

# Horizon Client 和 Agent 安全指南

Horizon Client 3.x/4.x 和 View Agent 6.2.x/Horizon Agent  
7.2/7.1/7.0.x

VMware Horizon 7 7.2



vmware®

您可以从 VMware 网站下载最新的技术文档:

<https://docs.vmware.com/cn/>。

如果您对本文档有任何意见或建议, 请将反馈信息发送至:

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

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

**威睿信息技术(中国)有限公司**  
北京办公室  
北京市  
朝阳区新源南路 8 号  
启皓北京东塔 8 层 801  
[www.vmware.com/cn](http://www.vmware.com/cn)

上海办公室  
上海市  
淮海中路 333 号  
瑞安大厦 804-809 室  
[www.vmware.com/cn](http://www.vmware.com/cn)

广州办公室  
广州市  
天河路 385 号  
太古汇一座 3502 室  
[www.vmware.com/cn](http://www.vmware.com/cn)

版权所有 © 2015-2017 VMware, Inc. 保留所有权利。 [版权和商标信息](#)

# 目录

## Horizon Client 和 Agent 安全指南 5

### 1 外部端口 6

了解 Horizon 7 通信协议 6

Horizon Agent 的防火墙规则 7

客户端和代理使用的 TCP 和 UDP 端口 8

### 2 安装的服务、守护程序和进程 11

View Agent 或 Horizon Agent 安装程序在 Windows 计算机上安装的服务 11

Windows 客户端上安装的服务 12

在其他客户端和 Linux 桌面中安装的守护程序 12

### 3 要保护的资源 14

实施用于保护客户端系统的最佳做法 14

配置文件位置 14

帐户 15

### 4 客户端和代理的安全性设置 16

配置证书检查 16

Horizon Agent 配置模板中的安全性相关设置 17

在 Linux 桌面上的配置文件中设置选项 18

HTML Access 的组策略设置 24

Horizon Client 配置模板中的安全性设置 25

配置 Horizon Client 证书验证模式 28

配置本地安全机构保护 29

### 5 配置安全协议和密码套件 30

安全协议和密码套件的默认策略 30

为特定客户端类型配置安全协议和密码套件 39

在 SSL/TLS 中禁用弱密码 39

为 HTML Access Agent 配置安全协议和密码套件 40

在 View 桌面上配置建议策略 41

### 6 客户端和代理日志文件位置 42

适用于 Windows 的 Horizon Client 日志 42

适用于 Mac 的 Horizon Client 日志 44

适用于 Linux 的 Horizon Client 日志 45

[移动设备上的 Horizon Client 日志](#) 46

[Windows 计算机的 Horizon Agent 日志](#) 47

[Linux 桌面日志](#) 48

## **7 应用安全修补程序** 50

[为 View Agent 或 Horizon Agent 应用修补程序](#) 50

[为 Horizon Client 应用修补程序](#) 51

# Horizon Client 和 Agent 安全指南

《Horizon Client 和 Agent 安全指南》提供了 VMware Horizon<sup>®</sup> Client<sup>™</sup> 和 Horizon Agent（对于 Horizon 7）或 VMware View Agent<sup>®</sup>（对于 Horizon 6）安全功能的简要参考。本指南是对《View 安全指南》指南的补充，后者是为 VMware Horizon<sup>™</sup> 6 和 Horizon 7 的所有主要和次要版本编写的。《Horizon Client 和 Agent 安全指南》指南每季度更新一次，这是随每季度发行的客户端和代理软件一起发行的。

Horizon Client 是最终用户为连接到远程应用程序或桌面从其客户端设备中启动的应用程序。View Agent（对于 Horizon 6）或 Horizon Agent（对于 Horizon 7）是在远程桌面或提供远程应用程序的 Microsoft RDS 主机的操作系统中运行的代理软件。本指南包括下列信息：

- 所需的系统登录帐户。在系统安装/引导期间创建的帐户登录 ID 以及如何更改默认值的说明。
- 安全性相关的配置选项和设置。
- 必须受到保护的资源，如安全性相关的配置文件和密码，以及对安全操作的建议访问控制。
- 日志文件的位置及其用途。
- 分配给服务用户的特权。
- 必须打开或启用以正确运行客户端和代理的外部接口、端口和服务。
- 有关客户如何获取并应用最新的安全更新或修补程序的信息。

## 目标读者

这些信息面向 IT 决策制定者、架构师、管理员以及其他必须熟悉 Horizon 6 或 Horizon 7 安全组件（包括客户端和代理）的人员。

## VMware 技术出版物词汇表

VMware 技术出版物提供您可能感到生疏的术语表。有关 VMware 技术文档中使用的术语的定义，请转至 <http://www.vmware.com/support/pubs>。

# 外部端口

为确保产品正常运行，必须根据您需要使用的功能打开不同的端口，以便远程桌面上的客户端和代理可以相互通信。

本章讨论了以下主题：

- 了解 [Horizon 7 通信协议](#)
- [Horizon Agent 的防火墙规则](#)
- 客户端和代理使用的 [TCP 和 UDP 端口](#)

## 了解 Horizon 7 通信协议

Horizon 7 组件之间通过几种不同的协议来交换消息。

[表 1-1. 默认端口](#) 中列出了每个协议所用的默认端口。必要时，您可以更改使用哪些端口号，以遵循组织策略或避免争用问题。

**表 1-1. 默认端口**

协议	端口
JMS	TCP 端口 4001
	TCP 端口 4002
HTTP	TCP 端口 80
HTTPS	TCP 端口 443
MMR/CDR	TCP 端口 9427（用于多媒体重定向和客户端驱动器重定向）
RDP	TCP 端口 3389
PCoIP	TCP 端口 4172
	UDP 端口 4172、50002 和 55000
USB 重定向	TCP 端口 32111。此端口还用于时区同步。
VMware Blast Extreme	TCP 端口 8443 和 22443
	UDP 端口 443、8443 和 22443
HTML Access	TCP 端口 8443 和 22443

## Horizon Agent 的防火墙规则

Horizon Agent 安装程序可以选择在远程桌面和 RDS 主机中配置 Windows 防火墙规则，以打开默认网络端口。如非特别注明，端口均为传入端口。

代理安装程序为入站 RDP 连接配置本地防火墙规则，以便与主机操作系统的当前 RDP 端口（通常为 3389）相匹配。

如果您指示代理安装程序不启用远程桌面支持，安装程序不会打开端口 3389 和 32111，您必须手动打开这些端口。

如果在安装后更改了 RDP 端口号，您必须更改关联的防火墙规则。要在安装后更改默认端口，必须手动重新配置 Windows 防火墙规则以允许通过更新后的端口进行访问。请参阅《View 安装指南》文档中的“替换 View 服务的默认端口”。

RDS 主机上的 Horizon Agent 中的 Windows 防火墙规则将一组连续的 UDP 端口（256 个）显示为入站流量的打开端口。这些端口供 Horizon Agent 上的 VMWare Blast Extreme 内部使用。RDS 主机上的一个特殊 Microsoft 签名驱动程序可阻止外部来源传送到这些端口的入站流量。该驱动程序导致 Windows 防火墙将端口视为已关闭。

如果您使用虚拟机模板作为桌面源，只有在模板为桌面域成员的情况下，防火墙异常才会在部署的桌面中继续存在。您可以使用 Microsoft 组策略设置管理本地防火墙例外规则。有关更多信息，请参阅 Microsoft 知识库 (KB) 文章 875357。

**表 1-2. 在代理安装期间打开的 TCP 和 UDP 端口**

协议	端口
RDP	TCP 端口 3389
USB 重定向和时区同步	TCP 端口 32111
MMR（多媒体重定向）和 CDR（客户端驱动器重定向）	TCP 端口 9427
PCoIP	TCP 端口 4172
	UDP 端口 4172（双向）
VMware Blast Extreme	TCP 端口 22443
	UDP 端口 22443（双向）
	<a href="#">注</a> UDP 不用于 Linux 桌面。
HTML Access	TCP 端口 22443

## 客户端和代理使用的 TCP 和 UDP 端口

View Agent（适用于 Horizon 6）、Horizon Agent（适用于 Horizon 7）和 Horizon Client 使用 TCP 和 UDP 端口在彼此之间以及与各种 Horizon 7 Server 组件之间进行网络访问。

**表 1-3. View Agent 或 Horizon Agent 使用的 TCP 和 UDP 端口**

源	端口	目标	端口	协议	说明
Horizon Client	*	View Agent/ Horizon Agent	3389	TCP	指向 View 桌面的 Microsoft RDP 流量（如果使用直接连接而不是安全加密链路连接）。
Horizon Client	*	View Agent/ Horizon Agent	9427	TCP	Windows Media MMR 重定向和客户端驱动器重定向（如果使用直接连接而不是安全加密链路连接）。  <a href="#">注</a> 使用 VMware Blast Extreme 时无需进行 CDR。
Horizon Client	*	View Agent/ Horizon Agent	32111	TCP	USB 重定向和时区同步（如果使用直接连接而不是安全加密链路连接）。
Horizon Client	*	View Agent/ Horizon Agent	4172	TCP 和 UDP	PCoIP（如果未使用 PCoIP 安全网关）。  <a href="#">注</a> 由于源端口有所不同，请参阅此表格下面的注释。
Horizon Client	*	Horizon Agent	22443	TCP 和 UDP	VMware Blast Extreme（如果使用直接连接而不是安全加密链路连接）。  <a href="#">注</a> UDP 不用于 Linux 桌面。
浏览器	*	View Agent/ Horizon Agent	22443	TCP	HTML Access（如果使用直接连接而不是安全加密链路连接）。
安全服务器、View 连接服务器或 Unified Access Gateway 设备	*	View Agent/ Horizon Agent	3389	TCP	到 View 桌面的 Microsoft RDP 流量（使用安全加密链路连接时）。
安全服务器、View 连接服务器或 Unified Access Gateway 设备	*	View Agent/ Horizon Agent	9427	TCP	Windows Media MMR 重定向和客户端驱动器重定向（使用安全加密链路连接时）。
安全服务器、View 连接服务器或 Unified Access Gateway 设备	*	View Agent/ Horizon Agent	32111	TCP	USB 重定向和时区同步（使用安全加密链路连接时）。
安全服务器、View 连接服务器或 Unified Access Gateway 设备	55000	View Agent/ Horizon Agent	4172	UDP	PCoIP（非 SALSA20）（如果使用 PCoIP 安全网关）。
安全服务器、View 连接服务器或 Unified Access Gateway 设备	*	View Agent/ Horizon Agent	4172	TCP	PCoIP（如果使用 PCoIP 安全网关）。
安全服务器、View 连接服务器或 Unified Access Gateway 设备	*	Horizon Agent	22443	TCP 和 UDP	VMware Blast Extreme（如果使用 Blast 安全网关）。  <a href="#">注</a> UDP 不用于 Linux 桌面。

源	端口	目标	端口	协议	说明
安全服务器、View 连接服务器或 Unified Access Gateway 设备	*	View Agent/ Horizon Agent	22443	TCP	HTML Access（如果使用 Blast 安全网关）。
View Agent/Horizon Agent	*	View 连接服务器	4001、 4002	TCP	JMS SSL 流量。
View Agent/Horizon Agent	4172	Horizon Client	*	UDP	PCoIP（如果未使用 PCoIP 安全网关）。  <b>注</b> 由于目标端口有所不同，请参阅此表格下面的注释。
View Agent/Horizon Agent	4172	View 连接服务器、安全服务器或 Unified Access Gateway 设备	55000	UDP	PCoIP（非 SALSA20）（如果使用 PCoIP 安全网关）。

**注** 代理用于 PCoIP 的 UDP 端口号可能会发生更改。如果正在使用端口 50002，代理将选择 50003。如果正在使用端口 50003，代理将选择 50004，依此类推。您必须使用 ANY 配置防火墙（表中列出星号 (\*) 的情况）。

**表 1-4. Horizon Client 使用的 TCP 和 UDP 端口**

源	端口	目标	端口	协议	说明
Horizon Client	*	View 连接服务器、安全服务器或 Unified Access Gateway 设备	443	TCP	用于登录 View 的 HTTPS。（在使用安全加密链路连接时此端口还用于转发）。  <b>注</b> Horizon Client 4.4 及更高版本支持 UDP 端口 443（见下文）。
Horizon Client 4.4 或更高版本	*	Unified Access Gateway 设备 2.9 或更高版本	443	UDP	如果使用 Blast 安全网关且已启用 UDP Tunnel Server，使用 HTTPS 登录 View。（在使用安全加密链路连接时此端口还用于转发）。
Unified Access Gateway 设备 2.9 或更高版本	443	Horizon Client 4.4 或更高版本	*	UDP	如果使用 Blast 安全网关且已启用 UDP Tunnel Server，使用 HTTPS 登录 View。（在使用安全加密链路连接时此端口还用于转发）。
Horizon Client	*	View Agent/ Horizon Agent	22443	TCP	HTML Access 和 VMware Blast Extreme（如果未使用 Blast 安全网关）。
Horizon Client	*	Horizon Agent	22443	UDP	VMware Blast Extreme（如果未使用 Blast 安全网关）。  <b>注</b> 不用于连接 Linux 桌面。
Horizon Agent	22443	Horizon Client	*	UDP	VMware Blast Extreme（如果未使用 Blast 安全网关）。  <b>注</b> 不用于连接 Linux 桌面。
Horizon Client	*	View Agent/ Horizon Agent	3389	TCP	指向 View 桌面的 Microsoft RDP 流量（如果使用直接连接而不是安全加密链路连接）。

源	端口	目标	端口	协议	说明
Horizon Client	*	View Agent/ Horizon Agent	9427	TCP	Windows Media MMR 重定向和客户端驱动器重定向（如果使用直接连接而不是安全加密链路连接）。  <b>注</b> 使用 VMware Blast Extreme 时无需进行 CDR。
Horizon Client	*	View Agent/ Horizon Agent	32111	TCP	USB 重定向和时区同步（如果使用直接连接而不是安全加密链路连接）。
Horizon Client	*	View Agent/ Horizon Agent	4172	TCP 和 UDP	PCoIP（如果未使用 PCoIP 安全网关）。  <b>注</b> 由于源端口有所不同，请参阅此表格下面的注释。
Horizon Client	*	View 连接服务器、安全服务器 或 Unified Access Gateway 设备	4172	TCP 和 UDP	PCoIP（非 SALSA20）（如果使用 PCoIP 安全网关）。  <b>注</b> 由于源端口有所不同，请参阅此表格下面的注释。
View Agent/Horizon Agent	4172	Horizon Client	*	UDP	PCoIP（如果未使用 PCoIP 安全网关）。  <b>注</b> 由于目标端口有所不同，请参阅此表格下面的注释。
安全服务器、View 连接 服务器或 Unified Access Gateway 设备	4172	Horizon Client	*	UDP	PCoIP（非 SALSA20）（如果使用 PCoIP 安全网关）。  <b>注</b> 由于目标端口有所不同，请参阅此表格下面的注释。
Horizon Client	*	View 连接服务器、安全服务器 或 Unified Access Gateway 设备	8443	TCP	HTML Access 和 VMware Blast Extreme（如果使用 Blast 安全网关）。
Horizon Client	*	View 连接服务器、安全服务器 或 Unified Access Gateway 设备	8443	UDP	VMware Blast Extreme（如果使用 Blast 安全网关）。  <b>注</b> 不用于连接 Linux 桌面。
View 连接服务器、安全 服务器或 Unified Access Gateway 设备	8443	Horizon Client	*	UDP	VMware Blast Extreme（如果使用 Blast 安全网关）。  <b>注</b> 不用于连接 Linux 桌面。

**注** 客户端用于 PCoIP 和 VMware Blast Extreme 的 UDP 端口号可能改变。如果正在使用端口 50002，客户端将选择 50003。如果正在使用端口 50003，客户端将选择 50004，依此类推。您必须使用 ANY 配置防火墙（表中列出星号 (\*) 的情况）。

## 安装的服务、守护程序和进程

在您运行客户端或代理安装程序时，会安装多个组件。

本章讨论了以下主题：

- [View Agent 或 Horizon Agent 安装程序在 Windows 计算机上安装的服务](#)
- [Windows 客户端上安装的服务](#)
- [在其他客户端和 Linux 桌面中安装的守护程序](#)

### View Agent 或 Horizon Agent 安装程序在 Windows 计算机上安装的服务

远程桌面和应用程序的运行取决于多项 Windows 服务。

**表 2-1. View Agent（对于 Horizon 6）或 Horizon Agent（对于 Horizon 7）服务**

服务名称	启动类型	说明
VMware Blast	自动	为 HTML Access 提供服务，以及使用 VMware Blast Extreme 协议连接到本地客户端。
VMware Horizon View Agent	自动	为 View Agent/Horizon Agent 提供服务。
VMware Horizon View Composer Guest Agent Server	自动	当此虚拟机属于 View Composer 链接克隆桌面池时提供服务。
VMware Horizon View Persona Management	自动（如果该功能已启用）；否则被禁用	为 VMware Persona Management 功能提供服务。
VMware Horizon View 脚本主机	已禁用	为运行启动会话脚本提供支持，在桌面会话开始前配置桌面安全策略（如有）。策略基于客户端设备和用户位置。
VMware Netlink Supervisor Service	自动	为了支持扫描仪重定向功能和串行端口重定向功能，为内核与用户空间进程之间的信息传输提供监控服务。
VMware Scanner Redirection Client Service	自动	（View Agent 6.0.2 和更高版本）为扫描仪重定向功能提供服务。
VMware Serial Com Client Service	自动	（View Agent 6.1.1 和更高版本）为串行端口重定向功能提供服务。
VMware Snapshot Provider	手动	为用于克隆的虚拟机快照提供服务。
VMware Tools	自动	为同步主机与客户机操作系统之间的对象提供支持，这可以提高虚拟机客户机操作系统的性能并增强虚拟机的管理功能。

服务名称	启动类型	说明
VMware USB Arbitration Service	自动	枚举连接到客户端的各种 USB 设备，确定哪些设备连接到客户端，哪些设备连接到远程桌面。
VMware View USB	自动	为 USB 重定向功能提供服务。

## Windows 客户端上安装的服务

Horizon Client 的运行取决于多项 Windows 服务。

**表 2-2. Horizon Client 服务**

服务名称	启动类型	说明
VMware Horizon Client	自动	提供 Horizon Client 服务。
VMware Netlink Supervisor Service	自动	为了支持扫描仪重定向功能和串行端口重定向功能，为内核与用户空间进程之间的信息传输提供监控服务。
VMware Scanner Redirection Client Service	自动	（Horizon Client 3.2 及更高版本）为扫描仪重定向功能提供服务。
VMware Serial Com Client Service	自动	（Horizon Client 3.4 及更高版本）为串行端口重定向功能提供服务。
VMware USB Arbitration Service	自动	枚举连接到客户端的各种 USB 设备，确定哪些设备连接到客户端，哪些设备连接到远程桌面。
VMware View USB	自动	为 USB 重定向功能提供服务。

**注** 在 Horizon Client 4.4 及更高版本中，该服务已被移除，而 USB 服务移动至 `vmware-remotemks.exe` 进程中。

## 在其他客户端和 Linux 桌面中安装的守护程序

出于安全目的，了解 Horizon Client 是否安装任何守护程序或进程很重要。

**表 2-3. 按客户端类型显示的、由 Horizon Client 安装的服务、进程或守护程序**

类型	服务、进程或守护程序
Linux 客户端	<ul style="list-style-type: none"> <li>■ <code>vmware-usbarbitrator</code>，它枚举连接到客户端的各种 USB 设备，并确定哪些设备连接到客户端，哪些设备连接到远程桌面。</li> <li>■ <code>vmware-view-used</code>，它为 USB 重定向功能提供服务。</li> </ul> <p><b>注</b> 如果您在安装过程中单击<b>安装后注册并启动服务</b>复选框，这些守护程序会自动启动。这些进程以 <code>root</code> 身份运行。</p>
Mac 客户端	Horizon Client 不会创建任何守护程序。
Chrome 客户端	Horizon Client 在一个 Android 进程中运行。Horizon Client 不会创建任何守护程序。
iOS 客户端	Horizon Client 不会创建任何守护程序。
Android 客户端	Horizon Client 在一个 Android 进程中运行。Horizon Client 不会创建任何守护程序。

类型	服务、进程或守护程序
Windows 应用商店客户端	Horizon Client 不会创建或触发任何系统服务。
Linux 桌面	<ul style="list-style-type: none"><li>■ StandaloneAgent，它以 root 特权运行，在 Linux 系统启动和运行时运行。StandaloneAgent 与 Horizon 连接服务器通信，以执行远程桌面会话管理（建立或停止会话、为连接服务器中的代理更新远程桌面状态）。</li><li>■ VMwareBlastServer，它由 StandaloneAgent 在接收到连接服务器的 StartSession 请求时启动。VMwareBlastServer 守护程序以 vmwblast（Linux Agent 安装时创建的系统帐户）特权运行。它通过内部 MKSControl 通道与 StandaloneAgent 通信，并使用 Blast 协议与 Horizon Client 通信。</li></ul>

# 要保护的资源

这些资源包括相关配置文件、密码和访问控制。

本章讨论了以下主题：

- 实施用于保护客户端系统的最佳做法
- 配置文件位置
- 帐户

## 实施用于保护客户端系统的最佳做法

请实施这些最佳做法来保护客户端系统。

- 确保客户端系统被配置为在空闲一定时间后进入睡眠状态，并在计算机被唤醒前要求用户输入密码。
- 要求用户在启动客户端系统时输入用户名和密码。不要将客户端系统配置为允许自动登录。
- 对于 Mac 客户端系统，请考虑为密钥串和用户帐户设置不同的密码。如果密码不同，用户会在系统为其输入任何密码前收到提示。另外还要考虑开启 FileVault 保护。

## 配置文件位置

必须保护的资源包括与安全性相关的配置文件。

表 3-1. 按客户端类型显示的配置文件位置

类型	目录路径
Linux 客户端	当 Horizon Client 启动时，配置设置将从多个位置按以下顺序进行处理： 1 /etc/vmware/view-default-config 2 ~/.vmware/view-preferences 3 /etc/vmware/view-mandatory-config 如果在多个位置都定义了某个设置，所采用的值是从最后的文件或命令行选项读取的值。
Windows 客户端	可能包含某些私人信息的用户设置位于以下文件中： C:\Users\user-name\AppData\Roaming\VMware\VMware Horizon View Client\prefs.txt

类型	目录路径
Mac 客户端	<p>在 Mac 客户端启动后生成了一些配置文件。</p> <ul style="list-style-type: none"> <li>■ <code>\$HOME/Library/Preferences/com.vmware.horizon.plist</code></li> <li>■ <code>\$HOME/Library/Preferences/com.vmware.vmr.plist</code></li> <li>■ <code>\$HOME/Library/Preferences/com.vmware.horizon.keyboard.plist</code></li> <li>■ <code>/Library/Preferences/com.vmware.horizon.plist</code></li> </ul>
Chrome 客户端	与安全性相关的设置位于用户界面中，而非配置文件中。配置文件对任何用户均不可见。
iOS 客户端	与安全性相关的设置位于用户界面中，而非配置文件中。配置文件对任何用户均不可见。
Android 客户端	与安全性相关的设置位于用户界面中，而非配置文件中。配置文件对任何用户均不可见。
Windows 应用商店客户端	与安全性相关的设置位于用户界面中，而非配置文件中。配置文件对任何用户均不可见。
View Agent 或 Horizon Agent（使用 Windows 操作系统的远程桌面）	与安全性相关设置仅位于 Windows 注册表中。
Linux 桌面	<p>您可以使用文本编辑器打开以下配置文件并指定与 SSL 相关的设置。</p> <p><code>/etc/vmware/viewagent-custom.conf</code></p>

## 帐户

客户端用户必须拥有 Active Directory 帐户。

### Horizon Client 用户帐户

在 Active Directory 中为有权访问远程桌面和应用程序的用户配置用户帐户。如果您打算使用 RDP 协议，用户帐户必须是远程桌面用户组的成员。

通常，最终用户不应是 Horizon 管理员。如果 Horizon 管理员需要验证用户体验，请创建并授权一个单独的测试帐户。在桌面上，Horizon 最终用户不应是特权组（例如管理员）成员，因为那样的话，他们就能修改锁定的配置文件和 Windows 注册表。

### 安装过程中创建的系统帐户

Horizon Client 应用程序不会在任何类型的客户端上创建任何服务用户帐户。对于适用于 Windows 的 Horizon Client 创建的服务，登录 ID 为 Local System。

在 Mac 客户端上，在首次启动时，用户必须授予本地管理员访问权限以启动 USB 和虚拟打印 (ThinPrint) 服务。在这些服务首次启动后，标准用户对它们便具有执行权限。同样地，在 Linux 客户端上，如果在安装过程中单击**安装后注册并启动服务**复选框，`vmware-usbarbitrator` 和 `vmware-view-used` 守护程序会自动启动。这些进程以 root 身份运行。

View Agent 或 Horizon Agent 不会在 Windows 桌面上创建任何服务用户帐户。在 Linux 桌面上，会创建一个系统帐户 `vmwblast`。在 Linux 桌面上，`StandaloneAgent` 守护程序以 root 特权运行，而 `VmwareBlastServer` 守护程序以 `vmwblast` 特权运行。

# 客户端和代理的安全性设置

可以通过多种客户端和代理设置调整配置的安全性。您可以通过使用组策略对象或编辑 Windows 注册表设置来访问远程桌面和 Windows 客户端的设置。

对于与日志收集有关的配置设置，请参阅第 6 章 [客户端和代理日志文件位置](#)。对于与安全协议和密码套件有关的配置设置，请参阅第 5 章 [配置安全协议和密码套件](#)。

本章讨论了以下主题：

- [配置证书检查](#)
- [Horizon Agent 配置模板中的安全性相关设置](#)
- [在 Linux 桌面上的配置文件中设置选项](#)
- [HTML Access 的组策略设置](#)
- [Horizon Client 配置模板中的安全性设置](#)
- [配置 Horizon Client 证书验证模式](#)
- [配置本地安全机构保护](#)

## 配置证书检查

管理员可以配置证书验证模式来实现一系列功能，例如始终执行完整验证。还可以配置是否允许最终用户在任意或部分服务器证书检查失败时选择是否拒绝客户端连接。

证书检查针对的是 View server 和 Horizon Client 之间的 SSL/TLS 连接。管理员可以配置验证模式来使用以下某个策略：

- 允许最终用户选择验证模式。该列表的其余部分介绍了三种验证模式。
- （不验证）不执行证书检查。
- （警告）如果自签名证书由服务器呈现，最终用户将收到警告。用户可以选择是否允许该类型的连接。
- （完整安全性）执行完整验证，并拒绝未通过完整验证的连接。

证书验证包括以下检查：

- 证书是否已被吊销？
- 除了验证发件人身份和加密服务器通信外，证书还有什么其他用途？也就是说，证书类型是否正确？
- 证书是否过期，还是仅在未来有效？也就是说，根据计算机时钟，证书是否有效？

- 证书上的公用名是否与发送它的服务器主机名称匹配？如果负载均衡器将 Horizon Client 重定向到使用与 Horizon Client 中输入的主机名不匹配的证书的服务器，会出现不匹配。可能出现不匹配的另一个原因是，您在客户端输入的是 IP 地址，而不是主机名。
- 证书是否由未知或不受信任的证书颁发机构 (CA) 签署？自签名证书是一种不受信任的 CA 类型。  
要通过这项检查，证书的信任链必须源于设备的本地证书存储区。

有关如何在特定类型客户端中配置证书检查的信息，请参阅适用于特定类型客户端的《使用 VMware Horizon Client》文档。这些文档可以从 Horizon Client 文档页面获取，网址为 [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs-archive.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs-archive.html)。这些文档还包含有关使用自签名证书的信息。

## Horizon Agent 配置模板中的安全性相关设置

Horizon Agent 的 ADMX 模板文件中提供了安全性相关设置。该 ADMX 模板文件名为 `vdm_agent.admx`。除非另作说明，上述设置中仅包含一项“计算机配置”设置。

安全性设置存储在客户机上的注册表 `HKLM\Software\VMware, Inc.\VMware VDM\Agent\Configuration` 中。

**表 4-1. View Agent（对于 Horizon 6）或 Horizon Agent（对于 Horizon 7）配置模板中的安全性相关设置**

设置	说明
AllowDirectRDP	<p>决定除 Horizon Client 设备之外的客户端是否可以使用 RDP 直接连接到远程桌面。如果禁用此设置，代理将只允许通过 Horizon Client 建立受 Horizon 管理的连接。</p> <p>从适用于 Mac 的 Horizon Client 中连接到远程桌面时，不要禁用 AllowDirectRDP 设置。如果禁用此设置，连接会失败并返回访问被拒绝错误。</p> <p>默认情况下，用户登录到 Horizon 7 桌面会话时，可以使用 RDP 从 Horizon 7 外部连接虚拟机。RDP 连接会终止 Horizon 7 桌面会话，并且用户未保存的数据和设置可能会丢失。关闭外部 RDP 连接后，用户才能登录到桌面。为避免这种情况，请禁用 AllowDirectRDP 设置。</p> <hr/> <p><b>重要事项</b> 必须在每个桌面的客户机操作系统上运行 Windows 远程桌面服务。您可以使用此设置防止用户通过 RDP 直接连接到其桌面。</p> <hr/> <p>默认情况下启用该设置。</p> <p>等效的 Windows 注册表值为 AllowDirectRDP。</p>
AllowSingleSignon	<p>确定是否通过单点登录 (SSO) 将用户连接到桌面和应用程序。启用该设置时，用户在登录到服务器时仅需要输入一次凭据。禁用该设置时，用户必须在进行远程连接时重新进行身份验证。</p> <p>默认情况下启用该设置。</p> <p>等效的 Windows 注册表值为 AllowSingleSignon。</p>
CommandsToRunOnConnect	<p>指定在会话首次连接时运行的一组命令或命令脚本。</p> <p>默认情况下未指定列表。</p> <p>等效的 Windows 注册表值为 CommandsToRunOnConnect。</p>
CommandsToRunOnDisconnect	<p>指定在会话断开连接时运行的一组命令或命令脚本。</p> <p>默认情况下未指定列表。</p> <p>等效的 Windows 注册表值为 CommandsToRunOnReconnect。</p>

设置	说明
CommandsToRunOnReconnect	指定在会话断开后重新连接时运行的一组命令或命令脚本。 默认情况下未指定列表。 等效的 Windows 注册表值为 CommandsToRunOnDisconnect。
ConnectionTicketTimeout	指定 Horizon 连接票证的有效时间（以秒为单位）。 连接代理时，Horizon Client 设备使用连接票证进行验证和单点登录。出于安全性原因，连接票证仅在有限时间内有效。当用户连接到远程桌面时，必须在连接票证超时或会话超时之前进行身份验证。如果未配置该设置，则使用默认超时时限 900 秒。 等效的 Windows 注册表值为 VdmConnectionTicketTimeout。
CredentialFilterExceptions	指定不允许加载代理 CredentialFilter 的可执行文件。文件名不得包含路径或后缀。使用分号分隔多个文件名。 默认情况下未指定列表。 等效的 Windows 注册表值为 CredentialFilterExceptions。

有关这些设置及其安全性影响的详细信息，请参阅《View 管理指南》文档。

## 在 Linux 桌面上的配置文件中设置选项

您可以向文件 `/etc/vmware/config` 或 `/etc/vmware/viewagent-custom.conf` 添加条目，以配置某些选项。

在 View Agent 或 Horizon Agent 的安装过程中，安装程序将两个配置模板文件 `config.template` 和 `viewagent-custom.conf.template` 复制到 `/etc/vmware` 中。此外，如果 `/etc/vmware/config` 和 `/etc/vmware/viewagent-custom.conf` 文件不存在，安装程序将 `config.template` 复制到 `config`，并将 `viewagent-custom.conf.template` 复制到 `viewagent-custom.conf`。在模板文件中会列出并记录所有配置选项。要设置某个选项，只需移除注释和更改相关值即可。

在进行配置更改后，重新引导 Linux 以使更改生效。

### `/etc/vmware/config` 中的配置选项

VMwareBlastServer 及其相关插件使用配置文件 `/etc/vmware/config`。

**注** 下表介绍了 Horizon Agent 配置文件中的各个代理强制执行的 USB 策略设置。Horizon Agent 使用这些设置确定是否能够将 USB 转发至主机。Horizon Agent 还会将这些设置传递到 Horizon Client，并根据您是指定合并 **(m)** 修改符以同时应用 Horizon Agent 筛选策略设置和 Horizon Client 筛选策略设置，还是覆盖 **(o)** 修改符以使用 Horizon Agent 筛选策略设置而不使用 Horizon Client 筛选策略设置来进行解释和执行。

**表 4-2. `/etc/vmware/config` 中的配置选项**

选项	值/格式	默认	说明
VVC.ScRedir.Enable	true 或 false	true	设置该选项以启用/禁用智能卡重定向。
VVC.logLevel	fatal error、warn、info、debug 或 trace	info	使用该选项设置 VVC 代理节点的日志级别。

选项	值/格式	默认	说明
VVC.RTAV.Enable	true 或 false	true	设置该选项以启用/禁用音频输入。
Clipboard.Direction	0, 1, 2, 或 3	2	<p>该选项确定剪贴板重定向策略。</p> <ul style="list-style-type: none"> <li>■ 0 - 禁用剪贴板重定向。</li> <li>■ 1 - 启用双向剪贴板重定向。</li> <li>■ 2 - 仅启用从客户端到远程桌面的剪贴板重定向。</li> <li>■ 3 - 仅启用从远程桌面到客户端的剪贴板重定向。</li> </ul>
cdrserver.logLevel	error、warn、info、debug、trace 或 verbose	info	使用该选项设置 <code>vmware-cdrserver.log</code> 的日志级别。
cdrserver.forcedByAdmin	true 或 false	false	设置该选项以禁止或允许客户端共享未通过 <code>cdrserver.shareFolders</code> 选项指定的其他文件夹。
cdrserver.sharedFolders	<i>file_path1,R; file_path2,; file_path3,R; . . .</i>	未定义	<p>指定客户端可与 Linux 桌面共享的一个或多个文件夹的文件路径。例如：</p> <ul style="list-style-type: none"> <li>■ 对于 Windows 客户端： <b>C:\spreadsheets,;D:\ebooks,R</b></li> <li>■ 对于非 Windows 客户端： <b>/tmp/spreadsheets,;/tmp/ebooks,;/home/finance,R</b></li> </ul>
cdrserver.permissions	R	RW	<p>使用该选项应用 Horizon Agent 对 Horizon Client 共享的文件夹具有的额外读取/写入权限。例如：</p> <ul style="list-style-type: none"> <li>■ 如果 Horizon Client 共享的文件夹具有 read 和 write 权限，而您设置了 <b>cdrserver.permissions=R</b>，则 Horizon Agent 只具有 read 访问权限。</li> <li>■ 如果 Horizon Client 共享的文件夹只具有 read 权限，而您设置了 <b>cdrserver.permissions=RW</b>，则 Horizon Agent 仍将只具有 read 访问权限。Horizon Agent 无法更改由 Horizon Client 设置的仅含 read 的属性。Horizon Agent 只能移除写入访问权限</li> </ul> <p>典型的用法包括：</p> <ul style="list-style-type: none"> <li>■ <b>cdrserver.permissions=R</b></li> <li>■ <b>#cdrserver.permissions=R</b>（即，将其注释掉或删除该条目）</li> </ul>
cdrserver.cacheEnable	true 或 false	true	设置该选项以启用或禁用从代理向客户端的写入缓存功能。
UsbRedirPlugin.log.logLevel	error、warn、info、debug、trace 或 verbose	info	使用该选项设置 USB 重定向插件的日志级别。
UsbRedirServer.log.logLevel	error、warn、info、debug、trace 或 verbose	info	使用该选项设置 USB 重定向服务器的日志级别。
viewusb.AllowAutoDeviceSplitting	<b>{m o}:</b> <b>{true false}</b>	未定义，等同于 false	<p>设置该选项以允许或禁止自动拆分复合 USB 设备。</p> <p>示例：<b>m:true</b></p>

选项	值/格式	默认	说明
viewusb.SplitExcludeVidPid	<b>{m o}:vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</b>	未定义	使用该选项按供应商和产品 ID 在拆分中排除或包含指定的复合 USB 设备。该设置的格式为 <b>vid-xxx1_pid-yyy1[;vid-xxx2_pid-yyy2;...]</b> 。您必须以十六进制格式指定 ID 号。可以使用通配符 (*) 代替 ID 中的单个数字。 示例: <b>m:vid-0f0f_pid-55**</b>
viewusb.SplitVidPid	<b>{m o}: vid-xxxx_pid-yyy([exintf:zz[;exintf:ww]])[;...]</b>	未定义	设置该选项以将由供应商和产品 ID 指定的复合 USB 设备的组件视为单独设备。该设置的格式为 <b>vid-xxxx_pid-yyy(exintf:zz[;exintf:ww])</b> 。可以使用 <b>exintf</b> 关键字通过指定组件的接口号从重定向中排除组件。您必须以十六进制格式指定 ID 号，以十进制格式（包含前导零）指定接口号。可以使用通配符 (*) 代替 ID 中的单个数字。 示例: <b>o:vid-0f0f_pid-*** (exintf-01);vid-0781_pid-554c(exintf:01;exintf:02)</b>  <b>注</b>  Horizon 不会自动包含您未明确排除的组件。您必须指定一个筛选策略（如 <b>Include VidPid Device</b> ）来包含这些组件。
viewusb.AllowAudioIn	<b>{m o}: {true false}</b>	未定义，等同于 true	使用该选项允许或禁止对音频输入设备进行重定向。示例: <b>o:false</b>
viewusb.AllowAudioOut	<b>{m o}: {true false}</b>	未定义，等同于 false	设置该选项以允许或禁止对音频输出设备进行重定向。
viewusb.AllowHIDBootable	<b>{m o}: {true false}</b>	未定义，等同于 true	使用该选项允许或禁止对引导时除键盘或鼠标之外的其他可用输入设备（又称为可引导的 HID 设备）进行重定向。
viewusb.AllowDevDescFailsafe	<b>{m o}: {true false}</b>	未定义，等同于 false	设置该选项以便即使在 Horizon Client 未能获取配置或设备描述符时，也允许或禁止对设备进行重定向。要在设备未能获取配置或设备描述符时也仍然允许对其进行重定向，可将该设备包含在 Include 筛选器中，例如 <b>IncludeVidPid</b> 或 <b>IncludePath</b> 。
viewusb.AllowKeyboardMouse	<b>{m o}: {true false}</b>	未定义，等同于 false	使用该选项允许或禁止对键盘以及集成指针设备（例如，鼠标、轨迹球或触摸板）进行重定向。
viewusb.AllowSmartcard	<b>{m o}: {true false}</b>	未定义，等同于 false	设置该选项以允许或禁止对智能卡设备进行重定向。
viewusb.AllowVideo	<b>{m o}: {true false}</b>	未定义，等同于 true	使用该选项允许或禁止对视频设备进行重定向。
viewusb.DisableRemoteConfig	<b>{m o}: {true false}</b>	未定义，等同于 false	设置该选项以禁止或允许在执行 USB 设备筛选时使用 Horizon Agent 设置。

选项	值/格式	默认	说明
viewusb.ExcludeAllDevices	{true false}	未定义，等同于 false	使用该选项在重定向中排除或包含所有 USB 设备。如果设置为 <b>true</b> ，可以使用其他策略设置来允许对特定设备或设备系列进行重定向。如果设置为 <b>false</b> ，可以使用其他策略设置来禁止对特定设备或设备系列进行重定向。如果将 Horizon Agent 上的 <b>ExcludeAllDevices</b> 的值设置为 <b>true</b> ，并将此设置传递到 Horizon Client，则 Horizon Agent 设置将覆盖 Horizon Client 设置。
viewusb.ExcludeFamily	{m o}: <i>family_name_1</i> ; <i>family_name_2</i> ; ...]	未定义	<p>使用该选项从重定向中排除设备系列。例如： <b>m:bluetooth;smart-card</b></p> <p>如果启用了自动设备拆分，Horizon 将检查复合 USB 设备的每个接口的设备系列以确定应排除哪些接口。如果禁用了自动设备拆分，Horizon 将检查整个复合 USB 设备的设备系列。</p> <p><b>注</b> 但是，默认情况下会从重定向中排除鼠标和键盘，因而不需要使用此设置来排除这些设备。</p>
viewusb.ExcludeVidPid	{m o}:vid-xxx1_ pid-yyy1[;vid- xxx2_pid- yyy2;...]	未定义	<p>设置该选项以从重定向中排除具有指定供应商和产品 ID 的设备。您必须以十六进制格式指定 ID 号。可以使用通配符 (*) 代替 ID 中的单个数字。</p> <p>例如: <b>o:vid-0781_pid-****;vid-0561_pid-554c</b></p>
viewusb.ExcludePath	{m o}:bus-x1[/ y1].../ port- z1[;bus-x2[/ y2].../port- z2;...]	未定义	<p>使用该选项从重定向中排除位于指定集线器或端口路径的设备。您必须以十六进制格式指定总线和端口号。在路径中不能使用通配符。</p> <p>例如： <b>m:bus-1/2/3_port- 02;bus-1/1/1/4_port-ff</b></p>
viewusb.IncludeFamily	{m  o}: <i>family_name_1</i> ; <i>family_name_2</i> ...	未定义	<p>设置该选项以包含可重定向的设备系列。</p> <p>例如: <b>o:storage; smart-card</b></p>
viewusb.IncludePath	{m o}:bus-x1[/ y1].../ port- z1[;bus-x2[/ y2].../ portz2;...]	未定义	<p>使用该选项包含位于指定集线器或端口路径的可重定向设备。您必须以十六进制格式指定总线和端口号。在路径中不能使用通配符。</p> <p>例如: <b>m:bus-1/2_port- 02;bus-1/7/1/4_port-0f</b></p>
viewusb.IncludeVidPid	{m o}:vid-xxx1_ pid-yyy1[;vid- xxx2_pid- yyy2;...]	未定义	<p>设置该选项以包含具有指定供应商和产品 ID 的可重定向设备。您必须以十六进制格式指定 ID 号。可以使用通配符 (*) 代替 ID 中的单个数字。</p> <p>例如: <b>o:vid-***_pid-0001;vid-0561_pid-554c</b></p>
mksVNCServer.useXExtButtonMapping	true 或 false	false	设置该选项以在 SLED 11 SP3 上启用或禁用左手鼠标支持。
mksvhan.clipboardSize	整数	1024	使用该选项指定用于复制和粘贴操作的剪贴板最大大小。
RemoteDisplay.maxBandwidthKbps	整数	4096000	指定 VMware Blast 会话的最大带宽，以千比特/秒 (kbps) 为单位。此带宽包括所有图像处理、音频、虚拟通道以及 VMware Blast 控制流量。最大值为 4 Gbps (4096000)。

选项	值/格式	默认	说明
RemoteDisplay.maxFPS	整数	60	指定屏幕更新的最大速率。使用此设置可管理用户占用的平均带宽。有效值应介于 3 和 60 之间。默认值为每秒更新 60 次。
RemoteDisplay.enableStats	true 或 false	false	启用或禁用 mks 日志中的 Blast 协议统计信息，例如带宽、FPS、RTT 等。
RemoteDisplay.allowH264	true 或 false	true	设置该选项以启用或禁用 H.264 编码。
vdpService.log.logLevel	fatal error、warn、info、debug 或 trace	info	使用该选项设置 vdpService 的日志级别。
RemoteDisplay.qpmaxH264	可用值范围：0-51	36	使用此选项可设置 H264minQP 量化参数，该参数用来为配置为使用 H.264 编码的远程显示指定最佳图像质量。应将该值设置为大于为 RemoteDisplay.qpminH264 设置的值。
RemoteDisplay.qpminH264	可用值范围：0-51	10	使用此选项可设置 H264maxQP 量化参数，该参数用来为配置为使用 H.264 编码的远程显示指定最低图像质量。应将该值设置为小于为 RemoteDisplay.qpmaxH264 设置的值。
RemoteDisplay.minQualityJPEG	可用值范围：1-100	25	指定使用 JPEG/PNG 编码时桌面显示的图像质量。低质量设置用于经常变化的屏幕区域，例如，发生滚动时。
RemoteDisplay.midQualityJPEG	可用值范围：1-100	35	指定使用 JPEG/PNG 编码时桌面显示的图像质量。用于设置桌面显示的中等质量设置。
RemoteDisplay.maxQualityJPEG	可用值范围：1-100	90	指定使用 JPEG/PNG 编码时桌面显示的图像质量。高质量设置用于较为静态的屏幕区域，从而产生更好的图像质量。

## /etc/vmware/viewagent-custom.conf 中的配置选项

Java Standalone Agent 使用配置文件 /etc/vmware/viewagent-custom.conf。

**表 4-3. /etc/vmware/viewagent-custom.conf 中的配置选项**

选项	值	默认	说明
Subnet	NULL 或采用 IP 地址/CIDR 格式的网络地址和掩码	NULL	<p>如果多个本地 IP 地址具有不同的子网，请使用该选项设置 Linux 代理为 View 连接服务器提供的子网。</p> <p>如果在 Linux 代理计算机上检测到多个子网配置，则需要使用该选项指定 Linux 代理应使用的正确子网。例如，如果在 Linux 计算机上安装了 Docker，则会将其作为虚拟网络适配器引入。要避免 Linux 代理将 Docker 作为虚拟网络适配器，您必须设置该选项以使用实际物理网络适配器。</p> <p>您必须指定 IP 地址/CIDR 格式的值。例如，Subnet=192.168.1.0/24。</p> <p>NULL 意味着 Linux 代理随机选择 IP 地址。</p>
SSOEnable	true 或 false	true	设置该选项以启用/禁用单点登录 (Single Sign-On, SSO)。

选项	值	默认	说明
SSOUserFormat	文本字符串	[username]	<p>使用该选项以指定用于单点登录的登录名称格式。默认值只包含用户名。如果还需要域名，请设置该选项。通常，登录名称是域名加上一个特殊字符，再加上用户名。如果特殊字符是反斜杠，则必须使用另一个反斜杠对其进行转义。登录名称格式示例：</p> <ul style="list-style-type: none"> <li>■ SSOUserFormat=[domain]\\[username]</li> <li>■ SSOUserFormat=[domain]+[username]</li> <li>■ SSOUserFormat=[username]@[domain]</li> </ul>
CDREnable	true 或 false	true	设置该选项以启用或禁用客户端驱动器重定向 (Client Drive Redirection, CDR) 功能。
USBEnable	true 或 false	true	设置该选项以启用或禁用 USB 重定向功能。
KeyboardLayoutSync	true 或 false	true	<p>使用该选项指定是否将客户端的系统区域设置列表和当前键盘布局与 Horizon Agent for Linux 桌面同步。</p> <p>启用或未配置此设置时，允许同步。禁用此设置时，不允许同步。</p> <p>只有适用于 Windows 的 Horizon Client 支持该功能，并且该功能仅适用于英语、法语、德语、日语、韩语、西班牙语、简体中文和繁体中文区域设置。</p>
StartBlastServerTime out	整数	20	该选项决定 VMwareBlastServer 进程初始化的时间长短（以秒为单位）。如果进程在此超时值内未准备就绪，用户登录将失败。
SSLCiphers	文本字符串	!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES	使用该选项以指定密码列表。您必须使用 <a href="https://www.openssl.org/docs/manmaster/man1/ciphers.html">https://www.openssl.org/docs/manmaster/man1/ciphers.html</a> 中定义的格式。
SSLProtocols	文本字符串	TLSv1_1:TLSv1_2	使用该选项以指定安全协议。支持的协议是 TLSv1.0、TLSv1.1 和 TLSv1.2。
SSLCipherServerPreference	true 或 false	true	使用该选项以启用或禁用选项 SSL_OP_CIPHER_SERVER_PREFERENCE。有关更多信息，请参阅 <a href="https://www.openssl.org/docs/manmaster/ssl/SSL_CTX_set_options.html">https://www.openssl.org/docs/manmaster/ssl/SSL_CTX_set_options.html</a> 。
UseGnomeFlashback	true 或 false	false	<p>该选项确定是否使用 GNOME Flashback (Metacity) 桌面环境（如果 Ubuntu 14.04 或 Ubuntu 16.04 系统中已安装该桌面）。无论 SSO 功能启用与否，该选项都会生效。</p> <p>将该选项设置为 TRUE 后，将会始终使用 GNOME Flashback (Metacity) 桌面环境，而不使用默认的桌面环境。</p> <p><b>提示</b> 要提升系统的性能，请在您的 Ubuntu 14.04 或 Ubuntu 16.04 系统中安装 GNOME Flashback (Metacity) 桌面后，配置 UseGnomeFlashback=TRUE。</p>

选项	值	默认	说明
LogCnt	整数	-1	使用该选项设置在 /tmp/vmware-root 中保留的日志文件数。 <ul style="list-style-type: none"> <li>■ -1 - 全部保留</li> <li>■ 0 - 全部删除</li> <li>■ &gt; 0 - 保留的日志计数。</li> </ul>
RunOnceScript			使用该选项以使克隆的虚拟机重新加入 AD。 设置在主机名发生更改后运行一次的脚本。指定的脚本仅在首次主机名更改后执行一次。在代理安装后，当代理服务启动并且主机名发生了更改时，该脚本会以 root 权限执行。 例如，对于 Winbind 解决方案，您必须通过 Winbind 使基础虚拟机加入 AD，并将该选项设置为一个脚本路径。这必须包含域重新加入命令 /usr/bin/net ads join -U <ADUserName>%<ADUserPassword>。在虚拟机克隆后，操作系统自定义将更改主机名。当代理服务启动时，将执行该脚本以使克隆的虚拟机加入 AD。
RunOnceScriptTimeout		120	使用此选项设置 RunOnceScript 选项的超时时间，以秒为单位。 例如，设置 RunOnceScriptTimeout=120

**注** VMwareBlastServer 进程有三个安全选项：SSLCiphers、SSLProtocols 和 SSLCipherServerPreference。在启动 VMwareBlastServer 进程时，Java Standalone Agent 将这些选项作为参数传递。启用 Blast 安全网关 (BSG) 时，这些选项会影响 BSG 和 Linux 桌面之间的连接。当 BSG 被禁用时，这些选项会影响客户端和 Linux 桌面之间的连接。

## HTML Access 的组策略设置

HTML Access 的组策略设置在模板文件中指定。ADMX 模板文件名为 vdm\_blast.admx。这些模板适用于 VMware Blast 显示协议，该协议是 HTML Access 使用的唯一显示协议。

对于 HTML Access 4.0 和 Horizon 7.0，《在 Horizon 7 中配置远程桌面功能》文档中的“VMware Blast 策略设置”描述了 VMware Blast 组策略设置。

如果您拥有 HTML Access 3.5 或更早版本和 Horizon 6.2.x 或更早版本，下表介绍了适用于 HTML Access 的组策略设置。Horizon 7.0 或更高版本提供更多 VMware Blast 组策略设置。

**表 4-4. HTML Access 3.5 和更早版本的组策略设置**

设置	说明
显示空白屏幕	控制在 HTML Access 会话期间是否可以从 Horizon 7 外部看到远程虚拟机。例如，管理员可以在用户通过 HTML Access 连接到桌面时使用 vSphere Web Client 在虚拟机中打开控制台。 当此设置启用或未配置时，若有人尝试在 HTML Access 会话活动期间从 Horizon 7 外部访问远程虚拟机，远程虚拟机会显示空白屏幕。
会话垃圾收集	控制对于已放弃远程会话的垃圾收集。当此设置启用时，您可以配置垃圾收集时间间隔和阈值。 时间间隔控制运行垃圾收集器的频度。时间间隔设置以毫秒为单位。 阈值决定已放弃的会话必须经过多长时间才可以列入删除候选。阈值设置以秒为单位。

设置	说明
配置剪贴板重定向	<p>确定允许执行剪贴板重定向的方向。只能复制和粘贴文本。您可以选择以下值之一：</p> <ul style="list-style-type: none"> <li>■ 仅启用从客户端到服务器（即仅允许从客户端系统向远程桌面执行复制和粘贴。）</li> <li>■ 禁用两个方向</li> <li>■ 启用两个方向</li> <li>■ 仅启用从服务器到客户端（即仅允许从远程桌面向客户端系统执行复制和粘贴。）</li> </ul> <p>该设置仅适用于 View Agent 或 Horizon Agent。</p> <p>如果此设置已禁用或未配置，默认值为仅启用服务器到客户端。</p>
HTTP 服务	<p>允许您更改 Blast Agent 服务的安全 (HTTPS) TCP 端口。默认端口为 22443。</p> <p>启用该设置可更改端口号。如果更改该设置，您还必须在受影响的远程桌面（安装了 View Agent 或 Horizon Agent）的防火墙上更新设置。</p>

## Horizon Client 配置模板中的安全性设置

Horizon Client 的 ADMX 模板文件的“安全性”部分和“脚本定义”部分中提供了安全性相关设置。该 ADMX 模板文件名为 `vdm_client.admx`。除非特别说明，上述设置中仅包含一项“计算机配置”设置。如果“用户配置”设置可用，而且您为它定义了一个值，它将覆盖等效的“计算机配置”设置。

下表介绍了 ADMX 模板文件的“安全性”部分中的设置。

**表 4-5. Horizon Client 配置模板：安全性设置**

设置	说明
Allow command line credentials (计算机配置设置)	<p>确定是否可以通过 Horizon Client 命令行选项提供用户凭据。如果禁用此设置，当用户从命令行运行 Horizon Client 时，<code>smartCardPIN</code> 和 <code>password</code> 选项不可用。</p> <p>默认情况下启用该设置。</p> <p>等效的 Windows 注册表值为 <code>AllowCmdLineCredentials</code>。</p>
Servers Trusted For Delegation (计算机配置设置)	<p>指定接受在用户选中以当前用户身份登录复选框时传送的用户身份和凭据信息的连接服务器实例。如果未指定任何连接服务器实例，则所有连接服务器实例都会接受该信息。</p> <p>要添加连接服务器实例，请使用以下格式之一：</p> <ul style="list-style-type: none"> <li>■ <code>domain\system\$</code></li> <li>■ <code>system\$@domain.com</code></li> <li>■ 连接服务器服务的服务主体名称 (Service Principal Name, SPN)。</li> </ul> <p>等效的 Windows 注册表值为 <code>BrokersTrustedForDelegation</code>。</p>

设置	说明
<b>Certificate verification mode</b> (计算机配置设置)	<p>配置 Horizon Client 执行的证书检查的级别。您可以选择其中一种模式：</p> <ul style="list-style-type: none"> <li>■ <b>No Security</b>。不检查证书。</li> <li>■ <b>Warn But Allow</b>。如果连接服务器主机提供自签名证书，将显示一条警告，但用户可以继续连接到连接服务器。证书名称不需要与用户在 Horizon Client 中提供的连接服务器名称匹配。如果发生任何其他证书错误状况，则会显示一个错误对话框，并禁止用户连接到连接服务器。<b>Warn But Allow</b> 为默认值。</li> <li>■ <b>Full Security</b>。如果出现任何类型的证书错误，则用户无法连接到连接服务器。用户将会看到证书错误。</li> </ul> <p>配置该组策略设置后，用户可以在 Horizon Client 中查看选定的证书验证模式，但无法配置该设置。<b>SSL</b> 配置对话框会通知用户：管理员已锁定该设置。</p> <p>未配置或禁用该设置时，Horizon Client 用户可以选择证书验证模式。</p> <p>如果您不希望将证书验证设置配置为组策略，您还可以通过修改 Windows 注册表设置来启用证书验证。</p>
<b>Default value of the 'Log in as current user' checkbox</b> (计算机和用户配置设置)	<p>指定 Horizon Client 连接对话框上的<b>以当前用户身份登录</b>复选框的默认值。</p> <p>这项设置将覆盖 Horizon Client 安装期间指定的默认值。</p> <p>如果用户通过命令行运行 Horizon Client 并指定了 <b>LogInAsCurrentUser</b> 选项，则该值将覆盖此设置。</p> <p>如果选中了<b>以当前用户身份登录</b>复选框，用户在登录到客户端系统时提供的身份和凭据信息将传送到连接服务器实例，并最终传送到远程桌面。如果取消选中该复选框，用户必须多次输入身份和凭据信息，才能访问远程桌面。</p> <p>默认情况下禁用此设置。</p> <p>等效的 Windows 注册表值为 <b>LogInAsCurrentUser</b>。</p>
<b>Display option to Log in as current user</b> (计算机和用户配置设置)	<p>确定<b>以当前用户身份登录</b>复选框是否显示在 Horizon Client 连接对话框上。</p> <p>如果显示该复选框，用户可选中或取消选中该复选框并覆盖其默认值。如果该复选框隐藏，用户将无法从 Horizon Client 连接对话框中覆盖其默认值。</p> <p>您可以通过 <b>Default value of the 'Log in as current user' checkbox</b> 策略设置指定<b>以当前用户身份登录</b>复选框的默认值。</p> <p>默认情况下启用该设置。</p> <p>等效的 Windows 注册表值为 <b>LogInAsCurrentUser_Display</b>。</p>
<b>Enable jump list integration</b> (计算机配置设置)	<p>确定在 Windows 7 和更高版本系统的任务栏上的 Horizon Client 图标中是否显示跳转列表。通过使用跳转列表，用户可以连接到最近使用的连接服务器实例和远程桌面。</p> <p>共享 Horizon Client 时，您可能不希望用户查看最近使用的桌面名称。因此，您可以通过禁用此设置来禁用跳转列表。</p> <p>默认情况下启用该设置。</p> <p>等效的 Windows 注册表值为 <b>EnableJumplist</b>。</p>
<b>Enable SSL encrypted framework channel</b> (计算机和用户配置设置)	<p>确定是否为 View 5.0 和更低版本桌面启用 SSL。在 View 5.0 之前，未加密通过端口 TCP 32111 发送到桌面的数据。</p> <ul style="list-style-type: none"> <li>■ <b>启用</b>：启用 SSL，但在远程桌面不支持 SSL 时允许回退到以前的未加密连接。例如，View 5.0 和更低版本桌面不支持 SSL。<b>启用</b>是默认设置。</li> <li>■ <b>禁用</b>：禁用 SSL。此设置不推荐使用，但调试时或通道未经过安全加密链路并可能由 WAN 加速器产品优化时可能很有用。</li> <li>■ <b>强制</b>：启用 SSL，并拒绝连接不支持 SSL 的桌面。</li> </ul> <p>等效的 Windows 注册表值为 <b>EnableTicketSSLAuth</b>。</p>

设置	说明
<b>Configures SSL protocols and cryptographic algorithms</b> (计算机和用户配置设置)	<p>在建立加密 SSL 连接之前，配置密码列表来限制某些加密算法和协议的使用。密码列表由以冒号分隔的一个或多个密码字符串组成。</p> <p><b>注</b> 所有密码字符串均区分大小写。</p> <ul style="list-style-type: none"> <li>■ Horizon Client 4.2 和更高版本的默认值为 <b>!aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES</b>。</li> <li>■ Horizon Client 4.0.1 和 4.1 的默认值为 <b>TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH</b>。</li> <li>■ Horizon Client 4.0 的默认值为 <b>TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH</b>。</li> <li>■ Horizon Client 3.5 的默认值为 <b>TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH</b>。</li> <li>■ Horizon Client 3.3 和 3.4 的默认值为 <b>TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH</b>。</li> <li>■ Horizon Client 3.2 和更低版本的值为 <b>SSLv3:TLSv1:TLSv1.1:AES:!aNULL:@STRENGTH</b>。</li> </ul> <p>这意味着在 Horizon Client 4.0.1 和 4.1 中，将启用 TLSv1.0、TLSv1.1 和 TLSv1.2。（将移除 SSL v2.0 和 v3.0。）如果不需要 TLSv1.0 与服务器兼容，则可以禁用 TLSv1.0。在 Horizon Client 4.0 中，将启用 TLS v1.1 和 TLS v1.2。（将禁用 TLS v1.0 并移除 SSL v2.0 和 v3.0。）在 Horizon Client 3.5 中，将启用 TLS v1.0、TLS v1.1 和 TLS v1.2。（将禁用 SSL v2.0 和 v3.0。）在 Horizon Client 3.3 和 3.4 中，将启用 TLS v1.0 和 TLS v1.1。（禁用了 SSL v2.0、SSL v3.0 和 TLS v1.2。）在 Horizon Client 3.2 和更低版本中，也将启用 SSL v3.0。（将禁用 SSL v2.0 和 TLS v1.2。）</p> <p>密码套件使用 128 位或 256 位 AES，移除匿名 DH 算法，然后按加密算法密钥长度的顺序排序当前密码列表。</p> <p>此配置的参考链接：<a href="http://www.openssl.org/docs/apps/ciphers.html">http://www.openssl.org/docs/apps/ciphers.html</a></p> <p>等效的 Windows 注册表值为 SSLCipherList。</p> <p>如果您不希望将该设置配置为组策略，您还可以通过将 SSLCipherList 值名称添加到客户端计算机上的以下注册表项之一来启用它。</p> <ul style="list-style-type: none"> <li>■ 对于 32 位 Windows: HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security</li> <li>■ 对于 64 位 Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security</li> </ul>
<b>Enable Single Sign-On for smart card authentication</b> (计算机配置设置)	<p>确定是否为智能卡身份验证启用单点登录。如果启用了单点登录，Horizon Client 将加密的智能卡 PIN 存储到临时内存中，然后再将其提交到连接服务器。如果禁用单点登录，Horizon Client 将不显示自定义 PIN 对话框。</p> <p>等效的 Windows 注册表值为 EnableSmartCardSSO。</p>
<b>Ignore bad SSL certificate date received from the server</b> (计算机配置设置)	<p>（仅限 View 4.6 和更低版本）确定是否忽略与无效的服务器证书日期关联的错误。在服务器发送过期证书时会发生这些错误。</p> <p>等效的 Windows 注册表值为 IgnoreCertDateInvalid。</p>
<b>Ignore certificate revocation problems</b> (计算机配置设置)	<p>（仅限 View 4.6 和更低版本）确定是否忽略与撤销的服务器证书关联的错误。当服务器发出一个已撤销的证书以及客户端无法验证证书的撤销状态时，会出现这种错误。</p> <p>默认情况下禁用此设置。</p> <p>等效的 Windows 注册表值为 IgnoreRevocation。</p>
<b>Ignore incorrect SSL certificate common name (host name field)</b> (计算机配置设置)	<p>（仅限 View 4.6 和更低版本）确定是否忽略与错误的服务器证书公用名关联的错误。在证书上的公用名与发送该证书的服务器主机名不匹配时会发生这些错误。</p> <p>等效的 Windows 注册表值为 IgnoreCertCnInvalid。</p>

设置	说明
Ignore incorrect usage problems (计算机配置设置)	(仅限 View 4.6 和更低版本) 确定是否忽略与服务器证书使用不当关联的错误。如果服务器发送的证书专用于某一用途，而不是用来验证发送者的身份和对服务器通信进行加密，则会发生这些错误。 等效的 Windows 注册表值为 IgnoreWrongUsage。
Ignore unknown certificate authority problems (计算机配置设置)	(仅限 View 4.6 和更低版本) 确定是否忽略与未知的服务器证书的证书颁发机构 (Certificate Authority, CA) 关联的错误。如果服务器发送的证书是由不受信任的第三方证书颁发机构签发的，则会发生这些错误。 等效的 Windows 注册表值为 IgnoreUnknownCa。

下表介绍了 ADMX 模板文件的“脚本定义”部分中的设置。

**表 4-6. 脚本定义部分中的安全性相关设置**

设置	说明
Connect all USB devices to the desktop on launch	确定桌面启动时是否将客户端系统中所有可用的 USB 设备都连接到桌面。 默认情况下禁用此设置。 等效的 Windows 注册表值为 connectUSB0nStartup。
Connect all USB devices to the desktop when they are plugged in	确定将 USB 设备插入客户端系统时是否将其都连接到桌面。 默认情况下禁用此设置。 等效的 Windows 注册表值为 connectUSB0nInsert。
Lagon Password	指定 Horizon Client 在登录过程中使用的密码。该密码由 Active Directory 存储在纯文本中。 默认情况下未定义此设置。 等效的 Windows 注册表值为 Password。

有关这些设置及其安全性影响的更多信息，请参阅《使用适用于 Windows 的 VMware Horizon Client》文档。

## 配置 Horizon Client 证书验证模式

您可以通过向 Windows 客户端计算机上的某个注册表项添加 CertCheckMode 值名称来配置 Horizon Client 证书验证模式。

在 32 位 Windows 系统上，该注册表项为 HKEY\_LOCAL\_MACHINE\Software\VMware, Inc.\VMware VDM\Client\Security。在 64 位 Windows 系统上，该注册表项为 HKLM\SOFTWARE\Wow6432Node\VMware, Inc.\VMware VDM\Client\Security。

对于该注册表项，使用以下值之一：

- 0 - 实施不验证服务器身份证书选项。
- 1 - 实施在连接到不受信任的服务器之前发出警告选项。
- 2 - 实施不要连接到不受信任的服务器选项。

您也可以通过配置证书验证模式组策略设置来配置 Horizon Client 证书验证模式。如果您在注册表项中配置了组策略设置和 CertCheckMode 设置，组策略设置优先于注册表项值。

配置组策略设置或注册表设置后，用户可以在 **Horizon Client** 中查看选定的证书验证模式，但无法配置该设置。

有关配置证书验证模式组策略设置的信息，请参阅 [Horizon Client 配置模板中的安全性设置](#)。

## 配置本地安全机构保护

Horizon Client 和 Horizon Agent 支持本地安全机构 (Local Security Authority, LSA) 保护。LSA 保护可防止其凭据不受保护的用户读取内存和注入代码。

有关配置 LSA 保护的更多信息，请参阅 [Microsoft Windows Server 文档](#)。

为 Horizon Client 4.4 及更低版本配置 LSA 保护后，以下功能将无法使用：

- 以当前用户身份登录

为 Horizon 7 版本 7.2 之前的 Horizon Agent 版本配置 LSA 保护后，以下功能将无法使用：

- 智能卡身份验证
- True SSO

## 配置安全协议和密码套件

您可以配置在 Horizon Client、View Agent/Horizon Agent 和 View Server 组件之间接受和建议使用的安全协议和密码套件。

本章讨论了以下主题：

- [安全协议和密码套件的默认策略](#)
- [为特定客户端类型配置安全协议和密码套件](#)
- [在 SSL/TLS 中禁用弱密码](#)
- [为 HTML Access Agent 配置安全协议和密码套件](#)
- [在 View 桌面上配置建议策略](#)

### 安全协议和密码套件的默认策略

默认情况下，全球接受和建议策略启用某些安全协议和密码套件。

下表列出了在 Windows、Linux、Mac、iOS、Android 和 Chrome 客户端系统上默认为 Horizon Client 4.4、4.3、4.2、4.1、4.0.1、4.0 和 3.x 启用的协议和密码套件。在适用于 Windows、Linux 和 Mac 的 Horizon Client 3.1（和更高版本）中，这些密码套件和协议还用于加密 USB 通道（USB 服务守护程序与 View Agent 或 Horizon Agent 之间的通信）。对于 Horizon Client 4.0 之前的版本，在连接到远程桌面时，USB 服务守护程序将 RC4（:RC4-SHA: +RC4）添加到密码控制字符串的末尾。从 Horizon Client 4.0 开始，不再添加 RC4。

### Horizon Client 4.2

---

**注** 从 Horizon Client 4.2 到 Horizon Client 4.4 无任何更改。

---

表 5-1. Horizon Client 4.2 上默认启用的安全协议和密码套件

默认安全协议	默认密码套件
TLS 1.2	<ul style="list-style-type: none"> <li>■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)</li> <li>■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)</li> <li>■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>
■ TLS 1.1	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
■ TLS 1.0	<ul style="list-style-type: none"> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>

默认情况下将启用 TLS 1.0，以确保 Horizon Client 可以默认连接到 VMware Horizon Air 服务器。默认密码字符串为 !aNULL:kECDH+AESGCM:ECDH+AESGCM:RSA+AESGCM:kECDH+AES:ECDH+AES:RSA+AES。如果不需要 TLS 1.0 与服务器兼容，则可以禁用 TLS 1.0。

## Horizon Client 4.0.1 和 4.1

表 5-2. Horizon Client 4.0.1 和 4.1 上默认启用的安全协议和密码套件

默认安全协议	默认密码套件
TLS 1.2	<ul style="list-style-type: none"> <li>■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>
<ul style="list-style-type: none"> <li>■ TLS 1.1</li> <li>■ TLS 1.0</li> </ul>	<ul style="list-style-type: none"> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>

默认情况下将启用 TLS 1.0，以确保 Horizon Client 可以默认连接到 VMware Horizon Air 服务器。默认密码字符串是 TLSv1:TLSv1.1:TLSv1.2:!aNULL:kECDH+AES:ECDH+AES:RSA+AES:@STRENGTH。如果不需要 TLS 1.0 与服务器兼容，则可以禁用 TLS 1.0。

## Horizon Client 4.0

表 5-3. Horizon Client 4.0 上默认启用的安全协议和密码套件

默认安全协议	默认密码套件
TLS 1.2	<ul style="list-style-type: none"> <li>■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>
■ TLS 1.1	<ul style="list-style-type: none"> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>

---

**重要事项** 将默认禁用 TLS 1.0。已移除 SSL 3.0。

---

## Horizon Client 3.5

表 5-4. Horizon Client 3.5 上默认启用的安全协议和密码套件

默认安全协议	默认密码套件
TLS 1.2	<ul style="list-style-type: none"> <li>■ TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)</li> <li>■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>
■ TLS 1.1	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
■ TLS 1.0	<ul style="list-style-type: none"> <li>■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)</li> <li>■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)</li> <li>■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)</li> <li>■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)</li> <li>■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)</li> </ul>

## Horizon Client 3.3 和 3.4

表 5-5. Horizon Client 3.3 和 3.4 上默认启用的安全协议和密码套件

默认安全协议	默认密码套件
■ TLS 1.1	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
■ TLS 1.0	■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
	■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
	■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
	■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
	■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
	■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
	■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

**注** 还支持 TLS 1.2，但它在默认情况下未被启用。要启用 TLS 1.2，请按照 [VMware 知识库文章 2121183](#) 中的说明操作。在这之后，支持表 5-4. [Horizon Client 3.5 上默认启用的安全协议和密码套件](#) 中列出的密码套件。

## Horizon Client 3.0、3.1 和 3.2

表 5-6. Horizon Client 3.0、3.1 和 3.2 上默认启用的安全协议和密码套件

默认安全协议	默认密码套件
■ TLS 1.1	■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
■ TLS 1.0	■ TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
■ SSL 3.0（仅在 Windows 客户端上启用）	■ TLS_SRP_SHA_DSS_WITH_AES_256_CBC_SHA (0xc022)
	■ TLS_SRP_SHA_RSA_WITH_AES_256_CBC_SHA (0xc021)
	■ TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
	■ TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
	■ TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
	■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
	■ TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
	■ TLS_SRP_SHA_DSS_WITH_AES_128_CBC_SHA (0xc01f)
	■ TLS_SRP_SHA_RSA_WITH_AES_128_CBC_SHA (0xc01e)
	■ TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
	■ TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
	■ TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
	■ TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

**注** 还支持 TLS 1.2，但它在默认情况下未被启用。要启用 TLS 1.2，请按照 [VMware 知识库文章 2121183](#) 中的说明操作。在这之后，支持表 5-4. [Horizon Client 3.5 上默认启用的安全协议和密码套件](#) 中列出的密码套件。

## 为特定客户端类型配置安全协议和密码套件

每种类型的客户端使用各自的方法配置协议和密码套件。

仅当 View server 不支持当前设置时，才应在 Horizon Client 中更改安全协议。如果为 Horizon Client 配置的安全协议未在客户端连接的 View Server 上启用，则会发生 TLS/SSL 错误，并且连接将失败。

要更改协议和密码的默认值，请使用特定于客户端的机制：

- 在 Windows 客户端系统中，您可以使用组策略设置或 Windows 注册表设置。有关信息，请参阅《使用适用于 Windows 的 VMware Horizon Client》文档。
- 在 Linux 客户端系统中，您可以使用配置文件属性或命令行选项。有关信息，请参阅《使用适用于 Linux 的 VMware Horizon Client》文档。
- 在 Mac 客户端系统上，您可以在 Horizon Client 中使用首选项设置。有关信息，请参阅《使用适用于 Mac 的 VMware Horizon Client》文档。
- 在 iOS、Android 和 Chrome OS 客户端系统上，您可以在 Horizon Client 设置中使用高级 SSL 选项设置。有关信息，请参阅适用的文档：《使用适用于 iOS 的 VMware Horizon Client》、《使用适用于 Android 的 VMware Horizon Client》或《使用适用于 Chrome OS 的 VMware Horizon Client》。

这些文档可以从 Horizon Client 文档页面获取，网址为 [https://www.vmware.com/support/viewclients/doc/viewclients\\_pubs-archive.html](https://www.vmware.com/support/viewclients/doc/viewclients_pubs-archive.html)。

## 在 SSL/TLS 中禁用弱密码

为了提高安全性，您可以配置域策略 GPO（组策略对象），以确保运行 View Agent 或 Horizon Agent 的基于 Windows 的计算机在使用 SSL/TLS 协议进行通信时不会使用弱密码。

### 步骤

- 1 在 Active Directory 服务器上编辑 GPO，方法是选择开始 > 管理工具 > 组策略管理，右键单击 GPO，然后选择编辑。
- 2 在组策略管理编辑器中，浏览到计算机配置 > 策略 > 管理模板 > 网络 > SSL 配置设置。
- 3 双击 **SSL 密码套件顺序**。
- 4 在“SSL 密码套件顺序”窗口中，单击已启用。
- 5 在“选项”窗格中，将“SSL 密码套件”文本框的全部内容替换为以下密码列表：

```
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA
```

为了便于查看，密码套件已分多行列在上方。将该列表粘贴到文本框中时，密码套件必须位于一行中，并且逗号后不含空格。

6 退出组策略管理编辑器。

7 重新启动 View Agent 或 Horizon Agent 计算机以使新的组策略生效。

## 为 HTML Access Agent 配置安全协议和密码套件

从 View Agent 6.2 开始，您可以通过编辑 Windows 注册表来配置 HTML Access Agent 使用的密码套件。从 View Agent 6.2.1 开始，您还可以配置使用的安全协议。您也可以在组策略对象 (GPO) 中指定这些配置。

对于 View Agent 6.2.1 及更高版本，默认情况下，此 HTML Access Agent 仅使用 TLS 1.1 和 TLS 1.2。允许使用的协议是 TLS 1.0、TLS 1.1 和 TLS 1.2（从低到高排序）。绝不允许使用 SSLv3 和更低版本的旧协议。SslProtocolLow 和 SslProtocolHigh 这两个注册表值决定 HTML Access Agent 将接受的协议范围。例如，设置 SslProtocolLow=tls\_1.0 和 SslProtocolHigh=tls\_1.2 将导致 HTML Access Agent 接受 TLS 1.0、TLS 1.1 和 TLS 1.2。默认设置是 SslProtocolLow=tls\_1.1 和 SslProtocolHigh=tls\_1.2。

您必须使用在 <https://www.openssl.org/docs/manmaster/man1/ciphers.html> 中的“密码列表格式”部分下定义的格式来指定密码列表。以下是默认密码列表：

```
ECDHE-RSA-AES256-SHA:AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

### 步骤

1 启动 Windows 注册表编辑器。

2 导航到 HKEY\_LOCAL\_MACHINE\SOFTWARE\VMware, Inc.\VMware Blast\Config 注册表项。

3 添加两个新的字符串 (REG\_SZ) 值 SslProtocolLow 和 SslProtocolHigh，用于指定协议范围。

这些注册表值的数据必须是 tls\_1.0、tls\_1.1 或 tls\_1.2。要仅启用一个协议，请为两个注册表值指定相同的协议。如果两个注册表值中任何一个值不存在，或者它的数据未设置为以上三个协议中的一个，则将使用默认协议。

4 添加一个新的字符串 (REG\_SZ) 值 SslCiphers，用于指定密码套件列表。

在注册表值的数据字段中键入或粘贴密码套件列表。例如，

```
ECDHE-RSA-AES256-SHA:HIGH:!AESGCM:!CAMELLIA:!3DES:!EDH:!EXPORT:!MD5:!PSK:!RC4:!SRP:!aNULL:!eNULL
```

5 重新启动 Windows 服务 VMware Blast。

要恢复为使用默认密码列表，请删除 SslCiphers 注册表值并重新启动 Windows 服务 VMware Blast。请勿简单地删除值的数据部分，因为这样 HTML Access Agent 会依据 OpenSSL 密码列表格式定义将所有密码视为不可接受。

HTML Access Agent 启动时，会将协议和密码信息写入其日志文件。您可以通过检查此日志文件来确定有效的值。

随着 VMware 不断改进网络安全方面的最佳实践，默认的安全协议和密码套件在将来可能还会变更。

## 在 View 桌面上配置建议策略

您可以在运行 Windows 的 View 桌面上配置建议策略，以控制到 View 连接服务器的消息总线连接的安全性。

确保将 View 连接服务器配置为接受相同的策略以避免连接失败。

### 步骤

- 1 在 View 桌面上启动 Windows 注册表编辑器。
- 2 导航到 HKEY\_LOCAL\_MACHINE\Software\VMware, Inc.\VMware VDM\Agent\Configuration 注册表项。
- 3 添加新的字符串 (REG\_SZ) 值 ClientSSLSecureProtocols。
- 4 将该值设置为一组密码套件，格式为：\LIST:protocol\_1,protocol\_2,...。

列出协议，先列出最新的协议。例如：

```
\LIST:TLSv1.2,TLSv1.1,TLSv1
```

- 5 添加新的字符串 (REG\_SZ) 值 ClientSSLCipherSuites。
- 6 将该值设置为一组密码套件，格式为：\LIST:cipher\_suite\_1,cipher\_suite\_2,...。

该列表应按优先顺序排列，先列出最优先的密码套件。例如：

```
\LIST:TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

## 客户端和代理日志文件位置

客户端和代理会创建日志文件，用于记录其组件的安装和运行情况。

本章讨论了以下主题：

- 适用于 Windows 的 Horizon Client 日志
- 适用于 Mac 的 Horizon Client 日志
- 适用于 Linux 的 Horizon Client 日志
- 移动设备上的 Horizon Client 日志
- Windows 计算机的 Horizon Agent 日志
- Linux 桌面日志

### 适用于 Windows 的 Horizon Client 日志

日志文件可以帮助排除安装、显示协议和各种功能组件方面的问题。您可以使用组策略设置配置某些日志文件的位置、详细级别和保留期限。

#### 日志位置

对于下表中的文件名，*YYYY* 表示年份，*MM* 表示月份，*DD* 表示日期，*XXXXXX* 为编号。

**表 6-1. 适用于 Windows 的 Horizon Client 日志文件**

日志类型	目录路径	文件名
安装	C:\Users\%username%\AppData\Local\Temp	vminst.log_XXXXXX_XXXXXX.txt vmmsi.log_XXXXXX_XXXXXX.txt
PCoIP 客户端 来自 vmware-remotemks.exe 进程	C:\Users\%username%\AppData\Local\Temp	pcoip_client_YYYY_MM_DD_XXXXXX.txt  <b>注</b> 您可以使用 GPO 配置从 0 至 3（最详细）的日志详细级别。请使用 View PCoIP 客户端会话变量 ADMX 模板文件 (pcoip.admx)。此设置的名称为 <b>配置 PCoIP 事件日志详细级别</b> 。
Horizon Client UI 来自 vmware-view.exe 进程	C:\Users\%username%\AppData\Local\VMware\VDM\Logs	vmware-horizon-viewclient-YYYY-MM-DD-XXXXXX.txt  <b>注</b> 您可以使用 GPO 配置日志位置。请使用 View 公共配置 ADMX 模板文件 vdm_common.admx。

日志类型	目录路径	文件名
Horizon Client 日志 来自 vmware-view.exe 进程	C:\Users\%username%\AppData\Local\Temp\vmware-username-XXXXXX	vmware-crtbora-XXXXXX.log
消息框架	C:\Users\%username%\AppData\Local\VMware\VDM\Logs	log-YYYY-MM-DD-XXXXXX.txt debug-YYYY-MM-DD-XXXXXX.txt
远程 MKS（鼠标、键盘、屏幕）日志 来自 vmware-remotemks.exe 进程	C:\Users\%username%\AppData\Local\Temp\vmware-username	ViewMP-Client-XXXXXX.log vmware-mks-XXXXXX.log vmware-rdeSvc-XXXXXX.log vmware-vvaClient-XXXXXX.log
Tsdr 客户端 来自 vmware-remotemks.exe 进程	C:\Users\%username%\AppData\Local\Temp\vmware-username	vmware-ViewTsdr-Client-XXXXXX.log
Tsmmr 客户端 来自 vmware-remotemks.exe 进程	C:\Users\%username%\AppData\Local\Temp\vmware-username	vmware-ViewTsmmr-Client-XXXXXX.log
VdpService 客户端 来自 vmware-remotemks.exe 进程	C:\Users\%username%\AppData\Local\Temp\vmware-username	vmware-vdpServiceClient-XXXXXX.log
WSNM 服务 来自 wsnm.exe 进程	C:\ProgramData\VMware\VDM\logs	debug-yyyy-mm-dd-XXXXXX.txt  <b>注</b> 您可以使用 GPO 配置日志位置。请使用 View 公共配置 ADMX 模板文件 vdm_common.admx。
USB 重定向 来自 vmware-view-usbd.exe 或 vmware-remotemks.exe 进程	C:\ProgramData\VMware\VDM\logs	debug-yyyy-mm-dd-XXXXXX.txt  在 Horizon Client 4.4 及更高版本中，vmware-view-usbd.exe 进程已被移除，而 USB 进程移动至 vmware-remotemks.exe 进程中。  <b>注</b> 您可以使用 GPO 配置日志位置。请使用 View 公共配置 ADMX 模板文件 vdm_common.admx。
串行端口重定向 来自 vmwsprrdpwks.exe 进程	C:\ProgramData\VMware\VDM\Logs	Serial*.txt Netlink*.txt
扫描仪重定向 来自 ftscanmgr.exe 进程	C:\ProgramData\VMware\VDM\Logs	Scanner*.txt Netlink*.txt

## 日志配置

您可以使用组策略设置进行一些配置更改：

- 对于 PCoIP 客户端日志，您可以配置从 0 至 3（最详细）的日志详细级别。请使用 View PCoIP 客户端会话变量 ADMX 模板文件 (pcoip.admx)。此设置的名称为**配置 PCoIP 事件日志详细级别**。
- 对于客户端 UI 日志，配置日志位置、详细级别和保留策略。请使用 View 公共配置 ADMX 模板文件 vdm\_common.admx。

- 对于 USB 重定向日志，配置日志位置、详细级别和保留策略。请使用 View 公共配置 ADMX 模板文件 `vdm_common.admx`。
- 对于 WSNM 服务日志，配置日志位置、详细级别和保留策略。请使用 View 公共配置 ADMX 模板文件 `vdm_common.admx`。

您也可以使用命令行命令设置详细级别。导航至 `C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT` 目录并输入以下命令：

```
support.bat loglevels
```

将显示新的命令提示符窗口，提示您选择一种详细级别。

## 收集日志包

您可以使用客户端 UI 或命令行命令将日志收集到 .zip 文件中，然后可将该文件发送至 VMware 技术支持部门。

- 在 **Horizon Client** 窗口中，从“选项”菜单中选择**支持信息**，然后在出现的对话框中单击**收集支持数据**。
- 从命令行导航至 `C:\Program Files (x86)\VMware\VMware Horizon View Client\DCT` 目录并输入以下命令：`support.bat`。

## 适用于 Mac 的 Horizon Client 日志

日志文件可以帮助排除安装、显示协议和各种功能组件方面的问题。您可以通过创建配置文件来配置详细级别。

### 日志位置

**表 6-2. 适用于 Mac 的 Horizon Client 日志文件**

日志类型	目录路径	文件名
Horizon Client UI	~/Library/Logs/VMware Horizon Client	
PCoIP 客户端	~/Library/Logs/VMware Horizon Client	
实时音频-视频	~/Library/Logs/VMware	vmware-RTAV-pid.log
USB 重定向	~/Library/Logs/VMware	
VChan	~/Library/Logs/VMware Horizon Client	
远程 MKS（鼠标、键盘、屏幕）日志	~/Library/Logs/VMware	
Crtbora	~/Library/Logs/VMware	

## 日志配置

在 Horizon Client 3.1 和更高版本中，Horizon Client 将在 Mac 客户端的 `~/Library/Logs/VMware Horizon Client` 目录下生成日志文件。管理员通过设置 Mac 客户端的 `/Library/Preferences/com.vmware.horizon.plist` 文件中的项，可以配置日志文件的最大数量和保留日志文件的最大天数。

**表 6-3. 日志文件收集的属性列表项**

项	说明
MaxDebugLogs	日志文件的最大数目。最大值为 100。
MaxDaysToKeepLogs	保留日志文件的最大天数。对该值没有限制。

当您启动 Horizon Client 时，将删除与这些条件不匹配的文件。

如果 MaxDebugLogs 或 MaxDaysToKeepLogs 项未在 `com.vmware.horizon.plist` 文件中设置，则日志文件的默认数量为 5，保留日志文件的默认天数为 7。

## 适用于 Linux 的 Horizon Client 日志

日志文件可以帮助排除安装、显示协议和各种功能组件方面的问题。您可以通过创建配置文件来配置详细级别。

### 日志位置

**表 6-4. 适用于 Linux 的 Horizon Client 日志文件**

日志类型	目录路径	文件名
安装	<code>/tmp/vmware-root/</code>	<code>.vmware-installer-pid.log</code> <code>vmware-vmis-pid.log</code>
Horizon Client UI	<code>/tmp/vmware-username/</code>	<code>vmware-horizon-client-pid.log</code>
PCoIP 客户端	<code>/tmp/teradici-username/</code>	<code>pcoip_client_YYYY_MM_DD_XXXXXX.log</code>
实时音频-视频	<code>/tmp/vmware-username/</code>	<code>vmware-RTAV-pid.log</code>
USB 重定向	<code>/tmp/vmware-root/</code>	<code>vmware-usbarb-pid.log</code> <code>vmware-view-usbd-pid.log</code>
VChan	<code>/tmp/vmware-username/</code>	<code>VChan-Client.log</code>
<b>注</b> 在设置 “ <code>export VMW_RDPVC_BRIDGE_LOG_ENABLED=1</code> ”后启用 RDPVCBridge 日志时，会创建此日志。		
远程 MKS（鼠标、键盘、屏幕）日志	<code>/tmp/vmware-username/</code>	<code>vmware-mks-pid.log</code> <code>vmware-MKSVchanClient-pid.log</code> <code>vmware-rdeSvc-pid.log</code>
VdpService 客户端	<code>/tmp/vmware-username/</code>	<code>vmware-vdpServiceClient-pid.log</code>
Tsdr 客户端	<code>/tmp/vmware-username/</code>	<code>vmware-ViewTsdr-Client-pid.log</code>

## 日志配置

您可以使用配置属性 (`view.defaultLogLevel`)，将客户端日志详细级别设置为 0（收集所有事件）至 6（仅收集重大事件）。

对于特定于 USB 的日志，您可以使用以下命令行命令：

```
vmware-usbarbitrator --verbose  
vmware-view-usbd -o log:trace
```

## 收集日志包

日志收集器位于 `/usr/bin/vmware-view-log-collector`。要使用日志收集器，您必须具有执行权限。您可以通过在 Linux 命令行输入以下命令来设置权限：

```
chmod +x /usr/bin/vmware-view-log-collector
```

您可以通过在 Linux 命令行输入以下命令来运行日志收集器：

```
/usr/bin/vmware-view-log-collector
```

## 移动设备上的 Horizon Client 日志

在移动设备上，您可能需要安装第三程序，以导航至日志文件的存储目录。移动客户端提供了将日志包发送至 VMware 的配置设置。由于日志记录可能影响性能，您只应在需要排除问题时启用日志记录。

### iOS 客户端日志

对于 iOS 客户端，日志文件位于 *User Programs/Horizon/* 下的 *tmp* 和 *Documents* 目录中。要导航至这些目录，您必须先安装 iFunbox 等第三方应用程序。

您可以在 Horizon Client 设置中开启日志记录设置，以启用日志记录。启用此设置后，如果客户端意外退出或您退出并重新启动客户端，系统会合并这些日志文件并将其压缩到一个 GZ 文件中。然后您可以通过电子邮件将日志包发送至 VMware。如果您的设备连接到 PC 或 Mac，还可以使用 iTunes 检索日志文件。

### Android 客户端日志

对于 Android 客户端，可以在以下目录找到日志文件：`Android/data/com.vmware.view.client.android/files/`。要导航至此目录，您必须先安装 File Explorer 或 My Files 等第三方应用程序。

默认情况下，仅会在此应用程序意外退出时创建日志。您可以在 Horizon Client 设置中开启启用日志设置，以更改此默认设置。要通过电子邮件将日志包发送至 VMware，您可以使用客户端的“常规设置”中的发送日志设置。

### Chrome 客户端日志

对于 Chrome 客户端，仅可以通过 JavaScript 控制台获取日志。

## Windows 应用商店客户端日志

对于已安装适用于 Windows 应用商店的 Horizon Client（而非适用于 Windows 的 Horizon Client）的 Windows 应用商店客户端，日志文件位于以下目录：C:\Users\%username%\AppData\Local\Packages\VMwareInc.VMwareViewClient\_23chmsjxv380w\LocalState\logs。

您可以在客户端的“常规设置”中开启启用高级日志记录设置，然后使用收集支持信息按钮，来启用日志记录。系统会提示您为日志选择一个文件夹，然后您可以像对任何其他文件夹一样压缩此文件夹。

## Windows 计算机的 Horizon Agent 日志

日志文件可以帮助排除安装、显示协议和各种功能组件方面的问题。您可以使用组策略设置配置某些日志文件的位置、详细级别和保留期限。

### 日志位置

对于下表中的文件名，YYYY 表示年份，MM 表示月份，DD 表示日期，XXXXXX 为编号。

**表 6-5. 适用于 Windows 的 Horizon Client 日志文件**

日志类型	目录路径	文件名
安装	C:\Users\%username%\AppData\Local\Temp	vminst.log_XXXXXX_XXXXXX.txt vmmsi.log_XXXXXX_XXXXXX.txt
View Agent（对于 Horizon 6）或 Horizon Agent（对于 Horizon 7）	<Drive Letter>:\ProgramData\VMware\VDM\logs	pcoip_agent_YYYY_MM_DD_XXXXXX.txt pcoip_agent_YYYY_MM_DD_XXXXXX.txt vmware-vdpServiceServer-XXXXXX.log Serial*.txt Scanner*.txt Netlink*.txt debug-yyyy-mm-dd-XXXXXX.txt
<b>注</b> 您可以使用 GPO 配置日志位置。请使用 View 公共配置 ADMX 模板文件 vdm_common.admx。		

### 日志配置

可以通过多种方法来配置日志记录选项。

- 您可以使用组策略设置配置日志位置、详细级别和保留策略。请使用 View 公共配置 ADMX 模板文件 vdm\_common.admx。
- 您可以使用命令行命令设置详细级别。导航到 C:\Program Files\VMware\VMware View\Agent\DCT 目录并输入以下命令：support.bat loglevels。将显示新的命令提示符窗口，提示您选择一种详细级别。
- 您可以使用 vdmadmin 命令和 -A 选项配置 View Agent 或 Horizon Agent 日志记录。有关说明，请参阅《View 管理指南》文档。

## 收集日志包

您可以使用命令行命令将日志收集到一个 .zip 文件中，然后可将该文件发送至 VMware 技术支持部门。从命令行中导航到 C:\Program Files\VMware\VMware View\Agent\DCT 目录并输入以下命令：  
support.bat。

## Linux 桌面日志

日志文件可以帮助排除安装、显示协议和各种功能组件方面的问题。您可以通过创建配置文件来配置详细级别。

### 日志位置

表 6-6. Linux 桌面日志文件

日志类型	目录路径
安装	/tmp/vmware-root
View Agent（对于 Horizon 6）或 Horizon Agent（对于 Horizon 7）	/var/log/vmware
View Agent（对于 Horizon 6）或 Horizon Agent（对于 Horizon 7）	/usr/lib/vmware/viewagent/viewagent-debug.log

### 日志配置

编辑 /etc/vmware/config 文件，配置日志记录。

## 收集日志包

您可以创建数据收集工具 (Data Collection Tool, DCT) 捆绑包，用来收集计算机的配置信息并记录到压缩的 tarball 中。在 Linux 桌面中打开命令提示符，运行 `dct-debug.sh` 脚本。

```
sudo /usr/lib/vmware/viewagent/bin/dct-debug.sh
```

将在执行该脚本的目录（当前的工作目录）中生成 tarball。文件名包含操作系统、时间戳和其他信息，例如：`ubuntu-12-vdm-sdct-20150201-0606-agent.tgz`

此命令用于从 /tmp/vmware-root 目录和 /var/log/vmware 目录收集日志文件，并收集以下系统日志和配置文件：

- /var/log/messages\*
- /var/log/syslog\*
- /var/log/boot\*.log
- /proc/cpuinfo、/proc/meminfo、/proc/vmstat、/proc/loadavg
- /var/log/audit/auth.log\*
- /etc/hosts

- `/etc/resolv.conf`
- `/etc/nsswitch.conf`
- `/var/log/Xorg*`
- `/etc/X11/xorg.conf`
- `/usr/lib/vmware/viewagent` 中的核心文件
- `/var/crash/_usr_lib_vmware_viewagent*` 中的任何崩溃文件

# 应用安全修补程序

修补程序版本可能包含以下 Horizon 7 组件的安装程序文件：View Composer、Horizon 连接服务器、View Agent 或 Horizon Agent 以及各种客户端。必须应用的修补程序组件取决于您的 Horizon 7 部署需要修复的错误。

根据需要修复的错误，按下列顺序安装适用的 Horizon 7 组件：

- 1 View Composer
- 2 连接服务器
- 3 View Agent（对于 Horizon 6）或 Horizon Agent（对于 Horizon 7）
- 4 Horizon Client

有关为服务器组件应用修补程序的说明，请参阅《View 升级指南》文档。

本章讨论了以下主题：

- [为 View Agent 或 Horizon Agent 应用修补程序](#)
- [为 Horizon Client 应用修补程序](#)

## 为 View Agent 或 Horizon Agent 应用修补程序

应用修补程序包括下载和运行修补程序版本的安装程序。

对于链接克隆桌面池中的父虚拟机、完整克隆池中的每个虚拟机桌面，或仅包含一个虚拟机桌面的池中的单个桌面虚拟机，需要执行以下步骤。

### 前提条件

确认您的域用户帐户在用于运行修补程序安装程序的主机上具有管理特权。

### 步骤

- 1 在所有父虚拟机、用于完整克隆模板的虚拟机、池中的完整克隆以及手动添加的各个虚拟机上，下载 View Agent（对于 Horizon 6）或 Horizon Agent（对于 Horizon 7）修补程序版本的安装程序文件。

有关下载的说明，请联系 VMware。

- 2 运行为 View Agent 或 Horizon Agent 修补程序版本下载的安装程序。

有关运行代理安装程序的信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档。

---

**注** 在 Horizon 6 版本 6.2 及更高版本中，安装修补程序之前无需卸载先前版本。

---

- 3 如果您在准备对 View Composer 应用修补程序时禁用了新虚拟机的置备，请重新启用置备。
- 4 对于将用于创建链接克隆桌面池的父虚拟机，请为虚拟机拍摄快照。  
有关拍摄快照的信息，请参阅 vSphere Client 联机帮助。
- 5 对于链接克隆桌面池，请使用创建的快照重构桌面池。
- 6 确认您可以使用 Horizon Client 登录到已修补的桌面池。
- 7 如果您取消了对任何链接克隆桌面池的任何刷新或重构操作，请重新安排这些任务。

## 为 Horizon Client 应用修补程序

在桌面客户端设备上，应用修补程序包括下载和运行修补程序版本的安装程序。在移动客户端上，应用修补程序只包括从销售应用程序的网站（如 Google Play、Windows 应用商店或 Apple App Store）安装更新。

### 步骤

- 1 在各个客户端系统中，下载 Horizon Client 修补程序版本的安装程序文件。  
有关下载的说明，请联系 VMware。或者您可以转到客户端下载页面，网址为 <http://www.vmware.com/go/viewclients>。如前所述，对于某些客户端，您可以从应用程序商店获取修补程序版本。
- 2 如果客户端设备是 Mac 或 Linux 台式机或笔记本电脑，请从设备上移除当前版本的客户端软件。  
删除应用程序时请使用特定于设备的惯常方法。  

---

**注** 对于适用于 Windows 的 Horizon Client 3.5 及更高版本，在 Windows 客户端上安装修补程序之前无需卸载先前版本。对于适用于 Windows 的 Horizon Client 4.1 及更高版本，可以启用“联机升级 Horizon Client”功能，以在 Windows 客户端上联机升级 Horizon Client。有关信息，请参阅适用于 Windows 的《使用 VMware Horizon Client》文档。对于适用于 Mac 4.4 及更高版本的 Horizon Client，可以启用“联机升级 Horizon Client”功能，以在 Mac 客户端上联机升级 Horizon Client。

---
- 3 如果适用，运行您为 Horizon Client 的修补程序版本下载的安装程序。  
如果您从 Apple App Store 或 Google Play 获取修补程序，应用程序通常会在您下载时进行安装，您无需运行安装程序。
- 4 确认使用新修补的 Horizon Client 可以登录到已修补的桌面池。