

# Horizon 7 安全

2018 年 12 月 13 日

VMware Horizon 7 7.7



vmware®

您可以从 VMware 网站下载最新的技术文档：

<https://docs.vmware.com/cn/>。

VMware 网站还提供了最近的产品更新。

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)

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)

# 目录

Horizon 7 安全性	5
<b>1 Horizon 7 帐户、资源和日志文件</b>	<b>6</b>
Horizon 7 帐户	6
Horizon 7 资源	7
Horizon 7 日志文件	7
<b>2 Horizon 7 安全性设置</b>	<b>9</b>
Horizon Administrator 中的安全性相关全局设置	9
Horizon Administrator 中的安全性相关服务器设置	11
View LDAP 中的安全性相关设置	12
<b>3 端口和服务</b>	<b>13</b>
Horizon 7 的 TCP 和 UDP 端口	13
Horizon 7 TrueSSO 端口	17
Horizon 7 Cloud Connector 虚拟设备端口	17
连接服务器主机上的服务	18
安全服务器上的服务	19
<b>4 证书指纹验证和自动生成证书</b>	<b>20</b>
<b>5 在连接服务器实例或安全服务器上配置安全协议和密码套件</b>	<b>21</b>
安全协议和密码套件的默认全局策略	21
配置全局接受和建议策略	22
在单个服务器上配置接受策略	23
在远程桌面上配置建议策略	25
在 Horizon 7 中禁用的旧协议和密码	25
<b>6 为 Blast 安全网关配置安全协议和密码套件</b>	<b>27</b>
为 Blast 安全网关 (BSG) 配置安全协议和密码套件	27
<b>7 为 PCoIP 安全网关配置安全协议和密码套件</b>	<b>29</b>
为 PCoIP 安全网关 (PSG) 配置安全协议和密码套件	29
<b>8 在安全的 Horizon 7 环境中部署 USB 设备</b>	<b>30</b>
对所有类型的设备禁用 USB 重定向	30
对特定设备禁用 USB 重定向	31

## 9 连接服务器和安全服务器上的 HTTP 保护措施 33

Internet 工程任务组标准 33

万维网联盟标准 34

其他保护措施 38

配置 HTTP 保护措施 42

# Horizon 7 安全性

《Horizon 7 安全指南》提供了对 VMware Horizon 7 的安全功能的简明参考。

- 所需的系统和数据库登录帐户。
- 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。
- 为确保 Horizon 7 正常运行而必须打开或启用的外部接口、端口和服务。

## 目标读者

本书信息面向 IT 决策制定者、架构师、管理员以及其他必须熟悉 Horizon 7 安全组件的读者。

# Horizon 7 帐户、资源和日志文件

为特定组件分配多个不同的帐户可避免向个人授予不必要的访问权限和特权。了解配置文件和其他包含敏感数据的文件的位置有助于为不同的主机系统设置安全保障。

**注** 从 Horizon 7.0 开始，View Agent 被重新命名为 Horizon Agent。

本章讨论了以下主题：

- [Horizon 7 帐户](#)
- [Horizon 7 资源](#)
- [Horizon 7 日志文件](#)

## Horizon 7 帐户

您必须设置系统和数据库帐户才能管理 Horizon 7 组件。

**表 1-1. Horizon 7 系统帐户**

Horizon 组件	所需帐户
Horizon Client	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。用户帐户必须是远程桌面用户组的成员，但无需 Horizon 管理员特权。
vCenter Server	在 Active Directory 中配置一个用户帐户，并使该帐户有权在 vCenter Server 中执行支持 Horizon 7 所需的必要操作。 有关所需特权的信息，请参阅《Horizon 7 安装指南》文档。
View Composer	AD operations account. 在 Active Directory 中创建一个用户帐户，以供 View Composer 使用。View Composer 需要使用该帐户将链接克隆桌面加入到您的 Active Directory 域。View Composer 用户的 AD 操作帐户不应该是 Horizon 管理帐户。为该帐户授予在指定的 Active Directory 容器中创建和移除计算机对象所需的最低特权。例如，该帐户不需要域管理员特权。  Standalone control account. 如果在与 vCenter Server 所在的相同计算机上安装 View Composer，Horizon 7 将使用相同的用户帐户来访问 vCenter Server 和 View Composer 服务。如果在独立的计算机上安装 View Composer，需配置一个单独的用户帐户，以便 Horizon 7 访问 View Composer。 有关 AD 操作帐户和独立控制帐户所需特权的信息，请参阅《Horizon 7 安装指南》文档。
连接服务器	在安装 Horizon 7 时，您可以指定特定的域用户、本地 Administrators 组或特定的域用户组以作为 Horizon 管理员。我们建议您创建专用的 Horizon 管理员域用户组。默认设置为当前登录的域用户。 在 Horizon Administrator 中，您可以使用 <b>View 配置 &gt; 管理员</b> 更改 Horizon 管理员列表。 有关所需特权的信息，请参阅《Horizon 7 管理指南》文档。

表 1-2. Horizon 数据库帐户

Horizon 组件	所需帐户
View Composer 数据库	存储 View Composer 数据的 SQL Server 或 Oracle 数据库。您要为可与 View Composer 用户帐户关联的数据库创建一个管理帐户。 有关设置 View Composer 数据库的信息，请参阅《Horizon 7 安装指南》文档。
Horizon 连接服务器使用的事件数据库	存储 Horizon 事件数据的 SQL Server 或 Oracle 数据库。您要为 Horizon Administrator 可用于访问事件数据的数据库创建一个管理帐户。 有关设置 View Composer 数据库的信息，请参阅《Horizon 7 安装指南》文档。

为减少安全漏洞风险，请采取以下措施：

- 在与组织使用的数据库服务器分开的单独服务器上配置 Horizon 7 数据库。
- 不允许一个用户帐户访问多个数据库。
- 配置单独帐户访问 View Composer 和事件数据库。

## Horizon 7 资源

Horizon 7 中包含若干配置文件和类似资源，必须为它们提供保护。

表 1-3. Horizon 连接服务器和安全服务器资源

资源	位置	保护
LDAP 设置	不适用。	LDAP 数据会作为基于角色的访问控制的一部分，自动得到保护。
LDAP 备份文件	%ProgramData%\VMware\VDM\backups	由访问控制保护。
locked.properties (安全网关配置文件)	install_directory\VMware\VMware View\Server\sslgateway\conf	确保该文件不被 Horizon 管理员以外的任何用户访问。
absg.properties (Blast 安全网关配置文件)	install_directory\VMware\VMware View\Server\appblastgateway	确保该文件不被 Horizon 管理员以外的任何用户访问。
日志文件	请参阅 <a href="#">Horizon 7 日志文件</a>	由访问控制保护。
web.xml (Tomcat 配置文件)	install_directory\VMware View\Server\broker\web apps\ROOT\Web INF	由访问控制保护。

## Horizon 7 日志文件

Horizon 7 会创建记录其组件安装和运行情况的日志文件。

**注** Horizon 7 日志文件专供 VMware 支持部门使用。VMware 建议您配置并使用事件数据库来监视 Horizon 7。有关更多信息，请参阅《Horizon 7 安装指南》和《Horizon 7 集成指南》文档。

表 1-4. Horizon 7 日志文件

Horizon 组件	文件路径和其他信息
所有组件（安装日志）	<p>%TEMP%\vminst.log_date_timestamp</p> <p>%TEMP%\vmmsi.log_date_timestamp</p>
Horizon Agent	<p>&lt;Drive Letter&gt;:\ProgramData\VMware\VDM\logs</p> <p>要访问 &lt;Drive Letter&gt;:\ProgramData\VMware\VDM\logs 中存储的 Horizon 7 日志文件，您必须使用具有高管理员特权的程序打开这些日志。右键单击应用程序文件，然后选择<b>以管理员身份运行</b>。</p> <p>如果配置了用户数据磁盘 (User Data Disk, UDD)，&lt;Drive Letter&gt; 可能对应于 UDD。</p> <p>PCoIP 的日志命名为 pcoip_agent*.log 和 pcoip_server*.log。</p>
已发布的应用程序	<p>SQL Server 或 Oracle 数据库服务器上配置的 Horizon 事件数据库。</p> <p>Windows 应用程序事件日志。默认情况下禁用。</p>
View Composer	<p>链接克隆桌面上的 %system_drive%\Windows\Temp\vmware-viewcomposer-ga-new.log。</p> <p>View Composer 日志中包含有关 QuickPrep 和 Sysprep 脚本执行情况的信息。日志记录了脚本执行的开始时间和结束时间，以及任何输出或错误消息。</p>
连接服务器或安全服务器	<p>&lt;Drive Letter&gt; : \ProgramData\VMware\VDM\logs。</p> <p>日志目录可在公共配置 ADMX 模板文件 (vdm_common.admx) 的日志配置设置中进行配置。</p> <p>PCoIP 安全网关日志将写入到名为 SecurityGateway_*.log 的文件，这些文件位于 PCoIP Secure Gateway 子目录中。</p> <p>Blast 安全网关日志将写入到名为 absg*.log 的文件，这些文件位于 Blast Secure Gateway 子目录中。</p>
Horizon 服务	<p>SQL Server 或 Oracle 数据库服务器上配置的 Horizon 事件数据库。</p> <p>Windows 系统事件日志。</p>



## Horizon 7 安全性设置

Horizon 7 中包含一些设置，您可以使用这些设置来调整配置的安全性。您可以根据需要使用 **Horizon Administrator** 或使用“ADSI 编辑”实用程序来访问这些设置。

---

**注** 有关 Horizon Client 和 Horizon Agent 安全设置的信息，请参阅《Horizon Client 和 Agent 安全指南》文档。

---

本章讨论了以下主题：

- [Horizon Administrator](#) 中的安全性相关全局设置
- [Horizon Administrator](#) 中的安全性相关服务器设置
- [View LDAP](#) 中的安全性相关设置

### Horizon Administrator 中的安全性相关全局设置

用于客户端会话和连接的安全性相关全局设置可通过 Horizon Administrator 中的 **View 配置 > 全局设置** 来访问。

表 2-1. 安全性相关的全局设置

设置	说明
更改数据恢复密码	<p>从加密备份还原 View LDAP 配置时需要提供密码。</p> <p>安装连接服务器 5.1 或更高版本时，需要提供一个数据恢复密码。安装后，可以在 Horizon Administrator 中更改此密码。</p> <p>备份连接服务器时，View LDAP 配置将导出为加密的 LDIF 数据。要通过 vdmimport 实用程序还原加密备份，需要提供数据恢复密码。密码包含的字符必须介于 1 到 128 个之间。请遵循组织的最佳实践来生成安全密码。</p>
消息安全模式	<p>决定在 Horizon 7 组件之间传递 JMS 消息时使用的安全机制。</p> <ul style="list-style-type: none"> <li>如果设置为<b>禁用</b>，消息安全模式将被禁用。</li> <li>如果设置为<b>已启用</b>，将对 JMS 消息执行旧消息签名和验证。Horizon 7 组件会拒绝未签名的消息。此模式支持混合使用 TLS 连接和纯 JMS 连接。</li> <li>如果设置为<b>已增强</b>，将对所有 JMS 连接使用 TLS 以加密所有消息。此外，还会启用访问控制，以限制 Horizon 7 组件可以向其发送消息以及从中接收消息的 JMS 主题。</li> <li>如果设置为<b>混合</b>，消息安全模式将被启用，但不会强制用于 View Manager 3.0 之前的 Horizon 7 组件。</li> </ul> <p>新安装的默认设置为<b>已增强</b>。如果从先前版本进行升级，则将保留在先前版本中使用的设置。</p> <p><b>重要</b> VMware 强烈建议您在将所有连接服务器实例、安全服务器和 Horizon 7 桌面升级到此版本后将消息安全模式设置为<b>已增强</b>。<b>已增强</b>设置提供多项重要的安全性改进功能和 MQ（消息队列）更新。</p>
增强安全状态（只读）	<p>将<b>消息安全模式</b>从<b>已启用</b>更改为<b>已增强</b>时显示的只读字段。由于更改分阶段进行，此字段根据阶段显示进度：</p> <ul style="list-style-type: none"> <li><b>等待 Message Bus 重新启动</b>是第一阶段。此状态将一直显示，直到您手动重新启动容器中的所有连接服务器实例或容器中所有连接服务器主机上的 VMware Horizon Message Bus 组件服务。</li> <li><b>等待增强</b>是下一阶段。重新启动所有 Horizon Message Bus 组件服务后，系统开始将所有桌面和安全服务器的消息安全模式更改为<b>已增强</b>。</li> <li><b>已增强</b>是最终状态，表明所有组件现在正在使用<b>已增强</b>消息安全模式。</li> </ul>
网络中断后对安全加密链路连接重新进行身份验证	<p>在 Horizon Client 通过安全加密链路连接到 Horizon 7 桌面和应用程序的情况下，确定在网络中断后是否必须重新对用户凭据进行身份验证。</p> <p>此设置可提高安全性。例如，如果笔记本电脑被盗并转移到了其他网络，用户将无法自动获取 Horizon 7 桌面和应用程序的访问权限，原因是网络连接已临时中断。</p> <p>默认情况下禁用此设置。</p>
强制断开用户连接	<p>自用户登录到 Horizon 7 时起达到指定分钟数后，断开所有桌面和应用程序连接。无论桌面和应用程序是被用户何时打开的，都将同时断开连接。</p> <p>默认值是 600 分钟。</p>
对于支持应用程序的客户端。 如果用户停止使用键盘和鼠标，则将断开应用程序连接并放弃 SSO 凭据	<p>在客户端设备上无键盘或鼠标活动时保护应用程序会话。如果设置为 <b>…分钟之后</b>，Horizon 7 将在无用户活动达到指定的分钟数后断开所有应用程序连接并放弃 SSO 凭据。桌面会话将断开连接。用户必须重新登录以重新连接被断开的应用程序或者启动新的桌面或应用程序。</p> <p>如果设置为<b>从不</b>，Horizon 7 将绝不会因用户不活动而断开应用程序连接或放弃 SSO 凭据。</p> <p>默认值为<b>从不</b>。</p>
其他客户端。 放弃 SSO 凭据	<p>在特定时间段后放弃 SSO 凭据。此设置适用于不支持应用程序远程的客户端。如果设置为 <b>…分钟之后</b>，那么自用户登录到 Horizon 7 时起达到指定分钟数后，用户必须重新登录以连接到桌面，而不管客户端设备上的用户活动情况如何。</p> <p>默认值为 <b>15 分钟之后</b>。</p>

表 2-1. 安全性相关的全局设置（续）

设置	说明
启用 IPsec 以执行安全服务器配对	确定是否为安全服务器和 Horizon 连接服务器实例之间的连接使用 Internet 协议安全性 (Internet Protocol Security, IPsec)。必须在 FIPS 模式下安装安全服务器之前禁用该设置，否则，配对将失败。默认情况下会使用 IPsec 进行安全服务器连接。
View Administrator 会话超时	<p>确定 Horizon Administrator 会话持续闲置多久后超时。</p> <p><b>重要</b> Horizon Administrator 会话超时值设置较高会增加未授权使用 Horizon Administrator 的风险。允许闲置会话持续较长时间时应慎重考虑。</p> <p>默认情况下，Horizon Administrator 会话超时为 30 分钟。会话超时值的设置范围为 1 到 4320 分钟之间。</p>

有关这些设置及其安全性影响的更多信息，请参阅《Horizon 7 管理指南》文档。

**注** 到 Horizon 7 的所有 Horizon Client 连接和 Horizon Administrator 连接都需要使用 TLS。如果您的 Horizon 7 部署使用负载均衡器或其他面向客户端的中间服务器，可以将 TLS 负载分流到这些负载均衡器或中间服务器，然后在单个连接服务器实例和安全服务器上配置非 TLS 连接。请参阅《Horizon 7 管理指南》文档中的“将 TLS 连接负载分流到中间服务器”。

## Horizon Administrator 中的安全性相关服务器设置

安全性相关的服务器设置可通过 Horizon Administrator 中的 **View 配置 > 服务器** 来访问。

表 2-2. 安全性相关的服务器设置

设置	说明
使用 PCoIP 安全网关与计算机建立 PCoIP 连接	<p>确定当用户使用 PCoIP 显示协议连接至 Horizon 7 桌面和应用程序时，Horizon Client 是否会和连接服务器或安全服务器主机建立另一条安全连接。</p> <p>如果禁用此设置，将绕开连接服务器或安全服务器主机，直接在客户端和 Horizon 7 桌面或远程桌面服务 (Remote Desktop Services, RDS) 主机之间建立桌面或应用程序会话。</p> <p>默认情况下禁用此设置。</p>
使用安全加密链路连接计算机	<p>确定当用户连接至 Horizon 7 桌面或应用程序时，Horizon Client 是否会和连接服务器或安全服务器主机建立另一条 HTTPS 连接。</p> <p>如果禁用此设置，将绕开连接服务器或安全服务器主机，直接在客户端和 Horizon 7 桌面或远程桌面服务 (RDS) 主机之间建立桌面或应用程序会话。</p> <p>默认情况下启用该设置。</p>
使用 Blast 安全网关对计算机进行 Blast 连接	<p>确定使用 Web 浏览器或 Blast Extreme 显示协议访问桌面的客户端是否使用 Blast 安全网关建立到连接服务器的安全加密链路。</p> <p>如果不启用此设置，使用 Blast Extreme 会话和 Web 浏览器的客户端将绕过连接服务器，而直接与 Horizon 7 桌面建立连接。</p> <p>默认情况下禁用此设置。</p>

有关这些设置及其安全性影响的更多信息，请参阅《Horizon 7 管理指南》文档。

## View LDAP 中的安全性相关设置

View LDAP 的对象路径 `cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int` 中提供了安全性相关设置。您可以使用“ADSI 编辑”实用程序，在连接服务器实例中更改这些设置的值。所做更改将自动传播到组中的所有其他连接服务器实例。

**表 2-3. View LDAP 中的安全性相关设置**

名称 - 值对	说明
<b>cs-allowunencryptedstartsession</b>	<p>属性为 <code>pae-NameValuePair</code>。</p> <p>此属性可以控制当启动某个远程用户会话时，连接服务器实例与桌面间是否需要使用安全加密链路。</p> <p>如果桌面计算机上安装了 <b>View Agent 5.1</b> 或更高版本或者 <b>Horizon Agent 7.0</b> 或更高版本，则始终需要使用安全加密链路，即，此属性不起作用。如果安装的 <b>View Agent</b> 版本早于 <b>View 5.1</b>，当桌面计算机不隶属于某个与连接服务器实例所在域之间存在双向信任关系的域时，无法建立安全加密链路。这种情况下，在确定是否可以在无安全加密链路的情况下启动远程用户会话时，此属性非常重要。</p> <p>无论在何种情况下，用户凭据和授权票证都受静态密钥保护。安全加密链路使用动态密钥，可进一步保证机密信息的安全性。</p> <p>如果设置为 <b>0</b>，那么在无法建立安全加密链路的情况下是不能启动远程用户会话的。当全部桌面都隶属于受信任的域或者全部桌面都安装了 <b>View Agent 5.1</b> 或更高版本时，此设置适用。</p> <p>如果设置为 <b>1</b>，即使不能建立安全加密链路，也能启动远程用户会话。当某些桌面安装了低版本的 <b>View Agent</b> 且不隶属于受信任的域时，此设置适用。</p> <p>默认设置为 <b>1</b>。</p>

## 端口和服务

某些 UDP 和 TCP 端口必须打开，以便 Horizon 7 组件可以相互通信。了解每种类型 Horizon 7 Server 上运行哪些 Windows 服务有助于识别不属于相应服务器的服务。

本章讨论了以下主题：

- [Horizon 7 的 TCP 和 UDP 端口](#)
- [Horizon 7 TrueSSO 端口](#)
- [Horizon 7 Cloud Connector 虚拟设备端口](#)
- [连接服务器主机上的服务](#)
- [安全服务器上的服务](#)

### Horizon 7 的 TCP 和 UDP 端口

Horizon 7 使用 TCP 和 UDP 端口进行组件之间的网络访问。

在安装过程中，Horizon 7 可以选择性地配置 Windows 防火墙规则以打开默认使用的端口。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《Horizon 7 安装指南》文档中的“替换 Horizon 7 服务的默认端口”。

有关 Horizon 7 用于进行与 TrueSSO 解决方案有关的证书登录的端口列表，请参阅 [Horizon 7 TrueSSO 端口](#)。

**表 3-1. Horizon 7 使用的 TCP 和 UDP 端口**

源	端口	目标	端口	协议	说明
安全服务器、连接服务器或 Unified Access Gateway 设备	55000	Horizon Agent	4172	UDP	PCoIP（非 SALSA20）（如果使用 PCoIP 安全网关）。
安全服务器、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）。 <a href="#">注</a> 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	500	连接服务器	500	UDP	IPsec 协商流量。
安全服务器	*	连接服务器	4001	TCP	JMS 流量。
安全服务器	*	连接服务器	4002	TCP	JMS SSL 流量。

表 3-1. Horizon 7 使用的 TCP 和 UDP 端口（续）

源	端口	目标	端口	协议	说明
安全服务器	*	连接服务器	8009	TCP	AJP13 转发的 Web 流量（如果未使用 IPsec）。
安全服务器	*	连接服务器	*	ESP	AJP13 转发的 Web 流量（使用 IPsec 而无 NAT 时）。
安全服务器	4500	连接服务器	4500	UDP	AJP13 转发的 Web 流量（当通过 NAT 设备使用 IPsec 时）。
安全服务器、连接服务器或 Unified Access Gateway 设备	*	Horizon Agent	3389	TCP	指向 Horizon 7 桌面的 Microsoft RDP 流量（使用安全加密链路连接时）。
安全服务器、连接服务器或 Unified Access Gateway 设备	*	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、连接服务器或 Unified Access Gateway 设备	*	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、连接服务器或 Unified Access Gateway 设备	*	Horizon Agent	4172	TCP	PCoIP（如果使用 PCoIP 安全网关）。
安全服务器、连接服务器或 Unified Access Gateway 设备	*	Horizon Agent	22443	TCP	VMware Blast Extreme（如果使用 Blast 安全网关）。
安全服务器、连接服务器或 Unified Access Gateway 设备	*	Horizon Agent	22443	TCP	HTML Access（如果使用 Blast 安全网关）。
Horizon Agent	4172	Horizon Client	*	UDP	PCoIP（如果未使用 PCoIP 安全网关）。 <a href="#">注</a> 由于目标端口有所不同，请参阅此表格下面的注释。
Horizon Agent	4172	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）。
Horizon Agent	4172	Unified Access Gateway 设备	*	UDP	PCoIP。Horizon 7 桌面和应用程序将 PCoIP 数据从 UDP 端口 4172 发回到 Unified Access Gateway 设备。 UDP 目标端口将作为已接收 UDP 数据包的源端口，由于是回复数据，通常不需要为此添加明确的防火墙规则。
Horizon Agent（未受管）	*	连接服务器实例	389	TCP	在安装未受管代理过程中进行 AD LDS 访问。 <a href="#">注</a> 有关此端口的其他用途，请参阅此表下面的注释。

表 3-1. Horizon 7 使用的 TCP 和 UDP 端口（续）

源	端口	目标	端口	协议	说明
Horizon Client	*	连接服务器、安全服务器或 Unified Access Gateway 设备	80	TCP	默认情况下启用 TLS（HTTPS 访问）进行客户端连接，但是在特定情况下可以使用端口 80（HTTP 访问）。请参阅 <a href="#">Horizon 7 中的 HTTP 重定向</a> 。
Horizon Client	*	连接服务器、安全服务器或 Unified Access Gateway 设备	443	TCP	用于登录 Horizon 7 的 HTTPS。（在使用安全加密链路连接时此端口还用于转发）。
Horizon Client	*	连接服务器、安全服务器或 Unified Access Gateway 设备	4172	TCP 和 UDP	PCoIP（如果使用 PCoIP 安全网关）。
Horizon Client	*	Horizon Agent	3389	TCP	指向 Horizon 7 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	*	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）。
Horizon Client	*	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	*	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
Horizon Client	*	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）。 <a href="#">注</a> 由于源端口有所不同，请参阅此表格下面的注释。
Web 浏览器	*	安全服务器或 Unified Access Gateway 设备	8443	TCP	HTML Access。
连接服务器	*	连接服务器	48080	TCP	用于连接服务器组件之间的内部通信。
连接服务器	*	vCenter Server 或 View Composer	80	TCP	SOAP 消息（如果对 vCenter Server 或 View Composer 访问禁用 TLS）。
连接服务器	*	vCenter Server	443	TCP	SOAP 消息（如果对 vCenter Server 访问启用 TLS）。
连接服务器	*	View Composer	18443	TCP	SOAP 消息（如果对 View Composer 访问启用 TLS）。
连接服务器	*	连接服务器	4100	TCP	JMS 路由器之间的流量。
连接服务器	*	连接服务器	4101	TCP	JMS TLS 路由器之间的流量。
连接服务器	*	连接服务器	8472	TCP	用于 Cloud Pod 架构中的容器间通信。
连接服务器	*	连接服务器	22389	TCP	用于在 Cloud Pod 架构中进行全局 LDAP 复制。
连接服务器	*	连接服务器	22636	TCP	用于在 Cloud Pod 架构中进行安全的全局 LDAP 复制。
连接服务器	*	连接服务器	32111	TCP	密钥共享流量。

表 3-1. Horizon 7 使用的 TCP 和 UDP 端口（续）

源	端口	目标	端口	协议	说明
连接服务器	*	证书颁发机构	*	HTTP、HTTPS	CRL 或 OCSP 查询
Unified Access Gateway 设备	*	连接服务器或负载均衡器	443	TCP	HTTPS 访问。Unified Access Gateway 设备通过 TCP 端口 443 进行连接，以便与一个连接服务器实例或多个连接服务器实例前面的负载均衡器进行通信。
View Composer 服务	*	ESXi 主机	902	TCP	在 View Composer 自定义链接克隆磁盘时使用，这些磁盘包括 View Composer 内部磁盘和永久磁盘及系统一次性磁盘（如已指定）。

**注** 客户端用于 PCoIP 的 UDP 端口号可能会发生更改。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）。

**注** Microsoft Windows Server 要求在 Horizon 7 环境中的所有连接服务器之间打开一系列动态端口。Microsoft Windows 需要使用这些端口来执行常规的远程过程调用 (RPC) 和 Active Directory 复制操作。有关动态端口范围的更多信息，请参阅 Microsoft Windows Server 文档。

**注** 在连接服务器实例上，可通过访问端口 389 来建立不常见的临时连接。在安装此表中所示的未受管代理时、在使用 LDAP 编辑器直接编辑数据库时，以及在使用 repadmin 等工具颁发命令时，可以访问此端口。安装 AD LDS 时，将出于这些目的创建防火墙规则，但是如果不需要访问此端口，可以将其禁用。

## Horizon 7 中的 HTTP 重定向

通过 HTTP 进行的连接尝试会以静默方式重定向到 HTTPS，但指向 Horizon Administrator 的连接尝试除外。较高版本的 Horizon Client 无需进行 HTTP 重定向，因为它们默认使用 HTTPS，但是当用户使用 Web 浏览器连接（例如下载 Horizon Client）时，HTTP 重定向是很有用的。

HTTP 重定向的问题在于它是一个非安全协议。如果用户没有在地址栏中输入 **https://** 的习惯，则攻击者将会攻击 Web 浏览器、安装恶意软件或盗取凭据，甚至在正确显示预期页面的时候也会如此。

**注** 仅当您外部防火墙配置为允许 TCP 端口 80 的入站流量时，才会出现外部连接的 HTTP 重定向。

通过 HTTP 向 Horizon Administrator 进行的连接尝试不会进行重定向。相反，将返回一条错误消息，指示必须使用 HTTPS。

要避免所有 HTTP 连接尝试的重定向，请参阅《Horizon 7 安装指南》文档中的“防止客户端连接到连接服务器的 HTTP 重定向”。

如果将 TLS 客户端连接负载分流到中间设备，还可以与连接服务器实例或安全服务器的端口 80 建立连接。请参阅《Horizon 7 管理指南》文档中的“将 TLS 连接负载分流到中间服务器”。

要允许更改 TLS 端口号后进行 HTTP 重定向，请参阅《Horizon 7 安装指南》文档中的“更改端口号以允许到连接服务器的 HTTP 重定向”。



## Horizon 7 TrueSSO 端口

Horizon 7 使用 TrueSSO 端口作为通信路径（端口和协议）和安全控制，在 Horizon Connection Server 和虚拟桌面或已发布的应用程序之间传递证书，以进行与 TrueSSO 解决方案有关的证书登录。

表 3-2. Horizon 7 使用的 TrueSSO 端口

源	目标	端口	协议	说明
Horizon Client	VMware Identity Manager 设备	TCP 443	HTTPS	从生成 SAML 断言和项目的 VMware Identity Manager 设备启动 Horizon 7。
Horizon Client	Horizon Connection Server	TCP 443	HTTPS	启动 Horizon Client。
Horizon Connection Server	VMware Identity Manager 设备	TCP 443	HTTPS	连接服务器对 VMware Identity Manager 执行 SAML 解析。VMware Identity Manager 验证项目并返回断言。
Horizon Connection Server	Horizon 注册服务器	TCP 32111		使用此注册服务器。
注册服务器	ADCS			注册服务器从 Microsoft 证书颁发机构 (Certificate Authority, CA) 请求证书，以生成一个临时的短期证书。 注册服务使用 TCP 135 RPC 与该 CA 进行初步通信，然后使用从 1024 - 5000 和 49152 - 65535 之间随机选择的一个端口。请参阅 <a href="https://support.microsoft.com/en-us/help/832017#method4">https://support.microsoft.com/en-us/help/832017#method4</a> 中的“证书服务”。 注册服务器还会与域控制器进行通信，使用所有相关端口来发现 DC，然后绑定到 Active Directory 并进行查询。 请参阅 <a href="https://support.microsoft.com/en-us/help/832017#method1">https://support.microsoft.com/en-us/help/832017#method1</a> 和 <a href="https://support.microsoft.com/en-us/help/832017#method12">https://support.microsoft.com/en-us/help/832017#method12</a> 。
Horizon Agent	Horizon Connection Server	TCP 4002	JMS over TLS	Horizon Agent 请求并接收用于登录的证书。
虚拟桌面或已发布的应用程序	AD DC			Windows 通过 Active Directory 验证此证书的真实性。因为可能需要大量端口，因此，请参阅相关 Microsoft 文档以了解端口和协议列表。
Horizon Client	Horizon Agent（协议会话）	TCP/UDP 22443	Blast	登录到 Windows 桌面或应用程序并在 Horizon Client 上启动一个远程会话。
Horizon Client	Horizon Agent（协议会话）	UDP 4172	PCoIP	登录到 Windows 桌面或应用程序，此时将在 Horizon Client 上启动一个远程会话。

## Horizon 7 Cloud Connector 虚拟设备端口

Horizon 7 使用端口来侦听各种请求，如从另一个 Horizon 7 Cloud Connector 虚拟设备升级，或与 VMware Horizon Cloud Service 配对和通信及对其进行身份验证。

表 3-3. Horizon 7 Cloud Connector 端口

源	端口	目标	端口	协议	说明
Horizon 7 Cloud Connector	*	VMware Horizon Cloud Service	443	HTTPS	与 VMware Horizon Cloud Service 配对并传输数据。
Horizon 7 Cloud Connector	*	连接服务器	443	HTTPS	对连接服务器的 API 调用。
新的 Horizon 7 Cloud Connector	*	现有 Horizon 7 Cloud Connector	22	SSH	侦听启动升级过程的请求。
Web 浏览器	*	Horizon 7 Cloud Connector	443	HTTPS	侦听启动配对过程的请求。
Horizon 7 Cloud Connector	*	证书颁发机构	*	HTTP、HTTPS	CRL 或 OCSP 查询

## 连接服务器主机上的服务

Horizon 7 的运行依赖于连接服务器主机上运行的若干服务。

表 3-4. Horizon 连接服务器主机服务

服务名称	启动类型	说明
VMware Horizon View Blast 安全网关	自动	提供安全 HTML Access 和 Blast Extreme 服务。如果客户端通过 Blast 安全网关连接到连接服务器，则必须运行此服务。
VMware Horizon View 连接服务器	自动	提供连接代理服务。必须始终运行此服务。如果启动或停止此服务，会同时启动或停止 Framework、Message Bus、Security Gateway 和 Web 服务。此服务不会启动或停止 VMwareVDMDS 服务或 VMware Horizon View 脚本主机服务。
VMware Horizon View Framework 组件	手动	提供事件日志、安全和 COM+ 框架服务。必须始终运行此服务。
VMware Horizon View Message Bus 组件	手动	在 Horizon 7 组件之间提供消息传递服务。必须始终运行此服务。
VMware Horizon View PCoIP 安全网关	手动	提供 PCoIP 安全网关服务。如果客户端通过 PCoIP 安全网关连接到连接服务器，则必须运行此服务。
VMware Horizon View 脚本主机	已禁用	对您删除虚拟机时运行的第三方脚本提供支持。默认情况下，此服务已被禁用。如果您需要运行脚本，应启用此服务。
VMware Horizon View Security Gateway 组件	手动	提供常见的网关服务。必须始终运行此服务。
VMware Horizon View Web 组件	手动	提供 Web 服务。必须始终运行此服务。
VMwareVDMDS	自动	提供 LDAP 目录服务。必须始终运行此服务。升级 Horizon 7 期间，此服务将确保正确迁移现有数据。

## 安全服务器上的服务

Horizon 7 的运行依赖于安全服务器上运行的若干服务。

表 3-5. 安全服务器服务

服务名称	启动类型	描述
VMware Horizon View Blast 安全网关	自动	提供安全 HTML Access 和 Blast Extreme 服务。如果客户端通过 Blast 安全网关连接到该安全服务器，则必须运行此服务。
VMware Horizon View 安全服务器	自动	提供安全服务器服务。必须始终运行此服务。如果您启动或停止此服务，会同时启动或停止 Framework 和 Security Gateway 服务。
VMware Horizon View Framework 组件	手动	提供事件日志、安全和 COM+ 框架服务。必须始终运行此服务。
VMware Horizon View PCoIP 安全 网关	手动	提供 PCoIP 安全网关服务。如果客户端通过 PCoIP 安全网关连接到该安全服务器，则必须运行此服务。
VMware Horizon View Security Gateway 组件	手动	提供常见的网关服务。必须始终运行此服务。

## 证书指纹验证和自动生成证书

Horizon 7 会使用许多公钥证书。其中一些证书使用的验证机制涉及到受信任的第三方，但这类机制有时不具备所需的精度、速度或灵活性。在某些情况下，Horizon 7 会使用称作指纹验证的替代机制。

指纹验证并不验证各个证书字段或构建信任链，而是将证书视为令牌，将整个字节序列（或其加密哈希）与预共享的字节序列或哈希进行匹配。通常情况下，预共享的字节序列或哈希会通过单独的受信任通道来即时共享，这意味着服务提供的证书可以确认就是预期的证书。

Horizon 消息总线可在连接服务器之间进行通信，也可在 Horizon Agent 和连接服务器实例之间进行通信。安装通道使用每消息签名和负载加密，而主通道由实施双向身份验证的 TLS 提供保护。当使用 TLS 保护通道时，客户端和服务器的身份验证都会使用 TLS 证书和指纹验证。对于 Horizon 消息总线通道，服务器始终充当消息路由器的角色。客户端也可以充当消息路由器，因为消息路由器就是通过这种方式共享消息的。但是，客户端可能是连接服务器实例、安全服务器或 Horizon Agent。

初始证书指纹和设置消息签名密钥分别以不同的方式提供。例如，在配对期间，安全服务器会与其连接服务器交换此信息。虽然会进行此初始交换，但后续签名密钥和证书指纹变换会通过设置通道进行通信。在连接服务器上，证书指纹存储在 LDAP 中，以便 Horizon Agent 可以与任何连接服务器进行通信，并且所有连接服务器都可以互相通信。Horizon 消息总线服务器证书和客户端证书会自动生成并定期进行交换，过期证书会自动删除，因此无需手动干预，或者说，实际上无法进行手动干预。主通道两端的证书均会按照计划自动生成，并通过安装通道交换。您无法自行替换这类证书。过期的证书会自动移除。

类似的机制也适用于容器间通信。

其他通信通道可以使用客户提供的证书，但默认设置为自动生成证书。这包括安全加密链路、注册服务器，Composer 和 vCenter 的连接，以及显示协议和辅助通道。有关如何替换这类证书的详细信息，请参阅《Horizon 7 管理指南》文档。默认证书在安装时生成，除在使用 PCoIP 的情况下，默认证书不会自动续订。如果没有 PKI 生成的证书可供 PCoIP 使用，PCoIP 将在每次启动时自动生成新的证书。即使使用 PKI 生成的证书，但其中大部分通道还会使用指纹验证。

Composer 证书和 vCenter 证书的验证会结合使用不同的技术。连接服务器实例始终会尝试使用 PKI 验证收到的证书。如果此验证失败，Horizon 7 管理员可以在查看证书后允许继续连接，这时连接服务器会记住该证书的加密哈希，以便在随后的指纹验证中自动接受该证书。

# 在连接服务器实例或安全服务器上配置安全协议和密码套件

## 5

您可以配置连接服务器接受的安全协议和密码套件。还可以定义适用于副本组中全部连接服务器实例的全局接受策略，也可以为各个连接服务器实例和安全服务器定义接受策略。

还可以配置连接服务器实例在连接 vCenter Server 和 View Composer 时会建议的安全协议和密码套件。您可以定义适用于副本组中全部连接服务器实例的全局建议策略。不能将单个实例定义为不受全局建议策略影响。

**注** 连接服务器的安全设置不适用于 Blast 安全网关 (BSG)。您必须为 BSG 单独配置安全性设置。请参阅第 6 章，为 Blast 安全网关配置安全协议和密码套件。

Oracle 的无限强度管辖策略文件是作为标准配置提供的，默认允许使用 256 位密钥。

本章讨论了以下主题：

- 安全协议和密码套件的默认全局策略
- 配置全局接受和建议策略
- 在单个服务器上配置接受策略
- 在远程桌面上配置建议策略
- 在 Horizon 7 中禁用的旧协议和密码

## 安全协议和密码套件的默认全局策略

默认情况下，全局接受和建议策略启用某些安全协议和密码套件。

表 5-1. 默认全局接受策略

默认安全协议	默认密码套件
<ul style="list-style-type: none"><li>■ TLS 1.2</li><li>■ TLS 1.1</li></ul>	<ul style="list-style-type: none"><li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256</li><li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA</li><li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384</li><li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA</li></ul>

表 5-2. 默认全局建议策略

默认安全协议	默认密码套件
<ul style="list-style-type: none"> <li>■ TLS 1.2</li> <li>■ TLS 1.1</li> </ul>	<ul style="list-style-type: none"> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256</li> <li>■ TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384</li> <li>■ TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA</li> <li>■ TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>■ TLS_RSA_WITH_AES_256_CBC_SHA</li> </ul>

出于性能考虑，默认情况下不启用 GCM 密码套件。

## 配置全局接受和建议策略

全局接受和建议策略是在 View LDAP 属性中定义的。这些策略适用于副本组中的所有连接服务器实例和安全服务器。要更改全局策略，可编辑任意连接服务器实例上的 View LDAP。

每项策略都是以下 View LDAP 位置中的一个单值属性：

cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int

## View LDAP 中定义的全局接受和建议策略

您可以编辑定义全局接受和建议策略的 View LDAP 属性。

### 全局接受策略

以下属性列出了安全协议。您必须先添加最新的协议，使列表井然有序：

```
pae-ServerSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
```

以下属性列出了密码套件。该示例显示了一个缩略表：

```
pae-ServerSSLCipherSuites = \LIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

以下属性可控制密码套件的优先级。通常，服务器的密码套件顺序无关紧要，因为使用的是客户端的顺序。要改为使用服务器的密码套件顺序，请设置以下属性：

```
pae-ServerSSLHonorClientOrder = 0
```

## 全局建议策略

以下属性列出了安全协议。您必须先添加最新的协议，使列表井然有序：

```
pae-ClientSSLSecureProtocols = \LIST:TLSv1.2,TLSv1.1,TLSv1
```

以下属性列出了密码套件。应对此表进行优先级排序。先添加优先级最高的密码套件，然后添加第二优先级套件，以此类推。该示例显示了一个缩略表：

```
pae-ClientSSLCipherSuites = \LIST:TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA
```

## 更改全局接受和建议策略

要更改安全协议和密码套件的全局接受和建议策略，需要使用“ADSI 编辑”实用程序编辑 View LDAP 属性。

### 前提条件

- 熟悉用于定义接受和建议策略的 View LDAP 属性。请参阅 [View LDAP 中定义的全局接受和建议策略](#)。
- 请参阅 Microsoft TechNet 网站，了解如何在您的 Windows Server 操作系统版本上使用“ADSI 编辑”实用程序。

### 步骤

- 1 在您的 View 连接服务器计算机上启动“ADSI 编辑”实用程序。
- 2 在控制台树中，选择**连接到**。
- 3 在**选择或键入可分辨名称或命名上下文**文本框中，键入可分辨名称 **DC=vdi, DC=vmware, DC=int**。
- 4 在**选择或键入域或服务器**文本框中，选择或键入 **localhost:389** 或 View 连接服务器计算机的完全限定域名 (FQDN)，后跟端口 389。  
  
例如：**localhost:389** 或 **mycomputer.mydomain.com:389**
- 5 展开“ADSI 编辑”树结构，接着展开 **OU=Properties**，选择 **OU=Global**，然后在右侧的窗格中选择 **OU=Common**。
- 6 在 **CN=Common, OU=Global, OU=Properties** 对象上，选择要更改的每个属性并键入一系列新的安全协议或密码套件。
- 7 如果您修改了 **pae-ServerSSLSecureProtocols**，在每个连接服务器实例和安全服务器上重新启动 Windows 服务 VMware Horizon View Security Gateway 组件。

修改 **pae-ClientSSLSecureProtocols** 后，您无需重新启动任何服务。

## 在单个服务器上配置接受策略

要在单个连接服务器实例或安全服务器上指定本地接受策略，必须在 **locked.properties** 文件中添加相关属性。如果服务器上还不存在 **locked.properties** 文件，则必须创建此文件。

您可以为每个要配置的安全协议添加一个 `secureProtocols.n` 条目。请使用以下语法：  
`secureProtocols.n=security protocol`。

您可以为每个要配置的密码套件添加一个 `enabledCipherSuite.n` 条目。请使用以下语法：  
`enabledCipherSuite.n=cipher suite`。

`n` 变量是在每个条目类型中按顺序添加的整数（1、2、3）。

您可以添加一个 `honorClientOrder` 条目以控制密码套件的优先级。通常，服务器的密码套件顺序无关紧要，因为使用的是客户端的顺序。要改为使用服务器的密码套件顺序，请使用以下语法：

```
honorClientOrder=false
```

请确保 `locked.properties` 文件中的条目语法正确，密码套件和安全协议的名称拼写无误。文件中出现任何错误都能导致客户端与服务器之间的协商失败。

### 步骤

- 1 在连接服务器或安全服务器计算机的 TLS/SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。  
 例如：`install_directory\VMware\VMware View\Server\sslgateway\conf\`
- 2 添加 `secureProtocols.n` 和 `enabledCipherSuite.n` 条目，包括关联的安全协议和密码套件。
- 3 保存 `locked.properties` 文件。
- 4 重新启动 VMware Horizon View 连接服务器服务或 VMware Horizon View 安全服务器服务，使所做的更改生效。

## 示例：单个服务器上的默认接受策略

以下示例显示了 `locked.properties` 文件中指定默认策略所需的条目：

```
# The following list should be ordered with the latest protocol first:

secureProtocols.1=TLSv1.2
secureProtocols.2=TLSv1.1

# This setting must be the latest protocol given in the list above:

preferredSecureProtocol=TLSv1.2

# The order of the following list is unimportant unless honorClientOrder is false:

enabledCipherSuite.1=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
enabledCipherSuite.2=TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
enabledCipherSuite.3=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
enabledCipherSuite.4=TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

# Use the client's ordering of cipher suites (ignores the ordering given above):

honorClientOrder=true
```



## 在远程桌面上配置建议策略

您可以在运行 Windows 的远程桌面上配置建议策略，以控制到连接服务器的消息总线连接的安全性。确保将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 启动远程桌面上的 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
```

## 在 Horizon 7 中禁用的旧协议和密码

默认情况下，将在 Horizon 7 中禁用不再视为安全的一些旧协议和密码。如果需要，您可以手动启用它们。

### DHE 密码套件

有关更多信息，请参阅 <http://kb.vmware.com/kb/2121183>。与 DSA 证书兼容的密码套件使用 Diffie-Hellman 临时密钥，从 Horizon 6 版本 6.2 开始，不再默认启用这些套件。

对于连接服务器实例、安全服务器和 Horizon 7 桌面，您可以按照本指南中所述，通过编辑 View LDAP 数据库、locked.properties 文件或注册表来启用这些密码套件。请参阅[更改全局接受和建议策略](#)、[在单个服务器上配置接受策略](#)和[在远程桌面上配置建议策略](#)。您可以定义一组密码套件，其中包含下面的一个或多个套件（按以下顺序）：

- TLS\_DHE\_DSS\_WITH\_AES\_128\_GCM\_SHA256（仅 TLS 1.2，不适用于 FIPS）
- TLS\_DHE\_DSS\_WITH\_AES\_256\_GCM\_SHA384（仅 TLS 1.2，不适用于 FIPS）
- TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA256（仅 TLS 1.2）
- TLS\_DHE\_DSS\_WITH\_AES\_128\_CBC\_SHA
- TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA256（仅 TLS 1.2）

## ■ TLS\_DHE\_DSS\_WITH\_AES\_256\_CBC\_SHA

对于 View Composer 和 View Agent Direct-Connection (VADC) 计算机，在执行《Horizon 7 安装指南》文档中的“在 SSL/TLS 中为 View Composer 和 Horizon Agent 计算机禁用弱密码”过程时，您可以通过在密码列表中添加以下内容来启用 DHE 密码套件。

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
```

**注** 无法为 ECDSA 证书启用支持。从不支持这些证书。

## SSLv3

在 Horizon 7 中，已移除 SSL 版本 3.0。

有关更多信息，请参阅 <http://tools.ietf.org/html/rfc7568>。

## RC4

有关更多信息，请参阅 <http://tools.ietf.org/html/rfc7465>。

对于连接服务器实例、安全服务器和 Horizon 7 桌面，您可以通过编辑配置文件 C:\Program Files\VMware\VMware View\Server\jre\lib\security\java.security，在连接服务器、安全服务器或 Horizon Agent 计算机上启用 RC4。该文件的末尾包含一个名为 `jdk.tls.legacyAlgorithms` 的多行条目。从该条目中移除 RC4\_128 及其后面的逗号，然后重新启动连接服务器、安全服务器或 Horizon Agent 计算机（视具体情况而定）。

对于 View Composer 和 View Agent Direct-Connection (VADC) 计算机，在执行《Horizon 7 安装指南》文档中的“在 SSL/TLS 中为 View Composer 和 Horizon Agent 计算机禁用弱密码”过程时，您可以通过在密码列表中添加以下内容来启用 RC4。

```
TLS_RSA_WITH_RC4_128_SHA
```

## TLS 1.0

在 Horizon 7 中，将默认禁用 TLS 1.0。

有关更多信息，请参阅 [https://www.pcisecuritystandards.org/documents/PCI\\_DSS\\_v3-1.pdf](https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf) 和 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf>。有关如何启用 TLS 1.0 的说明，请参阅《Horizon 7 升级指南》文档中的“对从连接服务器进行的 vCenter 连接启用 TLSv1”和“对从 View Composer 进行的 vCenter 和 ESXi 连接启用 TLSv1”部分。

# 为 Blast 安全网关配置安全协议和密码套件

# 6

连接服务器的安全设置不适用于 Blast 安全网关 (BSG)。您必须为 BSG 单独配置安全性设置。

## 为 Blast 安全网关 (BSG) 配置安全协议和密码套件

您可以通过编辑 `absg.properties` 文件来配置 BSG 的客户端侦听器接受的安全协议和密码套件。

允许使用的协议为 `tls1.0`、`tls1.1` 和 `tls1.2`（从低到高排序）。绝不允许使用 `SSLv3` 和更低版本的旧协议。`localHttpsProtocolLow` 和 `localHttpsProtocolHigh` 两个属性决定 BSG 侦听器将接受的协议范围。例如，设置 `localHttpsProtocolLow=tls1.0` 和 `localHttpsProtocolHigh=tls1.2` 将导致侦听器接受 `tls1.0`、`tls1.1` 和 `tls1.2`。默认设置是 `localHttpsProtocolLow=tls1.1` 和 `localHttpsProtocolHigh=tls1.2`。您可以通过检查 BSG 的 `absg.log` 文件来发现对于某个特定 BSG 实例有效的值。

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：

```
!aNULL:kECDH+AESGCM:ECDH+AESGCM:kECDH+AES:ECDH+AES
```

### 步骤

- 1 在连接服务器实例上，编辑 `install_directory\VMware\VMware View\Server\appblastgateway\absg.properties` 文件。

默认情况下，安装目录为 `%ProgramFiles%`。

- 2 编辑 `localHttpsProtocolLow` 和 `localHttpsProtocolHigh` 属性以指定协议范围。

例如，

```
localHttpsProtocolLow=tls1.0  
localHttpsProtocolHigh=tls1.2
```

要仅启用一个协议，请为 `localHttpsProtocolLow` 和 `localHttpsProtocolHigh` 指定相同的协议。

- 3 编辑 `localHttpsCipherSpec` 属性以指定密码套件列表。

例如，

```
localHttpsCipherSpec=!aNULL:kECDH+AESGCM:ECDH+AESGCM:kECDH+AES:ECDH+AES
```

#### 4 重新启动 Windows 服务 VMware Horizon Horizon 7 Blast 安全网关。

# 为 PCoIP 安全网关配置安全协议和密码套件

## 7

连接服务器的安全设置不适用于 PCoIP 安全网关 (PCoIP Secure Gateway, PSG)。您必须为 PSG 单独配置安全性设置。

## 为 PCoIP 安全网关 (PSG) 配置安全协议和密码套件

您可以通过编辑注册表来配置 PSG 的客户端侦听器接受的安全协议和密码套件。如果需要，也可以在 RDS 主机上执行此任务。

允许使用的协议为 **tls1.0**、**tls1.1** 和 **tls1.2**（从低到高排序）。绝不允许使用 **SSLv3** 和更低版本的旧协议。

以下是默认密码列表：

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:AES256-SHA256:AES256-SHA:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:AES128-SHA256:AES128-SHA:@STRENGTH
```

### 步骤

- 1 在连接服务器实例、安全服务器或 RDS 主机上，打开注册表编辑器，然后导航到 **HKLM\Software\Teradici\SecurityGateway**。
- 2 添加或编辑 **REG\_SZ** 注册表值 **SSLProtocol** 以指定协议列表。

例如，

```
tls1.2:tls1.1
```

- 3 添加或编辑 **REG\_SZ** 注册表值 **SSLCipherList** 以指定密码套件列表。

例如，

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256
```

# 在安全的 Horizon 7 环境中部署 USB 设备

## 8

USB 设备容易受到一种称为 BadUSB 的安全威胁，这使某些 USB 设备上的固件可能受到劫持，并被恶意软件取而代之。例如，可以使设备重定向网络流量或模拟键盘并捕获按键。可以配置 USB 重定向功能以防止 Horizon 7 部署出现此安全漏洞。

通过禁用 USB 重定向，可以防止任何 USB 设备重定向到用户的远程桌面和应用程序。或者，也可以禁用特定 USB 设备的重定向，只允许用户访问其远程桌面和应用程序上的特定设备。

是否执行这些步骤取决于您组织中的安全要求。这些步骤并不是强制性的。您可以安装 USB 重定向，并保持对 Horizon 7 部署中的所有 USB 设备启用此功能。至少，要慎重考虑组织应尝试限制其暴露于此安全漏洞的程度。

本章讨论了以下主题：

- 对所有类型的设备禁用 USB 重定向
- 对特定设备禁用 USB 重定向

## 对所有类型的设备禁用 USB 重定向

部分高度安全的环境要求您防止用户可能已连接到其客户端设备的所有 USB 设备重定向至其远程桌面和应用程序。您可以为所有桌面池、特定桌面池或桌面池中的特定用户禁用 USB 重定向。

选择以下适合您的情形的任何策略：

- 在桌面映像或 RDS 主机上安装 Horizon Agent 时，取消选中 **USB 重定向** 安装选项。（该选项默认为取消选中。）此方法可防止访问从桌面映像或 RDS 主机部署的所有远程桌面和应用程序上的 USB 设备。
- 在 Horizon Administrator 中，编辑特定池的 **USB 访问** 策略，以拒绝或允许访问。通过此方法，不必更改桌面映像，且可以控制对特定桌面和应用程序池中 USB 设备的访问。

只有全局 **USB 访问** 策略可用于已发布的桌面池和应用程序池。无法为单个已发布的桌面池或应用程序池设置此策略。

- 在 Horizon Administrator 中，当您在桌面或应用程序池级别设置策略后，可以通过选择 **用户覆盖** 设置和选择用户覆盖池中特定用户的策略。
- 根据需要在 Horizon Agent 端或在客户端将 **Exclude All Devices** 策略设置为 **true**。
- 使用智能策略创建一个策略，以禁用 **USB 重定向** Horizon 策略设置。通过此方法，您可以在满足特定条件的情况下禁用特定远程桌面上的 USB 重定向。例如，您可以配置一个策略，以在用户从您的企业网络外部连接到远程桌面时禁用 USB 重定向。

如果将 **Exclude All Devices** 策略设置为 **true**，Horizon Client 会阻止重定向所有 USB 设备。您可以使用其他策略设置以允许重定向指定设备或设备系列。如果将策略设置为 **false**，Horizon Client 将允许重定向所有 USB 设备（其他策略设置阻止的设备除外）。在 Horizon Agent 和 Horizon Client 上均可以设置此策略。下表显示了如何组合可以为 Horizon Agent 和 Horizon Client 设置的 **Exclude All Devices** 策略，从而为客户端计算机生成有效的策略。默认情况下，所有 USB 设备都可以被重定向，除非设备被阻止。

**表 8-1. 结合使用排除所有设备策略的影响**

在 Horizon Agent 上排除所有设备策略	在 Horizon Client 上排除所有设备策略	结合使用有效的排除所有设备策略
<b>false</b> 或未定义（包含所有 USB 设备）	<b>false</b> 或未定义（包含所有 USB 设备）	包含所有 USB 设备
<b>false</b> （包含所有 USB 设备）	<b>true</b> （排除所有 USB 设备）	排除所有 USB 设备
<b>true</b> （排除所有 USB 设备）	任意或未定义	排除所有 USB 设备

如果已将 **Disable Remote Configuration Download** 策略设置为 **true**，则 Horizon Agent 上 **Exclude All Devices** 的值不会传递给 Horizon Client，但 Horizon Agent 和 Horizon Client 会强制使用 **Exclude All Devices** 的本地值。

这些策略包含在 Horizon Agent 配置 ADMX 模板文件 (**vdm\_agent.admx**) 中。有关更多信息，请参阅《在 Horizon 7 中配置远程桌面功能》中的“Horizon Agent 配置 ADMX 模板中的 USB 设置”。

## 对特定设备禁用 USB 重定向

一些用户可能必须重定向特定的本地连接的 USB 设备，以便他们可以在其远程桌面或应用程序上执行任务。例如，某医生可能必须使用录音机 USB 设备录制患者的医疗信息。在这些情况下，无法禁止访问所有 USB 设备。您可以使用组策略设置启用或禁用特定设备的 USB 重定向。

对特定设备启用 USB 重定向之前，确保您信任与您企业中客户端计算机连接的物理设备。确保您信任您的供应链。如果可能，请跟踪 USB 设备的监管链。

此外，教育员工以确保他们不会从未知源连接设备。如果可能，将环境中的设备限制为仅接受已签发的固件更新、已通过 **FIPS 140-2 Level 3** 认证且不支持任何种类的字段可更新固件的设备。这些类型的 USB 设备供货困难，且根据您的设备要求可能无法找到。这些选择可能不实用，但它们值得考虑。

每个 USB 设备都具有其自己的供应商及用于在计算机上进行标识的产品 ID。通过配置 Horizon Agent 配置组策略设置，可以为已知的设备类型设置包含策略。通过此方法，可以消除允许将未知设备插入环境中的风险。

例如，可以防止除已知设备供应商和产品 ID **vid/pid=0123/abcd** 以外的所有设备重定向至远程桌面或应用程序：

```
ExcludeAllDevices    Enabled

IncludeVidPid        o:vid-0123_pid-abcd
```

**注** 此示例中的配置提供了保护措施，但是受到威胁的设备可报告任何 **vid/pid**，因此仍可能会发生潜在攻击。

默认情况下，Horizon 7 会阻止特定设备系列重定向至远程桌面或应用程序。例如，阻止 **HID**（人机接口设备）和键盘出现在客户机中。某些已发布的 **BadUSB** 代码以 USB 键盘设备为目标。

您可以防止特定设备系列重定向至远程桌面或应用程序。例如，可以阻止所有视频、音频和大容量存储设备：

```
ExcludeDeviceFamily    o:video;audio;storage
```

相反，可以通过防止重定向所有设备但允许使用特定设备系列来创建白名单。例如，可以阻止除存储设备以外的所有设备：

```
ExcludeAllDevices      Enabled
IncludeDeviceFamily    o:storage
```

当远程用户登录到桌面或应用程序并使其感染时，可能会出现其他风险。您可以防止 USB 访问来自公司防火墙外部的任何 Horizon 7 连接。可以从内部（而非外部）使用 USB 设备。

请注意，如果您阻止 TCP 端口 32111 以禁止从外部访问 USB 设备，将无法进行时区同步，因为端口 32111 也用于时区同步。对于零客户端，USB 流量将嵌入到 UDP 端口 4172 上的虚拟通道中。由于端口 4172 用于显示协议以及 USB 重定向，因此无法阻止端口 4172。如果需要，可以在零客户端上禁用 USB 重定向。有关详细信息，请参见零客户端产品文献或联系零客户端供应商。

设置策略以阻止特定设备系列或特定设备，可帮助缓解被 BadUSB 恶意软件感染的风险。这些策略不会缓解所有风险，但它们是整体安全策略的有效组成部分。

这些策略包含在 Horizon Agent 配置 ADMX 模板文件 (vdm\_agent.admx) 中。有关更多信息，请参阅《在 Horizon 7 中配置远程桌面功能》。



# 连接服务器和安全服务器上的 HTTP 保护措施

# 9

Horizon 7 采取某些措施以保护使用 HTTP 协议的通信。

本章讨论了以下主题：

- [Internet 工程任务组标准](#)
- [万维网联盟标准](#)
- [其他保护措施](#)
- [配置 HTTP 保护措施](#)

## Internet 工程任务组标准

连接服务器和安全服务器遵守一定的 Internet 工程任务组 (Internet Engineering Task Force, IETF) 标准。

- 默认启用 RFC 5746 传输层安全性 (TLS) - 重新协商标识扩展（又称为“安全重新协商”）。

---

**注** 默认情况下，将在连接服务器和安全服务器上禁用客户端启动的重新协商。要启用该功能，请编辑注册表值 [HKLM\SOFTWARE\VMware, Inc.\VMware VDM\plugins\wsnm\TunnelService\Params]JvmOptions 并从字符串中移除 **-Djdk.tls.rejectClientInitiatedRenegotiation=true**。

---

- 默认启用 RFC 6797 HTTP 严格传输安全性 (HSTS)（又称为“传输安全性”）。无法禁用此设置。
- 默认情况下，将启用 RFC 7034 HTTP 标头字段 X-Frame-Options（也称为“计数器点击劫持”）。您可以在 `locked.properties` 文件中添加 `x-frame-options=OFF` 条目以将其禁用。有关如何将属性添加到文件 `locked.properties` 的信息，请参见[配置 HTTP 保护措施](#)。

---

**注** 在 Horizon 7 版本 7.2 之前的版本中，更改此选项不会影响到 HTML Access 的连接。

---

- 默认情况下，将启用 RFC 6454 来源检查，这会防止跨站点请求伪造。您可以在 `locked.properties` 中添加 `checkOrigin=false` 条目以将其禁用。有关更多信息，请参阅[跨来源资源共享](#)。

---

**注** 在以前的版本中，将默认禁用该保护。

---

## 万维网联盟标准

连接服务器和安全服务器遵守一定的万维网联盟 (W3C) 标准。

- 跨来源资源共享 (Cross-Origin Resource Sharing, CORS) 会限制客户端的跨来源请求。您可以通过向 `locked.properties` 中添加条目 `enableCORS=true` 或 `enableCORS=false` 来启用或禁用此功能。
- 内容安全策略 (Content Security Policy, CSP) 可减少各类内容注入漏洞，默认情况下处于启用状态。您可以在 `locked.properties` 中添加 `enableCSP=false` 条目以将其禁用。

## 跨来源资源共享

跨来源资源共享 (CORS) 功能通过向客户端按需提供策略声明，并通过检查策略合规性请求，来控制客户端的跨来源请求。此功能可在需要进行配置和启用。

策略包含一组可获得接受的 HTTP 方法、请求的来源位置以及有效的具体内容类型。这些策略依据请求 URL 而异，可通过向 `locked.properties` 文件添加条目来根据需要进行重新配置。

属性名称后面的省略号表示该属性可以接受列表。

表 9-1. CORS 属性

属性	值的类型	主默认值	其他默认值
<code>enableCORS</code>	<code>true</code> <code>false</code>	<code>false</code>	<code>n/a</code>
<code>acceptContentType...</code>	<code>http-content-type</code>	<code>application/x-www-form-urlencoded,application/xml,text/xml</code>	<code>admin=application/x-amf</code> <code>newadmin=application/json,application/text,application/x-www-form-urlencoded</code> <code>portal=application/json</code> <code>sso-redirect=application/x-amf</code> <code>view-vlsi-rest=application/json</code>
<code>acceptHeader...</code>	<code>http-header-name</code>	<code>*</code>	<code>n/a</code>
<code>exposeHeader...</code>	<code>http-header-name</code>	<code>*</code>	<code>n/a</code>
<code>filterHeaders</code>	<code>true</code> <code>false</code>	<code>true</code>	<code>n/a</code>
<code>checkOrigin</code>	<code>true</code> <code>false</code>	<code>true</code>	<code>n/a</code>
<code>checkReferer</code>	<code>true</code> <code>false</code>	<code>false</code>	<code>n/a</code>

表 9-1. CORS 属性（续）

属性	值的类型	主默认值	其他默认值
allowCredentials	true false	false	admin=true broker=true misc=true newadmin=true portal=true saml=true sso-redirect=true tunnel=true view-vlsi=true view-vlsi-rest=true
allowMethod...	http-method-name	GET,HEAD,POST	misc=GET,HEAD saml=GET,HEAD sso-redirect=GET,HEAD
allowPreflight	true false	true	n/a
maxAge	cache-time	0	n/a
balancedHost	load-balancer-name	OFF	n/a
portalHost...	gateway-name	OFF	n/a
chromeExtension...	chrome-extension-hash	ppkfnjlimknmjoaempidmd lfchhehel	n/a
<p><b>注</b> 此值是适用于 Chrome 的 Horizon Client 的 Chrome 扩展 ID。</p>			

以下是 locked.properties 文件中 CORS 属性的示例。

```
enableCORS = true
allowPreflight = true
checkOrigin = true
checkOrigin-misc = false
allowMethod.1 = GET
allowMethod.2 = HEAD
allowMethod.3 = POST
allowMethod-saml.1 = GET
allowMethod-saml.2 = HEAD
acceptContentType.1 = application/x-www-form-urlencoded
acceptContentType.2 = application/xml
acceptContentType.3 = text/xml
```

## 来源检查

来源检查在默认情况下处于启用状态。启用后，将只有在没有来源或者来源与以下项相同时才会接受请求：外部 URL 指定的地址、**balancedHost** 地址、任何 **portalHost** 地址、任何 **chromeExtension** 哈希、**null** 或 **localhost**。如果来源不是这些项中的任何一个，则会记录“意外来源”(Unexpected Origin) 错误并返回 404 状态。

**注** 某些浏览器不会或不一定提供来源标头。（可选）在缺少来源标头的情况下，可以检查请求中的引用标头。引用标头的标头名称中包含一个“r”。要检查引用标头，请将以下属性添加到 **locked.properties** 文件中：

```
checkReferer=true
```

如果使用多个连接服务器主机或安全服务器进行负载平衡，您必须在 **locked.properties** 文件中添加一个 **balancedHost** 条目以指定负载平衡器地址。该地址使用端口 443。

如果客户端通过 **Unified Access Gateway** 设备或其他网关进行连接，您必须在 **locked.properties** 文件中添加 **portalHost** 条目以指定所有的网关地址。这些地址使用端口 443。您还必须指定 **portalHost** 条目，以通过与外部 URL 中指定的不同名称提供对连接服务器主机或安全服务器的访问。

Chrome 扩展客户端将初始来源设置为它们自己的身份。要成功进行连接，请在 **locked.properties** 文件中添加一个 **chromeExtension** 条目以注册此扩展。例如：

```
chromeExtension.1=bpifadopbphhpkkcfohecfadckmpjmd
```

## 内容安全策略

内容安全策略 (CSP) 功能通过向合规浏览器下达策略指令，可减少各类内容注入漏洞，如跨站点脚本 (XSS)。该功能在默认情况下为启用状态。通过向 **locked.properties** 中添加条目，可重新配置策略指令。

表 9-2. CSP 属性

属性	值的类型	主默认值	其他默认值
enableCSP	true false	true	n/a
content-security-policy	directives-list	default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe- eval' data:;style-src 'self' 'unsafe- inline';font-src 'self' data: ;frame-ancestors 'none'	newadmin = default-src 'self';script-src 'self' 'unsafe- inline' 'unsafe-eval' data:;style- src 'self' 'unsafe-inline';font-src 'self' data:;img-src 'self' data:;connect-src 'self' https:;frame-ancestors 'none' portal = default-src 'self';script-src 'self' 'unsafe- inline' 'unsafe-eval' data:;style- src 'self' 'unsafe-inline';font-src 'self' data:;img-src 'self' data: blob:;media-src 'self' blob:;connect-src 'self' wss:;frame-src 'self' blob:;child-src 'self' blob:;object-src 'self' blob:;frame-ancestors 'self'
x-content-type-options	OFF specification	nosniff	n/a
x-frame-options	OFF specification	deny	portal = sameorigin
x-xss-protection	OFF specification	1; mode=block	n/a

您可以将 CSP 属性添加到 `locked.properties` 文件中。示例 CSP 属性：

```
enableCSP = true
content-security-policy = default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval'
data:;style-src 'self'
'unsafe-inline';font-src 'self' data:
content-security-policy-newadmin = default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval'
data:;style-src 'self'
'unsafe-inline';font-src 'self' data:;img-src 'self' data:;connect-src 'self' https:
content-security-policy-portal = default-src 'self';script-src 'self' 'unsafe-inline' 'unsafe-eval'
data:;style-src 'self'
'unsafe-inline';font-src 'self' data:;img-src 'self' data: blob:;media-src 'self' blob:;connect-src
'self' wss:;frame-src
'self' blob:;child-src 'self' blob:;object-src 'self' blob:
x-content-type-options = nosniff
x-frame-options = deny
x-frame-options-portal = sameorigin
x-xss-protection = 1; mode=block
```

## 其他保护措施

除了 Internet 工程任务组和 W3 标准以外，Horizon 7 还采取其他措施以保护使用 HTTP 协议的通信。

### 减少 MIME 类型安全风险

默认情况下，Horizon 7 在其 HTTP 响应中发送 `x-content-type-options: nosniff` 标头以帮助防范基于 MIME 类型混淆的攻击。

您可以在 `locked.properties` 文件中添加以下条目以禁用该功能：

```
x-content-type-options=OFF
```

### 减轻跨站点脚本攻击

默认情况下，Horizon 7 在其 HTTP 响应中发送 `x-xss-protection=1; mode=block` 标头以使用 XSS（跨站点脚本）筛选功能减轻跨站点脚本攻击。

您可以在 `locked.properties` 文件中添加以下条目以禁用该功能：

```
x-xss-protection=OFF
```

### 内容类型检查

默认情况下，Horizon 7 仅接受具有以下声明的内容类型的请求：

- `application/x-www-form-urlencoded`
- `application/xml`
- `text/xml`

---

**注** 在以前的版本中，将默认禁用该保护。

---

要限制 View 接受的内容类型，请在 `locked.properties` 文件中添加以下条目：

```
acceptContentType.1=content-type
```

例如：

```
acceptContentType.1=x-www-form-urlencoded
```

要接受其他内容类型，请添加 `acceptContentType.2=content-type` 条目，依此类推。

要接受具有任何声明的内容类型的请求，请指定 `acceptContentType=*`。

---

**注** 在 Horizon 7 版本 7.2 之前的版本中，更改此列表不会影响到 Horizon Administrator 的连接。

---

## 客户端行为监控

连接服务器可用来处理客户端请求的资源有限，运行不正常的客户端可能会占用这些资源，从而无法为其他请求提供服务。客户端行为监控是一类可防止出现错误行为的检测和缓解措施。

### 握手监控

端口 443 上的 TLS 握手必须在可配置的时限内完成，否则将被强制终止。默认情况下，此时限为 10 秒。如果启用了智能卡身份验证，端口 443 上的 TLS 握手可以在 100 秒内完成。

如果需要，您可以通过在 `locked.properties` 文件中添加以下属性来调整端口 443 上的 TLS 握手时间：

```
handshakeLifetime = lifetime_in_seconds
```

例如：

```
handshakeLifetime = 20
```

（可选）可自动将导致 TLS 握手超时运行的客户端添加到黑名单中。请参阅[客户端黑名单](#)了解更多信息。

### 请求接收监控

HTTP 请求必须在 30 秒内完全接收，否则，连接将被强行终止。

或者，发送请求用时超过 30 秒的客户端可能会被自动添加到黑名单。请参阅[客户端黑名单](#)了解更多信息。

### 请求计数

单个客户端每分钟发送的 HTTP 请求数不应超过 100 个，尽管在超过此阈值时，默认情况下不会采取任何操作。

或者，超过此阈值的客户端可能会被自动添加到黑名单。请参阅[客户端黑名单](#)了解更多信息。

如果已启用客户端黑名单功能，您可能需要配置请求计数阈值。

您可以通过将以下属性添加至 `locked.properties` 文件来调整每个客户端的已处理 HTTP 请求的最大数量：

```
requestTallyThreshold = max_served_requests_in_30_seconds
```

例如：

```
requestTallyThreshold = 100
```

您可以通过将以下属性添加至 `locked.properties` 文件来调整每个客户端的失败 HTTP 请求的最大数量：

```
tarPitGraceThreshold = max_failed_requests_in_30_seconds
```

例如：

```
tarPitGraceThreshold = 5
```

## 客户端黑名单

这种类型的保护默认处于禁用状态，因为如果配置错误，可能会降低性能，让用户感到沮丧。如果使用网关（例如，**Unified Access Gateway** 设备），请勿启用客户端黑名单功能，因为网关会将所有客户端连接均显示为相同的 IP 地址。

如果启用此功能，来自黑名单上的客户端连接会被延迟一段可配置的时间，然后才会处理。如果来自同一客户端的多个连接同时被延迟，来自该客户端的后续连接会被拒绝，而不是延迟。可对此阈值进行配置。

您可以通过在 **locked.properties** 文件中添加以下属性来启用此功能：

```
secureHandshakeDelay = delay_in_milliseconds
```

例如：

```
secureHandshakeDelay = 2000
```

要禁用 HTTPS 连接的加入黑名单功能，请移除 **secureHandshakeDelay** 条目，或将其设置为 0。

发生 TLS 握手超时运行时，客户端的 IP 地址将被添加到黑名单中，最短时限为 **handshakeLifetime** 与 **secureHandshakeDelay** 之和。

使用以上示例中的值，运行不正常的客户端的 IP 地址被添加到黑名单的时限为 22 秒：

```
(20 * 1000) + 2000 = 22 seconds
```

每当来自相同 IP 地址的连接运行不正常时，都会延长该最短时限。在最短时限到期，并且也处理了来自相应 IP 地址的最后一次延迟连接后，便会将该 IP 地址从黑名单中移除。

TLS 握手超时运行不是将客户端加入黑名单的唯一原因。其他原因包括一系列已放弃的连接，或者一系列结果为错误的请求，例如，多次尝试访问不存在的 URL。这些不同触发因素的最短黑名单时限也各不相同。要将对这些其他触发因素的监控扩展到端口 80，请在 **locked.properties** 文件中添加以下条目：

```
insecureHandshakeDelay = delay_in_milliseconds
```

例如：

```
insecureHandshakeDelay = 1000
```

要禁用 HTTP 连接的加入黑名单功能，请移除 **insecureHandshakeDelay** 条目，或将其设置为 0。

## 行为监控属性

使用以下属性可监控客户端行为。以下属性包括可防止出现错误行为的检测和缓解属性。



表 9-3. 行为监控属性

属性	说明	默认值	动态
handshakeLifetime	TLS 握手的最长时间（以秒为单位）。	10 或 100（请参阅 <a href="#">握手监控</a> 。）	否
secureHandshakeDelay	打开加入黑名单功能时，在 TLS 握手之前的延迟时间（以毫秒为单位）。	0（加入黑名单功能关闭）	否
insecureHandshakeDelay	打开加入黑名单功能时，在非 TLS 握手之前的延迟时间（以毫秒为单位）。	0（加入黑名单功能关闭）	否
requestTallyThreshold	每 30 秒内客户端黑名单的已处理 HTTP 请求数。	50	否
tarPitGraceThreshold	每 30 秒内客户端黑名单的未处理 HTTP 请求数。	3	否
secureBlacklist...	打开加入黑名单功能时，端口 443 上立即拒绝的 IP 地址列表。	不适用	是
insecureBlacklist...	打开加入黑名单功能时，端口 80 上立即拒绝的 IP 地址列表。	不适用	是
secureWhitelist...	端口 443 上从黑名单中排除的 IP 地址列表。	不适用	是
insecureWhitelist...	端口 80 上从黑名单中排除的 IP 地址列表。	不适用	是

对动态条目的更改会立即生效，无需重新启动服务。

## 用户代理白名单

通过设置白名单可限制能够与 Horizon 7 交互的用户代理。默认情况下，接受所有用户代理。

**注** 这不是严格意义上的安全功能。用户代理检测依赖于连接客户端或浏览器提供的用户代理请求标头，而这类请求标头有可能被假冒。某些浏览器允许用户修改请求标头。

用户代理是由其名称和最低版本指定的。例如：

```
clientWhitelist-portal.1 = Chrome-14
clientWhitelist-portal.2 = Safari-5.1
```

这表示只允许 Google Chrome 版本 14 和更高版本，以及 Safari 版本 5.1 和更高版本使用 HTML Access 进行连接。所有浏览器都可以连接到其他服务。

您可以输入以下可识别用户代理名称：

- Android
- Chrome
- Edge

- IE
- Firefox
- Opera
- Safari

**注** Horizon 7 并非支持所有这些用户代理。这些是用户代理示例。

## 配置 HTTP 保护措施

要配置 HTTP 保护措施，您必须在连接服务器或安全服务器实例上的 SSL 网关配置文件夹中创建或编辑 `locked.properties` 文件。

例如，`install_directory\VMware\VMware View\Server\sslgateway\conf\locked.properties`。

- 使用以下语法配置 `locked.properties` 中的属性：

```
myProperty = newValue
```

- 属性名称始终区分大小写，而值可能区分大小写。= 符号两侧的空格是可选的。
- 对于 CORS 和 CSP 属性，既可以设置特定于服务的值，也可以设置主值。例如，管理员服务负责处理 Horizon Administrator 请求，可通过在属性名称后面附加 `-admin`，来为该服务设置相应属性，而不影响其他服务。

```
myProperty-admin = newValueForAdmin
```

- 如果指定了主值和特定于服务的值，则特定于服务的值适用于指定服务，而主值适用于所有其他服务。其唯一例外是特殊值 “OFF”。如果属性的主值设置为 “OFF”，将忽略此属性的所有特定于服务的值。

例如：

```
myProperty = OFF
myProperty-admin = newValueForAdmin    ; ignored
```

- 某些属性可以接受值列表。

要设置单个值，请输入以下属性：

```
myProperty = newValue
myProperty-admin = newValueForAdmin
```

要为接受列表值的属性设置多个值，您可以在单独的行上指定每个值：

```
myProperty.1 = newValue1
myProperty.2 = newValue2
myProperty-admin.1 = newValueForAdmin1
myProperty-admin.2 = newValueForAdmin2
```

- 要确定在进行特定于服务的配置时所使用的正确服务名称，请在调试日志中查找包含以下序列的行：

```
(ajp:admin:Request21) Request from abc.def.com/10.20.30.40: GET /admin/
```

在此示例中，服务名称为 **admin**。您可以使用以下典型的服务名称：

- **admin** (Horizon Administrator)
- **newadmin** (Horizon Console)
- **broker** (连接服务器)
- **docroot** (本地文件服务)
- **portal** (HTML Access)
- **saml** (SAML 通信) (VIDM)
- **tunnel** (安全隧道)
- **view-vlsi** (View API)
- **misc** (其他)