vSphere 安全性

Update 1
ESXi 5.5
vCenter Server 5.5

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-001361-00

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

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

《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 vSphere 环境中可用的安全功能，以及为使该环境免受攻击而可采取的措施。

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。

1 vSphere 环境中的安全性

要保护 vSphere 环境，您必须熟悉关于安全的各方面信息（包括身份验证、授权、用户和权限）以及保护 vCenter Server 系统、ESXi 主机和虚拟机的各方面信息。

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

本章讨论了以下主题：

安全和虚拟化层

VMware 设计了虚拟化层（或 VMkernel）来运行虚拟机。它控制着主机所使用的硬件，并调度虚拟机之间的硬件资源分配。由于 VMkernel 专用于支持虚拟机而不用于其他用途，因此其接口严格限制在管理虚拟机所需的 API。

ESXi 通过以下功能提供附加 VMkernel 保护：

内存强化安全

将 ESXi 内核、用户模式应用程序及可执行组件（如驱动程序和库）位于无法预测的随机内存地址中。在将该功能与微处理器提供的不可执行的内存保护结合使用时，可以提供保护，使恶意代码很难通过内存漏洞来利用系统漏洞。

内核模块完整性

数字签名确保由 VMkernel 加载的模块、驱动程序及应用程序的完整性和真实性。模块签名允许 ESXi 识别模块、驱动程序或应用程序的提供商以及它们是否通过 VMware 认证。VMware 软件和某些第三方驱动程序已获得 VMware 签名认证。

可信的平台模块 (TPM)

vSphere 使用 Intel 可信的平台模块/受信任的执行技术 (TPM/TXT)，根据硬件信任根提供管理程序映像的远程证明。管理程序映像由以下元素构成：

- VIB（软件包）格式的 ESXi 软件（管理程序）
- 第三方 VIB
- 第三方驱动程序

要利用该功能，ESXi 系统必须启用 TPM 和 TXT。

如果启用了 TPM 和 TXT，ESXi 会在系统引导时测量整个管理程序堆栈，并将这些测量值存储在 TPM 的平台配置寄存器 (PCR) 中。测量范围包括 ESXi 上运行的 VMkernel、内核模块、驱动程序、本机管理应用程序，以及所有引导时配置选项。系统上安装的所有 VIB 都会进行测量。

第三方解决方案可使用该功能构建验证程序，通过将映像与预期已知正常值的映像进行比较，检测管理程序映像的篡改。vSphere 未提供用于查看这些测量值的用户界面。

测量值在 vSphere API 中公开。根据 TXT 的可信计算组 (TCG) 标准，事件日志作为 API 的一部分提供。

安全和虚拟网络连接层

虚拟网络连接层包括虚拟网络适配器和虚拟交换机。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，主机可使用虚拟网络连接层与 iSCSI SAN 和 NAS 存储器等进行通信。

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

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

安全资源和信息

可以在 VMware 网站上查找其他的安全相关信息。

下表列出了安全主题以及这些主题的其他信息的所在位置。

表 1-1 Web 上的 VMware 安全资源

主题	资源
VMware 安全策略、最新安全预警、安全下载及安全主题重点讨论	http://www.vmware.com/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。
关于虚拟化和安全性的一般信息	VMware 虚拟安全技术资源中心 http://www.vmware.com/go/security
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
有关 VMware vCloud 网络和安全的信息。	http://www.vmware.com/go/vmsafe
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
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

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

vCenter Single Sign-On 是一个采用安全令牌交换机制的身份验证代理程序。用户通过 vCenter Single Sign-On 进行身份验证后，即可访问已被授权访问的所有已安装 vCenter 服务。由于所有通信的流量都会进行加密，且只有经过身份验证的用户才被授予访问权限，因此您的环境是安全的。

在安装或升级任何其他 vSphere 组件之前先安装或升级 vCenter Single Sign-On。请参见 *vSphere 安装和设置* 或 *vSphere 升级*文档。

有关为使用 vCenter Single Sign-On 的服务替换证书的信息，请参见第 35 页，第 3 章 “vSphere 安全证书和加密”。

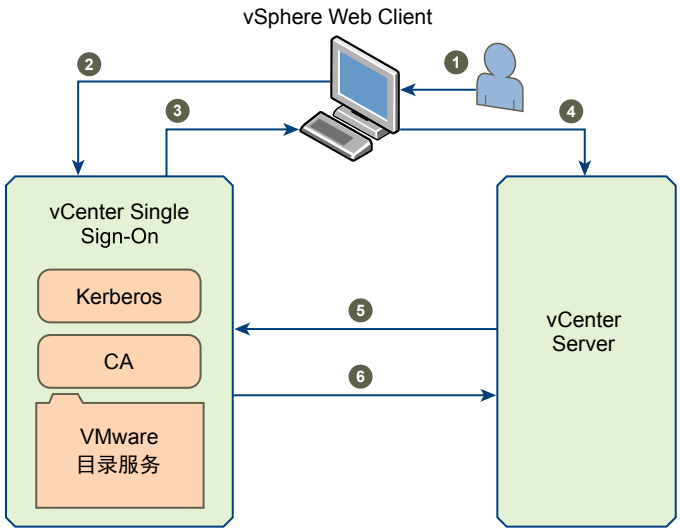
本章讨论了以下主题：

如何使用 vCenter Single Sign-On 保护您的环境

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

vCenter Single Sign-On 使用 STS（安全令牌服务）、用于实现安全通信的 SSL 以及通过 Active Directory 或 OpenLDAP 的身份验证的组合，如下图所示。

图 2-1 vCenter Single Sign-On 握手



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

用户还可以不使用密码而选中**使用 Windows 会话身份验证**复选框进行登录。该复选框在您安装 VMware 客户端集成插件后变为可用。

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

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

3 如果用户位于标识源中，vCenter Single Sign-On 会返回表示 vSphere Web Client 的用户的令牌。

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

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

6 vCenter Single Sign-On 服务器返回 vCenter Server 系统的令牌。

用户现在可以对 vCenter Server 进行身份验证，以及查看和修改用户具有权限的任何对象。

注意 首先，每个用户都分配有“无权访问”权限。vCenter Server 管理员必须至少为用户分配“只读”权限，用户才能登录。请参见第 56 页，“在 vSphere Web Client 中分配权限”和第 55 页，第 5 章“vCenter 用户管理任务”。

vCenter Single Sign-On 组件

vCenter Single Sign-On 包括安全令牌服务 (STS)、管理服务器和 vCenter Lookup Service 以及 VMware 目录服务 (vmdir)。

这些组件作为安装的一部分进行部署。

STS（安全令牌服务） 凡是通过 vCenter Single Sign-On 登录的用户，均可通过 STS 证书使用 vCenter Single Sign-On 支持的任意 vCenter 服务，而无需逐个进行身份验证。STS 服务会发出安全断言标记语言 (SAML) 令牌。这些安全令牌表示 vCenter Single Sign-On 支持的标识源类型之一中的用户标识。

管理服务器 管理服务器允许用户具有 vCenter Single Sign-On 的管理员特权，以便配置 vCenter Single Sign-On 服务器并管理 vSphere Web Client 中的用户和组。最初，只有用户 administrator@vsphere.local 具有此类特权。

vCenter Lookup Service vCenter Lookup Service 包含有关 vSphere 基础架构的拓扑信息，使 vSphere 组件可以安全地互相连接。除非您使用的是简单安装，否则在安装其他 vSphere 组件时系统会提示您输入 Lookup Service URL。例如，Inventory Service 和 vCenter Server 安装程序会请求提供 Lookup Service URL，然后联系此 Lookup Service 以查找 vCenter Single Sign-On。安装后，会在 vCenter Lookup Service 中注册 Inventory Service 和 vCenter Server 系统，以便其他 vSphere 组件（如 vSphere Web Client）可以找到它们。

VMware 目录服务 与 vsphere.local 域关联的目录服务。此服务是一个在端口 11711 上提供 LDAP 目录的多租户、多重管理目录服务。在多站点模式下，如果更新一个 VMware 目录服务实例中的 VMware 目录服务内容，则与所有其他 vCenter Single Sign-On 节点关联的 VMware 目录服务实例将自动更新。

vCenter Single Sign-On 如何影响 vCenter Server 安装

自版本 5.1 起，vSphere 将 vCenter Single Sign-On 组件作为 vCenter Server 管理基础架构的组成部分包含在内。此变更影响 vCenter Server 安装。

使用 vCenter Single Sign On 进行身份验证允许各种 vSphere 软件组件通过安全的令牌交换机制相互通信，从而使 VMware 云基础架构平台更加安全。

对于首次安装 vCenter Server，必须安装所有组件。在同一个环境中执行后续安装或者在添加服务时，不需要安装 vCenter Single Sign-On。一个 vCenter Single Sign-On 服务器可以为整个 vSphere 环境提供服务。安装一次 vCenter Single Sign-On 后，可以将所有新 vCenter Server 实例连接到同一 vCenter Single Sign-On 服务。您必须为每个 vCenter Server 实例安装一个 Inventory Service 实例。

简单安装

简单安装选项将在同一台主机或虚拟机上安装 vCenter Single Sign-On、vSphere Web Client、vCenter Inventory Service 和 vCenter Server。简单安装适用于大多数部署。

自定义安装

如果要自定义每个组件的位置和设置，可以按以下顺序执行自定义安装并选择各个安装选项，从而分别安装这些组件：

1 vCenter Single Sign-On

2 vSphere Web Client

3 vCenter Inventory Service

4 vCenter Server

可以将每个组件安装在不同的主机或虚拟机上。

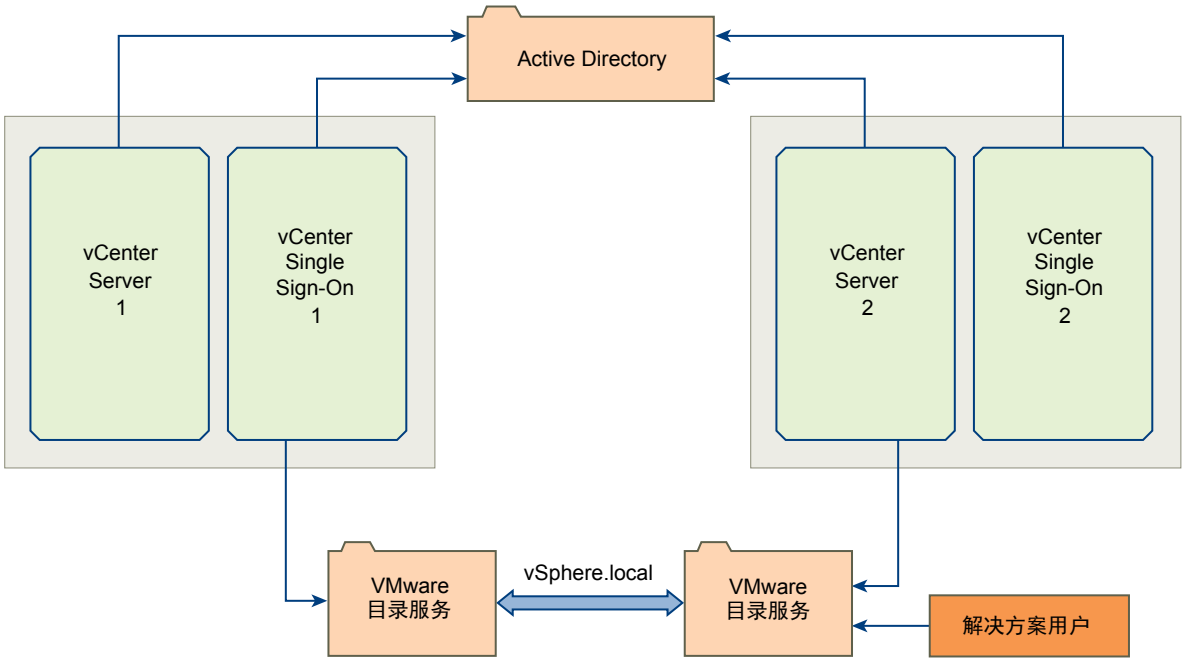
如果您决定安装多个 vCenter Server 系统，则可以指向每个 vCenter Server 的同一 vCenter Single Sign-On 实例。

在多个位置安装

与 vCenter Single Sign-On 5.1 版不同，vCenter Single Sign-On 5.5 会在各个位置之间同步身份验证数据。

如果您在多个位置安装了 vCenter Server 系统，则可以在每个位置安装 vCenter Single Sign-On 服务器。安装第二个及后续的 vCenter Single Sign-On 实例时，可以在安装过程中使这些实例指向第一个 vCenter Single Sign-On 实例。这两个实例将同步其 VMware 目录服务实例。对一个实例的更改将传播到另一个实例。

图 2-2 在多个位置安装 vCenter Single Sign-On



vCenter Single Sign-On 如何影响 vCenter Server 升级

升级后哪些用户可以登录 vCenter Server 取决于升级前的版本以及部署配置。

在升级至 vCenter Server 5.0 及更早版本（其中不包含 vCenter Single Sign-On 服务）的过程中，在 vCenter Server 中注册的本地操作系统用户和 Active Directory 用户都可以继续使用升级后的 vCenter Server。

如果您是从不包含 vCenter Single Sign-On 的版本升级至包含 vCenter Single Sign-On 的版本，则此行为将发生更改：vCenter Server 版本 5.1 或 vCenter Server 版本 5.5。

注意 使用 vCenter Single Sign-On 后，本地操作系统用户将远不如目录服务（如 Active Directory）中的用户重要。因此，很难，或甚至是无法保留本地操作系统用户作为经过身份验证的用户。

从早于 5.1 的版本升级之后，系统可能会在安装过程中提示您输入 vSphere 清单层次结构中根文件夹的管理员。如果用户存储从 vSphere 5.1 之前的版本更改为 vSphere 5.1 及更高版本，则可能会发生这种情况。请参见第 47 页，“权限的层次结构继承”。

简单安装升级

简单安装升级将安装或升级一个独立的 vCenter Server 以及相关组件。

如果从不包含 vCenter Single Sign-On 的 vCenter Server 版本升级至 vCenter Server 5.5，则 vCenter Single Sign-On 会识别现有的本地操作系统用户。此外，用户 administrator@vsphere.local 可以作为管理员用户登录 vCenter Single Sign-On 和 vCenter Server。如果您之前的安装支持 Active Directory 用户，则可以将 Active Directory 域添加为标识源。

如果升级 vCenter Single Sign-On 和 vCenter Server，则 vCenter Single Sign-On 会识别现有的本地操作系统用户。此外，用户 administrator@vsphere.local 可以作为管理员用户登录 vCenter Single Sign-On 和 vCenter Server。如果之前的安装包含作为标识源的 Active Directory 域，则升级后该标识源仍可用。由于 vCenter Server 仅支持一个默认标识源，因此用户在登录 (*DOMAIN**user*) 时可能必需指定该域。

自定义升级

自定义升级可以在不同的计算机上安装不同的 vCenter Server 组件，也可以在同一台计算机上安装第二个 vCenter Server 系统。您还可以使用自定义安装来升级在其他位置安装的环境。

如果从不包含 vCenter Single Sign-On 的 vCenter Server 版本升级至 vCenter Server 5.5，并且在 vCenter Server 之外的其他计算机上安装 vCenter Single Sign-On，则 vCenter Single Sign-On 将不会识别现有的本地操作系统用户。用户 administrator@vsphere.local 可以作为管理员用户登录 vCenter Single Sign-On 和 vCenter Server。如果您之前的安装支持 Active Directory 用户，则可以将 Active Directory 域添加为标识源。

如果要升级具有多站点模式 vCenter Single Sign-On 的 vCenter Server 版本，并且其他 vCenter Server 系统使用链接模式，则首先必须重新同步。然后可以升级所有 vCenter Single Sign-On 实例并保持链接模式功能不变。对于所有 vCenter Server 系统的单个视图，需要链接模式。仅当所有节点版本都相同时，才支持多站点 vCenter Single Sign-On。

如果要升级具有高可用性模式 vCenter Single Sign-On 的 vCenter Server 版本，则必须升级所有 vCenter Single Sign-On 高可用性实例。首先执行升级，升级完成后，通过使用 VMware HA 或 VMware Heartbeat 来保护 vCenter Server 和 vCenter Single Sign-On，以便配置高可用性。

注意 在多个位置安装 vCenter Server 版本 5.5 中包含的 vCenter Single Sign-On 组件时，如果在一个位置进行更改，则会为所有 vCenter Single Sign-On 实例更新 VMware 目录服务。

通过 vSphere 使用 vCenter Single Sign-On

当用户登录 vSphere 组件时，vCenter Single Sign-On 用于进行身份验证。用户必须通过 vCenter Single Sign-On 进行身份验证，并且必须已授予 vCenter Server 权限才能查看和管理 vSphere 对象。

当用户登录 vSphere Web Client 时，他们首先由 vCenter Single Sign-On 进行身份验证。对于经过身份验证的用户，vCenter Server 将检查权限。用户所能看到的内容和所能执行的操作均取决于 vCenter Server 和 ESXi 的 vSphere 权限设置以及环境中的应用程序。vCenter Server 管理员从 vSphere Web Client 中的**管理 > 权限**界面来分配这些权限，而不是通过 vCenter Single Sign-On。请参见第 47 页，第 4 章“vSphere 用户和权限”和第 55 页，第 5 章“vCenter 用户管理任务”。

vCenter Single Sign-On 和 vCenter Server 用户

用户可使用 vSphere Web Client，通过在 vSphere Web Client 登录页面上输入凭据向 vCenter Single Sign-On 进行身份验证。连接到 vCenter Server 后，通过身份验证的用户可以查看所有 vCenter Server 实例或对其具有权限的其他 vSphere 服务。无需进一步进行身份验证。经过身份验证的用户可对对象执行的操作取决于用户对这些对象的 vCenter Server 权限。请参见第 47 页，第 4 章“vSphere 用户和权限”和第 55 页，第 5 章“vCenter 用户管理任务”。

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

虽然大多数 vCenter Single Sign-On 管理任务需要 vCenter Single Sign-On 管理员凭据，但是可对 vCenter Single Sign-On 进行身份验证的所有用户均可重置其密码，即使该密码已过期也是如此。请参见第 18 页，“重置过期的 vCenter Single Sign-On 密码”。

vCenter Single Sign-On 管理员用户

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

要配置 vCenter Single Sign-On 并管理 vCenter Single Sign-On 用户和组，用户 administrator@vsphere.local 或具有 vCenter Single Sign-On 管理员权限的用户必须登录到 vSphere Web Client。根据身份验证，该用户可以访问 vCenter Single Sign-On 管理界面来管理标识源和默认域、指定密码策略并执行其他管理任务。请参见第 17 页，“配置 vCenter Single Sign-On”。

vSphere 的不同版本中的身份验证

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

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

ESXi 用户

ESXi 5.1 未与 Center Single Sign-On 集成。将 ESXi 主机明确添加到 Active Directory 域。请参见第 71 页，“将 ESXi 主机添加到 Active Directory 域”。

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

登录行为

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

- 默认域中的用户可使用其自身的用户名和密码进行登录。
- 如果用户位于已添加到 vCenter Single Sign-On 作为标识源的域而并非默认域中，则可以登录到 vCenter Server，但必须按照以下方式之一指定域。
  - 包含域名前缀，例如 MYDOMAIN\user1
  - 包含域，例如 user1@mydomain.com
- 如果用户位于不是 vCenter Single Sign-On 标识源的域中，则无法登录到 vCenter Server。如果添加到 vCenter Single Sign-On 的域是域层次结构的一部分，则 Active Directory 将确定层次结构中其他域的用户是否进行了身份验证。

配置 vCenter Single Sign-On

通过 vCenter Single Sign-On，您可添加标识源、管理默认域、配置密码策略，并编辑锁定策略。

可从 vSphere Web Client 配置 vCenter Single Sign-On。要配置 vCenter Single Sign-On，您必须拥有 vCenter Single Sign-On 管理员特权。vCenter Single Sign-On 管理员特权不同于 vCenter Server 或 ESXi 上的管理员角色。默认情况下，在全新安装中，只有用户 administrator@vsphere.local 才具有 vCenter Single Sign-On 服务器上的管理员特权。

- 重置过期的 vCenter Single Sign-On 密码第 18 页，

  默认情况下，vCenter Single Sign-On 密码（包括 administrator@vsphere.local 的密码）在 90 天后过期。密码即将过期时，vSphere Web Client 会发出警告。您可以从 vSphere Web Client 重置过期的密码。

- 编辑 vCenter Single Sign-On 密码策略第 18 页，

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

- 编辑 vCenter Single Sign-On 锁定策略第 19 页，

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

- 编辑 vCenter Single Sign-On 令牌策略第 19 页，

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

- 使用 vCenter Single Sign-On 标识 vCenter Server 的源第 20 页，

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

- 设置 vCenter Single Sign-On 的默认域第 21 页，

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

- 添加 vCenter Single Sign-On 标识源第 22 页，

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

- 编辑 vCenter Single Sign-On 标识源第 24 页，

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

- 移除 vCenter Single Sign-On 标识源第 24 页，

  vSphere 用户在标识源中定义。可从注册的标识源列表中移除标识源。

- 移除安全令牌服务 (STS) 证书第 25 页，

  vCenter Single Sign-On 提供了安全令牌服务 (STS)。安全令牌服务是一项发布、验证和续订安全令牌的 Web 服务。当现有 vCenter Single Sign-On STS 证书过期或发生更改时，您可以将其移除。

- 刷新安全令牌服务 (STS) 根证书第 25 页，

  vCenter Single Sign-On 提供了安全令牌服务 (STS)。安全令牌服务是一项发布、验证和续订安全令牌的 Web 服务。现有安全令牌服务证书过期或更改时，您可手动对其进行刷新。

- 确定 SSL 证书的过期日期第 26 页，

  CA 签名的 SSL 证书在预定义的使用期限之后过期。知道证书何时过期使您能够在过期日期之前重新替换或更新证书。

- 确定是否正在使用证书第 26 页，

  开始替换证书之前，可以检查您拥有的证书是否已在使用中。可以使用**计算使用情况**功能确定系统是否正在使用证书。

- vCenter Single Sign-On 使用 Windows 会话身份验证第 26 页，

  您可以在 vCenter Single Sign-On 中使用 Windows 会话身份验证 (SSPI)。要使该复选框显示在登录页面上，必须安装客户端集成插件。

重置过期的 vCenter Single Sign-On 密码

默认情况下，vCenter Single Sign-On 密码（包括 administrator@vsphere.local 的密码）在 90 天后过期。密码即将过期时，vSphere Web Client 会发出警告。您可以从 vSphere Web Client 重置过期的密码。

在 vSphere 5.5 及更高版本中，系统会在用户使用过期密码登录时提示其重置密码。要重置早期版本的 vCenter Single Sign-On 的密码，请参见该版本的产品的文档。

前提条件

您必须知晓该用户名对应的当前但已过期的密码。

步骤

1 转至 vSphere Web Client URL。

2 出现提示时，提供用户名、当前密码以及新密码。

如果您无法登录，请与 vCenter Single Sign-On 系统管理员联系以获得帮助。

编辑 vCenter Single Sign-On 密码策略

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

默认情况下，vCenter Single Sign-On 密码在 90 天后过期。密码即将过期时，vSphere Web Client 将向您发出提醒。如果您知道旧密码，则可以重置过期的密码。

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

请参见第 18 页，“重置过期的 vCenter Single Sign-On 密码”。

步骤

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

2 浏览到**管理 > Single Sign-On > 配置**。

3 单击**策略**选项卡，然后选择**密码策略**。

4 单击**编辑**。

5 编辑密码策略参数。

选项	描述
描述	密码策略描述。必填。
最长生命周期	用户必须更改密码前密码可存在的最大天数。
限制重用	不能选择的用户之前的密码个数。例如，如果用户不能重用最近五个密码中的任何一个，则键入 5。
最大长度	允许密码包含的最大字符数。

选项	描述
最小长度	密码必须包含的最少字符数。最小长度不得小于字母、数字和特殊字符要求的最小总和。
字符要求	密码必须包含的不同字符类型最小数目。 ■ 特殊：& # % ■ 字母：A b c D ■ 大写：A B C ■ 小写：a b c ■ 数字：1 2 3 字母字符最小数目不得小于大写和小写要求的总和。 密码中不得使用以下字符：非 ASCII 字符、分号 (;)、双引号 (")、单引号 (')、音调符号 (^) 和反斜线。
相同的相邻字符数	密码中允许的连续相同字符的最大个数。数字必须大于 0。例如，如果输入 1，则不允许使用以下密码：p@$$word。

6 单击**确定**。

编辑 vCenter Single Sign-On 锁定策略

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

如果用户使用错误的密码多次登录 vsphere.local，则将锁定用户。通过锁定策略，您可指定最多失败登录尝试次数，以及失败尝试之间经过的时长。该策略还可指定在自动解锁帐户之前必须经过的时长。

步骤

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

2 浏览到**管理 > Single Sign-On > 配置**。

3 单击**策略**选项卡，然后选择**锁定策略**。

4 单击**编辑**。

5 编辑参数。

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

6 单击**确定**。

编辑 vCenter Single Sign-On 令牌策略

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

步骤

1 登录到 vSphere Web Client。

2 选择**管理 > Single Sign-On**，然后选择**配置**。

3 单击**策略**选项卡，然后选择**令牌策略**。

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

4 编辑令牌策略配置参数。

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

5 单击**确定**。

使用 vCenter Single Sign-On 标识 vCenter Server 的源

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

标识源是用户和组数据的集合。用户和组数据存储在 Active Directory 中、OpenLDAP 中或者存储到本地安装了 vCenter Single Sign-On 的计算机操作系统。安装后，vCenter Single Sign-On 的每个实例都具有一个本地操作系统标识源 vpshere.local。此标识源是 vCenter Single Sign-On 的内部标识源。

vCenter Single Sign-On 管理员用户可以创建 vCenter Single Sign-On 用户和组。

标识源的类型

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

- Active Directory 版本 2003 及更高版本。vCenter Single Sign-On 仅允许您指定单个 Active Directory 域作为标识源。该域可包含子域或作为林的根域。在 vSphere Web Client 中显示为 **Active Directory (已集成 Windows 身份验证)**。
- Active Directory over LDAP。vCenter Single Sign-On 支持多个 Active Directory over LDAP 标识源。包含此标识源类型，以便与 vSphere 5.1 随附的 vCenter Single Sign-On 服务兼容。在 vSphere Web Client 中显示为 **Active Directory 作为 LDAP 服务器**。
- OpenLDAP 版本 2.4 及更高版本。vCenter Single Sign-On 支持多个 OpenLDAP 标识源。在 vSphere Web Client 中显示为 **OpenLDAP**。

- 本地操作系统用户。本地操作系统用户是运行 vCenter Single Sign-On 服务器的操作系统的本地用户。本地操作系统标识源仅在基本 vCenter Single Sign-On 服务器部署中存在，并在具有多个 vCenter Single Sign-On 实例的部署中不可用。仅允许一个本地操作系统标识源。在 vSphere Web Client 中显示为 **localos**。
- vCenter Single Sign-On 系统用户。每次安装 vCenter Single Sign-On 时都会创建一个名为 vsphere.local 的系统标识源。在 vSphere Web Client 中显示为 **vsphere.local**。

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

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

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

登录行为

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

- 默认域中的用户可使用其自身的用户名和密码进行登录。
- 如果用户位于已添加到 vCenter Single Sign-On 作为标识源的域而并非默认域中，则可以登录到 vCenter Server，但必须按照以下方式之一指定域。
  - 包含域名前缀，例如 MYDOMAIN\user1
  - 包含域，例如 user1@mydomain.com
- 如果用户位于不是 vCenter Single Sign-On 标识源的域中，则无法登录到 vCenter Server。如果添加到 vCenter Single Sign-On 的域是域层次结构的一部分，则 Active Directory 将确定层次结构中其他域的用户是否进行了身份验证。

vCenter Single Sign-On 不会传播从来自不同标识源的嵌套组获取的权限。例如，如果您将域管理员组添加到本地管理员组，则不会传播权限，因为本地操作系统和 Active Directory 均为独立的标识源。

设置 vCenter Single Sign-On 的默认域

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

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

- 默认域中的用户可使用其自身的用户名和密码进行登录。
- 如果用户位于已添加到 vCenter Single Sign-On 作为标识源的域而并非默认域中，则可以登录到 vCenter Server，但必须按照以下方式之一指定域。
  - 包含域名前缀，例如 MYDOMAIN\user1
  - 包含域，例如 user1@mydomain.com
- 如果用户位于不是 vCenter Single Sign-On 标识源的域中，则无法登录到 vCenter Server。如果添加到 vCenter Single Sign-On 的域是域层次结构的一部分，则 Active Directory 将确定层次结构中其他域的用户是否进行了身份验证。

步骤

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

2 浏览到**管理 > Single Sign-On > 配置**。

3 在**标识源**选项卡上，选择一个标识源，然后单击**设置为默认域**图标。

在域显示屏幕中，默认域显示在“域”列中（默认设置）。

添加 vCenter Single Sign-On 标识源

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

标识源可以是本机 Active Directory（已集成 Windows 身份验证）域，也可以是 OpenLDAP 目录服务。为实现向后兼容性，Active Directory 也可用作 LDAP 服务器。

一旦完成安装，以下默认标识源和用户立即可用：

localos	所有本地操作系统用户。这些用户可以获得 vCenter Server 的权限。如果要进行升级，已获得权限的这些用户将保留其权限。
vsphere.local	包含 vCenter Single Sign-On 内部用户。

步骤

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

2 浏览到**管理 > Single Sign-On > 配置**。

3 在**标识源**选项卡上，单击**添加标识源**图标。

4 选择标识源的类型，然后输入标识源设置。

选项	描述
Active Directory (已集成 Windows 身份验证)	对于本机 Active Directory 实施，请使用此选项。请参见第 23 页，“Active Directory 标识源设置”。
作为 LDAP 服务器的 Active Directory	此选项可用于向后兼容性。这需要您指定域控制器和其他信息。请参见第 23 页，“Active Directory LDAP Server 和 OpenLDAP Server 标识源设置”。
OpenLDAP	对于 OpenLDAP 标识源，请使用此选项。请参见第 23 页，“Active Directory LDAP Server 和 OpenLDAP Server 标识源设置”。
LocalOS	使用此选项可添加本地操作系统以作为标识源。系统仅提示您输入本地操作系统的名称。如果选择此选项，则指定计算机上的所有用户都对 vCenter Single Sign-On 可见，即使这些用户不属于其他域也是如此。

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

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

6 单击**确定**。

下一步

添加标识源时，所有用户均可进行身份验证，但只有**无权访问**权限。具有 vCenter Server **Modify.permissions** 特权的用户可向用户或一组用户分配权限，以便他们能够登录 vCenter Server。请参见第 56 页，“在 vSphere Web Client 中分配权限”。

Active Directory 标识源设置

如果选择“Active Directory (已集成 Windows 身份验证)”标识源类型，则可以使用本地计算机帐户作为 SPN（服务主体名称）或者明确指定一个 SPN。

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

表 2-1 添加标识源设置

字段	描述
域名	域的 FDQN。请勿在此字段中提供 IP 地址。
使用计算机帐户	选择此选项可将本地计算机帐户用作 SPN。选择此选项时，应仅指定域名。如果您希望重命名此计算机，请勿选择此选项。
使用 SPN	如果您希望重命名本地计算机，请选择此选项。必须指定 SPN、能够通过标识源进行身份验证的用户以及该用户的密码。
服务主体	有助于 Kerberos 识别 Active Directory 服务的 SPN。请在名称中包含域，例如 STS/example.com。 您可能需要运行 `setspn –S` 以添加要使用的用户。有关 `setspn` 的信息，请参见 Microsoft 文档。 SPN 在域中必须唯一。运行 `setspn –S` 可检查是否未创建重复项。
用户主体名称	能够通过此标识源进行身份验证的用户的名称。请使用电子邮件地址格式，例如jchin@mydomain.com。可以通过 Active Directory 服务界面编辑器 (ADSI Edit) 验证用户主体名称。
密码	用于通过此标识源进行身份验证的用户的密码，该用户是在用户主体名称中指定的用户。请包括域名，例如 jdoe@example.com。

Active Directory LDAP Server 和 OpenLDAP Server 标识源设置

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

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

表 2-2 LDAP Server Active Directory 和 OpenLDAP 设置

字段	描述
名称	标识源的名称。
用户的基本 DN	用户的基本域名。
域名	域的 FDQN，例如，example.com。请勿在此字段提供 IP 地址。
域别名	对于 Active Directory 标识源，该别名为域的 NetBIOS 名称。如果要使用 SSPI 身份验证，则将 Active Directory 域的 NetBIOS 名称添加为标识源的别名。 对于 OpenLDAP 标识源，如果不指定别名，则会添加大写字母域名。
组的基本 DN	组的基本域名。

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

字段	描述
主服务器 URL	域的主域控制器 LDAP 服务器。 请使用 ldap://hostname:port 或 ldaps://hostname:port 格式。端口通常为 389，用于 ldap： 连接，而 636 用于 ldaps: 连接。对于 Active Directory 多域控制器部署，该端口通常为 3268 用于 ldap: 连接，而 3269 用于 ldaps: 连接。 在主 LDAP URL 或辅助 LDAP URL 中使用 ldaps:// 时，需要一个证书为 Active Directory 服务器的 LDAPS 端点建立信任。
辅助服务器 URL	用于故障切换的辅助域控制器 LDAP 服务器的地址。
用户名	域中用户的 ID，该用户对用户和组的基本 DN 只具有最小只读权限。
密码	由“用户名”指定的用户的密码。

编辑 vCenter Single Sign-On 标识源

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

步骤

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

2 浏览到**管理 > Single Sign-On > 配置**。

3 单击**标识源**选项卡。

4 在表中右键单击标识源，然后选择**编辑标识源**。

5 编辑标识源设置。可用选项取决于所选标识源的类型。

选项	描述
Active Directory (已集成 Windows 身份验证)	对于本机 Active Directory 实施，请使用此选项。请参见第 23 页，“Active Directory 标识源设置”。
作为 LDAP 服务器的 Active Directory	此选项可用于向后兼容性。这需要您指定域控制器和其他信息。请参见第 23 页，“Active Directory LDAP Server 和 OpenLDAP Server 标识源设置”。
OpenLDAP	对于 OpenLDAP 标识源，请使用此选项。请参见第 23 页，“Active Directory LDAP Server 和 OpenLDAP Server 标识源设置”。
LocalOS	使用此选项可添加本地操作系统以作为标识源。系统仅提示您输入本地操作系统的名称。如果选择此选项，则指定计算机上的所有用户都对 vCenter Single Sign-On 可见，即使这些用户不属于其他域也是如此。

6 单击**测试连接**以确保可以连接到该标识源。

7 单击**确定**。

移除 vCenter Single Sign-On 标识源

vSphere 用户在标识源中定义。可从注册的标识源列表中移除标识源。

步骤

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

2 浏览到**管理 > Single Sign-On > 配置**。

3 在**标识源**选项卡上，选择一个标识源，然后单击**删除标识源**图标。

4 遇到确认提示时，请单击**是**。

移除安全令牌服务 (STS) 证书

vCenter Single Sign-On 提供了安全令牌服务 (STS)。安全令牌服务是一项发布、验证和续订安全令牌的 Web 服务。当现有 vCenter Single Sign-On STS 证书过期或发生更改时，您可以将其移除。

步骤

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

2 浏览到**管理 > Sign-On > 配置**。

3 选择**证书**选项卡。

4 选择 **STS 签名**选项卡，然后选择要移除的证书。

5 单击**删除 STS 签名证书**图标。

6 单击**是**。

此时证书将从 vCenter Single Sign-On 服务器中移除，且不再显示在 **STS 签名**选项卡上。

下一步

重新启动 vSphere Web Client。

刷新安全令牌服务 (STS) 根证书

vCenter Single Sign-On 提供了安全令牌服务 (STS)。安全令牌服务是一项发布、验证和续订安全令牌的 Web 服务。现有安全令牌服务证书过期或更改时，您可手动对其进行刷新。

STS 证书定期过期或更改，必须对其进行更新或刷新。在某些环境中，系统管理员可能会实施证书自动更新。如果未自动更新，您可以手动更新证书。

注意 vCenter 证书自动化工具只能替换 SSL 证书。此工具不能用于替换 STS 证书。

步骤

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

2 浏览到**管理 > Single Sign-On > 配置**。

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

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

如果密钥库文件有效，STS 证书表中会填充证书信息。

5 单击**确定**。

新证书信息会显示在 **STS 签名**选项卡上。

下一步

重新启动 vSphere Web Client 服务。

确定 SSL 证书的过期日期

CA 签名的 SSL 证书在预定义的使用期限之后过期。知道证书何时过期使您能够在过期日期之前重新替换或更新证书。

步骤

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

2 浏览到**管理 > Single Sign-On > 配置**。

3 单击**证书**选项卡，然后单击**标识源信任库**子选项卡。

4 查找证书并在**有效期至**文本框中确认过期日期。

您可能会在选项卡的顶部看到一个警告，表示证书将要过期。

下一步

更新或替换将要过期的 SSL 证书。

确定是否正在使用证书

开始替换证书之前，可以检查您拥有的证书是否已在使用中。可以使用**计算使用情况**功能确定系统是否正在使用证书。

步骤

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

2 浏览到**管理 > Single Sign-On > 配置**。

3 单击**证书**选项卡，然后单击**标识源信任库**子选项卡。

4 单击**计算使用情况**。

对于列表中的每个证书，vSphere Web Client 将与每个已注册的 LDAPS 标识源通信，以确定是否存在有效连接。

5 “由域使用”列显示证书是否正在使用，并帮助确定您是否能够安全地移除证书。

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

您可以在 vCenter Single Sign-On 中使用 Windows 会话身份验证 (SSPI)。要使该复选框显示在登录页面上，必须安装客户端集成插件。

使用 SSPI 可为当前已登录计算机的用户加快登录速度。

前提条件

必须正确设置 Windows 域。

步骤

1 导航到 vSphere Web Client 登录页面。

2 如果**使用 Windows 会话身份验证**复选框不可用，请单击位于登录页面底部的**下载客户端集成插件**。

3 如果浏览器通过发出证书错误或运行弹出窗口阻止程序阻止安装，请按照浏览器的“帮助”说明解决该问题。

4 如果系统提示您关闭其他浏览器，则执行此操作。

安装后，此插件将适用于所有浏览器。

5 退出然后重新启动浏览器。

重新启动后，便可以选中**使用 Windows 会话身份验证**复选框。

管理 vCenter Single Sign-On 用户和组

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

vCenter Single Sign-On 管理员用户可以执行以下任务。

- 添加 vCenter Single Sign-On 用户第 27 页，

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

- 禁用和启用 vCenter Single Sign-On 用户第 28 页，

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

- 删除 vCenter Single Sign-On 用户第 28 页，

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

- 编辑 vCenter Single Sign-On 用户第 29 页，

  您可从 vSphere Web Client 中更改 vCenter Single Sign-On 用户的密码或其他详细信息。您不能更改用户的用户名。

- 添加 vCenter Single Sign-On 组第 29 页，

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

- 编辑 vCenter Single Sign-On 组第 30 页，

  可以在 vSphere Web Client 中更改 vCenter Single Sign-On 组的描述。无法更改组名称。

- 向 vCenter Single Sign-On 组添加成员第 30 页，

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

- 从 vCenter Single Sign-On 组中移除成员第 31 页，

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

- 删除 vCenter Single Sign-On 应用程序用户第 31 页，

  vCenter Single Sign-On 可识别 vCenter 服务（例如 vCenter Server、vCenter Inventory Server 和 vSphere Web Client）以及向这些服务授予特权作为应用程序用户。

- 更改 vCenter Single Sign-On 密码第 31 页，

  vsphere.local 域中的用户可以从 vSphere Web Client 中更改其 vCenter Single Sign-On 密码。其他域中的用户更改密码时应遵循对应域的规则。

添加 vCenter Single Sign-On 用户

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

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

步骤

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

2 浏览到**管理 > Single Sign-On > 用户和组**。

3 在**用户**选项卡上，单击**新建用户**图标。

4 如果 vsphere.local 不是当前选择的域，请从下拉菜单中选择此域。

您不能将用户添加到其他域。

5 键入新用户的用户名和密码。

创建用户后，将不能更改其用户名。

密码必须符合系统的密码策略要求。

6 （可选）键入新用户的名字和姓氏。

7 （可选）输入此用户的电子邮件地址和描述。

8 单击**确定**。

添加某个用户时，该用户最初没有执行管理操作的权限。

下一步

将该用户添加到 vsphere.local 域中的一个组（例如，管理员组）。请参见第 30 页，“向 vCenter Single Sign-On 组添加成员”。

禁用和启用 vCenter Single Sign-On 用户

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

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

前提条件

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

步骤

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

2 浏览到**管理 > Single Sign-On > 用户和组**。

3 选择一个用户，单击**禁用**图标，然后在系统提示时单击**是**。

4 要再次启用此用户，请右键单击该用户，选择**启用**，然后在系统提示时单击**是**。

删除 vCenter Single Sign-On 用户

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

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

步骤

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

2 浏览到**管理 > Single Sign-On > 用户和组**。

3 选择**用户**选项卡，然后选择 vsphere.local 域。

4 在用户列表中，选择要删除的用户，然后单击**删除**图标。

请谨慎执行后续操作。您无法撤消此操作。

编辑 vCenter Single Sign-On 用户

您可从 vSphere Web Client 中更改 vCenter Single Sign-On 用户的密码或其他详细信息。您不能更改用户的用户名。

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

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

步骤

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

2 浏览到**管理 > Single Sign-On > 用户和组**。

3 单击**用户**选项卡。

4 右键单击用户，然后选择**编辑用户**。

5 对用户进行更改。

您不能更改用户的用户名。

密码必须符合系统的密码策略要求。

6 单击**确定**。

添加 vCenter Single Sign-On 组

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

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

步骤

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

2 浏览到**管理 > Single Sign-On > 用户和组**。

3 选择**组**选项卡上，单击**新建组**图标。

4 输入组的名称和描述。

创建组后，将不能更改组名称。

5 单击**确定**。

下一步

- 向组添加成员。

编辑 vCenter Single Sign-On 组

可以在 vSphere Web Client 中更改 vCenter Single Sign-On 组的描述。无法更改组名称。

vCenter Single Sign-On 组存储在 vCenter Single Sign-On 数据库中，该数据库在安装了 vCenter Single Sign-On 的系统上运行。这些组属于 vsphere.local 域。

步骤

1. 以 administrator@vsphere.local 或拥有 vCenter Single Sign-On 管理员特权的其他用户的身份登录到 vSphere Web Client。
2. 浏览到**管理 > Single Sign-On > 用户和组**。
3. 单击**组**选项卡。
4. 右键单击要编辑的组，然后选择**编辑组**。
5. 编辑组描述。

   创建组后，将不能更改组名称。
6. 单击**确定**。

向 vCenter Single Sign-On 组添加成员

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

在 vSphere Web Client 的**组**选项卡上列出的组在 vCenter Single Sign-On 内部，是 vsphere.local 域的一部分。您可以将其他域中的组成员添加到本地组。还可以嵌套组。

步骤

1. 以 administrator@vsphere.local 或拥有 vCenter Single Sign-On 管理员特权的其他用户的身份登录到 vSphere Web Client。
2. 浏览到**管理 > Single Sign-On > 用户和组**。
3. 单击**组**选项卡，然后单击组（例如“管理员”）。
4. 在“组成员”区域中，单击**添加成员**图标。
5. 选择包含要添加到组中的成员的标识源。
6. （可选）输入搜索词，然后单击**搜索**。
7. 选择成员，然后单击**添加**。

   可以同时添加多个成员。
8. 单击**确定**。

选定用户或组将成为该组的成员，并显示在“组”选项卡的底部面板中。

从 vCenter Single Sign-On 组中移除成员

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

步骤

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

2 浏览到**管理 > Single Sign-On > 用户和组**。

3 选择**组**选项卡，然后单击组。

4 在组成员列表中，选择要移除的用户或组，然后单击**移除成员**图标。

5 单击**确定**。

用户将从组中移除，但在系统中仍然可用。

删除 vCenter Single Sign-On 应用程序用户

vCenter Single Sign-On 可识别 vCenter 服务（例如 vCenter Server、vCenter Inventory Server 和 vSphere Web Client）以及向这些服务授予特权作为应用程序用户。

卸载 vCenter 服务时，默认情况下该服务将在卸载过程中从 vCenter Single Sign-On 应用程序用户的列表中移除。如果您强制移除某个应用程序，或者如果当应用程序用户仍在系统中时系统变为不可恢复，则您可以从 vSphere Web Client 中明确移除该应用程序用户。

重要事项 如果您移除了某个应用程序，该应用程序将不再能够访问 vCenter Single Sign-On。

步骤

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

2 浏览到**管理 > Single Sign-On > 用户和组**。

3 单击**应用程序用户**选项卡，然后单击应用程序用户名。

4 单击**删除应用程序用户**图标。

5 单击**是**。

应用程序（或解决方案）将不再能够访问 vCenter Server，并且无法发挥 vCenter 服务的作用。

更改 vCenter Single Sign-On 密码

vsphere.local 域中的用户可以从 vSphere Web Client 中更改其 vCenter Single Sign-On 密码。其他域中的用户更改密码时应遵循对应域的规则。

在 vCenter Single Sign-On 配置界面中定义的密码策略决定了密码何时过期。默认情况下，vCenter Single Sign-On 密码在 90 天后过期，但是系统管理员可以根据贵组织的策略对此默认值进行更改。密码即将过期时，vSphere Web Client 将向您发出提醒。如果您知道旧密码，则可以重置过期的密码。

步骤

1 使用您的 vCenter Single Sign-On 凭据登录到 vSphere Web Client。

2 在上方的导航窗格中“帮助”菜单的左侧，单击您的用户名以弹出下拉菜单。

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

3 选择**更改密码**，然后键入您的新密码。

4 键入新密码并确认。

该密码必须符合密码策略。

5 单击**确定**。

对 vCenter Single Sign-On 进行故障排除

配置 vCenter Single Sign-On 的过程可能很复杂。

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

vCenter Single Sign-On 安装失败

在 Windows 环境中，vCenter Single Sign-On 安装可能因多种原因失败。

问题

在 Windows 环境中，vCenter Single Sign-On 安装会失败。

原因

安装失败有多种原因。

解决方案

1 验证是否满足所有安装设置必备条件。

安装失败时，安装程序会显示类似以下内容的消息：`####: 安装因...失败 (####: Installation failed due to...)`

2 在命令行中，运行以下命令以收集 vCenter Single Sign-On 支持捆绑包。

```
C:\Windows\System32\cscript.exe "SSO Server\scripts\sso-support.wsf" /z
```

3 单击**确定**

4 查看 `%TEMP%\vminst.log` 中的日志，了解有关失败问题和可行解决方法的详细信息。

有关日志的完整列表，请参阅 VMware 知识库文章 2033430。

确定 Lookup Service 错误的原因

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

问题

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

原因

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

解决方案

1 验证运行 vCenter Single Sign-On、vCenter Server 和 Web Client 的主机上的时钟是否同步。

2 查看错误消息中指明的特定日志文件。

在该消息中，系统临时文件夹指的是 `%TEMP%`。

3 在日志文件中，搜索以下消息。

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

消息	原因和解决方案
java.net.ConnectException:连接超时：连接	IP 地址不正确、防火墙阻止了对 vCenter Single Sign-On 的访问，或者 vCenter Single Sign-On 过载。 确保防火墙未阻止 vCenter Single Sign-On 端口（默认为 7444），并且安装有 vCenter Single Sign-On 的计算机拥有足够多可用的 CPU、I/O 及 RAM 容量。
java.net.ConnectException:Connection refused:连接	IP 地址或 FQDN 不正确，并且 vCenter Single Sign-On 未启动或曾经启动过，但当前已停止运行。 通过检查 vCenter Single Sign-On 服务 (Windows) 和 vmware-sso 守护进程 (Linux) 的状态，确认 vCenter Single Sign-On 运行正常。 重新启动服务。如果这未能解决问题，请参见《vSphere 故障排除指南》的“恢复”部分。
异常状态代码：404. 初始化期间 SSO Server 发生故障	重新启动 vCenter Single Sign-On。如果这未能解决问题，请参见《vSphere 故障排除指南》的“恢复”部分。
UI 中显示的错误，以无法连接到 vCenter Single Sign-on (Could not connect to vCenter Single Sign-on) 开头。	您还会看到返回码 `SslHandshakeFailed`。这种错误并不常见。它表明所提供的解析为 vCenter Single Sign-On 主机的 IP 地址或 FQDN 不是安装 vCenter Single Sign-On 时所使用的 IP 地址或 FQDN。 在 `%TEMP%\VM_ssoreg.log` 中，找到包含以下消息的行。 `host name in certificate did not match:<install-configured FQDN or IP> != <A> or <B> or <C>`，其中 A 表示您在 vCenter Single Sign-On 安装期间输入的 FQDN，B 和 C 表示系统生成的允许替代值。 将配置更正为使用该日志文件中的 != 符号右侧的 FQDN。大多数情况下，使用在 vCenter Single Sign-On 安装期间指定的 FQDN。 如果这些替代值均不适用于您的网络配置，则请恢复您的 vCenter Single Sign-On SSL 配置。

无法使用 Active Directory 域身份验证进行登录

您从 vSphere Web Client 登录 vCenter Server 组件。使用您的 Active Directory 用户名和密码。身份验证失败。

问题

您将 Active Directory 标志源添加到 vCenter Single Sign-On，但用户无法登录 vCenter。

原因

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

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

解决方案

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

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

1 同步 vCenter Server Appliance 和 Active Directory 域控制器之间的时钟。

2 验证每个域控制器在 Active Directory 域 DNS 服务中是否均有指针记录 (PTR)，并验证 PTR 记录信息与控制器的 DNS 名称是否匹配。使用 vCenter Server Appliance 时，可以运行以下命令来执行此任务：

a 要列出域控制器，请运行以下命令：

```
# dig SRV _ldap._tcp.my-ad.com
```

相关地址位于回答部分，如以下示例中所示：

```
;; ANSWER SECTION:
_ldap._tcp.my-ad.com. (...) my-controller.my-ad.com
...
```

b 对于每个域控制器，请运行以下命令验证正向和反向解析：

```
# dig my-controller.my-ad.com
```

相关地址位于回答部分，如以下示例中所示：

```
;; ANSWER SECTION:
my-controller.my-ad.com (...) IN A controller IP address
...
```

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

相关地址位于回答部分，如以下示例中所示：

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

3 如果执行上述步骤未能解决问题，请从 Active Directory 域中删除 vCenter Server Appliance，然后重新加入域。

4 重新启动 vCenter Single Sign-On。

由于用户帐户被锁定，vCenter Server 登录失败

从 vSphere Web Client 登录页面登录 vCenter Server 时，出现指示帐户被锁定的错误。

问题

多次尝试均失败后，将无法使用 vCenter Single Sign-On 登录到 vSphere Web Client。您会看到消息指明您的帐户被锁定。

原因

您已超出失败登录尝试次数上限。

解决方案

- 如果作为系统域 (vsphere.local) 中的用户进行登录，请要求您的 vCenter Single Sign-On 管理员解锁您的帐户。或者，如果在密码策略中将此锁定设置为过期，则可以等待帐户解锁。
- 如果以 Active Directory 或 LDAP 域中的用户身份登录，请要求您的 Active Directory 或 LDAP 管理员解锁您的帐户。

vSphere 安全证书和加密 3

ESXi 和 vCenter Server 组件通过 SSL 安全地进行通信，从而确保保密性、数据完整性和身份验证。数据是专用的受保护数据，并且只要有人在传输过程中对其进行修改，就将被检测到。

默认情况下，vSphere 服务使用作为安装过程的一部分进行创建并存储在每个系统上的证书。这些默认证书是唯一的，使用这些证书后便可以开始使用软件，但它们不是由可信证书颁发机构 (CA) 签名的。

若要享受证书检查的最大优势，特别是，如果您要使用 Internet 上的 SSL 连接，则应安装由有效内部证书授权机构签名的新证书，或从您信任的安全授权机构那里购买新证书。

本章讨论了以下主题：

在 vSphere 中使用的证书

在 vSphere 环境中，不同类型的证书用于实现不同的目的。

vCenter Single Sign-On STS 服务发布的 SAML 令牌

凡是通过 vCenter Single Sign-On 登录的用户，均可通过 STS 证书使用 vCenter Single Sign-On 支持的任意 vCenter 服务，而无需逐个进行身份验证。STS 服务会发出安全断言标记语言 (SAML) 令牌。这些安全令牌表示受 vCenter Single Sign-On 支持的标识源类型之一中的用户标识。请参见第 11 页，“如何使用 vCenter Single Sign-On 保护您的环境”。

vCenter Single Sign-On 服务负责部署身份提供程序，该提供程序可发布由 vSphere 用于进行身份验证的 SAML 令牌。SAML 令牌是表示用户身份（用户名、名字、姓氏）的一块 XML。此外，SAML 令牌中包含组成员资格信息，以便能够用于授权操作。在 vCenter Single Sign-On 发布 SAML 令牌时，它将使用证书链对每个令牌进行签名，以便 vCenter Single Sign-On 的客户端可以验证 SAML 令牌是否来自可信源。

SSL 证书

SSL 证书可确保整个 vSphere 环境中的通信安全。加密之前，客户端验证 SSL 握手阶段提供的证书的真实性。此验证可防止“中间人”攻击。

VMware 产品使用标准 X.509 版本 3 (X.509v3) 证书来加密通过组件之间的安全套接字层 (SSL) 协议连接发送的会话信息。

vSphere 组件中包含默认证书。可以将默认证书替换为自签名证书或 CA 签名的证书。对于 vCenter 核心组件，可以使用证书自动化工具。

SSH 密钥

SSH 密钥用于控制对使用 Secure Shell (SSH) 协议的 ESXi 主机的访问。请参见第 83 页，“将 SSH 密钥上载到 ESXi 主机”。

密码强度

为了加密数据，发送组件（如网关或重定向程序）会应用加密算法或密码，在传输数据之前改变这些数据。接收组件使用密钥解密这些数据，将其还原为原始形式。目前有几种密码正在使用，每种密码提供的安全级别也有所差异。密码保护数据的能力的一种衡量方法是其密码强度，即加密密钥的位数。位数越大，密码越安全。

管理员在准备证书请求时会指定所需的密码强度。公司策略可能会规定管理员所选择的密码强度。

用于密钥交换的 256 位 AES 加密和 1024 位 RSA 是以下连接的默认值。

- vSphere Web Client 通过管理界面到 vCenter Server 和 ESXi 的连接。
- SDK 与 vCenter Server 和 ESXi 的连接。
- 到虚拟机控制台的连接。
- 到 ESXi 的 直接 SSH 连接。

证书替换概述

对于核心 vCenter 组件，可以使用证书自动化工具生成证书请求并将默认证书替换为自签名证书或 CA 签名的证书。还可以不使用此工具而从命令行生成请求、创建证书和替换证书。

信息来源

您希望替换证书的方式决定信息的来源。可以通过多种方式执行证书替换。

- 在 Windows 环境中使用证书替换工具，如本文档中所述。
- 在 Windows 中显式替换证书，如 VMware 知识库文章 2058519 中所述。
- 在 vCenter Server Appliance 中替换证书，如 VMware 知识库文章 2057223 中所述。

如果您希望使用 CA 签名的证书，则必须为每个组件生成一个证书请求 (CSR)。可以使用此工具生成 CSR。有关证书要求的列表，请参见第 39 页，“准备您的环境”。

证书替换工具概述

证书自动化工具是一个命令行工具，可帮助您替换下面列出的核心 vCenter 组件的证书。大多数情况下，应将默认证书替换为自定义证书。可以在安装所有 vCenter 组件后使用此工具。如果您向 vSphere 环境中添加了新组件，则可以重新运行此工具，对新组件执行证书替换操作。在 vCenter Server 系统或 vCenter Single Sign-On 服务器等 vCenter 组件上运行此工具时，将执行以下任务。

- 提示您提供所需输入。
- 验证输入（x.509 证书及 URL 格式）。
- 更新某个组件以及该组件公开的服务的相应 LookupService 条目的 SSL 证书（如有需要）。
- 重新启动相应的服务（如有需要）。

- 更新该组件对自身连接到的所有其他组件的信任。重新启动该组件（如有需要）。
- 根据需要向用户提供后续步骤。

注意 通过此工具进行证书替换已经过测试，可以对 vCenter Single Sign-On、vCenter Inventory Service、vCenter Server、vSphere Web Client、vSphere Update Manager、vCenter 日志浏览器和 vCenter Orchestrator 使用。如果您需要对其他 vSphere 组件执行证书替换，请参见该产品的 VMware 文档或 VMware 知识库中的说明。作为过程的一部分，您可能需要在支持的其中一个组件上更新证书。

此工具支持以下 vCenter 组件：

- vCenter Single Sign-On
- vCenter Inventory Service
- vCenter Server
- vSphere Web Client
- vSphere Update Manager
- vCenter 日志浏览器
- vCenter Orchestrator

每个组件都必须具有一个 SSL 证书和一个解决方案用户证书。大多数组件使用相同的证书来实现这两种目的。在 Windows 上，解决方案用户证书必须唯一，因此需要为每个组件提供一个唯一的 SSL 证书。

升级

如果您替换了 vSphere 版本 5.0 或 5.1 中的默认证书，然后升级到 vSphere 版本 5.5，则会迁移证书。如果您在升级过程中希望替换默认证书，可以在升级后运行证书自动化工具。

证书自动化工具部署选项

vCenter 证书自动化工具可自动为 Windows 操作系统中的核心 vCenter 组件续订证书。

此工具支持多种部署选项。此工具与用户的交互方式取决于部署选项。请参见第 36 页，“证书替换概述”

所有服务位于一台计算机上

您可以编辑 `ssl-environment.bat` 文件并输入环境特定的信息，然后在该计算机上运行此工具而不会收到提示。您还可以运行此工具并在提示时提供输入。

每项服务位于独立的计算机上

如果每项服务都在您的环境中的独立计算机或虚拟机上运行，请按照下述步骤进行操作以更新证书。如果其中某些服务在同一台计算机上运行，请按照证书自动化工具生成的 Update Planner 列表中的信息进行操作。如果您的环境中未包含某些服务，则可以跳过相应的步骤。

1. 在一台计算机上安装并运行此工具。此工具将生成 Update Planner 列表。
2. 在运行 vCenter Single Sign-on 的计算机上安装并运行此工具以更新 vCenter Single Sign-On SSL 证书。
3. 在 Inventory Service 计算机上安装并运行此工具。此工具将执行以下任务：
   a. 更新从 vCenter Inventory Service 到 vCenter Single Sign-On 的信任关系。
   b. 更新 vCenter Inventory Service SSL 证书。
4. 在运行 vCenter Server 的计算机上安装并运行此工具。此工具将执行以下任务：
   a. 更新从 vCenter Server 服务到 vCenter Single Sign-On 服务的信任关系。

b 更新 vCenter Server SSL 证书。

c 更新从 vCenter Server 到 vCenter Inventory Service 的信任关系。

d 更新从 vCenter Server 到 vSphere Update Manager 的信任关系。

5 在 vCenter Orchestrator 计算机上安装并运行此工具。此工具将执行以下任务：

a 更新从 vCenter Orchestrator 服务到 vCenter Single Sign-On 服务的信任关系。

b 更新从 vCenter Orchestrator 服务到 vCenter Server 服务的信任关系。

c 更新 vCenter Orchestrator SSL 证书。

6 在 vSphere Web Client 计算机上安装并运行此工具。此工具将执行以下任务：

a 更新从 vSphere Web Client 到 vCenter Single Sign-On 服务的信任关系。

b 更新从 vSphere Web Client 到 vCenter Inventory Service 的信任关系并重新启动该服务。

c 更新从 vSphere Web Client 到 vCenter Server 服务的信任关系并重新启动该服务。

d 更新从 vSphere Web Client 到 vCenter Orchestrator 服务的信任关系并重新启动该服务。

e 更新 vSphere Web Client SSL 证书。

必须重新启动 vSphere Web Client 才能完成信任关系的更新。

7 在日志浏览器计算机上安装并运行此工具。vSphere Web Client 和 vCenter 日志浏览器始终在同一台计算机上运行。此工具将执行以下任务。

a 更新从日志浏览器服务到 vCenter Single Sign-On 服务的信任关系。

b 更新日志浏览器 SSL 证书。

8 在 vSphere Update Manager 计算机上安装并运行此工具。

此工具将更新 vSphere Update Manager SSL 证书。作为证书更新的一部分，还将更新 vCenter Server 对 vSphere Update Manger 的信任。

混合模式部署

如果采用混合模式部署，例如，有两项服务位于某一台计算机上，有三项服务位于另一台计算机上，您可以按每项服务都位于不同计算机上的模式运行此工具。

使用 vCenter 证书自动化工具替换 vCenter 证书

如果公司策略有相关要求，您可以将默认的 vCenter SSL 证书替换为由 CA 签名的证书或自签名证书。vCenter 证书自动化工具是一个命令行工具，可帮助您按正确顺序替换环境中核心 vCenter 服务的证书。可以使用此工具生成证书请求、生成更新计划以及执行更新。

每项 vSphere 服务都具有一个标识，用于创建 x509 证书。可以通过 vCenter 证书自动化工具替换核心 vCenter 组件的证书。可以手动替换其他 vCenter 组件的证书。

- 使用 vCenter 证书自动化工具可替换安装在受支持的 Windows 操作系统中的 vCenter 组件的 SSL 证书。此工具可帮助您生成证书请求以及规划替换证书的过程。此工具支持 vCenter Single Sign-On、vCenter Inventory Service、vCenter Server、vSphere Web Client、vSphere Update Manager、vCenter 日志浏览器和 vCenter Orchestrator。
- 如果使用的是其他 vSphere 组件，请参见 VMware 文档或 VMware 知识库文章中的证书替换信息。
- 如果使用的是第三方组件，则必须手动替换证书。请参见 VMware 知识库文章 2058519。

- 如果使用的是 vCenter Server Appliance，请手动替换 SSL 证书。某些服务会共享证书。请参见 VMware 知识库文章 2057223。

替换证书包含多项任务。

1 准备您的环境第 39 页，

   在运行 vCenter 证书自动化工具之前，请确认您正运行于一个受支持的操作系统中，并确认使用的平台正确、证书满足要求，并且系统设置满足要求。

2 安装 vCenter 证书自动化工具第 41 页，

   可以在装有 vCenter 核心组件的每台计算机上安装 vCenter 证书自动化工具。要执行初始规划，可以在一台计算机上安装此工具。

3 预定义 vCenter 证书自动化工具的默认值第 41 页，

   在此工具的配置文件中预定义默认值有助于防止出现键入错误，并且可以节约时间。预定义默认值后，此工具不再提示您输入这些值。不能指定默认密码。

4 生成证书请求并设置 CA 签名证书第 42 页，

   如果您要使用由 CA（证书颁发机构）生成的受信任的证书，则必须创建证书请求并提交至 CA。

5 运行 Update Planner 第 42 页，

   Update Planner 属于 vCenter 证书自动化工具的一部分，可帮助您确定证书替换的正确顺序。请按照此工具建议的顺序执行各步骤以获得最佳结果。

6 运行证书自动化工具以更新 SSL 证书和信任第 44 页，

   获取 SSL 证书并生成更新步骤的列表后，可以运行此工具以替换现有证书、重新建立信任以及有选择地重新启动某些服务。

7 回滚更新第 45 页，

   每个更新操作都可成功执行一次证书和密钥的更新，或者失败但保留原始状态。如果更新失败，您可能需要回滚失败的步骤。

准备您的环境

在运行 vCenter 证书自动化工具之前，请确认您正运行于一个受支持的操作系统中，并确认使用的平台正确、证书满足要求，并且系统设置满足要求。

请查阅 VMware 知识库文章 2057340 中列出的已知问题。

支持的平台

该工具已在下述 Windows 操作系统中进行了测试。

- Windows 2008 R2 SP1
- Windows 2012 Standard

工具和产品版本

不同版本的 vSphere 支持不同版本的证书自动化工具。

- vSphere 5.1 支持 1.0 版的证书自动化工具
- vSphere 5.1 Update 1 支持 1.0.1 版的证书自动化工具
- vSphere 5.5 支持 5.5 版的证书自动化工具

证书要求

可以在运行该工具之前取得 CA 签名的证书，或者可以使用该工具生成证书请求。在运行该工具以更换证书之前，确保证书满足以下要求：

- 每个 vSphere 组件的 SSL 证书都有一个唯一的基本 DN。
- 证书和专用密钥满足以下要求：
  - 专用密钥算法：RSA
  - 专用密钥长度 >= 1024
  - 专用密钥标准：PKCS#1 或 PKCS#8
  - 专用密钥存储：PEM
- 建议的证书签名算法：
  - sha256WithRSAEncryption 1.2.840.113549.1.1.11
  - sha384WithRSAEncryption 1.2.840.113549.1.1.12
  - sha512WithRSAEncryption 1.2.840.113549.1.1.13

  注意 不建议使用的算法包括 md2WithRSAEncryption 1.2.840.113549.1.1.2、md5WithRSAEncryption 1.2.840.113549.1.1.4 和 sha1WithRSAEncryption 1.2.840.113549.1.1.5。不支持 OID 为 1.2.840.113549.1.1.10 的算法 RSASSA-PSS。
- 证书链格式满足以下要求：
  - 不包含任何注释的单个 PEM 文件。
  - 该文件以第一个证书的标头开始，即 `-----BEGIN CERTIFICATE-----`。
  - 自签名证书按从叶到根的顺序排列。
  - 文件中没有额外的证书。
  - 证书链完整。
- 证书和密钥的路径或文件名不包含以下任何特殊字符：
  - ^（脱字符）
  - %（百分号）
  - &（& 号）
  - ;（分号）
  -)（右括号）

  如果遇到上述字符，该工具将退出并引发异常，或者报告未找到证书或密钥文件。

系统要求

安装所有 vCenter 组件，获取管理员权限，并关闭从属解决方案，如下所述：

- 确认已安装并运行需要证书更新的所有 vCenter 组件，并且有权访问每个组件的服务器。
- 确认在运行工具时所在的一个或多个服务器上具有管理权限。尽管非管理员用户可以关闭和启动该工具，但如果没有正确权限，所有操作都将失败。
- 关闭环境中运行的以下从属解决方案：
  - VMware Site Recovery Manager

- vSphere Data Recovery
- vCloud Director
- 可能连接 vCenter Server 的任何第三方解决方案

安装 vCenter 证书自动化工具

可以在装有 vCenter 核心组件的每台计算机上安装 vCenter 证书自动化工具。要执行初始规划，可以在一台计算机上安装此工具。

在规划了证书更新且运行服务的每台物理机或虚拟机上安装此工具。安装此工具时可以采用多种配置。请参见第 37 页，“证书自动化工具部署选项”。

注意 不同版本的 vSphere 支持不同版本的证书自动化工具。

- vSphere 5.1 支持 1.0 版的证书自动化工具
- vSphere 5.1 Update 1 支持 1.0.1 版的证书自动化工具
- vSphere 5.5 支持 5.5 版的证书自动化工具

前提条件

- 验证是否已满足所有要求。请参见第 39 页，“准备您的环境”。
- 安装此工具之前，请为装有 vSphere 组件的每台计算机获取证书，或者使用此工具生成证书签名请求 (CSR) 并从证书颁发机构获取证书。请参见第 42 页，“生成证书请求并设置 CA 签名证书”。

步骤

1 下载 vCenter 证书自动化工具。

下载项位于 VMware vSphere 下载页面的“驱动程序和工具”部分。

2 对于初始规划，请将下载的 ZIP 文件复制到一台计算机并生成 Update Planner 列表。

3 您可能需要将下载的 ZIP 文件复制到装有 vCenter 核心组件的每一台计算机上，具体取决于您的部署情况。

4 将该文件解压到任意目录，但保留目录结构。

下一步

可以预定义首选默认值，请参见第 41 页，“预定义 vCenter 证书自动化工具的默认值”，或者响应在运行此工具时出现的提示。

如果有新版本的工具可用，您可以下载该版本并解压到其他目录，然后删除旧版本的工具。

预定义 vCenter 证书自动化工具的默认值

在此工具的配置文件中预定义默认值有助于防止出现键入错误，并且可以节约时间。预定义默认值后，此工具不再提示您输入这些值。不能指定默认密码。

预定义默认值并非必需的操作，但以后可以帮助您加快处理速度。如果此工具未遇到默认值，则会向您发出提示。

前提条件

确认 vCenter 证书自动化工具未运行。此工具在您启动时读取 `ssl-environment.bat` 中的值。

步骤

1 在文本编辑器中打开 `ssl-environment.bat`。

2 指定要为需要使用更新证书的每个 vSphere 组件更改的参数。

例如，对于 vCenter Server，可以编辑 `vc_cert_chain`、`vc_private_key` 和 `vc_username` 参数。

3 保存并关闭 `ssl-environment.bat`。

4 启动此工具。

此工具在您每次启动时选取默认值。

vCenter 证书自动化工具保存信息并使用该信息自动预填充所需的输入。

下一步

生成证书请求（如有需要）或运行 Update Planner（如果您在多台计算机上部署了此软件以规划证书更新任务）。请参见第 42 页，“运行 Update Planner”。

生成证书请求并设置 CA 签名证书

如果您要使用由 CA（证书颁发机构）生成的受信任的证书，则必须创建证书请求并提交至 CA。

您可以为每个组件手动创建证书请求，也可以使用 vCenter 证书自动化工具生成证书请求。有关手动生成和替换的详细说明，请参见 VMware 知识库文章 2061934。

为了增强安全性，请在将使用证书的计算机上生成每个证书和专用密钥。

注意 该过程说明了如何准备 CA 签名证书。此工具也可与自签名证书一起使用。

步骤

1 如果要在环境中使用以下服务，您可以使用此工具为这些服务生成证书请求。

- vCenter Single Sign-On 服务
- vCenter Inventory Service
- vCenter Server
- vCenter Orchestrator
- vSphere Web Client
- vCenter 日志浏览器
- vCenter Update Manager

2 向您要使用的 CA 提交证书请求。

CA 将返回生成的证书和密钥。

3 稍后向工具提供证书和密钥时，此工具将生成 vCenter Single Sign-On 基础架构所需的 PFX 和 JKS 文件，并将其放置在正确位置。

下一步

- 运行此工具可生成 Update Planner 信息。

运行 Update Planner

Update Planner 属于 vCenter 证书自动化工具的一部分，可帮助您确定证书替换的正确顺序。请按照此工具建议的顺序执行各步骤以获得最佳结果。

步骤

1 登录安装了 vCenter 证书自动化工具的计算机。

2 从命令行导航到此工具解压到的位置并运行以下命令。

```
ssl-updater.bat
```

3 出现提示时，选择 `1. Plan your steps to update SSL certificates`。

4 输入与要更新的服务对应的编号。

- 要更新多个 SSL 证书，请用逗号分隔各编号。例如，要更新 vCenter Single Sign-On、vCenter Server 和 vSphere Web Client 上的 SSL 证书，请键入 **`1,3,4`**
- 要更新此工具支持的所有服务上的证书，请键入 8。

vSphere Web Client 和 vCenter 日志浏览器始终在同一台计算机上运行。

注意 输入要更新的所有服务。如果您最初将某些服务排除在外并稍后重新运行 Update Planner，这些步骤可能不正确并且更新可能会失败。

Update Planner 显示要执行的任务以及执行顺序。

5 将 Update Planner 输出保存到文本文件中。

所有证书都将被替换的环境的示例输出如下所示。

```
1. Go to the machine with Single Sign-On installed and
- Update the Single Sign-On SSL certificate.

2. Go to the machine with Inventory Service installed and
- Update Inventory Service trust to Single Sign-On.

3. Go to the machine with Inventory Service installed and
- Update the Inventory Service SSL certificate.

4. Go to the machine with vCenter Server installed and
- Update vCenter Server trust to Single Sign-On.

5. Go to the machine with vCenter Server installed and
- Update the vCenter Server SSL certificate.

6. Go to the machine with vCenter Server installed and
- Update vCenter Server trust to Inventory Service.

7. Go to the machine with Inventory Service installed and
- Update the Inventory Service trust to vCenter Server.

8. Go to the machine with vCenter Orchestrator installed and
- Update vCenter Orchestrator trust to Single Sign-On.

9. Go to the machine with vCenter Orchestrator installed and
- Update vCenter Orchestrator trust to vCenter Server.

10. Go to the machine with vCenter Orchestrator installed and
- Update the vCenter Orchestrator SSL certificate.

11. Go to the machine with vSphere Web Client installed and
- Update vSphere Web Client trust to Single Sign-On.

12. Go to the machine with vSphere Web Client installed and
- Update vSphere Web Client trust to Inventory Service.
```

```
13. Go to the machine with vSphere Web Client installed and
- Update vSphere Web Client trust to vCenter Server.

14. Go to the machine with vSphere Web Client installed and
- Update the vSphere Web Client SSL certificate.

15. Go to the machine with Log Browser installed and
- Update the Log Browser trust to Single Sign-On.

16. Go to the machine with Log Browser installed and
- Update the Log Browser SSL certificate.

17. Go to the machine with vSphere Update Manager installed and
- Update the vSphere Update Manager SSL certificate.

18. Go to the machine with vSphere Update Manager installed and
- Update vSphere Update Manager trust to vCenter Server.
```

6 键入 **9** 返回主菜单。

下一步

更新证书和信任。请参见第 44 页，“运行证书自动化工具以更新 SSL 证书和信任”。

运行证书自动化工具以更新 SSL 证书和信任

获取 SSL 证书并生成更新步骤的列表后，可以运行此工具以替换现有证书、重新建立信任以及有选择地重新启动某些服务。

有关此工具如何在不同部署中运行的概述，请参见第 37 页，“证书自动化工具部署选项”。

此工具向您提供更新任务的列表并指定要在上面执行每项任务的计算机。如果您选择了一项任务，此工具将提示您提供输入以执行该任务。例如，要更新 Inventory Service，您应从菜单中选择“Inventory Service”。此工具将提示您输入更新 Inventory Service 到 Single Sign-On 的信任关系以及更新 Inventory Service SSL 证书选项的信息。

依次执行以下任务。如果 Update Planner 指示您在多台计算机上执行任务，请保持此工具在每个计算机上运行以避免重新输入信息。

步骤

1 移至任务列表中的第一台计算机，然后通过运行 `ssl-updater.bat` 启动此工具。

此工具不会按名称列出计算机，但会将您指向正在运行服务的计算机。

2 选择更新 SSL 证书。

3 出现提示时，指定要更新其证书的服务。

如果您预先指定了默认值，则此工具不会向您发出提示。

要更新多个 SSL 证书，请更新一项服务的证书，然后继续在部署了下一项服务的计算机上运行相应的服务。每个 vSphere 组件的 SSL 证书必须唯一。

4 出现提示时，键入请求的信息，例如新 SSL 链和专用密钥的位置、密码等。

5 继续操作直至提供所有信息。

6 检查 Planner 是否能够执行下个步骤。

您可能需要在其他计算机上部署并启动此工具以更新某些服务。

7 完成更新计划后，可以关闭命令提示窗口以结束您的会话。

回滚更新

每个更新操作都可成功执行一次证书和密钥的更新，或者失败但保留原始状态。如果更新失败，您可能需要回滚失败的步骤。

开始执行升级过程之前，vCenter 证书自动化工具会在备份文件夹中保留现有证书信息的副本，确保您能够回滚到之前使用的证书，以保持整个系统已启动且正在运行。

可以使用此工具的菜单项以便能够回滚到原始状态。

注意 回滚 vCenter Server 证书后，必须重新更新 vCenter Server 到 VMware Update Manager 的信任关系。

替换 vCenter Server Appliance 证书

您可以替换 vCenter Server Appliance 证书。由于证书自动化工具仅在 Windows 上受支持，因此您必须手动替换证书。

在 vCenter Server Appliance 上使用自签名证书或 CA 签名证书替换默认 SSL 证书和密钥是一个手动过程。在 Linux 上无法使用证书自动化工具来更新证书和密钥。

前提条件

获取证书文件（包括证书和专用密钥）。

步骤

- 请按照 VMware 知识库文章 2057223 中的步骤进行操作。

替换 vCenter Server Heartbeat 证书

如果您在使用当前证书时遇到问题，或者如果贵公司的安全策略要求替换证书，则可以替换默认 vCenter Server Heartbeat 证书。

前提条件

- 在要替换证书的系统中安装 OpenSSL。
- 获取证书文件 `rui.crt`、`rui.key` 和 `rui.pfx`。

步骤

1. 从 VMware 知识库文章替换 vCenter Server Heartbeat 6.x 的 SSL 证书（Replacing SSL Certificates for vCenter Server Heartbeat 6.x，知识库文章 2013041）中下载 `SSLImport.jar` 实用程序。
2. 按照该知识库文章中的步骤替换证书。

vSphere 用户和权限

4

vCenter Single Sign-On 支持身份验证，这表明它可以确定用户究竟是否可以访问 vSphere 组件。此外，必须授权每位用户查看或操作 vSphere 对象。

vCenter Server 允许通过权限和角色对授权进行精细控制。首先查看有关权限的阶层式继承、权限验证和相关主题的背景信息。然后移至 vCenter Server 用户管理任务（第 55 页，第 5 章“vCenter 用户管理任务”）。

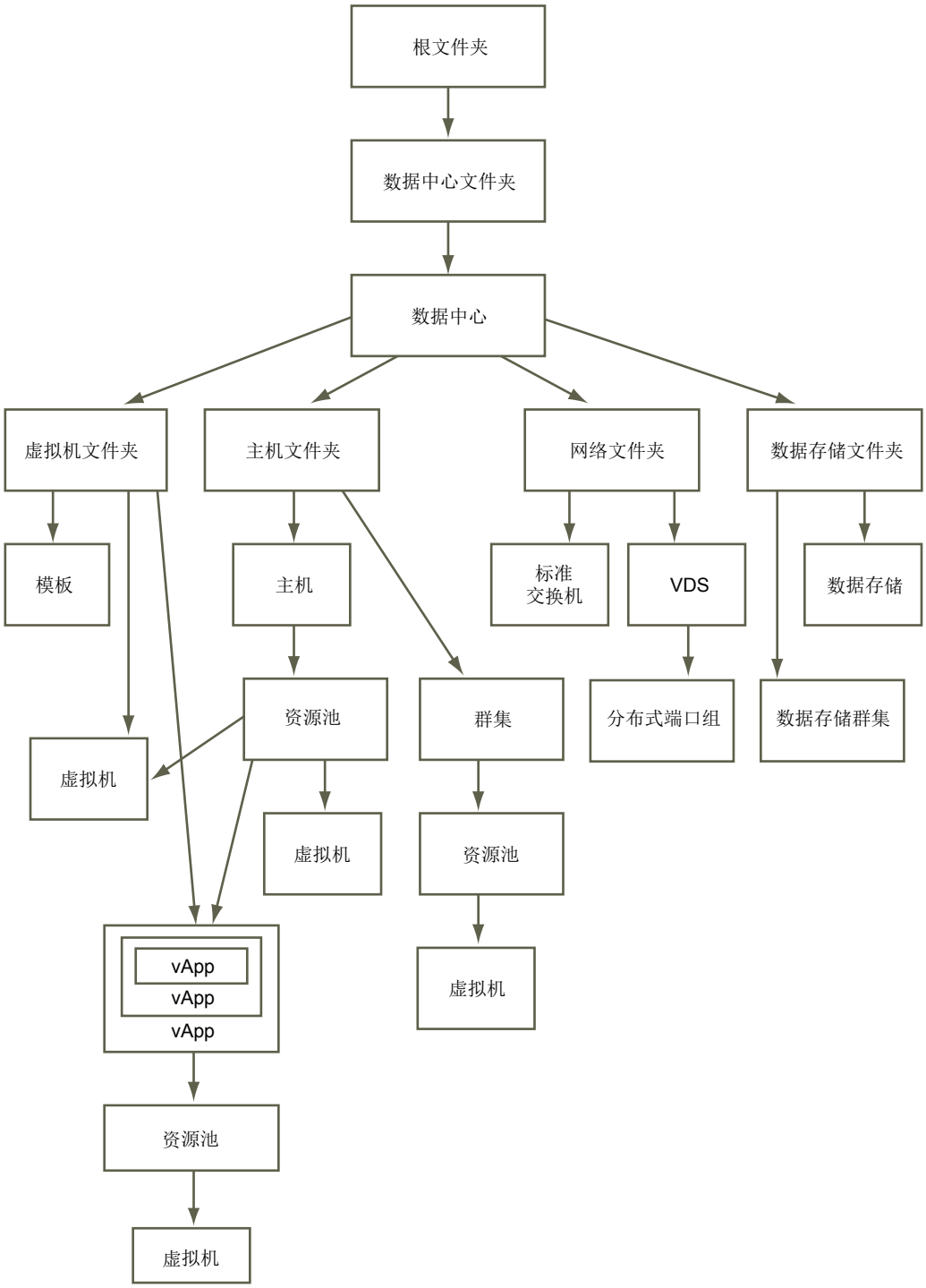
本章讨论了以下主题：

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。

图 4-1 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。要限制虚拟机上的用户的特权，必须同时在该虚拟机的父文件夹和父主机、群集或资源池上设置权限。

要为分布式交换机及其关联的分布式端口组设置权限，请为父对象（例如文件夹或数据中心）设置权限。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

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

全局实体从根 vCenter Server 系统中派生权限。

- 自定义字段
- 许可证
- 角色
- 统计间隔
- 会话

权限验证

使用活动目录的 vCenter Server 和 ESXi 主机会定期针对 Windows 活动目录域验证用户和组。一旦主机系统启动或到了 vCenter Server 设置中指定的固定时间间隔，即会执行验证。

例如，如果为用户 Smith 分配了权限并在域中将用户名更改为 Smith2，则在下次验证发生时主机会认为 Smith 已不存在并移除其权限。

再如，如果将用户 Smith 从域中移除，则在下次验证发生时所有权限都将被移除。如果在下次验证发生之前将新用户 Smith 添加到域，新用户 Smith 会接收分配给旧用户 Smith 的所有权限。

使用角色分配特权

角色是一组预定义的特权。特权定义用户执行操作和读取属性所需的个人权限。

当分配用户或组权限时，将用户或组与角色配对，并关联与清单对象配对的用户或组。单个用户对于清单中的不同对象可能有不同角色。例如，如果清单中有两个资源池（池 A 和池 B），可以为特定用户在池 A 上分配虚拟机用户角色而在池 B 上分配只读角色。执行上述分配后，该用户可以打开池 A 中的虚拟机，而只能查看池 B 中的虚拟机。

在主机上创建的角色与在 vCenter Server 系统上创建的角色是相互独立的。使用 vCenter Server 管理主机时，可以使用通过 vCenter Server 创建的角色。如果直接连接主机，则可以使用直接在主机上创建的角色。

vCenter Server 和 ESXi 主机提供以下默认系统角色和示例角色：

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 为方便起见提供了样本角色作为准则和建议。可以修改或移除这些角色。

有关创建、克隆和编辑角色的信息，请参见第 57 页，“vCenter Server 和 ESXi 中的角色”。

默认情况下，所有角色都允许用户调度任务。用户只能调度在创建任务时用户拥有执行权限的任务。

注意 即使所涉及到的用户已登录，对权限和角色的更改也会立即生效。但搜索除外，在搜索中，权限更改会在用户注销再重新登录之后才生效。

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，向组而不是单个用户授予权限。
- 仅在需要时授予权限。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。
- 使用文件夹将对象分组，使各组对象对应于要授予其的不同权限。
- 授予根 vCenter Server 级别的权限时要小心。具有根级别权限的用户有权访问 vCenter Server 上的全局数据，例如角色、自定义属性、vCenter Server 设置和许可证。对许可证和角色的更改会传播到链接模式组中的所有 vCenter Server 系统，即使用户在组中的所有 vCenter Server 系统上均没有权限。
- 大多数情况下，根据权限启用传播。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无权访问的层次结构的指定区域。

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。您可以在清单对象上使用适用角色以授予执行这些任务的权限，或者可以创建具有等效所需特权的自身角色。

表 4-1 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： ■ **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

表 4-1 常见任务的所需特权（续）

任务	所需特权	适用角色
从模板部署虚拟机	在目标文件夹或数据中心上： ■ **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
	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
将虚拟机移动到资源池中	在虚拟机或虚拟机的文件夹上： ■ **资源.将虚拟机分配给资源池** ■ **虚拟机.清单.移动**	管理员
	在目标资源池上： **资源.将虚拟机分配给资源池**	管理员
在虚拟机上安装客户机操作系统	在虚拟机或虚拟机的文件夹上： ■ **虚拟机.交互.回答问题** ■ **虚拟机.交互.控制台交互** ■ **虚拟机.交互.设备连接** ■ **虚拟机.交互.关闭电源** ■ **虚拟机.交互.打开电源** ■ **虚拟机.交互.重置** ■ **虚拟机.交互.配置 CD 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： ■ **数据存储.浏览数据存储** ■ **数据存储.低级别文件操作**	虚拟机超级用户或管理员
通过 vMotion 迁移虚拟机	在虚拟机或虚拟机的文件夹上： ■ **资源.迁移已打开电源的虚拟机** ■ **资源.将虚拟机分配给资源池**（如果目标资源池与源资源池不同）	资源池管理员或管理员
	在目标主机、群集或资源池上（如果与源主机、群集或资源池不同）： **资源.将虚拟机分配给资源池**	资源池管理员或管理员
冷迁移（重定位）虚拟机	在虚拟机或虚拟机的文件夹上： ■ **资源.迁移已关闭电源的虚拟机** ■ **资源.将虚拟机分配给资源池**（如果目标资源池与源资源池不同）	资源池管理员或管理员
	在目标主机、群集或资源池上（如果与源主机、群集或资源池不同）： **资源.将虚拟机分配给资源池**	资源池管理员或管理员

表 4-1 常见任务的所需特权（续）

任务	所需特权	适用角色
	在目标数据存储上（如果与源数据存储不同）： **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

密码要求

vCenter Server 和 ESXi 主机的密码要求有所不同。

vCenter Server 密码

在 vCenter Server 中，密码要求由 vCenter Single Sign-On 或配置的标识源规定，这些配置的标识源可以是 Active Directory、OpenLDAP，或 vCenter Single Sign-On 服务器的本地操作系统。请参见第 18 页，“编辑 vCenter Single Sign-On 密码策略”或查阅相关的 Active Directory 或 OpenLDAP 文档。

ESXi 密码

默认情况下，ESXi 强制执行用户密码的相关要求。

用户密码必须满足以下长度要求。

- 包含一类或两类字符的密码的长度必须至少为八个字符。
- 包含三类字符的密码的长度必须至少为七个字符。
- 包含全部四类字符的密码的长度必须至少为六个字符。

在创建密码时，应包含以下四类字符的组合：小写字母、大写字母、数字和特殊字符（如下划线或短划线）。

密码不得包含字根、admin 或任何形式的 administrator。

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。

还可以使用至少包含三个单词且每个单词有 8 到 40 个字符的密码短语。

示例：创建可接受的 ESXi 密码

下列候选密码满足 ESXi 的要求。

- xQaTEhbU:包含由两类字符组成的八个字符。
- xQaT3pb:包含由三类字符组成的七个字符。
- xQaT3#:包含由四类字符组成的六个字符。

下列候选密码不满足 ESXi 的要求。

- Xqat3hb:以大写字符开头，可将有效字符种类数减少到两种。仅使用两种字符类别时，需要 8 个字符。

- xQaTEh2:以数字结尾，可将有效字符种类数减少到两种。仅使用两种字符类别时，需要 8 个字符。

vCenter Server 用户目录设置

您可以限制在搜索用户和组时返回的结果数，以及为 vCenter Server 设置用户目录超时。

使用目录服务的 vCenter Server 系统将根据用户目录域定期验证用户和组。验证将根据 vCenter Server 设置中指定的固定时间间隔执行。例如，如果为用户 Smith 分配了权限并在域中将用户名更改为 Smith2，则在下次验证发生时主机会认为 Smith 已不存在并移除其权限。

再如，如果将用户 Smith 从域中移除，则在下次验证发生时所有权限都将被移除。如果在下次验证发生之前将新用户 Smith 添加到域，新用户 Smith 会接收分配给旧用户 Smith 的所有权限。

vCenter 用户管理任务 5

vCenter 环境中的用户必须进行身份验证，并且必须向其授予查看和更改 vSphere 对象所需的权限。管理员可以从 vSphere Web Client 执行用户管理任务。

本章讨论了以下主题：

管理 vCenter 组件的权限

权限是由用户及针对某对象（如虚拟机或 ESXi 主机）为用户分配的角色组成的访问角色。权限授予用户执行对象（向其分配了角色）上的角色所指定的活动的权限。

例如，要配置主机的内存，必须为用户授予包括**主机.配置.内存配置**特权的角色。通过将不同角色分配给不同对象的用户，您可控制用户可以在 vSphere 环境中执行的任务。

除 root 和 vpx 用户之外的所有其他用户最初在任何对象上均无访问权限，这意味着他们不能查看这些对象或对其执行操作。具有管理员特权的用户必须向这些用户授予权限以允许他们执行任务。

ESXi 和 vCenter Server 的特权列表相同。有关特权的完整列表，请参见第 137 页，第 11 章“定义的特权”。

多个权限

许多任务需要多个对象的权限。

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。虚拟机文件夹和资源池在层次结构中是相同级别。如果您在虚拟机的文件夹及其资源池上授予用户或组传播权限，则用户拥有从资源池和文件夹传播的特权。

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。

权限示例

这些规则可以帮助您确定必须在哪里分配权限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。

在 vSphere Web Client 中分配权限

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，可以在多个对象上同时分配相同的权限。

从 vSphere Web Client 中分配的权限必须完全与 ActiveDirectory 中的权限（包括大小写）匹配。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

对要修改权限的对象的父对象执行**权限.修改权限**。

步骤

1 在 vSphere Web Client 对象导航器中，浏览到对象。

2 单击**管理**选项卡，然后选择**权限**。

3 单击**添加权限**。

4 单击**添加**。

5 确定要获得该权限的用户或组。

   a 在**域**下拉菜单中选择用户或组所在的域。

   b 在“搜索”框中键入名称，或者从列表中选择名称。

   系统会搜索用户名、组名称和相关描述。

   c 选择用户或组，然后单击**添加**。

   名称将添加到**用户**或**组**列表中。

   d （可选）单击**检查名称**验证数据库中是否存在用户或组。

   e 单击**确定**。

6 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。

7 （可选）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。

8 验证用户和组是否都分配到了适当的权限，然后单击**确定**。

   服务器即会将该权限添加至该对象的权限列表中。

   权限列表引用将角色分配给该对象的所有用户和组，同时指明 vCenter Server 层次结构中分配该角色的位置。

在 vSphere Web Client 中更改权限

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

步骤

1 在 vSphere Web Client 对象导航器中，浏览到对象。

2 单击**管理**选项卡，然后选择**权限**。

3 单击行项目以选择用户或组和角色对。

4 单击**针对权限更改角色**。

5 在**分配的角色**下拉菜单中为用户或组选择角色。

6 要将特权传播至分配的清单对象的子对象，请单击**传播**复选框，然后单击**确定**。

在 vSphere Web Client 中移除权限

移除用户或组的权限并不会将用户或组从可用列表中移除，也不会从列表中移除可用项的角色。这样只会从所选的清单对象中移除用户（或组）和角色对。

步骤

1 在 vSphere Web Client 对象导航器中，浏览到对象。

2 单击**管理**选项卡，然后选择**权限**。

3 单击适当的行项目以选择用户或组和角色对。

4 单击**移除权限**。

vCenter Server 会移除权限设置。

在 vSphere Web Client 中更改权限验证设置

vCenter Server 定期根据用户目录中的用户和组验证其用户和组列表。根据验证结果，它会移除该域中不再存在的用户或组。可以禁用验证或更改两次验证之间的时间间隔。

步骤

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

2 选择**管理**选项卡，然后单击**设置**。

3 依次单击**常规**和**编辑**。

4 选择**用户目录**。

5 （可选）取消选中**验证**复选框以禁用验证。

默认情况下已启用验证。即使已禁用了验证，在 vCenter Server 系统启动时，系统也会验证用户和组。

6 （可选）如果已启用验证，则输入验证周期可指定两次验证之间的时间间隔（以分钟为单位）。

7 单击**确定**。

vCenter Server 和 ESXi 中的角色

vCenter Server 仅向已分配有与对象相关的权限的用户授予访问对象的权限。向用户分配与对象相关的权限时，将用户与角色进行配对。角色是一组预定义的特权。

vCenter Server 提供三种默认角色。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默认角色的特权。

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

vCenter Server 自定义角色（推荐）	可使用 vSphere Web Client 中的角色编辑功能创建自定义角色，以创建符合用户需求的特权组。
ESXi 自定义角色	可以使用 CLI 或 vSphere Client 为各个主机创建自定义角色。自定义主机角色无法从 vCenter Server 进行访问。

如果通过 vCenter Server 管理 ESXi 主机，则在主机和 vCenter Server 中维护自定义角色可能会导致混淆和误用。在大多数情况下，建议定义 vCenter Server 角色。

注意 如果添加自定义角色，并不向其分配任何特权，则角色将创建为只读角色，且具有以下三个系统定义的特权：**System.Anonymous**、**System.View** 和 **System.Read**。

在 vSphere Web Client 中创建角色

VMware 建议创建角色以满足环境的访问控制需求。

如果在属于链接模式中连接组的 vCenter Server 系统上创建或编辑角色，则所进行的更改将传播至组中所有其他的 vCenter Server 系统。对特定用户和对象的角色分配不会在已链接的 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 在 vSphere Web Client 中，浏览到**管理 > 角色管理器**。

2 在下拉菜单中选择 vCenter Server 系统。

3 单击**创建角色操作**。

4 键入新角色的名称。

5 选择角色的特权，然后单击**确定**。

在 vSphere Web Client 中编辑角色

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。

如果在属于链接模式中连接组的 vCenter Server 系统上创建或编辑角色，则所进行的更改将传播至组中所有其他的 vCenter Server 系统。对特定用户和对象的角色分配不会在已链接的 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 在 vSphere Web Client 中，浏览到**管理 > 角色管理器**。

2 在下拉菜单中选择 vCenter Server 系统。

3 选择某一角色，然后单击**编辑角色操作**。

4 为该角色选择特权，然后单击**确定**。

在 vSphere Web Client 中克隆角色

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。

如果在属于链接模式中连接组的 vCenter Server 系统上创建或编辑角色，则所进行的更改将传播至组中所有其他的 vCenter Server 系统。对特定用户和对象的角色分配不会在已链接的 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 在 vSphere Web Client 中，浏览到**管理 > 角色管理器**。

2 在下拉菜单中选择 vCenter Server 系统。

3 单击**克隆角色操作**。

4 键入克隆角色的名称。

5 选择角色的特权，然后单击**确定**。

在 vSphere Web Client 的大型域中调整搜索列表

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，则可以调整搜索设置。

注意 此步骤仅适用于 vCenter Server 用户列表。不能以同样方法搜索 ESXi 主机用户列表。

步骤

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

2 选择**管理**选项卡，然后单击**设置**。

3 依次单击**常规**和**编辑**。

4 选择**用户目录**。

5 根据需要更改值。

选项	描述
用户目录超时	连接到活动目录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	选中复选框以设置 vCenter Server 显示的用户和组的最大数目。
查询限制大小	在“选择用户或组”对话框中指定 vCenter Server 从所选域中显示的用户和组的最大数目。如果输入 0（零），则所有用户和组均会出现。

6 单击**确定**。

6 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：

强化 vCenter Server 主机操作系统

通过尽可能地确保主机操作系统（Windows 或 Linux）的安全，保护 vCenter Server 所运行的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*。

vCenter Server 特权的最佳做法

严格控制 vCenter Server 管理员特权，以增强系统的安全性。

- 对 vCenter Server 的完全管理权限应从本地 Windows 管理员帐户移除，并授予特殊用途的本地 vCenter Server 管理员帐户。仅可将完全 vSphere 管理权限授予需要该权限的管理员。请勿将该特权授予其成员未受到严格控制的任何组。
- 避免允许用户直接登录到 vCenter Server 系统。仅允许要执行合法任务的用户登录到系统，并确保对这些事件进行审核。

- 使用服务帐户而不是 Windows 帐户安装 vCenter Server。您可以使用服务帐户或 Windows 帐户运行 vCenter Server。使用服务帐户时可以为 SQL Server 启用 Windows 身份验证，这可增强安全性。服务帐户必须是本地计算机上的管理员。
- 重新启动 vCenter Server 时检查特权重新分配。如果在服务器的根文件夹上分配了管理员角色的用户或用户组无法被验证为有效的用户或组，则管理员特权会被移除并分配给本地 Windows 管理员组。
- 为 vCenter Server 数据库用户授予最小的特权。数据库用户仅需要特定于数据库访问的某些特权。此外，某些特权仅在进行安装和升级时需要。在安装或升级产品后，可以移除这些特权。

限制管理员特权的使用

默认情况下，vCenter Server 授予本地系统（可由域管理员访问）管理员完全管理员特权。为了将滥用该特权的风险降至最低，请将管理权限从本地操作系统的管理员帐户中移除，并将这些权限分配给特殊用途的本地 vSphere 管理员帐户。使用本地 vSphere 帐户创建各个用户帐户。

只将管理员特权授予必须拥有该特权的管理员。不要将该特权授予成员资格未严格控制的任何组。

步骤

1 创建将用于管理 vCenter Server 的用户帐户（例如 vi-admin）。

确保该用户不属于任何本地组（例如管理员组）。

2 以本地操作系统管理员身份登录 vCenter Server 系统，并将全局 vCenter Server 管理员的角色授予您所创建的用户帐户（例如 vi-admin）。

3 注销 vCenter Server，然后使用您所创建的用户帐户 (vi-admin) 登录。

4 验证该用户是否可执行 vCenter Server 管理员的所有任务。

5 移除分配给本地操作系统管理员用户或组的管理员特权。

限制管理员角色的使用

保护 vCenter Server 管理员角色，只将其分配给某些用户。

依赖与特定人员关联的用户帐户，防止 vCenter Server 管理员用户的经常使用。

前提条件

- 创建一个用户帐户来管理 vCenter Server，并将完全 vCenter Server 管理员特权分配给该用户。请参见第 55 页，“管理 vCenter 组件的权限”。
- 移除本地操作系统管理员的 vCenter Server 管理员特权。

步骤

1 以您所创建的 vCenter Server 管理员（例如 vi-admin）身份登录 vCenter Server 系统。

2 将完全管理员特权授予所需最少数目的人员。

3 以 vCenter Server 管理员身份注销。

下一步

保护 vCenter Server 管理员帐户密码。例如，创建由两部分组成的密码，每部分只有一个人知道，或将密码打印输出锁在保险箱内。

在 vSphere Web Client 中启用证书检查和验证主机指纹

为防止中间人攻击并充分利用证书提供的安全性，会在默认情况下启用证书检查。可以在 vSphere Web Client 中验证是否已启用证书检查。

注意 vCenter Server 证书在各次升级中均被保留。

步骤

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

2 选择**管理**选项卡，然后依次单击**设置**和**常规**。

3 单击**编辑**。

4 单击 **SSL 设置**，并验证是否已选中 **vCenter 需要已验证的主机 SSL 证书**。

5 如果有需要手动验证的主机，则可以比较主机列出的指纹和主机控制台中的指纹。

要获取主机指纹，请使用直接控制台用户界面 (DCUI)。

a 登录到直接控制台并按 F2 以访问“系统自定义”菜单。

b 选择**查看支持信息**。

在右侧列中将显示主机指纹。

6 如果指纹匹配，则选中主机旁边的**验证**复选框。

单击**确定**之后，未选中的主机将断开连接。

7 单击**确定**。

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 服务器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。

对网络文件复制启用 SSL 证书验证

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。您可为 NFC 操作禁用和重新启用 SSL 证书验证。

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。

步骤

1 使用 vSphere Web Client 连接到 vCenter Server。

2 选择**设置**选项卡，然后单击**高级设置**。

3 单击**编辑**。

4 在对话框的底部，输入以下“键”和“值”。

字段	值
键	nfc.useSSL
值	有效

5 单击**确定**。

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（仅限链接模式）
- 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。

限制 Linux 客户端的使用

默认情况下，客户端组件与 vCenter Server 系统或 ESXi 主机之间的通信由基于 SSL 的加密进行保护。这些组件的 Linux 版本不执行证书验证，因此应限制这些客户端的使用。

即使您已将 vCenter Server 系统和 ESXi 主机上的自签名证书替换为由本地根证书颁发机构签署的合法证书或第三方 CA 证书，但与 Linux 客户端的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 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。

验证 vSphere Web Client 的完整性

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。

为免受潜在危害，请勿安装来自受信任源以外的其他任何 vSphere Web Client 插件。

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 服务器的特权。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。

从 vCenter Server Virtual Appliance 移除 tcdump 软件包

默认情况下，vCenter Server 虚拟设备包含 tcdump 软件包。如果安全注意事项有明确要求，可移除此软件包。

通过 tcpdump 软件包，管理员可分析 TCP 数据包以进行故障排除和测试。但是在某些情况下，安全注意事项要求移除此软件包。例如，必须移除此软件包以确保符合 DIS STIG 中的 GEN003865，请以 root 身份运行以下命令，以便从系统中移除 tcpdump 软件包：

步骤

1 以 root 身份登录 vCenter Server Virtual Appliance。

2 运行下列命令。

```
rpm –e tcpdump
```

确保 ESXi 主机安全 7

限制对 ESXi 主机上服务和端口的访问对于保护 vSphere 环境免遭未经授权的入侵至关重要。

如果主机受到侵害，则该主机上的虚拟机也将面临着受到侵害的威胁。限制对服务和端口的访问；通过防火墙保护 ESXi 主机。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。

本章讨论了以下主题：

常规 ESXi 安全建议

为了避免主机遭到未经授权的入侵和误用，VMware 对几个参数、设置和活动施加了一些限制。可以根据配置需求而放宽这些限制。但这样做之前，要确保在受信任的环境中工作且已经采取了足够的其他安全措施，以便保护整个网络和连接到主机的设备。

评估主机安全和管理时请考虑以下建议。

- 限制用户访问。

  为了提高安全性，可限制用户访问直接控制台用户界面 (DCUI) 和 ESXi Shell，并实施访问安全策略（例如，通过设置密码限制）。

  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。

- 使用 vSphere Client 管理独立 ESXi 主机。

  尽可能使用 vSphere Client 或第三方网络管理工具来管理 ESXi 主机，而不是以根用户身份通过命令行界面工作。通过 vSphere Client，可以限制具有 ESXi Shell 访问权限的帐户，安全地委派职责，并设置角色以防止管理员和用户使用不必要的功能。

- 使用 vSphere Web Client 来管理受 vCenter Server 管理的 ESXi 主机。请勿通过 vSphere Client 直接访问受管主机，且不要从主机的 DUCI 对受管主机执行更改。

- 仅使用 VMware 源来升级 ESXi 组件。

  主机运行各种第三方软件包来支持管理界面或必须执行的任务。VMware 不支持从 VMware 源以外的任何其他源升级这些软件包。如果使用来自另一个源的下载文件或修补程序，就可能危及管理界面的安全或功能。定期查看第三方供应商站点和 VMware 知识库，以获知安全警示。

除了实施防火墙外，还使用其他方法降低主机的风险。

- ESXi 仅运行管理其功能所不可或缺的服务，而且分发仅限于运行 ESXi 所需的功能。
- 默认情况下，并非专用于对主机进行管理访问的所有端口均处于关闭状态。如果需要其他服务，则必须专门打开相应的端口。
- 默认情况下，弱密码被禁用，来自客户端的所有通信都通过 SSL 进行保护。用于保护通道安全的确切算法取决于 SSL 握手。在 ESXi 上创建的默认证书会使用带有 RSA 加密的 PKCS#1 SHA-256 作为签名算法。
- ESXi 在内部曾使用 Tomcat Web 服务来支持 Web 客户端进行的访问。Tomcat Web 服务经过修改后，仅运行 Web 客户端进行管理和监控所需的功能。因此，ESXi 不易遇到在更广泛的应用中所发现的 Tomcat 安全问题。
- VMware 监控可能影响 ESXi 安全的所有安全警示，并发布安全修补程序（如果需要）。
- 未安装诸如 FTP 和 Telnet 之类的不安全服务，且这些服务的端口在默认情况下是关闭的。由于 SSH 和 SFTP 之类较为安全的服务易于获取，因此，请始终避免使用这些不安全的服务来支持更为安全的替代方案。例如，使用带有 SSL 的 Telnet 而不是 Telnet 来访问虚拟串行端口。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，则必须显式打开相应端口才能支持这些服务。

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

禁用 Managed Object Browser (MOB)

Managed Object Browser 提供了一个浏览 VMkernel 对象模型的途径。但是，攻击者可使用该界面执行恶意配置更改或操作。通过 Managed Object Browser，您可更改主机配置。该界面主要用于调试 vSphere Web Services SDK。

步骤

1 使用 ESXi Shell 直接连接到主机。

2 （可选）通过运行以下命令，确定是否启用了 Managed Object Browser (MOB)。

```
vim-cmd proxysvc/service_list
```

如果服务正在运行，服务列表中会显示以下文本：

```
...
serverNamespace = '/mob',
accessMode = "httpsWithRedirect",
pipeName = "/var/run/vmware/proxy-mob",
...
```

3 通过运行以下命令禁用服务。

```
vim-cmd proxysvc/remove_service "/mob" "httpsWithRedirect"
```

更改立即生效，而且在重新引导后保留。

Managed Object Browser 不可再用于诊断。某些第三方工具使用该界面收集信息。

下一步

禁用 Managed Object Browser 后，请执行测试来验证第三方应用程序是否仍正常运行。

要重新启用该服务，请运行以下命令。

```
vim-cmd proxysvc/add_np_service "/mob" httpsWithRedirect /var/run/vmware/proxy-mob
```

禁用授权 (SSH) 密钥

通过授权密钥，您可在无需用户身份验证的情况下，通过 SSH 启用对 ESXi 主机的访问。为了提高主机安全性，请不要允许用户使用授权密钥访问主机。

如果某个用户的公用密钥在主机上的 `/etc/ssh/keys-root/authorized_keys` 文件中，则将其视为可信用户。允许可信远程用户在不提供密码的情况下访问主机。

步骤

- 对于日常操作，请禁用 ESXi 主机上的 SSH。
- 即使临时启用了 SSH，也要监控 `/etc/ssh/keys-root/authorized_keys` 文件的内容，确保不允许任何用户在未进行适当身份验证的情况下访问主机。
- 监控 `/etc/ssh/keys-root/authorized_keys` 文件，验证其是否为空且未将任何 SSH 密钥添加到该文件中。
- 如果发现 `/etc/ssh/keys-root/authorized_keys` 文件不为空，请移除所有密钥。

禁用授权密钥远程访问可能会限制您在不提供有效登录名的情况下在主机上远程运行命令的能力。例如，这可能会阻止您运行无需人工干预的远程脚本。

配置 SSL 超时

您可以通过在 ESXi 主机上编辑配置文件来为 ESXi 配置 SSL 超时。

可以为两种类型的空闲连接设置超时期间：

- 读取超时设置应用于已完成与 ESXi 的端口 443 的 SSL 握手进程的连接。
- 握手超时设置应用于尚未完成与 ESXi 的端口 443 的 SSL 握手进程的连接。

这两种连接超时设置均以毫秒为单位。

空闲连接在超过超时时间之后将断开。默认情况下，完全建立的 SSL 连接没有超时限制。

步骤

1 以具有管理员特权的用户身份登录到 ESXi Shell。

2 将目录更改为 `/etc/vmware/rhttpproxy/`。

3 使用文本编辑器打开 `config.xml` 文件。

4 输入 `<readTimeoutMs>` 值，以毫秒为单位。

例如，要将读取超时设置为 20 秒，请添加以下行。

```
<readTimeoutMs>20000</readTimeoutMs>
```

5 输入 <handshakeTimeoutMs> 值，以毫秒为单位。

例如，要将握手超时设置为 20 秒，请添加以下行。

```
<handshakeTimeoutMs>20000</handshakeTimeoutMs>
```

6 保存更改并关闭文件。

7 重新启动 rhttpproxy 进程：

```
/etc/init.d/rhttpproxy restart
```

示例：配置文件

文件 /etc/vmware/rhttpproxy/config.xml 的以下部分显示了 SSL 超时设置的添加位置。

```
<vmacore>
 ...
<http>
    ...
<readTimeoutMs>20000</readTimeoutMs>
    ...
</http>
 ...
<ssl>
  ...
<handshakeTimeoutMs>20000</handshakeTimeoutMs>
  ...
    </ssl>
</vmacore>
```

检查主机和 VIB 的接受程度

为保护 ESXi 主机的完整性，请不要允许用户安装未签名的（团体支持的）VIB。未签名的 VIB 包含未由 VMware 或其合作伙伴认证、接受或支持的代码。团体支持的 VIB 没有数字签名。

可以使用 ESXCLI 命令来设置主机的接受程度。该主机的接受程度限制必须与要添加到该主机的任何 VIB 的接受程度相同或更少。为了保护 ESXi 主机的安全性和完整性，请勿允许在生产系统的主机上安装未签名 (CommunitySupported) VIB。

支持以下接受程度。

VMwareCertified VMwareCertified 接受程度具有最严格的要求。此程度的 VIB 能够完全通过全面测试，该测试等效于相同技术的 VMware 内部质量保证测试。现在，只有 IOVP 驱动程序是以此程度发布的。VMware 受理此接受程度的 VIB 的支持致电。

VMwareAccepted 此接受程度的 VIB 通过验证测试，但是这些测试并未对软件的每个功能都进行全面测试。合作伙伴运行测试，VMware 验证结果。现在，以此程度发布的 VIB 包括 CIM 提供程序和 PSA 插件。VMware 将此接受程度的 VIB 支持致电转交给合作伙伴的支持组织。

PartnerSupported 接受程度为 PartnerSupported 的 VIB 是由 VMware 信任的合作伙伴发布的。合作伙伴执行所有测试。VMware 不验证结果。合作伙伴想要在 VMware 系统中启用的新的或非主流的技术将使用此程度。现在，驱动程序 VIB 技术（例如 Infiniband、ATAoE 和 SSD）处于此程度，且具有非标准的硬件驱动程序。VMware 将此接受程度的 VIB 支持致电转交给合作伙伴的支持组织。

CommunitySupported 团体支持接受程度用于由 VMware 合作伙伴程序外部的个人或公司创建的 VIB。此程度的 VIB 尚未通过任何 VMware 批准的测试程序，且不受 VMware 技术支持或 VMware 合作伙伴的支持。

步骤

1 连接至每个 ESXi 主机并通过运行以下命令确认已将接受程度设置为 VMwareCertified 或 VMwareAccepted。

```
esxcli software acceptance get
```

2 如果该主机的接受程度不是 VMwareCertified 或 VMwareAccepted，请通过运行以下命令确认是否有任何 VIB 的接受程度未设置为 VMwareCertified 或 VMwareAccepted。

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

3 通过运行以下命令删除接受程度设置为 PartnerSupported 或 CommunitySupported 的任何 VIB。

```
esxcli software vib remove ––vibname vib
```

4 通过运行以下命令更改主机的接受程度。

```
esxcli software acceptance set ––level acceptance_level
```

将 ESXi 主机添加到 Active Directory 域

由于 ESXi 不支持 vCenter Single Sign-On，因此也不支持您通过 vCenter Single Sign-On 设置的标识源。可以从 vSphere Web Client 将 ESXi 主机添加到 Active Directory 域。

步骤

1 在 vSphere Web Client 中选择 ESXi 主机。

2 在“设置”选项卡中，选择**系统**区域内的**身份验证服务**。

3 单击**加入域**，提供域设置，然后单击**确定**。

ESXi 防火墙配置

ESXi 在管理接口和网络之间设有防火墙。该防火墙在默认情况下启用。

安装时，ESXi 防火墙配置为阻止除第 117 页，“TCP 和 UDP 端口”中列出的默认服务的流量之外的输入和输出流量。

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。

在 ESXi 防火墙目录 `/etc/vmware/firewall/` 中的规则集配置文件中，对运行主机所需要的受支持的服务和管理代理进行了说明。该文件包含防火墙规则，并列出了每个规则与端口和协议之间的关系。

您不能向 ESXi 防火墙添加规则，除非创建并安装了包含规则集配置文件的 VIB。VIB 编写工具对 VMware 合作伙伴可用。

注意 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 74 页，“NFS 客户端规则集行为”。

规则集配置文件

规则集配置文件包含防火墙规则，并描述了每个规则与端口和协议之间的关系。规则集配置文件可以包含多个服务的规则集。

规则集配置文件位于 /etc/vmware/firewall/ 目录中。若要向主机安全配置文件添加服务，VMware 合作伙伴可以在配置文件中为服务创建一个包含端口规则的 VIB。VIB 编写工具对 VMware 合作伙伴可用。

通过 vibauthor 工具中的 VMware Fling，所有用户均可创建 VIB。要以客户支持的接受程度将 VIB 添加到 ESXi 主机，必须首先降低该主机的接受程度。降低主机接受程度后，可能会影响您的支持合同。请参见《安装和设置》文档。

ESXi 5.x ruleset.xml 格式与 ESX 和 ESXi 版本 4.x 中的格式相同，但是多了以下两个标记：enabled 和 required。ESXi 5.x 防火墙继续支持 4.x ruleset.xml 格式。

规则集配置文件中服务的每个规则集均包含以下信息。

- 服务的数字标识符（如果配置文件包含多个服务）。
- 规则集的唯一标识符，通常为服务的名称。
- 对于每个规则，文件都包含一个或多个端口规则，且每个端口规则均定义了方向、协议、端口类型以及端口号或端口号范围。
- 当应用规则集时，指示服务是处于启用还是禁用状态的标记。
- 指示规则集是否必需且无法禁用的信息。

示例：规则集配置文件

```
<ConfigRoot>
<service id='0000'>
<id>serviceName</id>
<rule id = '0000'>
<direction>inbound</direction>
<protocol>tcp</protocol>
<porttype>dst</porttype>
<port>80</port>
</rule>
<rule id='0001'>
<direction>inbound</direction>
<protocol>tcp</protocol>
<porttype>src</porttype>
<port>
<begin>1020</begin>
<end>1050</end>
</port>
</rule>
<enabled>true</enabled>
    <required>false</required>
</service>
</ConfigRoot>
```

使用 vSphere Web Client 允许或拒绝对 ESXi 服务或管理代理的访问

可以配置防火墙属性以允许或拒绝服务或管理代理进行访问。

将有关允许的服务和管理代理的信息添加到主机配置文件。可以在 vSphere Web Client 或命令行中启用或禁用这些服务和代理。

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重叠的服务。要最小化此行为的影响，可以指定允许访问主机上每项服务的 IP 地址。

步骤

1 在 vSphere Web Client 清单中，浏览到主机。

2 依次单击**管理**选项卡和**设置**。

3 单击**安全配置文件**。

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

4 在“防火墙”部分中，单击**编辑**。

5 选择要启用的规则集，或取消选择要禁用的规则集。

“入站端口”和“出站端口”列表示 vSphere Web Client 为该服务打开的端口。“协议”列表示该服务使用的协议。“守护进程”列表示与该服务关联的守护进程的状态。

6 单击**确定**。

在 vSphere Web Client 中添加允许的 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，会允许所有 IP 地址。

步骤

1 在 vSphere Web Client 清单中，浏览到主机。

2 依次单击**管理**选项卡和**设置**。

3 在“系统”下，单击**安全配置文件**。

4 在“防火墙”部分中，单击**编辑**，然后从列表中选择服务。

5 在“允许的 IP 地址”部分中，取消选择**允许从任何 IP 地址连接**，然后输入允许连接到主机的网络的 IP 地址。

使用逗号分隔 IP 地址。可以使用以下地址格式：

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

6 单击**确定**。

NFS 客户端规则集行为

NFS 客户端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。

添加或挂载 NFS 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 NFS 客户端规则集，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 NFS 客户端规则集，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。

移除或卸载 NFS 数据存储时，ESXi 会执行以下操作之一。

- 如果 ESXi 挂载在任意 NFS 数据存储上，则将从允许的出站 IP 地址列表中移除已卸载的 NFS 服务器的 IP 地址，且 NFS 客户端规则集将保持启用状态。
- 如果 ESXi 未挂载在任何 NFS 数据存储上，则将从允许的出站 IP 地址列表中移除卸载的 NFS 服务器的 IP 地址，并禁用 NFS 客户端规则集。

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

根据防火墙设置自动执行服务行为

ESXi 可对服务是否随防火墙端口状态启动的行为进行自动化。

自动化功能有助于确保当环境配置为启用服务功能时启动服务。例如，仅当某些端口打开时启动某网络服务可帮助避免这样的情况，即服务已启动，但无法完成实现预定目的所需的通信。

另外，某些协议（如 Kerberos）要求获取有关当前时间的准确信息。NTP 服务是获取准确时间信息的一种方式，但此服务只能在所需防火墙端口打开的情况下运作。如果所有端口均处于关闭状态，此服务将无法实现其目标。NTP 服务提供一个选项，可配置启动或停止此服务的条件。此配置包括一些选项，指定是否打开防火墙端口，然后是否根据这些条件启动或停止 NTP 服务。有多个可能的配置选项，所有选项均同时适用于 SSH 服务器。

注意 本节中所述的设置仅适用于通过 vSphere Web Client 或使用 vSphere Web Services SDK 创建的应用程序配置的服务设置。通过其他方式（如 ESXi Shell 或 `/etc/init.d/` 中的配置文件）进行的配置不会受这些设置影响。

- **如果任何端口打开则自动启动，如果所有端口关闭则停止**：VMware 针对这些服务建议的默认设置。如果任何端口打开，则客户端会尝试联系与相关服务有关的网络资源。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，但几乎不会对此类情况造成障碍。当适用的出站端口打开时，此服务将开始完成其任务。
- **与主机一起启动和停止**：服务在主机启动后立即启动，并在主机关机之前不久关闭。此选项与**如果任何端口打开则自动启动，如果所有端口关闭则停止**非常相似，都意味着此服务定期尝试完成其任务（例如尝试连接指定的 NTP 服务器）。如果端口先是处于关闭状态，但随后又打开了，客户端将在此后不久开始完成其任务。
- **手动启动和停止**：无论端口打开与否，主机都会保留用户指定的服务设置。当用户启动 NTP 服务后，只要主机仍然开启，该服务会一直运行。如果服务已启动且主机已关闭，该服务将在关机过程中停止，但是，主机一启动，该服务将再次启动，保留用户确定的状况。

注意 ESXi 防火墙会根据服务启动策略自动决定何时启用和禁用规则集。当服务启动时，也会启用其相应的规则集。当服务停止时，也会禁用相应的规则集。

ESXi 防火墙命令

可以在命令行处配置 ESXi 防火墙。

使用 ESXi Shell 的防火墙配置

vSphere Web Client 图形用户界面提供了执行许多配置任务的首选方式。但是，如有必要，可以使用 ESXi Shell 或 vSphere CLI 命令在命令行处配置 ESXi。请参见 *vSphere 命令行界面入门*

表 7-1 防火墙命令

命令	描述
`esxcli network firewall get`	返回防火墙启用或禁用状态，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。
`esxcli network firewall ruleset allowedip remove`	从指定的 IP 地址或 IP 地址范围移除对规则集的访问。
`esxcli network firewall ruleset rule list`	列出防火墙中的每个规则集的规则。

为 ESXi 分配权限

对于 ESXi，权限定义为访问角色，访问角色由用户及针对某对象（如虚拟机或 ESXi 主机）为用户分配的角色组成。权限授予用户执行对象（向其分配了角色）上的角色所指定的活动的权限。

*vSphere 单台主机管理*文档介绍了如何使用 vSphere Client 执行权限验证并分配和移除权限。此文档讨论了不同类型的权限。

指定在锁定模式下具有 DCUI 访问权限的用户

您可以指定能够登录处于锁定模式的主机的用户。具有 DCUI 访问权限的用户不需要拥有对主机的完整管理特权。您可以在 vSphere Web Client 的“高级设置”中授予 DCUI 访问特权。

在 vSphere 5.1 之前版本的 vSphere 中，根用户可以在处于锁定模式的主机上登录到 DCUI。在 vSphere 5.1 中，主机处于锁定模式时，您可以指定允许哪些本地 ESXi 用户登录到 DCUI。这些特殊用户不需要拥有对主机的完整管理特权。指定除匿名根用户之外的用户使您可以记录哪些用户对处于锁定模式的主机执行了操作。

重要事项 您使用 DCUI 禁用锁定模式后，所有具有 DCUI 访问特权的用户均被授予该主机上的管理员角色。

步骤

1 在 vSphere Web Client 对象导航器中，浏览到主机。

2 单击**管理**选项卡，然后选择**设置**。

3 单击**高级系统设置**，然后选择设置 **DCUI.Access**。

4 单击**编辑**，输入用户名并用逗号分隔开。

默认情况下，已指定根用户。只要指定了至少一个其他用户，即可从具有 DCUI 访问权限的用户列表中移除 root。

5 单击**确定**。

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。

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。虚拟机文件夹和资源池在层次结构中是相同级别。如果您在虚拟机的文件夹及其资源池上授予用户或组传播权限，则用户拥有从资源池和文件夹传播的特权。

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

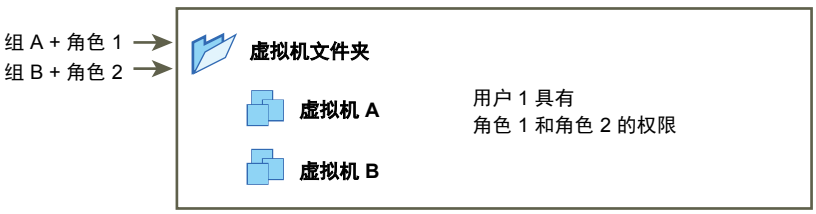
此示例说明了对象如何从组（在父对象上授予了权限）中继承多个权限。

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 可打开虚拟机电源。
- 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 未获得特定权限。

属于组 A 和组 B 的用户 1 登录。用户 1 可以同时打开虚拟机 A 和虚拟机 B 的电源并对其执行快照。

图 7-1 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。

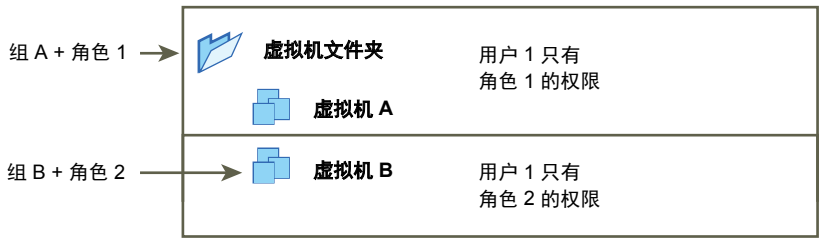
在此示例中，为两个不同对象上的两个不同的组分配了权限。

- 角色 1 可打开虚拟机电源。
- 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 可以打开虚拟机 A 的电源，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打开电源。

图 7-2 示例 2：子权限替代父权限



示例 3：用户权限替代组权限

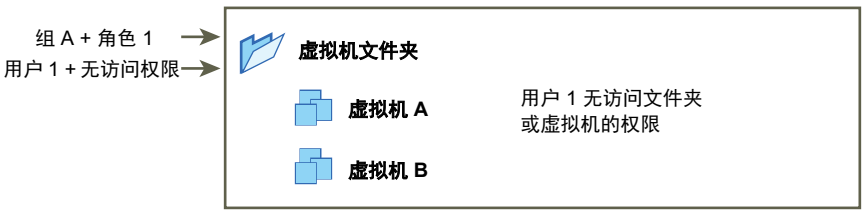
此示例说明了直接分配给单个用户的权限如何替代配给该用户所属组的权限。

在此示例中，权限分配给同一对象上的用户和组。

- 角色 1 可打开虚拟机电源。
- 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组权限。用户 1 无权访问虚拟机文件夹或虚拟机 A 和 B。

图 7-3 示例 3：用户权限替代组权限



root 用户权限

创建非 root 用户帐户以进行本地管理。

默认情况下，每个 ESXi 主机都有一个 root 用户帐户，该帐户具有完整的管理员特权，可用于本地管理，并可用于将主机连接到 vCenter Server。共享公共 root 帐户可以更方便地访问 ESXi 主机。

至少创建一个已命名用户帐户，并为其分配完整的管理员特权，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 用户本身。）

重要事项 如果您要移除 root 用户的访问权限，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。

注意 在 vSphere 5.1 及更高版本中，仅允许使用 root 用户向 vCenter Server 中添加主机，而不允许使用其他具有管理员特权的用户。

向另一个用户分配管理员角色有助于通过可跟踪性维护安全。vSphere Client 将管理员角色用户启动的所有操作记录为事件，并为您提供审核记录。如果所有管理员均以 root 用户身份登录主机，则不能分辨某项操作是哪个管理员执行的。如果在 root 级别创建了多个权限，而且每个权限均与不同的用户相关联，则可对每个管理员的操作进行跟踪。

vpxuser 权限

当 vCenter Server 管理主机活动时，它使用 vpxuser 权限。vpxuser 在将主机连接到 vCenter Server 时创建。

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 用户权限

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。

在 vSphere Web Client 中配置主机以使用 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，如果存在组 ESX Admins，则将向所有用户和组帐户分配对主机的完全管理权限。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。

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 GUID-B77341E3-9D7D-48B6-A221-B782C21AF98E#GUID-B77341E3-9D7D-48B6-A221-B782C21AF98E 或 VMware 知识库。

2 确保为主机配置的 DNS 服务器可以解析 Active Directory 控制器的主机名。

  a 在 vSphere Web Client 对象导航器中，浏览到主机。

  b 依次单击**管理**选项卡和**网络**。

  c 单击“DNS”，然后验证该主机的主机名和 DNS 服务器信息是否正确。

下一步

使用 vSphere Web Client 加入目录服务域。

在 vSphere Web Client 中向目录服务域添加主机

要使用目录服务，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 94 页，“在 vSphere Web Client 中使用 vSphere Authentication Proxy 将主机添加到域”。

步骤

1 在 vSphere Web Client 清单中，浏览到主机。

2 依次单击**管理**选项卡和**设置**。

3 在“系统”下，选择**身份验证服务**。

4 单击**加入域**。

5 输入域。

使用 **name.tld** 或 **name.tld/container/path** 形式。

6 输入有权将主机加入域的目录服务用户的用户名和密码，然后单击**确定**。

7 单击**确定**关闭“目录服务配置”对话框。

在 vSphere Web Client 中查看目录服务设置

可以查看主机用来对用户和目录服务器设置进行身份验证的目录服务器的类型（如果有）。

步骤

1 在 vSphere Web Client 清单中，浏览到主机。

2 依次单击**管理**选项卡和**设置**。

3 在“系统”下，选择**身份验证服务**。

“身份验证服务”页面将显示目录服务和域设置。

替换 ESXi SSL 证书和密钥

您公司的安全策略可能要求您在每台主机上将默认的 ESXi SSL 证书替换为受信任的证书。如果默认证书和密钥被意外删除，您也可以重新生成自签名证书和密钥。

SSL 证书用于证明通信中所涉及的组件的标识，并保护 vSphere 组件之间通信的安全。

默认情况下，vSphere 组件使用在安装过程中创建的自签名证书和密钥。只要用户在出现警告对话框时对证书及其指纹进行验证，那么，自签名证书就与外部证书颁发机构颁发的证书一样安全。

如果公司策略有相关要求，则可以将自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。同时，还请考虑替换证书以避免用户因随手单击而忽略浏览器警告。该警告可能会指示发生中间人攻击，只有检查证书和指纹才能防止此类攻击。

您可以通过多种方式来将默认证书替换为受信任的证书。

- 第 81 页，“从 ESXi Shell 替换默认 ESXi 证书和密钥”
- 第 82 页，“使用 vifs 命令替换默认的 ESXi 证书和密钥”
- 第 82 页，“使用 HTTPS PUT 替换默认的 ESXi 证书和密钥”

如果意外删除了默认自签名证书和密钥或更改了主机名，您可以从 ESXi Shell 中生成一个新的自签名证书和密钥。请参见第 81 页，“为 ESXi 生成新的自签名证书”。

准备您的环境进行 ESXi 证书替换

如果计划使用来自证书颁发机构的证书和密钥替换默认证书和密钥，请确保您的环境中安装了所需软件。

如果使用自签名证书，则您的环境无需满足这些要求。

- 包含 Web 服务器模板的 Microsoft CA（2000 或更高版本）
- 安装在将生成证书签名请求的系统上的 Microsoft Visual C++ 2008 Redistributable Package (x86)
- 安装在将生成证书签名请求的系统上的 OpenSSL 0.98r 或更高版本
- Putty 或其他 SSH 客户端（建议）
- WinSCP 或其他 SFTP/SCP 客户端
- vCenter Server
- ESXi 5.1 或更高版本

为 ESXi 生成新的自签名证书

通常，只有当更改主机名称或意外删除证书时，才要生成新证书。在某些情况下，必须强制主机生成新的证书。

注意 要领略证书检查功能的全部好处，尤其是要在外部使用加密远程连接时，请勿使用自签名证书。而是安装由有效的内部证书颁发机构签名的新证书，或者从受信任的安全颁发机构购买证书。

步骤

1 以具有管理员特权的用户身份登录到 ESXi Shell。

2 在 `/etc/vmware/ssl` 目录中，备份现有证书，方法是使用以下命令对其进行重命名。

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

注意 如果由于删除了证书而需要重新生成这些证书，则不必执行此步骤。

3 运行命令 `/sbin/generate-certificates` 生成新的证书。

4 重新启动主机。

生成证书时，会将这些证书放在正确的位置。您也可以选择将主机置于维护模式，安装新证书，然后使用直接控制台用户界面 (DCUI) 重新启动管理代理。

5 通过执行以下命令并将新证书文件的时间戳与 `orig.rui.crt` 和 `orig.rui.key` 进行比较，来确认主机是否已成功生成新证书。

```
ls -la
```

下一步

考虑将自签名证书和密钥替换为受信任的证书和密钥。

从 ESXi Shell 替换默认 ESXi 证书和密钥

ESXi 使用安装过程中自动生成的证书。这些证书是唯一的，使用这些证书后便可以开始使用服务器，但它们是不可验证的，而且不是由权威证书颁发机构 (CA) 签名的。本主题说明了如何使用自签名证书或 CA 签名证书来替换默认证书。

使用默认证书可能不符合您的组织的安全策略。如果需要可信证书颁发机构颁发的证书，则可以替换默认证书。

注意 如果主机启用了“验证证书”功能，则替换默认证书可能会导致 vCenter Server 停止管理主机。如果 vCenter Server 无法验证新证书，请断开主机连接，然后重新连接。

ESXi 仅支持使用 X.509 证书来加密通过服务器和客户端组件之间的 SSL 连接发送的会话信息。

前提条件

- 如果要使用 CA 签名的证书，请生成证书请求、将其发送至证书颁发机构，并将接收的证书存储在主机可访问的位置。
- 如果需要，从 vSphere Web Client 启用 ESXi Shell 或启用 SSH 流量。请参见第 85 页，“使用 vSphere Web Client 启用对 ESXi Shell 的访问”。
- 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 **Host.Config.AdvancedConfig** 特权。有关 ESXi 特权的更多信息，请参见《vSphere 单台主机管理》出版物。

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。

使用 vifs 命令替换默认的 ESXi 证书和密钥

ESXi 使用安装过程中自动生成的证书。这些证书是唯一的，使用这些证书后便可以开始使用服务器，但它们是不可验证的，而且不是由权威证书颁发机构 (CA) 签名的。

使用默认证书可能不符合您的组织的安全策略。如果需要可信证书颁发机构颁发的证书，则可以替换默认证书。

注意 如果主机启用了“验证证书”功能，则替换默认证书可能会导致 vCenter Server 停止管理主机。如果 vCenter Server 无法验证新证书，请断开主机连接，然后重新连接。

ESXi 仅支持使用 X.509 证书来加密通过服务器和客户端组件之间的 SSL 连接发送的会话信息。

前提条件

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 **Host.Config.AdvancedConfig** 特权。有关 ESXi 特权的更多信息，请参见《vSphere 单台主机管理》出版物。

步骤

1 备份现有证书。

2 按照证书颁发机构的说明生成证书请求。

3 在命令行中，使用 `vifs` 命令将证书上载到主机上合适的位置。

```
vifs --server hostname --username username --put rui.crt /etc/vmware/ssl
```

```
vifs --server hostname --username username --put rui.key /etc/vmware/ssl
```

4 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，然后使用直接控制台用户界面 (DCUI) 重新启动管理代理。

使用 HTTPS PUT 替换默认的 ESXi 证书和密钥

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。

步骤

1 在上载应用程序中，打开文件。

2 将文件发布到以下位置之一。

选项	描述
证书	https://hostname/host/ssl_crt
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 在直接控制台用户界面 (DCUI) 上，使用“重新启动管理代理”操作启动设置。

将 SSH 密钥上载到 ESXi 主机

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

可以使用 vifs vSphere CLI 命令将 SSH 密钥复制到主机。有关安装和使用 vSphere CLI 命令集的信息，请参见《vSphere 命令行界面入门指南》。也可以使用 HTTPS PUT 将 SSK 密钥复制到主机。

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

启用 SSH 并将 SSH 密钥添加到主机具有内在的风险，建议不在强化环境中使用。请参见第 69 页，“禁用授权 (SSH) 密钥”。

注意 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。

使用 vifs 命令上载 SSH 密钥

可以使用授权密钥通过 SSH 登录主机。可以使用 vifs 命令上载授权密钥。

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

可以将以下类型的 SSH 密钥上载到主机：

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

重要事项 请不要修改 /etc/ssh/sshd_config 文件。

步骤

◆ 在命令行中，使用 vifs 命令将 SSH 密钥上载到合适的位置。

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

密钥类型	位置
root 用户的授权密钥文件	/host/ssh_root_authorized keys 您必须具有完全管理员特权才可上载此文件。
DSA 密钥	/host/ssh_host_dsa_key
DSA 公用密钥	/host/ssh_host_dsa_key_pub

密钥类型	位置
RSA 密钥	`/host/ssh_host_rsa_key`
RSA 公用密钥	`/host/ssh_host_rsa_key_pub`

使用 HTTPS PUT 上载 SSH 密钥

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

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

可以使用 HTTPS PUT 将以下类型的 SSH 密钥上载到主机：

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

重要事项 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之一。

密钥类型	位置
root 用户的授权密钥文件	`https://`*主机名或 IP 地址*`/host/ssh_root_authorized keys` 您必须对主机具有完全管理员特权才可上载此文件。
DSA 密钥	`https://`*主机名或 IP 地址*`/host/ssh_host_dsa_key`
DSA 公用密钥	`https://`*主机名或 IP*`/host/ssh_host_dsa_key_pub`
RSA 密钥	`https://`*主机名或 IP*`/host/ssh_host_rsa_key`
RSA 公用密钥	`https://`*主机名或 IP*`/host/ssh_host_rsa_key_pub`

使用 ESXi Shell

默认情况下，ESXi 上的 ESXi Shell（以前称为技术支持模式或 TSM）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。无论主机是否以锁定模式运行，都可以启用和禁用 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。

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 vSphere 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。属于活动目录组 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 只有在需要时才启用 ESXi Shell。

- 使用 vSphere Web Client 启用对 ESXi Shell 的访问第 85 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 86 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 88 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。

- SSH 安全第 88 页，

  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。

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 83 页，“将 SSH 密钥上载到 ESXi 主机”。

步骤

1 在 vSphere Web Client 清单中，浏览到主机。

2 依次单击**管理**选项卡和**设置**。

3 在“系统”下，选择**安全配置文件**。

4 在“服务”面板中，单击**编辑**。

5 从列表中选择一种服务。

- ESXi Shell
- SSH
- 直接控制台 UI

6 单击**服务详细信息**，然后选择**手动启动和停止**启动策略。

如果选择**手动启动和停止**，则重新引导主机时不会启动服务。如果要在重新引导主机时启动服务，请选择**与主机一起启动和停止**。

7 选择**启动**以启用该服务。

8 单击**确定**。

下一步

设置 ESXi Shell 的可用性和闲置超时。请参见 第 86 页，“在 vSphere Web Client 中为 ESXi Shell 可用性创建超时” 和 第 86 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 依次单击**管理**选项卡和**设置**。

3 在“系统”下，选择**高级系统设置**。

4 选择 UserVars.ESXiShellTimeOut，然后单击**编辑**图标。

5 输入闲置超时设置。

您必须重新启动 SSH 服务和 ESXi Shell 服务，超时才能生效。

6 单击**确定**。

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

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

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

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

步骤

1 在 vSphere Web Client 清单中，浏览到主机。

2 依次单击**管理**选项卡和**设置**。

3 在“系统”下，选择**高级系统设置**。

4 选择 UserVars.ESXiShellInteractiveTimeOut，单击**编辑**图标，然后输入超时设置。

5 重新启动 ESXi Shell 服务和 SSH 服务，以使此超时生效。

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 87 页，“在直接控制台用户界面中为 ESXi Shell 可用性创建超时”和第 87 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到 ESXi Shell 时应用，而不会影响现有会话。

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

步骤

1 从“故障排除模式选项”菜单中，选择**修改 ESXi Shell 和 SSH 超时**，然后按 Enter。

2 输入闲置超时值（以秒为单位）。

您必须重新启动 SSH 服务和 ESXi Shell 服务，超时才能生效。

3 按 Enter 并按 Esc 直到返回到直接控制台用户界面的主菜单。

如果该会话闲置，则用户将在超时期限过后注销。

登录 ESXi Shell 以进行故障排除

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

步骤

1 使用以下方法之一登录 ESXi Shell。

- 如果可以直接访问主机，请在计算机的物理控制台上按 Alt+F1 打开登录页面。
- 如果要远程连接到主机，请使用 SSH 或其他远程控制台连接在主机上启动会话。

2 输入能够由主机识别的用户名和密码。

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。

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，所有操作都必须通过 vCenter Server 执行。只有 vpxuser 用户具有身份验证权限，其他任何用户都无法直接对主机执行操作。

当主机处于锁定模式时，您无法从管理服务器、脚本或 vMA 针对主机运行 vSphere CLI 命令。外部软件或管理工具可能无法从 ESXi 主机检索或修改信息。

注意 可以通过“DCUI 访问权限高级配置”选项向用户显式分配 DCUI 访问特权。该选项使用 DCUI.Access 作为密钥，使用 ESXi 用户以逗号分隔的列表作为值。该列表中的用户可以随时访问 DCUI，即使这些用户不是管理员（管理员角色），即使在主机处于锁定模式时，也是如此。

启用或禁用锁定模式会影响有权访问主机服务的用户类型，但不会影响这些服务的可用性。也就是说，如果启用了 ESXi Shell、SSH 或直接控制台用户界面 (DCUI) 服务，则不管主机是否处于锁定模式，这些服务都将继续运行。

可以通过使用添加主机向导将主机添加到 vCenter Server、使用 vSphere Web Client 管理主机或使用直接控制台用户界面 (DCUI) 启用锁定模式。

注意 如果使用直接控制台用户界面 (DCUI) 启用或禁用锁定模式，则主机上的用户和组的权限都将丢失。要保留这些权限，必须使用连接到 vCenter Server 的 vSphere Web Client 启用和禁用锁定模式。

锁定模式只适用于已添加到 vCenter Server 的 ESXi 主机。

锁定模式行为

启用锁定模式会影响有权访问主机服务的用户。

在启用锁定模式时登录的用户

在启用锁定模式之前，已登录 ESXi Shell 的用户仍保持登录并可以运行命令。但这些用户无法禁用锁定模式。其他任何用户（包括主机上的根用户和拥有管理员角色的用户）都不可以使用 ESXi Shell 登录处于锁定模式的主机。

通过 vCenter Server 访问

在 vCenter Server 系统上拥有管理员特权的用户可以使用 vSphere Web Client 禁用由 vCenter Server 系统管理的主机的锁定模式。

从 DCUI 访问

被授予 DCUI 访问特权的用户始终可以使用直接控制台用户界面 (DCUI) 直接登录到主机来禁用锁定模式，即使该用户不具有该主机上的管理员角色。您必须使用“高级设置”才能授予 DCUI 访问特权。

注意 您使用 DCUI 禁用锁定模式后，所有具有 DCUI 访问特权的用户均被授予该主机上的管理员角色。

如果主机上的 root 用户或具有管理员角色的用户尚未被授予 DCUI 访问特权，则他们不能通过 DCUI 直接登录到该主机。如果主机不受 vCenter Server 管理或者如果主机无法访问，则只有具有 DCUI 访问权限的用户才能登录到 DCUI 并禁用锁定模式。如果 DCUI 服务已停止，您必须重新安装 ESXi。

面向不同用户的锁定模式服务

下表显示了主机以锁定模式和正常模式运行时不同类型的用户可以使用的服务。一般说来，只能通过 vCenter Server 进行更改。root 用户可以从直接控制台界面进行更改，但不能从 ESXi Shell 或通过 SSH 会话进行更改。

表 7-2 锁定模式行为

服务	正常模式	锁定模式
vSphere WebServices API	所有用户，取决于 ESXi 权限	仅限 vCenter (vpxuser)
CIM 提供程序	主机上的根用户和具有管理员角色的用户	仅限 vCenter（票证）
直接控制台 UI (DCUI)	主机上的根用户和具有管理员角色的用户	根用户
ESXi Shell	主机上的根用户和具有管理员角色的用户	无用户
SSH	主机上的根用户和具有管理员角色的用户	无用户

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。也可以通过直接控制台用户界面 (DCUI) 启用或禁用锁定模式。

步骤

1 在 vSphere Web Client 清单中，浏览到主机。

2 依次单击**管理**选项卡和**设置**。

3 在“系统”下，选择**安全配置文件**。

4 在“锁定模式”面板中，单击**编辑**。

5 选择 **启用锁定模式**。

6 单击**确定**。

从直接控制台用户界面启用锁定模式

可以从直接控制台用户界面 (DCUI) 启用锁定模式。

注意 如果使用直接控制台用户界面启用或禁用锁定模式，则主机上用户的权限将会丢失。要保留这些权限，必须使用连接到 vCenter Server 的 vSphere Web Client 启用和禁用锁定模式。

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。

3 按 Esc 直到返回到直接控制台用户界面的主菜单。

指定在锁定模式下具有 DCUI 访问权限的用户

您可以指定能够登录处于锁定模式的主机的用户。具有 DCUI 访问权限的用户不需要拥有对主机的完整管理特权。您可以在 vSphere Web Client 的“高级设置”中授予 DCUI 访问特权。

在 vSphere 5.1 之前版本的 vSphere 中，根用户可以在处于锁定模式的主机上登录到 DCUI。在 vSphere 5.1 中，主机处于锁定模式时，您可以指定允许哪些本地 ESXi 用户登录到 DCUI。这些特殊用户不需要拥有对主机的完整管理特权。指定除匿名根用户之外的用户使您可以记录哪些用户对处于锁定模式的主机执行了操作。

重要事项 您使用 DCUI 禁用锁定模式后，所有具有 DCUI 访问特权的用户均被授予该主机上的管理员角色。

步骤

1 在 vSphere Web Client 对象导航器中，浏览到主机。

2 单击**管理**选项卡，然后选择**设置**。

3 单击**高级系统设置**，然后选择设置 **DCUI.Access**。

4 单击**编辑**，输入用户名并用逗号分隔开。

默认情况下，已指定根用户。只要指定了至少一个其他用户，即可从具有 DCUI 访问权限的用户列表中移除 root。

5 单击**确定**。

使用 vSphere Authentication Proxy

使用 vSphere Authentication Proxy 时，无需将活动目录凭据传输到主机。用户将主机添加到域时，会提供活动目录服务器的域名和身份验证代理服务器的 IP 地址。

安装 vSphere Authentication Proxy 服务

要使用 vSphere Authentication Proxy 服务进行身份验证，您必须在主机上安装该服务。

可以在与关联的 vCenter Server 相同的计算机上安装 vSphere Authentication Proxy，也可以在与 vCenter Server 具有网络连接的其他计算机上安装 vSphere Authentication Proxy。vCenter Server 5.0 之前的版本不支持 vSphere Authentication Proxy。

vSphere Authentication Proxy 服务绑定到 IPv4 地址以与 vCenter Server 进行通信，且不支持 IPv6。vCenter Server 可位于纯 IPv4、IPv4/IPv6 混合模式或纯 IPv6 的主机上，但是通过 vSphere Client 连接到 vCenter Server 的计算机必须具有 IPv4 地址，以便 vSphere Authentication Proxy 服务能够正常运行。

前提条件

- 确认您在安装 vSphere Authentication Proxy 服务的主机上具有管理员权限。
- 确认主机具有 Windows Installer 3.0 或更高版本。
- 确认主机具有支持的处理器和操作系统。vSphere Authentication Proxy 支持的处理器和操作系统与 vCenter Server 所支持的相同。
- 确认主机具有有效的 IPv4 地址。可以在纯 IPv4 或 IPv4/IPv6 混合模式的主机上安装 vSphere Authentication Proxy，但不能在纯 IPv6 的主机上安装 vSphere Authentication Proxy。
- 如果将 vSphere Authentication Proxy 安装到 Windows Server 2008 R2 主机上，可以从 support.microsoft.com 网站下载 Windows 知识库文章 981506 中所述的 Windows 热修补程序并进行安装。如果未安装此热修补程序，Authentication Proxy 适配器将无法进行初始化。出现该问题的同时还会在 `camadapter.log` 中显示类似于无法将 `CAM 网站与 CTL 进行绑定 (Failed to bind CAM website with CTL)` 和无法初始化 `CAMAdapter (Failed to initialize CAMAdapter)` 的错误消息。

收集以下信息以完成安装：

- 要安装 vSphere Authentication Proxy 的位置（如果不使用默认位置）。
- vSphere Authentication Proxy 将连接到的 vCenter Server 系统的 IP 地址或主机名、HTTP 端口和凭据。
- 用于在网络上标识 vSphere Authentication Proxy 主机的主机名或 IP 地址。

步骤

1 在要安装 vSphere Authentication Proxy 服务的主机上，安装 .NET Framework 3.5。

2 安装 vSphere Auto Deploy。

不必将 Auto Deploy 和 vSphere Authentication Proxy 服务安装在同一主机上。

3 将要安装身份验证代理服务的主机添加到域中。

4 使用域管理员帐户登录此主机。

5 在软件安装程序目录中，双击 `autorun.exe` 文件启动安装程序。

6 选择 **VMware vSphere Authentication Proxy**，然后单击**安装**。

7 按照向导提示完成安装。

在安装过程中，身份验证服务向注册了 Auto Deploy 的 vCenter Server 实例进行注册。

身份验证代理服务已安装在主机上。

注意 安装 vSphere Authentication Proxy 服务时，安装程序会创建一个具有相应特权的域帐户，以便运行身份验证代理服务。帐户名称以前缀 `CAM–` 开始，并具有一个与其关联的随机生成的 32 个字符的密码。密码设置为永不过期。请勿更改帐户设置。

下一步

将主机配置为使用身份验证代理服务来加入域。

配置主机以使用 vSphere Authentication Proxy 进行身份验证

安装 vSphere Authentication Proxy 服务（CAM 服务）后，必须配置主机以使用身份验证代理服务器对用户进行身份验证。

前提条件

按照第 90 页，“安装 vSphere Authentication Proxy 服务”中的说明在主机上安装 vSphere Authentication Proxy 服务（CAM 服务）。

步骤

1 使用主机上的 IIS 管理器设置 DHCP 范围。

通过设置范围，在管理网络中使用 DHCP 的主机可以使用身份验证代理服务。

选项	操作
适用于 IIS 6	a 浏览到**计算机帐户管理网站**。 b 右键单击虚拟目录 **CAM ISAPI**。 c 选择**属性 > 目录安全 > 编辑 IP 地址和域名限制 > 添加计算机组**。
适用于 IIS 7	a 浏览到**计算机帐户管理网站**。 b 在左窗格中单击 **CAM ISAPI** 虚拟目录，然后打开 **IPv4 地址和域限制**。 c 选择**添加允许条目 > IPv4 地址范围**。

2 如果 Auto Deploy 未置备某个主机，请将默认 SSL 证书更改为自签名证书或由商业证书颁发机构 (CA) 签名的证书。

选项	描述
自签名证书	如果使用自签名证书替换默认证书，请将主机添加到 vCenter Server，以便身份验证代理服务器信任该主机。
CA 签名证书	将 CA 签名的证书（DER 编码）添加到安装身份验证代理服务的系统上的本地可信证书存储，然后重新启动 vSphere Authentication Proxy Adapter 服务。 ■ 对于 Windows 2003，将证书文件复制到 `C:\Documents and Settings\All Users\Application Data\VMware\vSphere Authentication Proxy\trust`。 ■ 对于 Windows 2008，将证书文件复制到 `C:\Program Data\VMware\vSphere Authentication Proxy\trust`。

对 ESXi 的 vSphere Authentication Proxy 进行身份验证

使用 vSphere Authentication Proxy 将 ESXi 连接到某个域之前，必须对 ESXi 的 vSphere Authentication Proxy 服务器进行身份验证。如果使用主机配置文件将域与 vSphere Authentication Proxy 服务器连接，则无需对服务器进行身份验证。主机配置文件会对 ESXi 的代理服务器进行身份验证。

要对 ESXi 进行身份验证以使用 vSphere Authentication Proxy，请从 vSphere Authentication Proxy 系统中导出服务器证书，然后将其导入到 ESXi 中。只需对服务器进行一次身份验证。

注意 默认情况下，使用 vSphere Authentication Proxy 服务器加入域时，ESXi 必须对此服务器进行身份验证。确保始终启用此身份验证功能。如果必须禁用身份验证功能，则可使用“高级设置”对话框将 `UserVars.ActiveDirectoryVerifyCAMCertifcate` 属性设置为 0。

导出 vSphere Authentication Proxy 证书

要针对 ESXi 对 vSphere Authentication Proxy 进行身份验证，必须为 ESXi 提供代理服务器证书。

前提条件

按照第 90 页，“安装 vSphere Authentication Proxy 服务”中的说明在主机上安装 vSphere Authentication Proxy 服务。

步骤

1 在身份验证代理服务器系统中，使用 IIS Manager 导出证书。

选项	操作
适用于 IIS 6	a 右键单击**计算机帐户管理网站**。 b 选择**属性 > 目录安全 > 查看证书**。
适用于 IIS 7	a 在左窗格中，单击**计算机帐户管理网站**。 b 选择**绑定**打开“站点绑定”对话框。 c 选择 **https** 绑定。 d 选择**编辑 > 查看 SSL 证书**。

2 选择**详细信息 > 复制到文件**。

3 选择选项**不要导出专用密钥**和 **Base-64 编码 X.509 (CER)**。

下一步

将证书导入到 ESXi。

在 vSphere Web Client 中将 Proxy 服务器证书导入 ESXi

要针对 ESXi 对 vSphere Authentication Proxy 服务器进行身份验证，请将代理服务器证书上载到 ESXi。

使用 vSphere Web Client 用户界面将 vSphere Authentication Proxy 服务器证书上载到 ESXi。

前提条件

按照第 90 页，“安装 vSphere Authentication Proxy 服务”中的说明在主机上安装 vSphere Authentication Proxy 服务。

导出 vSphere Authentication Proxy 服务器证书，如第 93 页，“导出 vSphere Authentication Proxy 证书”中所述。

步骤

1 将身份验证代理服务器证书上载到主机可访问的临时位置。

a 在 vSphere Web Client 中，浏览到主机可访问的数据存储，然后单击**管理**选项卡。

b 单击**文件**，然后单击**上载文件**。

2 浏览到证书，然后选择**打开**。

若要从数据存储上载或下载文件，必须在使用 vSphere Web Client 的系统上安装客户端集成插件。

3 浏览到主机，然后单击**管理**选项卡。

4 选择**配置**选项卡，然后单击**身份验证服务**。

5 单击**导入证书**。

6 输入到主机上身份验证代理服务器证书文件的完整路径和身份验证代理服务器的 IP 地址。

使用“[*数据存储名称*] *文件路径*”形式输入代理服务器的路径。

7 单击**导入**。

下一步

设置主机使用 vSphere Authentication Proxy 服务器对用户进行身份验证。

在 vSphere Web Client 中使用 vSphere Authentication Proxy 将主机添加到域

将主机加入目录服务域时，可以使用 vSphere Authentication Proxy 服务器进行身份验证，而不传输用户提供的 Active Directory 凭据。

可以使用以下两种方法之一输入域名：

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

前提条件

- 通过 vSphere Web Client 连接到 vCenter Server 系统。
- 如果 ESXi 配置了 DHCP 地址，请设置 DHCP 范围。
- 如果 ESXi 使用静态 IP 地址进行了配置，请验证其关联配置文件是否已配置为使用 vSphere Authentication Proxy 服务来加入域，以便身份验证代理服务器可以信任 ESXi IP 地址。
- 如果 ESXi 使用自签名证书，请确认是否已将该主机添加到 vCenter Server。这可使身份验证代理服务器信任 ESXi。
- 如果 ESXi 使用的是 CA 签名证书且未使用 Auto Deploy 置备，请验证 CA 证书是否已添加到身份验证代理服务器的本地可信证书存储，如第 92 页，“配置主机以使用 vSphere Authentication Proxy 进行身份验证”中所述。
- 针对主机对 vSphere Authentication Proxy 服务器进行身份验证。

步骤

1 在 vSphere Web Client 中浏览到主机，然后单击**管理**选项卡。

2 单击**设置**，然后选择**身份验证服务**。

3 单击**加入域**。

4 输入域。

使用 **`name.tld`** 或 **`name.tld/container/path`** 形式。

5 选择**使用代理服务器**。

6 输入身份验证代理服务器的 IP 地址。

7 单击**确定**。

替换 ESXi 主机的 Authentication Proxy 证书

您可以导入 vSphere Web Client 中可信证书颁发机构颁发的证书

前提条件

- 将 Authentication Proxy 证书文件上载到 ESXi 主机。

步骤

1 在 vSphere Web Client 中选择 ESXi 主机。

2 在**设置**选项卡中，选择**系统**区域内的**身份验证服务**。

3 单击**导入证书**。

4 输入 SSL 证书路径和 vSphere Authentication Proxy 服务器。

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。

- 不要使用密码或密码短语设置证书。ESXi 不支持密码或密码短语（也称为加密密钥）。如果设置密码或密码短语，则 ESXi 进程将无法正常启动。
- 您可以配置 Web 代理，以便它在非默认位置中搜索证书。对于倾向于将其证书集中在单台计算机上以便使多台主机可使用证书的公司而言，此功能相当有用。

小心 如果证书未存储在主机本地（例如，存储在 NFS 共享上），则在 ESXi 失去网络连接时，该主机将无法访问这些证书。因此，连接到主机的客户端无法成功地参与同主机的安全 SSL 握手。

- 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，请针对 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 vCenter Server 时，证书保持在原位。

将 Web 代理配置为在非默认位置中搜索证书

您可以配置 Web 代理，以便它在非默认位置中搜索证书。对于将其证书集中在单台计算机上以便使多台主机可使用证书的公司而言，此功能相当有用。

步骤

1 以具有管理员特权的用户身份登录到 ESXi Shell。

2 将目录更改为 `/etc/vmware/rhttpproxy/`。

3 使用文本编辑器打开 `config.xml` 文件，并找到以下 XML 分段。

```
<ssl>
<!-- The server private key file -->
<privateKey>/etc/vmware/ssl/rui.key</privateKey>
<!-- The server side certificate file -->
<certificate>/etc/vmware/ssl/rui.crt</certificate>
</ssl>
```

4 使用从受信任证书颁发机构接收的专用密钥文件的绝对路径来替换 `/etc/vmware/ssl/rui.key`。

此路径可以位于主机上，也可以位于用来存储贵公司的证书和密钥的集中式计算机上。

注意 保持 `<privateKey>` 和 `</privateKey>` XML 标记不变。

5 使用从可信证书颁发机构接收的证书文件的绝对路径来替换 `/etc/vmware/ssl/rui.crt`。

小心 不要删除原始 `rui.key` 和 `rui.crt` 文件。主机会使用这些文件。

6 保存更改并关闭文件。

7 重新启动 rhttpproxy 进程：

```
/etc/init.d/rhttpproxy restart
```

更改 Web 代理服务的安全设置

可更改此安全配置，以便可通过 HTTP 连接直接访问各种服务。

要为 vSphere 5.0 及更早版本配置安全设置，请参见第 97 页，“更改 Web 代理服务 5.0 及更早版本的安全设置”。

步骤

1 以具有管理员特权的用户身份登录到 ESXi Shell。

2 将目录更改为 `/etc/vmware/rhttpproxy`。

3 使用文本编辑器打开 `endpoints.conf` 文件。

4 根据需要更改安全设置。

例如，您可能要修改与使用 HTTPS 的服务相对应的条目，以添加 HTTP 访问选项。

选项	描述
connection-type	可接受的值包括： ■ 本地 ■ 远程 ■ namedpipe ■ localtunnel ■ remotetunnel ■ namedpipetunnel
endpoint-address	■ 对于 *local* 和 *localtunnel*，请提供端口号。 ■ 对于 *remote* 和 *remotetunnel*，请提供 *HostName/IP_address:Port*。 ■ 对于 *namedpipe* 和 *namedpipetunnel*，请提供命名的管道在文件系统中的位置。
HTTP 访问模式	服务允许的通信形式。可接受的值包括： ■ allow - 允许 HTTP 访问。 ■ redirect – 如果 Endpoint 地址是本地端口，则客户端将重定向至 443。如果 Endpoint 地址是远程主机，则客户端将重定向至该主机。 ■ reject - 无 HTTP 访问。
HTTPS 访问模式	可接受的值包括： ■ allow - 允许 HTTPS 访问。 ■ reject - 不允许 HTTPS 访问。

5 保存更改并关闭文件。

以下示例显示了完整的 endpoints.conf 文件。

```
# Endpoint Connection-type Endpoint-address HTTP-access-Mode HTTPS-access-mode
/ local 8309 redirect allow
/sdk local 8307 redirect allow
/client/clients.xml local 8309 allow allow
/ui local 8308 redirect allow
/vpxa local 8089 reject allow
/mob namedpipe /var/run/vmware/proxy-mob redirect allow
/wsman local 8889 redirect allow
/sdkTunnel namedpipetunnel /var/run/vmware/proxy-sdk-tunnel allow reject
/ha-nfc local 12001 allow allow
/nfc local 12000 allow allow
```

下一步

对 `endpoints.conf` 文件进行更改后，使用命令 `kill -HUP <pid_of_rhttpproxy>` 可使反向代理重新加载新的 Endpoint

更改 Web 代理服务 5.0 及更早版本的安全设置

可更改此安全配置，以便可通过 HTTP 连接直接访问各种服务。

这些步骤适用于版本 5.0 及更早版本。从版本 5.1 开始，需要修改的文件将完全不同。有关修改新文件的说明，请参见第 96 页，“更改 Web 代理服务的安全设置”。

步骤

1 以具有管理员特权的用户身份登录到 ESXi Shell。

2 将目录更改为 `/etc/vmware/hostd/directory`。

3 使用文本编辑器打开 `proxy.xml` 文件。

文件内容通常如下所示：

```
<ConfigRoot>
<EndpointList>
<_length>10</_length>
<_type>vim.ProxyService.EndpointSpec[]</_type>
<e id="0">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8309</port>
<serverNamespace>/</serverNamespace>
</e>
<e id="1">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>8309</port>
<serverNamespace>/client/clients.xml</serverNamespace>
</e>
<e id="2">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>12001</port>
<serverNamespace>/ha-nfc</serverNamespace>
</e>
<e id="3">
```

```
<_type>vim.ProxyService.NamedPipeServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<pipeName>/var/run/vmware/proxy-mob</pipeName>
<serverNamespace>/mob</serverNamespace>
</e>
<e id="4">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>12000</port>
<serverNamespace>/nfc</serverNamespace>
</e>
<e id="5">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8307</port>
<serverNamespace>/sdk</serverNamespace>
</e>
<e id="6">
<_type>vim.ProxyService.NamedPipeTunnelSpec</_type>
<accessMode>httpOnly</accessMode>
<pipeName>/var/run/vmware/proxy-sdk-tunnel</pipeName>
<serverNamespace>/sdkTunnel</serverNamespace>
</e>
<e id="7">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8308</port>
<serverNamespace>/ui</serverNamespace>
</e>
<e id="8">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsOnly</accessMode>
<port>8089</port>
<serverNamespace>/vpxa</serverNamespace>
</e>
<e id="9">
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpsWithRedirect</accessMode>
<port>8889</port>
<serverNamespace>/wsman</serverNamespace>
</e>
</EndpointList>
</ConfigRoot>
```

4 根据需要更改安全设置。

例如，您可能要修改与使用 HTTPS 的服务相对应的条目，以添加 HTTP 访问选项。

选项	描述
e id	服务器 ID XML 标记的 ID 编号。ID 编号在 HTTP 区域中必须是唯一的。
_type	正在移动的服务的名称。

选项	描述
accessmode	服务允许的通信形式。可接受的值包括： ■ httpOnly - 只能通过纯文本 HTTP 连接来访问服务。 ■ httpsOnly - 只能通过 HTTPS 连接来访问服务。 ■ httpsWithRedirect - 只能通过 HTTPS 连接来访问服务。通过 HTTP 发出的请求将被重定向到相应的 HTTPS URL。 ■ httpAndHttps - 可通过 HTTP 和 HTTPS 两种连接来访问服务。
端口	分配给该服务的端口号。可以为服务分配其他端口号。
serverNamespace	提供此服务的服务器的命名空间，例如 `/sdk` 或 `/mob`。

5 保存更改并关闭文件。

6 重新启动 `hostd` 进程：

```
/etc/init.d/hostd restart
```

vSphere Auto Deploy 安全注意事项

要最有效地保护您的环境，请注意 Auto Deploy 与主机配置文件结合使用时可能存在的安全风险。

网络安全

保护您的网络，就像其他任何基于 PXE 的部署方法一样。vSphere Auto Deploy 通过 SSL 传输数据，以防止意外干扰和侦听。但是，在 PXE 引导期间不会检查客户端或 Auto Deploy 服务器的真实性。

通过完全隔离在其中使用 Auto Deploy 的网络，可以大幅降低 Auto Deploy 的安全风险。

引导映像和主机配置文件安全

vSphere Auto Deploy 服务器下载到计算机中的引导映像可以具有以下组件。

- 映像配置文件所包含的 VIB 软件包始终包含在引导映像中。
- 如果 Auto Deploy 规则设置为使用主机配置文件或主机自定义设置置备主机，则主机配置文件和主机自定义便包含在引导映像中。
  - 主机配置文件和主机自定义附带的管理员（根帐户）密码和用户密码进行了 MD5 加密。
  - 与配置文件关联的其他任何密码均采用明文形式。如果使用主机配置文件设置 Active Directory，则密码不受保护。

    使用 vSphere Authentication Service 设置 Active Directory 以避免公开 Active Directory 密码。如果使用主机配置文件设置 Active Directory，则密码不受保护。
- 主机的公用和专用 SSL 密钥和证书都包含在引导映像中。

管理 ESXi 日志文件

日志文件是对攻击进行故障排除和获取有关违反主机安全信息的一个重要组件。将日志记录在安全、集中式日志服务器上能有助于防止日志篡改。远程日志记录也能提供长期的审核记录。

采取下列措施来提高主机的安全性。

- 配置持久日志记录到数据存储。默认情况下，ESXi 主机上的日志存储在内存文件系统中。因此，当您重新引导主机时，日志将会丢失，并且仅存储 24 小时的日志数据。当启用持久日志记录时，您将会有专用的服务器活动记录用于主机。
- 中央主机上的远程日志记录可让您将日志文件收集到中央主机上，其中您使用单一工具便能监控所有主机。您也可以执行汇总分析和搜索日志数据，这可能会泄漏某些信息，例如对多个主机的协同攻击。

- 使用远程命令行（例如 vCLI 或 PowerCLI）或使用 API 客户端在 ESXi 主机上配置远程安全 syslog。
- 查询 syslog 配置以确保配置了有效的 syslog 服务器，包括正确的端口。

在 ESXi 主机上配置 Syslog

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

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

有关使用 vCLI 命令的详细信息，请参见 *vSphere 命令行界面入门*。

步骤

1 在 vSphere Web Client 清单中，选择主机。

2 单击**管理**选项卡。

3 在“系统”面板中，单击**高级系统设置**。

4 查找“高级系统设置”列表中的 **Syslog** 部分。

5 要全局设置日志记录，请选择要更改的设置，然后单击“编辑”图标。

选项	描述
Syslog.global.defaultRotate	设置要保留的存档的最大数目。可以在全局范围内设置该数目，也可以为单个子记录器设置该数目。
Syslog.global.defaultSize	在系统轮换日志前，设置日志的默认大小 (KB)。可以在全局范围内设置该数目，也可以为单个子记录器设置该数目。
Syslog.global.LogDir	存储日志的目录。该目录可能位于挂载的 NFS 或 VMFS 卷中。只有本地文件系统中的 `/scratch` 目录在重新引导后仍然存在。目录应指定为 [*数据存储名称*] *文件路径*，其中，路径是相对于支持数据存储卷的根目录的路径。例如，路径 `[storage1] /systemlogs` 将映射为路径 `/vmfs/volumes/storage1/systemlogs`。
Syslog.global.logDirUnique	选择此选项将使用 ESXi 主机的名称在 **Syslog.global.LogDir** 指定的目录下创建子目录。如果多个 ESXi 主机使用同一个 NFS 目录，则唯一的目录非常有用。
Syslog.global.LogHost	向其转发 syslog 消息的远程主机，以及远程主机在其上接收 syslog 消息的端口。可以包括协议和端口，例如 `ssl://hostName1:514`。支持 UDP（默认）、TCP 和 SSL。远程主机必须安装并正确配置 syslog 以接收转发的 syslog 消息。有关配置的信息，请参见远程主机上所安装的 syslog 服务的文档。

6 （可选）覆盖任何日志的默认日志大小和日志轮换。

a 单击要自定义的日志的名称。

b 单击“编辑”图标，然后输入所需的轮换和日志大小数量。

7 单击**确定**。

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/vpxa.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，并且可用来进行故障排除。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/vwmare.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

当启用 Fault Tolerance (FT) 时，VMware vLockstep 可捕获主虚拟机上发生的输入和事件，并将这些输入和事件发送到正在另一主机上运行的辅助虚拟机。

主虚拟机和辅助虚拟机之间的此日志记录通信未加密，并且包含客户机网络和存储 I/O 数据以及客户机操作系统的内存内容。此通信可以包含敏感数据，如纯文本格式的密码。要避免泄露这类数据，请确保此网络的安全，特别是避免遭受“中间人”攻击。例如，将专用网络用于 FT 日志记录通信。

8 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。请像保护物理计算机一样确保虚拟机的安全。

本章讨论了以下主题：

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。

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、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。

安装防病毒软件

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。

配置客户机操作系统的日志记录级别

虚拟机可以将故障排除信息写入存储在 VMFS 卷上的虚拟机日志文件中。虚拟机用户和进程可能会有意或无意地误用日志记录，这会导致日志文件中充满大量数据。随着时间的推移，日志文件会占用大量文件系统空间，从而造成拒绝服务。

为避免该问题，可考虑修改虚拟机客户机操作系统的日志记录设置。这些设置可以限制日志文件的总大小和数量。通常，在每次重新引导主机时都会生成一个新的日志文件，因此文件会变的非常大。通过限制日志文件的最大大小，可以确保更频繁的生成新日志文件。VMware 建议保存 10 个日志文件，每个文件的大小限制为 100 KB。这些值的大小足以让您捕获充分的信息，用以调试可能会出现的大多数问题。

每向日志写入一个条目，都会检查一遍日志的大小。如果超过了限制，下一个条目将写入新的日志。如果存在的日志文件数量达到最大，则会删除最早的日志文件。通过写入超大的日志条目可以尝试发动避免这些限制的拒绝服务攻击，但由于每个日志条目的大小限制在 4KB 以下，因此，日志文件的大小不会比配置限制大 4KB 以上。

禁用虚拟机中不必要的功能

虚拟机中运行的任何服务都有可能引发攻击。通过禁用不必要的系统组件（不是支持系统上运行的应用程序或服务所必需的），可减少会受到攻击的组件数量。

通常，虚拟机需要的服务或功能不像物理服务器那样多。对系统进行虚拟化时，请评估特定服务或功能是否必要。

步骤

- 禁用操作系统中未使用的服务。

  例如，如果系统运行文件服务器，则应关闭所有 Web 服务。

- 断开未使用的物理设备（例如 CD/DVD 驱动器、软盘驱动器和 USB 适配器）的连接。

  请参见第 104 页，“移除不必要的硬件设备”。

- 关闭屏幕保护程序。
- 除非必要，否则不要在 Linux、BSD 或 Solaris 客户机操作系统上运行 X Window 系统。

移除不必要的硬件设备

启用或连接的任何设备都可能成为攻击渠道。虚拟机上不具有特权的用户和进程可以连接或断开硬件设备（如网络适配器和 CD-ROM 驱动器）。攻击者可利用该能力破坏虚拟机安全性。移除不必要的硬件设备可帮助防止攻击。

使用以下准则提高虚拟机安全性。

- 确保未连接未授权的设备，并移除所有不需要或不使用的硬件设备。
- 从虚拟机中禁用不必要的虚拟设备。具有虚拟机访问权限的攻击者可以连接已断开的 CD-ROM 驱动器并访问遗留在驱动器中介质上的敏感信息，或者断开网络适配器以将虚拟机与其网络隔离，从而造成拒绝服务。
- 确保不会将任何不需要的设备连接到虚拟机。串行和并行端口很少在数据中心环境中用于虚拟机，而 CD/DVD 驱动器通常仅在软件安装期间临时连接。
- 对于不需要的不太常用的设备，参数不得呈现或其值必须为 false。确保以下参数未呈现或设置为 false，除非需要设备。

参数	值	设备
floppyX.present	无效	软盘驱动器
serialX.present	无效	串行端口
parallelX.present	无效	并行端口
usb.present	无效	USB 控制器
ideX:Y.present	无效	CD-ROM

禁用未公开的功能

VMware 虚拟机在 vSphere 系统与托管虚拟化平台（例如 Workstation 和 Fusion）上都能运行。在 vSphere 系统上运行虚拟机时，无需启用某些 VMX 参数。禁用这些参数可降低出现漏洞的可能性。

前提条件

关闭虚拟机。

步骤

1 在 vSphere Web Client 清单中查找虚拟机。

a 要查找虚拟机，请选择数据中心、文件夹、群集、资源池或主机。

b 单击**相关对象**选项卡，然后单击**虚拟机**。

2 右键单击虚拟机，然后单击**编辑设置**。

3 选择**虚拟机选项**。

4 单击**高级**，然后单击**编辑配置**。

5 添加或编辑以下参数。

名称	值
isolation.tools.unity.push.update.disable	TRUE
isolation.tools.ghi.launchmenu.change	TRUE
isolation.tools.memSchedFakeSampleStats.disable	TRUE
isolation.tools.getCreds.disable	TRUE
isolation.tools.ghi.autologon.disable	TRUE
isolation.bios.bbs.disable	TRUE
isolation.tools.hgfsServerSet.disable	TRUE

6 单击**确定**。

将 `isolation.tools.hgfsServerSet.disable` 设置为 true 可禁用客户机 HGFS 服务器在主机上的注册。使用 HGFS 将文件传入和传出客户机操作系统的 API（例如某些 VIX 命令或 VMware Tools 自动升级实用程序）将无法正常运行。

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 Client 将其启用。

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	值
isolation.tools.copy.disable	有效
isolation.tools.paste.disable	有效

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

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，vCenter Server 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。为了降低损害客户机保密性、可用性或完整性的风险，请创建没有**客户机操作**特权的非客户机访问角色。

为安全起见，请严格限制对虚拟数据中心的访问，严格程度与限制对物理物理数据中心的访问相同。为避免授予用户完全管理员访问权限，请将非客户机访问角色应用于需要管理员特权但无权与客户机操作系统内的文件和程序交互的用户。

例如，某项配置可能包括其上带有敏感信息的基础架构中的虚拟机。通过 vMotion 和 Storage vMotion 进行迁移等任务要求 IT 角色有权访问该虚拟机。在这种情况下，您需要禁用客户机操作系统中的部分远程操作，以确保该 IT 角色无法访问敏感信息。

前提条件

验证您对在其上创建该角色的 vCenter Server 系统是否拥有**管理员**特权。

步骤

1 以对要在其上创建该角色的 vCenter Server 系统拥有**管理员**特权的用户身份登录 vSphere Web Client。

2 单击**管理**，然后选择**访问 > 角色**。

3 单击**创建角色**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

将需要**管理员**特权但无客户机访问特权的用户分配到新建角色，确保将这些用户从默认管理员角色中移除。

在 vSphere Web Client 中阻止虚拟机用户或进程与设备断开连接

虚拟机内不具有 root 或管理员特权的用户和进程能够连接设备（如网络适配器和 CD-ROM 驱动器）或断开设备的连接，还能够修改设备设置。若要提高虚拟机安全性，请移除这些设备。如果不想永久移除设备，可以阻止虚拟机用户或进程在客户机操作系统中连接设备或与设备断开连接。

前提条件

关闭虚拟机。

步骤

1 在 vSphere Web Client 清单中查找虚拟机。

a 要查找虚拟机，请选择数据中心、文件夹、群集、资源池或主机。

b 单击**相关对象**选项卡，然后单击**虚拟机**。

2 右键单击虚拟机，然后单击**编辑设置**。

3 选择**虚拟机选项 > 高级**，然后单击**编辑配置**。

4 验证以下值是否在“名称”和“值”列中，或者单击**添加行**来添加这些值。

名称	值
isolation.device.connectable.disable	有效
isolation.device.edit.disable	有效

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

5 单击**确定**以关闭“配置参数”对话框，然后再次单击**确定**以关闭“虚拟机属性”对话框。

限制客户机操作系统写入主机内存

客户机操作系统进程会通过 VMware Tools 向主机发送信息性消息。如果不限制主机存储这些消息的数据量，则无限的数据流将为攻击者提供发起拒绝服务 (DoS) 攻击的机会。

客户机操作进程发送的信息性消息称之为 `setinfo` 消息，并且通常包含定义虚拟机特性的名称/值对或主机存储的标识符（例如，`ipaddress=10.17.87.224`）。包含这些名称/值对的配置文件大小限制为 1 MB，这样可防止攻击者通过编写模仿 VMware Tools 的软件并使用任意配置数据填写主机内存，从而占用虚拟机所需的空间来发动 DoS 攻击。

如果名称/值对需要超过 1 MB 的存储空间，则可以根据需要更改值。另外，还可以阻止客户机操作系统进程将任何名称/值对写入到配置文件。

在 vSphere Web Client 中修改客户机操作系统的可变内存限制

如果配置文件中存储的自定义信息较多，可以增加客户机操作系统的可变内存限制。

前提条件

关闭虚拟机。

步骤

1 在 vSphere Web Client 清单中查找虚拟机。

a 要查找虚拟机，请选择数据中心、文件夹、群集、资源池或主机。

b 单击**相关对象**选项卡，然后单击**虚拟机**。

2 右键单击虚拟机，然后单击**编辑设置**。

3 选择**虚拟机选项 > 高级**，然后单击**编辑配置**。

4 添加或编辑参数 `tools.setInfo.sizeLimit`，并将值设置为字节数。

5 单击**确定**。

阻止客户机操作系统进程向主机发送配置消息

可以阻止客户机将任何名称/值对写入到配置文件中。该选择适合必须阻止客户机操作系统修改配置设置的情况。

前提条件

关闭虚拟机。

步骤

1 使用 vSphere Client 登录到 vCenter Server 系统。

2 在“清单”面板中选择虚拟机。

3 在**摘要**选项卡中，单击**编辑设置**。

4 选择**选项 > 高级 > 常规**，然后单击**配置参数**。

5 单击**添加行**，并在“名称”和“值”列中键入以下值。

- 在“名称”列中：**`isolation.tools.setinfo.disable`**
- 在“值”列中：**`true`**

6 单击**确定**以关闭“配置参数”对话框，然后再次单击**确定**以关闭“虚拟机属性”对话框。

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

您可以在 vSphere Web Client 中将模板转换为虚拟机，然后再转换回模板，从而轻松更新模板。有关模板的详细信息，请参见 *vSphere 虚拟机管理*文档。

您可以使用 vSphere Update Manager 自动修补模板中的操作系统和某些应用程序。请参见《vSphere Update Manager》文档。

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（例如设置共享和限制）来控制虚拟机消耗的服务器资源。

默认情况下，主机上的所有虚拟机平均共享资源。

步骤

- 使用共享或预留保证资源分配给关键的虚拟机。

  对以下虚拟机的资源消耗进行约束限制：更有可能受到攻击风险的虚拟机，或运行据悉很有可能大量消耗资源的应用程序的虚拟机。

下一步

有关共享和限制的信息，请参见 *vSphere 资源管理*文档。

限制信息性消息从虚拟机流向 VMX 文件

限制信息性消息从虚拟机流向 VMX 文件，从而避免填充数据存储和造成拒绝服务 (DoS)。如果您不控制虚拟机的 VMX 文件的大小，并且 VMX 的信息量超过数据存储的容量，则会造成拒绝服务。

默认情况下，包含信息性名称值对的配置文件将限制为 1 MB。此容量在大多数情况下是足够的，但是在必要时可以更改此值。例如，如果向配置文件中存储的自定义信息较多，可以增加该限制值。

注意 请仔细考量所需要的信息量。如果信息量超过数据存储的容量，则可能会造成拒绝服务。

即使 VMX 文件中未列出 sizeLimit 参数，也会应用 1 MB 的默认限制。

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* 是虚拟机文件驻留的存储设备的名称。例如，`/vmfs/volumes/vol1/vm-finance/`。

2. 使用文本编辑器在 VMX 文件中添加或编辑下列行：

   ```
   tools.setInfo.sizeLimit=104857
   ```

3. 保存并关闭文件。

在 vSphere Web Client 中防止虚拟磁盘压缩

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。

步骤

1. 在 vSphere Web Client 清单中查找虚拟机。
   a. 要查找虚拟机，请选择数据中心、文件夹、群集、资源池或主机。
   b. 单击**相关对象**选项卡，然后单击**虚拟机**。
2. 右键单击虚拟机，然后单击**编辑设置**。
3. 选择**虚拟机选项**。
4. 单击**高级**，然后单击**编辑配置**。

5 添加或编辑以下参数。

名称	值
isolation.tools.diskWiper.disable	TRUE
isolation.tools.diskShrink.disable	TRUE

6 单击**确定**。

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。

尽量少用虚拟机控制台

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

步骤

- 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。

配置客户机操作系统的日志记录级别

虚拟机可以将故障排除信息写入存储在 VMFS 卷上的虚拟机日志文件中。虚拟机用户和进程可能会有意或无意地误用日志记录，这会导致日志文件中充满大量数据。随着时间的推移，日志文件会占用大量文件系统空间，从而造成拒绝服务。

为避免该问题，可考虑修改虚拟机客户机操作系统的日志记录设置。这些设置可以限制日志文件的总大小和数量。通常，在每次重新引导主机时都会生成一个新的日志文件，因此文件会变的非常大。通过限制日志文件的最大大小，可以确保更频繁的生成新日志文件。VMware 建议保存 10 个日志文件，每个文件的大小限制为 100 KB。这些值的大小足以让您捕获充分的信息，用以调试可能会出现的大多数问题。

每向日志写入一个条目，都会检查一遍日志的大小。如果超过了限制，下一个条目将写入新的日志。如果存在的日志文件数量达到最大，则会删除最早的日志文件。通过写入超大的日志条目可以尝试发动避免这些限制的 DoS 攻击，但由于每个日志条目的大小限制在 4 KB 以下，因此，日志文件的大小不会比配置限制大 4 KB 以上。

在 vSphere Web Client 中限制日志文件数量

要防止虚拟机用户和进程创建大量日志文件，从而导致服务拒绝，可以限制虚拟机日志文件的数量。您无法限制个别虚拟机的日志文件大小。

可以通过编辑 `/etc/config/vmware` 文件中的 `vms.log.xxx` 参数来更改主机中所有虚拟机的日志记录设置。

前提条件

关闭虚拟机。

步骤

1 在 vSphere Web Client 清单中查找虚拟机。

  a 要查找虚拟机，请选择数据中心、文件夹、群集、资源池或主机。

  b 单击**相关对象**选项卡，然后单击**虚拟机**。

2 右键单击虚拟机，然后单击**编辑设置**。

3 选择**虚拟机选项**。

4 单击**高级**，然后单击**编辑配置**。

5 根据要保留的文件数目，添加或编辑 log.keepOld 参数。例如，要保留 10 个日志文件（达到 10 个文件后，在创建新文件时将删除最早的文件），请输入 **10**。

6 单击**确定**。

在 vSphere Web Client 中禁用客户机操作系统的日志记录

如果选择不将故障排除信息写入 VMFS 卷上存储的虚拟机日志文件，则可以同时停止日志记录。

如果禁用客户机操作系统的日志记录，请注意您可能无法收集到充足的日志以进行故障排除。而且，如果在禁用日志后出现虚拟机问题，VMware 不提供技术支持。

步骤

1 在 vSphere Web Client 清单中查找虚拟机。

a 要查找虚拟机，请选择数据中心、文件夹、群集、资源池或主机。

b 单击**相关对象**选项卡，然后单击**虚拟机**。

2 右键单击虚拟机，然后单击**编辑设置**。

3 选择**虚拟机选项 > 高级**。

4 在“设置”中，取消选中**启用日志记录**。

5 单击**确定**。

9 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*文档。

本章讨论了以下主题：

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 114 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 121 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路径之外的所有通信路径。管理员在防火墙打开的路径或端口允许防火墙内外设备间的流量。

重要事项 ESXi 5.5 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打算如何使用网络以及如何为给定的组件提供所需的安全。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，可对所用配置进行设置，以便在虚拟网络的入口点设有防火墙来保护整组虚拟机。

针对有 vCenter Server 的配置设立防火墙

如果要通过 vCenter Server 访问 ESXi 主机，则通常会使用防火墙保护 vCenter Server。该防火墙可为网络提供基本保护。

防火墙可能位于客户端和 vCenter Server 之间。或者，根据您的部署情况，vCenter Server 和客户端可能均受防火墙保护。重点是确保在您认为的系统入口点有防火墙。

有关 TCP 和 UDP 端口的完整列表，包括用于 vSphere vMotion™ 和 vSphere Fault Tolerance 的端口，请参见第 117 页，“TCP 和 UDP 端口”。

配置有 vCenter Server 的网络可以通过 vSphere Web Client 或第三方网络管理客户端接收通信，这些客户端使用 SDK 与主机相连接。在正常操作期间，vCenter Server 会在指定的端口上侦听其受管主机和客户端的数据。vCenter Server 还假设其受管主机会在指定的端口上侦听 vCenter Server 的数据。如果任何这些元素之间有防火墙，必须确保防火墙中有打开的端口以支持数据传输。

视您计划如何使用网络及各种设备所需安全级别而定，可能还需要在网络中的许多其他访问点设立防火墙。根据为网络配置确定的安全风险选择防火墙位置。下面列出了 ESXi 实施中常用的防火墙位置。

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

  如果在 ESXi 主机间添加防火墙并打算在服务器间迁移虚拟机、执行克隆操作或使用 vMotion，还必须在用来将源主机和目标主机隔开的防火墙中打开端口，以便源主机与目标主机进行通信。
- ESXi 主机和网络存储器（例如 NFS 或 iSCSI 存储器）之间。这些端口并非专用于 VMware，您可以根据网络规范进行配置。

通过防火墙连接到 vCenter Server

vCenter Server 使用端口 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。

要使 vCenter Server 能够从 vSphere Web Client 接收数据，请在防火墙中打开端口 443，以便允许将数据从 vSphere Web Client 传输到 vCenter Server。有关在防火墙中配置端口的其他信息，请联系防火墙系统管理员。

如果正在使用 vSphere Web Client，并且不希望将端口 443 用作 vSphere Web Client 与 vCenter Server 通信的端口，则可以通过在 vSphere Web Client 中更改 vCenter Server 设置来切换到另一个端口。要了解如何更改这些设置，请参见《vCenter Server and Host Management》文档 *vCenter Server 和主机管理*。

针对没有 vCenter Server 的配置设立防火墙

可以将客户端直接连接到 ESXi 网络，而不使用 vCenter Server。

如果未配置 vCenter Server，网络会通过 vSphere Client、任一 vSphere 命令行界面、vSphere Web Services SDK 或第三方客户端来接收通信。在多数情况下，其防火墙需求会与配置有 vCenter Server 的情况基本相同，但有几个重要区别。

- 与包含 vCenter Server 的配置一样，应确保有防火墙保护 ESXi 层，或保护客户端及 ESXi 层，具体取决于您的配置。该防火墙可为网络提供基本保护。所使用的防火墙端口与配置了 vCenter Server 的情况相同。
- 此类配置中的许可证是您在每个主机上安装的 ESXi 包的一部分。由于许可功能驻留在服务器上，因此不需要单独的许可证服务器。这就免除了在许可证服务器与 ESXi 网络间设立防火墙的需要。

通过防火墙连接 ESXi 主机

如果在两台 ESXi 主机间设有防火墙，并希望允许主机间的事务或使用 vCenter Server 执行任何源或目标活动（例如 vSphere High Availability (vSphere HA) 通信、迁移、克隆或 vMotion），则必须配置一个可供受管主机接收数据的连接。

要配置用于接收数据的连接，请打开用于 vSphere High Availability、vMotion、vSphere Fault Tolerance 等服务的通信的端口。有关配置文件、vSphere Web Client 访问权限以及防火墙命令的讨论，请参见第 71 页，“ESXi 防火墙配置”。有关端口列表，请参见第 117 页，“TCP 和 UDP 端口”。有关配置端口的其他信息，请咨询防火墙系统管理员。

通过防火墙连接到虚拟机控制台

通过 vCenter Server 将客户端连接到 ESXi 主机时，用户和管理员与虚拟机控制台的通信都需要某些端口。这些端口支持不同的客户端功能，与 ESXi 上的不同层相连接，并使用不同的身份验证协议。

连接到虚拟机控制台的方法取决于您是否使用 vSphere Web Client 或者您是否使用 vSphere SDK 等不同的客户端。

使用 vSphere Web Client 进行连接

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

涉及以下端口。

端口 9443 和端口 9090

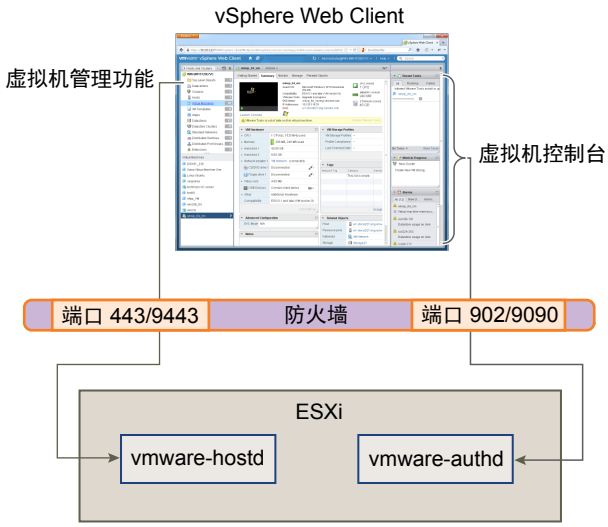
vSphere Web Client 使用端口 9443 实现与 vCenter Server 的 HTTPS 通信，使用端口 9090 实现与 vCenter Server 的 HTTP 通信。如果用户能够访问 vCenter Server，则他们还能访问各个 ESXi 主机和虚拟机。

可以在 vSphere Web Client 安装期间更改这些端口。

端口 443 和端口 902

如果 vCenter Server 系统与 vCenter Server 管理的 ESXi 主机之间存在防火墙，请在防火墙中打开端口 443 和 902 以允许数据从 vCenter Server 传输到 ESXi 主机。

图 9-1 用于 vSphere Web Client 与 vCenter Server 管理的 ESXi 主机的通信的端口



有关配置端口的其他信息，请咨询防火墙系统管理员。

通过 vCenter Server 和 vSphere Client 进行连接

通过 vSphere Client 进行连接时，所需的端口取决于您是直接连接到 ESXi 主机还是连接到 vCenter Server 系统。

端口 443

端口 443 通过 Tomcat Web 服务或 SDK 将 vSphere Web Services SDK 等客户端连接到 ESXi。主机进程将端口 443 数据多路复用到适当的接收方以进行处理。

vSphere SDK 直接连接到 ESXi 时，可以使用此端口来支持与主机及其虚拟机相关的任何管理功能。端口 443 是 vSphere SDK 等客户端向 ESXi 发送数据时使用的端口。VMware 不支持为这些连接配置其他端口。

端口 902

这是 vCenter Server 从 ESXi 接收数据时使用的端口。

端口 902 通过 VMware 授权守护进程 (`vmware-authd`) 将 vCenter Server 连接至主机。此守护进程将端口 902 的数据分多路传输到适当的接收方进行处理。VMware 不支持为该连接配置其他端口。

通过 vSphere Client 直接连接

通过 vSphere Client，您可以直接连接到 ESXi 主机。

端口 902

vSphere Client 使用此端口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。

TCP 和 UDP 端口

可以使用预定的 TCP 和 UDP 端口访问 vCenter Server、ESXi 主机和其他网络组件。若要从防火墙外管理网络组件，可能需重新配置防火墙以允许在适当端口的访问。

下表列出了 TCP 和 UDP 端口，以及每个端口的用途和类型。在安装时默认打开的端口用（默认）进行指示。要了解不同版本 vSphere 的所有 vSphere 组件的最新端口列表，请参见 http://kb.vmware.com/kb/1012382。

表 9-1 TCP 和 UDP 端口

端口	用途	流量类型
22	SSH 服务器 (vSphere Client)	入站 TCP
53（默认）	DNS 客户端	入站和出站 UDP
68（默认）	DHCP 客户端	入站和出站 UDP
80（默认）	HTTP 访问 vCenter Server 需要使用端口 80 进行直接 HTTP 连接。端口 80 将请求重定向到 HTTPS 端口 443。如果意外使用 http://server 而非 https://server，则此重定向将有所帮助 WS 管理（也需要打开端口 443）	入站 TCP 出站 TCP、UDP
88, 2013	Kerberos 的控制接口 RPC，由 vCenter Single Sign-On 使用	
111（默认）	RPC 服务，vCenter Server Appliance 使用该服务进行 NIS 注册	入站和出站 TCP
123	NTP 客户端	出站 UDP
135（默认）	用于将 vCenter Server Appliance 加入到 Active Directory 域中。	入站和出站 TCP
161（默认）	SNMP 服务器	入站 UDP

表 9-1 TCP 和 UDP 端口（续）

端口	用途	流量类型
443（默认）	vCenter Server 系统侦听来自 vSphere Client 的连接时所使用的默认端口。要使 vCenter Server 系统从 vSphere Client 接收数据，请在防火墙中打开端口 443。 vCenter Server 系统还使用端口 443 监控从 SDK 客户端传输的数据。 此端口也用于以下服务： ■ WS 管理（也需要打开端口 80） ■ vSphere Client 对 vSphere Update Manager 的访问 ■ 第三方网络管理客户端与 vCenter Server 的连接 ■ 第三方网络管理客户端对主机的访问	入站 TCP
427（默认）	CIM 客户端使用服务位置协议版本 2 (SLPv2) 查找 CIM 服务器。	入站和出站 UDP
513（默认）	用于记录活动的 vCenter Server Appliance	入站 UDP
902（默认）	vCenter Server 系统用来将数据发送到托管主机的默认端口。托管主机也会通过 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。 不得在 vSphere Client 和主机之间阻塞端口 902。vSphere Client 使用此端口显示虚拟机控制台。	入站和出站 TCP、出站 UDP
903	当 vSphere Client 直接连接到 ESXi 主机（而非 vCenter Server）时，从 vSphere Client 访问虚拟机控制台。 MKS 事务 (xinetd/vmware-authd-mks)	入站 TCP
1234、1235（默认）	vSphere Replication	出站 TCP
2012	vCenter Single Sign-On vmdir 的控制接口 RPC。	
2014	所有 VMCA（VMware 证书颁发机构）API 的 RPC 端口	
2049	来自 NFS 存储设备的事务 此端口用于 VMKernel 接口。	入站和出站 TCP
3260	到 iSCSI 存储设备的事务	出站 TCP
5900-5964	由 VNC 等管理工具使用的 RFB 协议	入站和出站 TCP
5988（默认）	通过 HTTP 的 CIM 事务	入站 TCP
5989（默认）	通过 HTTPS 的 CIM XML 事务	入站和出站 TCP
7444	vCenter Single Sign-On HTTPS	
8000（默认）	来自 vMotion 的请求	入站和出站 TCP
8009	用于使 vCenter Server Appliance 与 Tomcat 进行通信的 AJP 连接器端口	出站 TCP
8100、8200（默认）	主机之间的流量，用于 vSphere Fault Tolerance (FT)	入站和出站 TCP、UDP
8182	主机之间的流量，用于 vSphere High Availability (HA)	入站和出站 TCP、入站和出站 UDP
9009	用于使 vCenter Server Appliance 能够与 vSphere Web Client 进行通信	入站和出站 TCP
9090	用户访问特定主机上的虚拟机时生成的远程控制台流量。 vSphere Web Client 对虚拟机控制台进行 HTTPS 访问	入站 TCP
9443	vSphere Web Client 对 ESXi 主机进行 HTTP 访问	入站 TCP
11711	vCenter Single Sign-On LDAP	

表 9-1 TCP 和 UDP 端口（续）

端口	用途	流量类型
11712	vCenter Single Sign-On LDAP	
12721	VMware Identity Management 服务	

除了 TCP 和 UDP 端口外，还可根据需要配置其他端口。

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*出版物中的“安全策略”部分。

.

确保标准交换机 MAC 地址安全

可以通过限制一些 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。

可以通过限制以下模式来保护通过标准交换机的流量不受此类型第 2 层的攻击：

- 混杂模式
- MAC 地址更改
- 伪信号

要更改某个端口的任何默认设置，请修改 vSphere Web Client 中标准交换机或端口组的安全策略。

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 网络负载平衡时）。在标准多播模式下使用 Microsoft 网络负载平衡时，适配器不能共享 MAC 地址。

伪信号

伪信号选项将影响从虚拟机传输的流量。

当**伪信号**选项设置为**接受**时，ESXi 不会比较源 MAC 地址和有效 MAC 地址。

要防止 MAC 模拟，可将**伪信号**选项设置为**拒绝**。这样，主机将对客户机操作系统传输的源 MAC 地址与其虚拟机适配器的有效 MAC 地址进行比较，以确认是否匹配。如果地址不匹配，ESXi 主机将丢弃数据包。

客户机操作系统检测不到其虚拟机适配器无法使用模拟 MAC 地址发送数据包。ESXi 主机会在带有模拟地址的任何数据包递送之前将其截断，而客户机操作系统可能假设数据包已被丢弃。

混杂模式运行

混杂模式会清除虚拟机适配器执行的任何接收筛选，以便客户机操作系统接收在网络上观察到的所有流量。默认情况下，虚拟机适配器不能在混杂模式中运行。

尽管混杂模式对于跟踪网络活动很有用，但它是一种不安全的运行模式，因为混杂模式中的任何适配器均可访问数据包，即使某些数据包是否仅由特定的网络适配器接收也是如此。这意味着虚拟机中的管理员或根用户可以查看发往其他客户机或主机操作系统的流量。

注意 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 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 确认已禁用配置了静态绑定的分布式端口组的自动扩展功能。

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 API/SDK 文档》。

2 确保已完整记录所有 vSphere Distributed Switch 的全部专用 VLAN ID。

3 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。

4 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 121 页，“混杂模式运行”）
- MAC 地址更改（请参见 第 120 页，“MAC 地址更改”）
- 伪信号（请参见第 120 页，“伪信号”）

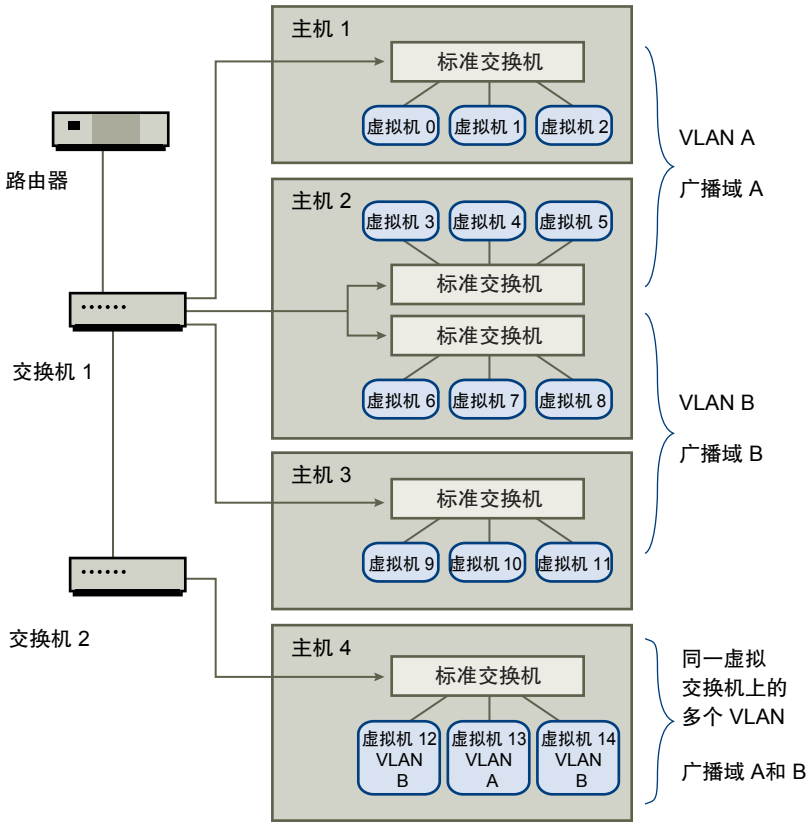
通过 VLAN 确保虚拟机安全

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 9-2 VLAN 布局示例



在此配置中，会计部门的所有员工均使用 VLAN A 中的虚拟机，销售部门的员工使用 VLAN B 中的虚拟机。

路由器将包含会计数据的数据包转发至交换机。这些数据包将被标记为仅分发至 VLAN A。因此，数据将被局限在广播域 A 内，无法传送到广播域 B，除非对路由器进行此配置。

该 VLAN 配置可防止销售人员截取传至会计部门的数据包。还可防止会计部门接收传至销售组的数据包。一个虚拟交换机可为不同 VLAN 中的虚拟机服务。

VLAN 安全注意事项

如何设置 VLAN 以确保网络组件安全取决于客户机操作系统以及网络设备的配置方式。

ESXi 配备完整的符合 IEEE 802.1q 的 VLAN 实施。VMware 不能对如何设置 VLAN 提出具体建议，但当您使用 VLAN 部署作为安全执行策略一部分时，应考虑以下因素。

确保 VLAN 安全

管理员可使用几个选项确保其 vSphere 环境中 VLAN 的安全。

步骤

1 确保端口组未配置为上游物理交换机预留的 VLAN 值

请勿使用为物理交换机预留的值设置 VLAN ID。

2 确保端口组未配置为 VLAN 4095，除非用于虚拟客户机标记 (VGT)。

vSphere 中存在三种 VLAN 标记类型：

- 外部交换机标记 (EST)

- 虚拟交换机标记 (VST) - 虚拟交换机使用已配置的 VLAN ID 标记传入附加虚拟机的流量，并将 VLAN 标记从传出虚拟机的流量中移除。要设置 VST 模式，请分配 1 到 4095 之间的 VLAN ID。
- 虚拟客户机标记 (VGT) - 虚拟机处理 VLAN 流量。要激活 VGT 模式，请将 VLAN ID 设置为 4095。在 Distributed Switch 上，还可以使用 **VLAN 中继**选项允许基于 VLAN 的虚拟机流量。

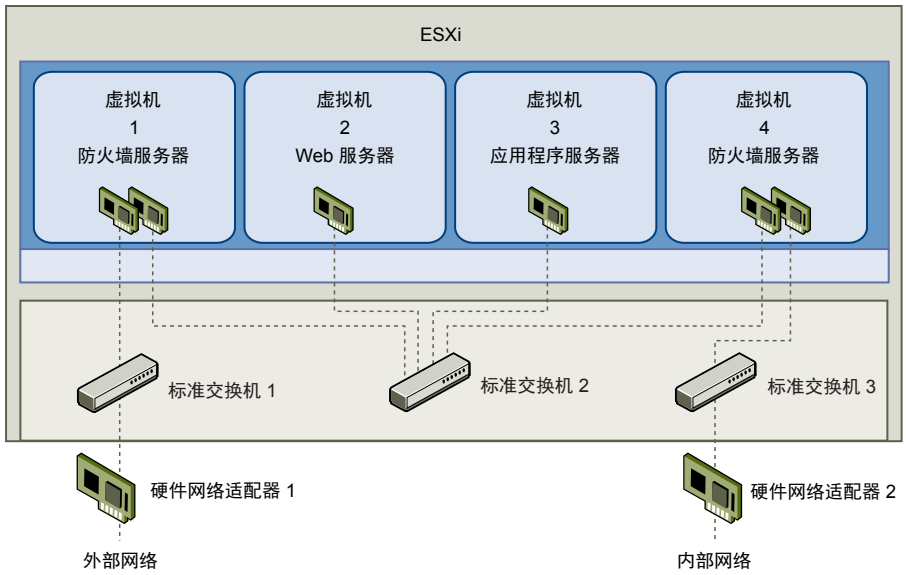
在标准交换机上，可以在交换机或端口组级别上配置 VLAN 网络连接模式，而在 Distributed Switch 上，则在分布式端口组或端口级别。

3 确保完全记录了每台虚拟交换机上的所有 VLAN，而且每台虚拟交换机有且仅有所需的 VLAN。

在单台 ESXi 主机上创建网络 DMZ

在单台主机上创建网络隔离区 (DMZ) 是使用 ESXi 隔离和虚拟网络功能配置安全环境的一个示例。

图 9-3 在单台 ESXi 主机上配置的 DMZ



在此示例中，将四个虚拟机配置为在标准交换机 2 上创建虚拟 DMZ：

- 虚拟机 1 和虚拟机 4 运行防火墙，并通过标准交换机连接到物理网络适配器。这两个虚拟机均使用多个交换机。
- 虚拟机 2 运行 Web 服务器，同时虚拟机 3 作为应用程序服务器运行。这两个虚拟机均连接到一个虚拟交换机。

Web 服务器和应用程序服务器占用两个防火墙之间的 DMZ。这两个元素之间的媒介是用来连接防火墙和服务器的标准交换机 2。此交换机未与 DMZ 之外的任何元素进行直接连接，且通过两个防火墙与外部流量相隔离。

从运行角度来看，外部流量通过硬件网络适配器 1（由标准交换机 1 路由）从 Internet 进入虚拟机 1，并由此虚拟机上安装的防火墙进行验证。如果经防火墙授权，流量可路由至 DMZ 中的标准交换机，即标准交换机 2。由于 Web 服务器和应用程序服务器也连接至此交换机，因此，它们可以满足外部请求。

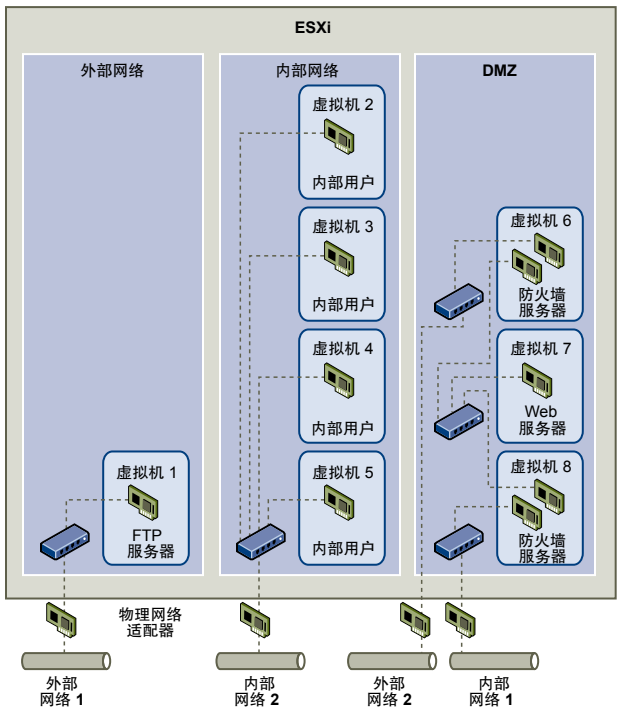
标准交换机 2 还与虚拟机 4 相连。此虚拟机在 DMZ 和内部企业网络之间提供防火墙。此防火墙对来自 Web 服务器和应用程序服务器的数据包进行筛选。验证后的数据包将通过标准交换机 3 路由至硬件网络适配器 2。硬件网络适配器 2 与内部企业网络相连。

在单台主机上创建 DMZ 时，可使用相当轻量的防火墙。尽管此配置中的虚拟机无法直接控制其他虚拟机或访问其内存，但是所有虚拟机仍然通过虚拟网络处于连接状态。此网络可能会传播病毒，或成为其他类型攻击的对象。DMZ 中虚拟机的安全性等同于连接到同一网络的独立物理机。

在单台 ESXi 主机中创建多个网络

ESXi 系统的设计可让您将一些虚拟机组连接至内部网络，并将一些虚拟机组连接至外部网络，而将另一些虚拟机组同时连接至外部和内部网络，而这一切都在同一主机上进行。此功能是由对虚拟机的基本隔离和对虚拟网络连接功能的有计划使用组合而成的。

图 9-4 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
`--sa-source=` ***源地址***	必需。指定源地址。
`--sa-destination=` ***目标地址***	必需。指定目标地址。
`--sa-mode=` ***模式***	必需。指定模式 `transport` 或 `tunnel`。
`--sa-spi=` ***安全参数索引***	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。
`--encryption-algorithm=` ***加密算法***	必需。使用以下参数之一指定加密算法。 ■ `3des-cbc` ■ `aes128-cbc` ■ `null` `null` 不提供任何加密。
`--encryption-key=` ***加密密钥***	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。
`--integrity-algorithm=` ***身份验证算法***	必需。指定身份验证算法 `hmac-sha1` 或 `hmac-sha2-256`。
`--integrity-key=` ***身份验证密钥***	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。
`--sa-name=` ***名称***	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 0x697076367265616479 6c6f676f33646573736362636f757432
--integrity-algorithm hmac-sha1
--integrity-key 0x69707636726561647 96c6f67736861316f757432
--sa-name sa1
```

移除安全关联

可从主机中移除安全关联。

可以使用 `esxcli` vSphere CLI 命令移除安全关联。

前提条件

请确保要使用的安全关联当前未在使用。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***。

列出可用的安全策略

ESXi 可以提供主机上所有安全策略的列表。

可以使用 esxcli vSphere CLI 命令获取可用安全策略的列表。

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 126 页，“添加安全关联”中所述，添加具有相应身份验证和加密参数的安全关联。

步骤

- 在命令提示符下输入命令 **esxcli network ip ipsec sp add** 并使用下列一个或多个选项。

选项	描述
--sp-source= *源地址*	必需。指定源 IP 地址和前缀长度。
--sp-destination= *目标地址*	必需。指定目标地址和前缀长度。
--source-port= *端口*	必需。指定源端口。源端口号必须是介于 0 和 65535 之间的一个数字。
--destination-port= *端口*	必需。指定目标端口。源端口号必须是介于 0 和 65535 之间的一个数字。
--upper-layer-protocol= *协议*	使用以下参数之一指定上层协议。 ■ tcp ■ udp ■ icmp6 ■ 任意
--flow-direction= *方向*	使用 in 或 out 指定要监控流量的方向。
--action= *操作*	使用以下参数之一指定在遇到具有指定参数的流量时要采取的操作。 ■ none：不采取任何操作。 ■ discard：不允许数据进出。 ■ ipsec：使用安全关联中提供的身份验证和加密信息来确定数据是否来自受信任的源。
--sp-mode= *模式*	指定模式 tunnel 或 transport。
--sa-name= *安全关联名称*	必需。为要使用的安全策略提供安全关联名称。
--sp-name= *名称*	必需。请提供一个安全策略名称。

示例：新安全策略命令

为了方便阅读，下面的示例包含额外的换行符。

```
esxcli network ip ipsec add
--sp-source=2001:db8:1::/64
--sp-destination=2002:db8:1::/64
--source-port=23
--destination-port=25
--upper-layer-protocol=tcp
--flow-direction=out
--action=ipsec
--sp-mode=transport
--sa-name=sa1
--sp-name=sp1
```

移除安全策略

可以从 ESXi 主机中移除安全策略。

可以使用 `esxcli` vSphere CLI 命令移除安全策略。

前提条件

请确保要使用的安全策略当前未在使用。如果尝试移除正在使用中的安全策略，则移除操作将失败。

步骤

- 在命令提示符下，输入命令 **`esxcli network ip ipsec sp remove --sa-name`** ***安全策略名称***。

  要移除所有安全策略，请输入命令 **`esxcli network ip ipsec sp remove --remove-all`**。

确保 SNMP 配置正确

如果未正确配置 SNMP，则监控信息可能会被发送到恶意主机。然后恶意主机可能会使用此信息计划实施攻击。

步骤

1. 运行 `esxcli system snmp get` 确定当前是否使用 SNMP。
2. 如果您的系统确实需要 SNMP，则通过运行 `esxcli system snmp set --enable true` 命令确保其不在运行。
3. 如果您的系统使用 SNMP，请参见“监控和性能”发布了解 SNMP 3 的安装信息。

   必须在每台 ESXi 主机上配置 SNMP。可以使用 vCLI、PowerCLI 或 vSphere Web Services SDK 进行配置。

仅在需要时才在 vSphere Network Appliance 中使用虚拟交换机

如果您未使用运用 vSphere Network Appliance API (DvFilter) 的产品，请勿将主机配置为向虚拟机发送网络信息。如果 vSphere Network Appliance API 处于启用状态，则攻击者可能会尝试将虚拟机连接到筛选器。此连接可能会提供对主机上其他虚拟机网络的访问。

如果您正在使用运用此 API 的产品，请验证是否已正确配置主机。请参见《开发和部署 vSphere 解决方案、vService 和 ESX 代理》中有关 DvFilter 的部分。如果您的主机设置为使用 API，请确保 `Net.DVFilterBindIpAddress` 参数的值与使用 API 的产品相匹配。

步骤

1 要确保 `Net.DVFilterBindIpAddress` 内核参数的值正确，请使用 vSphere Web Client 找到该参数。

   a 选择主机，然后单击“管理”选项卡。

   b 在“系统”下，选择“高级系统设置”。

   c 向下滚动至 Net.DVFilterBindIpAddress，并验证该参数的值是否为空。

   参数并非严格按照字母顺序排列。请滚动，直到您找到该参数。

2 如果未使用 DvFilter 设置，请确保值为空。

3 如果使用 DvFilter 设置，请确保该参数的值与使用 DvFilter 的产品所使用的值相匹配。

10 确保虚拟机和主机安全的最佳做法

创建并配置主机和虚拟机时，请考虑基本的安全建议。

本章讨论了以下主题：

同步 vSphere 网络上的时钟

在安装 vCenter Single Sign-On 之前，请安装 vSphere Web Client 或部署 vCenter Server Appliance，确保 vSphere 网络上所有计算机的时钟均已同步。

如果 vCenter Server 网络计算机的时钟未同步，则在网络计算机相互通信时，可能会将对时间敏感的 SSL 证书视为无效。未同步的时钟可能会导致验证问题，从而使 vSphere Web Client 安装失败或使 vCenter Server Appliance vpxd 服务无法启动。

请确保运行 vCenter 组件的任一 Windows 主机都与 NTP 服务器保持同步。请参见知识库文章《Windows 计时最佳做法（包括 NTP）》。

- 使 ESX 和 ESXi 时钟与网络时间服务器同步第 131 页，

  安装 vCenter Single Sign-On、vSphere Web Client 或 vCenter Server Appliance 之前，请确保 vSphere 网络上所有计算机的时钟均已同步。

- 将 vCenter Server Appliance 时钟与 NTP 服务器同步第 132 页，

  在部署 vCenter Server Appliance 之前，确保网络中所有计算机的时钟均已同步。如果时钟未同步，会导致安装和身份验证出现错误。

使 ESX 和 ESXi 时钟与网络时间服务器同步

安装 vCenter Single Sign-On、vSphere Web Client 或 vCenter Server Appliance 之前，请确保 vSphere 网络上所有计算机的时钟均已同步。

步骤

1 在 vSphere Web Client 中，连接至 vCenter Server。

2 在清单中选择主机。

3 选择**管理**选项卡。

4 选择**设置**。

5 在“系统”部分中，选择**时间配置**。

6 单击**编辑**并设置 NTP 服务器。

a 选择**使用网络时间协议 (启用 NTP 客户端)**。

b 设置 NTP 服务启动策略。

c 输入要与其同步的 NTP 服务器的 IP 地址。

d 在“NTP 服务状态”部分中单击**启动**或**重新启动**。

7 单击**确定**。

此时，主机将与 NTP 服务器同步。

将 vCenter Server Appliance 时钟与 NTP 服务器同步

在部署 vCenter Server Appliance 之前，确保网络中所有计算机的时钟均已同步。如果时钟未同步，会导致安装和身份验证出现错误。

在加入了 Windows 域的系统中，vCenter Server Appliance 时钟将自动与域控制器同步。在其他系统上，您可通过 VMware Tools 启用同步时钟。或者，您也可执行以下过程。

步骤

1 打开 Web 浏览器并导航到 vCenter Server Appliance 管理界面 (https://*vCenter-Appliance-Address*:5480/)。

2 以根用户身份登录。

3 在 vCenter Server 选项卡中选择“时间”子选项卡。

4 选择一个或多个可用选项。

选项	描述
不同步	不执行同步。
NTP 同步	选择该选项并指定一个或多个 NTP 服务器，可直接将设备配置为与 NTP 服务器同步。
VMware Tools 同步	选择该选项可同步所有虚拟机。
Active Directory 同步	仅当将设备添加到 Active Directory 域时该选项才可用。如果选择该选项，则其他所有选项都将不可用。

5 单击**保存设置**。

vCenter Server Appliance 时钟将与 NTP 服务器同步。

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。

通过身份验证确保 iSCSI 设备的安全

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 Kerberos、安全远程协议 (SRP) 或公用密钥身份验证方法。此外，它也不支持 IPsec 身份验证和加密。

使用 vSphere Web Client 可确定当前是否正在执行身份验证，并配置身份验证方法。

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。

控制基于 CIM 的硬件监控工具访问

公用信息模型 (CIM) 系统提供了一个接口，便于使用一组标准 API 从远程应用程序进行硬件级别管理。为了确保 CIM 接口安全，请仅为这些应用程序提供必需的最小访问权限。如果某个应用程序已经置备有根或完全管理员帐户且该应用程序受到影响，则整个虚拟环境就可能会受到影响。

CIM 是一种开放式标准，用于为 ESXi 硬件资源的无代理且基于标准的监控定义一个框架。该框架由一个 CIM 对象管理器（通常称为“CIM 代理程序”）和一组 CIM 提供程序构成。

CIM 提供程序用作提供设备驱动程序和基础硬件管理访问权限的机制。硬件供应商（包括服务器制造商和特定硬件设备供应商）可编写提供程序，以便对其特定设备进行监控和管理。VMware 还会编写一些提供程序，用于对服务器硬件、ESXi 存储基础架构和虚拟化特定资源实施监控。这些提供程序在 ESXi 系统内运行，因此极其轻量且侧重于特定管理任务。CIM 代理程序从所有 CIM 提供程序获取信息，并通过标准 API（最常见的一个是 WS-MAN）将其呈现给外界。

请不要为远程应用程序提供访问 CIM 接口的 root 凭据。而是应该创建这些应用程序专用的服务帐户，并为 ESXi 系统上定义的任何本地帐户以及 vCenter Server 中定义的任何角色授予对 CIM 信息的只读访问权限。

步骤

1 创建特定于 CIM 应用程序的服务帐户。

2 授予在 ESXi 系统中定义的所有本地帐户以及在 vCenter Server 中定义的所有角色对 CIM 信息的只读访问权限。

3 （可选）如果应用程序需要对 CIM 接口的写入访问权限，请创建一个要应用于服务帐户的角色，使其仅拥有以下两项特权：

   - **主机.配置.系统管理**
   - **主机.CIM.CIM 交互**

   根据监控应用程序的工作方式，该角色可以是主机上的本地角色，也可以在 vCenter Server 中集中定义。

当用户使用为 CIM 应用程序创建的服务帐户登录主机时，该用户仅拥有**系统管理**和 **CIM 交互**特权或只读访问权限。

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。改用 vSphere 或 vSphere 命令行界面（vCLI、PowerCLI 等）之一在所有主机上同时执行此任务。

步骤

1 在托管虚拟机的 ESXi 系统上，浏览到 VMX 文件。

虚拟机配置文件位于 `/vmfs/volumes/datastore` 目录中，其中 *datastore* 是存储虚拟机文件的存储设备的名称。

2 在 VMX 文件中，验证是否设置了以下参数。

```
tools.guestlib.enableHostInfo=FALSE
```

3 保存并关闭文件。

您无法从客户机虚拟机中检索有关主机的性能信息。

11 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：

警报

警报特权控制在清单对象上设置警报并对其作出响应的能力。

此表介绍了创建、修改警报以及对警报做出响应所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-1 警报特权

特权名称	描述	要求
警报.确认警报	允许阻止所有已触发警报上的所有警报操作。	对其定义了警报的对象
警报.创建警报	允许创建新警报。 如果通过自定义操作创建警报，则在用户创建警报时，将验证执行操作的特权。	对其定义了警报的对象
警报.禁用警报操作	允许阻止警报操作在触发警报后发生。此操作不会禁用警报。	对其定义了警报的对象
警报.修改警报	允许更改警报的属性。	对其定义了警报的对象
警报.移除警报	允许删除警报。	对其定义了警报的对象
警报.设置警报状态	允许更改所配置的事件警报的状态。状态可以更改为**正常**、**警告**或**警示**。	对其定义了警报的对象

数据中心

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。

下表介绍了创建和编辑数据中心所需的特权。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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-2 数据中心特权

特权名称	描述	要求
数据中心.创建数据中心	允许创建新数据中心。	数据中心文件夹或根对象
数据中心.移动数据中心	允许移动数据中心。 特权必须存在于源位置和目标位置。	数据中心、源位置和目标位置
数据中心.网络配置文件配置	允许为数据中心配置网络配置文件。	数据中心
数据中心.查询 IP 池分配	允许 IP 地址池的配置。	数据中心
数据中心.重新配置数据中心	允许重新配置数据中心。	数据中心
数据中心.释放 IP 分配	允许为数据中心发布分配的 IP 分配。	数据中心
数据中心.移除数据中心	允许移除数据中心。 为了有执行此操作的权限，必须将此特权分配给该对象及其父对象。	数据中心加父对象
数据中心.重命名数据中心	允许更改数据中心的名称。	数据中心

数据存储

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。

下表介绍了使用数据存储所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-3 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。 特权必须存在于源位置和目标位置。	数据存储、源位置和目标位置
数据存储.移除数据存储	允许移除数据存储。 此特权已弃用。 要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。	数据存储
数据存储.移除文件	允许在数据存储中删除文件。 此特权已弃用。分配**低级别文件操作**特权。	数据存储

表 11-3 数据存储特权 （续）

特权名称	描述	要求
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

数据存储群集

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。

下表介绍了用于配置数据存储群集的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-4 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

vSphere Distributed Switch

vSphere Distributed Switch 特权控制执行与 vSphere Distributed Switch 管理相关的任务的能力。

此表描述创建和配置 vSphere Distributed Switch 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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-5 vSphere Distributed Switch 特权

特权名称	描述	要求
vSphere Distributed Switch.创建	允许创建 vSphere Distributed Switch。	数据中心、网络文件夹
vSphere Distributed Switch.删除	允许移除 vSphere Distributed Switch。 要有执行此操作的权限，必须将此特权分配给该对象及其父对象。	vSphere Distributed Switch
vSphere Distributed Switch.主机操作	允许更改 vSphere Distributed Switch 的主机成员。	vSphere Distributed Switch
vSphere Distributed Switch.修改	允许更改 vSphere Distributed Switch 的配置。	vSphere Distributed Switch
vSphere Distributed Switch.移动	允许将 vSphere Distributed Switch 移动到其他文件夹。	vSphere Distributed Switch
vSphere Distributed Switch.Network I/O Control 操作	允许更改 vSphere Distributed Switch 的资源设置。	vSphere Distributed Switch
vSphere Distributed Switch.策略操作	允许更改 vSphere Distributed Switch 的策略。	vSphere Distributed Switch
vSphere Distributed Switch.端口配置操作	允许更改 vSphere Distributed Switch 中端口的配置。	vSphere Distributed Switch

表 11-5 vSphere Distributed Switch 特权 （续）

特权名称	描述	要求
vSphere Distributed Switch.端口设置操作	允许更改 vSphere Distributed Switch 中端口的设置。	vSphere Distributed Switch
vSphere Distributed Switch.VSPAN 操作	允许更改 vSphere Distributed Switch 的 VSPAN 配置。	vSphere Distributed Switch

ESX Agent Manager

ESX Agent Manager 特权控制与 ESX Agent Manager 和代理虚拟机相关的操作。

下表描述了与 ESX Agent Manager 和代理虚拟机相关的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-6 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

扩展特权控制安装和管理扩展的能力。

下表描述安装和管理插件所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-7 扩展特权

特权名称	描述	要求
扩展.注册扩展	允许注册扩展（插件）。	根 vCenter Server
扩展.取消注册扩展	允许取消注册扩展（插件）。	根 vCenter Server
扩展.更新扩展	允许更新扩展（插件）。	根 vCenter Server

文件夹

文件夹特权控制创建和管理文件夹的功能。

下表描述创建和管理文件夹所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-8 文件夹特权

特权名称	描述	要求
文件夹.创建文件夹	允许创建新文件夹。	文件夹
文件夹.删除文件夹	允许删除文件夹。 要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。	文件夹
文件夹.移动文件夹	允许移动文件夹。 特权必须存在于源位置和目标位置。	文件夹
文件夹.重命名文件夹	允许更改文件夹的名称。	文件夹

全局

全局特权控制与任务、脚本和扩展相关的全局任务。

下表描述了 vSphere Web Client 中全局任务所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-9 全局特权

特权名称	描述	要求
全局.充当 vCenter Server	允许准备或启动 vMotion 发送操作或 vMotion 接收操作。	根 vCenter Server
全局.取消任务	允许取消正在运行或已排队的任务。	与任务相关的清单对象
全局.容量规划	允许使用容量规划来规划物理机到虚拟机的整合。	根 vCenter Server
全局.诊断	允许检索诊断文件、日志头、二进制文件或诊断捆绑包的列表。 要避免潜在的安全破坏，请将此特权限制为 vCenter Server 管理员角色。	根 vCenter Server
全局.禁用方法	允许 vCenter Server 扩展的服务器对 vCenter Server 管理的对象禁用某些操作。	根 vCenter Server
全局.启用方法	允许 vCenter Server 扩展的服务器对 vCenter Server 管理的对象启用某些操作。	根 vCenter Server
全局.全局标记	允许添加或移除全局标记。	根主机或 vCenter Server
全局.健康状况	允许查看 vCenter Server 组件的健康状况。	根 vCenter Server
全局.许可证	允许查看安装的许可证并添加或移除许可证。	根主机或 vCenter Server
全局.记录事件	允许针对特定的受管实体记录用户定义的事件。	任何对象
全局.管理自定义属性	允许添加、移除或重命名自定义字段定义。	根 vCenter Server
全局.代理	允许访问内部接口以将端点添加到代理或从代理移除端点。	根 vCenter Server
全局.脚本操作	允许调度与警报一起使用的脚本操作。	任何对象
全局.服务管理器	允许在 vSphere CLI 中使用 `resxtop` 命令。	根主机或 vCenter Server
全局.设置自定义属性	允许查看、创建或移除受管对象的自定义属性。	任何对象
全局.设置	允许读取并修改运行时 vCenter Server 配置设置。	根 vCenter Server
全局.系统标记	允许添加或移除系统标记。	根 vCenter Server

主机 CIM

主机 CIM 特权控制主机健康状况监控的 CIM 使用。

下表描述了用于 CIM 主机健康状况监控的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-10 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

主机配置特权控制配置主机的能力。

下表描述了配置主机设置所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-11 主机配置特权

特权名称	描述	要求
主机.配置.高级设置	允许在主机配置中设置高级选项。	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 PciPassthru 设置	允许更改主机的 PciPassthru 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。ESX 主机上不支持锁定模式。	主机
主机.配置.更改 SNMP 设置	允许配置、重新启动和停止 SNMP 代理。	主机
主机.配置.连接	允许更改主机的连接状态（已连接或已断开连接）。	主机
主机.配置.固件	允许更新 ESXi 主机的固件。	主机
主机.配置.超线程	允许启用和禁用主机 CPU 调度程序中的超线程。	主机
主机.配置.映像配置	允许更改与主机关联的映像。	
主机.配置.维护	允许使主机进入和退出维护模式，以及关闭和重新启动主机。	主机
主机.配置.内存配置	允许修改主机配置	主机
主机.配置.网络配置	允许配置网络、防火墙和 vMotion 网络。	主机
主机.配置.电源	允许配置主机电源管理设置。	主机
主机.配置.查询修补程序	允许查询可安装的修补程序并将修补程序安装在主机上。	主机
主机.配置.安全配置文件和防火墙	允许配置 Internet 服务，如 SSH、Telnet、SNMP 和主机防火墙。	主机
主机.配置.存储器分区配置	允许管理 VMFS 数据存储和诊断分区。具有此特权的用户可以扫描新存储设备并管理 iSCSI。	主机
主机.配置.系统管理	允许扩展以便操作主机上的文件系统。	主机

表 11-11 主机配置特权 （续）

特权名称	描述	要求
主机.配置.系统资源	允许更新系统资源层次结构的配置。	主机
主机.配置.虚拟机自动启动配置	允许更改单个主机上虚拟机的自动启动和自动停止顺序。	主机

主机清单

主机清单特权控制向清单添加主机、向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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-12 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。 特权必须存在于源位置和目标位置。	群集
主机.清单.移动主机	允许将一组现有主机移入或移出群集。 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。 要有执行此操作的权限，必须将此特权分配给该对象及其父对象。	群集、主机
主机.清单.移除主机	允许移除主机。 要有执行此操作的权限，必须将此特权分配给该对象及其父对象。	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

主机本地操作特权控制当 vSphere Client 直接连接到主机时执行的操作。

下表描述了当 vSphere Client 直接连接到单个主机时执行的操作所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-13 主机本地操作特权

特权名称	描述	要求
主机.本地操作.将主机添加到 vCenter	允许安装和卸载主机上的 vCenter 代理，如 vpxa 和 aam。	根主机
主机.本地操作.创建虚拟机	允许在磁盘上从头开始创建新的虚拟机，而不在主机上注册。	根主机
主机.本地操作.删除虚拟机	允许在磁盘上删除虚拟机。支持注册和未注册的虚拟机。	根主机
主机.本地操作.提取 NVRAM 内容	允许提取主机的 NVRAM 内容。	

表 11-13 主机本地操作特权 （续）

特权名称	描述	要求
主机.本地操作.管理用户组	允许在主机上管理本地帐户。	根主机
主机.本地操作.重新配置虚拟机	允许对虚拟机进行重新配置。	根主机
主机.本地操作.重新布局快照	允许更改虚拟机快照的布局。	根主机

主机 vSphere Replication

主机 vSphere Replication 特权可控制对主机的虚拟机使用复制的情况。

下表描述了 VMware vCenter Site Recovery Manager™ 进行虚拟机复制所用的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-14 主机 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

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。

下表描述了创建和修改主机配置文件所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-15 主机配置文件特权

特权名称	描述	要求
主机配置文件.清除	允许清除配置文件相关信息。	根 vCenter Server
主机配置文件.创建	允许创建主机配置文件。	根 vCenter Server
主机配置文件.删除	允许删除主机配置文件。	根 vCenter Server
主机配置文件.编辑	允许编辑主机配置文件。	根 vCenter Server
主机配置文件.导出	允许导出主机配置文件。	根 vCenter Server
主机配置文件.查看	允许查看主机配置文件。	根 vCenter Server

网络

网络特权控制与网络管理相关的任务。

下表描述网络管理所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-16 网络特权

特权名称	描述	要求
网络.分配网络	允许将网络分配到虚拟机。	网络、虚拟机
网络.配置	允许配置网络。	网络、虚拟机
网络.移动网络	允许在文件夹之间移动网络。 特权必须存在于源位置和目标位置。	网络
网络.移除	允许移除网络。 此特权已弃用。 要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。	网络

性能

性能特权对修改性能统计信息设置进行控制。

下表描述修改性能统计信息设置所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-17 性能特权

特权名称	描述	要求
性能.修改时间间隔	允许创建、移除和更新性能数据收集时间间隔。	根 vCenter Server

权限

权限特权控制角色和权限的分配。

下表描述分配角色和权限所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-18 权限特权

特权名称	描述	要求
权限.修改权限	允许为实体定义一个或多个权限规则，或者如果实体上的特定用户或组已经有规则，则更新规则。 要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。	任何对象加父对象
权限.修改角色	允许更新角色的名称及其特权。	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

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。

下表描述了查看和更新存储配置文件所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-19 配置文件驱动的存储特权

特权名称	描述	要求
配置文件驱动的存储.配置文件驱动的存储更新	允许对存储配置文件进行更改，如创建和更新存储功能和虚拟机存储配置文件。	根 vCenter Server
配置文件驱动的存储.配置文件驱动的存储视图	允许查看定义的存储功能和存储配置文件。	根 vCenter Server

资源

资源特权控制资源池的创建和管理，以及虚拟机的迁移。

该表描述控制资源管理和虚拟机迁移的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-20 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。 特权必须存在于源位置和目标位置。	资源池
资源.查询 vMotion	允许查询虚拟机与一组主机的一般 vMotion 兼容性。	根 vCenter Server
资源.重定位	允许执行从虚拟机至特定资源池或主机的冷迁移。	虚拟机
资源.移除资源池	允许删除资源池。 要有执行此操作的权限，必须将此特权分配给该对象及其父对象。	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

已调度任务特权控制已调度任务的创建、编辑和移除。

该表描述创建和修改调度任务所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-21 已调度任务特权

特权名称	描述	要求
已调度任务.创建任务	允许调度任务。在调度时，需要一定的特权来执行已调度的操作。	任何对象
已调度任务.修改任务	允许重新配置已调度任务的属性。	任何对象
已调度任务.移除任务	允许移除队列中的已调度任务。	任何对象
已调度任务.运行任务	允许立即运行已调度任务。 创建和运行已调度任务也需要执行关联操作的权限。	任何对象

会话

会话特权控制扩展打开 vCenter Server 上的会话的能力。

该表描述与 vCenter Server 上的会话关联的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-22 会话特权

特权名称	描述	要求
会话.模拟用户	允许模拟其他用户。该功能由扩展使用。	根 vCenter Server
会话.消息	允许在消息中设置全局日志。	根 vCenter Server
会话.验证会话	允许验证会话有效性。	根 vCenter Server
会话.查看和停止会话	允许查看会话以及强制注销一个或多个已登录的用户。	根 vCenter Server

存储视图

存储视图特权可控制在 vCenter Server 上配置和使用存储视图的能力。

该表描述配置和使用存储视图所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-23 存储视图特权

特权名称	描述	要求
存储视图.配置服务	允许更改各个选项，例如报告更新时间间隔和数据库连接信息。	根 vCenter Server
存储视图.查看	允许查看“存储视图”选项卡。	根 vCenter Server

任务

任务特权控制扩展在 vCenter Server 上创建和更新任务的能力。

该表描述与任务相关的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-24 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。	根 vCenter Server
任务.更新任务	允许扩展更新用户定义的任务。	根 vCenter Server

vApp

vApp 特权控制与部署和配置 vApp 相关的操作。

下表描述与 vApp 相关的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-25 vApp 特权

特权名称	描述	要求
vApp.添加虚拟机	允许将虚拟机添加到 vApp。	vApp
vApp.分配资源池	允许将资源池分配到 vApp。	vApp
vApp.分配 vApp	允许将一个 vApp 分配给另一个 vApp	vApp
vApp.克隆	允许克隆 vApp。	vApp
vApp.创建	允许创建 vApp。	vApp
vApp.删除	允许删除 vApp。 要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。	vApp
vApp.导出	允许从 vSphere 导出 vApp。	vApp
vApp.导入	允许将 vApp 导入 vSphere。	vApp
vApp.移动	允许将 vApp 移动到新清单位置。	vApp
vApp.关闭电源	允许对 vApp 执行关闭电源操作。	vApp
vApp.打开电源	允许对 vApp 执行打开电源操作。	vApp
vApp.重命名	允许重命名 vApp。	vApp
vApp.挂起	允许暂停 vApp。	vApp
vApp.取消注册	允许取消注册 vApp。 要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。	vApp
vApp.查看 OVF 环境	允许在 vApp 中查看已打开电源的虚拟机的 OVF 环境。	vApp
vApp.vApp 应用程序配置	允许修改 vApp 的内部结构，例如产品信息和属性。	vApp
vApp.vApp 实例配置	允许修改 vApp 的实例配置，例如策略。	vApp
vApp.vApp 管理者配置	允许扩展或解决方案将 vApp 标记为由该扩展或解决方案管理。 没有与此特权关联的 vSphere Web Client 用户界面元素。	vApp
vApp.vApp 资源配置	允许修改 vApp 的资源配置。 要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。	vApp

vCenter Inventory Service 标记

vCenter Inventory Service 标记特权控制创建和删除标记和标记类别的功能，并分配和移除 vSphere 清单对象上的标记。

下表描述与标记相关的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-26 vCenter Inventory Service 特权

特权名称	描述	要求
vCenter Inventory Service.vCenter Inventory Service 标记.分配或取消分配 Inventory Service 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
vCenter Inventory Service.vCenter Inventory Service 标记.创建 Inventory Service 标记类别	允许创建标记类别。	任何对象
vCenter Inventory Service.vCenter Inventory Service 标记.创建 Inventory Service 标记	允许创建标记。	任何对象
vCenter Inventory Service.vCenter Inventory Service 标记.删除 Inventory Service 标记类别	允许删除标记类别。	任何对象
vCenter Inventory Service.vCenter Inventory Service 标记.删除 Inventory Service 标记	允许删除标记。	任何对象
vCenter Inventory Service.vCenter Inventory Service 标记.编辑 Inventory Service 标记类别	允许编辑标记类别。	任何对象
vCenter Inventory Service.vCenter Inventory Service 标记.编辑 Inventory Service 标记	允许编辑标记。	任何对象

虚拟机配置

虚拟机配置特权控制配置虚拟机选项和设备的能力。

此表描述配置虚拟机选项和设备所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-27 虚拟机配置特权

特权名称	描述	要求
虚拟机.配置.添加现有磁盘	允许将现有虚拟磁盘添加到虚拟机。	虚拟机
虚拟机.配置.添加新磁盘	允许创建新虚拟磁盘以添加到虚拟机。	虚拟机
虚拟机.配置.添加或移除设备	允许添加或移除任何非磁盘设备。	虚拟机
虚拟机.配置.高级	允许在虚拟机的配置文件中添加或修改高级参数。	虚拟机
虚拟机.配置.更改 CPU 计数	允许更改虚拟 CPU 的数目。	虚拟机
虚拟机.配置.更改资源	允许更改给定资源池中一组虚拟机节点的资源配置。	虚拟机
虚拟机.配置.配置管理者	允许扩展或解决方案将虚拟机标记为由该扩展或解决方案管理。	虚拟机

表 11-27 虚拟机配置特权（续）

特权名称	描述	要求
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.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。 设置此参数将替代用于修改裸设备（包括连接状况）的任何其他特权。	虚拟机
虚拟机.配置.基于路径重新加载	允许更改虚拟机配置路径，而保留虚拟机的标识。诸如 VMware vCenter Site Recovery Manager 等解决方案使用此操作在故障切换和故障恢复期间保持虚拟机的标识。	虚拟机
虚拟机.配置.移除磁盘	允许移除虚拟磁盘设备。	虚拟机
虚拟机.配置.重命名	允许重命名虚拟机或修改虚拟机的相关注释。	虚拟机
虚拟机.配置.重置客户机信息	允许编辑虚拟机的客户机操作系统信息。	虚拟机
虚拟机.配置.设置注释	允许添加或编辑虚拟机注释。	虚拟机
虚拟机.配置.设置	允许更改常规虚拟机设置。	虚拟机
虚拟机.配置.交换文件放置位置	允许更改虚拟机的交换文件放置策略。	虚拟机
虚拟机.配置.解锁虚拟机	允许对虚拟机进行解密。	虚拟机
虚拟机.配置.升级虚拟机兼容性	允许升级虚拟机的虚拟机兼容性版本。	虚拟机

虚拟机客户机操作

虚拟机客户机操作特权控制与虚拟机的客户机操作系统中的文件和程序交互的能力。

该表描述通过 VMware vSphere API 访问的虚拟机客户机操作所需的特权。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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-28 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.客户机操作修改	允许在虚拟机中对客户机操作系统进行修改的虚拟机客户机操作，如向虚拟机传输文件。 没有与此特权关联的 vSphere Web Client 用户界面元素。	虚拟机
虚拟机.客户机操作.客户机操作程序执行	允许在虚拟机中执行程序的虚拟机客户机操作。 没有与此特权关联的 vSphere Web Client 用户界面元素。	虚拟机
虚拟机.客户机操作.客户机操作查询	允许对客户机操作系统进行查询的虚拟机客户机操作，如在客户机操作系统中列出文件。 没有与此特权关联的 vSphere Web Client 用户界面元素。	虚拟机

虚拟机交互

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。

此表描述虚拟机交互所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-29 虚拟机交互

特权名称	描述	要求
虚拟机.交互.回答问题	允许解决虚拟机状态转换的问题或运行时错误。	虚拟机
虚拟机.交互.备份虚拟机上的操作	允许对虚拟机执行备份操作。	虚拟机
虚拟机.交互.配置 CD 媒体	允许配置虚拟 DVD 或 CD-ROM 设备。	虚拟机
虚拟机.交互.配置软盘媒体	允许配置虚拟软盘设备。	虚拟机
虚拟机.交互.控制台交互	允许与虚拟机的虚拟鼠标、键盘和屏幕交互。	虚拟机
虚拟机.交互.创建屏幕截图	允许创建虚拟机屏幕截图。	虚拟机
虚拟机.交互.对所有磁盘执行碎片整理	允许对虚拟机上的所有磁盘执行碎片整理操作。	虚拟机
虚拟机.交互.设备连接	允许更改虚拟机的可断开虚拟设备的连接状况。	虚拟机
虚拟机.交互.禁用 Fault Tolerance	允许使用 Fault Tolerance 禁用虚拟机的辅助虚拟机。	虚拟机
虚拟机.交互.启用 Fault Tolerance	允许使用 Fault Tolerance 启用虚拟机的辅助虚拟机。	虚拟机
虚拟机.交互.通过 VIX API 执行客户机操作系统管理	允许通过 VIX API 管理虚拟机的操作系统。	虚拟机
虚拟机.交互.插入 USP HID 扫描代码	允许插入 USP HID 扫描代码。	虚拟机
虚拟机.交互.执行擦除或压缩操作	允许对虚拟机执行擦除或压缩操作。	虚拟机
虚拟机.交互.关闭电源	允许关闭已打开电源的虚拟机的电源。此操作将关闭客户机操作系统。	虚拟机
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

表 11-29 虚拟机交互（续）

特权名称	描述	要求
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.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
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

虚拟机清单特权控制虚拟机的添加、移动和移除。

此表描述在清单中添加、移动和移除虚拟机所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-30 虚拟机清单特权

特权名称	描述	要求
虚拟机.清单.从现有项创建	允许通过从模板克隆或部署，基于现有虚拟机或模板创建虚拟机。	群集、主机、虚拟机文件夹
虚拟机.清单.新建	允许创建虚拟机并为其执行分配资源。	群集、主机、虚拟机文件夹
虚拟机.清单.移动	允许在层次结构中重定位虚拟机。 特权必须存在于源位置和目标位置。	虚拟机
虚拟机.清单.注册	允许将现有虚拟机添加到 vCenter Server 或主机清单。	群集、主机、虚拟机文件夹
虚拟机.清单.移除	允许删除虚拟机。删除操作将从磁盘移除虚拟机的基础文件。 要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。	虚拟机
虚拟机.清单.取消注册	允许从 vCenter Server 或主机清单中取消注册虚拟机。 要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。	虚拟机

虚拟机置备

虚拟机置备特权控制与部署和自定义虚拟机相关的活动。

此表描述虚拟机置备所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-31 虚拟机置备特权

特权名称	描述	要求
虚拟机.置备.允许访问磁盘	允许打开虚拟机上的磁盘进行随机读写访问。常用于远程磁盘装载。	虚拟机
虚拟机.置备.允许对磁盘进行只读访问	允许打开虚拟机上的磁盘进行随机读取访问。常用于远程磁盘装载。	虚拟机
虚拟机.置备.允许下载虚拟机	允许读取与虚拟机关联的文件，包括 vmx、磁盘文件、日志和 nvram。	根主机或 vCenter Server
虚拟机.置备.允许上载虚拟机文件	允许写入与虚拟机关联的文件，包括 vmx、磁盘文件、日志和 nvram。	根主机或 vCenter Server
虚拟机.置备.克隆模板	允许克隆模板。	模板
虚拟机.置备.克隆虚拟机	允许克隆现有虚拟机和资源分配。	虚拟机
虚拟机.置备.从虚拟机创建模板	允许从虚拟机创建新模板。	虚拟机
虚拟机.置备.自定义	允许自定义虚拟机的客户机操作系统，而不移动虚拟机。	虚拟机
虚拟机.置备.部署模板	允许从模板部署虚拟机。	模板
虚拟机.置备.标记为模板	允许将现有已关闭电源的虚拟机标记为模板。	虚拟机
虚拟机.置备.标记为虚拟机	允许将现有模板标记为虚拟机。	模板
虚拟机.置备.修改自定义规范	允许创建、修改或删除自定义规范。	根 vCenter Server
虚拟机.置备.升级磁盘	允许升级虚拟机的磁盘。	虚拟机
虚拟机.置备.读取自定义规范	允许读取自定义规范。	虚拟机

虚拟机快照管理特权

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。

此表描述处理虚拟机快照所需的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-32 虚拟机状况特权

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

虚拟机 vSphere Replication 特权可控制对虚拟机使用复制的情况。

下表描述了 VMware vCenter Site Recovery Manager™ 进行虚拟机复制所用的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-33 虚拟机 vSphere Replication

特权名称	描述	要求
虚拟机.vSphere Replication.配置 vSphere Replication	允许对虚拟机进行复制配置。	虚拟机
虚拟机.vSphere Replication.管理 vSphere Replication	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 vSphere Replication	允许监控复制。	虚拟机

dvPort 组

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-34 分布式虚拟端口组特权

特权名称	描述	要求
Distributed Switch.创建	允许创建分布式虚拟端口组。	虚拟端口组
Distributed Switch.删除	允许删除分布式虚拟端口组。 要有执行此操作的权限，必须将此特权分配给该对象及其父对象。	虚拟端口组
Distributed Switch.修改	允许修改分布式虚拟端口组的配置。	虚拟端口组
Distributed Switch.策略操作	允许设置分布式虚拟端口组的策略。	虚拟端口组
Distributed Switch.端口配置操作	允许设置分布式虚拟端口组的范围。	虚拟端口组

vService

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。

此表描述与 vService 依赖关系相关的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-35 vService

特权名称	描述	要求
vService.创建依赖关系	允许创建虚拟机或 vApp 的 vService 依赖关系。	vApp 和虚拟机
vService.破坏依赖关系	允许移除虚拟机或 vApp 的 vService 依赖关系。	vApp 和虚拟机
vService.重新配置依赖关系配置	允许重新配置依赖关系以更新提供程序或绑定。	vApp 和虚拟机
vService.更新依赖关系	允许更新依赖关系以配置名称或描述。	vApp 和虚拟机

VRM 策略

VRM 策略特权可控制查询和更新虚拟权限管理策略的能力。

此表描述与虚拟权限管理相关的特权。

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。“要求对象”列中列出的对象必须具有特权组，可以直接具有，也可以通过继承获得。

表 11-36 VRM 策略特权

特权名称	描述	要求
VRMPolicy.查询 VRMPolicy	允许查询虚拟权限管理策略。	虚拟机
VRMPolicy.更新 VRMPolicy	允许更新虚拟权限管理策略。	虚拟机

索引

V

W

X

Y

Z