锁定模式”。您可以从 vSphere Web Client 中启用正常锁定模式和严格锁定模式。
- 使用直接控制台用户界面 (DCUI)。请参见第 62 页，“从直接控制台用户界面启用或禁用正常锁定模式”。

特权用户可从 vSphere Web Client 中禁用锁定模式。这些用户可以从直接控制台界面禁用正常锁定模式，但无法从直接控制台界面禁用严格锁定模式。

注意 如果使用直接控制台用户界面启用或禁用锁定模式，则主机上用户和组的权限都将丢失。要保留这些权限，可以使用 vSphere Web Client 启用和禁用锁定模式。

锁定模式行为

在锁定模式下，一些服务会被禁用，一些服务只允许特定用户访问。

面向不同用户的锁定模式服务

当主机正在运行时，可用服务取决于锁定模式是否启用以及锁定模式的类型。

- 在严格锁定模式和正常锁定模式下，特权用户可以通过 vCenter Server 或通过 vSphere Web Client 或使用 vSphere Web Services SDK 访问主机。
- 严格锁定模式和正常锁定模式下的直接控制台界面行为有所不同。
 - 在严格锁定模式下，直接控制台用户界面 (DCUI) 服务处于禁用状态。
 - 在正常锁定模式下，异常用户列表中具有管理员特权的帐户和 DCUI.Access 高级系统设置中指定的用户可以访问直接控制台界面。
- 如果已启用 ESXi Shell 或 SSH 且将主机置于严格锁定模式或正常锁定模式，则异常用户列表中具有管理员特权的帐户可以使用这些服务。对于所有其他用户，ESXi Shell 或 SSH 访问处于禁用状态。从 vSphere 6.0 开始，不具备管理员特权的用户的 ESXi 或 SSH 会话将终止。

严格锁定模式和正常锁定模式下的所有访问均会记入日志。

表 3-9 锁定模式行为

服务	正常模式	正常锁定模式	严格的锁定模式
vSphere Web Services API	所有用户，基于权限	vCenter (vpxuser) 异常用户，基于权限 vCloud Director (vsiauser, 如果可用)	vCenter (vpxuser) 异常用户，基于权限 vCloud Director (vsiauser, 如果可用)
CIM 提供程序	具有主机管理员特权的用户	vCenter (vpxuser) 异常用户，基于权限。 vCloud Director (vsiauser, 如果可用)	vCenter (vpxuser) 异常，基于权限。 vCloud Director (vsiauser, 如果可用)
直接控制台 UI (DCUI)	具有主机管理员特权的用户和 DCUI.Access 高级选项中指定的用户	DCUI.Access 高级选项中定义的用户 具有主机管理员特权的异常用户	DCUI 服务停止
ESXi Shell (如果已启用)	具有主机管理员特权的用户	DCUI.Access 高级选项中定义的用户 具有主机管理员特权的异常用户	DCUI.Access 高级选项中定义的用户 具有主机管理员特权的异常用户
SSH (如果已启用)	具有主机管理员特权的用户	DCUI.Access 高级选项中定义的用户 具有主机管理员特权的异常用户	DCUI.Access 高级选项中定义的用户 具有主机管理员特权的异常用户

启用锁定模式时登录到 ESXi Shell 的用户

在启用锁定模式之前，如果用户已登录 ESXi Shell 或通过 SSH 访问主机，则异常用户列表中具有主机管理员特权的用户仍保持登录状态。从 vSphere 6.0 开始，所有其他用户的该会话将终止。在正常锁定模式和严格锁定模式下均适用。

使用 vSphere Web Client 启用锁定模式

启用锁定模式以要求所有配置更改都通过 vCenter Server 进行。vSphere 6.0 及更高版本支持正常锁定模式和严格锁定模式。

要完全禁用对主机的所有直接访问，可以选择严格锁定模式。启用严格锁定模式后，如果 vCenter Server 不可用，并且 SSH 和 ESXi Shell 处于禁用状态，用户将无法访问主机。请参见第 60 页，“锁定模式行为”。

步骤

- 1 在 vSphere Web 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。如果启用了 SSH 或 ESXi Shell，则可以访问。
严格	只能通过 vCenter Server 访问主机。如果启用了 SSH 或 ESXi Shell，DCUI.Access 高级选项中的帐户以及具有管理员特权的“异常用户”帐户的正在运行的会话仍处于启用状态。所有其他会话将终止。

- 6 单击**确定**。

使用 vSphere Web Client 禁用锁定模式

禁用锁定模式可允许配置更改通过直接连接传递到 ESXi 主机。保留锁定模式处于启用状态可增强环境的安全性。

在 vSphere 6.0 中，可以按如下所示禁用锁定模式：

从 vSphere Web Client 中 用户可以从 vSphere Web Client 中禁用正常锁定模式和严格锁定模式。

从直接控制台用户界面 能够在 ESXi 主机上访问直接控制台用户界面的用户可以禁用正常锁定模式。在严格锁定模式下，直接控制台界面服务已停止。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 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**无**以禁用锁定模式。

系统将退出锁定模式，vCenter Server 将显示一条警报，并向审核日志中添加一个条目。

从直接控制台用户界面启用或禁用正常锁定模式

可以从直接控制台用户界面 (DCUI) 启用和禁用正常锁定模式。只能从 vSphere Web Client 启用和禁用严格锁定模式。

主机处于正常锁定模式时，以下帐户可以访问直接控制台用户界面：

- “异常用户”列表中对主机具有管理员特权的帐户。“异常用户”列表针对服务帐户（例如备份代理）提供。
- 在主机的 DCUI.Access 高级选项中定义的用户。此选项可在出现灾难性故障时用于启用访问权限。

在 ESXi 6.0 及更高版本中，用户权限在您从直接控制台界面启用锁定模式时预留，在您禁用锁定模式时还原。

注意 如果您在未退出锁定模式的情况下将处于锁定模式的主机升级到 ESXi 6.0，并且在升级后退出锁定模式，则在进入锁定模式之前定义的所有权限将丢失。系统会将管理员角色分配给在 DCUI.Access 高级选项中找到的所有用户，以保证主机仍可访问。

要保留权限，请在升级之前从 vSphere Web Client 禁用主机的锁定模式。

步骤

- 1 在主机的直接控制台用户界面上，按 F2 并登录。
- 2 滚动至**配置锁定模式**设置并按 Enter 切换当前设置。
- 3 按 Esc 直到返回到直接控制台用户界面的主菜单。

指定在锁定模式下拥有访问特权的帐户

您可以指定能够直接访问 ESXi 主机的服务帐户，方法是将这些帐户添加到“异常用户”列表。如果出现灾难性 vCenter Server 故障，您可以指定能够访问 ESXi 主机的单个用户。

启用锁定模式后不同的帐户默认能够执行的操作以及如何更改默认行为取决于 vSphere 环境的版本。

- 在 vSphere 5.1 之前的 vSphere 版本中，只有 root 用户能够在锁定模式下的 ESXi 主机上登录到直接控制台用户界面。
- 在 vSphere 5.1 及更高版本中，您可以将用户添加到每个主机的 DCUI.Access 高级系统设置中。该选项在出现灾难性 vCenter Server 故障时使用，拥有此访问权限的用户的密码通常锁入保险箱内。DCUI.Access 列表中的用户不需要拥有对主机的完全管理特权。
- 在 vSphere 6.0 及更高版本中，仍支持 DCUI.Access 高级系统设置。此外，vSphere 6.0 及更高版本还支持“异常用户”列表，该列表面向必须直接登录主机的服务帐户提供。“异常用户”列表中拥有管理员特权的帐户可以登录 ESXi Shell。此外，这些用户还可以在正常锁定模式下登录主机的 DCUI，并且能够退出锁定模式。

请从 vSphere Web Client 指定异常用户。

注意 异常用户是指具有在本地为 ESXi 主机定义的特权的主机本地用户或 Active Directory 用户。当主机处于锁定模式时，作为 Active Directory 组成员的用户会丢失其权限。

将用户添加到 DCUI.Access 高级选项

如果您无法从 vCenter Server 访问主机，DCUI.Access 高级选项的主要用途是允许您在出现灾难性故障时退出锁定模式。可以通过从 vSphere Web Client 编辑主机的“高级设置”向列表中添加用户。

注意 无论具有何种特权，DCUI.Access 列表中的用户都可以更改锁定模式设置。这会影响到主机的安全性。对于需要直接访问主机的服务帐户，请考虑改为将用户添加到“例外用户”列表中。例外用户只能执行自己有权执行的任务。请参见第 63 页，“指定锁定模式异常用户”。

步骤

1 在 vSphere Web Client 对象导航器中，浏览到主机。

2 单击**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 用户并指定帐户以增强可审核性。

6 单击**确定**。

指定锁定模式异常用户

在 vSphere 6.0 及更高版本中，您可以从 vSphere Web Client 将用户添加到“异常用户”列表。主机进入锁定模式时，这些用户不会丢失其权限。将备份代理等服务帐户添加到“异常用户”列表是有意义的。

主机进入锁定模式时，异常用户不会丢失其特权。这些帐户通常表示需要在锁定模式下继续运行的第三方解决方案和外部应用程序。

注意 “异常用户”列表针对用于执行非常特殊的任务的服务帐户提供，而非针对管理员提供。将管理员用户添加到“异常用户”列表违背了锁定模式的初衷。

异常用户是指具有在本地为 ESXi 主机定义的特权的主机本地用户或 Active Directory 用户。他们不是 Active Directory 组的成员，也不是 vCenter Server 用户。根据其权限，不允许这些用户在主机上执行操作。例如，这意味着只读用户无法在主机上禁用锁定模式。

步骤

1 在 vSphere Web Client 清单中，浏览到主机。

2 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**异常用户**，然后单击加号图标以添加异常用户。

管理主机和 VIB 的接受级别

VIB 的接受级别由该 VIB 的证书数量决定。主机的接受级别由最低 VIB 接受级别决定。如果您要允许较低接受级别的 VIB，您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。

该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（由社区支持的）VIB。

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

支持以下接受级别。

VMwareCertified	VMwareCertified 接受程度具有最严格的要求。此程度的 VIB 能够完全通过全面测试，该测试等效于相同技术的 VMware 内部质量保证测试。现在，只有 IOVP 驱动程序是以此程度发布的。VMware 受理此接受程度的 VIB 的支持致电。
VMwareAccepted	此接受程度的 VIB 通过验证测试，但是这些测试并未对软件的每个功能都进行全面测试。合作伙伴运行测试，VMware 验证结果。现在，以此程度发布的 VIB 包括 CIM 提供程序和 PSA 插件。VMware 将此接受程度的 VIB 支持致电转交给合作伙伴的支持组织。
PartnerSupported	接受程度为 PartnerSupported 的 VIB 是由 VMware 信任的合作伙伴发布的。合作伙伴执行所有测试。VMware 不验证结果。合作伙伴想要在 VMware 系统中启用的新的或非主流的技术将使用此程度。现在，驱动程序 VIB 技术（例如 Infiniband、ATAoE 和 SSD）处于此程度，且具有非标准的硬件驱动程序。VMware 将此接受程度的 VIB 支持致电转交给合作伙伴的支持组织。
CommunitySupported	CommunitySupported 接受程度用于由 VMware 合作伙伴程序外部的个人或公司创建的 VIB。此程度的 VIB 尚未通过任何 VMware 批准的测试程序，且不受 VMware 技术支持或 VMware 合作伙伴的支持。

步骤

- 1 连接至每个 ESXi 主机并通过运行以下命令确认已将接受级别设置为由 VMware 认证、由 VMware 接受或由合作伙伴支持。
`esxcli software acceptance get`
- 2 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`
- 3 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`
- 4 通过运行以下命令更改主机的接受级别。
`esxcli software acceptance set --level acceptance_level`

为 ESXi 主机分配特权

在大多数情况下，通过为 vCenter Server 系统管理的 ESXi 主机对象分配权限，可向用户授予特权。如果使用的是独立 ESXi 主机，则可以直接分配特权。

为 vCenter Server 管理的 ESXi 主机分配权限

如果 ESXi 主机由 vCenter Server 管理，请通过 vSphere Web Client 执行管理任务。

您可以在 vCenter Server 对象层次结构中选择 ESXi 主机对象，并将管理员角色分配给有限的几个用户，使其能够直接管理 ESXi 主机。请参见第 25 页，“使用角色分配特权”。

最佳做法是至少创建一个指定用户帐户，并为其分配对主机的完全管理特权，然后使用该帐户，而不是 root 帐户。为 root 帐户设置一个高度复杂的密码，并限制 root 帐户的使用。不要移除 root 帐户。

为独立的 ESXi 主机分配权限

如果您的环境不包含 vCenter Server 系统，则会预定义以下用户。

- root 用户。请参见第 65 页，“root 用户特权”。
- vpxuser。请参见第 65 页，“vpxuser 特权”。
- dcui 用户。请参见第 66 页，“dcui 用户特权”。

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。

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。

从 vSphere 6.0 开始，您可以使用 ESXCLI 帐户管理命令管理 ESXi 本地用户帐户。您可以使用 ESXCLI 权限管理命令设置或移除对 Active Directory 帐户（用户和组）及对 ESXi 本地帐户（仅限用户）的权限。

注意 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。

root 用户特权

默认情况下，每个 ESXi 主机都有一个具有管理员角色的 root 用户帐户。该 root 用户帐户可用于本地管理，并可用于将主机连接到 vCenter Server。

此公共 root 帐户可以更方便地访问 ESXi 主机，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。

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。

重要事项 如果您要移除 root 用户的访问特权，则必须首先在 root 级别创建另一个权限，以便向另一用户分配管理员角色。

vpxuser 特权

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

vCenter Server 对其管理的主机拥有管理员特权。例如，vCenter Server 可将虚拟机移至和移离主机，并执行支持虚拟机所必需的配置更改。

vCenter Server 管理员可在主机上执行可以由 Root 用户执行的大多数任务，并调度任务和处理模板等。但是，vCenter Server 管理员不能为主机直接创建、删除或编辑本地用户和组。这些任务只能由具有管理员权限的用户直接在每个主机上执行。

注意 不能使用 Active Directory 管理 vpxuser。



小心 不要以任何方式更改 vpxuser。不要更改其密码。不要更改其权限。如果进行了更改，在通过 vCenter Server 处理主机时可能会出现问题。

dcui 用户特权

dcui 用户以管理员权限在主机上操作。此用户的主要目的是从直接控制台用户界面 (DCUI) 配置锁定模式的主机。此用户将充当直接控制台的代理，无法由交互式用户来修改或使用。

使用 Active Directory 管理 ESXi 用户

可以将 ESXi 配置为使用像 Active Directory 这样的目录服务来管理用户。

如果要在每台主机上都创建本地用户帐户，则涉及到必须在多个主机间同步帐户名和密码的问题。若将 ESXi 主机加入到 Active Directory 域中，则无需再创建和维护本地用户帐户。使用 Active Directory 进行用户身份验证可以简化 ESXi 主机配置，并能降低可导致出现未授权访问的配置问题的风险。

当使用活动目录时，将主机添加到域时用户会提供活动目录凭据以及活动目录服务器的域名。

配置主机以使用 Active Directory

可以对主机进行配置，以便使用目录服务（如 Active Directory）来管理用户和组。

向 Active Directory 中添加 ESXi 主机时，如果存在 DOMAIN 组 **ESX Admins**，则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。请参见第 68 页，“使用 vSphere Authentication Proxy”。

注意 在 Active Directory 中定义用户帐户设置时，可以按计算机名称限制用户能够登录的计算机。默认情况下，未对用户帐户设置任何相关限制。如果设置了此限制，对用户帐户的 LDAP 绑定请求将失败，并显示消息 LDAP 绑定失败 (LDAP binding not successful)，即使该请求来自列出的计算机也是如此。可以通过将 Active Directory 服务器的 netBIOS 名称添加到用户帐户能够登录的计算机列表来避免此问题。

前提条件

- 确认您拥有 Active Directory 域。请参见目录服务器文档。
- 确认 ESXi 的主机名完全符合 Active Directory 林的域名条件。

全限定域名 = 主机名.域名

步骤

- 1 使用 NTP 将 ESXi 和目录服务系统的时间同步。

有关如何使用 Microsoft 域控制器同步 ESXi 时间的信息，请参阅第 147 页，“使 ESXi 时钟与网络时间服务器同步”或 VMware 知识库。

- 2 确保为主机配置的 DNS 服务器可以解析 Active Directory 控制器的主机名。
 - a 在 vSphere Web Client 对象导航器中，浏览到主机。
 - b 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。

下一步

使用 vSphere Web Client 加入目录服务域。请参见第 67 页，“[将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。请参见第 68 页，“[使用 vSphere Authentication Proxy](#)”。

将主机添加到目录服务域

要让主机使用目录服务，必须将主机加入到目录服务域。

可以使用以下两种方法之一输入域名：

- **name.tld**（例如 **domain.com**）：在默认容器下会创建该帐户。
- **name.tld/container/path**（例如 **domain.com/OU1/OU2**）：在特定组织单元 (OU) 下会创建该帐户。

要使用 vSphere Authentication Proxy 服务，请参见第 68 页，“[使用 vSphere Authentication Proxy](#)”。

步骤

- 1 在 vSphere Web 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。

查看目录服务设置

可以查看目录服务器的类型（如果有），主机将使用此类型对用户和目录服务器设置进行身份验证。

步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 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。

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。

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。

请参见第 50 页，“在 Auto Deploy 中使用自定义证书”。

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中，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。

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

启用 vSphere Authentication Proxy

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。如果您要在环境中使用 vSphere Authentication Proxy，可以通过 vSphere Web Client 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，当您在 vSphere Web Client 中指定 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 通过 vSphere Web Client 连接到 vCenter Server 系统。
- 2 单击**系统管理**，然后在**部署**下单击**系统配置**。
- 3 单击**服务**，然后单击 **VMware vSphere Authentication Proxy** 服务。
- 4 单击窗口顶部的菜单栏中绿色的**启动服务**图标。

- 5 （可选）启动该服务后，单击**操作 > 编辑启动类型**，然后单击**自动**以实现自动启动。

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 Web Client 将域添加到 vSphere Authentication Proxy

您可以通过 vSphere Web Client 或使用 `camconfig` 命令将域添加到 vSphere Authentication Proxy。

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 Web Client 连接到 vCenter Server 系统。
- 2 单击**系统管理**，然后在**部署**下单击**系统配置**。
- 3 依次单击**服务**、**VMware vSphere Authentication Proxy 服务**和**编辑**。
- 4 输入 vSphere Authentication Proxy 将向其添加主机的域名称，以及拥有将主机添加到域的 Active Directory 特权的用户名。
该对话框中的其他字段仅供参考。
- 5 单击省略号图标添加并确认用户密码，然后单击**确定**。

使用 camconfig 命令向 vSphere Authentication Proxy 添加域

您可以通过 vSphere Web Client 或使用 `camconfig` 命令向 vSphere Authentication 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 Appliance 或 vCenter Server Windows 计算机。
- 2 运行以下命令以启用对 Bash shell 的访问。
`shell`
- 3 转到 `camconfig` 脚本所在的目录。

操作系统	位置
vCenter Server Appliance	/usr/lib/vmware-vmcam/bin/
vCenter Server Windows	C:\Program Files\VMware\CIS\vmcamd\

- 4 运行以下命令将域和用户 Active Directory 凭据添加到 Authentication Proxy 配置。

`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然用户，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 将使用 `user` 指定的用户名为 ESXi 主机在 Active Directory 中创建帐户，所以该用户必须具有在即将添加主机的 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 使用的是 CA 签名证书，请确认是否已将 CA 签名证书添加到 vCenter Server 系统。请参见 [第 39 页](#)，“ESXi 主机的证书管理”。

步骤

- 1 通过 vSphere Web Client 连接到 vCenter Server 系统。
- 2 在 vSphere Web Client 中浏览到该主机，然后单击**配置**。
- 3 在**设置**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**。

启用 vSphere Authentication Proxy 的客户端身份验证

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，您可以启用客户端身份验证。如果启用了客户端身份验证，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，当您添加主机到 vCenter Server 时，该主机会计入一个由 vCenter Server 受信任 root CA 签名的证书。vSphere Authentication Proxy 信任 vCenter Server 受信任 root CA。
- 如果您计划替换环境中的 ESXi 证书，请先执行替换，然后再启用 vSphere Authentication Proxy。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 Appliance 或 vCenter Server Windows 计算机。

- 2 运行以下命令以启用对 Bash shell 的访问。

```
shell
```

- 3 转到 **camconfig** 脚本所在的目录。

操作系统	位置
vCenter Server Appliance	/usr/lib/vmware-vmcam/bin/
vCenter Server Windows	C:\Program Files\VMware\CIS\vmcamd\

- 4 请运行以下命令以启用客户端身份验证。

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

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

- 5 如果您稍后要再次禁用客户端身份验证，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。可以在以下位置找到该证书。

vCenter Server Appliance	/var/lib/vmware/vmcam/ssl/rui.crt
vCenter Server Windows	C:\ProgramData\VMware\vCenterServer\data\vmcamd\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 在 vSphere Web Client 中，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` 键入证书文件路径，然后单击**确定**。

为 vSphere Authentication Proxy 生成新证书

如果要生成 VMCA 置备的新证书，或包括 VMCA 作为辅助证书的新证书，请完成本主题中的各个步骤。

如果要使用第三方或企业 CA 签名的自定义证书，请参见第 72 页，“[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/certool --genkey --privkey=/var/lib/vmware/vmcam/ssl/rui.key --
pubkey=/tmp/vmcam.pub --server=localhost
```

对于 *localhost*，请提供 Platform Services Controller 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/certool --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 Platform Services Controller 的 FQDN。

设置 vSphere Authentication Proxy 以使用自定义证书

要对 vSphere Authentication Proxy 使用自定义证书，需生成 CSR，将其发送到 CA 进行签名，并将已签名证书和密钥文件放置在 vSphere Authentication Proxy 可以访问的位置。

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:olearyf-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。

操作系统	位置
vCenter Server Appliance	/var/lib/vmware/vmcam/ssl/rui.crt
vCenter Server Windows	C:\ProgramData\VMware\vCenterServer\data\vmcamd\ssl\rui.crt

3 取消注册 vSphere Authentication Proxy。

- a 转到 camregister 脚本所在的目录。

操作系统	命令
vCenter Server Appliance	/var/lib/vmware-vmcam/bin
vCenter Server Windows	C:\ProgramData\VMware\vCenterServer\data\vmcamd\ssl\rui.c rt

- 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
vSphere Web Client	a 单击 系统管理 ，然后在 部署 下单击 系统配置 。 b 单击 服务 ，然后单击 VMware vSphere Authentication Proxy 服务并停止该服务。
CLI	service-control --stop vmcam

- 5 将现有 `ru1.crt` 证书和 `ru1.key` 文件替换为从 CA 收到的文件。
 - 6 重新启动 vSphere Authentication Proxy 服务。
 - 7 通过运行以下命令，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_ru1.crt -k full_path_to_ru1.key
```

## 配置 ESXi 的智能卡身份验证

可以使用智能卡身份验证登录到 ESXi 直接控制台用户界面 (DCUI)，方法是使用个人身份验证 (PIV)、通用访问卡 (CAC) 或 SC650 智能卡，而不是指定用户名和密码。

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 主机将读取该卡上的凭据。
- 2 ESXi DCUI 会显示登录 ID，并提示您输入 PIN。
- 3 输入 PIN 后，ESXi 主机将将其与存储在智能卡上的 PIN 匹配，并使用 Active Directory 验证智能卡上的证书。
- 4 成功验证智能卡证书后，ESXi 将让您登录到 DCUI。

按下 F3 即可从 DCUI 切换到用户名和密码身份验证。

在连续几次输入错误的 PIN（通常三次）后，智能卡上的芯片将锁定。如果智能卡已锁定，则只有选定人员才能将其解锁。

## 启用智能卡身份验证

启用智能卡身份验证可提示提供智能卡和 PIN 组合来登录到 ESXi DCUI。

### 前提条件

- 设置基础架构以处理智能卡身份验证，例如 Active Directory 域中的帐户、智能读卡器和智能卡。
- 将 ESXi 配置为加入一个支持智能卡身份验证的 Active Directory 域。有关详细信息，请参见第 66 页，“使用 Active Directory 管理 ESXi 用户”。
- 使用 vSphere Web Client 添加根证书。请参见第 39 页，“ESXi 主机的证书管理”。

### 步骤

- 1 在 vSphere Web Client 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。
- 7 打开“智能卡身份验证”页面，选中**启用智能卡身份验证**复选框，然后单击**确定**。

## 禁用智能卡身份验证

禁用智能卡身份验证以返回 ESXi DCUI 登录的默认用户名和密码身份验证。

### 步骤

- 1 在 vSphere Web Client 中，浏览到主机。
- 2 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。

---

**注意** 如果 Active Directory (AD) 域服务器可用，则丢失与 vCenter Server 的网络连接不会影响智能卡身份验证。

---

## 在锁定模式下使用智能卡身份验证

启用时，ESXi 主机上的锁定模式可提高主机的安全性并限制对 DCUI 的访问。锁定模式可能禁用智能卡身份验证功能。

在正常锁定模式下，只有“异常用户”列表中具有管理员特权的用户才能访问 DCUI。异常用户是指具有在本地为 ESXi 主机定义的特权的主机本地用户或 Active Directory 用户。如果要在正常锁定模式下使用智能卡身份验证，则必须从 vSphere Web Client 将用户添加到“异常用户”列表。主机进入正常锁定模式时，这些用户不会丢失其权限且可以登录到 DCUI。有关详细信息，请参见第 63 页，“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

默认情况下，ESXi 主机上的 ESXi Shell 处于禁用状态。如有必要，可以启用对 shell 的本地或远程访问。

启用 ESXi Shell 仅用于故障排除。ESXi Shell 不受锁定模式影响。以锁定模式运行的主机不会阻止您启用或禁用 ESXi Shell。

### ESXi Shell

启用此服务以本地访问 ESXi Shell。

### SSH

启用此服务以使用 SSH 远程访问 ESXi Shell。

请参见 *vSphere 安全性*。

### 直接控制台 UI (DCUI)

如果在锁定模式下运行时启用此服务，您可以以 Root 用户身份在本地登录到直接控制台用户界面并禁用锁定模式。然后可以直接连接到 VMware Host Client 或通过启用 ESXi Shell 来访问主机。

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`）。

---

**注意** 只有在真正需要访问 ESXi Shell 时才启用它。

---

- [使用 vSphere Web Client 启用对 ESXi Shell 的访问](#) 第 76 页，  
可以使用 vSphere Web Client 启用对 ESXi Shell 的本地和远程 (SSH) 访问，并设置空闲时间和可用性超时。
- [使用直接控制台用户界面 \(DCUI\) 启用对 ESXi Shell 的访问](#) 第 77 页，  
通过直接控制台用户界面 (DCUI)，您可以使用基于文本的菜单在本地与主机进行交互。请仔细评估您的环境安全要求是否支持启用直接控制台用户界面。
- [登录 ESXi Shell 以进行故障排除](#) 第 79 页，  
使用 vSphere Web Client、vSphere CLI 或 vSphere PowerCLI 执行 ESXi 配置任务。登录 ESXi Shell（以前称为技术支持模式或 TSM）仅进行故障排除。

## 使用 vSphere Web Client 启用对 ESXi Shell 的访问

可以使用 vSphere Web Client 启用对 ESXi Shell 的本地和远程 (SSH) 访问，并设置空闲时间和可用性超时。

---

**注意** 使用 vSphere Web Client、远程命令行工具（vCLI 和 PowerCLI）和已发布的 API 来访问主机。除非是在要求启用 SSH 访问的特殊情况下，否则不要启用使用 SSH 远程访问主机的功能。

---

### 前提条件

如果要使用授权 SSH 密钥，可以上载该密钥。请参见 [第 35 页，“ESXi SSH 密钥”](#)。

### 步骤

- 1 在 vSphere Web 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“服务”面板中，单击**编辑**。
- 5 从列表中选择一种服务。
  - ESXi Shell
  - SSH
  - 直接控制台 UI
- 6 单击**服务详细信息**，然后选择**手动启动和停止**启动策略。  
如果选择**手动启动和停止**，则重新引导主机时不会启动服务。如果要在重新引导主机时启动服务，请选择**与主机一起启动和停止**。
- 7 选择**启动**以启用该服务。
- 8 单击**确定**。

### 下一步

设置 ESXi Shell 的可用性和闲置超时。请参见 [第 77 页，“在 vSphere Web Client 中为 ESXi Shell 可用性创建超时”](#) 和 [第 77 页，“在 vSphere Web Client 中为闲置的 ESXi Shell 会话创建超时”](#)

## 在 vSphere Web Client 中为 ESXi Shell 可用性创建超时

默认情况下，ESXi Shell 处于禁用状态。您可设置 ESXi Shell 可用性超时，提高启用 shell 时的安全性。

可用性超时设置是在启用 ESXi Shell 之后和必须登录之前，可以经过的时间量。超过超时期限之后，该服务会禁用，并且不允许用户登录。

### 步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 单击**配置**。
- 3 在“系统”下，选择**高级系统设置**。
- 4 选择 UserVars.ESXiShellTimeOut 并单击**编辑**。
- 5 输入闲置超时设置。  
您必须重新启动 SSH 服务和 ESXi Shell 服务，超时才能生效。
- 6 单击**确定**。

如果在经过超时期限后您已登录，您的会话将持续。但是，您注销或您的会话终止后，用户将无法登录。

## 在 vSphere Web Client 中为闲置的 ESXi Shell 会话创建超时

如果用户在主机上启用了 ESXi Shell，但却忘记了注销会话，则闲置会话将无限期保持连接状态。打开的连接会提高他人获得主机访问特权的可能性。您可以通过为闲置会话设置超时来防止出现此问题。

闲置超时是指用户从闲置交互式会话注销之前可以经过的时间量。您可以从直接控制台界面 (DCUI) 或 vSphere Web Client 中控制本地和远程 (SSH) 会话的时间量。

### 步骤

- 1 在 vSphere Web Client 清单中，浏览到主机。
- 2 单击**配置**。
- 3 在“系统”下，选择**高级系统设置**。
- 4 选择 UserVars.ESXiShellInteractiveTimeOut，单击**编辑**图标，然后输入超时设置。
- 5 重新启动 ESXi Shell 服务和 SSH 服务，以使此超时生效。

如果该会话闲置，则用户将在超时期限过后注销。

## 使用直接控制台用户界面 (DCUI) 启用对 ESXi Shell 的访问

通过直接控制台用户界面 (DCUI)，您可以使用基于文本的菜单在本地与主机进行交互。请仔细评估您的环境安全要求是否支持启用直接控制台用户界面。

可以使用直接控制台用户界面启用对 ESXi Shell 的本地和远程访问。

---

**注意** 使用直接控制台用户界面、vSphere Web Client、ESXCLI 或其他管理工具对主机进行的更改，会每隔一小时或在正常关机时提交到永久存储。如果在提交这些更改之前主机出现故障，则可能会丢失这些更改。

---

### 步骤

- 1 从直接控制台用户界面中，按 F2 访问“系统自定义”菜单。
- 2 选择**故障排除选项**，然后按 Enter。

- 3 从“故障排除模式选项”菜单中，选择要启用的服务。
  - 启用 ESXi Shell
  - 启用 SSH
- 4 按 Enter 以启用该服务。
- 5 按 Esc 直到返回到直接控制台用户界面的主菜单。

### 下一步

设置 ESXi Shell 的可用性和闲置超时。请参见第 78 页，“在直接控制台用户界面中为 ESXi Shell 可用性创建超时”和第 78 页，“为闲置 ESXi Shell 会话创建超时”。

## 在直接控制台用户界面中为 ESXi Shell 可用性创建超时

默认情况下，ESXi Shell 处于禁用状态。您可设置 ESXi Shell 可用性超时，提高启用 shell 时的安全性。

可用性超时设置是在启用 ESXi Shell 之后和必须登录之前，可以经过的时间量。超过超时期限之后，该服务会禁用，并且不允许用户登录。

### 步骤

- 1 从“故障排除模式选项”菜单中，选择**修改 ESXi Shell 和 SSH 超时**，然后按 Enter。
- 2 输入可用性超时。

您必须重新启动 SSH 服务和 ESXi Shell 服务，超时才能生效。
- 3 按 Enter 并按 Esc 直到返回到直接控制台用户界面的主菜单。
- 4 单击**确定**。

如果在经过超时期限后您已登录，您的会话将持续。但是，您注销或您的会话终止后，用户将无法登录。

## 为闲置 ESXi Shell 会话创建超时

如果用户在主机上启用了 ESXi Shell，但却忘记了注销会话，则闲置会话将无限期保持连接状态。打开的连接会提高他人获得主机访问特权的可能性。您可以通过为闲置会话设置超时来防止出现此问题。

闲置超时是用户从闲置交互式会话注销之前可以经过的时间量。对闲置超时的更改会在下次用户登录 ESXi Shell 时应用。更改不影响现有会话。

您可以在直接控制台用户界面中设置以秒为单位的超时值，或在 vSphere Web Client 中设置以分钟为单位的超时值。

### 步骤

- 1 从“故障排除模式选项”菜单中，选择**修改 ESXi Shell 和 SSH 超时**，然后按 Enter。
- 2 输入闲置超时值（以秒为单位）。

您必须重新启动 SSH 服务和 ESXi Shell 服务，超时才能生效。
- 3 按 Enter 并按 Esc 直到返回到直接控制台用户界面的主菜单。

如果该会话闲置，则用户将在超时期限过后注销。

## 登录 ESXi Shell 以进行故障排除

使用 vSphere Web Client、vSphere CLI 或 vSphere PowerCLI 执行 ESXi 配置任务。登录 ESXi Shell（以前称为技术支持模式或 TSM）仅进行故障排除。

### 步骤

- 1 使用以下方法之一登录 ESXi Shell。
  - 如果可以访问主机，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

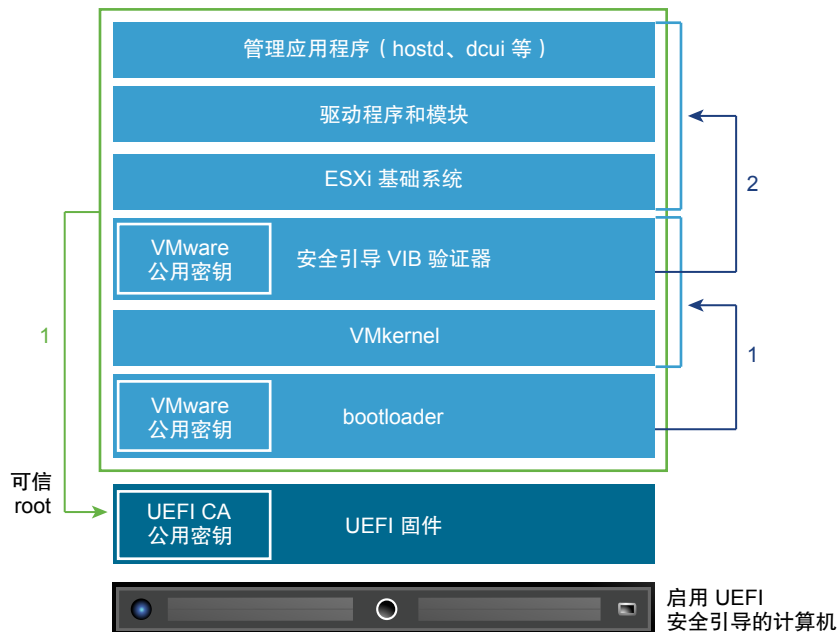
安全引导属于 UEFI 固件标准的一部分。启用安全引导后，计算机会拒绝加载任何 UEFI 驱动程序或应用程序，除非操作系统引导加载程序以加密形式进行签名。从 vSphere 6.5 开始，如果在硬件中启用了安全引导，则 ESXi 会加以支持。

### UEFI 安全引导概述

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。

**注意** 在升级到 ESXi 6.5 的主机上使用 UEFI 安全引导之前，请按照第 80 页，“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。如果使用 **esxcli** 命令升级 ESXi 主机，则升级不会更新引导加载程序。在这种情况下，无法在此系统上执行安全引导。

图 3-1 UEFI 安全引导



启用安全引导后，引导顺序如下所示。

- 1 从 vSphere 6.5 开始，ESXi 引导加载程序包含 VMware 公用密钥。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。

## 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 vib(s) (XX)
```

要使用安全引导解决问题，请执行以下步骤。

- 1 禁用安全引导并重新引导主机。
- 2 运行安全引导验证脚本（请参见第 80 页，“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

如果硬件支持 UEFI 安全引导，您可能可以为 ESXi 主机启用安全引导。是否可行取决于您执行升级的方式。您可以在执行升级后运行验证脚本以确定是否支持安全引导。

UEFI 安全引导需要保留原始 VIB 签名。早期版本的 ESXi 不会保留签名，但是升级过程会更新 VIB 签名。

- 如果使用 ISO 升级，升级后的 VIB 会保留签名。
- 如果使用 ESXCLI 命令升级，升级后的 VIB 不会保留签名。在这种情况下，无法在此系统上执行安全引导。

即使使用 ISO 升级，升级过程也无法保留第三方 VIB 的签名。在这种情况下，系统上的安全引导将失败。

---

### 注意

---

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。



## 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。

采取下列措施来提高主机的安全性。

- 配置持久日志记录到数据存储。默认情况下，ESXi 主机上的日志存储在内存文件系统中。因此，当您重新引导主机时，日志将会丢失，并且仅存储 24 小时的日志数据。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 CLI（例如 vCLI 或 PowerCLI）或使用 API 客户端可以在 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

所有 ESXi 主机均运行 syslog 服务 (vmsyslogd)，该服务将来自 VMkernel 和其他系统组件的消息写到日志文件中。

可以使用 vSphere Web Client 或 `esxcli system syslog vCLI` 命令来配置 syslog 服务。

有关使用 vCLI 命令的详细信息，请参见 *vSphere Command-Line Interface 入门*。

### 步骤

- 1 在 vSphere Web Client 清单中，选择主机。
- 2 单击 **配置**。
- 3 在“系统”下，单击 **高级系统设置**。
- 4 筛选出 **syslog**。
- 5 要全局设置日志记录，请选择要更改的设置，然后单击 **编辑**。

| 选项                                 | 描述                                                                                                                                                                                                                                          |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Syslog.global.defaultRotate</b> | 要保留的存档的最大数目。可以在全局范围内设置该数目，也可以为单个子记录器设置该数目。                                                                                                                                                                                                  |
| <b>Syslog.global.defaultSize</b>   | 在系统轮换日志之前，日志的默认大小 (KB)。可以在全局范围内设置该数目，也可以为单个子记录器设置该数目。                                                                                                                                                                                       |
| <b>Syslog.global.LogDir</b>        | 存储日志的目录。该目录可能位于挂载的 NFS 或 VMFS 卷中。只有本地文件系统中的 <code>/scratch</code> 目录在重新引导后仍然存在。将目录指定为 <code>[数据存储名称] 文件路径</code> ，其中，路径是相对于支持数据存储卷的根目录的路径。例如，路径 <code>[storage1] /systemlogs</code> 将映射为路径 <code>/vmfs/volumes/storage1/systemlogs</code> 。 |
| <b>Syslog.global.logDirUnique</b>  | 选择此选项将使用 ESXi 主机的名称在 <b>Syslog.global.LogDir</b> 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。                                                                                                                                           |
| <b>Syslog.global.LogHost</b>       | 向其转发 syslog 消息的远程主机，以及远程主机在其上接收 syslog 消息的端口。可以包括协议和端口，例如 <code>ssl://hostName1:1514</code> 。支持 UDP（默认）、TCP 和 SSL。远程主机必须安装并正确配置 syslog 以接收转发的 syslog 消息。有关配置的信息，请参见远程主机上所安装的 syslog 服务的文档。                                                  |

- 6 (可选) 覆盖任何日志的默认日志大小和日志轮换。
  - a 单击要自定义的日志的名称。
  - b 单击**编辑**，然后输入所需的轮换数和日志大小。
- 7 单击**确定**。

对 syslog 选项的更改将立即生效。

## ESXi 日志文件地址

ESXi 通过使用 syslog 功能，在日志文件中记录主机活动。

| 组件           | 位置                                                                                                    | 用途                                                           |
|--------------|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| VMkernel     | /var/log/vmkernel.log                                                                                 | 记录与虚拟机以及 ESXi 有关的活动。                                         |
| VMkernel 警告  | /var/log/vmkwarning.log                                                                               | 记录与虚拟机有关的活动。                                                 |
| 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）。                            |
| 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。                                |
| vCenter 代理日志 | /var/log/vpxa.log                                                                                     | 包含与 vCenter Server 通信的代理的有关信息（如果主机由 vCenter Server 管理）。      |
| Shell 日志     | /var/log/shell.log                                                                                    | 包含键入 ESXi Shell 的所有命令以及 Shell 事件（例如启用 Shell）的记录。             |
| 身份验证         | /var/log/auth.log                                                                                     | 包含与本地系统身份验证相关的所有事件。                                          |
| 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。                       |
| 虚拟机          | 与受影响虚拟机的配置文件（名为 vmware.log 和 vmware*.log）具有相同目录。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。 |

## 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，然后将他们发送至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。

## 确保 vCenter Server 系统安全

---

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：

- 第 83 页，“vCenter Server 安全性最佳做法”
- 第 88 页，“验证旧版 ESXi 主机的指纹”
- 第 88 页，“验证“对网络文件复制的 SSL 证书验证”是否已启用”
- 第 89 页，“vCenter Server 和 Platform Services Controller 所需的端口”
- 第 92 页，“其他 vCenter Server TCP 和 UDP 端口”

### vCenter Server 安全性最佳做法

遵循 vCenter Server 安全性最佳做法有助于确保 vSphere 环境的完整性。

#### vCenter Server 访问控制的最佳做法

严格控制对不同 vCenter Server 组件的访问，以增强系统的安全性。

以下准则有助于确保环境的安全性。

##### 使用指定帐户

- 如果本地 Windows 管理员帐户当前拥有管理员角色 vCenter Server，请移除此角色，并将角色分配给一个或多个指定的 vCenter Server 管理员帐户。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人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。

---

**注意** 从 vSphere 6.0 开始，默认情况下，本地管理员不再对 vCenter Server 拥有完全管理权限。

---

- 请使用服务帐户而不是 Windows 帐户安装 vCenter Server。服务帐户必须是本地计算机上的管理员。
- 请确保应用程序在连接到 vCenter Server 系统时使用唯一的服务帐户。

## 监控 vCenter Server 管理员用户的特权

并非所有管理员用户都必须具有管理员角色。而是应该创建具有一组适当特权的自定义角色，并将其分配给其他管理员。

具有 vCenter Server 管理员角色的用户对层次结构中的所有对象都拥有特权。例如，默认情况下，管理员角色允许用户与虚拟机客户机操作系统内的文件和程序交互。将该角色分配给过多的用户可能会降低虚拟机数据的保密性、可用性或完整性。请创建一个角色，以便向管理员授予他们所需的特权，但移除部分虚拟机管理特权。

## 最大程度地减少访问

请勿允许用户直接登录到 vCenter Server 主机。登录到 vCenter Server 主机的用户可能会更改设置以及修改进程，从而会有意或无意地造成危害。这些用户还可能访问 vCenter 凭据，例如 SSL 证书。请仅允许要执行合法任务的用户登录到系统，并确保对登录事件进行审核。

## 为 vCenter Server 数据库用户授予最小的特权

数据库用户仅需要特定于数据库访问的某些特权。

某些特权仅在进行安装和升级时需要。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.浏览数据存储**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 Web 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 vCenter Server 管理员角色的用户可与虚拟机客户机操作系统中的文件和程序交互。为了降低损害客户机保密性、可用性或完整性的风险，请创建没有**客户机操作**特权的非客户机自定义访问角色。请参见第 102 页，“[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。请参见第 85 页，“[设置 vCenter Server 密码策略](#)”。

---

**注意** 请确保密码时效策略的时间不能太短。

---

## 在 vCenter Server 重新启动后检查特权

请在重新启动 vCenter Server 时检查特权的重新分配情况。如果重新启动时无法验证在 root 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）。

## 使用高 RDP 加密级别

在基础架构中的每台 Windows 计算机上，请务必设置远程桌面主机配置设置，以确保适用于您环境的加密级别最高。

## 验证 vSphere Web Client 证书

指示其中一个 vSphere Web Client 或其他客户端应用程序的用户切勿忽略证书验证警告。若不进行证书验证，用户可能会受到 MiTM 攻击。

## 设置 vCenter Server 密码策略

默认情况下，vCenter Server 会每 30 天自动更改一次 vpxuser 密码。可以从 vSphere Web Client 中更改该值。

### 步骤

- 1 在 vSphere Web Client 对象层次结构中选择 vCenter Server。
- 2 单击**配置**。
- 3 单击**高级设置**，然后在筛选框中输入 **VimPasswordExpirationInDays**。
- 4 根据您的要求设置 **VirtualCenter.VimPasswordExpirationInDays**。

## 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。

## 保护 vCenter Server Windows 主机

通过尽可能地确保主机环境的安全，保护运行 vCenter Server 的 Windows 主机免遭漏洞和攻击的威胁。

- 为 vCenter Server 系统维持一个支持的操作系统、数据库和硬件。如果 vCenter Server 未在受支持的操作系统上运行，则可能无法正常运行，从而使 vCenter Server 易受攻击。
- 使 vCenter Server 系统保持适当地修补。通过使操作系统及时更新最新的修补程序，可让 vCenter Server 不容易受到攻击。
- 对 vCenter Server 主机提供操作系统保护。提供的保护包括防病毒软件和反恶意软件。
- 在基础架构中的每台 Windows 计算机上，请务必根据行业标准准则或内部准则设置远程桌面 (RDP) 主机配置设置，以确保加密级别最高。

有关操作系统和数据库兼容性的信息，请参见 *vSphere 兼容性列表*。

## 限制 vCenter Server 网络连接

为提高安全性，请避免将 vCenter Server 系统放置在管理网络之外的任何网络上，并确保 vSphere 管理流量位于受限网络上。通过限制网络连接，可以限制特定类型的攻击。

vCenter Server 仅需要访问管理网络。避免将 vCenter Server 系统放置在其他网络（如生产网络、存储网络或有权访问 Internet 的任何网络）上。vCenter Server 不需要访问 vMotion 在其中运行的网络。

vCenter Server 需要与以下系统建立网络连接。

- 所有 ESXi 主机。
- vCenter Server 数据库。

- 其他 vCenter Server 系统（如果 vCenter Server 系统是用于复制标记、权限等的常见 vCenter Single Sign-On 域的一部分）。
- 有权运行管理客户端的系统。例如，vSphere Web Client（您在其中使用 PowerCLI 的 Windows 系统）或任何其他基于 SDK 的客户端。
- 运行加载项组件（例如 VMware vSphere Update Manager）的系统。
- 基础架构服务，例如 DNS、Active Directory 和 NTP。
- 运行对 vCenter Server 系统功能至关重要的组件的其他系统。

使用运行 vCenter Server 系统的 Windows 系统上的本地防火墙或使用网络防火墙。包含基于 IP 的访问限制，这样只有必要的组件才能与 vCenter Server 系统通信。

## 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。

即使您已将 vCenter Server 系统和 ESXi 主机上的 VMCA 签名证书替换为由第三方 CA 签名的证书，但与 Linux 客户端的某些通信仍然容易受到中间人的攻击。以下组件在 Linux 操作系统上运行时易受攻击。

- vCLI 命令
- vSphere SDK for Perl 脚本
- 使用 vSphere Web Services SDK 编写的程序

如果强制执行适当的控制，则可放宽对使用 Linux 客户端的限制。

- 仅限授权系统访问管理网络。
- 使用防火墙确保只允许授权主机访问 vCenter Server。
- 使用跳转盒系统确保 Linux 客户端受跳转限制。

## 检查已安装的插件

vSphere Web Client 扩展在登录用户的相同特权级别下运行。恶意扩展可以伪装成有用的插件并执行有害的操作，例如盗取凭据或更改系统配置。为增强安全性，请使用仅包含来自受信任源的授权扩展的 vSphere Web Client 安装。

vCenter 安装包含 vSphere Web Client 可扩展性框架，其提供通过菜单选项或工具栏图标（提供对 vCenter 加载项组件或外部基于 Web 的功能的访问）来扩展 vSphere Web Client 的功能。在此灵活性下，存在引入意外功能的风险。例如，如果管理员在 vSphere Web Client 的一个实例中安装插件，则该插件可以使用该管理员的特权级别执行任意命令。

为了保护 vSphere Web Client 免受潜在的危害，可以定期检查所有已安装的插件并确保所有插件均来自受信任的源。

### 前提条件

您必须具有访问 vCenter Single Sign-On 服务的特权。这些特权与 vCenter Server 特权不同。

### 步骤

- 1 以 administrator@vsphere.local 或拥有 vCenter Single Sign-On 特权用户的身份登录到 vSphere Web Client。
- 2 在主页上，选择**管理**，然后选择**解决方案**下的**客户端插件**
- 3 检查客户端插件列表。

## vCenter Server Appliance 安全性最佳做法

遵循确保 vCenter Server 系统安全的所有最佳做法，进而确保 vCenter Server Appliance 安全。下述额外步骤将有助于提高设备的安全性。

### 配置 NTP

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。使用 NTP，还可以更轻松地跟踪日志文件中的入侵者。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。请参见第 149 页，“将 vCenter Server Appliance 中的时间与 NTP 服务器同步”。

### 限制 vCenter Server Appliance 网络访问

限制对与 vCenter Server Appliance 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。请参见第 89 页，“vCenter Server 和 Platform Services Controller 所需的端口”和第 92 页，“其他 vCenter Server TCP 和 UDP 端口”。请遵循 VMware 知识库文章 2047585 中的准则，使用与 DISA STIG 相符的防火墙设置设置您的环境。

## 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，请参见第 34 页，“ESXi 密码和帐户锁定”。

### vCenter Single Sign-On 管理员密码

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

此用户的密码长度不得超过 20 个字符。从 vSphere 6.0 开始，允许使用非 ASCII 字符。管理员可以更改默认密码策略。请参见 *Platform Services Controller 管理* 文档。

### vCenter Server 密码

在 vCenter Server 中，密码要求由 vCenter Single Sign-On 或配置的标识源规定，这些配置的标识源可以是 Active Directory 和 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。您可以使用 vCenter Single Sign-On 锁定策略更改这些默认值。请参见 *Platform Services Controller 管理* 文档。

自 vSphere 6.0 起，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。

## 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 管理员可以通过使用 `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 及更高的版本中，默认情况下，将为主机分配 VMCA 证书。如果将证书模式更改为指纹，则可以继续为旧版主机使用指纹模式。您可以在 vSphere Web Client 中验证指纹。

---

**注意** 默认情况下，证书在各次升级中均被保留。

---

### 步骤

- 1 在 vSphere Web Client 对象导航器中，浏览到 vCenter Server 系统。
- 2 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 **确定**。

## 验证“对网络文件复制的 SSL 证书验证”是否已启用

网络文件复制 (NFC) 可为 vSphere 组件提供文件类型感知 FTP 服务。从 vSphere 5.5 开始，默认情况下，ESXi 会使用 NFC 执行在数据存储之间复制和移动数据等操作，但如果 NFC 处于禁用状态，则可能需要启用它。

如果启用了基于 NFC 的 SSL，则通过 NFC 在 vSphere 组件之间建立的连接将是安全的。该连接有助于防止数据中心内受到中间人攻击。

由于通过 SSL 使用 NFC 会造成性能降低，因此在某些开发环境中您可能会考虑禁用此高级设置。

---

**注意** 如果使用脚本检查此值，请将此值明确设为 True。

---

### 步骤

- 1 通过 vSphere Web Client 连接到 vCenter Server。
- 2 单击 **配置**。



- 3 单击**高级设置**，并在对话框底部输入以下键和值。

| 字段 | 值                 |
|----|-------------------|
| 键  | config.nfc.useSSL |
| 值  | 有效                |

- 4 单击**确定**。

## vCenter Server 和 Platform Services Controller 所需的端口

Windows 上和设备中的 vCenter Server 系统都必须能够将数据发送到每个受管主机，并从 vSphere Web Client 和 Platform Services Controller 服务接收数据。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彼此接收数据。

如果端口正在使用中或被列入了黑名单，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。

**注意** 在 Microsoft Windows Server 2008 及更高版本中，默认情况下会启用防火墙。

**表 4-1** 组件之间的通信所需的端口

| 端口 | 协议      | 描述                                                                                                                                                                                                                                                                                                                                                                                                                        | 必需                                                                    | 用于节点到节点通信 |
|----|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|-----------|
| 22 | TCP/UDP | SSHD 的系统端口。                                                                                                                                                                                                                                                                                                                                                                                                               | 设备部署<br>■ vCenter Server<br>■ Platform Services Controller            | 否         |
| 80 | TCP     | vCenter Server 需要使用端口 80 进行直接 HTTP 连接。端口 80 会将请求重定向到 HTTPS 端口 443。如果意外使用了 http://server 而不是 https://server，此重定向将非常有用。<br>WS 管理（也需要打开端口 443）。<br>如果使用与 vCenter Server 存储在同一个虚拟机或物理服务器上的 Microsoft SQL 数据库，则 SQL 报告服务将使用端口 80。安装或升级 vCenter Server 时，安装程序将提示您更改 vCenter Server 的 HTTP 端口。将 vCenter Server HTTP 端口更改为自定义值可以确保安装或升级成功。<br><b>重要事项</b> 在 Windows 上安装 vCenter Server 和 Platform Services Controller 时，可以更改此端口号。 | Windows 安装和设备部署<br>■ vCenter Server<br>■ Platform Services Controller | 否         |
| 88 | TCP     | Active Directory 服务器。                                                                                                                                                                                                                                                                                                                                                                                                     | Platform Services Controller 的 Windows 安装和设备部署                        | 否         |

表 4-1 组件之间的通信所需的端口（续）

| 端口  | 协议      | 描述                                                                                                                                                                                                                                                                                                                                                                                                                 | 必需                                                                                                                         | 用于节点到节点通信                                                                                                                                                                                             |
|-----|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 389 | TCP/UDP | 此端口在 vCenter Server 的本地和所有远程实例上必须处于打开状态。这是 vCenter Server 组的目录服务的 LDAP 端口号。如果此端口上正在运行另一服务，则最好移除该服务，或将其端口更改为其他端口。可以在从 1025 到 65535 的任一端口上运行 LDAP 服务。<br>如果此实例充当 Microsoft Windows Active Directory，请将端口号从 389 更改为从 1025 到 65535 的任一可用端口。                                                                                                                                                                            | Platform Services Controller 的 Windows 安装和设备部署                                                                             | <ul style="list-style-type: none"> <li>■ vCenter Server 到 Platform Services Controller</li> <li>■ Platform Services Controller 到 Platform Services Controller</li> </ul>                              |
| 443 | TCP     | vCenter Server 系统侦听来自 vSphere Web Client 的连接时所使用的默认端口。要使 vCenter Server 系统从 vSphere Web Client 接收数据，请在防火墙中打开端口 443。<br>vCenter Server 系统还使用端口 443 监控从 SDK 客户端传输的数据。<br>此端口也用于以下服务： <ul style="list-style-type: none"> <li>■ WS 管理（也需要打开端口 80）</li> <li>■ 第三方网络管理客户端与 vCenter Server 的连接</li> <li>■ 第三方网络管理客户端对主机的访问</li> </ul> <b>重要事项</b> 在 Windows 上安装 vCenter Server 和 Platform Services Controller 时，可以更改此端口号。 | Windows 安装和设备部署 <ul style="list-style-type: none"> <li>■ vCenter Server</li> <li>■ Platform Services Controller</li> </ul> | <ul style="list-style-type: none"> <li>■ vCenter Server 到 vCenter Server</li> <li>■ vCenter Server 到 Platform Services Controller</li> <li>■ Platform Services Controller 到 vCenter Server</li> </ul> |
| 514 | UDP     | Windows 上 vCenter Server 的 vSphere Syslog Collector 端口以及 vCenter Server Appliance 的 vSphere Syslog 服务端口<br><b>重要事项</b> 在 Windows 上安装 vCenter Server 和 Platform Services Controller 时，可以更改此端口号。                                                                                                                                                                                                                     | Windows 安装和设备部署 <ul style="list-style-type: none"> <li>■ vCenter Server</li> <li>■ Platform Services Controller</li> </ul> | 否                                                                                                                                                                                                     |
| 636 | TCP     | vCenter Single Sign-On LDAP                                                                                                                                                                                                                                                                                                                                                                                        | -                                                                                                                          | 仅用于与 vSphere 6.0 实现向后兼容性。<br>vCenter Server 6.0 到 Platform Services Controller 6.5                                                                                                                    |
| 902 | TCP/UDP | vCenter Server 系统用来将数据发送到受管主机的默认端口。受管主机也会通过 UDP 端口 902 定期向 vCenter Server 系统发送检测信号。服务器和主机之间或各个主机之间的防火墙不得阻止此端口。<br>不得在 VMware Host Client 和主机之间阻塞端口 902。VMware Host Client 使用此端口显示虚拟机控制台<br><b>重要事项</b> 在 Windows 上安装 vCenter Server 时，可以更改此端口号。                                                                                                                                                                    | vCenter Server 的 Windows 安装和设备部署                                                                                           | 否                                                                                                                                                                                                     |

表 4-1 组件之间的通信所需的端口（续）

| 端口   | 协议      | 描述                                                                                                                                                                                                      | 必需                                                                    | 用于节点到节点通信                                                                                                                                                           |
|------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1514 | TCP/UDP | Windows 上 vCenter Server 的 vSphere Syslog Collector TLS 端口以及 vCenter Server Appliance 的 vSphere Syslog 服务 TLS 端口<br><b>重要事项</b> 在 Windows 上安装 vCenter Server 和 Platform Services Controller 时，可以更改此端口号。 | Windows 安装和设备部署<br>■ vCenter Server<br>■ Platform Services Controller | 否                                                                                                                                                                   |
| 2012 | TCP     | vCenter Single Sign-On 的控制接口 RPC                                                                                                                                                                        | Platform Services Controller 的 Windows 安装和设备部署                        | ■ vCenter Server 到 Platform Services Controller<br>■ Platform Services Controller 到 vCenter Server<br>■ Platform Services Controller 到 Platform Services Controller |
| 2014 | TCP     | 所有 VMCA (VMware Certificate Authority) API 的 RPC 端口<br><b>重要事项</b> 在 Windows 上安装 Platform Services Controller 时，可以更改此端口号。                                                                               | Platform Services Controller 的 Windows 安装和设备部署                        | ■ vCenter Server 到 Platform Services Controller<br>■ Platform Services Controller 到 vCenter Server                                                                  |
| 2020 | TCP/UDP | 身份验证框架管理<br><b>重要事项</b> 在 Windows 上安装 vCenter Server 和 Platform Services Controller 时，可以更改此端口号。                                                                                                         | Windows 安装和设备部署<br>■ vCenter Server<br>■ Platform Services Controller | ■ vCenter Server 到 Platform Services Controller<br>■ Platform Services Controller 到 vCenter Server                                                                  |
| 6500 | TCP/UDP | ESXi Dump Collector 端口<br><b>重要事项</b> 在 Windows 上安装 vCenter Server 时，可以更改此端口号。                                                                                                                          | vCenter Server 的 Windows 安装和设备部署                                      | 否                                                                                                                                                                   |
| 6501 | TCP     | Auto Deploy 服务<br><b>重要事项</b> 在 Windows 上安装 vCenter Server 时，可以更改此端口号。                                                                                                                                  | vCenter Server 的 Windows 安装和设备部署                                      | 否                                                                                                                                                                   |
| 6502 | TCP     | Auto Deploy 管理<br><b>重要事项</b> 在 Windows 上安装 vCenter Server 时，可以更改此端口号。                                                                                                                                  | vCenter Server 的 Windows 安装和设备部署                                      | 否                                                                                                                                                                   |
| 7444 | TCP     | 安全令牌服务                                                                                                                                                                                                  | Platform Services Controller 的 Windows 安装和设备部署                        | ■ vCenter Server 到 Platform Services Controller<br>■ Platform Services Controller 到 vCenter Server                                                                  |

**表 4-1** 组件之间的通信所需的端口（续）

| 端口    | 协议  | 描述                          | 必需                               | 用于节点到节点通信                                                                                             |
|-------|-----|-----------------------------|----------------------------------|-------------------------------------------------------------------------------------------------------|
| 9123  | TCP | Migration Assistant 端口      | vCenter Server 的 Windows 安装和设备部署 | 源 vCenter Server 或 vCenter Single Sign-On 到目标 vCenter Server Appliance 或 Platform Services Controller |
| 9443  | TCP | vSphere Web Client HTTPS    | vCenter Server 的 Windows 安装和设备部署 | 否                                                                                                     |
| 11711 | TCP | vCenter Single Sign-On LDAP | -                                | 仅用于与 vSphere 5.5 实现向后兼容性。<br>vCenter Single Sign-On 5.5 到 Platform Services Controller 6.5            |
| 11712 | TCP | vCenter Single Sign-On LDAP | -                                | 仅用于与 vSphere 5.5 实现向后兼容性。<br>vCenter Single Sign-On 5.5 到 Platform Services Controller 6.5            |

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

有关防火墙配置的详细信息，请参见 *vSphere 安全性* 文档。

## 其他 vCenter Server TCP 和 UDP 端口

vCenter Server 可通过预定的 TCP 和 UDP 端口进行访问。若要从防火墙外管理网络组件，可能需重新配置防火墙以允许在适当端口的访问。

第 89 页，“vCenter Server 和 Platform Services Controller 所需的端口”列出了安装程序在默认安装过程中打开的端口。某些服务（例如，NTP）或通常与 vCenter Server 一起安装的应用程序需要使用一些其他端口。

除了这些端口外，您可以根据需要配置其他端口。

**表 4-2** vCenter Server TCP 和 UDP 端口

| 端口               | 协议  | 描述                                                                                                                                    |
|------------------|-----|---------------------------------------------------------------------------------------------------------------------------------------|
| 123 (UDP)        | UDP | NTP 客户端。如果您正在 ESXi 主机上部署 vCenter Server Appliance，则两者必须时间同步（通常通过 NTP 服务器），且必须打开相应的端口。                                                 |
| 135              | TCP | 对于 vCenter Server Appliance，指定此端口用于 Active Directory 身份验证。<br>对于 vCenter Server Windows 安装，此端口用于链接模式，而端口 88 用于 Active Directory 身份验证。 |
| 161              | UDP | SNMP 服务器。                                                                                                                             |
| 636              | TCP | vCenter Single Sign-On LDAPS（6.0 及更高版本）                                                                                               |
| 8084, 9084, 9087 | TCP | 由 vSphere Update Manager 使用                                                                                                           |
| 8109             | TCP | VMware Syslog Collector。如果您要集中收集，则需要该服务。                                                                                              |

**表 4-2** vCenter Server TCP 和 UDP 端口（续）

| 端口                          | 协议  | 描述                                                                  |
|-----------------------------|-----|---------------------------------------------------------------------|
| 15007,<br>15008             | TCP | vService Manager (VSM)。此服务用于注册 vCenter Server 扩展。仅当要使用的扩展需要时才打开此端口。 |
| 31031、<br>44046<br>(默<br>认) | TCP | vSphere Replication。                                                |

以下端口仅限内部使用。

**表 4-3** vCenter Server TCP 和 UDP 端口

| 端口                                          | 描述                                            |
|---------------------------------------------|-----------------------------------------------|
| 5443                                        | vCenter Server 图形用户界面内部端口。                    |
| 5444,<br>5432                               | 监控 vPostgreSQL 的内部端口。                         |
| 5090                                        | vCenter Server 图形用户界面内部端口。                    |
| 7080                                        | 安全令牌服务内部端口。                                   |
| 7081                                        | Platform Services Controller 内部端口。            |
| 8000                                        | ESXi Dump Collector 内部端口。                     |
| 8006                                        | 用于监控 Virtual SAN 运行状况。                        |
| 8085                                        | vCenter 服务 (vpxd) SDK 使用的内部端口。                |
| 8095                                        | VMware vCenter 服务源端口。                         |
| 8098,<br>8099                               | 由 VMware Image Builder Manager 使用。            |
| 8190,<br>8191,<br>22000,<br>22100,<br>21100 | VMware vSphere Profile-Driven Storage Service |
| 8200,<br>8201,<br>5480                      | 设备管理内部端口。                                     |
| 8300,<br>8301                               | 设备管理保留端口。                                     |
| 8900                                        | 监控 API 内部端口。                                  |
| 9090                                        | vSphere Web Client 内部端口。                      |
| 10080                                       | Inventory Service 内部端口。                       |
| 10201                                       | Message Bus Configuration Service 内部端口。       |
| 11080                                       | 用于 HTTP 和开机画面的 vCenter Server Appliance 内部端口。 |
| 12721                                       | 安全令牌服务内部端口。                                   |
| 12080                                       | License Service 内部端口。                         |
| 12346,<br>12347,<br>4298                    | 用于 VMware vSphere Management SDK (vAPI) 的内部端口 |
| 13080,<br>6070                              | 由性能图表服务内部使用。                                  |

**表 4-3** vCenter Server TCP 和 UDP 端口（续）

| 端口              | 描述                      |
|-----------------|-------------------------|
| 14080           | 由 syslog 服务内部使用。        |
| 15005,<br>15006 | ESX Agent Manager 内部端口。 |
| 16666,<br>16667 | 内容库端口                   |
| 18090           | 内容管理器内部端口。              |
| 18091           | Component Manager 内部端口。 |

## 确保虚拟机安全

---

在虚拟机中运行的客户机操作系统会与物理系统一样遭遇相同的安全风险。请确保虚拟机与物理机一样安全，并遵循本文档和**强化指南**中介绍的最佳做法。

本章讨论了以下主题：

- [第 95 页](#)，“为虚拟机启用或禁用 UEFI 安全引导”
- [第 96 页](#)，“限制信息性消息从虚拟机流向 VMX 文件”
- [第 97 页](#)，“防止虚拟磁盘压缩”
- [第 97 页](#)，“虚拟机安全性最佳做法”

### 为虚拟机启用或禁用 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启用安全引导的方式来启用安全引导。

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（包括安全引导撤销列表）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，然后再启动安全引导。

---

**注意** 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。

---

## 前提条件

只有在满足所有必备条件的情况下，才能启用安全引导。如果不满足必备条件，则 vSphere Web 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。有关最新信息，请参见 *VMware 兼容性指南*。

---

**注意** 不能将使用 BIOS 引导的虚拟机升级到使用 UEFI 引导的虚拟机。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，则可以对该虚拟机启用安全引导。

---

- 关闭虚拟机。如果虚拟机正在运行，则该复选框将灰显。

要对虚拟机启用或禁用 UEFI 安全引导，您需要拥有**虚拟机.配置.设置**特权。

## 步骤

- 1 登录到 vSphere Web Client，然后选择虚拟机。
- 2 在**编辑设置**对话框中，打开**引导选项**，并确保固件设置为 **EFI**。
- 3 单击**启用安全引导**复选框，然后单击**确定**。
- 4 如果以后要禁用安全引导，可以再次单击该复选框。

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器并造成拒绝服务 (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器容量时，会造成 DoS 问题。

虚拟机配置文件（VMX 文件）的限制默认为 1 MB。此容量通常情况下足够使用，但是您可以根据需要更改此值。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。

---

**注意** 请仔细考量所需要的信息量。如果信息量超过数据存储器容量，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 使用 vSphere Web Client 登录到 vCenter Server 系统，然后查找虚拟机。
  - a 在导航器中，选择**虚拟机和模板**。
  - b 在层次结构中查找虚拟机。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 选择**虚拟机选项**。
- 4 单击**高级**，然后单击**编辑配置**。
- 5 添加或编辑 `tools.setInfo.sizeLimit` 参数。



## 防止虚拟磁盘压缩

客户机操作系统中的非管理用户能够压缩虚拟磁盘。压缩虚拟磁盘将回收未使用的磁盘空间。但是，如果重复压缩虚拟磁盘，磁盘会变得不可用且造成拒绝服务。为了避免这种情况，请禁用压缩虚拟磁盘的功能。

### 前提条件

- 关闭虚拟机。
- 验证您是否对虚拟机拥有 root 或管理员特权。

### 步骤

- 1 使用 vSphere Web Client 登录到 vCenter Server 系统，然后查找虚拟机。
  - a 在导航器中，选择**虚拟机和模板**。
  - b 在层次结构中查找虚拟机。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 选择**虚拟机选项**。
- 4 单击**高级**，然后单击**编辑配置**。
- 5 添加或编辑以下参数。

| 名称                                        | 值    |
|-------------------------------------------|------|
| <b>isolation.tools.diskWiper.disable</b>  | TRUE |
| <b>isolation.tools.diskShrink.disable</b> | TRUE |

- 6 单击**确定**。

如果禁用此功能，当数据存储空间不足时您将无法压缩虚拟机磁盘。

## 虚拟机安全性最佳做法

遵循虚拟机安全性最佳做法有助于确保 vSphere 部署的完整性。

- [虚拟机常规保护](#)第 98 页，  
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](#)第 98 页，  
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](#)第 98 页，  
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](#)第 99 页，  
当一个虚拟机消耗过多主机资源而使主机上的其他虚拟机无法执行其预期功能时，可能会出现拒绝服务 (DoS)。为防止虚拟机造成 DoS 问题，请使用主机资源管理功能（例如设置份额和使用资源池）。
- [禁用虚拟机中不必要的功能](#)第 99 页，  
虚拟机中运行的任何服务都有可能引发攻击。通过禁用支持系统上运行的应用程序或服务非必需的系统组件，可以降低这种风险。

## 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：

### 修补程序及其他保护措施

保持所有安全措施最新，包括应用适当的修补程序。跟踪已关闭电源的休眠虚拟机中的更新特别重要，因为这些虚拟机常常会被忽略。例如，确保对您虚拟基础架构中的每台虚拟机均启用防病毒软件、防间谍软件、入侵检测及其他保护措施。还应确保您具有足够的空间来存储虚拟机日志。

### 防病毒扫描

由于每台虚拟机都承载着标准操作系统，因此必须安装防病毒软件，使其免遭病毒感染。根据虚拟机的使用方式，可能还需要安装软件防火墙。

请错开病毒扫描的调度，尤其是在具有大量虚拟机的部署中。如果同时扫描所有虚拟机，环境中的系统性能将大幅下降。因为软件防火墙和防病毒软件需要占用大量虚拟化资源，因此您可以根据虚拟机性能平衡这两个安全措施的需求，尤其是在您确信虚拟机处于充分可信的环境中时。

### 串行端口

串行端口是用于将外围设备连接到虚拟机的接口。串行端口通常用于物理系统上，以提供与服务器控制台的直接、低级别连接，且虚拟串行端口允许对虚拟机进行相同的访问。串行端口允许低级别访问，此类访问通常没有诸如登录或特权之类的严格控制。

## 使用模板来部署虚拟机

在虚拟机上手动安装客户机操作系统和应用程序时，会带来配置错误的风险。通过使用模板捕捉未安装任何应用程序的强化基础操作系统映像，可以确保通过已知的安全基准级别创建所有虚拟机。

您可以使用包含已强化、修补且正确配置的操作系统的模板来创建其他特定于应用程序的模板，也可以使用应用程序模板来部署虚拟机。

### 步骤

- ◆ 提供模板来创建虚拟机，模板中包含强化、修补且正确配置的操作系统的部署。

如果可能，还可在模板中部署应用程序。确保应用程序不依赖于特定于要部署的虚拟机的信息。

### 下一步

有关模板的详细信息，请参见 *vSphere 虚拟机管理* 文档。

## 尽量少用虚拟机控制台

虚拟机控制台为虚拟机提供的功能与物理服务器上的监视器相同。具有虚拟机控制台访问权限的用户可以访问虚拟机电源管理和可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。

## 防止虚拟机取代资源

当一个虚拟机消耗过多主机资源而使主机上的其他虚拟机无法执行其预期功能时，可能会出现拒绝服务 (DoS)。为防止虚拟机造成 DoS 问题，请使用主机资源管理功能（例如设置份额和使用资源池）。

默认情况下，ESXi 主机上的所有虚拟机平均共享资源。可以使用份额和资源池以防止出现拒绝服务攻击，从而导致一个虚拟机消耗过多主机资源，使同一主机上的其他虚拟机无法执行其预期功能。

除非完全了解有关影响，否则不要使用限制。

### 步骤

- 1 为每个虚拟机置备刚好足以正常运行的资源（CPU 和内存）。
  - 2 使用“份额”保证资源分配给关键的虚拟机。
  - 3 将具有类似要求的虚拟机分组到资源池。
  - 4 在每个资源池中，保持将“份额”设置为默认值，以确保池中的每个虚拟机获得大致相同的资源优先级。
- 使用此设置，单个虚拟机无法使用比资源池中其他虚拟机更多的资源。

### 下一步

有关共享和限制的信息，请参见 *vSphere 资源管理* 文档。

## 禁用虚拟机中不必要的功能

虚拟机中运行的任何服务都有可能引发攻击。通过禁用支持系统上运行的应用程序或服务非必需的系统组件，可以降低这种风险。

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。

### 步骤

- 禁用操作系统中未使用的服务。  
例如，如果系统运行文件服务器，则应关闭所有 Web 服务。
- 断开未使用的物理设备（例如 CD/DVD 驱动器、软盘驱动器和 USB 适配器）的连接。
- 禁用未使用的功能，例如未使用的显示功能或 HGFS（主机客户机文件系统）。
- 关闭屏幕保护程序。
- 除非必要，否则不要在 Linux、BSD 或 Solaris 客户机操作系统上运行 X Window 系统。

## 移除不必要的硬件设备

启用或连接的任何设备都可能成为攻击渠道。虚拟机上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任何媒体上的敏感信息。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。
- 从虚拟机中禁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 使用 vSphere Web Client 登录到 vCenter Server 系统。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 禁用不需要的硬件设备。

包括检查以下设备：

- 软盘驱动器
- 串行端口
- 并行端口
- USB 控制器
- CD-ROM 驱动器

**禁用未使用的显示功能**

攻击者可以使用未使用的显示功能作为将恶意代码插入环境的向量。禁用环境中未使用的功能。

**步骤**

- 1 使用 vSphere Web Client 登录到 vCenter Server 系统，然后查找虚拟机。
  - a 在导航器中，选择**虚拟机和模板**。
  - b 在层次结构中查找虚拟机。
- 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                                                                                                              |
|---------------------|-----------------------------------------------------------------------------------------------------------------|
| <b>svga.vgaonly</b> | 如果将此参数设置为 TRUE，则高级图形功能将不再运行。仅字符单元控制台模式可用。如果使用此设置，则 <b>mks.enable3d</b> 不起作用。<br><b>注意</b> 将此设置仅应用到不需要虚拟化显卡的虚拟机。 |
| <b>mks.enable3d</b> | 在不需要 3D 功能的虚拟机上将此参数设置为 FALSE。                                                                                   |

**禁用未公开的功能**

VMware 虚拟机可以在 vSphere 环境中托管虚拟平台上运行，如 VMware Workstation 和 VMware Fusion。在 vSphere 环境中运行虚拟机时，无需启用某些虚拟机参数。禁用这些参数可降低出现漏洞的风险。

**前提条件**

关闭虚拟机。

**步骤**

- 1 使用 vSphere Web Client 登录到 vCenter Server 系统，然后查找虚拟机。
  - a 在导航器中，选择**虚拟机和模板**。
  - b 在层次结构中查找虚拟机。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 选择**虚拟机选项**。

- 4 单击**高级**，然后单击**编辑配置**。
- 5 添加或编辑以下参数以将其设置为 TRUE。
  - `isolation.tools.unity.push.update.disable`
  - `isolation.tools.ghi.launchmenu.change`
  - `isolation.tools.memSchedFakeSampleStats.disable`
  - `isolation.tools.getCreds.disable`
  - `isolation.tools.ghi.autologon.disable`
  - `isolation.bios.bbs.disable`
  - `isolation.tools.hgfsServerSet.disable`
- 6 单击**确定**。

## 禁用 HGFS 文件传输

某些操作（如 VMware Tools 自动升级）使用虚拟化管理程序中名为主机客户机文件系统 (HGFS) 的组件。在高安全性环境中，您可以禁用此组件以将攻击者可能使用 HGFS 在客户机操作系统中传输文件的风险降到最低。

### 步骤

- 1 使用 vSphere Web Client 登录到 vCenter Server 系统，然后查找虚拟机。
  - a 在导航器中，选择**虚拟机和模板**。
  - b 在层次结构中查找虚拟机。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 选择**虚拟机选项**。
- 4 单击**高级**，然后单击**编辑配置**。
- 5 验证 `isolation.tools.hgfsServerSet.disable` 参数是否已设置为 TRUE。

如果更改此值，VMX 进程将不再响应 Tools 进程的命令。使用 HGFS 将文件传入和传出客户机操作系统的 API（例如某些 VIX 命令或 VMware Tools auto-upgrade 实用程序）将不再运行。

## 禁用客户机操作系统和远程控制台之间的复制和粘贴操作

默认情况下，客户机操作系统和远程控制台之间的复制和粘贴操作处于禁用状态。为了确保环境安全，请保留默认设置。如果需要复制和粘贴操作，则必须使用 vSphere Web Client 将其启用。

默认情况下，这些选项设置为建议的值。但是，如果要启用审核工具来检查设置是否正确，则必须将这些选项明确设为 true。

### 前提条件

关闭虚拟机。

### 步骤

- 1 使用 vSphere Web Client 登录到 vCenter Server 系统。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 单击**虚拟机选项**，然后单击**编辑配置**。

- 4 确保“名称”和“值”列中存在以下值，或单击**添加行**进行添加。

| 名称                                                | 建议的值 |
|---------------------------------------------------|------|
| <code>isolation.tools.copy.disable</code>         | 有效   |
| <code>isolation.tools.paste.disable</code>        | 有效   |
| <code>isolation.tools.setGUIOptions.enable</code> | 无效   |

这些选项将替代在客户机操作系统的 VMware Tools 控制面板中做出的任何设置。

- 5 单击**确定**。
- 6 （可选）如果更改了配置参数，则要重新启动虚拟机。

## 限制公开复制到剪贴板中的敏感数据

默认情况下，已禁用针对主机的复制和粘贴操作，以防止公开已复制到剪贴板中的敏感数据。

当在运行 VMware Tools 的虚拟机上启用复制和粘贴时，可以在客户机操作系统和远程控制台之间进行复制和粘贴。控制台窗口获得焦点时，虚拟机中运行的非特权用户和进程均可以访问虚拟机控制台的剪贴板。如果用户在使用控制台前将敏感信息复制到剪贴板中，就可能在无意中向虚拟机暴露敏感数据。为防止此问题，默认情况下已禁用针对客户机操作系统的复制和粘贴操作。

可以在必要时为虚拟机启用复制和粘贴操作。

## 限制用户在虚拟机中运行命令

默认情况下，具有 vCenter Server 管理员角色的用户可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**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。将禁用客户机访问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，请禁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 Web Client。
- 2 单击**系统管理**，然后选择**角色**。
- 3 单击**创建角色操作**图标，然后键入角色的名称。  
例如，键入**无客户机访问权限的管理员**。
- 4 选择**所有特权**。
- 5 通过取消选择**所有特权.虚拟机.客户机操作**，移除一组客户机操作特权。
- 6 单击**确定**。

### 下一步

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。如果不想移除设备，可以更改客户机操作系统设置，以防止虚拟机用户或进程更改设备状态。

### 前提条件

关闭虚拟机。

### 步骤

- 1 使用 vSphere Web Client 登录到 vCenter Server 系统，然后查找虚拟机。
  - a 在导航器中，选择**虚拟机和模板**。
  - b 在层次结构中查找虚拟机。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 选择**虚拟机选项**。
- 4 单击**高级**，然后单击**编辑配置**。
- 5 验证以下值是否在“名称”和“值”列中，或者单击**添加行**来添加这些值。

| 名称                                          | 值  |
|---------------------------------------------|----|
| <b>isolation.device.connectable.disable</b> | 有效 |
| <b>isolation.device.edit.disable</b>        | 有效 |

这些选项将替代在客户机操作系统的 VMware Tools 控制面板中做出的任何设置。

- 6 单击**确定**以关闭“配置参数”对话框，然后再次单击**确定**。

## 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 使用 vSphere Web Client 登录到 vCenter Server 系统，然后查找虚拟机。
  - a 在导航器中，选择**虚拟机和模板**。
  - b 在层次结构中查找虚拟机。
- 2 右键单击虚拟机，然后单击**编辑设置**。
- 3 选择**虚拟机选项**。
- 4 单击**高级**，然后单击**编辑配置**。
- 5 单击**添加行**，并在“名称”和“值”列中键入以下值。

| 列         | 值                                      |
|-----------|----------------------------------------|
| <b>名称</b> | <b>isolation.tools.setinfo.disable</b> |
| <b>值</b>  | <b>true</b>                            |

- 6 单击**确定**以关闭“配置参数”对话框，然后再次单击**确定**。

## 避免使用独立非持久磁盘

如果使用的是独立非持久磁盘，成功入侵的攻击者可以通过关机或重新启动系统来销毁计算机受到影响的证据。如果虚拟机上没有持久的活动记录，管理员可能对攻击一无所知。因此，应该避免使用独立非持久磁盘。

### 步骤

- ◆ 确保虚拟机活动已远程记录在单独的服务器（例如 syslog 服务器或等价的基于 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

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。



## 虚拟机加密

从 vSphere 6.5 开始，您可以利用虚拟机加密。加密不仅能保护虚拟机，而且还能保护虚拟机磁盘和其他文件。您可以在 vCenter Server 和密钥管理服务器 (Key Management Server, KMS) 之间设置可信连接。然后，vCenter Server 可以根据需要从 KMS 检索密钥。

您可以用不同方式管理虚拟机加密的各个方面。

- 管理与 KMS 的可信连接的设置，以及通过 vSphere Web Client 执行大多数加密工作流。
- 通过 vSphere Web Services SDK 管理部分高级功能的自动化。请参见 *vSphere Web Services SDK 编程指南* 和 *VMware vSphere API 参考*。
- 直接在 ESXi 主机上使用 `crypto-util` 命令行工具来处理某些特殊情况（例如，解密 `vm-support` 包中的核心转储）。



vSphere 虚拟机加密概览 ([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_vsphere\\_virtual\\_machine\\_encryption\\_overview](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vsphere_virtual_machine_encryption_overview))

本章讨论了以下主题：

- 第 105 页，“vSphere 虚拟机加密如何保护您的环境”
- 第 107 页，“vSphere 虚拟机加密组件”
- 第 108 页，“加密过程流”
- 第 109 页，“虚拟磁盘加密”
- 第 110 页，“加密任务的必备条件和必需特权”
- 第 111 页，“加密 vSphere vMotion”
- 第 111 页，“加密最佳做法、局限性和互操作性”

### vSphere 虚拟机加密 如何保护您的环境

利用 vSphere 虚拟机加密功能，您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。

#### 使用哪些密钥

有两种类型的密钥用于加密。

- ESXi 主机生成内部密钥并使用这些密钥加密虚拟机和磁盘。这些密钥将用作 DEK，是 XTS-AES-256 密钥。
- vCenter Server 会从 KMS 请求密钥。这些密钥将用作密钥加密密钥 (KEK)，是 AES-256 密钥。vCenter Server 仅存储每个 KEK 的 ID，但不存储密钥本身。

- 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 KMS 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。

## 哪些内容加密

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。vCenter Server 从 KMS 检索的密钥会解锁 VMX 文件中包含内部密钥和其他密钥的加密包。

如果使用 vSphere Web Client 创建加密虚拟机，所有虚拟磁盘在默认情况下都会加密。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。

---

**注意** 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。

通过 vSphere API，您可以使用新的 KEK 执行浅层重新加密操作，或者使用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。请参见第 127 页，“vSphere 虚拟机加密和核心转储”。

---

**注意** vCenter Server 系统上的核心转储未加密。请务必保护对 vCenter Server 系统的访问。

---



---

**注意** 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，请参见第 114 页，“虚拟机加密互操作性”。

---

## 哪些内容未加密

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 VMSD 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。

## 哪些用户可以执行加密操作

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。请参见第 156 页，“加密操作特权”。默认管理员系统角色包括**加密操作**特权。新的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。

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 Web Client 支持许多加密操作。对于其他任务，您可以使用 vSphere API。

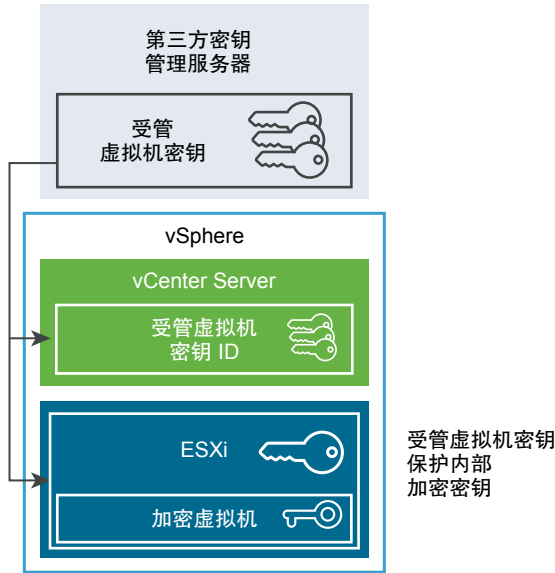
表 6-1 用于执行加密操作的界面

| 界面                       | 操作                                                                          | 信息                                                                        |
|--------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------|
| vSphere Web Client       | 创建加密虚拟机<br>加密和解密虚拟机                                                         | 本书。                                                                       |
| vSphere Web Services SDK | 创建加密虚拟机<br>加密和解密虚拟机<br>执行虚拟机的深层重新加密（使用不同的 DEK）。<br>执行虚拟机的浅层重新加密（使用不同的 KEK）。 | <i>vSphere Web Services SDK 编程指南</i><br><i>VMware vSphere API 参考</i>      |
| crypto-util              | 解密已加密核心转储、检查文件是否已加密并直接在 ESXi 主机上执行其他管理任务。                                   | 命令行帮助。<br><a href="#">第 127 页</a> ，“ <a href="#">vSphere 虚拟机加密和核心转储</a> ” |

## vSphere 虚拟机加密 组件

一个外部 KMS、vCenter Server 系统和 ESXi 主机构成了 vSphere 虚拟机加密解决方案。

图 6-1 vSphere 虚拟机加密 架构



### 密钥管理服务器

vCenter Server 将从外部 KMS 请求密钥。KMS 将生成密钥并进行存储，并将密钥传递给 vCenter Server 以进行分发。

您可以使用 vSphere Web Client 或 vSphere API 将 KMS 实例的群集添加到 vCenter Server 系统。如果在群集中使用多个 KMS 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环境中使用不同的 KMS 供应商，则可以为每个 KMS 添加 KMS 群集并指定默认 KMS 群集。所添加的第一个群集将成为默认群集。您可以在以后指定默认群集。

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 KMS。

### vCenter Server

只有 vCenter Server 具有用于登录到 KMS 的凭据。ESXi 主机不具有这些凭据。vCenter Server 将从 KMS 获取密钥，并将其推送给 ESXi 主机。vCenter Server 不会存储 KMS 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的特权。您可以使用 vSphere Web 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。请参见第 110 页，“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 Web 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 KMS 的密钥用作密钥加密密钥 (Key Encryption Key, KEK)。

## ESXi 主机

ESXi 主机负责处理加密工作流的几个方面。

- 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。当前用户的角色必须具有加密操作特权。请参见第 110 页，“加密任务的必备条件和必需特权”和第 156 页，“加密操作特权”。
- 确保在将已加密虚拟机的客户机数据存储到磁盘时对其进行加密。
- 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。

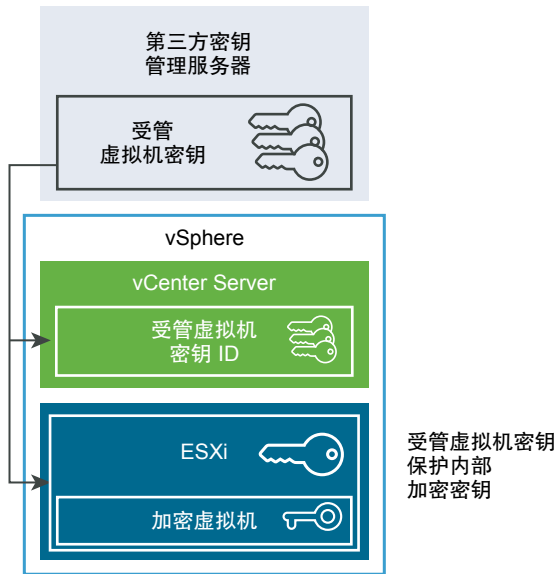
ESXi 主机生成的密钥在本文档中称为内部密钥。这些密钥通常用作数据加密密钥 (Data Encryption Key, DEK)。

## 加密过程流

vCenter Server 连接到 KMS 后，具有所需特权的用户可以创建加密虚拟机和磁盘。这些用户也可以执行其他加密任务，例如，加密现有虚拟机以及解密加密的虚拟机。

过程流包含 KMS、vCenter Server 和 ESXi 主机。

图 6-2 vSphere 虚拟机加密 架构



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 从默认 KMS 请求一个新密钥。该密钥将用作 KEK。
- 2 vCenter Server 存储该密钥 ID，并将该密钥传递给 ESXi 主机。如果 ESXi 主机是某个群集的一部分，则 vCenter Server 会将该 KEK 发送至该群集中的每一个主机。

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 KMS，所以主机将继续使用相同的 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。

如果稍后想要解密虚拟机，可以更改其存储策略。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。



加密虚拟机和磁盘 ([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_encrypting\\_vms\\_and\\_disks](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_encrypting_vms_and_disks))

## 虚拟磁盘加密

从 vSphere Web Client 创建加密虚拟机时，所有虚拟磁盘都将进行加密。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 6-2 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。<br>创建虚拟机之后，可以明确更改每个磁盘的存储策略。请参见第 126 页，“更改虚拟磁盘的加密策略”。 |
| 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）。         |
| 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。                                                                 |
| 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。                                                               |
| 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。vSphere Web Client 会显示大小和其他属性（包括加密状态），但不会显示正确的存储策略。为了确保一致性，请更改存储策略。                  |
| 将现有加密磁盘添加到未加密的虚拟机                         | 不支持此用例。                                                                                             |

## 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**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。

### 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。**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.为群集添加主机**
- **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。

为了进一步限制用户可执行的操作，您可以克隆**无加密管理员**角色，进而创建仅具有一些**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：允许用户加密但不能解密虚拟机，或者不授予管理操作特权。请参见第 25 页，“使用角色分配特权”。

### 主机加密模式

只有在为 ESXi 主机启用主机加密模式时，才能对虚拟机进行加密。通常自动启用主机加密模式，但也可以明确启用该模式。可从 vSphere Web Client 或通过 vSphere API 检查和明确设置当前主机加密模式。

有关说明，请参见第 122 页，“以显式方式启用主机加密模式”。

主机加密模式启用后，不易禁用。请参见第 123 页，“禁用主机加密模式”。

加密操作尝试启用主机加密模式时会自动更改。例如，假定您将加密虚拟机添加到独立主机，主机加密模式不会启用。如果您在主机上拥有所需的特权，则加密模式将自动更改为启用。

假设一个群集有三个 ESXi 主机，即主机 A、B 和 C。您将加密虚拟机添加到主机 A，发生的具体情况取决于几个要素。

- 如果主机 A、B 和 C 已经启用加密，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 已启用加密，而主机 C 未启用加密，则系统按照下面所述继续运行。
  - 如果您在各主机上同时拥有**加密操作.加密新项**和**加密操作.注册主机**特权，那么虚拟机创建过程在主机 C 上启用加密。加密过程在主机 C 上启用主机加密模式，并将密钥推送到群集中的各主机。  
对于这种情况，您也可以在主机 C 上明确启用主机加密。
  - 如果您对虚拟机或虚拟机文件夹只拥有**加密操作.加密新项**特权，那么虚拟机创建将成功，密钥在主机 A 和主机 B 上将变为可用。主机 C 仍然禁用加密且没有虚拟机密钥。
- 如果所有主机均未启用加密，并且您拥有**加密操作.注册主机**特权，那么虚拟机创建过程会在该主机上启用主机加密。否则，将出现错误。

### 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

从 vSphere 6.5 起，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。加密 vSphere vMotion 支持未加密虚拟机的所有 vSphere vMotion 版本，包括跨 vCenter Server 系统迁移。不支持跨 vCenter Server 系统迁移加密虚拟机。

对于加密磁盘，数据进行加密传输。对于未加密的磁盘，不支持 Storage vMotion 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。

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”。

|            |                                                                                  |
|------------|----------------------------------------------------------------------------------|
| <b>已禁用</b> | 不使用加密 vSphere vMotion。                                                           |
| <b>视情况</b> | 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。      |
| <b>必需</b>  | 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 迁移。 |

加密虚拟机时，虚拟机会记录加密 vSphere vMotion 的当前设置。如果您稍后禁用虚拟机加密，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。

有关启用和禁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。

## 加密最佳做法、局限性和互操作性

适用于物理机加密的所有最佳做法和局限性也适用于虚拟机加密。鉴于虚拟机加密架构的特点，我们额外提出一些建议。在计划您的虚拟机加密策略时，请注意互操作性方面的限制。

### 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。

#### 一般最佳做法

请遵循以下一般最佳做法以避免遇到问题。

- 不要加密任何 vCenter Server Appliance 虚拟机。
- 如果 ESXi 主机崩溃，请尽快检索支持包。如果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。如果重新引导了主机，则主机密钥可能已更改，并且您无法再生成使用密码的支持包或使用该主机密钥解密支持包中的核心转储。
- 谨慎管理 KMS 群集名称。如果已在使用的 KMS 的 KMS 群集名称发生更改，则使用此 KMS 中的密钥加密的虚拟机在打开电源或进行注册时将进入无效状态。在这种情况下，请从 vCenter Server 中移除该 KMS，然后为其添加最初使用的群集名称。
- 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。
- 加密过程在将主机上的数据写入到存储之前会对其进行加密。后端存储功能（如去重和压缩）可能对加密的虚拟机无效。使用 vSphere 虚拟机加密时会权衡考虑存储。
- 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需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，请参见第 127 页，“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 Web 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。未加密的核心转储或日志不受影响。

- 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。
- 更改主机密钥之前，请生成使用密码的 vm-support 包，以便以后可以访问任何可能已使用旧主机密钥进行加密的核心转储。

## 密钥生命周期管理最佳做法

请实施可保证 KMS 可用性并监控 KMS 上的密钥的最佳做法。

- 您需要负责实施可确保 KMS 可用性的策略。

如果 KMS 不可用，则要求 vCenter Server 从 KMS 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 KMS 解决方案都包含高可用性功能。您可以使用 vSphere Web Client 或 API 来指定密钥服务器群集和关联的 KMS 实例。

- 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，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 KMS 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 KMS 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 KMS 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》。

## 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。请参见第 114 页，“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。

## 性能最佳做法

- 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。

## 存储策略最佳做法

不要修改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。

---

**注意** 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*。

## 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，请参见第 114 页，“虚拟机加密互操作性”。

### 限制条件

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置备格式更改为精简置备格式，虚拟机磁盘将保持延迟置零厚置备格式。
- 无法使用 **编辑设置** 菜单对虚拟机及其磁盘进行加密。您必须更改存储策略。可以通过使用 **编辑设置** 菜单或更改存储策略来执行其他加密任务（例如，对已加密虚拟机的未加密磁盘进行加密）。请参见第 124 页，“加密现有虚拟机或虚拟磁盘”。
- 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，请参见第 109 页，“虚拟磁盘加密”。

- 将虚拟机移动到其他群集之前，请解密核心转储。

vCenter Server 不会存储 KMS 密钥，只会跟踪密钥 ID。因此，vCenter Server 不会持久存储 ESXi 主机密钥。

在某些情况下，例如当您 ESXi 主机移动到其他群集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。

## 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 Web 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，请参见第 126 页，“解决缺少密钥问题”。

## 虚拟机加密互操作性

在可与 vSphere 6.5 进行交互操作的设备和功能方面，vSphere 虚拟机加密 具有一些限制。

无法对已加密虚拟机执行某些任务。

- 对于大多数虚拟机加密操作，您必须关闭虚拟机的电源。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。
- 无法挂起或恢复已加密虚拟机。
- 快照操作具有一些限制。
  - 在为已加密虚拟机生成快照时，无法选中**捕获虚拟机内存**复选框。
  - 无法对具有现有快照的虚拟机进行加密。请在执行加密之前整合所有现有快照。

某些功能无法与 vSphere 虚拟机加密配合工作。

- vSphere Fault Tolerance
- 支持克隆。
  - 支持完整克隆。克隆将继承父加密状态，包括密钥。您可以重新加密完整克隆以使用新密钥，也可以解密完整克隆。
  - 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。
- vSphere ESXi Dump Collector
- 通过 vMotion 将已加密虚拟机迁移到其他 vCenter Server 实例。支持通过 vMotion 以加密方式迁移未加密虚拟机。
- vSphere Replication
- 内容库
- 并非所有使用 VMware vSphere Storage API - Data Protection (VADP) 执行虚拟磁盘备份的备份解决方案均受支持。
  - 不支持 VADP SAN 备份解决方案。
  - 如果供应商支持对在备份工作流中创建的代理虚拟机进行加密，则 VADP 热添加备份解决方案受支持。供应商必须具有**加密操作.加密虚拟机**特权。

- 支持 VADP NBD-SSL 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。
- 可以将“vSphere 虚拟机加密”与混合模式 IPv6 结合使用，但不能与纯 IPv6 环境结合使用。不支持仅使用 IPv6 地址连接到 KMS。
- 无法在其他 VMware 产品（例如 VMware Workstation）上使用“vSphere 虚拟机加密”进行加密。
- 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。

某些类型的虚拟机磁盘配置不支持 vSphere 虚拟机加密。

- VMware vSphere Flash Read Cache
- 第一类磁盘
- RDM（Raw Device Mapping，裸设备映射）
- 多写入程序或共享磁盘 (MSCS/WSFC/Oracle RAC)。如果虚拟磁盘已加密，则当您尝试在虚拟机的**编辑设置**页面中选择“多写入程序”时，**确定**按钮将处于禁用状态。



## 在 vSphere 环境中使用加密

要在 vSphere 环境中使用加密，您需要进行一些准备。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。

可以使用 API 和 `crypto-util` CLI 执行附加任务。有关该工具的详细信息，请参见 API 文档的 *vSphere Web Services SDK 编程指南* 和 `crypto-util` 命令行帮助。

本章讨论了以下主题：

- 第 117 页，“设置密钥管理服务器群集”
- 第 122 页，“创建加密存储策略”
- 第 122 页，“以显式方式启用主机加密模式”
- 第 123 页，“禁用主机加密模式”
- 第 123 页，“创建加密虚拟机”
- 第 124 页，“克隆加密虚拟机”
- 第 124 页，“加密现有虚拟机或虚拟磁盘”
- 第 125 页，“解密加密虚拟机或虚拟磁盘”
- 第 126 页，“更改虚拟磁盘的加密策略”
- 第 126 页，“解决缺少密钥问题”
- 第 127 页，“vSphere 虚拟机加密和核心转储”

### 设置密钥管理服务器群集

必须先设置密钥管理服务器 (KMS) 群集，之后才能开始执行虚拟机加密任务。此任务包括添加 KMS 以及与 KMS 建立信任。添加群集时，系统会提示您将其设为默认群集。您可以明确更改默认群集。vCenter Server 从默认群集置备密钥。

KMS 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。



虚拟机加密密钥管理服务器设置 ([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_vm\\_encryption\\_key\\_server\\_setup](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vm_encryption_key_server_setup))

## 将 KMS 添加到 vCenter Server

通过 vSphere Web Client 或使用公用 API 将 KMS 添加到您的 vCenter Server 系统。

vCenter Server 在您添加首个 KMS 实例时创建 KMS 群集。

- 添加 KMS 时，系统会提示您将此群集设置为默认群集。您稍后可以明确更改此默认群集。
- vCenter Server 创建首个群集后，您可以将同一供应商的 KMS 实例添加到该群集。
- 您可以设置只有一个 KMS 实例的群集。
- 如果您的环境支持来自不同供应商的 KMS 解决方案，则您可以添加多个 KMS 群集。
- 如果您的环境包含多个 KMS 群集，且您删除了默认群集，则您必须明确地设置默认群集。请参见第 121 页，“设置默认 KMS 群集”。

### 前提条件

- 验证密钥服务器是否在 *vSphere 兼容性列表* 中，是否与 KMIP 1.1 兼容，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**。
- 不支持仅使用 IPv6 地址连接到 KMS。

### 步骤

- 1 使用 vSphere Web Client 登录到 vCenter Server 系统。
- 2 浏览清单列表，然后选择 vCenter Server 实例。
- 3 依次单击 **配置** 和 **密钥管理服务器**。
- 4 单击 **添加 KMS**，在向导中指定 KMS 信息，然后单击 **确定**。

| 选项            | 值                                                                    |
|---------------|----------------------------------------------------------------------|
| <b>KMS 群集</b> | 选择 <b>创建新群集</b> 以创建一个新群集。如果存在一个群集，您可以选择该群集。                          |
| <b>群集名称</b>   | KMS 群集的名称。如果您的 vCenter Server 实例不可用，您可能需要此名称连接到 KMS。                 |
| <b>服务器别名</b>  | KMS 的别名。如果您的 vCenter Server 实例不可用，您可能需要此别名连接到 KMS。                   |
| <b>服务器地址</b>  | KMS 的 IP 地址或 FQDN。                                                   |
| <b>服务器端口</b>  | vCenter Server 连接到 KMS 的端口。                                          |
| <b>代理地址</b>   | 连接到 KMS 的可选代理地址。                                                     |
| <b>代理端口</b>   | 连接到 KMS 的可选代理端口。                                                     |
| <b>用户名</b>    | 一些 KMS 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 KMS 支持此功能且您准备使用时指定用户名。 |
| <b>密码</b>     | 一些 KMS 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 KMS 支持此功能且您准备使用时指定密码。  |

## 通过交换证书来建立信任连接

将 KMS 添加到 vCenter Server 系统后，可以建立信任连接。具体过程取决于 KMS 接受的证书和公司策略。

### 前提条件

添加 KMS 群集。

**步骤**

- 1 登录到 vSphere Web Client，并选择 vCenter Server 系统。
- 2 单击**配置**，然后选择**密钥管理服务器**。
- 3 选择要与之建立信任连接的 KMS 实例。
- 4 单击**与 KMS 建立信任**。
- 5 选择适用于服务器的选项，然后完成各个步骤。

| 选项                | 请参见                               |
|-------------------|-----------------------------------|
| <b>Root CA 证书</b> | 第 119 页，“使用“root CA 证书”选项建立信任连接”。 |
| <b>证书</b>         | 第 119 页，“使用“证书”选项建立信任连接”。         |
| <b>新建证书签名请求</b>   | 第 120 页，“使用“新建证书签名请求”选项建立信任连接”。   |
| <b>上载证书和私有密钥</b>  | 第 120 页，“使用“上载证书和私有密钥”选项建立信任连接”。  |

**使用“root CA 证书”选项建立信任连接**

某些 KMS 供应商（例如 SafeNet）要求将 root CA 证书上载到 KMS。随后，此 KMS 即会信任 root CA 签名的所有证书。

vSphere 虚拟机加密使用的 root 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。

**注意** 仅当要替换现有证书时才生成 root CA 证书。如果执行此操作，root 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 root CA 证书。

**步骤**

- 1 登录到 vSphere Web Client，并选择 vCenter Server 系统。
- 2 单击**配置**，然后选择**密钥管理服务器**。
- 3 选择要与之建立信任连接的 KMS 实例。
- 4 选择 **root CA 证书**，然后单击**确定**。  
“下载 root CA 证书”对话框将填充 vCenter Server 用于加密的 root 证书。此证书存储在 VECS 中。
- 5 将证书复制到剪贴板，或将证书作为文件下载。
- 6 按照您的 KMS 供应商的说明，将证书上载到其系统中。

**注意** 某些 KMS 供应商（例如 SafeNet）要求 KMS 供应商重新启动 KMS 以发现上载的 root 证书。

**下一步**

完成证书交换。请参见第 121 页，“完成信任设置”。

**使用“证书”选项建立信任连接**

某些 KMS 供应商（例如 Vormetric）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 登录到 vSphere Web Client，并选择 vCenter Server 系统。
- 2 单击**配置**，然后选择**密钥管理服务器**。
- 3 选择要与之建立信任连接的 KMS 实例。
- 4 选择**证书**，然后单击**确定**。  
“下载证书”对话框将填充 vCenter Server 用于加密的 root 证书。此证书存储在 VECS 中。

---

**注意** 除非您要替换现有证书，否则请勿生成新证书。

---

- 5 将证书复制到剪贴板，或将其作为文件下载。
- 6 按照您的 KMS 供应商的说明，将证书上传到 KMS。

**下一步**

完成信任关系。请参见第 121 页，“完成信任设置”。

**使用“新建证书签名请求”选项建立信任连接**

某些 KMS 供应商（例如 Thales）要求 vCenter Server 生成证书签名请求 (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传到 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传到 vCenter Server。

**步骤**

- 1 登录到 vSphere Web Client，并选择 vCenter Server 系统。
- 2 单击**配置**，然后选择**密钥管理服务器**。
- 3 选择要与之建立信任连接的 KMS 实例。
- 4 选择**新建证书签名请求**，然后单击**确定**。
- 5 在该对话框中，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，然后单击**确定**。  
仅当您要明确生成 CSR 时才使用该对话框中的**生成新的 CSR** 按钮。使用该选项会使基于旧 CSR 签名的任何证书变为无效。
- 6 按照 KMS 供应商的说明提交 CSR
- 7 收到来自 KMS 供应商的已签名证书时，再次单击**密钥管理服务器**，然后再次选择**新建证书签名请求**。
- 8 将已签名证书复制到底部文本框中，或单击**上传文件**并上传文件，然后单击**确定**。

**下一步**

完成信任关系。请参见第 121 页，“完成信任设置”。

**使用“上传证书和私有密钥”选项建立信任连接**

某些 KMS 供应商（例如 HyTrust）要求您将 KMS 服务器证书和私有密钥上传到 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。上传这些文件之后，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 登录到 vSphere Web Client，并选择 vCenter Server 系统。
- 2 单击**配置**，然后选择**密钥管理服务器**。
- 3 选择要与之建立信任连接的 KMS 实例。
- 4 选择**上载证书和私有密钥**，然后单击**确定**。
- 5 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。
- 6 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。
- 7 单击**确定**。

**下一步**

完成信任关系。请参见第 121 页，“完成信任设置”。

**设置默认 KMS 群集**

如果您未将第一个群集设置为默认群集，或者您的环境使用多个群集且您移除了默认群集，则必须设置默认 KMS 群集。

**前提条件**

最佳做法是，验证密钥管理服务器选项卡中的“连接状态”是否显示“正常”和一个绿色复选标记。

**步骤**

- 1 登录到 vSphere Web Client，并选择 vCenter Server 系统。
- 2 单击**配置**选项卡，然后单击**更多**下面的**密钥管理服务器**。
- 3 选择群集并单击**将 KMS 群集设置为默认值**。  
请勿选择服务器。设置默认值的菜单仅可用于群集。
- 4 单击**是**。  
相应群集名称旁将出现 **default** 字样。

**完成信任设置**

除非**添加服务器**对话框提示您信任 KMS，否则您在完成证书交换后必须以显式方式建立信任。

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**刷新 KMS 证书**选项以显式方式信任证书。
- 通过使用**上载 KMS 证书**选项，可以将 KMS 叶证书或 KMS CA 证书上载到 vCenter Server。

---

**注意** 如果上载 root 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 登录到 vSphere Web Client，并选择 vCenter Server 系统。
- 2 单击**配置**，然后选择**密钥管理服务器**。
- 3 选择要与之建立信任连接的 KMS 实例。

- 4 要建立信任关系，请刷新或上载 KMS 证书。

| 选项        | 操作                                                                                                                                              |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| 刷新 KMS 证书 | <ol style="list-style-type: none"> <li>a 单击<b>所有操作</b>，然后选择<b>刷新 KMS 证书</b>。</li> <li>b 在显示的对话框中，单击<b>信任</b>。</li> </ol>                        |
| 上载 KMS 证书 | <ol style="list-style-type: none"> <li>a 单击<b>所有操作</b>，然后选择<b>上载 KMS 证书</b>。</li> <li>b 在显示的对话框中，单击<b>上载文件</b>，上载证书文件，然后单击<b>确定</b>。</li> </ol> |

## 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 筛选器结合使用，请参见 *vSphere 存储* 文档了解详细信息。

### 前提条件

- 建立与 KMS 的连接。

尽管您可以在未建立 KMS 连接的情况下创建虚拟机加密存储策略，但是只有建立与 KMS 服务器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 Web 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**创建虚拟机存储策略**。
- 4 指定存储策略值。
  - a 输入存储策略名称和可选描述，然后单击**下一步**。
  - b 如果您对此向导不甚了解，请查看**策略结构**信息，然后单击**下一步**。
  - c 选中**使用虚拟机存储策略中的常用规则**复选框。
  - d 单击**添加组件**，选择**加密 > 默认加密属性**，然后单击**下一步**。  
 这些默认属性适用于大多数情况。仅当您希望将加密与缓存或复制等其他功能结合使用时才需要自定义策略。
  - e 取消选中**使用存储策略中的规则集**复选框，然后单击**下一步**。
  - f 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**。
  - g 检查信息，然后单击**完成**。

## 以显式方式启用主机加密模式

如果要执行加密任务，例如，在 ESXi 主机上创建加密虚拟机，必须启用主机加密模式。大多数情况下，在执行加密任务时，会自动启用主机加密模式。

在某些情况下，需要以显式方式启用加密模式。请参见第 110 页，“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 要启用主机加密模式，请执行以下步骤。
- 2 使用 vSphere Web Client 连接到 vCenter Server。
- 3 选择 ESXi 主机，然后单击**配置**。
- 4 在“系统”下，单击**安全配置文件**。
- 5 向下滚动到“主机加密模式”，然后单击**编辑**。
- 6 选择**已启用**，然后单击**确定**。

## 禁用主机加密模式

在执行加密任务时，会自动启用主机加密模式。启用主机加密模式之后，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，则可禁用加密模式。

**步骤**

- 1 从主机取消注册所有加密虚拟机
- 2 从 vCenter Server 取消注册主机。
- 3 重新引导主机。
- 4 重新向 vCenter Server 注册主机。

只要不将加密虚拟机添加到主机，就会禁用主机加密模式。

## 创建加密虚拟机

设置 KMS 后，就可以开始创建加密虚拟机。如果使用加密存储策略创建新虚拟机，则将加密新虚拟机。

**注意** 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。在可能的情况下，在创建过程中加密虚拟机。

**前提条件**

- 建立与 KMS 的可信连接并选择默认 KMS。
- 创建加密存储策略。
- 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 Web 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 主机或群集。
- 3 右键单击对象，选择**新建虚拟机** > **新建虚拟机**，并按照提示创建加密虚拟机。

| 选项              | 操作         |
|-----------------|------------|
| <b>选择创建类型</b>   | 创建虚拟机。     |
| <b>选择名称和文件夹</b> | 指定名称和目标位置。 |

| 选项               | 操作                                                          |
|------------------|-------------------------------------------------------------|
| <b>选择计算资源</b>    | 指定您拥有创建加密虚拟机特权的对象。请参见第 110 页，“加密任务的必备条件和必需特权”。              |
| <b>选择存储</b>      | 在虚拟机存储策略中，选择加密存储策略。选择兼容的数据存储。                               |
| <b>选择兼容性</b>     | 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。                     |
| <b>选择客户机操作系统</b> | 选择您计划稍后安装在虚拟机上的客户机操作系统。                                     |
| <b>自定义硬件</b>     | 自定义硬件，例如，通过更改磁盘大小或 CPU。<br>您创建的任何新硬盘都将被加密。您可以稍后更改各个硬盘的存储策略。 |
| <b>即将完成</b>      | 检查信息，然后单击 <b>完成</b> 。                                       |

## 克隆加密虚拟机

克隆加密虚拟机时，克隆将使用相同的密钥进行加密。要更改克隆的密钥，请关闭克隆的电源并使用 API 对克隆进行浅重新加密。请参见 *vSphere Web Services SDK 编程指南*。

您不需关闭虚拟机电源即可对其进行克隆。

### 前提条件

- 建立与 KMS 的可信连接并选择默认 KMS。
- 创建加密存储策略。
- 所需特权：
  - 加密操作.克隆
  - 如果未启用主机加密模式，则还必须拥有加密操作.注册主机特权。

### 步骤

- 1 使用 vSphere Web 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 主机或群集。
- 3 请右键单击虚拟机，并按照提示创建加密虚拟机的克隆。

| 选项              | 操作                                                  |
|-----------------|-----------------------------------------------------|
| <b>选择名称和文件夹</b> | 指定克隆的名称和目标位置。                                       |
| <b>选择计算资源</b>   | 指定您拥有创建加密虚拟机特权的对象。请参见第 110 页，“加密任务的必备条件和必需特权”。      |
| <b>选择存储</b>     | 在 <b>选择虚拟磁盘格式</b> 菜单中做出选择，并选择数据存储。不能在克隆操作过程中更改存储策略。 |
| <b>选择克隆选项</b>   | 按 <i>vSphere 虚拟机管理</i> 文档中的论述，选择克隆选项。               |
| <b>即将完成</b>     | 检查信息，然后单击 <b>完成</b> 。                               |

## 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。

您无法使用**编辑设置**菜单加密虚拟机。您可以使用**编辑设置**菜单对加密虚拟机的虚拟磁盘进行加密。

### 前提条件

- 建立与 KMS 的可信连接并选择默认 KMS。
- 创建加密存储策略。

- 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 Web 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 从下拉菜单选择要使用的存储策略。
  - 要加密虚拟机及其硬盘，请选择加密存储策略并单击**应用于全部**。
  - 要加密虚拟机，但不加密虚拟磁盘，请为虚拟机主页选择加密存储策略，而为虚拟磁盘选择其他存储策略，然后单击**应用**。  
您无法对未加密虚拟机的虚拟磁盘进行加密。
- 4 （可选）如果愿意，您也可以通过**编辑设置**菜单加密虚拟磁盘。
  - a 右键单击虚拟机，然后选择**编辑设置**
  - b 保持**虚拟硬件**处于选中状态。
  - c 打开您要为其更改存储策略的虚拟磁盘，然后从**虚拟机存储策略**下拉菜单选择一个选项。
  - d 单击**确定**。

## 解密加密虚拟机或虚拟磁盘

您可以通过更改虚拟机的存储策略对其解密。

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加密 VMotion，请明确地更改此设置。

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 Web 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 从下拉菜单中选择存储策略。
  - 要解密虚拟机及其硬盘，请单击**应用于全部**。
  - 要解密虚拟磁盘，而非虚拟机，请从表中下拉菜单针对虚拟磁盘选择存储策略。请勿更改虚拟机主页的策略。  
您无法解密虚拟机而让磁盘保持加密状态。
- 4 单击**确定**。

- 5 (可选) 您现在可以更改加密 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 Web Client 创建加密虚拟机时，在创建虚拟机过程中添加的所有虚拟磁盘都会被加密。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。

---

**注意** 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。

---

请参见第 109 页，“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。

### 步骤

- 1 在 vSphere Web Client 中右键单击虚拟机，然后选择**虚拟机策略 > 编辑虚拟机存储策略**。
- 2 选择要更改其存储策略的硬盘，然后选择需要的策略，例如，数据存储默认值。

## 解决缺少密钥问题

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)，您仍可以取消注册或重新加载虚拟机，但无法执行诸如删除虚拟机或打开虚拟机电源等其他虚拟机操作。虚拟机处于锁定状态。

如果虚拟机密钥不可用，vSphere Web Client 中的虚拟机状态将显示为无效，并且无法打开虚拟机电源。如果虚拟机密钥可用但加密磁盘的密钥不可用，虚拟机状态不会显示为无效，但无法打开虚拟机电源并会产生以下错误：

The disk [/path/to/the/disk.vmdk] is encrypted and no password was provided.

### 步骤

- 1 如果 vCenter Server 系统和 KMS 之间的连接有问题，请还原此连接。  
当 KMS 变为可用时，虚拟机即会解锁。
- 2 如果连接已还原但在尝试注册虚拟机时产生了错误，请确认您对 vCenter Server 系统具有**加密操作.管理密钥**特权。  
当密钥可用时，无需具有此特权便可打开加密虚拟机的电源，但是，如果需要再次检索密钥，则必须具有此特权才能注册虚拟机。
- 3 如果 KMS 上的密钥不再处于活动状态，应请求 KMS 管理员还原密钥。  
如果要打开其电源的虚拟机已从清单中移除且已很长时间未予注册，便可能会发生这种情况。如果您重新引导 ESXi 主机且 KMS 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 KMS 管理员重新激活与此密钥 ID 关联的密钥。  
如果可在 KMS 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 KMS 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，或设置与 KMS 客户端不同的 vCenter Server 系统。  
您必须使用相同的群集名称，但 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 KMS 中检索密钥，并且虚拟机将解锁。

## 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。

---

**注意** 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 主机崩溃且为该主机启用了加密模式时，将生成加密核心转储，同时主机将重新引导。核心转储将使用 ESXi 密钥缓存中的主机密钥进行加密。后续操作取决于若干因素。

- 在大多数情况下，重新引导后 vCenter Server 将从 KMS 检索主机密钥并尝试将该密钥推送到 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。请参见第 128 页，“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，您也许可以从 KMS 检索密钥。请参见第 126 页，“解决缺少密钥问题”。
- 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。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。请参见第 127 页，“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。请至少确保运行 vCenter Server 的 Windows 系统或 vCenter Server Appliance 受保护。请参见第 83 页，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 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 Web 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。

---

**注意** 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 Web Client 登录到 vCenter Server 系统。
- 2 单击**主机和群集**，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**完成**。
- 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。请遵循您组织的安全和隐私权政策，以保护主机密钥等敏感信息。

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。

---

**注意** **crypto-util** 面向高级用户。

---

**前提条件**

用于加密核心转储的 ESXi 主机密钥必须在生成核心转储的 ESXi 主机上可用。



**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，或者如果 SSH 访问已禁用，您可能需要先启用访问。

- 2 确定核心转储是否已加密。

| 选项              | 描述                                                                     |
|-----------------|------------------------------------------------------------------------|
| <b>监控程序核心转储</b> | <code>crypto-util envelope describe vmmcores.ve</code>                 |
| <b>zdump 文件</b> | <code>crypto-util envelope describe<br/>--offset 4096 zdumpFile</code> |

- 3 根据相应的类型解密核心转储。

| 选项              | 描述                                                                                          |
|-----------------|---------------------------------------------------------------------------------------------|
| <b>监控程序核心转储</b> | <code>crypto-util envelope extract vmmcores.ve vmmcores</code>                              |
| <b>zdump 文件</b> | <code>crypto-util envelope extract --offset 4096 zdumpEncrypted<br/>zdumpUnencrypted</code> |



## 确保 vSphere 网络安全

确保 vSphere 网络安全是保护环境的至关重要的一部分。可以通过不同的方式确保不同 vSphere 组件的安全。有关 vSphere 环境中的网络的详细信息，请参见 *vSphere 网络连接* 文档。

本章讨论了以下主题：

- 第 131 页，“vSphere 网络安全简介”
- 第 132 页，“使用防火墙确保网络安全”
- 第 134 页，“确保物理交换机安全”
- 第 135 页，“使用安全策略确保标准交换机端口安全”
- 第 135 页，“确保 vSphere 标准交换机的安全”
- 第 136 页，“确保 vSphere Distributed Switch 和分布式端口组的安全”
- 第 137 页，“通过 VLAN 确保虚拟机安全”
- 第 139 页，“在单台 ESXi 主机中创建多个网络”
- 第 140 页，“Internet 协议安全”
- 第 143 页，“确保 SNMP 配置正确”
- 第 144 页，“vSphere 网络连接安全性最佳做法”

### vSphere 网络安全简介

vSphere 环境中的网络安全不仅具有保护物理网络环境的特性，而且具有一些仅适用于虚拟机的特性。

#### 防火墙

为虚拟网络增加防火墙保护，方法是在其中的部分或所有虚拟机上安装和配置基于主机的防火墙。

为提高效率，可设置专用虚拟机以太网或虚拟网络。有了虚拟网络，可在网络最前面的虚拟机上安装基于主机的防火墙。此防火墙可以充当物理网络适配器和虚拟网络中剩余虚拟机之间的保护性缓存。

由于基于主机的防火墙会降低性能，因此请先根据性能目标对安全需求进行权衡，然后再决定在虚拟网络中的其他虚拟机上安装基于主机的防火墙。

请参见第 132 页，“使用防火墙确保网络安全”。

## 分段

将主机中的不同虚拟机区域置于不同网络段上。如果将每个虚拟机区域隔离在自己的网络段中，可以大大降低虚拟机区域间泄漏数据的风险。分段可防止多种威胁，包括地址解析协议 (ARP) 欺骗，即攻击者操作 ARP 表格以重新映射 MAC 和 IP 地址，从而访问进出主机的网络流量。攻击者使用 ARP 欺骗生成中间人 (MITM) 攻击、执行拒绝服务 (DoS) 攻击，劫持目标系统并以其他方式破坏虚拟网络。

仔细计划分段可降低虚拟机区域间传输数据包的几率，从而防止嗅探攻击（此类攻击需向受害者发送网络流量）。此外，攻击者无法使用一个虚拟机区域中的不安全服务访问主机中的其他虚拟机区域。可以使用两种方法之一实施分段。每种方法具有不同优势。

- 为虚拟机区域使用单独的物理网络适配器以确保将区域隔离。为虚拟机区域使用单独的物理网络适配器可能是最安全的方法，并且更不容易在初次创建段之后出现配置错误。
- 设置虚拟局域网 (VLAN) 以帮助保护网络。VLAN 几乎能够提供以物理方式实施单独网络所具有的所有安全优势，但省去了硬件开销，可为您节省部署和维护附加设备、线缆等硬件的成本，是一种可行的解决方案。请参见第 137 页，“通过 VLAN 确保虚拟机安全”。

## 阻止未授权的访问

如果将虚拟机网络连接到物理网络，则其遭到破坏的风险不亚于由物理机组成的网络。即使虚拟机网络已与任何物理网络隔离，虚拟机也可能遭到网络中其他虚拟机的攻击。用于确保虚拟机安全的要求通常与确保物理机安全的要求相同。

虚拟机是相互独立的。一个虚拟机无法读取或写入另一个虚拟机的内存、访问其数据、使用其应用程序等等。但在网络中，任何虚拟机或虚拟机组仍可能遭到其他虚拟机的未授权访问，因此可能需要通过外部手段加强保护。

## 使用防火墙确保网络安全

安全管理员使用防火墙保护网络或网络中的选定组件免遭侵袭。

防火墙可控制对其保护范围内的设备的访问，方法是关闭除管理员显式或隐式指定的授权端口之外的所有端口。管理员打开的端口允许防火墙内外设备间的流量。

---

**重要事项** ESXi 5.5 及更高版本中的 ESXi 防火墙不允许按网络筛选 vMotion 流量。因此，必须在外部防火墙上安装规则，才能确保 vMotion 套接字没有入站连接。

---

在虚拟机环境中，可以为组件之间的防火墙规划布局。

- 物理机（例如，vCenter Server 系统）和 ESXi 主机之间的防火墙。
- 一个虚拟机与另一个虚拟机之间的防火墙（例如，在作为外部 Web 服务器的虚拟机与连接到公司内部网络的虚拟机之间）。
- 物理机与虚拟机之间的防火墙（例如，在物理网络适配器卡和虚拟机之间设立防火墙）。

防火墙在 ESXi 配置中的使用方式取决于您计划如何使用网络以及给定的组件所需的安全性。例如，如果在您创建的虚拟网络中的每个虚拟机专用于运行同一部门的不同基准测试套件，那么从一个虚拟机对另一个虚拟机进行不利访问的风险极小。因此，防火墙存在于虚拟机之间的配置不是必需的。但是，为了防止干扰外部主机的测试运行，可在虚拟网络的入口点配置防火墙来保护整组虚拟机。

有关防火墙端口图，请参见 VMware 知识库文章 [2131180](#)。

## 针对具有 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 TCP 和 UDP 端口的完整列表，请参见 [第 89 页](#)，“vCenter Server 和 Platform Services Controller 所需的端口”和 [第 92 页](#)，“其他 vCenter Server TCP 和 UDP 端口”。

配置了 vCenter Server 的网络可以通过 vSphere Web 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 Web Client 或第三方网络管理客户端与 vCenter Server 之间。
- Web 浏览器与 ESXi 主机之间（如果用户通过 Web 浏览器访问虚拟机）。
- vSphere Web Client 与 ESXi 主机之间（如果用户通过 vSphere Web Client 访问虚拟机）。此连接是 vSphere Web Client 与 vCenter Server 之间连接的补充，它需要一个不同的端口。
- vCenter Server 与 ESXi 主机之间。
- 网络中的 ESXi 主机之间。尽管主机之间的流量通常被认为是可信的，但是，如果您关注计算机的安全漏洞，可在主机间添加防火墙。  
如果在 ESXi 主机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，您可以根据网络规范进行配置。

## 通过防火墙连接到 vCenter Server

默认情况下，vCenter Server 使用 TCP 端口 443 侦听其客户端的数据传输。如果 vCenter Server 及其客户端之间设有防火墙，则必须配置一个可供 vCenter Server 接收其客户端数据的连接。

在防火墙中打开 TCP 端口 443 以允许 vCenter Server 接收数据。防火墙配置取决于您的站点所用策略，有关信息，请咨询您本地的防火墙系统管理员。

如果不希望将端口 443 用作 vSphere Web Client 与 vCenter Server 之间的通信端口，可以切换到其他端口。如何打开端口取决于您使用的是 vCenter Server Appliance 还是 Windows vCenter Server。

如果仍在使用 VMware Host Client，请参见 *vSphere 单台主机管理 - VMware Host Client* 文档。

## 针对没有 vCenter Server 的配置设立防火墙

如果您的环境中不包括 vCenter Server，您可以直接将客户端连接到 ESXi 网络。

独立主机通过 VMware Host Client、任一 vSphere Command-Line Interface、vSphere Web Services SDK 或第三方客户端来接收通信。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 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 Web Client 访问权限以及防火墙命令的讨论，请参见第 52 页，[“ESXi 防火墙配置”](#)。有关端口列表，请参见第 53 页，[“ESXi 主机的入站和出站防火墙端口”](#)。

## 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 Web Client 进行连接还是通过 VMware Host Client 直接连接到 ESXi 主机。

### 通过 vSphere Web Client 连接到基于浏览器的虚拟机控制台

使用 vSphere Web Client 进行连接时，您始终连接到用于管理 ESXi 主机的 vCenter Server 系统，并从该处访问虚拟机控制台。

如果使用 vSphere Web Client 连接到基于浏览器的虚拟机控制台，则必须允许进行以下访问：

- 防火墙必须允许 vSphere Web Client 访问端口 9443 上的 vCenter Server。
- 防火墙必须允许 vCenter Server 访问端口 902 上的 ESXi 主机。

### 通过 vSphere Web Client 连接到独立虚拟机控制台

如果使用 vSphere Web Client 连接到独立虚拟机控制台，则必须允许进行以下访问：

- 防火墙必须允许 vSphere Web Client 访问端口 9443 上的 vCenter Server。
- 防火墙必须允许独立虚拟机控制台访问端口 9443 上的 vCenter Server 和端口 902 上的 ESXi 主机。

### 使用 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。

---

**注意** 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。

为了最好地保护主机，请确保物理交换机端口已配置为禁用跨树，并确保为外部物理交换机和虚拟交换机标记 (VST) 模式下的虚拟机之间的中继链接配置了非协商选项。

### 步骤

- 1 登录物理交换机并确保禁用了跨树协议，或确保为连接 ESXi 主机的所有物理交换机端口配置了 Port Fast。

- 2 对于执行桥接或路由的虚拟机，定期检查第一个上游物理交换机端口是否配置为禁用 BPDU Guard 和 Port Fast，但启用跨树协议。  
在 vSphere 5.1 及更高版本中，为了防止物理交换机受到潜在的拒绝服务 (DoS) 攻击，可以在 ESXi 主机上启动客户机 BPDU 筛选器。
- 3 登录物理交换机并确保连接 ESXi 主机的物理交换机端口上未启用动态中继协议 (DTP)。
- 4 如果物理交换机端口连接虚拟交换机 VLAN 中继端口，则定期检查物理交换机端口以确保它们被正确配置为中继端口。

## 使用安全策略确保标准交换机端口安全

就物理网络适配器而言，虚拟机网络适配器可以发送可能来自不同计算机的帧，或者模拟另一台计算机，以便能够接收针对该计算机的网络帧。同样，与物理网络适配器相同，可以对虚拟机网络适配器进行配置，以便其可以接收针对其他计算机的帧。这两种情形都具有一定的安全风险。

为网络创建标准交换机时，将在 vSphere Web Client 中添加端口组，以便为附加到该交换机上的虚拟机和 VMkernel 适配器强制执行系统流量策略。

在为标准交换机添加 VMkernel 端口组或虚拟机端口组的过程中，ESXi 会为组中的端口配置安全策略。可以使用此安全策略确保主机能防止其虚拟机的客户机操作系统模拟网络中的其他计算机。实施此安全功能的目的在于使负责模拟的客户机操作系统检测不到模拟行为已被阻止。

安全策略决定您对虚拟机执行的防模拟和截断攻击保护的强度。为了正确使用安全配置文件中的设置，必须了解虚拟机网络适配器如何控制传送及此级别的攻击如何进行。请参见 *vSphere 网络连接* 出版物中的“安全策略”部分。

.

## 确保 vSphere 标准交换机的安全

可以通过使用交换机的安全设置限制一些 MAC 地址模式来保护标准交换机流量不受第 2 层的攻击。

每个虚拟机网络适配器均包含一个初始 MAC 地址和一个有效 MAC 地址。

**初始 MAC 地址** 创建适配器时将分配初始 MAC 地址。尽管可以从客户机操作系统外部重新配置初始 MAC 地址，但不能由客户机操作系统进行更改。

**有效 MAC 地址** 每个适配器均具有一个有效 MAC 地址，可筛选与该有效 MAC 地址不同的目标 MAC 地址的入站网络流量。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。

虚拟机网络适配器一经创建后，其有效 MAC 地址与初始 MAC 地址相同。客户机操作系统可随时将有效 MAC 地址更改为其他值。如果操作系统更改了有效 MAC 地址，其网络适配器将接收传至新 MAC 地址的网络流量。

通过网络适配器发送数据包时，客户机操作系统通常将其适配器的有效 MAC 地址输入以太网帧的源 MAC 地址字段中。它还将接收网络适配器的 MAC 地址输入目标 MAC 地址字段中。接收网络适配器仅在数据包中的目标 MAC 地址与其自身有效的 MAC 地址匹配时才接受数据包。

操作系统可发送带有模拟源 MAC 地址的帧。这意味着操作系统便可通过模拟接收网络授权的网络适配器对网络中的设备进行恶意攻击。

通过在端口组或端口上配置安全策略，保护虚拟流量免受模拟和第 2 层拦截攻击。

分布式端口组和端口上的安全策略包括以下选项：

- 混杂模式（请参见第 136 页，“混杂模式运行”）
- MAC 地址更改（请参见第 136 页，“MAC 地址更改”）

- 伪信号（请参见第 136 页，“伪传输”）

您可以通过从 vSphere Web Client 选择与主机关联的虚拟交换机来查看和更改默认设置。请参见 *vSphere 网络连接文档*。

## MAC 地址更改

虚拟交换机的安全策略包括一个 **MAC 地址更改** 选项。此选项影响虚拟机接收的流量。

当 **Mac 地址更改** 选项设置为 **接受** 时，ESXi 接受将有效 MAC 地址更改为非初始 MAC 地址的其他地址的请求。

当 **Mac 地址更改** 选项设置为 **拒绝** 时，ESXi 不接受将有效 MAC 地址更改为非初始 MAC 地址的其他地址的请求。此选项可保护主机免受 MAC 模拟的威胁。虚拟机适配器用于发送请求的端口将被禁用，必须在有效 MAC 地址与初始 MAC 地址匹配后虚拟机适配器才能再接收帧。客户机操作系统检测不到 MAC 地址更改请求已被拒绝。

---

**注意** iSCSI 启动器依赖于能够从某些类型的存储器获取 MAC 地址更改。如果将 ESXi iSCSI 与 iSCSI 存储器一起使用，则将 **MAC 地址更改** 选项设置为 **接受**。

---

有时您可能确实需要多个适配器在网络中使用同一 MAC 地址（例如在单播模式中使用 Microsoft 网络负载均衡时）。在标准多播模式中使用 Microsoft 网络负载均衡时，适配器不能共享 MAC 地址。

## 伪传输

**伪信号** 选项将影响从虚拟机传输的流量。

当 **伪信号** 选项设置为 **接受** 时，ESXi 不会比较源 MAC 地址和有效 MAC 地址。

要防止 MAC 模拟，可将 **伪信号** 选项设置为 **拒绝**。这样，主机将对客户机操作系统传输的源 MAC 地址与其虚拟机适配器的有效 MAC 地址进行比较，以确认是否匹配。如果地址不匹配，ESXi 主机将丢弃数据包。

客户机操作系统检测不到其虚拟机适配器无法使用模拟 MAC 地址发送数据包。ESXi 主机在带有模拟地址的任何数据包递送之前将其截断，而客户机操作系统可能假设数据包已被丢弃。

## 混杂模式运行

混杂模式会清除虚拟机适配器执行的任何接收筛选，以便客户机操作系统接收在网络上观察到的所有流量。默认情况下，虚拟机适配器不能在混杂模式中运行。

尽管混杂模式对于跟踪网络活动很有用，但它是一种不安全的运行模式，因为混杂模式中的任何适配器均可访问数据包，即使某些数据包是否仅由特定的网络适配器接收也是如此。这意味着虚拟机中的管理员或根用户可以查看发往其他客户机或主机操作系统的流量。

---

**注意** 有时您可能确实需要将标准虚拟交换机或分布式虚拟交换机配置为在混杂模式中运行（例如运行网络入侵检测软件或数据包嗅探器时）。

---

## 确保 vSphere Distributed Switch 和分布式端口组的安全

管理员可选择多种方式来确保其 vSphere 环境中的 vSphere Distributed Switch 安全。

### 步骤

- 1 对于具有静态绑定的分布式端口组，验证已禁用了自动扩展功能。

默认情况下，自动扩展在 vSphere 5.1 及更高版本中处于启用状态。

要禁用自动扩展，请使用 vSphere Web Services SDK 或命令行界面配置分布式端口组下的 `autoExpand` 属性。请参见《*vSphere Web Services SDK*》文档。

- 2 确保已完整记录所有 vSphere Distributed Switch 的全部专用 VLAN ID。



- 3 如果您在 dvPortgroup 上使用 VLAN 标记，则 VLAN ID 必须与外部可识别 VLAN 的上游交换机上的 ID 相对应。如果未完整跟踪 VLAN ID，错误地重用 ID 可能会使不适当的物理机和虚拟机之间产生流量。同样，VLAN ID 错误或缺失可能导致无法在物理机和虚拟机之间传递流量。
- 4 确保与 vSphere Distributed Switch 关联的虚拟端口组上不存在任何未使用的端口。
- 5 标记所有 vSphere Distributed Switch。

与 ESXi 主机关联的 vSphere Distributed Switch 需要交换机名称字段。此标签可以充当交换机的功能描述符，就像与物理交换机关联的主机名称一样。vSphere Distributed Switch 上的标签表示交换机的功能或 IP 子网。例如，可以将交换机标记为内部交换机，以表示该交换机仅用于虚拟机的专用虚拟交换机之间的内部网络，并且未绑定任何物理网络适配器。

- 6 如果当前未使用 vSphere Distributed Switch 的网络健康检查功能，请禁用该功能。

默认情况下，网络健康检查功能处于禁用状态。启用后，健康检查包将包含有关攻击者可能使用的主机、交换机和端口的信息。网络健康检查功能仅用于故障排除，完成故障排除后应将其关闭。

- 7 通过在端口组或端口上配置安全策略，保护虚拟流量免受模拟和第 2 层拦截攻击。

分布式端口组和端口上的安全策略包括以下选项：

- 混杂模式（请参见第 136 页，“混杂模式运行”）
- MAC 地址更改（请参见第 136 页，“MAC 地址更改”）
- 伪信号（请参见第 136 页，“伪传输”）

您可以查看和更改当前设置，方法是从 Distributed Switch 的右键菜单中选择**管理分布式端口组**，然后在向导中选择**安全性**。请参见 *vSphere 网络连接* 文档。

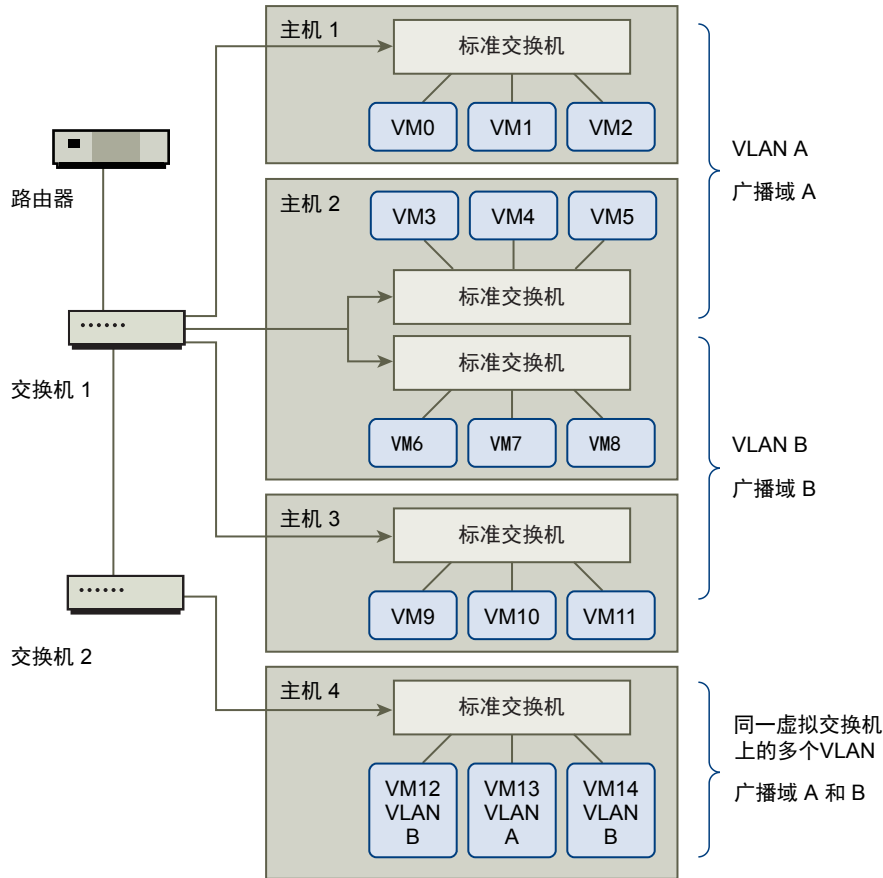
## 通过 VLAN 确保虚拟机安全

网络可能是任何系统中最脆弱的环节之一。虚拟机网络需要的保护丝毫不应少于物理网络。使用 VLAN 可以提高您的环境的网络安全性。

VLAN 是一种 IEEE 标准的网络方案，通过特定的标记方法将数据包的传送限制在 VLAN 中的端口内。若配置正确，VLAN 将是您保护一组虚拟机免遭意外或恶意侵袭的可靠方法。

VLAN 可让您对物理网络进行分段，以便只有属于相同 VLAN 的网络中的两个虚拟机才能相互传输数据包。例如，会计记录和会计帐务是一家公司最敏感的内部信息。如果公司的销售、货运和会计员工均使用同一物理网络中的虚拟机，可设置 VLAN 以保护会计部门的虚拟机。

图 8-1 VLAN 布局示例



在此配置中，会计部门的所有员工均使用 VLAN A 中的虚拟机，销售部门的员工使用 VLAN B 中的虚拟机。

路由器将包含会计数据的数据包转发至交换机。这些数据包将被标记为仅分发至 VLAN A。因此，数据将被局限在广播域 A 内，无法传送到广播域 B，除非对路由器进行此配置。

该 VLAN 配置可防止销售人员截取传至会计部门的数据包。还可防止会计部门接收传至销售组的数据包。一个虚拟交换机可为不同 VLAN 中的虚拟机服务。

## VLAN 安全注意事项

如何设置 VLAN 以确保网络组件安全取决于客户机操作系统以及网络设备的配置方式。

ESXi 配备完整的符合 IEEE 802.1q 的 VLAN 实施。VMware 不能对如何设置 VLAN 提出具体建议，但当您使用 VLAN 部署作为安全执行策略一部分时，应考虑以下因素。

## 确保 VLAN 安全

管理员可使用几个选项确保其 vSphere 环境中 VLAN 的安全。

### 步骤

- 1 确保端口组未配置为上游物理交换机预留的 VLAN 值  
请勿使用为物理交换机预留的值设置 VLAN ID。

- 2 确保端口组未配置为 VLAN 4095，除非用于虚拟客户机标记 (VGT)。

vSphere 中存在三种 VLAN 标记类型：

- 外部交换机标记 (EST)
- 虚拟交换机标记 (VST) - 虚拟交换机使用已配置的 VLAN ID 标记传入附加虚拟机的流量，并将 VLAN 标记从传出虚拟机的流量中移除。要设置 VST 模式，请分配 1 到 4095 之间的 VLAN ID。
- 虚拟客户机标记 (VGT) - 虚拟机处理 VLAN 流量。要激活 VGT 模式，请将 VLAN ID 设置为 4095。在 Distributed Switch 上，还可以使用 VLAN 中继选项允许基于 VLAN 的虚拟机流量。

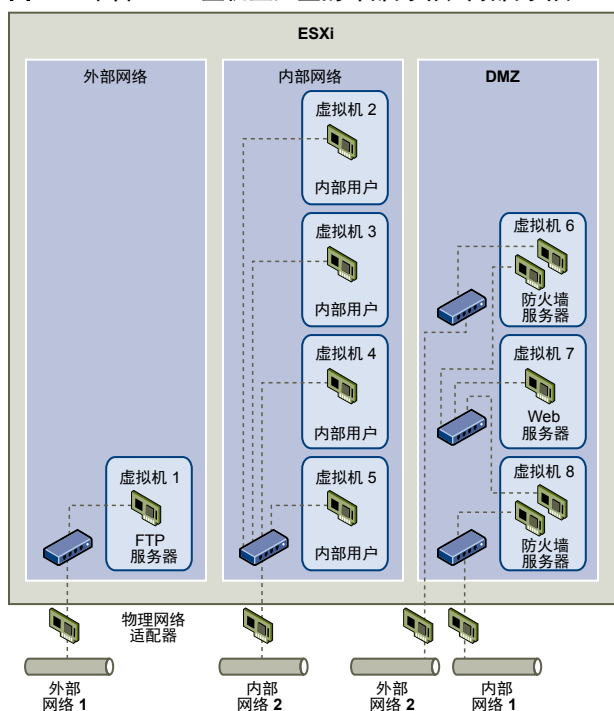
在标准交换机上，可以在交换机或端口组级别上配置 VLAN 网络连接模式，而在 Distributed Switch 上，则在分布式端口组或端口级别。

- 3 确保完全记录了每台虚拟交换机上的所有 VLAN，而且每台虚拟交换机有且仅有所需的 VLAN。

## 在单台 ESXi 主机中创建多个网络

ESXi 系统的设计可让您将一些虚拟机组连接至内部网络，并将一些虚拟机组连接至外部网络，而将另一些虚拟机组同时连接至外部和内部网络，而这一切都在同一主机上进行。此功能是由对虚拟机的基本隔离和对虚拟网络连接功能的有计划使用组合而成的。

图 8-2 单台 ESXi 主机上配置的外部网络、内部网络和 DMZ



在图中，系统管理员将主机配置到三个不同的虚拟机区域中：FTP 服务器、内部虚拟机和 DMZ。每个区域均提供唯一功能。

### FTP 服务器

虚拟机 1 是使用 FTP 软件配置的，可作为从外部资源（例如，由供应商本地化的表单和辅助材料）发出及向其发送的数据的存储区域。

此虚拟机仅与外部网络相关联。它自身拥有可用来与外部网络 1 相连接的虚拟交换机和物理网络适配器。此网络专用于公司在从外部来源接收数据时所使用的服务器。例如，公司使用外部网络 1 从供应商接收 FTP 流量，并允许供应商通过 FTP 访问存储在外部可用服务器上的数据。除了服务于虚拟机 1，外部网络 1 也服务于在整个站点内不同 ESXi 主机上配置的 FTP 服务器。

由于虚拟机 1 不与主机中的任何虚拟机共享虚拟交换机或物理网络适配器，因此，其他驻留的虚拟机无法通过虚拟机 1 网络收发数据包。此限制可防止嗅探攻击（嗅探攻击需向受害者发送网络流量）。更为重要的是，攻击者再也无法使用 FTP 固有的漏洞来访问任何主机的其他虚拟机。

### 内部虚拟机

虚拟机 2 至 5 仅供内部使用。这些虚拟机用来处理和存储公司机密数据（例如，医疗记录、法律裁决和欺诈调查）。因此，系统管理员必须确保为这些虚拟机提供最高级别的保护。

这些虚拟机通过其自身的虚拟交换机和网络适配器连接到内部网络 2。内部网络 2 仅供内部人员使用（例如，索赔专员、内部律师或调解员）。

虚拟机 2 至 5 可通过虚拟交换机与另一个虚拟机进行通信，也可通过物理网络适配器与内部网络 2 上其他位置的内部虚拟机进行通信。它们不能与对外计算机进行通信。如同 FTP 服务器一样，这些虚拟机不能通过其他虚拟机网络收发数据包。同样，主机的其他虚拟机不能通过虚拟机 2 至 5 收发数据包。

### DMZ

虚拟机 6 至 8 配置为可供营销小组用于发布公司外部网站的 DMZ。

这组虚拟机与外部网络 2 和内部网络 1 相关联。公司使用外部网络 2 来支持营销部门和财务部门用来托管公司网站的 Web 服务器及公司为外部用户托管的其他 Web 设施。内部网络 1 是营销部门用于向公司网站发布内容、张贴下载内容及维护服务（例如，用户论坛）的媒介。

由于这些网络与外部网络 1 和内部网络 2 相隔离，因此虚拟机无任何共享联络点（交换机或适配器），FTP 服务器或内部虚拟机组也不存在任何攻击风险。

通过利用虚拟机隔离、正确配置虚拟交换机及维护网络独立，系统管理员可在同一 ESXi 主机上容纳所有三个虚拟机区域，并完全不用担心数据或资源流失。

公司使用多个内部和外部网络，并确保每组的虚拟交换机和物理网络适配器与其他组的虚拟交换机和物理网络适配器完全独立，从而在虚拟机组中强制实施隔离。

由于没有任何虚拟交换机横跨虚拟机区域，因此系统管理员可成功地消除虚拟机区域之间的数据包泄漏风险。虚拟机本身无法向另一个虚拟交换机直接泄漏数据包。仅在以下情况下，数据包才会在虚拟交换机之间移动：

- 这些虚拟交换机连接到同一物理 LAN。
- 这些虚拟交换机连接到可用于传输数据包的公用虚拟机。

这些条件均未出现在样本配置中。如果系统管理员要确认不存在公用虚拟交换路径，则可通过在 vSphere Web Client 中查看网络交换机布局，以检查是否可能存在共享联系点。

为了保护虚拟机的资源，系统管理员为每台虚拟机配置了资源预留和限制，从而降低了 DoS 和 DDoS 攻击的风险。系统管理员在 DMZ 的前后端安装了软件防火墙，确保主机受到物理防火墙的保护，并配置了联网的存储器资源以使每个资源均有自己的虚拟交换机，从而为 ESXi 主机和虚拟机提供了进一步保护。

## Internet 协议安全

Internet 协议安全 (IPsec) 用于确保进出主机的 IP 通信安全。ESXi 主机支持使用 IPv6 的 IPsec。

在主机上设置 IPsec 时，可对入站和出站数据包启用身份验证和加密。对 IP 流量进行加密的时间和方式取决于如何设置系统的安全关联和安全策略。

安全关联确定系统对流量进行加密的方式。在创建安全关联时，可指定安全关联的源和目标、加密参数以及名称。

安全策略确定系统应对流量进行加密的时间。安全策略包括源和目标信息、要加密的流量的协议和方向、模式（transport 或 tunnel）以及要使用的安全关联。

列出可用的安全关联

ESXi 可提供可供安全策略使用的所有安全关联的列表。该列表包含用户创建的安全关联，以及 VMkernel 使用 Internet 密钥交换安装的任何安全关联。

可以使用 esxcli vSphere CLI 命令获取可用安全关联的列表。

步骤

- ◆ 在命令提示符下，输入命令 `esxcli network ip ipsec sa list`。

ESXi 将显示所有可用安全关联的列表。

添加 IPsec 安全关联

添加安全关联以指定关联的 IP 流量的加密参数。

可以使用 esxcli vSphere CLI 命令添加安全关联。

步骤

- ◆ 在命令提示符下输入命令 `esxcli network ip ipsec sa add` 并使用下列一个或多个选项。

| 选项                                         | 描述                                                                                                                         |
|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <code>--sa-source= 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 <code>transport</code> 或 <code>tunnel</code> 。                                                                     |
| <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 <code>hmac-sha1</code> 或 <code>hmac-sha2-256</code> 。                                                          |
| <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 0x6970763672656164796c6f676f336465736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x6970763672656164796c6f67736861316f757432
--sa-name sa1
```

## 移除 IPsec 安全关联

可以使用 ESXCLI vSphere CLI 命令移除安全关联。

### 前提条件

验证要使用的安全关联当前未在使用中。如果尝试移除正在使用中的安全关联，则移除操作将失败。

### 步骤

- ◆ 在命令提示符下，输入命令 **esxcli network ip ipsec sa remove --sa-name 安全关联名称**

## 列出可用的 IPsec 安全策略

可以使用 ESXCLI vSphere CLI 命令列出可用的安全策略。

### 步骤

- ◆ 在命令提示符下，输入命令 **esxcli network ip ipsec sp list**。

主机将显示所有可用安全策略的列表。

## 创建 IPSec 安全策略

创建安全策略可以确定何时使用在安全关联中设置的身份验证和加密参数。可以使用 ESXCLI vSphere CLI 命令添加安全策略。

### 前提条件

在创建安全策略之前，可按第 141 页，“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>■ 任意</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> |

| 选项                             | 描述                                                  |
|--------------------------------|-----------------------------------------------------|
| <code>--sp-mode= 模式</code>     | 指定模式 <code>tunnel</code> 或 <code>transport</code> 。 |
| <code>--sa-name= 安全关联名称</code> | 必需。为要使用的安全策略提供安全关联名称。                               |
| <code>--sp-name= 名称</code>     | 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=sa1
--sp-name=sp1
```

## 移除 IPsec 安全策略

可以使用 ESXCLI vSphere CLI 命令移除 ESXi 主机中的安全策略。

### 前提条件

验证要使用的安全策略当前未在使用中。如果尝试移除正在使用中的安全策略，则移除操作将失败。

### 步骤

- ◆ 在命令提示符下，输入命令 `esxcli network ip ipsec sp remove --sa-name 安全策略名称`。
- 要移除所有安全策略，请输入命令 `esxcli network ip ipsec sp remove --remove-all`。

## 确保 SNMP 配置正确

如果未正确配置 SNMP，则监控信息可能会被发送到恶意主机。然后恶意主机可能会使用此信息计划实施攻击。必须在每台 ESXi 主机上配置 SNMP。可以使用 vCLI、PowerCLI 或 vSphere Web Services SDK 进行配置。

### 步骤

- 1 运行 `esxcli system snmp get` 确定当前是否使用 SNMP。
- 2 如果您的系统确实需要 SNMP，请运行 `esxcli system snmp set --enable true` 命令确保它正在运行。
- 3 如果您的系统使用 SNMP，请参见 *监控和性能* 出版物了解 SNMP 3 的安装信息。

## vSphere 网络连接安全性最佳做法

遵循网络安全最佳做法有助于确保 vSphere 部署的完整性。

### 常规网络连接安全建议

遵循常规网络连接安全建议是确保网络环境安全的第一步。然后可以转到特殊区域，例如使用防火墙或使用 IPsec 确保网络安全。

- 如果已启用跨树，请确保为物理交换机端口配置了 **Portfast**。由于 VMware 虚拟交换机不支持 STP，连接到 ESXi 主机的物理交换机端口必须配置 **Portfast** 以避免物理交换机网络内出现循环。如果未设置 **Portfast**，则可能出现性能和连接问题。
- 确保分布式虚拟交换机的 **Netflow** 流量仅发送至授权的收集器 IP 地址。**Netflow** 导出未加密，可以包含有关虚拟网络的信息。该信息会增加被“中间人”成功攻击的潜在可能。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。物理交换机使用 VLAN 1 作为其本机 VLAN。本机 VLAN 上的帧不会标记为 1。ESXi 没有本机 VLAN。在端口组中指定了 VLAN 的帧具有标记，而在端口组中未指定 VLAN 的帧则没有标记。此配置可能会导致出现问题，因为标记为 1 的虚拟机最终会属于物理交换机的本机 VLAN。

例如，Cisco 物理交换机中 VLAN 1 上的帧没有标记，因为 VLAN 1 是该物理交换机上的本机 VLAN。但是，ESXi 主机上指定为 VLAN 1 的帧会标记为 1。因此，ESXi 主机上发往本机 VLAN 的流量无法正确路由，因为它标记为 1，而不是没有标记。物理交换机上来自本机 VLAN 的流量不可见，因为它没有标记。如果 ESXi 虚拟交换机端口组使用本机 VLAN ID，则从该端口发出的虚拟机流量对于该交换机上的本机 VLAN 不可见，因为该交换机应接收不带标记的流量。

- 确保未将端口组配置为上游物理交换机预留的 VLAN 值。物理交换机预留了某些 VLAN ID 以供内部使用，并且通常会禁止接收配置为这些值的流量。例如，Cisco Catalyst 交换机通常会预留 VLAN 1001 - 1024 和 4094。使用预留的 VLAN 可能会导致网络上出现拒绝服务问题。
- 确保未将端口组配置为 VLAN 4095（采用虚拟客户机标记 (VGT) 时除外）。将端口组设置为 VLAN 4095 会激活 VGT 模式。在此模式下，虚拟交换机会将所有网络帧传递给虚拟机，而不会修改 VLAN 标记，相反，它会将其留给虚拟机进行处理。
- 限制分布式虚拟交换机上的端口级配置替代。默认情况下，端口级配置替代处于禁用状态。如果启用了替代，则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。



## 标记网络组件

标识网络架构的不同组件非常关键，有助于确保网络发展过程中不会引入错误。

遵循以下最佳实践：

- 确保端口组配置了明确的网络标签。这些标签可以作为端口组的功能描述符，帮助您在网络愈发复杂时标识每个端口组的功能。
- 确保每个 vSphere Distributed Switch 具有明确的网络标签，可指示交换机的功能或 IP 子网。此标签可以作为交换机的功能描述符，就像物理交换机需要主机名称一样。例如，您可以将交换机标记为内部，以表示此交换机用于内部网络。无法更改标准虚拟交换机的标签。

## 记录和检查 vSphere VLAN 环境

定期检查 VLAN 环境以避免解决问题。完整记录 VLAN 环境并确保 VLAN ID 仅使用一次。您的文档可助于故障排除，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 VLAN ID

如果要在虚拟交换机上使用 VLAN 标记，则 ID 必须与外部可识别 VLAN 的上游交换机上的 ID 相对应。如果未完全跟踪 VLAN ID，则错误重用的 ID 可能允许错误物理机和虚拟机之间的流量。同样，如果 VLAN ID 错误或缺失，则在希望流量通过的物理机和虚拟机之间的流量可能被阻止。

#### 2 确保已完整记录所有分布式虚拟端口组（dvPortgroup 实例）的 VLAN ID

如果要在 dvPortgroup 上使用 VLAN 标记，则 ID 必须与外部可识别 VLAN 的上游交换机上的 ID 相对应。如果未完全跟踪 VLAN ID，则错误重用的 ID 可能允许错误物理机和虚拟机之间的流量。同样，如果 VLAN ID 错误或缺失，则在希望流量通过的物理机和虚拟机之间的流量可能被阻止。

#### 3 确保已完整记录所有分布式虚拟交换机的专用 VLAN ID

分布式虚拟交换机的专用 VLAN (PVLAN) 需要主 VLAN ID 和辅助 VLAN ID。这些 ID 必须与外部可识别 PVLAN 的上游交换机上的 ID 相对应。如果未完全跟踪 VLAN ID，则错误重用的 ID 可能允许错误物理机和虚拟机之间的流量。同样，如果 PVLAN ID 错误或缺失，则在希望流量通过的物理机和虚拟机之间的流量可能被阻止。

#### 4 验证 VLAN 中继链接只连接到充当中继链接的物理交换机端口。

在将虚拟交换机连接到 VLAN 中继端口时，必须在上行链路端口上正确配置虚拟交换机和物理交换机。如果未正确配置物理交换机，具有 VLAN 802.1q 标头的帧将被转发到不该接收这些帧的交换机。

## 采用可靠的网络隔离做法

采用可靠的网络隔离做法可显著增强 vSphere 环境的网络安全性。

### 隔离管理网络

通过 vSphere 管理网络可以访问每个组件上的 vSphere 管理界面。在管理界面上运行的服务会让攻击者有机会获得系统的访问特权。远程攻击可能从获取对本网络的访问权限开始。如果攻击者获得了对管理网络的访问权限，则会为进一步入侵提供集结基础。

通过按 ESXi 主机或群集上运行的最安全虚拟机的安全级别保护管理网络，严格控制对管理网络的访问。无论以何种方式限制管理网络，管理员都必须能够访问此网络以配置 ESXi 主机和 vCenter Server 系统。

将 vSphere 管理端口组置于通用 vSwitch 上的专用 VLAN 中。只要 vSphere 管理端口组的 VLAN 未用于生产虚拟机，就可以与生产（虚拟机）流量共享 vSwitch。确认网络段未路由到其他网络，但如果网络中存在管理相关的其他实体（例如，与 vSphere Replication 一起使用时），则可以路由到该网络。尤其要注意的是，确保不可将生产虚拟机流量路由到此网络。

可通过以下方法之一严格控制对管理功能的访问。

- 对于特别敏感的环境，可配置受控网关或其他控制方法以访问管理网络。例如，要求管理员通过 VPN 连接到管理网络，且只允许受信任的管理员访问管理网络。
- 配置运行管理客户端的跳转盒。

## 隔离存储流量

请确保隔离基于 IP 的存储流量。基于 IP 的存储包括 iSCSI 和 NFS。虚拟机可能与基于 IP 的存储配置共享虚拟交换机和 VLAN。此类型的配置可能会向未经授权的虚拟机用户公开基于 IP 的存储流量。

基于 IP 的存储通常未加密，任何可以访问此网络的人均可对其进行查看。要限制未经授权的用户查看基于 IP 的存储流量，请采用逻辑方式将基于 IP 的存储网络流量与生产流量分隔开来。在与 VMkernel 管理网络分隔开来的 VLAN 或网络段上配置基于 IP 的存储适配器，以限制未经授权的用户查看该流量。

## 隔离 vMotion 流量

vMotion 迁移信息以纯文本形式传输。可以访问此信息流经的网络的任何人均可查看此信息。潜在的攻击者可能会拦截 vMotion 流量以获取虚拟机的内存内容。攻击者还可能筹划 MiTM 攻击以在迁移期间修改有关内容。

请在隔离的网络中将 vMotion 流量与生产流量分隔开来。请将网络设置为不可路由，即确保第 3 层路由器未跨越此网络和其他网络，以防止外部对网络进行访问。

vMotion 端口组应位于通用 vSwitch 上的专用 VLAN 中。只要 vMotion 端口组的 VLAN 未用于生产虚拟机，就可以与生产（虚拟机）流量共享 vSwitch。

## 仅在需要时才在 vSphere Network Appliance API 中使用虚拟交换机

如果您未使用运用 vSphere Network Appliance API (DvFilter) 的产品，请勿将主机配置为向虚拟机发送网络信息。如果 vSphere Network Appliance API 处于启用状态，则攻击者可能会尝试将虚拟机连接到筛选器。此连接可能会提供对主机上其他虚拟机网络的访问。

如果您正在使用运用此 API 的产品，请验证是否已正确配置主机。请参见《*开发和部署 vSphere 解决方案、vService 和 ESX 代理*》中有关 DvFilter 的部分。如果您的主机设置为使用 API，请确保 Net.DVFilterBindIpAddress 参数的值与使用 API 的产品相匹配。

### 步骤

- 1 登录到 vSphere Web Client。
- 2 选择主机，然后单击**配置**。
- 3 在“系统”下，选择**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”字段中键入 **DVFilter** 以显示所有相关的参数。
- 5 确认设置。
  - 如果未使用 DvFilter 设置，请确保值为空。
  - 如果使用 DvFilter 设置，请确保该参数的值与使用 DvFilter 的产品所使用的值相匹配。

## 涉及多个 vSphere 组件的最佳做法

一些安全性最佳做法（如在环境中设置 NTP）可影响多个 vSphere 组件。在配置环境时，请考虑这些建议。

请查看第 31 页，第 3 章“确保 ESXi 主机安全”和第 95 页，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：

- 第 147 页，“同步 vSphere 网络连接上的时钟”
- 第 150 页，“存储安全性最佳做法”
- 第 152 页，“验证是否已禁止向客户机发送主机性能数据”
- 第 152 页，“为 ESXi Shell 和 vSphere Web 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 网络中的计算机上的时钟不同步，则可能无法在网络计算机之间的通信中将对时间敏感的 SSL 证书 识别为有效。

未同步的时钟可能会导致身份验证问题，从而使安装失败或使 vCenter Server Appliance vpxd 服务无法启动。

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。请参见知识库文章 <http://kb.vmware.com/kb/1318>。

要将 ESXi 时钟与 NTP 服务器同步，您可以使用 VMware Host Client。有关编辑 ESXi 主机的时间配置的信息，请参见《vSphere 单台主机管理》。

- 使 ESXi 时钟与网络时间服务器同步第 147 页，  
在安装 vCenter Server 或部署 vCenter Server Appliance 之前，请确保 vSphere 网络连接中所有计算机的时钟均已同步。
- 在 vCenter Server Appliance 中配置时间同步设置第 148 页，  
您可以在部署后更改 vCenter Server Appliance 中的时间同步设置。

### 使 ESXi 时钟与网络时间服务器同步

在安装 vCenter Server 或部署 vCenter Server Appliance 之前，请确保 vSphere 网络连接中所有计算机的时钟均已同步。

此任务将介绍如何从 VMware Host Client 设置 NTP。您可以改用 `vicfg-ntp` vCLI 命令。请参见《vSphere Command-Line Interface 参考》。

#### 步骤

- 1 启动 VMware Host Client，然后连接到 ESXi 主机。

- 2 单击**配置**。
- 3 在**系统**下，单击**时间配置**，然后单击**编辑**。
- 4 选择**使用网络时间协议 (启用 NTP 客户端)**。
- 5 在“添加 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 （可选）设置启动策略和服务状态。
- 7 单击**确定**。

此时，主机将与 NTP 服务器同步。

## 在 vCenter Server Appliance 中配置时间同步设置

您可以在部署后更改 vCenter Server Appliance 中的时间同步设置。

部署 vCenter Server Appliance 时，可以通过使用 NTP 服务器或 VMware Tools 来选择时间同步方法。如果 vSphere 网络中的时间设置发生变更，可以通过使用设备 shell 中的命令来编辑 vCenter Server Appliance 并配置时间同步设置。

启用周期性时间同步时，VMware Tools 将客户机操作系统的时间设置为与主机的时间相同。

执行时间同步之后，VMware Tools 会每分钟检查一次，以确定客户机操作系统和主机上的时钟是否仍然匹配。如果不匹配，则将同步客户机操作系统上的时钟以与主机上的时钟匹配。

本机时间同步软件（例如网络时间协议 (NTP)）通常比 VMware Tools 周期性时间同步更准确，因此成为用户的首选。您可以在 vCenter Server Appliance 中仅使用一种形式的周期性时间同步。如果您决定使用本机时间同步软件，则会禁用 vCenter Server Appliance VMware Tools 周期性时间同步，反之亦然。

### 使用 VMware Tools 时间同步

您可以将 vCenter Server Appliance 设置为使用 VMware Tools 时间同步。

#### 步骤

- 1 访问设备 shell 并以具有管理员或超级管理员角色的用户身份登录。  
具有超级管理员角色的默认用户是 **root**。
- 2 运行以下命令以启用 VMware Tools 时间同步。  

```
timesync.set --mode host
```
- 3 （可选）运行以下命令，确认您已成功应用 VMware Tools 时间同步。  

```
timesync.get
```

  
命令返回时间同步处于主机模式。

设备的时间已与 ESXi 主机的时间同步。

### 在 vCenter Server Appliance 配置中添加或替换 NTP 服务器

要设置 vCenter Server Appliance 以使用基于 NTP 的时间同步，必须将 NTP 服务器添加到 vCenter Server Appliance 配置中。

#### 步骤

- 1 访问设备 shell 并以具有管理员或超级管理员角色的用户身份登录。  
具有超级管理员角色的默认用户是 **root**。

- 2 通过运行 `ntp.server.add` 命令将 NTP 服务器添加到 vCenter Server Appliance 配置中。

例如，运行以下命令：

```
ntp.server.add --servers IP-addresses-or-host-names
```

此处，*IP-addresses-or-host-names* 是 NTP 服务器的 IP 地址或主机名的逗号分隔列表。

此命令可将 NTP 服务器添加到配置中。如果时间同步基于 NTP 服务器，则将重新启动 NTP 守护进程以重新加载新的 NTP 服务器。否则，此命令仅将新的 NTP 服务器添加到现有 NTP 配置中。

- 3 （可选）要删除旧的 NTP 服务器并将新的 NTP 服务器添加到 vCenter Server Appliance 配置中，请运行 `ntp.server.set` 命令。

例如，运行以下命令：

```
ntp.server.set --servers IP-addresses-or-host-names
```

此处，*IP-addresses-or-host-names* 是 NTP 服务器的 IP 地址或主机名的逗号分隔列表。

此命令可从配置中删除旧的 NTP 服务器，并在配置中设置输入 NTP 服务器。如果时间同步基于 NTP 服务器，则将重新启动 NTP 守护进程以重新加载新的 NTP 配置。否则，此命令仅使用您作为输入提供的服务器替换 NTP 配置中的服务器。

- 4 （可选）运行以下命令，确认您已成功应用新的 NTP 配置设置。

```
ntp.get
```

命令返回配置以进行 NTP 同步的服务器的空格分隔列表。如果已启用 NTP 同步，此命令返回 NTP 配置处于启用状态。如果已禁用 NTP 同步，此命令返回 NTP 配置处于禁用状态。

## 下一步

如果已禁用 NTP 配置，您可以将 vCenter Server Appliance 中的时间同步设置配置为基于 NTP 服务器。请参见第 149 页，“[将 vCenter Server Appliance 中的时间与 NTP 服务器同步](#)”。

## 将 vCenter Server Appliance 中的时间与 NTP 服务器同步

您可以将 vCenter Server Appliance 中的时间同步设置配置为基于 NTP 服务器。

### 前提条件

在 vCenter Server Appliance 配置中设置一个或多个网络时间协议 (NTP) 服务器。请参见第 148 页，“[在 vCenter Server Appliance 配置中添加或替换 NTP 服务器](#)”。

### 步骤

- 1 访问设备 shell 并以具有管理员或超级管理员角色的用户身份登录。

具有超级管理员角色的默认用户是 `root`。

- 2 运行以下命令以启用基于 NTP 的时间同步。

```
timesync.set --mode NTP
```

- 3 （可选）运行以下命令，确认您已成功应用 NTP 同步。

```
timesync.get
```

命令返回时间同步处于 NTP 模式。

## 存储安全性最佳做法

遵循存储安全供应商概述的存储安全性最佳做法。您也可以利用 CHAP 和双向 CHAP 确保 iSCSI 存储器的安全、屏蔽 SAN 资源并对其进行分区以及配置 NFS 4.1 的 Kerberos 凭据。

另请参见 *管理 VMware Virtual SAN* 文档。

### 确保 iSCSI 存储器安全

为主机配置的存储器可能包括一个或多个使用 iSCSI 的存储区域网络 (SAN)。在主机上配置 iSCSI 时，可采取几种措施最小化安全风险。

iSCSI 是一种使用 TCP/IP 协议通过网络端口（而不是通过直接连接 SCSI 设备）来访问 SCSI 设备和交换数据记录的方法。在 iSCSI 事务中，原始 SCSI 数据块被封装在 iSCSI 记录中并传输至请求数据的设备或用户。

iSCSI SAN 可让您有效地利用现有以太网架构为主机提供对其可动态共享的资源的访问。iSCSI SAN 可为依赖公用存储池服务多个用户的环境提供经济的存储解决方案。与任何网络系统一样，iSCSI SAN 也可能遭到安全破坏。

---

**注意** 用于确保 iSCSI SAN 安全的要求和过程与可用于主机的 iSCSI 硬件适配器和通过主机直接配置的 iSCSI 相同。

---

### 确保 iSCSI 设备安全

确保 iSCSI 设备免遭不利入侵的一种方法就是，每当主机尝试访问目标 LUN 上的数据时都要求 iSCSI 设备（或称目标）对主机（或称启动器）进行身份验证。

身份验证的目的是证明启动器具有访问目标的权利，这是在您配置身份验证时授予的权利。

对于 iSCSI，ESXi 不支持安全远程协议 (SRP) 或公用密钥身份验证方法。您只能将 Kerberos 与 NFS 4.1 配合使用。

ESXi 支持 CHAP 和双向 CHAP 身份验证。*vSphere 存储* 文档介绍了如何为 iSCSI 设备选择最佳的身份验证方法以及如何设置 CHAP。

确保 CHAP 密钥的唯一性。每个主机的双向身份验证密钥应不同；如果可能，向服务器进行身份验证的每个客户端的密钥也应不同。这将确保在单个主机受到影响时，攻击者无法创建其他任意主机并向存储设备进行身份验证。使用单个共享密钥时，如果一个主机受到影响，则可能允许攻击者向存储设备进行身份验证。

### 保护 iSCSI SAN

计划 iSCSI 配置时，应采取一些措施提高 iSCSI SAN 的整体安全。iSCSI 配置是否安全取决于 IP 网络，因此在设置网络时执行良好的安全标准可帮助保护 iSCSI 存储器。

下面是执行良好安全标准的一些具体建议。

#### 保护传输数据

iSCSI SAN 中的一个主要安全风险便是攻击者会嗅探传输的存储数据。

采取其他措施以防止攻击者能够轻易看见 iSCSI 数据。无论是 iSCSI 硬件适配器还是 ESXi iSCSI 启动器，均不会对其传输至目标和从目标接收的数据进行加密，这会造成数据更易遭到嗅探攻击。

允许虚拟机与 iSCSI 配置共享标准交换机和 VLAN 可能导致 iSCSI 流量遭到虚拟机攻击者滥用。为帮助确保入侵者无法侦听 iSCSI 传送数据，请确保任何虚拟机都无法看到 iSCSI 存储网络。

要实现这一目的，您可以这么操作：如果使用 iSCSI 硬件适配器，请确保 iSCSI 适配器和 ESXi 物理网络适配器未由于共享交换机或某种其他方式而无意地在主机外部连接。如果直接通过 ESXi 主机配置 iSCSI，可以不与虚拟机使用同一标准交换机，而改用其他标准交换机来配置 iSCSI 存储器。

除了通过提供专用标准交换机来保护 iSCSI SAN 外，还可以在 iSCSI SAN 自己的 VLAN 上对其进行配置以提高性能和安全性。将 iSCSI 配置放在单独的 VLAN 上可确保只有 iSCSI 适配器可以看到 iSCSI SAN 内的传送数据。此外，来自其他来源的网络拥堵不会影响 iSCSI 流量。

### 保护 iSCSI 端口安全

当运行 iSCSI 设备时，ESXi 不会打开任何侦听网络连接的端口。此措施可降低入侵者通过空闲端口侵入 ESXi 并控制主机的几率。因此，运行 iSCSI 不会在连接的 ESXi 端产生任何额外安全风险。

您运行的任何 iSCSI 目标设备都必须具有一个或多个打开的 TCP 端口以侦听 iSCSI 连接。如果 iSCSI 设备软件中存在任何安全漏洞，则数据遭遇的风险并非 ESXi 所造成。要降低此风险，请安装存储设备制造商提供的所有安全修补程序并对连接 iSCSI 网络的设备进行限制。

## 屏蔽 SAN 资源并对其进行分区

可以使用区域分配和 LUN 屏蔽来分隔 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 上安装的分 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 9-1 Kerberos 安全类型**

|                                |               | ESXi 6.0 | ESXi 6.5 |
|--------------------------------|---------------|----------|----------|
| 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 数据的集成校验和  | 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 数据的集成校验和  |          | 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。

## 验证是否已禁止向客户机发送主机性能数据

在安装了 VMware Tools 的 Windows 操作系统中，vSphere 会包含虚拟机性能计数器。通过性能计数器，虚拟机所有者可在客户机操作系统内进行准确的性能分析。默认情况下，vSphere 不会向客户机虚拟机公开主机信息。

默认情况下，向客户机虚拟机发送主机性能数据的功能处于禁用状态。此默认设置将阻止虚拟机获取有关物理主机的详细信息，并且在出现违反虚拟机安全的行为时，使主机数据不可用。

---

**注意** 以下步骤说明了基本过程。请考虑使用 vSphere Command-Line Interface (vCLI、PowerCLI 等) 之一在所有主机上同时执行此任务。

---

### 步骤

- 1 在托管虚拟机的 ESXi 系统上，浏览到 VMX 文件。

虚拟机配置文件位于 `/vmfs/volumes/datastore` 目录中，其中 `datastore` 是存储虚拟机文件的存储设备的名称。

- 2 在 VMX 文件中，验证是否设置了以下参数。

```
tools.guestlib.enableHostInfo=FALSE
```

- 3 保存并关闭文件。

您无法从客户机虚拟机中检索有关主机的性能信息。

## 为 ESXi Shell 和 vSphere Web Client 设置超时

要防止入侵者使用闲置会话，请务必为 ESXi Shell 和 vSphere Web Client 设置超时。

### ESXi Shell 超时

对于 ESXi Shell，您可以在 vSphere Web Client 及在直接控制台用户界面 (DCUI) 中设置以下超时。

#### 可用性超时

可用性超时设置是在启用 ESXi Shell 之后和必须登录之前，可以经过的时间量。超过超时期限之后，该服务会禁用，并且不允许用户登录。

#### 闲置超时

闲置超时是用户从闲置交互式会话注销之前可以经过的时间量。对闲置超时的更改会在下次用户登录 ESXi Shell 时应用。更改不影响现有会话。

### vSphere Web Client 超时

默认情况下，vSphere Web Client 会话会在 120 分钟后终止。您可以在 `webclient.properties` 文件中更改此默认值，如 *vCenter Server 和主机管理* 文档中所述。



## 定义的特权

---

下表列出了一些默认特权，为角色选定这些特权时，可以与用户配对，也可以将其分配给对象。此附录中的表使用 VC 表示 vCenter Server，使用 HC 表示主机客户端（一个独立的 ESXi 或 Workstation 主机）。

在设置权限时，确认对所有对象类型的每项特定操作均设置了适当的特权。除了要拥有对正待操作的对象的访问权限之外，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：

- 第 154 页，“警报特权”
- 第 155 页，“Auto Deploy 和镜像配置文件特权”
- 第 155 页，“证书特权”
- 第 155 页，“内容库特权”
- 第 156 页，“加密操作特权”
- 第 157 页，“数据中心特权”
- 第 158 页，“数据存储特权”
- 第 159 页，“数据存储群集特权”
- 第 159 页，“Distributed Switch 特权”
- 第 159 页，“ESX Agent Manager 特权”
- 第 160 页，“扩展特权”
- 第 160 页，“文件夹特权”
- 第 160 页，“全局特权”
- 第 161 页，“主机 CIM 特权”
- 第 161 页，“主机配置特权”
- 第 162 页，“主机清单”
- 第 163 页，“主机本地操作特权”
- 第 163 页，“主机 vSphere Replication 特权”
- 第 163 页，“主机配置文件特权”
- 第 164 页，“网络特权”

- 第 164 页，“性能特权”
- 第 164 页，“权限特权”
- 第 165 页，“配置文件驱动的存储特权”
- 第 165 页，“资源特权”
- 第 166 页，“已调度任务特权”
- 第 166 页，“会话特权”
- 第 166 页，“存储视图特权”
- 第 167 页，“任务特权”
- 第 167 页，“Transfer Service 特权”
- 第 167 页，“虚拟机配置特权”
- 第 168 页，“虚拟机客户机操作特权”
- 第 169 页，“虚拟机交互特权”
- 第 173 页，“虚拟机清单特权”
- 第 173 页，“虚拟机置备特权”
- 第 174 页，“虚拟机服务配置特权”
- 第 174 页，“虚拟机快照管理特权”
- 第 174 页，“虚拟机 vSphere Replication 特权”
- 第 175 页，“dvPort 组特权”
- 第 175 页，“vApp 特权”
- 第 176 页，“vServices 特权”
- 第 176 页，“vSphere 标记特权”

## 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 10-1 警报特权**

| 特权名称      | 描述                                                          | 要求         |
|-----------|-------------------------------------------------------------|------------|
| 警报.确认警报   | 允许阻止对所有已触发警报的所有警报操作。                                        | 对其定义了警报的对象 |
| 警报.创建警报   | 允许创建新警报。<br>如果通过自定义操作创建警报，则在用户创建警报时，将验证执行操作的特权。             | 对其定义了警报的对象 |
| 警报.禁用警报操作 | 允许阻止警报操作在触发警报后发生。此操作不会禁用警报。                                 | 对其定义了警报的对象 |
| 警报.修改警报   | 允许更改警报的属性。                                                  | 对其定义了警报的对象 |
| 警报.移除警报   | 允许删除警报。                                                     | 对其定义了警报的对象 |
| 警报.设置警报状态 | 允许更改所配置的事件警报的状态。状态可以更改为 <b>正常</b> 、 <b>警告</b> 或 <b>警示</b> 。 | 对其定义了警报的对象 |

## Auto Deploy 和镜像配置文件特权

Auto Deploy 特权控制可以对 Auto Deploy 规则执行不同任务的用户和可以关联主机的用户。Auto Deploy 特权还用于控制可以创建或编辑映像配置文件的用户。

下表说明了可以管理 Auto Deploy 规则和规则集的用户以及可以创建和编辑映像配置文件的用户。请参见 *vSphere 安装和设置*。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

**表 10-2** Auto Deploy 特权

| 特权名称                  | 描述                             | 要求             |
|-----------------------|--------------------------------|----------------|
| Auto Deploy.主机.管理计算机  | 允许用户运行用于关联主机与计算机的 PowerCLI 命令。 | vCenter Server |
| Auto Deploy.映像配置文件.创建 | 允许创建映像配置文件。                    | vCenter Server |
| Auto Deploy.映像配置文件.编辑 | 允许编辑映像配置文件。                    | vCenter Server |
| Auto Deploy.规则.创建     | 允许创建 Auto Deploy 规则。           | vCenter Server |
| Auto Deploy.规则.删除     | 允许删除 Auto Deploy 规则。           | vCenter Server |
| Auto Deploy.规则.编辑     | 允许编辑 Auto Deploy 规则。           | vCenter Server |
| Auto Deploy.规则集.激活    | 允许激活 Auto Deploy 规则集。          | vCenter Server |
| Auto Deploy.规则集.编辑    | 允许编辑 Auto Deploy 规则集。          | vCenter Server |

## 证书特权

证书特权控制哪些用户可以管理 ESXi 证书。

此特权决定哪些用户可以对 ESXi 主机执行证书管理。有关 vCenter Server 证书管理的信息，请参见 *Platform Services Controller 管理* 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 10-3** 主机证书特权

| 特权名称    | 描述                 | 要求             |
|---------|--------------------|----------------|
| 证书.管理证书 | 允许对 ESXi 主机进行证书管理。 | vCenter Server |

## 内容库特权

内容库可简单、有效地管理虚拟机模板和 vApp。内容库特权控制可以查看或管理内容库不同方面的用户。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-4 内容库特权

| 特权名称       | 描述                                                                                                                   | 要求                 |
|------------|----------------------------------------------------------------------------------------------------------------------|--------------------|
| 内容库.添加库项目  | 允许在库中添加项目。                                                                                                           | 库                  |
| 内容库.创建本地库  | 允许在指定的 vCenter Server 系统上创建本地库。                                                                                      | vCenter Server     |
| 内容库.创建已订阅库 | 允许创建已订阅库。                                                                                                            | vCenter Server     |
| 内容库.删除库项目  | 允许删除库项目。                                                                                                             | 库。将此权限设置为传播到所有库项目。 |
| 内容库.删除本地库  | 允许删除本地库。                                                                                                             | 库                  |
| 内容库.删除已订阅库 | 允许删除已订阅库。                                                                                                            | 库                  |
| 内容库.下载文件   | 允许从内容库下载文件。                                                                                                          | 库                  |
| 内容库.逐出库项目  | 允许逐出项目。可以缓存也可以不缓存已订阅库的内容。如果缓存内容，则可以通过逐出库项目来发布该库项目（如果您具有此特权）。                                                         | 库。将此权限设置为传播到所有库项目。 |
| 内容库.逐出已订阅库 | 允许逐出已订阅库。可以缓存也可以不缓存已订阅库的内容。如果缓存内容，则可以通过逐出库来发布该库（如果您具有此特权）。                                                           | 库                  |
| 内容库.导入存储   | 如果源文件 URL 以 ds:// 或 file:// 开头，则允许用户导入库项目。默认情况下，将禁用内容库管理员的此特权，因为从存储 URL 导入意味着导入内容，只有在需要时以及在要执行导入的用户当前存在安全问题时，才启用此特权。 | 库                  |
| 内容库.探查订阅信息 | 此特权允许解决方案用户和 API 探查远程库的订阅信息，包括 URL、SSL 证书和密码。由此产生的结构将说明订阅配置是否成功或是否存在 SSL 错误等问题。                                      | 库                  |
| 内容库.读取存储   | 允许读取内容库存储。                                                                                                           | 库                  |
| 内容库.同步库项目  | 允许同步库项目。                                                                                                             | 库。将此权限设置为传播到所有库项目。 |
| 内容库.同步已订阅库 | 允许同步已订阅库。                                                                                                            | 库                  |
| 内容库.类型自检   | 允许解决方案用户或 API 自检内容库服务的类型支持插件。                                                                                        | 库                  |
| 内容库.更新配置设置 | 允许更新配置设置。<br>没有与此特权关联的 vSphere Web Client 用户界面元素。                                                                    | 库                  |
| 内容库.更新文件   | 允许将内容上载到内容库。还允许从库项目中移除文件。                                                                                            | 库                  |
| 内容库.更新库    | 允许更新内容库。                                                                                                             | 库                  |
| 内容库.更新库项目  | 允许更新库项目。                                                                                                             | 库。将此权限设置为传播到所有库项目。 |
| 内容库.更新本地库  | 允许更新本地库。                                                                                                             | 库                  |
| 内容库.更新已订阅库 | 允许更新已订阅库的属性。                                                                                                         | 库                  |
| 内容库.查看配置设置 | 允许查看配置设置。<br>没有与此特权关联的 vSphere Web Client 用户界面元素。                                                                    | 库                  |

## 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 10-5 加密操作特权

| 特权名称         | 描述                                                                                          | 要求                         |
|--------------|---------------------------------------------------------------------------------------------|----------------------------|
| 加密操作.直接访问    | 允许用户访问加密资源。例如，用户可以导出虚拟机、拥有虚拟机的 NFC 访问权限等。                                                   | 虚拟机、主机或数据存储                |
| 加密操作.添加磁盘    | 允许用户向加密虚拟机添加磁盘。                                                                             | 虚拟机                        |
| 加密操作.克隆      | 允许用户克隆加密虚拟机。                                                                                | 虚拟机                        |
| 加密操作.解密      | 允许用户解密虚拟机或磁盘。                                                                               | 虚拟机                        |
| 加密操作.加密      | 允许用户加密虚拟机或虚拟机磁盘。                                                                            | 虚拟机                        |
| 加密操作.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                     |
| 加密操作.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    |
| 加密操作.管理密钥服务器 | 允许用户管理 vCenter Server 系统的密钥管理服务器。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。         |
| 加密操作.管理密钥    | 允许用户执行密钥管理操作。不支持通过 vSphere Web Client 执行这些操作，但可以通过使用 <code>crypto-util</code> 或 API 执行。     | vCenter Server root 文件夹    |
| 加密操作.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。不支持迁移到其他 vCenter Server 实例。 | 虚拟机                        |
| 加密操作.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                        |
| 加密操作.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                     |
| 加密操作.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），群集（对于群集中的主机） |

## 数据中心特权

数据中心特权控制在 vSphere Web Client 清单中创建和编辑数据中心的能力。

所有数据中心特权仅用于 vCenter Server。**创建数据中心**特权在数据中心文件夹或根对象上定义。所有其他数据中心特权与数据中心、数据中心文件夹或根对象配对。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-6 数据中心特权

| 特权名称            | 描述                                          | 要求          |
|-----------------|---------------------------------------------|-------------|
| 数据中心.创建数据中心     | 允许创建新数据中心。                                  | 数据中心文件夹或根对象 |
| 数据中心.移动数据中心     | 允许移动数据中心。<br>特权必须存在于源位置和目标位置。               | 数据中心、源和目标   |
| 数据中心.网络协议配置文件配置 | 允许为数据中心配置网络配置文件。                            | 数据中心        |
| 数据中心.查询 IP 池分配  | 允许 IP 地址池的配置。                               | 数据中心        |
| 数据中心.重新配置数据中心   | 允许重新配置数据中心。                                 | 数据中心        |
| 数据中心.释放 IP 分配   | 允许为数据中心发布分配的 IP 分配。                         | 数据中心        |
| 数据中心.移除数据中心     | 允许移除数据中心。<br>为了有执行此操作的权限，必须将此特权分配给该对象及其父对象。 | 数据中心加父对象    |
| 数据中心.重命名数据中心    | 允许更改数据中心的名称。                                | 数据中心        |

## 数据存储特权

数据存储特权控制在数据存储上浏览、管理和分配空间的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-7 数据存储特权

| 特权名称          | 描述                                                        | 要求            |
|---------------|-----------------------------------------------------------|---------------|
| 数据存储.分配空间     | 允许在数据存储上为虚拟机、快照、克隆或虚拟磁盘分配空间。                              | 数据存储          |
| 数据存储.浏览数据存储   | 允许浏览数据存储上的文件。                                             | 数据存储          |
| 数据存储.配置数据存储   | 允许配置数据存储。                                                 | 数据存储          |
| 数据存储.低级别文件操作  | 允许在数据存储浏览器中执行读取、写入、删除和重命名操作。                              | 数据存储          |
| 数据存储.移动数据存储   | 允许在文件夹之间移动数据存储。<br>特权必须存在于源位置和目标位置。                       | 数据存储、源位置和目标位置 |
| 数据存储.移除数据存储   | 允许移除数据存储。<br>此特权已弃用。<br>要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。 | 数据存储          |
| 数据存储.移除文件     | 允许在数据存储中删除文件。<br>此特权已弃用。分配 <b>低级别文件操作</b> 特权。             | 数据存储          |
| 数据存储.重命名数据存储  | 允许重命名数据存储。                                                | 数据存储          |
| 数据存储.更新虚拟机文件  | 允许在对数据存储进行再签名之后，更新指向数据存储中虚拟机文件的文件路径。                      | 数据存储          |
| 数据存储.更新虚拟机元数据 | 允许更新与数据存储关联的虚拟机元数据。                                       | 数据存储          |

## 数据存储群集特权

数据存储群集特权可控制数据存储群集的配置，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 10-8 数据存储群集特权**

| 特权名称            | 描述                               | 要求     |
|-----------------|----------------------------------|--------|
| 数据存储群集.配置数据存储群集 | 允许创建和配置数据存储群集设置，以实现 Storage DRS。 | 数据存储群集 |

## 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 10-9 vSphere Distributed Switch 特权**

| 特权名称                                      | 描述                                                            | 要求                 |
|-------------------------------------------|---------------------------------------------------------------|--------------------|
| Distributed Switch.创建                     | 允许创建 Distributed Switch。                                      | 数据中心、网络文件夹         |
| Distributed Switch.删除                     | 允许移除 Distributed Switch。<br>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 |
| Distributed Switch.主机操作                   | 允许更改 Distributed Switch 的主机成员。                                | Distributed Switch |
| Distributed Switch.修改                     | 允许更改 Distributed Switch 的配置。                                  | Distributed Switch |
| Distributed Switch.移动                     | 允许将 vSphere Distributed Switch 移动到其他文件夹。                      | Distributed Switch |
| Distributed Switch.Network I/O Control 操作 | 允许更改 vSphere Distributed Switch 的资源设置。                        | Distributed Switch |
| Distributed Switch.策略操作                   | 允许更改 vSphere Distributed Switch 的策略。                          | Distributed Switch |
| Distributed Switch.端口配置操作                 | 允许更改 vSphere Distributed Switch 中端口的配置。                       | Distributed Switch |
| Distributed Switch.端口设置操作                 | 允许更改 vSphere Distributed Switch 中端口的设置。                       | Distributed Switch |
| Distributed Switch.VSPAN 操作               | 允许更改 vSphere Distributed Switch 的 VSPAN 配置。                   | Distributed Switch |

## ESX Agent Manager 特权

ESX Agent Manager 特权控制与 ESX Agent Manager 和代理虚拟机相关的操作。ESX Agent Manager 这项服务允许您安装管理虚拟机，这些虚拟机与主机绑定在一起，不受用于迁移虚拟机的 VMware DRS 或其他服务的影响。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-10 ESX Agent Manager

| 特权名称                 | 描述                        | 要求  |
|----------------------|---------------------------|-----|
| ESX Agent Manager.配置 | 允许在主机或群集上部署代理虚拟机。         | 虚拟机 |
| ESX Agent Manager.修改 | 允许对代理虚拟机进行修改，如关闭电源或删除虚拟机。 | 虚拟机 |
| ESX Agent View.查看    | 允许查看代理虚拟机。                | 虚拟机 |

## 扩展特权

扩展特权控制安装和管理扩展的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-11 扩展特权

| 特权名称      | 描述            | 要求                  |
|-----------|---------------|---------------------|
| 扩展.注册扩展   | 允许注册扩展（插件）。   | Root vCenter Server |
| 扩展.取消注册扩展 | 允许取消注册扩展（插件）。 | Root vCenter Server |
| 扩展.更新扩展   | 允许更新扩展（插件）。   | Root vCenter Server |

## 文件夹特权

文件夹特权控制创建和管理文件夹的功能。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-12 文件夹特权

| 特权名称       | 描述                                            | 要求  |
|------------|-----------------------------------------------|-----|
| 文件夹.创建文件夹  | 允许创建新文件夹。                                     | 文件夹 |
| 文件夹.删除文件夹  | 允许删除文件夹。<br>要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。 | 文件夹 |
| 文件夹.移动文件夹  | 允许移动文件夹。<br>特权必须存在于源位置和目标位置。                  | 文件夹 |
| 文件夹.重命名文件夹 | 允许更改文件夹的名称。                                   | 文件夹 |

## 全局特权

全局特权控制与任务、脚本和扩展相关的全局任务。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。



表 10-13 全局特权

| 特权名称                 | 描述                                                                        | 要求                      |
|----------------------|---------------------------------------------------------------------------|-------------------------|
| 全局.充当 vCenter Server | 允许准备或启动 vMotion 发送操作或 vMotion 接收操作。                                       | Root vCenter Server     |
| 全局.取消任务              | 允许取消正在运行或已排队的任务。                                                          | 与任务相关的清单对象              |
| 全局.容量规划              | 允许使用容量规划来规划物理机到虚拟机的整合。                                                    | Root vCenter Server     |
| 全局.诊断                | 允许检索诊断文件、日志头、二进制文件或诊断捆绑包的列表。<br>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。 | Root vCenter Server     |
| 全局.禁用方法              | 允许 vCenter Server 扩展的服务器对 vCenter Server 管理的对象禁用某些操作。                     | Root vCenter Server     |
| 全局.启用方法              | 允许 vCenter Server 扩展的服务器对 vCenter Server 管理的对象启用某些操作。                     | Root vCenter Server     |
| 全局.全局标记              | 允许添加或移除全局标记。                                                              | Root 主机或 vCenter Server |
| 全局.运行状况              | 允许查看 vCenter Server 组件的健康状况。                                              | Root vCenter Server     |
| 全局.许可证               | 允许查看安装的许可证并添加或移除许可证。                                                      | Root 主机或 vCenter Server |
| 全局.记录事件              | 允许针对特定的受管实体记录用户定义的事件。                                                     | 任何对象                    |
| 全局.管理自定义属性           | 允许添加、移除或重命名自定义字段定义。                                                       | Root vCenter Server     |
| 全局.代理                | 允许访问内部接口以将端点添加到代理或从代理移除端点。                                                | Root vCenter Server     |
| 全局.脚本操作              | 允许调度与警报一起使用的脚本操作。                                                         | 任何对象                    |
| 全局.服务管理器             | 允许在 vSphere CLI 中使用 <code>resxtp</code> 命令。                               | Root 主机或 vCenter Server |
| 全局.设置自定义属性           | 允许查看、创建或移除受管对象的自定义属性。                                                     | 任何对象                    |
| 全局.设置                | 允许读取并修改运行时 vCenter Server 配置设置。                                           | Root vCenter Server     |
| 全局.系统标记              | 允许添加或移除系统标记。                                                              | Root vCenter Server     |

## 主机 CIM 特权

主机 CIM 特权控制主机健康状况监控的 CIM 使用。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-14 主机 CIM 特权

| 特权名称          | 描述                   | 要求 |
|---------------|----------------------|----|
| 主机.CIM.CIM 交互 | 允许客户端获取用于 CIM 服务的票证。 | 主机 |

## 主机配置特权

主机配置特权控制配置主机的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-15 主机配置特权

| 特权名称                    | 描述                                              | 要求 |
|-------------------------|-------------------------------------------------|----|
| 主机.配置.高级设置              | 允许设置高级主机配置选项。                                   | 主机 |
| 主机.配置.身份验证存储            | 允许配置 Active Directory 身份验证存储。                   | 主机 |
| 主机.配置.更改 PciPassthru 设置 | 允许更改主机的 PciPassthru 设置。                         | 主机 |
| 主机.配置.更改 SNMP 设置        | 允许更改主机的 SNMP 设置。                                | 主机 |
| 主机.配置.更改日期和时间设置         | 允许更改主机上的日期和时间设置。                                | 主机 |
| 主机.配置.更改设置              | 允许在 ESXi 主机上设置锁定模式。                             | 主机 |
| 主机.配置.连接                | 允许更改主机的连接状态（已连接或已断开连接）。                         | 主机 |
| 主机.配置.固件                | 允许更新 ESXi 主机的固件。                                | 主机 |
| 主机.配置.超线程               | 允许启用和禁用主机 CPU 调度程序中的超线程。                        | 主机 |
| 主机.配置.映像配置              | 允许更改与主机关联的映像。                                   |    |
| 主机.配置.维护                | 允许使主机进入和退出维护模式，以及关闭和重新启动主机。                     | 主机 |
| 主机.配置.内存配置              | 允许修改主机配置。                                       | 主机 |
| 主机.配置.网络配置              | 允许配置网络、防火墙和 vMotion 网络。                         | 主机 |
| 主机.配置.电源                | 允许配置主机电源管理设置。                                   | 主机 |
| 主机.配置.查询修补程序            | 允许查询可安装的修补程序并将修补程序安装在主机上。                       | 主机 |
| 主机.配置.安全配置文件和防火墙        | 允许配置 Internet 服务，如 SSH、Telnet、SNMP 和主机防火墙。      | 主机 |
| 主机.配置.存储分区配置            | 允许管理 VMFS 数据存储和诊断分区。具有此特权的用户可以扫描新存储设备并管理 iSCSI。 | 主机 |
| 主机.配置.系统管理              | 允许扩展以便操作主机上的文件系统。                               | 主机 |
| 主机.配置.系统资源              | 允许更新系统资源层次结构的配置。                                | 主机 |
| 主机.配置.虚拟机自动启动配置         | 允许更改单个主机上虚拟机的自动启动和自动停止顺序。                       | 主机 |

## 主机清单

主机清单特权控制向清单添加主机、向群集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群集所需的特权。

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 10-16 主机清单特权

| 特权名称            | 描述                                     | 要求    |
|-----------------|----------------------------------------|-------|
| 主机.清单.将主机添加到群集  | 允许将主机添加到现有群集。                          | 群集    |
| 主机.清单.添加独立主机    | 允许添加独立主机。                              | 主机文件夹 |
| 主机.清单.创建群集      | 允许创建新群集。                               | 主机文件夹 |
| 主机.清单.修改群集      | 允许更改群集的属性。                             | 群集    |
| 主机.清单.移动群集或独立主机 | 允许在文件夹之间移动群集或独立主机。<br>特权必须存在于源位置和目标位置。 | 群集    |

表 10-16 主机清单特权（续）

| 特权名称        | 描述                                                | 要求     |
|-------------|---------------------------------------------------|--------|
| 主机.清单.移动主机  | 允许将一组现有主机移入或移出群集。<br>特权必须存在于源位置和目标位置。             | 群集     |
| 主机.清单.移除群集  | 允许删除群集或独立主机。<br>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。 | 群集、主机  |
| 主机.清单.移除主机  | 允许移除主机。<br>要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。      | 主机加父对象 |
| 主机.清单.重命名群集 | 允许重命名群集。                                          | 群集     |

## 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 10-17 主机本地操作特权

| 特权名称                   | 描述                                   | 要求      |
|------------------------|--------------------------------------|---------|
| 主机.本地操作.将主机添加到 vCenter | 允许安装和卸载主机上的 vCenter 代理，如 vpxa 和 aam。 | Root 主机 |
| 主机.本地操作.创建虚拟机          | 允许在磁盘上从头开始创建新的虚拟机，而不在主机上注册。          | Root 主机 |
| 主机.本地操作.删除虚拟机          | 允许在磁盘上删除虚拟机。支持注册和未注册的虚拟机。            | Root 主机 |
| 主机.本地操作.管理用户组          | 允许在主机上管理本地帐户。                        | Root 主机 |
| 主机.本地操作.重新配置虚拟机        | 允许对虚拟机进行重新配置。                        | Root 主机 |

## 主机 vSphere Replication 特权

主机 vSphere Replication 特权控制 VMware vCenter Site Recovery Manager™ 对主机使用虚拟机复制。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-18 主机 vSphere Replication 特权

| 特权名称                        | 描述              | 要求 |
|-----------------------------|-----------------|----|
| 主机.vSphere Replication.管理复制 | 允许管理此主机上的虚拟机复制。 | 主机 |

## 主机配置文件特权

主机配置文件特权控制与创建和修改主机配置文件相关的操作。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

**表 10-19 主机配置文件特权**

| 特权名称      | 描述            | 要求                  |
|-----------|---------------|---------------------|
| 主机配置文件.清除 | 允许清除配置文件相关信息。 | Root vCenter Server |
| 主机配置文件.创建 | 允许创建主机配置文件。   | Root vCenter Server |
| 主机配置文件.删除 | 允许删除主机配置文件。   | Root vCenter Server |
| 主机配置文件.编辑 | 允许编辑主机配置文件。   | Root vCenter Server |
| 主机配置文件.导出 | 允许导出主机配置文件。   | Root vCenter Server |
| 主机配置文件.查看 | 允许查看主机配置文件。   | Root vCenter Server |

## 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 10-20 网络特权**

| 特权名称    | 描述                                                      | 要求     |
|---------|---------------------------------------------------------|--------|
| 网络.分配网络 | 允许将网络分配到虚拟机。                                            | 网络、虚拟机 |
| 网络.配置   | 允许配置网络。                                                 | 网络、虚拟机 |
| 网络.移动网络 | 允许在文件夹之间移动网络。<br>特权必须存在于源位置和目标位置。                       | 网络     |
| 网络.移除   | 允许移除网络。<br>此特权已弃用。<br>要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。 | 网络     |

## 性能特权

性能特权对修改性能统计信息设置进行控制。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

**表 10-21 性能特权**

| 特权名称      | 描述                    | 要求                  |
|-----------|-----------------------|---------------------|
| 性能.修改时间间隔 | 允许创建、移除和更新性能数据收集时间间隔。 | Root vCenter Server |

## 权限特权

权限特权控制角色和权限的分配。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-22 权限特权

| 特权名称        | 描述                                                                                | 要求       |
|-------------|-----------------------------------------------------------------------------------|----------|
| 权限.修改权限     | 允许为实体定义一个或多个权限规则，或者如果实体上的特定用户或组已经具有规则，则更新规则。<br>要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。 | 任何对象加父对象 |
| 权限.修改特权     | 允许修改特权的组或描述。<br>没有与此特权关联的 vSphere Web Client 用户界面元素。                              |          |
| 权限.修改角色     | 允许更新角色名称以及与角色关联的特权。                                                               | 任何对象     |
| 权限.重新指定角色权限 | 允许将某角色的所有权限重新分配给其他角色。                                                             | 任何对象     |

## 配置文件驱动的存储特权

配置文件驱动的存储特权控制与存储配置文件相关的操作。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-23 配置文件驱动的存储特权

| 特权名称                  | 描述                                    | 要求                  |
|-----------------------|---------------------------------------|---------------------|
| 配置文件驱动的存储.配置文件驱动的存储更新 | 允许对存储配置文件进行更改，如创建和更新存储功能和虚拟机存储配置文件。   | Root vCenter Server |
| 配置文件驱动的存储.配置文件驱动的存储视图 | 允许查看定义的 Storage Capabilities 和存储配置文件。 | Root vCenter Server |

## 资源特权

资源特权控制资源池的创建和管理，以及虚拟机的迁移。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-24 资源特权

| 特权名称             | 描述                                  | 要求                  |
|------------------|-------------------------------------|---------------------|
| 资源.应用建议          | 允许接受服务器提供的建议以通过 vMotion 执行迁移。       | 群集                  |
| 资源.将 vApp 分配给资源池 | 允许将 vApp 分配到资源池。                    | 资源池                 |
| 资源.将虚拟机分配给资源池    | 允许将虚拟机分配到资源池。                       | 资源池                 |
| 资源.创建资源池         | 允许创建资源池。                            | 资源池、群集              |
| 资源.迁移已关闭电源的虚拟机   | 允许将已关闭电源的虚拟机迁移到其他资源池或主机。            | 虚拟机                 |
| 资源.迁移已打开电源的虚拟机   | 允许通过 vMotion 将已打开电源的虚拟机迁移到其他资源池或主机。 |                     |
| 资源.修改资源池         | 允许更改资源池的分配。                         | 资源池                 |
| 资源.移动资源池         | 允许移动资源池。<br>特权必须存在于源位置和目标位置。        | 资源池                 |
| 资源.查询 vMotion    | 允许查询虚拟机与一组主机的一般 vMotion 兼容性。        | Root vCenter Server |

表 10-24 资源特权（续）

| 特权名称      | 描述                                            | 要求  |
|-----------|-----------------------------------------------|-----|
| 资源.移除资源池  | 允许删除资源池。<br>要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。 | 资源池 |
| 资源.重命名资源池 | 允许重命名资源池。                                     | 资源池 |

## 已调度任务特权

已调度任务特权控制已调度任务的创建、编辑和移除。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-25 已调度任务特权

| 特权名称      | 描述                                      | 要求   |
|-----------|-----------------------------------------|------|
| 调度任务.创建任务 | 允许调度任务。在调度时，需要一定的特权来执行已调度的操作。           | 任何对象 |
| 调度任务.修改任务 | 允许重新配置已调度任务的属性。                         | 任何对象 |
| 调度任务.移除任务 | 允许移除队列中的已调度任务。                          | 任何对象 |
| 调度任务.运行任务 | 允许立即运行已调度任务。<br>创建和运行已调度任务也需要执行关联操作的权限。 | 任何对象 |

## 会话特权

会话特权控制扩展打开 vCenter Server 系统上的会话的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-26 会话特权

| 特权名称       | 描述                       | 要求                  |
|------------|--------------------------|---------------------|
| 会话.模拟用户    | 允许模拟其他用户。该功能由扩展使用。       | Root vCenter Server |
| 会话.消息      | 允许在消息中设置全局日志。            | Root vCenter Server |
| 会话.验证会话    | 允许验证会话有效性。               | Root vCenter Server |
| 会话.查看和停止会话 | 允许查看会话以及强制注销一个或多个已登录的用户。 | Root vCenter Server |

## 存储视图特权

存储视图特权控制存储监控服务 API 的特权。从 vSphere 6.0 开始，存储视图已弃用，这些特权不再适用于它们。

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 10-27 存储视图特权

| 特权名称      | 描述                                                                   | 要求                  |
|-----------|----------------------------------------------------------------------|---------------------|
| 存储视图.配置服务 | 允许特权用户使用所有存储监控服务 API。对于只读存储监控服务 API 的特权，使用 <a href="#">存储视图.查看</a> 。 | Root vCenter Server |
| 存储视图.查看   | 允许特权用户使用只读存储监控服务 API。                                                | Root vCenter Server |

## 任务特权

任务特权控制扩展在 vCenter Server 上创建和更新任务的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-28 任务特权

| 特权名称    | 描述                                                     | 要求                  |
|---------|--------------------------------------------------------|---------------------|
| 任务.创建任务 | 允许扩展创建用户定义的任务。<br>没有与此特权关联的 vSphere Web Client 用户界面元素。 | Root vCenter Server |
| 任务.更新任务 | 允许扩展更新用户定义的任务。<br>没有与此特权关联的 vSphere Web Client 用户界面元素。 | Root vCenter Server |

## Transfer Service 特权

Transfer Service 特权是 VMware 的内部特权。请勿使用这些特权。

## 虚拟机配置特权

虚拟机配置特权控制配置虚拟机选项和设备的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-29 虚拟机配置特权

| 特权名称             | 描述                           | 要求  |
|------------------|------------------------------|-----|
| 虚拟机.配置.添加现有磁盘    | 允许将现有虚拟磁盘添加到虚拟机。             | 虚拟机 |
| 虚拟机.配置.添加新磁盘     | 允许创建新虚拟磁盘以添加到虚拟机。            | 虚拟机 |
| 虚拟机.配置.添加或移除设备   | 允许添加或移除任何非磁盘设备。              | 虚拟机 |
| 虚拟机.配置.高级        | 允许在虚拟机的配置文件中添加或修改高级参数。       | 虚拟机 |
| 虚拟机.配置.更改 CPU 数目 | 允许更改虚拟 CPU 的数目。              | 虚拟机 |
| 虚拟机.配置.更改资源      | 允许更改给定资源池中一组虚拟机节点的资源配置。      | 虚拟机 |
| 虚拟机.配置.配置托管主体    | 允许扩展或解决方案将虚拟机标记为由该扩展或解决方案管理。 | 虚拟机 |
| 虚拟机.配置.磁盘更改跟踪    | 允许启用或禁用虚拟机的磁盘更改跟踪。           | 虚拟机 |
| 虚拟机.配置.磁盘租用      | 允许磁盘为虚拟机租用操作。                | 虚拟机 |

表 10-29 虚拟机配置特权（续）

| 特权名称                          | 描述                                                                                            | 要求  |
|-------------------------------|-----------------------------------------------------------------------------------------------|-----|
| 虚拟机.配置.显示连接设置                 | 允许配置虚拟机远程控制台选项。                                                                               | 虚拟机 |
| 虚拟机.配置.扩展虚拟磁盘                 | 允许扩展虚拟磁盘的大小。                                                                                  | 虚拟机 |
| 虚拟机.配置.主机 USB 设备              | 允许将基于主机的 USB 设备连接到虚拟机。                                                                        | 虚拟机 |
| 虚拟机.配置.内存                     | 允许更改分配给虚拟机的内存量。                                                                               | 虚拟机 |
| 虚拟机.配置.修改设备设置                 | 允许更改现有设备的属性。                                                                                  | 虚拟机 |
| 虚拟机.配置.查询 Fault Tolerance 兼容性 | 允许检查虚拟机的兼容性是否符合 Fault Tolerance 的要求。                                                          | 虚拟机 |
| 虚拟机.配置.查询无所有者的文件              | 允许查询无所有者的文件。                                                                                  | 虚拟机 |
| 虚拟机.配置.裸设备                    | 允许添加或移除裸磁盘映射或 SCSI 直通设备。<br>设置此参数将替代用于修改裸设备（包括连接状况）的任何其他特权。                                   | 虚拟机 |
| 虚拟机.配置.基于路径重新加载               | 允许更改虚拟机配置路径，而保留虚拟机的标识。诸如 VMware vCenter Site Recovery Manager 等解决方案使用此操作在故障切换和故障恢复期间保持虚拟机的标识。 | 虚拟机 |
| 虚拟机.配置.移除磁盘                   | 允许移除虚拟磁盘设备。                                                                                   | 虚拟机 |
| 虚拟机.配置.重命名                    | 允许重命名虚拟机或修改虚拟机的相关注释。                                                                          | 虚拟机 |
| 虚拟机.配置.重置客户机信息                | 允许编辑虚拟机的客户机操作系统信息。                                                                            | 虚拟机 |
| 虚拟机.配置.设置注释                   | 允许添加或编辑虚拟机注释。                                                                                 | 虚拟机 |
| 虚拟机.配置.设置                     | 允许更改常规虚拟机设置。                                                                                  | 虚拟机 |
| 虚拟机.配置.交换文件位置                 | 允许更改虚拟机的交换文件放置策略。                                                                             | 虚拟机 |
| 虚拟机.配置.切换派生父项                 |                                                                                               |     |
| 虚拟机.配置.升级虚拟机兼容性               | 允许升级虚拟机的虚拟机兼容性版本。                                                                             | 虚拟机 |

## 虚拟机客户机操作特权

虚拟机客户机操作特权控制使用 API 与虚拟机的客户机操作系统中的文件和程序交互的能力。

有关这些操作的详细信息，请参见《VMware vSphere API 参考》。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-30 虚拟机客户机操作

| 特权名称                | 描述                     | 生效对象 |
|---------------------|------------------------|------|
| 虚拟机.客户机操作.客户机操作别名修改 | 允许对虚拟机别名进行修改的虚拟机客户机操作。 | 虚拟机  |
| 虚拟机.客户机操作.客户机操作别名查询 | 允许对虚拟机别名进行查询的虚拟机客户机操作。 | 虚拟机  |



表 10-30 虚拟机客户机操作（续）

| 特权名称                | 描述                                                                              | 生效对象 |
|---------------------|---------------------------------------------------------------------------------|------|
| 虚拟机.客户机操作.客户机操作修改   | 允许在虚拟机中对客户机操作系统进行修改的虚拟机客户机操作，如向虚拟机传输文件。<br>没有与此特权关联的 vSphere Web Client 用户界面元素。 | 虚拟机  |
| 虚拟机.客户机操作.客户机操作程序执行 | 允许在虚拟机中执行程序的虚拟机客户机操作。<br>没有与此特权关联的 vSphere Web Client 用户界面元素。                   | 虚拟机  |
| 虚拟机.客户机操作.客户机操作查询   | 允许对客户机操作系统进行查询的虚拟机客户机操作，如在客户机操作系统中列出文件。<br>没有与此特权关联的 vSphere Web Client 用户界面元素。 | 虚拟机  |

## 虚拟机交互特权

虚拟机交互特权控制与虚拟机控制台交互、配置媒体、执行电源操作和安装 VMware Tools 的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-31 虚拟机交互

| 特权名称             | 描述                      | 要求  |
|------------------|-------------------------|-----|
| 虚拟机.交互.回答问题      | 允许解决虚拟机状态转换的问题或运行时错误。   | 虚拟机 |
| 虚拟机.交互.虚拟机上的备份操作 | 允许对虚拟机执行备份操作。           | 虚拟机 |
| 虚拟机.交互.配置 CD 媒体  | 允许配置虚拟 DVD 或 CD-ROM 设备。 | 虚拟机 |
| 虚拟机.交互.配置软盘媒体    | 允许配置虚拟软盘设备。             | 虚拟机 |
| 虚拟机.交互.控制台交互     | 允许与虚拟机的虚拟鼠标、键盘和屏幕交互。    | 虚拟机 |

表 10-31 虚拟机交互（续）

| 特权名称                          | 描述                       | 要求  |
|-------------------------------|--------------------------|-----|
| 虚拟机.交互.创建屏幕截图                 | 允许创建虚拟机屏幕截图。             | 虚拟机 |
| 虚拟机.交互.对所有磁盘执行碎片整理            | 允许对虚拟机上的所有磁盘执行碎片整理操作。    | 虚拟机 |
| 虚拟机.交互.设备连接                   | 允许更改虚拟机的可断开虚拟设备的连接状况。    | 虚拟机 |
| 虚拟机.交互.拖放                     | 允许在虚拟机和远程客户端之间拖放文件。      | 虚拟机 |
| 虚拟机.交互.通过 VIX API 执行客户机操作系统管理 | 允许通过 VIX API 管理虚拟机的操作系统。 | 虚拟机 |
| 虚拟机.交互.插入 USB HID 扫描代码        | 允许插入 USB HID 扫描代码。       | 虚拟机 |
| 虚拟机.交互.暂停或取消暂停                | 允许暂停或取消暂停虚拟机。            | 虚拟机 |
| 虚拟机.交互.执行擦除或压缩操作              | 允许对虚拟机执行擦除或压缩操作。         | 虚拟机 |

表 10-31 虚拟机交互（续）

| 特权名称                      | 描述                              | 要求  |
|---------------------------|---------------------------------|-----|
| 虚拟机.交互.关闭电源               | 允许关闭已打开电源的虚拟机的电源。此操作将关闭客户机操作系统。 | 虚拟机 |
| 虚拟机.交互.打开电源               | 允许打开已关闭电源的虚拟机的电源，以及恢复挂起的虚拟机。    | 虚拟机 |
| 虚拟机.交互.记录虚拟机上的会话          | 允许记录虚拟机上的会话。                    | 虚拟机 |
| 虚拟机.交互.重放虚拟机上的会话          | 允许重放虚拟机上已记录的会话。                 | 虚拟机 |
| 虚拟机.交互.重置                 | 允许重置虚拟机并重新引导客户机操作系统。            | 虚拟机 |
| 虚拟机.交互.恢复 Fault Tolerance | 允许恢复虚拟机的 Fault Tolerance 功能。    | 虚拟机 |
| 虚拟机.交互.挂起                 | 允许挂起已打开电源的虚拟机。此操作将客户机置于待机模式。    | 虚拟机 |

表 10-31 虚拟机交互（续）

| 特权名称                      | 描述                                               | 要求  |
|---------------------------|--------------------------------------------------|-----|
| 虚拟机.交互.挂起 Fault Tolerance | 允许暂停虚拟机的 Fault Tolerance 功能。                     | 虚拟机 |
| 虚拟机.交互.测试故障切换             | 允许通过使辅助虚拟机成为主虚拟机测试 Fault Tolerance 故障切换。         | 虚拟机 |
| 虚拟机.交互.测试重新启动辅助虚拟机        | 允许使用 Fault Tolerance 终止虚拟机的辅助虚拟机。                | 虚拟机 |
| 虚拟机.交互.关闭 Fault Tolerance | 允许关闭虚拟机的 Fault Tolerance 功能。                     | 虚拟机 |
| 虚拟机.交互.打开 Fault Tolerance | 允许打开虚拟机的 Fault Tolerance 功能。                     | 虚拟机 |
| 虚拟机.交互.VMware Tools 安装    | 允许以 CD-ROM 形式为客户机操作系统装载和卸载 VMware Tools CD 安装程序。 | 虚拟机 |

## 虚拟机清单特权

虚拟机清单特权控制虚拟机的添加、移动和移除。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

**表 10-32 虚拟机清单特权**

| 特权名称          | 描述                                                                     | 要求           |
|---------------|------------------------------------------------------------------------|--------------|
| 虚拟机.清单.从现有项创建 | 允许通过从模板克隆或部署，基于现有虚拟机或模板创建虚拟机。                                          | 群集、主机、虚拟机文件夹 |
| 虚拟机.清单.新建     | 允许创建虚拟机并为其执行分配资源。                                                      | 群集、主机、虚拟机文件夹 |
| 虚拟机.清单.移动     | 允许在层次结构中重定位虚拟机。<br>特权必须存在于源位置和目标位置。                                    | 虚拟机          |
| 虚拟机.清单.注册     | 允许将现有虚拟机添加到 vCenter Server 或主机清单。                                      | 群集、主机、虚拟机文件夹 |
| 虚拟机.清单.移除     | 允许删除虚拟机。删除操作将从磁盘移除虚拟机的基础文件。<br>要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。       | 虚拟机          |
| 虚拟机.清单.取消注册   | 允许从 vCenter Server 或主机清单中取消注册虚拟机。<br>要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。 | 虚拟机          |

## 虚拟机置备特权

虚拟机置备特权控制与部署和自定义虚拟机相关的活动。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

**表 10-33 虚拟机置备特权**

| 特权名称               | 描述                                      | 要求                      |
|--------------------|-----------------------------------------|-------------------------|
| 虚拟机.置备.允许访问磁盘      | 允许打开虚拟机上的磁盘进行随机读写访问。常用于远程磁盘装载。          | 虚拟机                     |
| 虚拟机.置备.允许访问文件      | 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                     |
| 虚拟机.置备.允许对磁盘进行只读访问 | 允许打开虚拟机上的磁盘进行随机读取访问。常用于远程磁盘装载。          | 虚拟机                     |
| 虚拟机.置备.允许下载虚拟机     | 允许读取与虚拟机关联的文件，包括 vmx、磁盘文件、日志和 nvram。    | Root 主机或 vCenter Server |
| 虚拟机.置备.允许上载虚拟机文件   | 允许写入与虚拟机关联的文件，包括 vmx、磁盘文件、日志和 nvram。    | Root 主机或 vCenter Server |
| 虚拟机.置备.克隆模板        | 允许克隆模板。                                 | 模板                      |
| 虚拟机.置备.克隆虚拟机       | 允许克隆现有虚拟机和资源分配。                         | 虚拟机                     |
| 虚拟机.置备.从虚拟机创建模板    | 允许从虚拟机创建新模板。                            | 虚拟机                     |
| 虚拟机.置备.自定义         | 允许自定义虚拟机的客户机操作系统，而不移除虚拟机。               | 虚拟机                     |
| 虚拟机.置备.部署模板        | 允许从模板部署虚拟机。                             | 模板                      |
| 虚拟机.置备.标记为模板       | 允许将现有已关闭电源的虚拟机标记为模板。                    | 虚拟机                     |

**表 10-33 虚拟机置备特权（续）**

| 特权名称           | 描述               | 要求                  |
|----------------|------------------|---------------------|
| 虚拟机.置备.标记为虚拟机  | 允许将现有模板标记为虚拟机。   | 模板                  |
| 虚拟机.置备.修改自定义规范 | 允许创建、修改或删除自定义规范。 | Root vCenter Server |
| 虚拟机.置备.升级磁盘    | 允许升级虚拟机的磁盘。      | 虚拟机                 |
| 虚拟机.置备.读取自定义规范 | 允许读取自定义规范。       | 虚拟机                 |

## 虚拟机服务配置特权

虚拟机服务配置特权控制哪些用户可以执行有关服务配置的监控和管理任务。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

**注意** 在 vSphere 6.0 中，不能使用 vSphere Web Client 分配或移除此特权。

**表 10-34 虚拟机服务配置特权**

| 特权名称                | 描述                |
|---------------------|-------------------|
| 虚拟机.服务配置.允许通知       | 允许生成和使用有关服务状态的通知。 |
| 虚拟机.服务配置.允许轮询全局事件通知 | 允许查询是否存在任何通知。     |
| 虚拟机.服务配置.管理服务配置     | 允许创建、修改和删除虚拟机服务。  |
| 虚拟机.服务配置.修改服务配置     | 允许修改现有的虚拟机服务配置。   |
| 虚拟机.服务配置.查询服务配置     | 允许检索虚拟机服务的列表。     |
| 虚拟机.服务配置.读取服务配置     | 允许检索现有的虚拟机服务配置。   |

## 虚拟机快照管理特权

虚拟机快照管理特权控制执行、删除、重命名和恢复快照的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

**表 10-35 虚拟机状况特权**

| 特权名称           | 描述                    | 要求  |
|----------------|-----------------------|-----|
| 虚拟机.快照管理.创建快照  | 允许按照虚拟机的当前状况创建快照。     | 虚拟机 |
| 虚拟机.快照管理.移除快照  | 允许从快照历史记录移除快照。        | 虚拟机 |
| 虚拟机.快照管理.重命名快照 | 允许使用新名称和/或新描述重命名快照。   | 虚拟机 |
| 虚拟机.快照管理.恢复快照  | 允许将虚拟机设置为在给定快照中所处的状况。 | 虚拟机 |

## 虚拟机 vSphere Replication 特权

虚拟机 vSphere Replication 特权控制 VMware vCenter Site Recovery Manager™ 对虚拟机使用复制。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-36 虚拟机 vSphere Replication

| 特权名称                         | 描述                      | 要求  |
|------------------------------|-------------------------|-----|
| 虚拟机.vSphere Replication.配置复制 | 允许对虚拟机进行复制配置。           | 虚拟机 |
| 虚拟机.vSphere Replication.管理复制 | 允许在复制时触发完全同步、联机同步或脱机同步。 | 虚拟机 |
| 虚拟机.vSphere Replication.监控复制 | 允许监控复制。                 | 虚拟机 |

## dvPort 组特权

分布式虚拟端口组特权控制创建、删除和修改分布式虚拟端口组的能力。

下表描述创建和配置分布式虚拟端口组所需的特权。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-37 分布式虚拟端口组特权

| 特权名称          | 描述                                                 | 要求    |
|---------------|----------------------------------------------------|-------|
| dvPort 组.创建   | 允许创建分布式虚拟端口组。                                      | 虚拟端口组 |
| dvPort 组.删除   | 允许删除分布式虚拟端口组。<br>要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。 | 虚拟端口组 |
| dvPort 组.修改   | 允许修改分布式虚拟端口组的配置。                                   | 虚拟端口组 |
| dvPort 组.策略操作 | 允许设置分布式虚拟端口组的策略。                                   | 虚拟端口组 |
| dvPort 组.范围操作 | 允许设置分布式虚拟端口组的范围。                                   | 虚拟端口组 |

## vApp 特权

vApp 特权控制与部署和配置 vApp 相关的操作。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-38 vApp 特权

| 特权名称         | 描述                                              | 要求   |
|--------------|-------------------------------------------------|------|
| vApp.添加虚拟机   | 允许将虚拟机添加到 vApp。                                 | vApp |
| vApp.分配资源池   | 允许将资源池分配到 vApp。                                 | vApp |
| vApp.分配 vApp | 允许将一个 vApp 分配给另一个 vApp                          | vApp |
| vApp.克隆      | 允许克隆 vApp。                                      | vApp |
| vApp.创建      | 允许创建 vApp。                                      | vApp |
| vApp.删除      | 允许删除 vApp。<br>要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。 | vApp |
| vApp.导出      | 允许从 vSphere 导出 vApp。                            | vApp |
| vApp.导入      | 允许将 vApp 导入 vSphere。                            | vApp |

表 10-38 vApp 特权（续）

| 特权名称                    | 描述                                                                      | 要求   |
|-------------------------|-------------------------------------------------------------------------|------|
| <b>vApp.移动</b>          | 允许将 vApp 移动到新清单位置。                                                      | vApp |
| <b>vApp.关闭电源</b>        | 允许对 vApp 执行关闭电源操作。                                                      | vApp |
| <b>vApp.打开电源</b>        | 允许对 vApp 执行打开电源操作。                                                      | vApp |
| <b>vApp.重命名</b>         | 允许重命名 vApp。                                                             | vApp |
| <b>vApp.挂起</b>          | 允许暂停 vApp。                                                              | vApp |
| <b>vApp.取消注册</b>        | 允许取消注册 vApp。<br>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 |
| <b>vApp.查看 OVF 环境</b>   | 允许在 vApp 中查看已打开电源的虚拟机的 OVF 环境。                                          | vApp |
| <b>vApp.vApp 应用程序配置</b> | 允许修改 vApp 的内部结构，例如产品信息和属性。                                              | vApp |
| <b>vApp.vApp 实例配置</b>   | 允许修改 vApp 的实例配置，例如策略。                                                   | vApp |
| <b>vApp.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。<br>没有与此特权关联的 vSphere Web Client 用户界面元素。 | vApp |
| <b>vApp.vApp 资源配置</b>   | 允许修改 vApp 的资源配置。<br>要获得执行此操作的权限，用户或组必须在对象及其父对象中分配此特权。                   | vApp |

## vServices 特权

vService 特权控制创建、配置和更新虚拟机和 vApp 的 vService 依赖关系的能力。

您可以在层次结构中的不同级别设置此特权。例如，如果您在文件夹级别设置了某项特权，则可以将此特权传播到该文件夹中的一个或多个对象。“要求”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 10-39 vService

| 特权名称                       | 描述                             | 要求        |
|----------------------------|--------------------------------|-----------|
| <b>vService.创建依赖关系</b>     | 允许创建虚拟机或 vApp 的 vService 依赖关系。 | vApp 和虚拟机 |
| <b>vService.破坏依赖关系</b>     | 允许移除虚拟机或 vApp 的 vService 依赖关系。 | vApp 和虚拟机 |
| <b>vService.重新配置依赖关系配置</b> | 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 |
| <b>vService.更新依赖关系</b>     | 允许更新依赖关系以配置名称或描述。              | vApp 和虚拟机 |

## 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 10-40 vSphere 标记特权

| 特权名称                          | 描述                                    | 要求   |
|-------------------------------|---------------------------------------|------|
| vSphere 标记.分配或取消分配 vSphere 标记 | 允许对 vCenter Server 清单中的对象分配标记或取消分配标记。 | 任何对象 |
| vSphere 标记.创建 vSphere 标记      | 允许创建标记。                               | 任何对象 |
| vSphere 标记.创建 vSphere 标记类别    | 允许创建标记类别。                             | 任何对象 |
| vSphere 标记.创建 vSphere 标记范围    | 允许创建标记范围。                             | 任何对象 |
| vSphere 标记.删除 vSphere 标记      | 允许删除标记。                               | 任何对象 |
| vSphere 标记.删除 vSphere 标记类别    | 允许删除标记类别。                             | 任何对象 |
| vSphere 标记.删除 vSphere 标记范围    | 允许删除标记范围。                             | 任何对象 |
| vSphere 标记.编辑 vSphere 标记      | 允许编辑标记。                               | 任何对象 |
| vSphere 标记.编辑 vSphere 标记类别    | 允许编辑标记类别。                             | 任何对象 |
| vSphere 标记.编辑 vSphere 标记范围    | 允许编辑标记范围。                             | 任何对象 |
| vSphere 标记.修改类别的 UsedBy 字段    | 允许更改标记类别的 UsedBy 字段。                  | 任何对象 |
| vSphere 标记.修改标记的 UsedBy 字段    | 允许更改标记的 UsedBy 字段。                    | 任何对象 |



# 索引

## 符号

- 存储安全性最佳做法 150
- Distributed Switch, 特权 159
- 防火墙端口
  - 概览 132
  - 具有 vCenter Server 的配置 132
  - 连接到 vCenter Server 133
  - 没有 vCenter Server 的配置 133
  - vSphere Host Client 直接连接 133
  - vSphere Web Client 和 vCenter Server 132
  - 主机到主机 134
- 基于 NTP 的时间同步 149
- NTP 服务器, 添加 148
- vCenter Sever Appliance, 替换 NTP 服务器 148
- vSphere Distributed Switch 136
- vSphere Web Client 安全性 152

## 数字

- 3D 功能 100

## A

- Active Directory 66, 67, 70
- 安全
  - 标准交换机端口 135
  - 带有 VLAN 的虚拟机 137
  - 单台主机中的 DMZ 139
  - iSCSI 存储器 150
  - 权限 21
  - 认证 14
  - vCenter Server 11
  - VLAN 跳转 138
  - VMware 策略 14
  - 虚拟化层 9
  - 虚拟网络连接层 12
  - 主机 32
  - 最佳做法 147
- 安全策略
  - 创建 142
  - 可用 142
  - 列出 142
  - 移除 143
- 安全关联
  - 可用 141
  - 列出 141

- 添加 141

- 移除 142

- 安全建议 58, 144

- 安全配置文件 52, 58

- 安全性和 PCI 设备 37

- 安全引导, 升级后的主机 80

- Authentication Proxy

- 启用 68

- 添加域 69

- 自定义证书 72

- Auto Deploy

- 安全 38

- 特权 155

- vSphere Authentication Proxy 68

## B

- 备份 ESXi 证书 51

- 标记, 特权 176

- 标记对象权限 24

- 标准交换机

- 和 iSCSI 150

- 混杂模式 135

- MAC 地址更改 135

- 伪信号 135

- 标准交换机安全 138

- 标准交换机端口, 安全 135

## C

- CA 签名证书 47, 48

- CAM

- 客户端身份验证 70

- 启用 68

- 添加域 69

- CAM 证书 71

- camconfig, 将 CAM 添加到域 69

- 策略, 安全 142

- 插件, 特权 160

- 超时

- ESXi Shell 76–78

- 设置 76

- CIM 工具访问, 限制 39

- crypto-util 128

- 存储监控服务 API 特权 166

- 存储器, 通过 VLAN 和虚拟交换机确保安全 138

- 存储视图, 特权 166

**D**

dcui **66**  
 DCUI 访问权限 **62**  
 dcui 用户特权, dcui **66**  
 DCUI.Access **62**  
 DCUI.Access 高级系统设置 **62**  
 第三方软件支持策略 **14**  
 DMZ **139**  
 端口  
   防火墙 **89**  
   配置 **89**  
 对称密钥 **120**  
 DvFilter **146**

**E**

ESX Agent Manager, 特权 **159**  
 esxcli 防火墙 **56**  
 ESXi  
   日志文件 **82**  
   syslog 服务 **81**  
 ESXi 安全引导 **79**  
 ESXi 出站防火墙端口 **53**  
 ESXi CSR 要求 **47**  
 ESXi 密码 **13**  
 ESXi 日志文件 **81**  
 ESXi 进站防火墙端口 **53**  
 ESXi Shell  
   超时 **77, 78**  
   登录 **79**  
   配置 **75**  
   启用 **75–77**  
   设置超时 **77**  
   设置可用性超时 **76**  
   设置闲置超时 **76**  
   使用 vSphere Web Client 启用 **76**  
   SSH 连接 **35**  
   远程连接 **79**  
   直接连接 **79**  
 ESXi Shell 的可用性超时 **78**  
 ESXi Shell 可用性的超时 **78**  
 ESXi 网络连接 **37**  
 ESXi 证书  
   还原 **51**  
   替换 **46**  
 ESXi 证书, 备份 **51**  
 ESXi 证书, 默认设置 **43**  
 ESXi 证书详细信息 **45**  
 esxi 指纹证书模式 **46**  
 esxi 自定义证书模式 **46**

**F**

防病毒软件, 安装 **98**  
 防火墙  
   命令 **56**  
   NFS 客户端 **55**  
   配置 **56**  
   用于服务访问 **52**  
   用于管理代理访问 **52**  
 防火墙设置 **53**  
 访问, 特权 **153**  
 反间谍软件 **11**  
 Fault Tolerance (FT)  
   安全 **82**  
   日志记录 **82**  
 分布式交换机, 权限 **17**  
 分布式虚拟端口组特权 **175**  
 分配全局权限 **24**  
 服务, syslogd **81**  
 复制和粘贴  
   客户机操作系统 **102**  
   为客户机操作系统禁用 **101**  
 虚拟机 **102**

**G**

隔离  
   标准交换机 **12**  
   VLAN **12**  
   虚拟网络连接层 **12**  
 共享限制, 主机安全 **99**  
 管理访问  
   防火墙 **52**  
   TCP 和 UDP 端口 **92**  
 管理界面  
   确保安全 **31**  
   通过 VLAN 和虚拟交换机确保安全 **138**  
 管理网络 **37**  
 管理员角色 **26**  
 管理证书 **155**

**H**

核心转储和虚拟机加密 **127**  
 核心转储加密 **105**  
 HGFS 文件传输 **101**  
 HTTPS PUT, 上载证书和密钥 **36, 48**  
 还原 ESXi 证书 **51**  
 会话, 特权 **166**  
 混杂模式 **135, 136**  
 Hytrust **120**

**I**

Image Builder 安全 **63**  
 Internet 协议安全 (IPsec) **140**

IP 地址, 添加允许的 **53**

IPsec, , 请参见 Internet 协议安全 (IPsec)

iSCSI

- 身份验证 **150**
- 安全 **150**
- 保护传输数据 **150**
- 保护端口安全 **150**
- QLogic iSCSI 适配器 **150**

**J**

加密

- 过程流 **108**
- 权限 **110**
- 缺少密钥 **126**

加密 vMotion **111**

加密, 虚拟机或虚拟磁盘 **124**

加密操作, 特权 **156**

加密存储策略 **122, 126**

加密局限性 **111**

加密权限 **110**

加密虚拟机 **123**

加密最佳做法 **111**

将群集设置为默认值 **121**

交换机 **134**

解密, 加密虚拟机或硬盘 **125**

仅 VGA 模式 **100**

警报, 特权 **154**

禁用

- 对 vSphere SDK 禁用 SSL **38**
- 客户机操作系统的日志记录 **103**

基于 Linux 的客户端, 限制与 vCenter Server 结合使用 **86**

基于 VMware Tools 的时间同步 **148**

角色

- 安全 **26**
- 创建 **27, 28**
- 管理员 **26**
- 和权限 **26**
- 默认 **26**
- 特权, 列表 **153**
- 无权访问 **26**
- 移除 **22**
- 只读 **26**
- 最佳做法 **28**

**K**

客户端, 防火墙 **89**

客户端身份验证, CAM **70**

客户机操作系统

- 复制和粘贴 **102**

- 禁用日志记录 **103**
- 启用复制和粘贴 **101**

克隆, 加密虚拟机 **124**

KMIP 服务器 **118**

KMIP 服务器

- 将群集设置为默认值 **121**

Root CA **119**

添加到 vCenter Server **121**

证书 **118**

KMS 服务器, “新建证书签名请求”选项 **120**

KMS 群集 **118**

跨越 **144**

扩展, 特权 **160**

## L

类别, 特权 **176**

了解密码 **13**

例外用户列表 **58**

LUN 屏蔽 **151**

## M

MAC 地址更改 **135, 136**

Managed Object Browser, 禁用 **37**

密码, 概览 **13**

密码要求 **34, 87**

密钥

- 上载 **35, 36, 48**
- 授权 **35, 36**
- SSH **35, 36**

密钥服务器, 交换证书 **118**

密钥服务器群集 **118**

默认证书, 用 CA 签名证书替换 **47, 48**

模板, 主机安全 **98**

目录服务

- Active Directory **66**
- 配置主机 **66**

目录服务器, 查看 **67**

## N

内容库, 特权 **155**

Netflow **144**

NFC, 启用 SSL **88**

NFS 4.1, Kerberos 凭据 **151**

NFS 客户端, 防火墙规则集 **55**

NTP **66**

## P

PCI 设备 **37**

PCIe 设备 **37**

配置端口 **89**

配置文件加密 **105**

Portfast **144**

PowerCLI 11

PowerCLI 主机管理 33

## Q

强化 vCenter Server 主机操作系统 85

迁移

加密虚拟机 111

使用加密 vMotion 111

全局权限, 分配 24

全局特权 160

权限

分布式交换机 17

分配 21, 25, 71

概览 21

更改 22

管理员 21

和特权 21

继承 17, 19, 20

root 用户 21

设置 19

特权 164

替代 20

vpxuser 21

移除 22

用户 65

最佳做法 28

权限验证 23

权限验证时间 23

确保 vCenter Server Appliance 安全 87

确保网络安全 131

确保虚拟机安全 95

群集, 密钥管理服务器 117

区域分配 151

## R

任务, 特权 167

日志记录

为客户机操作系统禁用 103

主机安全 81

日志文件

查找 82

ESXi 81, 82

Root CA, KMIP 服务器 119

root 登录, 权限 21, 65

软盘 99

## S

SAN 151

SDK, 防火墙端口和虚拟机控制台 134

设备断开连接, 在 vSphere Web Client 中阻止 103

身份验证

iSCSI 存储器 150

智能卡 74

身份验证代理, 客户端身份验证 70

失败安装日志 85

时间同步

基于 NTP 149

基于 VMware Tools 148

时间同步设置 148

使用脚本管理主机配置 33

受管实体, 权限 17

授权 15, 16

数据存储, 特权 158

数据存储群集, 特权 159

数据中心, 特权 157

SMS API 特权 166

SNMP 143

SSH

安全设置 35

ESXi Shell 35

SSH 密钥 35

SSL, 对 NFC 启用 88

SSO 密码 13

stp 134

锁定模式

不同的产品版本 62

DCUI 访问权限 62

DCUI.Access 62

启用 61, 62

vSphere Web Client 61

行为 60

灾难性 vCenter Server 故障 62

直接控制台用户界面 62

锁定模式, 禁用 61

锁定模式, vSphere 6.0 及更高版本 63

锁定模式例外用户 58

所需特权, 常见任务的 29

syslog 81

## T

TCP 端口 92

特权

Auto Deploy 155

标记 176

插件 160

传输服务 167

存储视图 166

Distributed Switch 159

dvPort 组 175

ESX Agent Manager 159

分配 25

- 会话 166
  - 警报 154
  - 扩展 160
  - 类别 176
  - 内容库 155
  - 配置 161
  - 全局 160
  - 权限 164
  - 任务 167
  - 数据存储 158
  - 数据存储群集 159
  - 数据中心 157
  - vApp 175
  - vCenter Inventory Service 176
  - vCenter Server 83
  - vService 176
  - 网络 164
  - 文件夹 160
  - 性能 164
  - 虚拟机 173
  - 虚拟机 vSphere Replication 174
  - 虚拟机服务配置 174
  - 虚拟机交互 169
  - 虚拟机客户机操作 168
  - 虚拟机快照管理 174
  - 虚拟机配置 167
  - 虚拟机置备 173
  - 已调度任务 166
  - 映像配置文件 155
  - 证书 155
  - 主机 CIM 161
  - 主机 vSphere Replication 163
  - 主机本地操作 163
  - 主机配置文件 163, 165
  - 主机清单 162
  - 资源 165
  - 特权, 所需, 常见任务的 29
  - 特权和权限 21
  - 替换, 默认证书 47, 48
  - 同步 vSphere 网络连接上的 ESXi 时钟 147
  - 同步 vSphere 网络连接上的时钟 147
  - TRUSTED\_ROOTS 49
  - 退出自动化工具 64
- ## U
- UDP 端口 92
  - UEFI 安全引导
    - 升级后的主机 80
    - 虚拟机 95
- ## V
- vApp, 特权 175
  - vCenter Inventory Service
    - 标记 176
    - 特权 176
  - vCenter Server
    - 端口 89
    - 防火墙端口 132
    - 特权 83
    - 添加 KMIP 服务器 121
    - 通过防火墙连接 133
  - vCenter Server 安全性 83, 85
  - vCenter Server 安全性最佳做法 83
  - vCenter Server Appliance
    - 基于 NTP 的时间同步 149
    - 添加 NTP 服务器 148
    - 安全性最佳做法 87
    - 基于 VMware Tools 的时间同步 148
    - 时间同步设置 148
  - vCenter Server 密码策略 85
  - vCenter Server 主机操作系统, 强化 85
  - VGT 138
  - vifs, 上载证书和密钥 35
  - VirtualCenter.VimPasswordExpirationInDays 85
  - VLAN
    - 安全 137
    - 第 2 层安全 138
    - 和 iSCSI 150
    - VLAN 跳转 138
  - VLAN 安全 138
  - VLAN 文档 145
  - VMCA 模式切换 41
  - vMotion, 通过 VLAN 和虚拟交换机确保安全 138
  - vmx 文件, 编辑 96
  - vpzd.certmgmt.mode 46
  - vpxuser 65
  - vService, 特权 176
  - vSphere 安全概述 9
  - vSphere Authentication Proxy 66, 68, 70
  - vSphere Authentication Proxy 证书 71
  - vSphere Host Client, 用于直接连接的防火墙端口 133
  - vSphere Network Appliance 146
- ## W
- 网络
    - 安全 137
    - 特权 164
  - 网络安全 131, 144
  - 网络标签 145
  - 网络隔离 145

网络连接, 限制 85

网络文件复制 (NFC) 88

未公开的功能, 禁用 100

伪信号 135, 136

文件夹, 特权 160

无权访问角色 26

## X

闲置会话超时 77, 78

限制基于 Linux 的客户端与 vCenter Server 结合使用 86

限制客户机操作特权 102

性能, 特权 164

性能数据, 禁用发送 152

“新建证书签名请求”选项, KMS 服务器 120

信任连接 119

信息性消息, 限制 96

续订 ESXi 证书 45

虚拟磁盘, 压缩 97

虚拟磁盘加密 109

虚拟磁盘描述符文件加密 105

虚拟化管理程序安全 9

虚拟机

安全引导 95

复制和粘贴 102

隔离 139

交互特权 169

禁用复制和粘贴 101

禁用日志记录 103

客户机操作特权 168

快照管理特权 174

配置特权 167

清单特权 173

确保安全 96, 104

vSphere Replication 特权 174

在 vSphere Web Client 中阻止设备断开连接 103

置备特权 173

虚拟机安全性

禁用功能 100

VMX 参数 100

最佳做法 97

虚拟机服务配置, 特权 174

虚拟机加密

概览 105

互操作性 114

架构 107

虚拟机控制台, 主机安全 98

虚拟客户机标记 138

virtual network ( 虚拟网络 ), 安全 137

虚拟网络连接层和安全 12

## Y

样本角色 25

严格的锁定模式 58

已撤销证书 85

已调度任务, 特权 166

已过期证书 85

硬件设备 99

映像配置文件特权 155

用户管理 15

用户和权限 15

用户目录超时 23

用户权限, vpxuser 65

由 vCenter Server 使用的端口 89

远程操作, 在虚拟机中禁用 102

允许的 IP 地址, 防火墙 53

## Z

在虚拟机中禁用远程操作 102

证书

对 vSphere SDK 禁用 SSL 38

过期 85

检查 88

上载 48

特权 155

已撤销 85

主机升级 41

证书过期 44

证书详细信息 44

证书信息 44

只读角色 26

直接控制台用户界面 (DCUI) 62

直接控制台用户界面访问 62

智能卡身份验证

回退 75

禁用 75

配置 74

启用 74

在锁定模式下 75

指纹, 主机 88

指纹证书 41

主机

本地操作特权 163

CIM 特权 161

配置特权 161

清单特权 162

vSphere Replication 特权 163

指纹 88

主机安全

CIM 工具 39

禁用 MOB 37

Managed Object Browser 37



- 日志记录 **81**
- 使用模板 **98**
- 未签名的 VIB **63**
- 性能数据 **152**
- 虚拟磁盘缩小 **97**
- 虚拟机控制台 **98**
- 资源管理 **99**
- 主机到主机的防火墙端口 **134**
- 主机防火墙 **89**
- 主机管理特权, 用户 **66**
- 主机加密模式
  - 更改 **122**
  - 禁用 **123**
- 主机名称, 配置 **66**
- 主机配置文件, 特权 **163, 165**
- 主机升级和证书 **41**
- 自定义角色 **25**
- 自定义证书
  - Auto Deploy **50**
  - ESXi **49**
- 资源, 特权 **165**
- 最佳做法
  - 安全 **147**
  - 角色 **28**
  - 权限 **28**

