

Horizon 7 管理指南

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

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
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

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

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

目录

Horizon 7 管理指南 6

1 使用 Horizon Administrator 7

- Horizon Administrator 和 Horizon 连接服务器 7
- 登录到 Horizon Administrator 8
- 有关使用 Horizon Administrator 界面的提示 8
- 排除 Horizon Administrator 中的文本显示故障 10

2 配置 Horizon 连接服务器 11

- 配置 vCenter Server 和 View Composer 11
- 备份 Horizon 连接服务器 23
- 配置客户端会话设置 23
- 禁用或启用 Horizon 连接服务器 35
- 编辑外部 URL 35
- 加入或退出客户体验计划 36
- View LDAP 目录 37

3 设置智能卡身份验证 39

- 使用智能卡登录 39
- 在 Horizon 连接服务器上配置智能卡身份验证 40
- 在第三方解决方案上配置智能卡身份验证 45
- 为智能卡身份验证准备 Active Directory 46
- 验证智能卡身份验证配置 48
- 使用智能卡证书撤销检查 49

4 设置其他类型的用户身份验证 53

- 使用双因素身份验证 53
- 使用 SAML 身份验证 57
- 配置生物身份验证 62

5 在不需要凭据的情况下对用户进行身份验证 64

- 为已发布的应用程序提供未验证访问 64
- 为用户配置混合登录 70
- 使用基于 Windows 的 Horizon Client 所提供的“以当前用户身份登录”功能 71
- 在移动和 Mac Horizon Client 中保存凭据 72
- 设置 True SSO 73

- 6 配置基于角色的委托管理 97**
 - [了解角色和特权 97](#)
 - [使用访问组委派池和场的管理权 98](#)
 - [了解权限 99](#)
 - [对管理员进行管理 100](#)
 - [管理和查看权限 101](#)
 - [管理和查看访问组 103](#)
 - [管理自定义角色 105](#)
 - [预定义的角色和特权 107](#)
 - [执行常见任务所需的特权 111](#)
 - [针对管理员用户和组的最佳实践 113](#)
- 7 在 Horizon Administrator 和 Active Directory 中配置策略 115**
 - [在 Horizon Administrator 中设置策略 115](#)
 - [使用 Horizon 7 组策略管理模板文件 117](#)
- 8 维护 Horizon 7 组件 124**
 - [备份和还原 Horizon 7 配置数据 124](#)
 - [监控 Horizon 7 组件 132](#)
 - [监视计算机状态 133](#)
 - [了解 Horizon 7 服务 134](#)
 - [更改产品许可证密钥 135](#)
 - [监视产品许可证使用情况 136](#)
 - [从 Active Directory 更新常规用户信息 137](#)
 - [将 View Composer 迁移至另一台计算机 138](#)
 - [更新连接服务器实例、安全服务器或 View Composer 上的证书 143](#)
 - [客户体验改进计划 144](#)
- 9 在 Horizon Administrator 中管理 ThinApp 应用程序 145**
 - [Horizon 7 对 ThinApp 应用程序的要求 145](#)
 - [捕获和存储应用程序包 146](#)
 - [将 ThinApp 应用程序分配到计算机和桌面池 149](#)
 - [在 Horizon Administrator 中维护 ThinApp 应用程序 156](#)
 - [在 Horizon Administrator 中监视 ThinApp 应用程序并进行故障排除 159](#)
 - [ThinApp 配置示例 162](#)
- 10 设置 Kiosk 模式的客户端 164**
 - [配置 Kiosk 模式的客户端 164](#)
- 11 对 Horizon 7 进行故障排除 174**
 - [使用 Horizon Help Desk Tool 174](#)

- 使用 VMware 登录监视器 184
- 使用 VMware Horizon 性能跟踪器 188
- 监视系统运行状况 191
- 在 Horizon 7 中监视事件 192
- 收集 Horizon 7 的诊断信息 193
- 更新支持请求 197
- 排除安全服务器与 Horizon 连接服务器配对失败的故障 197
- 排除 Horizon 7 Server 证书撤销检查中的故障 198
- 排除智能卡证书撤销检查中的故障 199
- 更多故障排除信息 200

12 使用 vdmadmin 命令 201

- vdmadmin 命令用法 202
- 使用 -A 选项在 Horizon Agent 中配置日志 204
- 使用 -A 选项覆盖 IP 地址 206
- 使用 -F 选项更新外部安全主体 208
- 使用 -H 选项列出并显示运行状况监视器 208
- 使用 -I 选项列出并显示 Horizon 7 运行报告 210
- 使用 -I 选项以 Syslog 格式生成 Horizon 7 事件日志消息 211
- 使用 -L 选项分配专用计算机 212
- 使用 -M 选项显示有关计算机的信息 213
- 使用 -M 选项回收虚拟机上的磁盘空间 215
- 使用 -N 选项配置域过滤器 216
- 配置域过滤器 218
- 使用 -O 和 -P 选项显示未授权用户的计算机和策略 222
- 使用 -Q 选项在 Kiosk 模式下配置客户端 223
- 使用 -R 选项显示计算机的首个用户 228
- 使用 -S 选项移除连接服务器实例或安全服务器条目 228
- 使用 -T 选项为管理员提供辅助凭据 229
- 使用 -U 选项显示用户信息 231
- 使用 -V 选项解锁或锁定虚拟机 231
- 使用 -X 选项检测 and 解决 LDAP 条目和模式冲突 233

Horizon 7 管理指南

《Horizon 7 管理指南》介绍了如何配置和管理 VMware Horizon[®] 7，其中包括如何在 Horizon Administrator 中配置 Horizon 连接服务器、创建管理员、设置用户身份验证、配置策略以及管理 VMware ThinApp[®] 应用程序。本文档还介绍了如何对 Horizon 7 组件进行维护和故障排除。

目标读者

本文档中的信息面向任何需要配置和管理 VMware Horizon 7 的人员。本文档中的信息专门为已熟练掌握虚拟机技术和数据中心操作、并具有丰富经验的 Windows 或 Linux 系统管理员编写。

使用 Horizon Administrator

Horizon Administrator 是一个 Web 界面，您可以通过此界面配置 Horizon 连接服务器并管理远程桌面和应用程序。

有关您使用 Horizon Administrator、cmdlet 和 vdmadmin 所能执行操作的对比，请参阅《Horizon 7 集成指南》文档。

本章讨论了以下主题：

- [Horizon Administrator 和 Horizon 连接服务器](#)
- [登录到 Horizon Administrator](#)
- [有关使用 Horizon Administrator 界面的提示](#)
- [排除 Horizon Administrator 中的文本显示故障](#)

Horizon Administrator 和 Horizon 连接服务器

Horizon Administrator 为 Horizon 7 提供了基于 Web 的管理界面。

Horizon 连接服务器可以具有多个实例来作为副本服务器或安全服务器。根据您的 Horizon 7 部署，您可以对每个连接服务器实例获取一个 Horizon Administrator 界面。

可使用以下最佳做法将 Horizon Administrator 与连接服务器配合使用：

- 使用连接服务器的主机名和 IP 地址登录到 Horizon Administrator。使用 Horizon Administrator 界面管理连接服务器以及任何关联的安全服务器或副本服务器。
- 在容器环境中，确认所有管理员使用同一连接服务器的主机名和 IP 地址登录到 Horizon Administrator。不要使用负载均衡器的主机名和 IP 地址访问 Horizon Administrator 网页。
- 为了确定您所使用的连接服务器容器，您可以查看 Horizon Administrator 标题和 Web 浏览器选项卡中的容器名称。

注 如果使用 Unified Access Gateway 设备而不是安全服务器，您必须使用 Unified Access Gateway REST API 管理 Unified Access Gateway 设备。早期版本的 Unified Access Gateway 称为 Access Point。有关更多信息，请参阅《部署和配置 Unified Access Gateway》。

登录到 Horizon Administrator

要执行初始配置任务，必须登录到 Horizon Administrator。您可以通过安全 (TLS) 连接访问 Horizon Administrator。

前提条件

- 确认已在专用计算机上安装 Horizon 连接服务器。
- 确认您使用的是 Horizon Administrator 支持的 Web 浏览器。有关 Horizon Administrator 的要求，请参阅《Horizon 7 安装指南》文档。

步骤

- 1 打开 Web 浏览器并输入以下 URL，其中 **server** 是连接服务器实例的主机名。

https://server/admin

注 当主机名不可解析时，如果您需要访问连接服务器实例，则可以使用 IP 地址。但是，您连接的主机将与为连接服务器实例配置的 TLS 证书不匹配，从而导致访问被阻止或访问的安全性降低。

对 Horizon Administrator 的访问取决于连接服务器计算机上配置的证书类型。

如果在连接服务器主机上打开 Web 浏览器，请使用 **https://127.0.0.1**（而非 **https://localhost**）进行连接。该方法可以避免在解析 **localhost** 时遭受潜在 DNS 攻击，从而提高安全性。

选项	说明
为 View 连接服务器配置一个由 CA 签发的证书。	首次连接时，您的 Web 浏览器会显示 Horizon Administrator。
配置了 View 连接服务器提供的默认自签名证书。	第一次连接时，Web 浏览器可能会显示一个页面，警告与该地址相关联的安全证书不是由受信任的证书颁发机构颁发的。 单击 忽略 可继续使用当前的 TLS 证书。

- 2 使用具有管理员角色的帐户登录。

当您在副本组中安装独立的连接服务器实例或第一个连接服务器实例时，可以为管理员角色指定首个分配。默认情况下，会选择安装连接服务器时使用的帐户，但您也可以将此帐户更改为管理员本地组或域的全局组。

如果您选择管理员本地组，那么您可以使用直接添加到此组或通过全局组成员资格添加到此组的任何域用户。您不能使用添加到此组的本地用户。

登录到 Horizon Administrator 后，您可以使用 **View 配置 > 管理员**来更改具有管理员角色的用户和组列表。

有关使用 Horizon Administrator 界面的提示

您可以使用 Horizon Administrator 用户界面的功能在 Horizon 页面中导航以及对 Horizon 对象进行查找、筛选和排序。

Horizon Administrator 中包含许多常见用户界面功能。例如，每个页面左侧的导航窗格都可将您引导至其他 Horizon Administrator 页面。使用搜索过滤器可以选择与搜索对象相关的过滤条件。

下表介绍了其他一些可帮助您使用 Horizon Administrator 的功能。

表 1-1. Horizon Administrator 导航和显示功能

Horizon Administrator 功能	说明
在 Horizon Administrator 页面中前后导航	<p>单击浏览器的后退按钮，转到之前显示的 Horizon Administrator 页面。单击前进按钮返回当前页面。</p> <p>如果您在使用 Horizon Administrator 向导或对话框时单击浏览器的后退按钮，则会返回到 Horizon Administrator 主页面。您在向导或对话框中输入的信息将丢失。</p> <p>在低于 View 5.1 的版本中，无法使用浏览器的后退和前进按钮在 Horizon Administrator 内导航。Horizon Administrator 窗口提供单独的后退和前进按钮进行导航。这些按钮在 View 5.1 版本中已删除。</p>
将 Horizon Administrator 页面加入书签	您可以在浏览器中将 Horizon Administrator 页面加入书签。
多列排序	<p>通过使用多列排序功能，您可以按多种方式对 Horizon 对象进行排序。</p> <p>单击 Horizon Administrator 表第一行中的标题，可根据该标题按字母顺序对 Horizon 对象进行排序。</p> <p>例如，在资源 > 计算机页面中，您可以单击桌面池以按桌面所在的池对桌面进行排序。数字 1 将显示在标题旁边，表示它是主要排序列。您可以再次单击该标题，以便反转排序顺序。排序顺序由向上或向下箭头表示。</p> <p>要使用辅助项对 Horizon 对象进行排序，请按住 Ctrl 键并单击另一个标题。</p> <p>例如，在“计算机”表中，您可以单击用户，根据桌面专属的用户执行辅助排序。数字 2 将显示在辅助标题旁边。在此示例中，桌面将按池以及每个池中的用户进行排序。您可以继续按住 Ctrl 键按重要性对表中的所有列进行降序排序。</p> <p>按下 Ctrl+Shift 组合键同时单击某个排序项可将该项取消。</p> <p>例如，您可能希望显示池中处于特定状态且存储在特定数据存储中的桌面。您可以选择资源 > 计算机，单击数据存储标题，然后按住 Ctrl 键并单击状态标题。</p>
自定义表列	<p>您可以通过隐藏选定列并锁定第一列来自定义 Horizon Administrator 表列的显示。利用此功能，您可以控制包含许多列的大型表（如目录 > 桌面池）的显示。</p> <p>右键单击任意列标题，显示用于执行以下操作的上下文菜单：</p> <ul style="list-style-type: none"> ■ 隐藏选定列。 ■ 自定义各列。对话框显示表中的所有列。您可以选择要显示或隐藏的列。 ■ 锁定第一列。此选项强制最左侧的列在您水平滚动包含多列的表时一直显示。例如，在目录 > 桌面池页面中，桌面 ID 会在您水平滚动以查看其他桌面特征时一直显示。
选择 Horizon 对象和显示 Horizon 对象的详细信息	<p>在列出 Horizon 对象的 Horizon Administrator 表中，可以选择对象或显示对象详细信息。</p> <ul style="list-style-type: none"> ■ 要选择一个对象，请在表中单击该对象行的任意位置。在页面顶端，用来管理该对象的菜单和命令将会激活。 ■ 要显示对象详细信息，请双击对象行中的左侧单元格。此时将出现一个新的页面，其中会显示该对象的详细信息。 <p>例如，在目录 > 桌面池页面中，单击某个池的行中的任意位置可激活影响该池的命令。双击左侧列中的 ID 单元格将显示一个新的页面，其中包含了该池的详细信息。</p>

表 1-1. Horizon Administrator 导航和显示功能（续）

Horizon Administrator 功能	说明
展开对话框以查看详细信息	您可以展开 Horizon Administrator 对话框以查看详细信息，如表列中的桌面名称和用户名。 要展开对话框，请将鼠标放在对话框右下角的点上并拖动该角。
显示 Horizon 对象的上下文菜单	您可以右键单击 Horizon Administrator 表中的 Horizon 对象以显示上下文菜单。通过上下文菜单，您可以访问对选定 Horizon 对象执行操作的命令。 例如，在目录 > 桌面池页面中，您可以右键单击桌面池以显示添加、编辑、删除、禁用 (或启用) 置备等命令。

排除 Horizon Administrator 中的文本显示故障

如果您的 Web 浏览器在非 Windows 操作系统（如 Linux、UNIX 或 Mac OS）上运行，Horizon Administrator 中的文本会无法正常显示。

问题

Horizon Administrator 界面中的文本显示为乱码。例如，单词中间出现空格。

原因

Horizon Administrator 需要使用 Microsoft 专用字体。

解决方案

在计算机上安装 Microsoft 专用字体。

目前，Microsoft 网站不提供 Microsoft 字体，但您可以从其他独立网站进行下载。

配置 Horizon 连接服务器

当您安装 Horizon 连接服务器并对其执行初始配置后，可以向 Horizon 7 部署中添加 vCenter Server 实例和 View Composer 服务，设置可委托管理员职责的角色，以及计划配置数据的备份。

本章讨论了以下主题：

- 配置 vCenter Server 和 View Composer
- 备份 Horizon 连接服务器
- 配置客户端会话设置
- 禁用或启用 Horizon 连接服务器
- 编辑外部 URL
- 加入或退出客户体验计划
- View LDAP 目录

配置 vCenter Server 和 View Composer

要将虚拟机用作远程桌面，必须配置 View，使其与 vCenter Server 通信。要创建和管理链接克隆桌面池，必须在 Horizon Administrator 中配置 View Composer 设置。

也可为 Horizon 7 配置存储设置。您可允许 ESXi 主机回收链接克隆虚拟机上的磁盘空间。为了允许 ESXi 主机缓存虚拟机数据，您必须为 vCenter Server 启用 View Storage Accelerator。

为 View Composer AD 操作创建用户帐户

如果使用 View Composer，则必须在 Active Directory 中创建一个用户帐户，以允许 View Composer 在 Active Directory 中执行特定操作。View Composer 需要使用该帐户将链接克隆虚拟机加入到您的 Active Directory 域中。

为确保安全性，您应当创建一个单独的用户帐户，以供 View Composer 使用。通过创建单独的帐户，可以确保该帐户不具有针对其他目的定义的额外特权。您可以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，View Composer 帐户不需要域管理员特权。

步骤

- 1 在 Active Directory 中，在您的连接服务器主机所在的域或某个受信任的域中创建一个用户帐户。

- 2 在用于创建和接收链接克隆计算机帐户的 **Active Directory** 容器中，授予该帐户**创建计算机对象**、**删除计算机对象**和**写入全部属性**权限。

以下列表显示了该用户帐户需要的所有权限，包括默认分配的权限：

- 列出内容
- 读取全部属性
- 写入全部属性
- 读取权限
- 重置密码
- 创建计算机对象
- 删除计算机对象

注 如果为桌面池选择**允许重用预先存在的计算机帐户**设置，则所需的权限较少。确保已将以下权限分配给用户帐户：

- 列出内容
- 读取全部属性
- 读取权限
- 重置密码

- 3 确保该用户帐户的权限可应用于 **Active Directory** 容器及其所有子对象。

后续步骤

在 **Horizon Administrator** 中执行以下操作时指定该帐户：在“添加 vCenter Server”向导中配置 **View Composer** 域，以及配置和部署链接克隆桌面池。

将 vCenter Server 实例添加到 Horizon 7

您必须将 **Horizon 7** 配置为连接到 **Horizon 7** 部署中的 **vCenter Server** 实例。**vCenter Server** 可创建并管理 **Horizon 7** 在桌面池中使用的虚拟机。

如果是在链接模式组中运行 **vCenter Server** 实例，就必须将每个 **Horizon 7** 实例分别添加到 **View Manager**。

Horizon 7 使用安全通道 (SSL) 连接至 **vCenter Server** 实例。

前提条件

- 安装连接服务器产品许可证密钥。
- 准备一个有权在 **vCenter Server** 中执行支持 **Horizon 7** 所需操作的 **vCenter Server** 用户。要使用 **View Composer**，您必须为该用户授予额外的特权。

有关为 **Horizon 7** 配置 **vCenter Server** 用户的详细信息，请参阅《**Horizon 7 安装指南**》文档。

- 确认 vCenter Server 主机上安装了 TLS/SSL 服务器证书。在生产环境中，安装由受信任证书颁发机构 (Certificate Authority, CA) 签名的有效证书。

在测试环境中，您可以使用随 vCenter Server 一起安装的默认证书，但在 Horizon 7 中添加 vCenter Server 时必须接受证书指纹。

- 确认副本组中的所有连接服务器实例都信任 vCenter Server 主机上安装的服务器证书的根 CA 证书。检查根 CA 证书是否位于连接服务器主机上 Windows 本地计算机证书存储区中的受信任的根证书颁发机构 > 证书文件夹中。如果没有，请将根 CA 证书导入 Windows 本机证书存储区。

请参阅《Horizon 7 安装指南》文档中的“将根证书和中间证书导入 Windows 证书存储区”。

- 确认 vCenter Server 实例包含 ESXi 主机。如果 vCenter Server 实例中未配置主机，则无法在 Horizon 7 中添加实例。
- 如果您要升级到 vSphere 5.5 或更高版本，请确认您用作 vCenter Server 用户的域管理员帐户已由 vCenter Server 本地用户明确分配了登录 vCenter Server 的权限。
- 如果您计划以 FIPS 模式使用 Horizon 7，请确认您具有 vCenter Server 6.0 或更高版本以及 ESXi 6.0 或更高版本的主机。

有关更多信息，请参阅《Horizon 7 安装指南》文档中的“以 FIPS 模式安装 Horizon 7”。

- 熟悉用于确定 vCenter Server 和 View Composer 最大操作数限制的设置。请参阅 [vCenter Server](#) 和 [View Composer](#) 的并发操作数限制和设置并发电源操作率来支持远程桌面登录风暴。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。
- 2 在 **vCenter Server** 选项卡上，单击**添加**。
- 3 在 vCenter Server 设置**服务器地址**文本框中，键入 vCenter Server 实例的完全限定域名 (FQDN)。

FQDN 包含主机名和域名。例如，在 FQDN *myserverhost.companydomain.com* 中，*myserverhost* 是主机名，*companydomain.com* 是域名。

注 如果通过 DNS 名称或 URL 来输入服务器，则 Horizon 7 不会执行 DNS 查找来确认管理员之前是否是否使用 IP 地址将该服务器添加到 Horizon 7 中的。如果同时使用 DNS 名称和 IP 地址添加 vCenter Server，则会发生冲突。

- 4 键入 vCenter Server 用户的名称。
例如：**domain\user** 或 **user@domain.com**
- 5 键入 vCenter Server 用户密码。
- 6 （可选）键入该 vCenter Server 实例的描述。
- 7 键入 TCP 端口号。
默认端口为 443。
- 8 在“高级设置”下，设置 vCenter Server 和 View Composer 操作的并发操作数限制。
- 9 单击**下一步**显示 View Composer 设置页面。

后续步骤

配置 View Composer 设置。

- 如果为 vCenter Server 实例配置了 SSL 签名证书，且连接服务器信任根证书，则“添加 vCenter Server”向导会显示“View Composer 设置”页面。
- 如果为 vCenter Server 实例配置了默认证书，则必须先确定是否接受现有证书的指纹。请参阅[接受默认 TLS 证书的指纹](#)。

如果 Horizon 7 使用多个 vCenter Server 实例，请重复执行此步骤添加其他 vCenter Server 实例。

配置 View Composer 设置

要使用 View Composer，必须配置允许 Horizon 7 连接到 VMware Horizon View Composer 服务的设置。View Composer 可安装在独立的主机上，也可与 vCenter Server 安装在同一主机上。

在每个 VMware Horizon View Composer 服务和 vCenter Server 实例之间必须存在一对一的映射关系。每个 View Composer 服务仅适用于一个 vCenter Server 实例。每个 vCenter Server 实例仅能与一个 VMware Horizon View Composer 服务相关联。

完成 Horizon 7 的初始部署后，您可将 VMware Horizon View Composer 服务迁移到一个新的主机以支持不断增长和变化的 Horizon 7 部署。您可编辑 Horizon Administrator 中的初始 View Composer 设置，但是必须执行附加步骤来确保迁移成功。请参阅[将 View Composer 迁移至另一台计算机](#)。

前提条件

- 确认您在 Active Directory 中创建了一个有权从您的链接克隆所在 Active Directory 域添加和删除虚拟机的用户。请参阅[为 View Composer AD 操作创建用户帐户](#)。
- 确认您已将 Horizon 7 配置为连接到 vCenter Server。为此，您必须完成“添加 vCenter Server”向导中的“vCenter Server 信息”页面。请参阅[将 vCenter Server 实例添加到 Horizon 7](#)。
- 确认该 VMware Horizon View Composer 服务尚未配置为连接到不同的 vCenter Server 实例。

步骤

- 1 在 Horizon Administrator 中，完成“添加 vCenter Server”向导中的“vCenter Server 信息”页面。
 - a 选择 **View 配置 > 服务器**。
 - b 在 **vCenter Server** 选项卡上，单击**添加**并提供 vCenter Server 设置。
- 2 在“View Composer 设置”页面上，如果您未使用 View Composer，则请选择**不使用 View Composer**。

如果选择**不使用 View Composer**，则其他的 View Composer 设置将无效。单击**下一步**后，“添加 vCenter Server”向导会显示“存储设置”页面，但不会显示“View Composer 域”页面。

3 如果使用 View Composer，请选择 View Composer 主机的位置。

选项	说明
View Composer 与 vCenter Server 安装在同一主机上。	a 选择 View Composer 与 vCenter Server 一同安装 。 b 确保端口号与您在 vCenter Server 上安装 VMware Horizon View Composer 服务时指定的端口号相一致。默认端口号为 18443。
View Composer 安装在独立的主机上。	a 选择 独立的 View Composer Server 。 b 在 View Composer Server 地址文本框中，键入 View Composer 主机的完全限定域名 (FQDN)。 c 键入 View Composer 用户的名称。 例如: domain.com\user 或 user@domain.com d 键入 View Composer 用户的密码。 e 确保端口号与您安装 VMware Horizon View Composer 服务时指定的端口号相一致。默认端口号为 18443。

4 单击下一步显示“View Composer 域”页面。

后续步骤

配置 View Composer 域。

- 如果为 View Composer 实例配置了 TLS 签名证书，且连接服务器信任根证书，则“添加 vCenter Server”向导会显示“View Composer 域”页面。
- 如果为 View Composer 实例配置了默认证书，则必须先确定是否接受现有证书的指纹。请参阅[接受默认 TLS 证书的指纹](#)。

配置 View Composer 域

您必须配置一个 Active Directory 域，以便 View Composer 在其中部署链接克隆桌面。可以为 View Composer 配置多个域。先将 vCenter Server 和 View Composer 设置添加到 View 后，即可通过在 Horizon Administrator 中编辑 vCenter Server 实例来添加更多 View Composer 域。

前提条件

- 您的 Active Directory 管理员必须为 AD 操作创建 View Composer 用户。此域用户必须具有在包含链接克隆的 Active Directory 域中添加和移除虚拟机的权限。有关此用户所需权限的信息，请参阅[View Composer AD 操作创建用户帐户](#)。
- 在 Horizon Administrator 中，确认您已完成“添加 vCenter Server”向导中的“vCenter Server 信息”和“View Composer 设置”页面。

步骤

- 1 在“View Composer 域”页面中，单击**添加**为 AD 操作帐户信息添加 View Composer 用户。
- 2 键入 Active Directory 域的域名。

例如: **domain.com**

3 键入 View Composer 用户的域用户名，包括域名。

例如：`domain.com\admin`

4 键入帐户密码。

5 单击**确定**。

6 要添加在部署链接克隆池的其他 Active Directory 域中具有特权的域用户帐户，请重复以上的步骤。

7 单击**下一步**显示“存储设置”页面。

后续步骤

启用虚拟机磁盘空间回收，并为 Horizon 7 配置 View Storage Accelerator。

允许 vSphere 回收链接克隆虚拟机中的磁盘空间

在 vSphere 5.1 及更高版本中，可以启用 Horizon 7 的磁盘空间回收功能。从 vSphere 5.1 开始，Horizon 7 能够以高效的磁盘格式创建链接克隆虚拟机，这种磁盘格式允许 ESXi 主机回收链接克隆中未使用的磁盘空间，从而减少链接克隆所需的总存储空间。

随着用户与链接克隆桌面的交互，克隆的操作系统磁盘会逐渐增大，最终会使用几乎与完整克隆桌面相同的磁盘空间。磁盘空间回收有助于减少操作系统磁盘的大小，无需刷新或重构链接克隆。在虚拟机处于开启状态时以及用户与远程桌面交互时，都可以回收空间。

对于无法利用存储空间节省策略（例如，注销时刷新）的部署来说，磁盘空间回收功能尤其有用。例如，在专用远程桌面上安装用户应用程序的知识型员工在远程桌面刷新或重构时，可能会丢失自己的个人应用程序。通过磁盘空间回收，Horizon 7 可以将链接克隆的大小保持在接近于这些克隆初次置备后启动时的较小大小。

此功能由两部分组成：节省空间的磁盘格式和空间回收操作。

在 vSphere 5.1 或更高版本环境中，如果父虚拟机的虚拟硬件版本为 9 或更高版本，无论是否启用空间回收操作，Horizon 7 都会创建具有能节省空间的操作系统磁盘的链接克隆。

要启用空间回收操作，您必须使用 Horizon Administrator 启用 vCenter Server 的空间回收，并回收各桌面池的虚拟机磁盘空间。vCenter Server 的空间回收设置支持您在所有受 vCenter Server 实例管理的桌面池上禁用此功能。禁用 vCenter Server 的该功能会覆盖桌面池级别的设置。

以下指导原则适用于空间回收功能：

- 仅对链接克隆上能节省空间的操作系统磁盘有效。
- 这不会影响 View Composer 永久磁盘。
- 仅适用于 vSphere 5.1 或更高版本且虚拟硬件版本为 9 或更高版本的虚拟机。
- 不适用于完整克隆桌面。
- 适用于具有 SCSI 控制器的虚拟机。不支持 IDE 控制器。

如果池中包含具有能节省空间的磁盘的虚拟机，则不支持本地 NFS 快照技术 (VAAI)。

前提条件

- 确认 vCenter Server 和 ESXi 主机（包括群集中的所有 ESXi 主机）版本为 5.1，且具有 ESXi 5.1 下载补丁程序 ESXi510-201212001 或更高版本。

步骤

- 1 在 Horizon Administrator 中，完成“添加 vCenter Server”向导中“存储设置”页面之前的各页面。
 - a 选择 **View 配置 > 服务器**。
 - b 在 **vCenter Server** 选项卡上，单击**添加**。
 - c 完成“vCenter Server 信息”、“View Composer 设置”和“View Composer 域”三个页面。
- 2 在“存储设置”页面中，确保选中**启用空间回收**。

如果是全新安装 Horizon 7 5.2 或更高版本，默认已选中空间回收功能。如果是从 Horizon 7 5.1 或更早版本升级到 Horizon 7 5.2 或更高版本，则必须选中**启用空间回收**。

后续步骤

在“存储设置”页面中配置 View Storage Accelerator。

要完成 Horizon 7 中的磁盘空间回收配置，需要为桌面池设置空间回收。

为 vCenter Server 配置 View Storage Accelerator

在 vSphere 5.1 及更高版本中，可以将 ESXi 主机配置为缓存虚拟机磁盘数据。这项称为 View Storage Accelerator 的功能可以使用 ESXi 主机中的 Content Based Read Cache (CBRC) 功能。View Storage Accelerator 可以在发生 I/O 风暴（大量虚拟机同时启动或同时运行多个防病毒扫描时可能会发生）时提高 Horizon 7 性能。对于需要频繁加载应用程序或数据的管理员或用户来说，这项功能同样有益。主机不再从存储系统中一遍遍地读取整个操作系统或应用程序，而是从缓存中读取常规数据块。

通过在引导风暴时减少 IOPS 数量，View Storage Accelerator 降低了对存储阵列的需求，使您可以用更少的存储 I/O 带宽支持 Horizon 7 部署。

按照此过程中所述，在 Horizon Administrator 中选择 vCenter Server 向导中的 View Storage Accelerator 设置，启用 ESXi 主机上的缓存功能。

确保也为单独的桌面池配置了 View Storage Accelerator。要对某个桌面池进行操作，必须针对 vCenter Server 和该桌面池启用 View Storage Accelerator。

默认情况下，已为桌面池启用 View Storage Accelerator。可以在创建或编辑池时禁用或启用此功能。最佳方法是在首次创建桌面池时启用此功能。如果通过编辑现有池来启用此功能，您必须确保先创建新副本及其摘要磁盘，再置备链接克隆。可以通过将池重构为新的快照或者将池重新平衡为新的数据存储来创建新副本。仅当桌面池中的虚拟机处于关闭状态时，才能为它们配置摘要文件。

您可以在包含链接克隆的桌面池和包含完整虚拟机的桌面池中启用 View Storage Accelerator。

启用了 View Storage Accelerator 的池不支持本地 NFS 快照技术 (VAAI)。

View Storage Accelerator 现在可在使用 **Horizon 7** 副本分层的配置下运行，在此配置中，副本存储于单独的数据存储中，而不是链接克隆中。虽然将 **Horizon 7** 副本分层与 **View Storage Accelerator** 搭配使用在性能方面并没有太大的实质性提升，但是通过将副本存储到单独的数据存储，还是能够带来一些容量方面的好处。因此，我们对这种组合方式进行了测试，并提供支持。

重要 如果您计划使用此功能，并且正在使用多个共享某些 **ESXi** 主机的 **View** 容器，则必须为共享的 **ESXi** 主机上的所有池启用 **View Storage Accelerator** 功能。如果多个容器中的设置不一致，可能会导致共享 **ESXi** 主机上的虚拟机出现不稳定。

前提条件

- 确认 **vCenter Server** 和 **ESXi** 主机版本为 **5.1** 或更高。
在 **ESXi** 群集中，确认所有主机的版本均为 **5.1** 或更高。
- 确认在 **vCenter Server** 中为 **vCenter Server** 用户分配了 **主机 > 配置 > 高级设置** 特权。
请参阅《**Horizon 7 安装指南**》文档中的主题，其中对 **vCenter Server** 用户所需的 **Horizon 7** 和 **View Composer** 特权进行了说明。

步骤

- 1 在 **Horizon Administrator** 中，完成“添加 **vCenter Server**”向导中“存储设置”页面之前的各页面。
 - a 选择 **View 配置 > 服务器**。
 - b 在 **vCenter Server** 选项卡上，单击**添加**。
 - c 完成“**vCenter Server** 信息”、“**View Composer** 设置”和“**View Composer** 域”三个页面。
- 2 在“存储设置”页面上，确保选中**启用 View Storage Accelerator** 复选框。
该复选框默认为选中。
- 3 指定默认的主机缓存大小。
默认的缓存大小适用于此 **vCenter Server** 实例管理的所有 **ESXi** 主机。
默认值为 **1,024 MB**。缓存大小必须在 **100 MB** 和 **2,048 MB** 之间。
- 4 要为单个 **ESXi** 主机指定不同的缓存大小，请选择 **ESXi** 主机并单击**编辑缓存大小**。
 - a 在“主机缓存”对话框中，选中 **覆盖默认主机缓存大小**。
 - b 键入一个介于 **100 MB** 和 **2,048 MB** 之间的**主机缓存大小**值，并单击**确定**。
- 5 在“存储设置”页面上，单击**下一步**。
- 6 单击**完成**在 **Horizon 7** 中添加 **vCenter Server**、**View Composer** 和存储设置。

后续步骤

配置客户端会话和连接设置。请参阅[配置客户端会话设置](#)。

要完成 **Horizon 7** 中的 **View Storage Accelerator** 设置，请为桌面池配置 **View Storage Accelerator**。请参阅《在 **Horizon 7** 中设置虚拟桌面》文档中的“为桌面池配置 **View Storage Accelerator**”。

vCenter Server 和 View Composer 的并发操作数限制

在将 vCenter Server 添加到 Horizon 7 或编辑 vCenter Server 设置时，您可以配置多个选项，这些选项用来设置由 vCenter Server 和 View Composer 所执行的并发操作的最大数量。

您可以在 vCenter Server 信息页上的“高级设置”面板中配置这些选项。

表 2-1. vCenter Server 和 View Composer 的并发操作数限制

设置	说明
最大并发 vCenter 置备操作数量	<p>确定连接服务器在此 vCenter Server 实例中置备和删除完整虚拟机时可以发出的最大并发请求数。</p> <p>默认值为 20。</p> <p>此设置仅适用于完整的虚拟机。</p>
最大并发电源操作数量	<p>确定此 vCenter Server 实例中的连接服务器所管理的虚拟机上可以发生的最大并发电源操作数（启动、关闭、挂起等）。</p> <p>默认值为 50。</p> <p>有关计算该设置的值的指导原则，请参阅设置并发电源操作率来支持远程桌面登录风暴。</p> <p>此设置适用于完整的虚拟机和链接克隆。</p>
最大并发 View Composer 维护操作数量	<p>确定在此 View Composer 实例所管理的链接克隆上可以发生的最大并发 View Composer 刷新、重构和重新平衡操作数。</p> <p>默认值为 12。</p> <p>必须先注销包含活动会话的远程桌面，然后才能开始维护操作。如果强制用户在维护操作开始时立即注销，则需要注销的远程桌面上的最大并发操作数将只达到所配置的值的一半。例如，如果将此设置配置为 24，并强制用户注销，则需要注销的远程桌面上的最大并发操作数为 12。</p> <p>此设置仅适用于链接克隆。</p>
最大并发 View Composer 置备操作数量	<p>确定在此 View Composer 实例所管理的链接克隆上可以发生的最大并发创建和删除操作数。</p> <p>默认值为 8。</p> <p>此设置仅适用于链接克隆。</p>

设置并发电源操作率来支持远程桌面登录风暴

最大并发电源操作数量设置用于控制可在 vCenter Server 实例的远程桌面虚拟机上发生的最大并发电源操作数量。这一限制默认设置为 50。当大量用户同时登录其桌面时，可更改此值以支持开机峰值速率。

作为最佳实践，您可通过试运行来确定此设置的正确值。有关规划指导原则，请参阅《[Horizon 7 架构规划指南](#)》文档中的“体系结构设计元素与规划指导原则”。

所需并发电源操作数量基于桌面开启的峰值速率，以及桌面开启、引导到可供连接所花费的时间。总之，建议的电源操作限制值就是桌面启动所花费的总时间乘以开机峰值速率。

例如，桌面的平均启动时间在二到三分钟之间。因此，并发电源操作限制值应是开机峰值速率的 3 倍。默认设置 50 应该可支持每分钟 16 个桌面的开机峰值速率。

系统等待桌面启动的最长时间为五分钟。如果启动时间更长的话，有可能会出现其他错误。为了保守起见，您可将并发电源操作限制值设为开机峰值速率的 5 倍。采用这种谨慎方法，默认设置 50 可以支持每分钟 10 个桌面的开机峰值速率。

登录操作以及桌面开启操作，通常会平均分布在特定时段内。您可以估算开机峰值速率，方法是：假设开机峰值发生在时段中间，在此期间大约 40% 的开机操作发生在该时段的 1/6 时间内。例如，如果用户在上午 8:00 到 9:00 之间登录，时段为一小时，40% 的登录操作会发生在上午 8:25 到 8:35 这 10 分钟之内。如果有 2000 名用户，其中 20% 的用户关闭了桌面，那么这 400 个桌面开启操作中会有 40% 发生在这 10 分钟之内。开机峰值速率为每分钟 16 个桌面。

接受默认 TLS 证书的指纹

在向 Horizon 7 添加 vCenter Server 和 View Composer 实例时，必须确保用于 vCenter Server 和 View Composer 实例的 TLS 证书有效且受连接服务器信任。如果随 vCenter Server 和 View Composer 一起安装的默认证书仍然存在，则必须确定是否接受这些证书的指纹。

如果为 vCenter Server 或 View Composer 实例配置了 CA 签发的证书，且根证书受连接服务器信任，则无需接受证书指纹。无需采取任何操作。

如果使用 CA 签发的证书替换默认证书，但连接服务器不信任根证书，则必须确定是否接受证书指纹。指纹是证书的加密哈希值。通过指纹可以快速确定提供的证书是否与另一个证书（例如之前接受的证书）相同。

注 如果您在同一 Windows Server 主机上安装 vCenter Server 和 View Composer，它们可以使用相同的 TLS 证书，但必须单独为每个组件配置证书。

有关配置 TLS 证书的详细信息，请参阅《Horizon 7 安装指南》文档中的“为 View Server 配置 TLS 证书”。

您首先需要使用“添加 vCenter Server”向导在 Horizon Administrator 中添加 vCenter Server 和 View Composer。如果证书不受信任而您也未接受指纹，则无法添加 vCenter Server 和 View Composer。

添加这些服务器后，您可以在“编辑 vCenter Server”对话框中重新配置它们。

注 从较早的版本进行升级时，如果 vCenter Server 或 View Composer 证书不受信任，或者您使用不受信任的证书替换了受信任证书，您也必须接受证书指纹。

在 Horizon Administrator 控制板上，vCenter Server 或 View Composer 图标会变为红色，并会显示“检测到无效的证书”对话框。在 Horizon Administrator 中，单击 **View 配置 > 服务器**，并编辑与 View Composer 服务关联的 vCenter Server 条目。然后，单击 vCenter Server 设置中的 **编辑**，按照提示确认并接受自签名的证书。

同样，在 Horizon Administrator 中，您可以配置 SAML 身份验证器供连接服务器实例使用。如果 SAML 服务器证书不受连接服务器信任，您必须确定是否接受证书指纹。如果不接受指纹，就无法在 Horizon 7 中配置 SAML 身份验证器。配置 SAML 身份验证器后，您可以在“编辑连接服务器”对话框中重新配置它。

步骤

- 1 当 Horizon Administrator 显示“检测到无效的证书”对话框时，单击**查看证书**。
- 2 检查“证书信息”窗口中的证书指纹。

3 检查为 vCenter Server 或 View Composer 实例配置的证书指纹。

- a 在 vCenter Server 或 View Composer 主机上，启动 MMC 插件并打开 Windows 证书存储区。
- b 导航至 vCenter Server 或 View Composer 证书。
- c 单击“证书详细信息”选项卡显示证书指纹。

同样还需要检查 SAML 身份验证器的证书指纹。如果可以，请针对 SAML 身份验证器主机执行之前的步骤。

4 验证“证书信息”窗口中的指纹是否与 vCenter Server 或 View Composer 实例的指纹相匹配。

同样还需要验证这些指纹是否与 SAML 身份验证器相匹配。

5 确定是否接受证书指纹。

选项	说明
指纹匹配。	单击 接受 以使用默认证书。
指纹不匹配。	单击 拒绝 。 对不匹配的证书进行故障排除。例如，您可能为 vCenter Server 或 View Composer 提供了错误的 IP 地址。

从 Horizon 7 中移除 vCenter Server 实例

您可以移除 Horizon 7 与 vCenter Server 实例之间的连接。移除后，Horizon 7 将不再管理在该 vCenter Server 实例中创建的虚拟机。

前提条件

删除所有与 vCenter Server 实例关联的虚拟机。有关删除虚拟机的更多信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“删除桌面池”。

步骤

- 1 在 Horizon Administrator 中，单击 **View 配置 > 服务器**。
- 2 在 **vCenter Server** 选项卡上，选择 vCenter Server 实例。
- 3 单击**移除**。

将显示一个对话框，警告您 Horizon 7 将不再能够访问由此 vCenter Server 实例管理的虚拟机。

- 4 单击**确定**。

Horizon 7 无法再访问在 vCenter Server 实例中创建的虚拟机。

从 Horizon 7 中移除 View Composer

您可以移除 Horizon 7 和关联到 vCenter Server 实例的 VMware Horizon View Composer 服务之间的连接。

在您禁用与 View Composer 的连接之前，必须先从 Horizon 7 中移除所有由 View Composer 创建的链接克隆虚拟机。如果仍存在任何关联的链接克隆，Horizon 7 会阻止您移除 View Composer。禁用与 View Composer 的连接之后，Horizon 7 将无法置备或管理新的链接克隆。

步骤

- 1 移除由 View Composer 创建的链接克隆桌面池。
 - a 在 Horizon Administrator 中，选择**目录 > 桌面池**。
 - b 选择链接克隆桌面池并单击**删除**。
 这时将出现一个对话框，警告您将从 Horizon 7 中永久删除链接克隆桌面池。如果链接克隆虚拟机是使用永久磁盘配置的，您可以分离或删除永久磁盘。
 - c 单击**确定**。
 随后将从 vCenter Server 中删除虚拟机。此外，还会移除相关的 View Composer 数据库条目以及由 View Composer 创建的副本。
 - d 对于由 View Composer 创建的每个链接克隆桌面池，均重复上述步骤。
- 2 选择 **View 配置 > 服务器**。
- 3 在 **vCenter Server** 选项卡上，选择与 View Composer 关联的 vCenter Server 实例。
- 4 单击**编辑**。
- 5 在“View Composer Server 设置”下，单击**编辑**，选择**不使用 View Composer**，然后单击**确定**。

您将无法再在此 vCenter Server 实例中创建链接克隆桌面池，但您可以继续在 vCenter Server 实例中创建及管理完整虚拟机桌面池。

后续步骤

如果您想要在其他主机上安装 View Composer 并将 Horizon 7 重新配置为连接到新的 VMware Horizon View Composer 服务，则必须执行一些额外的步骤。请参阅[迁移不包含链接克隆虚拟机的 View Composer](#)。

vCenter Server 唯一 ID 冲突

如果在您的环境中配置了多个 vCenter Server 实例，添加新实例时可能会因为唯一 ID 冲突而失败。

问题

您尝试向 Horizon 7 中添加一个 vCenter Server 实例，但是新 vCenter Server 实例的唯一 ID 与现有实例的 ID 冲突。

原因

两个 vCenter Server 实例不能使用相同的唯一 ID，默认情况下，vCenter Server 唯一 ID 是随机生成的，但您可以对它进行编辑。

解决方案

- 1 在 vSphere Client 中，单击**管理 > vCenter Server 设置 > 运行时设置**。
- 2 键入一个新的唯一 ID，然后单击**确定**。

有关编辑 vCenter Server 唯一 ID 值的详细信息，请参阅 vSphere 文档。

备份 Horizon 连接服务器

完成对 Horizon 连接服务器的初始配置后，您应当计划对 Horizon 7 和 View Composer 配置数据进行定期备份。

有关备份和还原 Horizon 7 配置的信息，请参阅[备份和还原 Horizon 7 配置数据](#)。

配置客户端会话设置

您可以对能够影响由连接服务器实例或复制组管理的客户端会话和连接的全局设置进行配置。您可以设置会话超时长度，显示登录前消息和警告消息，以及设置安全相关客户端连接选项。

设置客户端会话和连接选项

您可以配置全局设置，以确定客户端会话和连接的工作方式。

全局设置并不专门针对某一个连接服务器实例。它们会影响由独立的连接服务器实例或副本实例组管理的所有客户端会话。

您也可以对连接服务器实例进行配置，使其在 Horizon Client 与远程桌面之间使用直接的非安全加密链路连接。请参阅[配置安全加密链路](#)和[PCoIP 安全网关](#)，了解有关配置直接连接的信息。

前提条件

熟悉全局设置。请参阅[客户端会话的全局设置](#)和[客户端会话和连接的全局安全性设置](#)。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 全局设置**。
- 2 选择要配置常规设置还是安全性设置。

选项	说明
常规全局设置	在“常规”窗格中，单击 编辑 。
全局安全性设置	在“安全性”窗格中，单击 编辑 。

- 3 配置全局设置。
- 4 单击**确定**。

后续步骤

您可以更改安装过程中提供的数据恢复密码。请参阅[更改数据恢复密码](#)。

更改数据恢复密码

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 View Administrator 中更改此密码。从备份还原 View LDAP 配置时需要提供此密码。

备份连接服务器时，View LDAP 配置将导出为加密的 LDIF 数据。要恢复加密的备份 Horizon 7 配置，必须提供数据恢复密码。

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。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 全局设置**。
- 2 在“安全”窗格中，单击**更改数据恢复密码**。
- 3 键入并再次键入新的密码。
- 4 （可选）键入密码提醒。

注 也可以在安排要备份的 Horizon 7 配置数据时更改数据恢复密码。请参阅[计划 Horizon 7 配置备份](#)。

后续步骤

使用 vdmimport 实用程序还原备份 Horizon 7 配置时，请提供新密码。

客户端会话的全局设置

常规全局设置决定会话超时时长、SSO 实现和超时限制、Horizon Administrator 中的状态更新、是否显示登录前提示和警告消息、Horizon Administrator 是否将 Windows Server 视为支持的远程桌面操作系统，以及其他设置。

对下表中任何设置所做的更改都将立即生效。您不需要重新启动 Horizon 7 连接服务器或 Horizon Client。

表 2-2. 客户端会话的常规全局设置

设置	说明
View Administrator 会话超时	<p>确定 Horizon Administrator 会话持续闲置多久后超时。</p> <p>重要 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。可将会话超时时间设置为 1 到 4320 分钟（72 小时）间的任何值。</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>对于不支持应用程序远程的客户端，如果此设置的值为从不或大于 1200 分钟，将应用 1200 分钟的最大超时值。</p> <p>默认值为 600 分钟之后。</p>

表 2-2. 客户端会话的常规全局设置（续）

设置	说明
单点登录 (SSO)	<p>如果启用了 SSO，Horizon 7 可缓存用户的凭据，使用户不必提供凭据登录远程 Windows 会话便可启动远程桌面或应用程序。默认值为已启用。</p> <p>如果您打算使用 Horizon 7 或更高版本中引入的 True SSO 功能，则必须启用 SSO。通过 True SSO，当用户使用 Active Directory 凭据以外的其他某种身份验证形式登录时，在用户登录到 VMware Identity Manager 后，True SSO 功能会生成短期证书以供使用，而不是生成缓存凭据。</p> <p>注 如果桌面是从 Horizon Client 中启动，并被用户或 Windows 根据安全策略锁定，并且运行的是 Horizon 7 Agent 6.0 或更高版本或者 Horizon Agent 7.0 或更高版本，Horizon 7 连接服务器将放弃用户的 SSO 凭据。用户必须提供登录凭据才能启动新桌面或新应用程序，或者重新连接到任何已断开连接的桌面或应用程序。要再次启用 SSO，用户必须断开与 Horizon 7 连接服务器的连接或退出 Horizon Client，然后重新连接 Horizon 7 连接服务器。但是，如果桌面是从 Workspace ONE 或 VMware Identity Manager 中启动，当桌面被锁定时，将不会丢弃 SSO 凭据。</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，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…分钟之后，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。桌面会话不会断开连接。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>此设置也适用于 True SSO 功能。丢弃 SSO 凭据后，系统将提示用户提供 Active Directory 凭据。如果用户登录 VMware Identity Manager 时未使用 AD 凭据，并且也不知道要输入的 AD 凭据是什么，则用户可以注销 VMware Identity Manager，然后重新登录，以访问其远程桌面和应用程序。</p> <p>重要 用户必须注意，当他们同时打开了应用程序和桌面时，应用程序会因为超时而断开连接，桌面则会保持连接。用户不能依赖此超时来保护他们的桌面。</p> <p>如果设置为从不，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。默认值为从不。</p>
其他客户端。 放弃 SSO 凭据：	<p>在指定的分钟后放弃 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…分钟之后，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>如果设置为从不，Horizon 7 将存储 SSO 凭据，直到用户关闭 Horizon Client 或达到强制断开用户连接超时值为止（以先发生者为准）。</p> <p>默认值为15 分钟之后。</p>
启用自动状态更新	<p>确定 Horizon Administrator 左上角的全局状态窗格是否每隔几分钟显示一次状态更新。Horizon Administrator 的仪表板页面也会每隔几分钟更新一次。</p> <p>默认情况下不启用此设置。</p>
显示登录前的消息	<p>当 Horizon Client 用户登录时，向其显示免责声明或其他消息。</p> <p>在“全局设置”对话框的文本框中键入您的信息或说明。</p> <p>如果不希望显示任何消息，请不要选中该复选框。</p>
强制注销前显示警告	<p>当用户因为计划更新或即时更新（如要开始桌面刷新操作）被强制注销时，显示一条警告信息。此设置还可确定从显示警告到注销用户之间的时间间隔。</p> <p>选中该框可显示警告消息。</p> <p>键入从显示警告到注销用户之间的分钟数。默认值是 5 分钟。</p> <p>键入您的警告消息。您可以使用默认的消息：</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p>您的桌面将按计划执行一项重要更新，并将在 5 分钟后关闭。请立即保存尚未保存的工作。</p> </div>

表 2-2. 客户端会话的常规全局设置（续）

设置	说明
启用 Windows Server 桌面	<p>决定是否可以选择可用的 Windows Server 2008 R2 和 Windows Server 2012 R2 计算机用作桌面。启用此设置后，Horizon Administrator 将显示所有可用的 Windows Server 计算机，包括安装了 Horizon 7 Server 组件的计算机。</p> <p>注 Horizon Agent 软件无法与任何其他 Horizon 7 server 软件组件（包括安全服务器、Horizon 7 连接服务器或 Horizon 7 Composer）共存于同一虚拟机或物理机上。</p>
关闭 HTML Access 的选项卡时清除凭据	<p>当用户在 HTML Access Client 中关闭连接到远程桌面或应用程序的选项卡，或者关闭连接到桌面和应用程序选择页面的选项卡时，从缓存中移除用户的凭据。</p> <p>启用此设置时，在以下 HTML Access 客户端场景中，Horizon 7 也会从缓存中移除凭据：</p> <ul style="list-style-type: none"> ■ 用户刷新桌面和应用程序选择页面或远程会话页面。 ■ 服务器提供自签名证书，用户启动远程桌面或应用程序，并且用户在系统显示安全警告时接受证书。 ■ 用户在包含远程会话的选项卡中运行 URI 命令。 <p>如果禁用此设置，则凭据将保留在缓存中。默认情况下将禁用此功能。</p> <p>注 此功能在 Horizon 7 版本 7.0.2 及更高版本中可用。</p>
Mirage 服务器配置	<p>允许您使用 <code>mirage://server-name:port</code> 或 <code>mirages://server-name:port</code> 格式指定 Mirage 服务器的 URL。其中的服务器名称是完全限定域名。如果不指定端口号，则将使用默认端口号 8000。</p> <p>注 您可以通过在桌面池设置中指定 Mirage 服务器来覆盖此全局设置。</p> <p>还可以在 Horizon Administrator 中指定 Mirage 服务器来代替在安装 Mirage 客户端时指定 Mirage 服务器。为确定哪些 Mirage 版本支持在 Horizon Administrator 中指定该服务器，请参阅 Mirage 文档（位于 https://www.vmware.com/support/pubs/mirage_pubs.html）。</p>
在客户端用户界面中隐藏服务器信息	<p>启用此安全设置，在 Horizon Client 4.4 或更高版本中隐藏服务器 URL 信息。</p>
在客户端用户界面中隐藏域列表	<p>启用此安全设置，在 Horizon Client 4.4 或更高版本中隐藏域下拉菜单。</p> <p>在用户登录到启用了在客户端用户界面中隐藏域列表全局设置的连接服务器实例时，将在 Horizon Client 中隐藏域下拉菜单，用户可以在 Horizon Client 用户名文本框中提供域信息。例如，用户必须按照 <code>domain\username</code> 或 <code>username@domain</code> 格式输入其用户名。</p> <p>重要 如果启用在客户端用户界面中隐藏服务器信息和在客户端用户界面中隐藏域列表设置，并为连接服务器实例选择双因素身份验证（RSA SecureID 或 RADIUS），则不要强制实施 Windows 用户名匹配。实施 Windows 用户名匹配将禁止用户在用户名文本框中输入域信息，登录将始终失败。有关更多信息，请参阅《Horizon 7 管理指南》文档中有关双因素身份验证的主题。</p>

客户端会话和连接的全局安全性设置

全局安全性设置决定了网络中断后是否对客户端重新进行身份验证、是否启用消息安全模式以及是否使用 IPsec 用于安全服务器连接。

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[将 TLS 连接负载分流到中间服务器](#)。

表 2-3. 客户端会话和连接的全局安全性设置

设置	说明
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 使用安全加密链路连接访问远程桌面的情况下，决定网络中断后是否必须对用户凭据重新进行身份验证。</p> <p>如果选择此设置，当安全加密链路连接中断时，Horizon Client 会要求用户重新进行身份验证，然后才能重新连接。</p> <p>此设置可提高安全性。例如，如果一台笔记本电脑被盗并转移到其他网络，用户在不输入凭据的情况下，将无法自动获得对远程桌面的访问权限。</p> <p>如果不选择此设置，客户端将重新连接到远程桌面，而不要求用户重新进行身份验证。</p> <p>不使用安全加密链路时，此设置无效。</p>
消息安全模式	<p>确定用于在各个组件之间发送 JMS 消息的安全机制</p> <ul style="list-style-type: none"> ■ 当此模式设置为已启用时，将会对 Horizon 7 组件之间传输的 JMS 消息进行签名和验证。 ■ 如果将该模式设置为已增强，将会通过相互身份验证的 TLS，JMS 连接和对 JMS 主题的访问控制来提供安全功能。 <p>有关详细信息，请参阅 Horizon 7 组件的消息安全模式。</p> <p>对于新安装，默认情况下消息安全模式设置为已增强。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>
增强安全状态（只读）	<p>将消息安全模式从已启用更改为已增强时显示的只读字段。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"> ■ 等待 Message Bus 重新启动是第一阶段。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。 ■ 等待增强是下一阶段。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已增强。 ■ 已增强是最终状态，表明所有组件现在正使用已增强消息安全模式。 <p>还可以使用 vdmutil 命令行实用程序监控进度。请参阅使用 vdmutil 实用程序配置 JMS 消息安全模式。</p>
使用 IPsec 进行安全服务器连接	<p>确定是否为安全服务器和连接服务器实例之间的连接使用 Internet 协议安全性 (Internet Protocol Security, IPsec)。</p> <p>默认情况下，已启用安全连接（使用 IPsec）来进行安全服务器连接。</p>

注 如果您从较低的 Horizon 7 版本升级到 View 5.1 或更高版本，全局设置**要求使用 SSL 进行客户端连接**会显示在 Horizon Administrator 中，但前提是升级前您已在 Horizon 7 配置中禁用了该设置。因为是 Horizon 7 的所有 Horizon Client 连接和 Horizon Administrator 连接要求使用 TLS，所以全新安装 Horizon 7 5.1 或更高版本时不显示此设置。另外，如果升级之前的 Horizon 7 配置中启用了该设置，升级后也不会显示此设置。

升级后，如果您不启用**需要使用 SSL 进行客户端连接**设置，Horizon Client 的 HTTPS 连接将失败，除非它们连接到某个已配置为使用 HTTP 进行接续连接的中间设备。请参阅[将 TLS 连接负载分流到中间服务器](#)。

Horizon 7 组件的消息安全模式

您可以设置消息安全模式以指定在 Horizon 7 组件之间传输 JMS 消息时使用的安全机制。

下表显示了可以在配置消息安全模式时选择的选项。要设置某个选项，请从“全局设置”对话框窗口中的**消息安全模式**列表中选择所需选项。

表 2-4. 消息安全模式选项

选项	说明
已禁用	禁用消息安全模式。
混合	启用消息安全模式，但并非强制使用。 您可以使用此模式来检测 Horizon 7 环境中版本低于 Horizon 7 3.0 的组件。连接服务器生成的日志文件包含这些组件的相关信息。不建议使用此设置。仅使用此设置发现需要升级的组件。
已启用	已使用消息签名和加密组合启用了消息安全模式。如果签名丢失或无效或者消息在签名后被修改，将拒绝 JMS 消息。某些 JMS 消息进行了加密，因为其中包含用户凭据等敏感信息。如果使用已启用设置，则还可以使用 IPSec 对连接服务器实例之间以及连接服务器实例与安全服务器之间的所有 JMS 消息进行加密。 注 不允许版本低于 3.0 的 Horizon 7 组件与其他 Horizon 7 组件通信。
已增强	SSL 用于所有 JMS 连接。还启用了 JMS 访问控制，以便桌面、安全服务器和连接服务器实例可以仅发送和接收特定主题的 JMS 消息。 版本低于 Horizon 6 版本 6.1 的 Horizon 7 组件无法与连接服务器 6.1 实例通信。 注 使用此模式要求在基于 DMZ 的安全服务器与其配对的连接服务器实例之间打开 TCP 端口 4002。

首次在系统中安装 Horizon 7 时，消息安全模式设置为**已增强**。如果从先前版本升级 Horizon 7，消息安全模式将保持现有设置不变。

重要 如果您计划将已升级的 Horizon 7 环境从**已启用**更改为**已增强**，则必须先将所有连接服务器实例、安全服务器和 Horizon 7 桌面升级到 Horizon 6 版本 6.1 或更高版本。将设置更改为**已增强**后，新设置将分阶段进行。

- 1 必须手动重新启动容器中所有连接服务器主机上的 VMware Horizon View Message Bus 组件服务，或重新启动连接服务器实例。
- 2 重新启动这些服务后，连接服务器实例会在所有桌面和安全服务器上重新配置消息安全模式，从而将此模式更改为**已增强**。
- 3 要在 Horizon Administrator 中监视进度，请转至 **View 配置 > 全局设置**。

当所有组件都已转换为“已增强”模式时，安全选项卡上的**增强安全状态**项将显示**已增强**。

此外，您还可以使用 `vdmutil` 命令行实用程序监控进度。请参阅[使用 vdmutil 实用程序配置 JMS 消息安全模式](#)。

低于 Horizon 6 版本 6.1 的 Horizon 7 组件无法与使用“已增强”模式的连接服务器 6.1 实例通信。

如果您计划将活动 Horizon 7 环境从**已禁用**更改为**已启用**或从**已启用**更改为**已禁用**，请在做出最终更改前将其短时间更改为**混合**模式。例如，如果您当前的模式为**已禁用**，请先更改为**混合**模式并保持一天，然后再更改为**已启用**。在**混合**模式下，签名将被附加到消息中，但未验证，这允许消息模式的更改传播到整个环境中。

使用 vdmutil 实用程序配置 JMS 消息安全模式

您可以使用 `vdmutil` 命令行界面配置和管理 JMS 消息在 Horizon 7 组件之间传递时所使用的安全机制。

实用程序的语法和位置

vdmutil 命令可以执行与早期版本的 Horizon 7 随附的 **lmvutil** 命令相同的操作。此外，**vdmutil** 命令还拥有可确定正在使用的消息安全模式和监控将所有 Horizon 7 组件更改为已增强模式的过程的选项。在 Windows 命令提示符下，使用以下 **vdmutil** 命令格式。

```
vdmutil command_option [additional_option argument] ...
```

您可以使用的附加选项取决于命令选项。本主题重点介绍消息安全模式的选项。有关与 Cloud Pod 架构相关的其他选项，请参阅《在 Horizon 7 中管理 Cloud Pod 架构》文档。

默认情况下，**vdmutil** 命令可执行文件的路径为 **C:\Program Files\VMware\VMware View\Server\tools\bin**。为避免在命令行中输入此路径，可以将此路径添加到 **PATH** 环境变量中。

身份验证

必须以具有管理员角色的用户身份运行该命令。可以使用 **Horizon Administrator** 将管理员角色分配给用户。请参阅第 6 章，配置基于角色的委托管理。

vdmutil 命令包括用于指定进行身份验证时使用的用户名、域和密码的选项。

表 2-5. vdmutil 命令身份验证选项

选项	说明
--authAs	Horizon 7 管理员用户的名称。请勿使用域\用户名或用户主体名称 (User Principal Name, UPN) 格式。
--authDomain	--authAs 选项中指定的 Horizon 7 管理员用户的完全限定域名。
--authPassword	--authAs 选项中指定的 Horizon 7 管理员用户的密码。在命令行中输入 "*" 来代替密码会导致 vdmutil 命令提示输入密码，并且不会在命令历史记录中保留敏感密码。

必须将身份验证选项与除了 **--help** **--verbose** 之外的所有 **vdmutil** 命令选项结合使用。

特定于 JMS 消息安全模式的选项

下表仅列出了与查看、设置或监控 JMS 消息安全模式有关的 **vdmutil** 命令行选项。有关可与特定选项结合使用的参数列表，请使用 **--help** 命令行选项。

操作成功时，**vdmutil** 命令将返回 0；操作失败时，将返回故障特定的非零代码。**vdmutil** 命令会将错误消息写入标准错误。当某个操作生成输出时，或通过使用 **--verbose** 选项启用了详细日志记录时，**vdmutil** 命令会使用美国英语将输出写入标准输出。

表 2-6. vdmutil 命令选项

选项	说明
--activatePendingConnectionServerCertificates	在本地容器中为连接服务器实例激活等待处理的安全证书。
--countPendingMsgSecStatus	计算阻止转换到已增强模式或从已增强模式转换的计算机数量。
--createPendingConnectionServerCertificates	在本地容器中为连接服务器实例创建新的等待处理的安全证书。
--getMsgSecLevel	获取本地容器的增强消息安全状态。此状态与将 Horizon 7 环境中所有组件的 JMS 消息安全模式从已启用更改为已增强的过程有关。
--getMsgSecMode	获取本地容器的消息安全模式。

表 2-6. vdmutil 命令选项（续）

选项	说明
--help	列出 vdmutil 命令选项。您也可以在某些特定命令上使用 --help，例如 --setMsgSecMode --help。
--listMsgBusSecStatus	列出本地容器中所有连接服务器的消息总线安全状态。
--listPendingMsgSecStatus	列出阻止转换到已增强模式或从已增强模式转换的计算机。默认情况下，仅限于 25 个条目。
--setMsgSecMode	设置本地容器的消息安全模式。
--verbose	启用详细的日志记录。您可以将此选项添加到任何其他选项，以获取详细的命令输出。vdmutil 命令可写入标准输出。

配置安全加密链路和 PCoIP 安全网关

启用安全加密链路后，当用户连接到远程桌面时，Horizon Client 会与 View 连接服务器或安全服务器主机建立另一个 HTTPS 连接。

启用 PCoIP 安全网关后，当用户使用 PCoIP 显示协议连接到远程桌面时，Horizon Client 会与连接服务器或安全服务器主机再建立一个安全连接。

注 通过使用 Horizon 6 版本 6.2 和更高版本，您可以使用 Unified Access Gateway 设备（而不是安全服务器）安全地对 Horizon 6 服务器和桌面进行外部访问。如果使用 Unified Access Gateway 设备，您必须在连接服务器实例上禁用安全网关，并在 Unified Access Gateway 设备上启用这些网关。有关更多信息，请参阅《部署和配置 Unified Access Gateway》。

如果不启用安全加密链路或 PCoIP 安全网关，将绕过连接服务器或安全服务器主机，直接在客户端系统与远程桌面虚拟机之间建立会话。这种连接类型被称为直接连接。

重要 为外部客户端提供安全连接的常规网络配置通常都包含安全服务器。要使用 Horizon Administrator 启用或禁用安全服务器上的安全加密链路和 PCoIP 安全网关，您必须编辑与安全服务器配对的连接服务器实例。

在外部客户端直接连接到连接服务器主机的网络配置中，可以通过在 Horizon Administrator 中编辑该连接服务器实例来启用或禁用安全加密链路和 PCoIP 安全网关。

前提条件

- 如果您打算启用 PCoIP 安全网关，请确认连接服务器实例以及与其配对的安全服务器为 Horizon 7 4.6 或更高版本。
- 如果您要将某个安全服务器与一个已启用 PCoIP 安全网关的连接服务器实例进行配对，请确认该安全服务器为 Horizon 7 4.6 或更高版本。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。
- 2 在 **连接服务器** 选项卡上，选择连接服务器实例，并单击 **编辑**。

3 配置是否使用安全加密链路连接。

选项	说明
启用安全加密链路连接	选择使用安全加密链路连接计算机。
禁用安全加密链路连接	取消选中使用安全加密链路连接计算机。

默认情况下，安全加密链路连接为启用状态。

4 配置是否使用 PCoIP 安全网关。

选项	说明
启用 PCoIP 安全网关	选择使用 PCoIP 安全网关与计算机建立 PCoIP 连接
禁用 PCoIP 安全网关	取消选择使用 PCoIP 安全网关与计算机建立 PCoIP 连接

默认禁用 PCoIP 安全网关。

5 单击确定保存更改。

配置 Blast 安全网关

在 Horizon Administrator 中，您可以配置使用 Blast 安全网关来提供对远程桌面和应用程序的安全访问（通过 HTML Access，或通过使用 VMware Blast 显示协议的客户端连接）。

Blast 安全网关包含 Blast Extreme 自适应传输 (BEAT) 网络连接，可进行动态调整以适应网络条件，例如不断变化的网速和数据包丢失。

- 仅当在 Unified Access Gateway 设备上运行时，Blast 安全网关才支持 BEAT 网络连接。
- 连接到 Unified Access Gateway 设备版本 3.3 或更高版本时，可以同时使用 TCP 端口 8443 上和 UDP 端口 8443（对于 BEAT）上处理使用 IPv4 的 Horizon Client 和使用 IPv6 的 Horizon Client。
- 使用典型网络条件的 Horizon Client 必须连接到连接服务器（BSG 被禁用）、安全服务器（BSG 被禁用）或版本高于 2.8 的 Unified Access Gateway 设备。如果 Horizon Client 使用典型的网络条件连接到连接服务器（BSG 已启用）、安全服务器（BSG 已启用）或版本低于 2.8 的 Unified Access Gateway 设备，该客户端会自动检测网络条件，并回退至 TCP 网络连接。
- 使用较差网络条件的 Horizon Client 必须连接到版本为 2.9 或更高版本的 Unified Access Gateway 设备（已启用 UDP Tunnel Server）。如果 Horizon Client 使用较差的网络条件连接到连接服务器（BSG 已启用）、安全服务器（BSG 已启用）或版本低于 2.8 的 Unified Access Gateway 设备，该客户端会自动检测网络条件，并回退至 TCP 网络连接。
- Horizon Client 使用较差的网络条件连接到连接服务器（BSG 被禁用）、安全服务器（BSG 被禁用）或版本为 2.9 或更高版本的 Unified Access Gateway 设备（已启用 UDP Tunnel Server），或版本为 2.8 的 Unified Access Gateway 设备，该客户端会自动检测网络条件，并回退至典型的网络条件。

有关详细信息，请参阅 <https://docs.vmware.com/cn/VMware-Horizon-Client/index.html> 网址上的 Horizon Client 文档。

注 您还可以使用 Unified Access Gateway 设备而不是安全服务器，对 Horizon 7 服务器和桌面进行安全外部访问。如果使用 Unified Access Gateway 设备，您必须在连接服务器实例上禁用安全网关，并在 Unified Access Gateway 设备上启用这些网关。有关更多信息，请参阅《部署和配置 Unified Access Gateway》。

如果未启用 Blast 安全网关，客户端设备和客户端 Web 浏览器会使用 VMware Blast Extreme 协议绕过 Blast 安全网关，而与远程桌面虚拟机和应用程序建立直接连接。

重要 为外部用户提供安全连接的常规网络配置通常都包含安全服务器。要启用或禁用安全服务器上的 Blast 安全网关，您必须编辑与安全服务器配对的连接服务器实例。如果外部用户直接连接到连接服务器主机，可以通过编辑该连接服务器实例来启用或禁用 Blast 安全网关。

前提条件

如果用户使用 VMware Identity Manager 选择了远程桌面，请确认 VMware Identity Manager 已安装并配置与连接服务器配合使用，且连接服务器已与 SAML 2.0 身份验证服务器配对。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。
- 2 在 **连接服务器** 选项卡上，选择连接服务器实例，并单击 **编辑**。
- 3 配置是否使用 Blast 安全网关。

选项	说明
启用 Blast 安全网关	选择使用 Blast 安全网关对计算机进行 Blast 连接
为 HTML Access 启用 Blast 安全网关	选择使用 Blast 安全网关仅对计算机进行 HTML Access Blast 连接
禁用 Blast 安全网关	选择不使用 Blast 安全网关

默认情况下，Blast 安全网关为启用状态。

- 4 单击 **确定** 保存更改。

将 TLS 连接负载分流到中间服务器

Horizon Client 必须使用 HTTPS 连接到 Horizon 7。如果 Horizon Client 连接到负载均衡器或其他中间服务器（这些负载均衡器和中间服务器能够将连接传递至连接服务器实例或安全服务器），您可将 TLS 负载分流到中间服务器。

将 TLS 负载分流服务器的证书导入到 Horizon 7 Server

如果将 TLS 连接负载分流到中间服务器，您必须将中间服务器的证书导入到连接服务器实例或连接到中间服务器的安全服务器中。同一个 TLS 服务器证书必须同时位于正在进行负载分流的中间服务器和连接到中间服务器并且已被负载分流的 Horizon 7 Server 中。

如果您部署安全服务器，则中间服务器和连接到该中间服务器的安全服务器必须拥有相同的 TLS 证书。您不必在已与安全服务器配对但未直接连接到中间服务器的连接服务器实例上安装相同的 TLS 证书。

如果您未部署安全服务器，或者如果您的混合网络环境包含一些安全服务器和一些面向外部的连接服务器实例，则中间服务器和连接到该中间服务器的任何连接服务器实例都必须拥有相同的 TLS 证书。

如果中间服务器的证书未安装在连接服务器实例或安全服务器上，则客户端无法验证其与 Horizon 7 的连接。在这种情况下，Horizon 7 server 发送的证书指纹与 Horizon Client 连接的中间服务器上的证书不一致。

不要混淆负载平衡与 TLS 负载分流。前者适用于任何被配置为提供 TLS 负载分流功能的设备，包括某些类型的负载平衡程序。但是，单纯的负载平衡不要求在设备之间复制证书。

有关将证书导入 Horizon 7 Server 的信息，请参阅《Horizon 7 安装指南》文档中的“将签名的服务器证书导入到 Windows 证书存储区”。

将 Horizon 7 Server 外部 URL 设置为将客户端指向 TLS 负载分流服务器

如果 TLS 负载分流到中间服务器，并且 Horizon Client 设备使用安全加密链路连接 Horizon 7，则必须将安全加密链路外部 URL 设置为客户端可以用来访问中间服务器的地址。

在连接到中间服务器的连接服务器实例或安全服务器上配置外部 URL 设置。

如果部署安全服务器，则安全服务器需要外部 URL，但与安全服务器配对的连接服务器不需要。

如果未部署安全服务器，或者使用包含部分安全服务器和部分对外的连接服务器实例的混合网络环境，则连接到中间服务器的任何连接服务器实例都需要使用外部 URL。

注 无法对来自 PCoIP 安全网关 (PCoIP Secure Gateway, PSG) 或 Blast 安全网关的 TLS 连接进行负载分流。PCoIP 外部 URL 和 Blast 安全网关外部 URL 必须允许客户端连接到托管 PSG 和 Blast 安全网关的计算机。除非规划为在中间服务器与 Horizon 7 Server 之间需要使用 TLS 连接，否则不要将 PCoIP 外部 URL 和 Blast 外部 URL 重置为指向中间服务器。

有关配置外部 URL 的信息，请参阅《Horizon 7 安装指南》文档中的“为 PCoIP 安全网关和安全加密链路连接配置外部 URL”。

允许源自中间服务器的 HTTP 连接

TLS 负载分流到中间服务器后，您可以将连接服务器实例或安全服务器配置为允许源自面向客户端的中间设备的 HTTP 连接。中间设备必须接受 HTTPS 作为 Horizon Client 连接。

要允许在 Horizon 7 Server 与中间设备之间建立 HTTP 连接，必须在允许 HTTP 连接的每个连接服务器实例和安全服务器上配置 `locked.properties` 文件。

即使允许在 Horizon 7 Server 与中间设备之间建立 HTTP 连接，也不能在 Horizon 7 中禁用 TLS。Horizon 7 Server 继续接受 HTTPS 连接以及 HTTP 连接。

注 如果您的 Horizon Client 使用智能卡身份验证，这些客户端必须直接与连接服务器或安全服务器建立 HTTPS 连接。智能卡身份验证不支持 TLS 负载分流。

步骤

- 1 在连接服务器或安全服务器主机的 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\locked.properties`
- 2 要配置 Horizon 7 server 的协议, 请添加 `serverProtocol` 属性并将其设置为 `http`。
值 `http` 必须以小写键入。
- 3 (可选) 添加属性以在 Horizon 7 server 上配置非默认 HTTP 侦听端口和网络接口。
 - 要将 HTTP 侦听端口从 80 更改为其他端口, 请将 `serverPortNonTLS` 设置为中间设备已配置连接的另一个端口号。
 - 如果 Horizon 7 Server 具有多个网络接口, 而您希望该服务器只侦听一个接口上的 HTTP 连接, 请将 `serverHostNonTLS` 设置为该网络接口的 IP 地址。
- 4 保存 `locked.properties` 文件。
- 5 重新启动连接服务器服务或安全服务器服务, 使所做的更改生效。

示例: locked.properties 文件

此文件允许与 Horizon 7 Server 建立非 TLS HTTP 连接。Horizon 7 Server 面向客户端的网络接口的 IP 地址为 10.20.30.40。此服务器使用默认端口 80 来侦听 HTTP 连接。值 `http` 必须为小写。

```
serverProtocol=http
serverHostNonTLS=10.20.30.40
```

配置 Horizon 连接服务器或安全服务器主机的网关位置

默认情况下, Horizon 连接服务器实例会将网关位置设置为 `Internal`, 而安全服务器会将网关位置设置为 `External`。您可以通过设置 `locked.properties` 文件中的 `gatewayLocation` 属性来更改默认网关位置。

网关位置确定远程桌面中 `ViewClient_Broker_GatewayLocation` 注册表项的值。您可以将该值和智能策略结合使用, 以创建仅当用户从企业网络内部或外部连接到远程桌面时才生效的策略。有关详细信息, 请参阅《在 Horizon 7 中配置远程桌面功能》文档中的“使用智能策略”。

步骤

- 1 在 Horizon 连接服务器或安全服务器主机的 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\locked.properties`。
`locked.properties` 文件中的属性区分大小写。

- 2 向 `locked.properties` 文件添加以下行：

```
gatewayLocation=value
```

`value` 可以为 `External` 或 `Internal`。`External` 指示网关可用于企业网络外部的用户。`Internal` 指示网关仅可用于企业网络内部的用户。

例如：`gatewayLocation=External`

- 3 保存 `locked.properties` 文件。
- 4 重新启动 VMware Horizon 连接服务器服务或 VMware Horizon 安全服务器服务，以使所做的更改生效。

禁用或启用 Horizon 连接服务器

您可以禁用连接服务器实例，以阻止用户登录到其虚拟或发布的桌面和应用程序。禁用实例后，可以重新启用。

禁用某个连接服务器实例时，当前已登录到桌面和应用程序的用户不会受到影响。

您的 Horizon 7 部署决定了禁用实例会对用户产生怎样的影响。

- 如果是单一独立的连接服务器实例，用户将无法登录到其桌面或应用程序。他们无法连接到连接服务器。
- 如果是连接服务器副本实例，那么您的网络拓扑结构将确定用户是否可以路由到另一个副本实例。如果用户可以访问另一实例，他们将可以登录到自己的桌面和应用程序。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。
- 2 在 **连接服务器** 选项卡上，选择连接服务器实例。
- 3 单击 **已禁用**。

您可以通过单击 **已启用** 再次启用该实例。

编辑外部 URL

您可以使用 Horizon Administrator 编辑连接服务器实例和安全服务器的外部 URL。

默认情况下，仅位于同一网络且使用安全加密链路的客户端可以联络连接服务器或安全服务器主机。在网络外运行的安全加密链路客户端必须使用客户端可解析的 URL 来连接连接服务器或安全服务器主机。

用户通过 PCoIP 显示协议连接到远程桌面时，Horizon Client 可进一步连接到连接服务器或安全服务器主机上的 PCoIP 安全网关。要使用 PCoIP 安全网关，客户端系统必须能够访问允许该客户端连接连接服务器或安全服务器主机的 IP 地址。在 PCoIP 外部 URL 中指定此 IP 地址。

第三个 URL 允许用户通过 Blast 安全网关建立安全连接。

安全加密链路外部 URL、PCoIP 外部 URL 和 Blast 外部 URL 都必须是客户端系统用于连接此主机的地址。

注 您无法编辑尚未升级到连接服务器 4.5 或更高版本的安全服务器的外部 URL。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。

选项	操作
View 连接服务器实例	在 连接服务器 选项卡中选择连接服务器实例，然后单击 编辑 。
安全服务器	在 安全服务器 选项卡中选择安全服务器并单击 编辑 。

- 2 在**外部 URL** 文本框中键入安全加密链路的外部 URL。

URL 必须包含协议、客户端可解析的主机名和端口号。

例如：<https://view.example.com:443>

注 如果您需要在主机名不可解析时访问连接服务器实例或安全服务器，可以使用 IP 地址。但您联络的主机将与为连接服务器实例或安全服务器配置的 SSL 证书不匹配，导致访问被阻止或访问的安全性降低。

- 3 在 **PCoIP 外部 URL** 文本框中键入 PCoIP 安全网关的外部 URL。

将 PCoIP 外部 URL 指定为包含端口号 **4172** 的 IP 地址。请勿包含协议名。

例如：10.20.30.40:4172

URL 中必须包含客户端系统可用于连接此安全服务器或连接服务器实例的 IP 地址和端口号。

- 4 在 **Blast 外部 URL** 文本框中键入 Blast 安全网关的外部 URL。

URL 必须包含 HTTPS 协议、客户端可解析的主机名和端口号。

例如：<https://myserver.example.com:8443>

默认情况下，URL 包含安全加密链路外部 URL 的 FQDN 和默认端口号 **8443**。URL 中必须包含客户端系统可用于连接此主机的 FQDN 和端口号。

- 5 确认此对话框中的所有地址都允许客户端系统连接此主机。

- 6 单击**确定**保存更改。

外部 URL 将立即更新。无需重新启动连接服务器服务或安全服务器服务，所做更改即可生效。

加入或退出客户体验计划

使用新配置安装连接服务器时，您可以选择参加客户体验提升计划。如果您在安装后改变主意，可以使用 Horizon Administrator 加入或退出该计划。

如果您参加该计划，VMware 会收集有关您的部署的匿名数据，以用于改进 VMware 对用户需求的响应。不收集能确定组织身份的数据。

要查看用于收集数据的字段列表，包括匿名收集的字段，请参阅 [GUID-4FDD21B3-5F28-419F-AA16-4C7578996A54#GUID-4FDD21B3-5F28-419F-AA16-4C7578996A54](#)。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 产品许可和使用情况**。

- 2 在“客户体验计划”窗格中，单击**编辑设置**。
- 3 选中或取消选中**向 VMware 发送匿名数据**复选框来决定是参加还是退出计划。
- 4 （可选）如果您参加计划，可以选择地理位置、业务类型和贵组织的员工数量。
- 5 单击**确定**。

View LDAP 目录

View LDAP 是所有 Horizon 7 配置信息的数据存储库。View LDAP 是一种嵌入式轻型目录访问协议 (Lightweight Directory Access Protocol, LDAP) 目录，它与连接服务器安装程序一起提供。

View LDAP 包含 Horizon 7 所使用的标准 LDAP 目录组件。

- Horizon 7 模式定义
- 目录信息树 (DIT) 定义
- 访问控制列表 (ACL)

View LDAP 包含了表示 Horizon 7 对象的目录条目。

- 远程桌面条目，表示每个可访问的桌面。每个条目均包含对 Active Directory 中有权使用此桌面的 Windows 用户和组的外部安全主体 (Foreign Security Principal, FSP) 条目的引用。
- 远程桌面池条目，表示被集中管理的多个桌面
- 虚拟机条目，表示每个远程桌面的 vCenter Server 虚拟机
- Horizon 7 组件条目，用于存储配置设置

此外，View LDAP 还包含一组 Horizon 7 插件 DLL，可为其他 Horizon 7 组件提供自动化服务和通知服务。

注 安全服务器实例不包含 View LDAP 目录。

LDAP 复制

安装连接服务器的副本实例时，Horizon 7 会从现有连接服务器实例复制 View LDAP 配置数据。副本组中所有连接服务器实例上的 View LDAP 配置数据均保持相同。更改一个实例时，更新的信息将复制到其他实例。

如果一个副本实例出现故障，组中的其他实例会继续运行。当出现故障的实例恢复活动时，其配置数据将自动更新，以对故障期间发生的更改进行同步。在 Horizon 7 及更高版本中，每 15 分钟执行一次复制状态检查，以确定每个实例是否可以与副本组中的其他服务器进行通信，以及每个实例是否可以从该组中的其他服务器获取 LDAP 更新。

您可以使用 Horizon Administrator 中的仪表板来检查复制状态。如果仪表板中的任何连接服务器实例具有红色图标，单击该图标可查看复制状态。复制功能可能会因以下任何原因而受到影响：

- 防火墙可能会阻止通信
- 连接服务器实例上可能停止 VMware VDMDS 服务
- VMware VDMDS DSA 选项可能会阻止复制

■ 发生网络问题

默认情况下，每隔 15 分钟检查一次复制。您可以在连接服务器实例上使用“ADSI 编辑”更改间隔。要设置分钟数，请连接到 **DC=vdi,DC=vmware,DC=int** 并编辑 **CN=Common,OU=Global,OU=Properties** 对象上的 **pae-ReplicationStatusDataExpiryInMins** 属性。

pae-ReplicationStatusDataExpiryInMins 属性值应在 10 分钟到 1440 分钟（一天）之间。如果该属性值小于 10 分钟，则 Horizon 7 将其视为 10 分钟。如果该属性值大于 1440 分钟，则 Horizon 7 将其视为 1440 分钟。

设置智能卡身份验证

为了增强安全性，可以对连接服务器实例或安全服务器进行配置，以使用户和管理员能够使用智能卡进行身份验证。

智能卡是一种内含计算机芯片的小型塑料卡。其中的芯片就像一个微型计算机，具备数据安全存储，可存储私钥和公钥证书。美国国防部使用的智能卡类型称为通用访问卡 (CAC)。

使用智能卡身份验证时，用户或管理员可以将智能卡插入连接到客户端计算机的智能卡读卡器中，然后输入 PIN。智能卡身份验证通过验证用户是否具有智能卡以及用户是否知道 PIN 来提供双因素身份验证。

有关实现智能卡身份验证的硬件和软件要求的信息，请参阅《Horizon 7 安装指南》文档。Microsoft TechNet 网站中包含为 Windows 系统规划和实施智能卡身份验证方面的详细信息。

要使用智能卡，客户端计算机必须具有智能卡中间件和智能卡读卡器。要在智能卡上安装证书，您必须将一台计算机设置为注册站点。如需了解一个特定类型的 Horizon Client 是否支持智能卡，请参阅 <https://docs.vmware.com/cn/VMware-Horizon-Client/index.html> 网站上的 Horizon Client 文档。

本章讨论了以下主题：

- 使用智能卡登录
- 在 Horizon 连接服务器上配置智能卡身份验证
- 在第三方解决方案上配置智能卡身份验证
- 为智能卡身份验证准备 Active Directory
- 验证智能卡身份验证配置
- 使用智能卡证书撤销检查

使用智能卡登录

当用户或管理员将智能卡插入智能卡读卡器中后，如果客户端操作系统是 Windows，智能卡上的用户证书将被复制到客户端系统上的本地证书存储中。本地证书存储中的证书可供客户端计算机上运行的所有应用程序（包括 Horizon Client）使用。

当用户或管理员与配置为使用智能卡身份验证的连接服务器实例或安全服务器建立连接时，连接服务器实例或安全服务器将向客户端系统发送受信任的证书颁发机构 (CA) 列表。客户端系统将依据可用的用户证书来检查受信任 CA 列表，选择合适的证书，然后提示用户或管理员输入智能卡 PIN 码。如果存在多个有效的用户证书，客户端系统会提示用户或管理员选择其中一个证书。

客户端系统将用户证书发送给连接服务器实例或安全服务器，连接服务器实例或安全服务器将通过检查证书的信任和有效期限对其进行检验。通常情况下，只要签发了用户证书而且该证书有效，用户和管理员即可成功通过身份验证。如果配置了证书撤销检查，已撤销用户证书的用户或管理员将无法通过身份验证。

在一些环境中，用户的智能卡证书可以映射到多个 **Active Directory** 域用户帐户。用户可能有多个具有管理员权限的帐户，因此需要指定在智能卡登录时“用户名提示”字段中使用哪个帐户。要使 **Horizon Client** 登录对话框中显示“用户名提示”字段，管理员必须在 **Horizon Administrator** 中为连接服务器实例启用智能卡用户名提示功能。然后，在智能卡登录期间，智能卡用户可以在“用户名提示”字段中输入用户名或 UPN。

如果您的环境使用 **Unified Access Gateway** 设备来确保外部访问的安全，则必须配置 **Unified Access Gateway** 设备，以使其支持智能卡用户名提示功能。仅 **Unified Access Gateway 2.7.2** 和更高版本支持智能卡用户名提示功能。有关在 **Access Point** 中启用智能卡用户名提示功能的信息，请参阅《部署和配置 **Unified Access Gateway**》文档。

在 **Horizon Client** 中使用智能卡身份验证时，不支持显示协议切换。要在 **Horizon Client** 中使用智能卡进行身份验证后更改显示协议，用户必须注销并重新登录。

在 Horizon 连接服务器上配置智能卡身份验证

要配置智能卡身份验证，您必须获得一个根证书并将其添加到服务器信任存储区文件，修改连接服务器配置属性，并配置智能卡身份验证设置。根据您的具体环境，您可能需要执行附加步骤。

步骤

1 获取证书颁发机构证书

您必须为用户和管理员提供的智能卡上的所有受信任的用户证书获取所有相应的 **CA**（证书颁发机构）证书。如果用户的智能卡证书是由中间证书颁发机构颁发的，则这些证书包括根证书，并且可以包括中间证书。

2 从 Windows 获取 CA 证书

如果您拥有 **CA** 签发的用户证书或包含 **CA** 签发的用户证书的智能卡，且 **Windows** 信任此根证书，则可以从 **Windows** 导出此根证书。如果用户证书的颁发者是中间证书颁发机构，则您可以导出该证书。

3 将 CA 证书添加到服务器信任存储区文件中

您必须将信任的所有用户和管理员的根证书和/或中间证书添加到服务器信任存储区文件中。连接服务器实例和安全服务器使用此信息对智能卡用户和管理员进行身份验证。

4 修改 Horizon 连接服务器配置属性

您必须修改连接服务器或安全服务器主机上的连接服务器配置属性，才能启用智能卡身份验证。

5 在 Horizon Administrator 中配置智能卡设置

您可以使用 **Horizon Administrator** 指定设置，以适应不同的智能卡身份验证情形。

获取证书颁发机构证书

您必须为用户和管理员提供的智能卡上的所有受信任的用户证书获取所有相应的 **CA**（证书颁发机构）证书。如果用户的智能卡证书是由中间证书颁发机构颁发的，则这些证书包括根证书，并且可以包括中间证书。

如果您没有获取对用户和管理员提供的智能卡上的证书签名的 CA 的根证书或中间证书，则可以从 CA 签名的用户证书或包含此类证书的智能卡中导出这些证书。请参阅[从 Windows 获取 CA 证书](#)。

步骤

- ◆ 从以下某个源中获取 CA 证书。
 - 运行 Microsoft 证书服务的 Microsoft IIS 服务器。有关安装 Microsoft IIS、颁发证书以及在组织中分发证书的信息，请参见 Microsoft TechNet 网站。
 - 受信任的 CA 签名的公用根证书。如果环境中具有智能卡基础架构，以及标准的智能卡分发和身份验证方式，就属于最常用的根证书源。

后续步骤

将根证书和/或中间证书添加到服务器信任存储区文件中。

从 Windows 获取 CA 证书

如果您拥有 CA 签发的用户证书或包含 CA 签发的用户证书的智能卡，且 Windows 信任此根证书，则可以从 Windows 导出此根证书。如果用户证书的颁发者是中间证书颁发机构，则您可以导出该证书。

步骤

- 1 如果用户证书存储在智能卡上，您只需将智能卡插入读卡器，就可以将用户证书添加到您的个人存储区中。
如果用户证书未显示在您的个人存储区中，可使用读取器软件将用户证书导出到文件中。此文件在该流程的步骤 4 中使用。
- 2 在 Internet Explorer 中，选择**工具 > Internet 选项**。
- 3 在**内容**选项卡上，单击**证书**。
- 4 在**个人**选项卡上，选择您要使用的证书，然后单击**查看**。
如果用户证书未显示在列表中，请单击**导入**从文件中手动导入该证书。导入证书后，您就可以从列表中选择该证书。
- 5 在**证书路径**选项卡上，选择树状结构顶端的证书，然后单击**查看证书**。
如果用户证书是作为信任层次结构的一部分签发的，则签发证书可能由另一较高级别的证书签发。选择父证书（即实际签发用户证书的证书）作为您的根证书。在某些情况下，颁发者可能是中间 CA。
- 6 在**详细信息**选项卡上，单击**复制到文件**。
屏幕上将显示**证书导出向导**。
- 7 单击**下一步 > 下一步**，然后键入要导出的文件的名称和位置。
- 8 单击**下一步**将该文件作为根证书保存到指定的位置。

后续步骤

将 CA 证书添加到服务器信任存储区文件中。

将 CA 证书添加到服务器信任存储区文件中

您必须将信任的所有用户和管理员的根证书和/或中间证书添加到服务器信任存储区文件中。连接服务器实例和安全服务器使用此信息对智能卡用户和管理员进行身份验证。

前提条件

- 获取用于对用户或管理员提供的智能卡上的证书进行签名的根证书或中间证书。请参阅[获取证书颁发机构证书](#)和从 [Windows](#) 获取 CA 证书。

重要 如果用户的智能卡证书是由中间证书颁发机构颁发的，则这些证书可以包括中间证书。

- 确认 **keytool** 实用程序已添加到连接服务器或安全服务器主机上的系统路径。有关更多信息，请参阅《Horizon 7 安装指南》文档。

步骤

- 1 在连接服务器或安全服务器主机上，使用 **keytool** 实用程序将根证书和/或中间证书导入服务器信任存储区文件中。

例如：

```
keytool -import -alias alias -file root_certificate -keystore truststorefile.key
```

在此命令中，**alias** 是信任存储区文件中新条目的唯一名称（区分大小写），**root_certificate** 是已获得或导出的根证书或中间证书，**truststorefile.key** 是要将根证书添加到的信任存储区文件的名称。如果该文件不存在，请在当前目录中创建。

注 **keytool** 实用程序可能会提示您为信任存储区文件创建密码。如果您以后需要向信任存储区文件中添加更多证书，就必须提供此密码。

- 2 将信任存储区文件复制到连接服务器或安全服务器主机上的 **SSL** 网关配置文件夹下。

例如：**install_directory\VMware\VMware
View\Server\sslgateway\conf\truststorefile.key**

后续步骤

修改连接服务器配置属性以启用智能卡身份验证。

修改 Horizon 连接服务器配置属性

您必须修改连接服务器或安全服务器主机上的连接服务器配置属性，才能启用智能卡身份验证。

前提条件

将所有可信用户证书的证书颁发机构 (Certificate Authority, CA) 证书添加到服务器信任存储区文件中。如果用户的智能卡证书是由中间证书颁发机构颁发的，则这些证书包括根证书，并且可以包括中间证书。

步骤

- 1 在连接服务器或安全服务器主机的 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\locked.properties`。
- 2 将 `trustKeyfile`、`trustStoretype` 和 `useCertAuth` 属性添加到 `locked.properties` 文件中。
 - a 将 `trustKeyfile` 属性设为您的信任存储区文件名。
 - b 将 `trustStoretype` 设置为 `jks`。
 - c 将 `useCertAuth` 属性设为 `true`，以启用证书身份验证。
- 3 重新启动连接服务器服务或安全服务器服务，使所做的更改生效。

示例：locked.properties 文件

此处所示的文件指定所有受信任用户的根证书位于 `lonqa.key` 文件中，将信任存储区类型设置为 `jks`，并启用了证书身份验证。

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
```

后续步骤

如果您为连接服务器实例配置了智能卡身份验证，请在 **Horizon Administrator** 中配置智能卡身份验证设置。您无需为安全服务器配置智能卡身份验证设置。在 **Horizon** 连接服务器实例上配置的设置也会应用于配对的安全服务器。

在 Horizon Administrator 中配置智能卡设置

您可以使用 **Horizon Administrator** 指定设置，以适应不同的智能卡身份验证情形。

当您在连接服务器实例上配置这些设置时，这些设置还将应用于与其配对的安全服务器。

前提条件

- 在连接服务器主机上修改连接服务器配置属性。
- 确认 **Horizon Client** 直接与连接服务器或安全服务器主机建立 **HTTPS** 连接。如果将 **TLS** 负载分流到中间设备，将不支持智能卡身份验证。

步骤

- 1 在 **Horizon Administrator** 中，选择 **View 配置 > 服务器**。
- 2 在 **连接服务器** 选项卡上，选择连接服务器实例，并单击 **编辑**。

3 要为远程桌面和应用程序用户配置智能卡身份验证，请执行以下步骤。

- a 在**身份验证**选项卡上，从“**View 身份验证**”部分的**用户的智能卡身份验证**下拉菜单中选择一个配置选项。

选项	操作
不允许	在该连接服务器实例上禁用了智能卡身份验证。
可选	用户可以使用智能卡身份验证或密码身份验证连接到该连接服务器实例。如果智能卡身份验证失败，用户就必须提供密码。
需要	<p>用户连接到该连接服务器实例时必须使用智能卡身份验证。</p> <p>要求进行智能卡身份验证时，连接到连接服务器实例时选择以当前用户身份登录复选框的用户的身份验证将失败。这些用户登录到连接服务器时必须用智能卡和 PIN 码重新进行身份验证。</p> <p>注 智能卡身份验证仅可替换 Windows 密码身份验证。如果已启用 SecuriD，用户就必须同时使用 SecuriD 和智能卡身份验证机制进行身份验证。</p>

- b 配置智能卡移除策略。

当智能卡身份验证被设置为**不允许**时，您无法配置智能卡移除策略。

选项	操作
用户移除智能卡后断开用户与 View 连接服务器的连接。	选择 移除智能卡时断开用户会话 复选框。
在用户移除智能卡时保持用户与 View 连接服务器的连接，并允许用户无需重新进行身份验证即可启动新的桌面或应用程序会话。	取消选择 移除智能卡时断开用户会话 复选框。

智能卡移除策略不适用于在选择了**以当前用户身份登录**复选框的情况下连接连接服务器实例的用户，即使他们使用智能卡来登录到其客户端系统，也无法使用此策略。

- c 配置智能卡用户名提示功能。

当智能卡身份验证被设置为**不允许**时，您无法配置智能卡用户名提示功能。

选项	操作
允许用户使用单个智能卡证书对多个用户帐户进行身份验证。	选中 允许智能卡用户名提示 复选框。
禁止用户使用单个智能卡证书对多个用户帐户进行身份验证。	取消选中 允许智能卡用户名提示 复选框。

- 4 要为登录到 **Horizon Administrator** 的管理员配置智能卡身份验证，请单击 **身份验证** 选项卡，然后从“**View 管理身份验证**”部分的 **管理员的智能卡身份验证** 下拉菜单中选择一个配置选项。

选项	操作
不允许	在该连接服务器实例上禁用了智能卡身份验证。
可选	管理员可以使用智能卡身份验证或密码身份验证方式登录到 Horizon Administrator 。如果智能卡身份验证失败，管理员必须提供密码。
需要	管理员必须在登录到 Horizon Administrator 时使用智能卡身份验证。

- 5 单击 **确定**。

- 6 重新启动连接服务器服务。

必须重新启动连接服务器服务，对智能卡设置所做的更改才能生效，但有一个例外。您可以在 **可选** 和 **必需** 之间更改智能卡身份验证设置，而无需重新启动连接服务器服务。

智能卡设置的更改不会影响当前已登录的用户和管理员。

后续步骤

如果需要，准备 **Active Directory** 以进行智能卡身份验证。请参阅 [为智能卡身份验证准备 Active Directory](#)。

验证智能卡身份验证配置。请参阅 [验证智能卡身份验证配置](#)。

在第三方解决方案上配置智能卡身份验证

第三方解决方案（如负载均衡器和网关）可以传送包含智能卡的 **X.590** 证书和加密的 **PIN** 的 **SAML** 声明以执行智能卡身份验证。

本主题简要说明了在设置第三方解决方案以完成以下操作时涉及的任务：在伙伴设备验证相关的 **X.590** 证书后，为连接服务器提供该证书。由于该功能使用 **SAML** 身份验证，其中的一个任务是在 **Horizon Administrator** 中创建 **SAML** 身份验证器。

有关在 **Unified Access Gateway** 上配置智能卡身份验证的信息，请参阅《部署和配置 **Unified Access Gateway**》。

步骤

- 1 为第三方网关或负载均衡器创建一个 **SAML** 身份验证器。
请参阅 [在 Horizon Administrator 中配置 SAML 身份验证器](#)。
- 2 延长连接服务器元数据的过期时间，以免远程会话在 24 小时后就终止。
请参阅 [在连接服务器上更改服务提供程序元数据的过期时间](#)。
- 3 如有必要，请配置第三方设备以使用连接服务器中的服务提供程序元数据。
请参阅第三方设备的产品文档。
- 4 在第三方设备上配置智能卡设置。
请参阅第三方设备的产品文档。

为智能卡身份验证准备 Active Directory

实施智能卡身份验证时，您可能需要在 Active Directory 中执行特定的任务。

- **为智能卡用户添加 UPN**

由于智能卡登录依赖用户主体名称 (UPN)，因此在 Horizon 7 中使用智能卡进行身份验证的用户和管理员的 Active Directory 帐户必须具备有效的 UPN。

- **将根证书添加到 Enterprise NTAAuth 存储**

如果使用 CA 颁发智能卡登录或域控制器证书，则必须将根证书添加到 Active Directory 中的 Enterprise NTAAuth 存储。如果 Windows 域控制器充当根 CA，则不需要执行此步骤。

- **将根证书添加到受信任的根证书颁发机构**

如果使用证书颁发机构 (CA) 颁发智能卡登录或域控制器证书，则必须将根证书添加到 Active Directory 中受信任的根证书颁发机构组策略中。如果 Windows 域控制器充当根 CA，则不需要执行此步骤。

- **将中间证书添加到中间证书颁发机构**

如果使用中间证书颁发机构 (CA) 颁发智能卡登录或域控制器证书，则必须将中间证书添加到 Active Directory 的中间证书颁发机构组策略中。

为智能卡用户添加 UPN

由于智能卡登录依赖用户主体名称 (UPN)，因此在 Horizon 7 中使用智能卡进行身份验证的用户和管理员的 Active Directory 帐户必须具备有效的 UPN。

如果智能卡用户所在的域和颁发根证书的域不同，您必须将用户的 UPN 设置为受信任 CA 的根证书内包含的使用者备用名称 (SAN)。如果您的根证书是从智能卡用户当前所在域中的服务器上颁发的，则不需要修改用户的 UPN。

注 即便是从同一个域颁发证书，您仍然可能需要设置内置 Active Directory 帐户的 UPN。内置帐户（包括 Administrator 帐户）在默认情况下未设置 UPN。

前提条件

- 通过查看证书属性，获取受信任 CA 的根证书中包含的 SAN。
- 如果您的 Active Directory 服务器上没有“ADSI 编辑”实用程序，请从 Microsoft 网站下载并安装相应的 Windows 支持工具。

步骤

- 1 在 Active Directory 服务器上，启动“ADSI 编辑”实用程序。
- 2 在左侧窗格中，展开用户所在的域并双击 CN=Users。
- 3 在右侧窗格中，右键单击用户，然后单击**属性**。
- 4 双击 userPrincipalName 属性并键入受信任 CA 证书的 SAN 值。
- 5 单击**确定**保存属性设置。

将根证书添加到 Enterprise NTAAuth 存储

如果使用 CA 颁发智能卡登录或域控制器证书，则必须将根证书添加到 Active Directory 中的 Enterprise NTAAuth 存储。如果 Windows 域控制器充当根 CA，则不需要执行此步骤。

步骤

- ◆ 在 Active Directory 服务器上使用 `certutil` 命令，将证书发布到 Enterprise NTAAuth 存储区中。

例如：`certutil -dspublish -f CA 根证书路径 NTAAuthCA`

此时该 CA 即为颁发此类证书的受信任机构。

将根证书添加到受信任的根证书颁发机构

如果使用证书颁发机构 (CA) 颁发智能卡登录或域控制器证书，则必须将根证书添加到 Active Directory 中受信任的根证书颁发机构组策略中。如果 Windows 域控制器充当根 CA，则不需要执行此步骤。

步骤

- 1 在 Active Directory 服务器上，导航至组策略管理插件。

AD 版本	导航路径
Windows 2003	<ol style="list-style-type: none"> a 选择开始 > 所有程序 > 管理工具 > Active Directory 用户和计算机。 b 右键单击域，然后单击属性。 c 在组策略选项卡上，单击打开以打开组策略管理插件。 d 右键单击默认域策略并单击编辑。
Windows 2008	<ol style="list-style-type: none"> a 选择开始 > 管理工具 > 组策略管理。 b 展开您的域，右键单击默认域策略并单击编辑。
Windows 2012 R2	<ol style="list-style-type: none"> a 选择开始 > 管理工具 > 组策略管理。 b 展开您的域，右键单击默认域策略并单击编辑。
Windows 2016	<ol style="list-style-type: none"> a 选择开始 > 管理工具 > 组策略管理。 b 展开您的域，右键单击默认域策略并单击编辑。

- 2 展开计算机配置区域，然后打开 Windows 设置\安全性设置\公钥。
- 3 右键单击受信任的根证书颁发机构，然后选择导入。
- 4 按照向导中的提示导入根证书（如 rootCA.cer）并单击确定。
- 5 关闭“组策略”窗口。

此时，域中的所有系统在其信任的根存储中都有一个根证书的副本。

后续步骤

如果中间证书颁发机构 (CA) 为您颁发了智能卡登录或域控制器证书，请将此中间证书添加到 Active Directory 中的中间证书颁发机构组策略中。请参阅[将中间证书添加到中间证书颁发机构](#)。

将中间证书添加到中间证书颁发机构

如果使用中间证书颁发机构 (CA) 颁发智能卡登录或域控制器证书，则必须将中间证书添加到 Active Directory 的中间证书颁发机构组策略中。

步骤

- 1 在 Active Directory 服务器上，导航至组策略管理插件。

AD 版本	导航路径
Windows 2003	<ol style="list-style-type: none"> a 选择开始 > 所有程序 > 管理工具 > Active Directory 用户和计算机。 b 右键单击域，然后单击属性。 c 在组策略选项卡上，单击打开以打开组策略管理插件。 d 右键单击默认域策略并单击编辑。
Windows 2008	<ol style="list-style-type: none"> a 选择开始 > 管理工具 > 组策略管理。 b 展开您的域，右键单击默认域策略并单击编辑。
Windows 2012 R2	<ol style="list-style-type: none"> a 选择开始 > 管理工具 > 组策略管理。 b 展开您的域，右键单击默认域策略并单击编辑。
Windows 2016	<ol style="list-style-type: none"> a 选择开始 > 管理工具 > 组策略管理。 b 展开您的域，右键单击默认域策略并单击编辑。

- 2 展开**计算机配置**区域，然后打开 **Windows 设置\安全性设置\公钥策略**。
- 3 右键单击**中间证书颁发机构**，然后选择**导入**。
- 4 按照向导中的提示导入中间证书（如 **intermediateCA.cer**）并单击**确定**。
- 5 关闭“组策略”窗口。

此时，域中的所有系统在其中间证书颁发机构存储区中都有一个中间证书的副本。

验证智能卡身份验证配置

当您首次设置智能卡身份验证后，或智能卡身份验证无法正常工作，应检查您的智能卡身份验证配置。

步骤

- 确认每个客户端系统都配有智能卡中间件、带有有效证书的智能卡以及智能卡读卡器。确认最终用户有 Horizon Client。

有关配置智能卡软件和硬件的信息，请参见您的智能卡供应商提供的文档。

- 在每个客户端系统上，选择**开始 > 设置 > 控制面板 > Internet 选项 > 内容 > 证书 > 个人**以验证证书是否可用于智能卡身份验证。

当用户或管理员将智能卡插入智能卡读卡器时，Windows 将证书从智能卡复制到用户的计算机。客户端系统上的应用程序（包括 Horizon Client）可以使用这些证书。

- 在连接服务器或安全服务器主机的 `locked.properties` 文件中，检查 `useCertAuth` 的属性是否被设置为 **true** 且拼写正确。

`locked.properties` 文件位于 `install_directory\VMware\VMware`

`View\Server\sslgateway\conf` 中。`useCertAuth` 属性通常会被错误地拼写为 `userCertAuth`。

- 如果您在连接服务器实例上配置了智能卡身份验证，请在 **Horizon Administrator** 中检查智能卡的身份验证设置。
 - a 选择 **View 配置 > 服务器**。
 - b 在**连接服务器**选项卡上，选择连接服务器实例，并单击**编辑**。
 - c 如果为用户配置了智能卡身份验证，则在**身份验证**选项卡上，验证用户的智能卡身份验证是否设置为**可选或必需**。
 - d 如果为管理员配置了智能卡身份验证，则在**身份验证**选项卡上，验证**管理员智能卡身份验证**是否设置为**可选或必需**。

必须重新启动连接服务器服务，对智能卡设置所做的更改才能生效。

- 如果智能卡用户所在的域不是颁发根证书的域，请验证用户的 **UPN** 是否设置为受信任 **CA** 的根证书内包含的 **SAN**。
 - a 通过查看证书属性，找出受信任 **CA** 的根证书中包含的 **SAN**。
 - b 在 **Active Directory** 服务器上，选择**开始 > 管理工具 > Active Directory 用户和计算机**。
 - c 右键单击**用户**文件夹中的用户，然后选择**属性**。
UPN 显示在**帐户**选项卡上的**用户登录名**文本框中。
- 如果智能卡用户选择使用 **PCoIP** 显示协议或 **VMware Blast** 显示协议连接到单会话桌面，请确认单用户计算机上已安装称为智能卡重定向的 **View Agent** 或 **Horizon Agent** 组件。通过智能卡功能，用户可以使用智能卡登录到单会话桌面。已安装“远程桌面服务”角色的 **RDS** 主机自动支持智能卡功能，因而您无需安装该功能。
- 检查连接服务器或安全服务器主机上的 `drive:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` 中的日志文件中的消息是否指明已启用智能卡身份验证。

使用智能卡证书撤销检查

通过配置证书撤销检查，可以阻止已撤销用户证书的用户通过智能卡进行身份验证。当用户离开组织、丢失智能卡或从一个部门调往另一个部门时，其证书通常会被撤销。

Horizon 7 支持通过证书撤销列表 (Certificate Revocation List, CRL) 和联机证书状态协议 (Online Certificate Status Protocol, OCSP) 进行证书撤销检查。CRL 是由颁发证书的 **CA** 发布的吊销证书列表。OCSP 是一种证书验证协议，用于获取 **X.509** 证书的撤销状态。

您可以在连接服务器实例或安全服务器上配置证书撤销检查。如果连接服务器实例与安全服务器配对，则您要在安全服务器上配置证书撤销检查。CA 必须能够从连接服务器或安全服务器主机上访问。

您可以在同一个连接服务器实例或安全服务器上配置 CRL 和 OCSP。如果您配置了两种类型的证书撤销检查，Horizon 7 会首先尝试使用 OCSP 检查，如果 OCSP 检查失败，则转而进行 CRL 检查。如果 CRL 失败，Horizon 7 不会改用 OCSP。

- [登录时进行 CRL 检查](#)

如果配置了 CRL 检查，Horizon 7 会构造并读取 CRL 以确定用户证书的撤销状态。

- [登录时进行 OCSP 证书撤销检查](#)

如果您配置了 OCSP 证书撤销检查，Horizon 7 会向 OCSP Responder 发送请求，以确定特定用户证书的撤销状态。Horizon 7 将使用 OCSP 签发证书，以检验它从 OCSP Responder 收到的响应的真伪。

- [配置 CRL 检查](#)

如果您配置了 CRL 检查，Horizon 7 将读取 CRL，以确定智能卡用户证书的撤销状态。

- [配置 OCSP 证书撤销检查](#)

如果您配置了 OCSP 证书撤销检查，Horizon 7 会向 OCSP Responder 发送验证请求，以确定智能卡用户证书的撤销状态。

- [智能卡证书撤销检查属性](#)

您可以设置 `locked.properties` 文件中的值，以启用和配置智能卡证书撤销检查。

登录时进行 CRL 检查

如果配置了 CRL 检查，Horizon 7 会构造并读取 CRL 以确定用户证书的撤销状态。

如果证书已撤销，并且智能卡身份验证是可选操作，则**输入您的用户名和密码**对话框将出现，而用户必须提供密码进行身份验证。如果必须进行智能卡身份验证，用户会收到错误消息，并且被禁止进行身份验证。如果 Horizon 7 无法读取 CRL，也会发生同样的事件。

登录时进行 OCSP 证书撤销检查

如果您配置了 OCSP 证书撤销检查，Horizon 7 会向 OCSP Responder 发送请求，以确定特定用户证书的撤销状态。Horizon 7 将使用 OCSP 签发证书，以检验它从 OCSP Responder 收到的响应的真伪。

如果用户证书已撤销，并且智能卡身份验证是可选操作，则**输入您的用户名和密码**对话框将出现，而用户必须提供密码进行身份验证。如果必须进行智能卡身份验证，用户会收到错误消息，并且被禁止进行身份验证。

如果 Horizon 7 没有收到 OCSP Responder 的响应或响应无效，就会重新进行 CRL 检查。

配置 CRL 检查

如果您配置了 CRL 检查，Horizon 7 将读取 CRL，以确定智能卡用户证书的撤销状态。

前提条件

熟悉用于 CRL 检查的 `locked.properties` 文件属性。请参阅[智能卡证书撤销检查属性](#)。

步骤

- 1 在连接服务器或安全服务器主机的 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\locked.properties`。
- 2 将 `enableRevocationChecking` 和 `crlLocation` 属性添加到 `locked.properties` 文件中。
 - a 将 `enableRevocationChecking` 属性设为 **true**, 以启用智能卡证书撤销检查。
 - b 将 `crlLocation` 属性设为 CRL 的地址。此值可以是 URL 或文件路径。
- 3 重新启动连接服务器服务或安全服务器服务, 使所做的更改生效。

示例: `locked.properties` 文件

列出的文件可启用智能卡身份验证和智能卡证书撤销检查, 配置 CRL 检查并为 CRL 位置指定一个 URL。

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
crlLocation=http://root.ocsp.net/certEnroll/ocsp-R00T_CA.crl
```

配置 OCSP 证书撤销检查

如果您配置了 OCSP 证书撤销检查, Horizon 7 会向 OCSP Responder 发送验证请求, 以确定智能卡用户证书的撤销状态。

前提条件

熟悉用于 OCSP 证书撤销检查的 `locked.properties` 文件属性。请参阅[智能卡证书撤销检查属性](#)。

步骤

- 1 在连接服务器或安全服务器主机的 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\locked.properties`。
- 2 将 `enableRevocationChecking`、`enableOCSP`、`ocspURL` 和 `ocspSigningCert` 属性添加到 `locked.properties` 文件中。
 - a 将 `enableRevocationChecking` 属性设为 **true**, 以启用智能卡证书撤销检查。
 - b 将 `enableOCSP` 属性设为 **true**, 以启用 OCSP 证书撤销检查。
 - c 将 `ocspURL` 设为 OCSP Responder 的 URL。
 - d 将 `ocspSigningCert` 属性设为包含 OCSP Responder 签发证书的文件的位罝。
- 3 重新启动连接服务器服务或安全服务器服务, 使所做的更改生效。

示例：locked.properties 文件

列出的文件可启用智能卡身份验证和智能卡证书撤销检查，配置 CRL 与 OCSP 证书撤销检查，指定 OCSP Responder 的位置，并识别包含 OCSP 签发证书的文件。

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.lonqa.int/ocsp
```

智能卡证书撤销检查属性

您可以设置 `locked.properties` 文件中的值，以启用和配置智能卡证书撤销检查。

表 3-1 列出了证书撤销检查的 `locked.properties` 文件属性。

表 3-1. 智能卡证书撤销检查属性

属性	说明
<code>enableRevocationChecking</code>	将该属性设为 true 可启用证书撤销检查。 如果该属性设为 false ，则禁用证书撤销检查，并忽略其他所有证书撤销检查属性。 默认值为 false 。
<code>crlLocation</code>	指定 CRL 的位置，可以是 URL 或文件路径。 如果您不指定 URL 或者指定的 URL 无效，在 <code>allowCertCRLs</code> 被设为 true 或尚未指定时，Horizon 7 将使用用户证书上的 CRL 列表。 如果 Horizon 7 无法访问 CRL，则 CRL 检查将会失败。
<code>allowCertCRLs</code>	如果该属性设为 true ，Horizon 7 将从用户证书中提取 CRL 列表。 默认值为 true 。
<code>enableOCSP</code>	将该属性设为 true 可启用 OCSP 证书撤销检查。 默认值为 false 。
<code>ocspURL</code>	指定 OCSP Responder 的 URL。
<code>ocspResponderCert</code>	指定包含 OCSP Responder 签发证书的文件。Horizon 7 使用该证书检验 OCSP Responder 响应的真伪。
<code>ocspSendNonce</code>	如果该属性设为 true ，nonce 将会随 OCSP 请求发送，以防止重复响应。 默认值为 false 。
<code>ocspCRLFailover</code>	该属性设为 true 时，如果 OCSP 证书撤销检查失败，Horizon 7 将进行 CRL 检查。 默认值为 true 。

设置其他类型的用户身份验证

Horizon 7 可利用您现有的 **Active Directory** 基础架构对用户和管理员进行身份验证和管理。除了智能卡身份验证之外，您还可以将 **Horizon 7** 与其他形式的身份验证（例如，生物识别身份验证或双因素身份验证解决方案，如 **RSA SecurID** 和 **RADIUS**）相集成，以对远程桌面和应用程序用户进行身份验证。

本章讨论了以下主题：

- [使用双因素身份验证](#)
- [使用 SAML 身份验证](#)
- [配置生物身份验证](#)

使用双因素身份验证

您可以配置 **Horizon** 连接服务器实例，以便要求用户使用 **RSA SecurID** 身份验证或 **RADIUS**（远程身份验证拨入用户服务）身份验证。

- **RADIUS** 支持提供了各种基于令牌的备用双因素身份验证选项。
- **Horizon 7** 还提供了一个开放的标准扩展接口，以允许第三方解决方案供应商将高级身份验证扩展集成到 **Horizon 7** 中。

由于双因素身份验证解决方案（如 **RSA SecurID** 和 **RADIUS**）需要使用安装在不同服务器上的身份验证管理器，因此您必须配置这些服务器并使其可供连接服务器主机访问。例如，如果您使用 **RSA SecurID**，则身份验证管理器将会是 **RSA Authentication Manager**。如果您使用 **RADIUS**，则身份验证管理器将会是 **RADIUS** 服务器。

要使用双因素身份验证，每个用户必须具有由其身份验证管理器注册的令牌（如 **RSA SecurID** 令牌）。双因素身份验证令牌是一个可以按固定间隔生成身份验证代码的硬件或软件。通常身份验证需要同时提供 **PIN** 码和身份验证代码。

如果您有多个连接服务器实例，则可以在一些实例上配置双因素身份验证，在另一些实例上配置其他的用户身份验证方法。例如，您可以仅为那些通过 **Internet** 从企业网络外部访问远程桌面和应用程序的用户配置双因素身份验证。

Horizon 7 通过了 **RSA SecurID Ready** 程序的认证，支持各种 **SecurID** 功能，包括新建 **PIN** 模式、下一个令牌代码模式、**RSA Authentication Manager** 以及负载平衡等。

- [使用双因素身份验证登录](#)

当用户连接到启用了 **RSA SecurID** 身份验证或 **RADIUS** 身份验证的 **View** 连接服务器实例时，**Horizon Client** 中将显示特殊登录对话框。

- 在 [Horizon Administrator](#) 中启用双因素身份验证

通过在 [Horizon Administrator](#) 中修改连接服务器设置，您可以为连接服务器实例启用 RSA SecurID 身份验证或 RADIUS 身份验证。

- 排除 [RSA SecurID](#) 访问被拒故障

Horizon Client 通过 RSA SecurID 身份验证进行连接时，访问被拒绝。

- 排除 [RADIUS](#) 访问被拒故障

Horizon Client 通过 RADIUS 双因素身份验证进行连接时访问被拒绝。

使用双因素身份验证登录

当用户连接到启用了 RSA SecurID 身份验证或 RADIUS 身份验证的 View 连接服务器实例时，Horizon Client 中将显示特殊登录对话框。

用户在特殊登录对话框中输入其 RSA SecurID 或 RADIUS 身份验证的用户名和通行码。双重身份验证的通行码通常由 PIN 后跟令牌代码组成。

- 用户输入其 RSA SecurID 用户名和通行码后，如果 RSA Authentication Manager 要求输入新的 RSA SecurID PIN 码，将出现 PIN 码对话框。设置新的 PIN 码后，系统将提示用户先等待下一个令牌代码再登录。如果 RSA Authentication Manager 配置为采用系统生成的 PIN 码，将出现确认 PIN 码的对话框。
- 登录 Horizon 7 时，RADIUS 身份验证的工作方式与 RSA SecurID 很像。如果 RADIUS 服务器发出访问质询，Horizon Client 会显示与 RSA SecurID 的下一令牌代码提示相似的对话框。目前支持的 RADIUS 质询仅限于提示输入文本。不显示 RADIUS 服务器发出的任何质询文本。目前不支持更复杂格式的质询，如多项选择和图像选择。

用户在 Horizon Client 中输入凭据后，RADIUS 服务器可以向用户的手机发送一条包含代码的文字短信或电子邮件或者文本（使用其他消息外发机制）。用户可以将此文本和代码输入 Horizon Client 来完成身份验证。

- 由于某些 RADIUS 供应商提供从 Active Directory 导入用户的功能，因此在提示用户输入 RADIUS 身份验证用户名和通行码之前，可能会先提示他们提供 Active Directory 凭据。

在 Horizon Administrator 中启用双因素身份验证

通过在 [Horizon Administrator](#) 中修改连接服务器设置，您可以为连接服务器实例启用 RSA SecurID 身份验证或 RADIUS 身份验证。

前提条件

在身份验证管理器服务器上安装并配置双因素身份验证软件，如 RSA SecurID 软件或 RADIUS 软件。

- 对于 RSA SecurID 身份验证，从 RSA Authentication Manager 中导出连接服务器实例的 `sdconf.rec` 文件。请参阅 [RSA Authentication Manager](#) 文档。
- 对于 RADIUS 身份验证，请遵循供应商的配置文档。记录 RADIUS 服务器的主机名或 IP 地址、其侦听 RADIUS 身份验证的端口号（通常为 1812）、身份验证类型（PAP、CHAP、MS-CHAPv1 或 MS-CHAPv2）以及共享密码。您将会在 [Horizon Administrator](#) 中输入这些值。可以为主要和辅助 RADIUS 身份验证器输入这些值。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。
- 2 在**连接服务器**选项卡中，选择服务器，然后单击**编辑**。
- 3 在**身份验证**选项卡上，从“高级身份验证”部分中的**双因素身份验证**下拉列表中选择 **RSA SecurID** 或 **RADIUS**。
- 4 要强制要求 RSA SecurID 或 RADIUS 用户名与 Active Directory 中的用户名匹配，请选择**强制要求 SecurID 与 Windows 用户名匹配**或**强制要求双因素与 Windows 用户名匹配**。

如果选择此选项，用户必须使用同一 RSA SecurID 或 RADIUS 用户名进行 Active Directory 身份验证。如果不选择此选项，则可以使用不同的用户名。

- 5 对于 RSA SecurID，单击**上传文件**，键入 `sdconf.rec` 文件的位置，或单击**浏览**搜索该文件。
- 6 对于 RADIUS 身份验证，完成其余字段：

- a 如果初始 RADIUS 身份验证使用可触发令牌代码带外传输的 Windows 身份验证，且此令牌代码用作 RADIUS 质询的一部分，则选择**使用相同的用户名和密码进行 RADIUS 和 Windows 身份验证**。

如果您选中此复选框，则在 RADIUS 身份验证使用 Windows 用户名和密码时，将不会在 RADIUS 身份验证后提示用户输入 Windows 凭据。用户不必在 RADIUS 身份验证后重新输入 Windows 用户名和密码。

- b 从**身份验证器**下拉列表中，选择**创建新的身份验证器**，并完成此页。

- 如果您不希望启用 RADIUS 计帐，请将**记帐端口**设置为 **0**。仅在您的 RADIUS 服务器支持收集计帐数据时，将此端口设置为非零数字。如果 RADIUS 服务器不支持计帐消息，且您将此端口设置为非零数字，则将发送并忽略这些消息，然后重试多次，从而导致身份验证发生延迟。

可使用计帐数据来根据使用时间和数据给用户开具帐单。还可将计帐数据用于统计目的和常规的网络监视。

- 如果指定领域前缀字符串，则会将其放在用户名的开头并发送到 RADIUS 服务器。例如，如果在 Horizon Client 中输入的用户名为 `jdoe`，且指定领域前缀 `DOMAIN-A\`，则会将用户名 `DOMAIN-A\jdoe` 发送到 RADIUS 服务器。同样，如果使用领域后缀或词尾字符串 `@mycorp.com`，则会将用户名 `jdoe@mycorp.com` 发送到 RADIUS 服务器。

- 7 单击**确定**保存更改。

您无需重新启动连接服务器服务。系统将自动分发必要的配置文件，配置设置可立即生效。

当用户打开 Horizon Client 并向连接服务器进行身份验证时，系统将提示他们进行双因素身份验证。对于 RADIUS 身份验证，登录对话框将显示包含您指定的令牌标签的文本提示。

更改 RADIUS 身份验证设置将会影响在更改配置后启动的远程桌面和应用程序会话。当前会话不会受到 RADIUS 身份验证设置更改的影响。

后续步骤

如果您具有连接服务器实例的副本组，且希望也对其设置 RADIUS 身份验证，则可以重新使用现有的 RADIUS 身份验证器配置。

排除 RSA SecurID 访问被拒故障

Horizon Client 通过 RSA SecurID 身份验证进行连接时，访问被拒绝。

问题

使用 RSA SecurID 的 Horizon Client 连接显示 Access Denied（访问被拒绝），并且 RSA Authentication Manager 日志监视器显示错误消息 Node Verification Failed（验证节点失败）。

原因

此时需重置 RSA Agent 主机节点秘密。

解决方案

- 1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。
- 2 在 **连接服务器** 选项卡上，选择连接服务器，然后单击 **编辑**。
- 3 在 **身份验证** 选项卡上，选择 **清除节点密钥**。
- 4 单击 **确定** 清除节点密钥。
- 5 在运行 RSA Authentication Manager 的计算机上，选择 **开始 > 程序 > RSA Security > RSA Authentication Manager Host Mode**。
- 6 选择 **代理主机 > 编辑代理主机**。
- 7 从列表中选择 **View 连接服务器** 并取消选择 **已创建节点秘密** 复选框。
每当您进行编辑时，将默认选中 **已创建节点秘密**。
- 8 单击 **确定**。

排除 RADIUS 访问被拒故障

Horizon Client 通过 RADIUS 双因素身份验证进行连接时访问被拒绝。

问题

使用 RADIUS 双因素身份验证进行 Horizon Client 连接时显示 Access Denied。

原因

RADIUS 没有收到 RADIUS 服务器的回复，从而导致 Horizon 7 超时。

解决方案

以下常见的配置错误通常会导致出现这种情况：

- 尚未将 RADIUS 服务器配置为接受 View 连接服务器实例作为 RADIUS 客户端。必须将使用 RADIUS 的每个 View 连接服务器实例设置为 RADIUS 服务器上的客户端。请参阅您的 RADIUS 双因素身份验证产品对应的文档。
- View 连接服务器实例和 RADIUS 服务器上的共享密码值不匹配。

使用 SAML 身份验证

安全断言标记语言 (SAML) 是一种基于 XML 的标准，用于在不同安全域之间描述和交换身份验证及授权信息。SAML 使用称为 SAML 断言的 XML 文档在身份提供程序与服务提供程序之间传递有关用户的信息。

您可以使用 SAML 身份验证将 Horizon 7 与 VMware Workspace ONE、VMware Identity Manager 或者合格的第三方负载均衡器或网关相集成。为第三方设备配置 SAML 时，请参阅供应商文档以了解有关配置 Horizon 7 以便与该设备配合使用的信息。如果启用了 SSO，登录到 VMware Identity Manager 或第三方设备的用户无需再次进行登录，即可启动远程桌面和应用程序。您还可以使用 SAML 身份验证在 VMware Access Point 或第三方设备上实施智能卡身份验证。

要将身份验证职责委派给 Workspace ONE、VMware Identity Manager 或第三方设备，您必须在 Horizon 7 中创建一个 SAML 身份验证器。SAML 身份验证器包含在 Horizon 7 与 Workspace ONE、VMware Identity Manager 或第三方设备之间交换的信任和元数据信息。您需要将 SAML 身份验证器与连接服务器实例进行关联。

为 VMware Identity Manager 集成使用 SAML 身份验证

Horizon 7 与 VMware Identity Manager（以前称为 Workspace ONE）的集成使用 SAML 2.0 标准建立相互信任关系，这对于单点登录 (Single Sign-On, SSO) 功能而言很重要。如果启用了 SSO，使用 Active Directory 凭据登录到 VMware Identity Manager 或 Workspace ONE 的用户无需再次进行登录，即可启动远程桌面和应用程序。

将 VMware Identity Manager 与 Horizon 7 集成后，VMware Identity Manager 会在用户登录到 VMware Identity Manager 并单击桌面或应用程序图标时生成唯一的 SAML 项目。VMware Identity Manager 将使用此 SAML 项目创建一个统一资源标识符 (Universal Resource Identifier, URI)。该 URI 中包含有关桌面或应用程序池所在的连接服务器实例、要启动哪个桌面或应用程序以及 SAML 项目的信息。

VMware Identity Manager 将 SAML 项目发送到 Horizon Client，Horizon Client 转而又将该项目发送到连接服务器实例。连接服务器实例使用 SAML 项目从 VMware Identity Manager 中检索 SAML 断言。

连接服务器实例检索到 SAML 断言后，会验证该断言、解密用户的密码，然后使用解密的密码启动桌面或应用程序。

设置 VMware Identity Manager 与 Horizon 7 的集成涉及到使用 Horizon 7 信息配置 VMware Identity Manager 以及配置 Horizon 7 将身份验证职责委托给 VMware Identity Manager。

要将身份验证职责委托给 VMware Identity Manager，您必须在 Horizon 7 中创建一个 SAML 身份验证器。SAML 身份验证器包含 Horizon 7 与 VMware Identity Manager 之间的信任和元数据交换信息。您需要将 SAML 身份验证器与连接服务器实例进行关联。

注 如果您想要通过 VMware Identity Manager 提供对桌面和应用程序的访问，请确认您在 Horizon Administrator 中以拥有根访问组的管理员角色的用户身份来创建桌面和应用程序池。如果您向用户提供根访问组以外的其他访问组的管理员角色，VMware Identity Manager 将不会识别您在 Horizon 7 中配置的 SAML 身份验证器，并且您也将无法在 VMware Identity Manager 中配置池。

在 Horizon Administrator 中配置 SAML 身份验证器

要从 VMware Identity Manager 中启动远程桌面和应用程序，或者通过第三方负载均衡器或网关连接到远程桌面和应用程序，您必须在 Horizon Administrator 中创建一个 SAML 身份验证器。SAML 身份验证器包含 Horizon 7 和客户端连接到的设备之间交换的信任 and 元数据信息。

您需要将 SAML 身份验证器与连接服务器实例进行关联。如果您的部署包括多个连接服务器实例，则必须将 SAML 身份验证器与每个实例都进行关联。

您可以同时启用一个静态身份验证器和多个动态身份验证器。您可以配置 vIDM（动态）和 Unified Access Gateway（静态）身份验证器并将其保持活动状态。您可以通过这两种身份验证器之一建立连接。

您可以在连接服务器上配置多个 SAML 身份验证器，并且所有身份验证器可以同时处于活动状态。不过，在连接服务器上配置各个 SAML 身份验证器的实体 ID 不能相同。

仪表板中的 SAML 身份验证器的状态始终是绿色的，因为它实质上是静态的预定义元数据。红色和绿色切换仅适用于动态身份验证器。

有关为 VMware Unified Access Gateway 设备配置 SAML 身份验证器的信息，请参阅《部署和配置 Unified Access Gateway》。

前提条件

- 确认安装并配置了 Workspace ONE、VMware Identity Manager 或者第三方网关或负载均衡器。请参阅该产品的安装文档。
- 确认连接服务器主机上安装了 SAML 服务器证书的签名 CA 的根证书。VMware 建议不要配置 SAML 身份验证器使用自签名证书。有关证书身份验证的信息，请参阅《Horizon 7 安装指南》文档。
- 记下 Workspace ONE 服务器、VMware Identity Manager 服务器或面向外部的负载均衡器的 FQDN 或 IP 地址。
- （可选）如果您使用 Workspace ONE 或 VMware Identity Manager，则记下连接器 Web 界面的 URL。
- 如果您为要求生成 SAML 元数据并创建静态身份验证器的 Unified Access Gateway 或第三方设备创建身份验证器，则在设备上执行此过程以生成 SAML 元数据，然后复制该元数据。

步骤

- 1 在 Horizon Administrator 中，选择**配置 > 服务器**。
- 2 在**连接服务器**选项卡上，选择一个要与 SAML 身份验证器关联的服务器实例，然后单击**编辑**。

- 在身份验证选项卡上，从将身份验证委派给 VMware Horizon (SAML 2.0 身份验证器) 下拉菜单中选择一项设置来启用或禁用 SAML 身份验证器。

选项	说明
已禁用	禁用 SAML 身份验证。您只能从 Horizon Client 中启动远程桌面和应用程序。
已允许	启用 SAML 身份验证。您可以从 Horizon Client 和 VMware Identity Manager 或第三方设备中启动远程桌面和应用程序。
需要	启用 SAML 身份验证。您只能从 VMware Identity Manager 或第三方设备中启动远程桌面和应用程序。无法从 Horizon Client 中手动启动桌面或应用程序。

您可以根据自己的需要，将部署中的每个连接服务器实例配置为使用不同的 SAML 身份验证设置。

- 单击**管理 SAML 身份验证器**，然后单击**添加**。
- 在“添加 SAML 2.0 身份验证器”对话框中配置 SAML 身份验证器。

选项	说明
类型	对于 Unified Access Gateway 或第三方设备，选择 静态 。对于 VMware Identity Manager，选择 动态 。对于动态身份验证器，您可以指定一个元数据 URL 和一个管理 URL。对于静态身份验证器，您必须先在 Unified Access Gateway 或第三方设备上生成元数据，然后将该元数据复制并粘贴到 SAML 元数据 文本框中。
标签	用于标识 SAML 身份验证器的唯一名称。
说明	SAML 身份验证器的简要描述。此值为可选项。
元数据 URL	（对于动态身份验证器）此 URL 用于检索在 SAML 身份提供程序和连接服务器实例之间交换 SAML 信息所需的全部信息。在 URL <code>https://<YOUR HORIZON SERVER NAME>/SAAS/API/1.0/GET/metadata/idp.xml</code> 中，单击 <YOUR HORIZON SERVER NAME> ，然后将其替换为 VMware Identity Manager 服务器或面向外部的负载均衡器（第三方设备）的 FQDN 或 IP 地址。
管理 URL	（对于动态身份验证器）此 URL 用于访问 SAML 身份提供程序的管理控制台。对于 VMware Identity Manager，此 URL 应指向 VMware Identity Manager Connector Web 界面。此值为可选项。
SAML 元数据	（对于静态身份验证器）您从 Unified Access Gateway 或第三方设备中生成并复制的元数据文本。
已为连接服务器启用	选中此复选框可启用身份验证器。您可以启用多个身份验证器。只有已启用的身份验证器才会显示在列表中。

- 单击**确定**保存 SAML 身份验证器的配置。

如果您提供了有效信息，则必须接受自签名证书（不建议）或为 Horizon 7 和 VMware Identity Manager 或第三方设备使用可信证书。

“管理 SAML 身份验证器”对话框显示新创建的身份验证器。

- 在 Horizon Administrator 仪表板上的“系统运行状况”部分，选择**其他组件 > SAML 2.0 身份验证器**，然后选择您之前添加的 SAML 身份验证器并验证详细信息。

如果配置成功，身份验证器的运行状况将显示为绿色。如果证书不可信、VMware Identity Manager 不可用或者元数据 URL 无效，身份验证器的运行状况可能会显示红色。如果证书不可信，您或许可以单击**验证**来验证和接受该证书。

后续步骤

延长连接服务器元数据的过期时间，以免远程会话在 24 小时后就终止。请参阅[在连接服务器上更改服务提供程序元数据的过期时间](#)。

为 VMware Identity Manager 配置代理支持

Horizon 7 为 VMware Identity Manager (vIDM) 服务器提供了代理支持。代理详细信息（如主机名和端口号）可以在 ADAM 数据库中进行配置，而 HTTP 请求将通过代理来路由。

此功能支持混合部署，在这种部署中，内部部署的 Horizon 7 可以与云中托管的 vIDM 服务器进行通信。

前提条件

步骤

- 1 在您的连接服务器主机上启动“ADSI 编辑”实用程序。
- 2 展开以下对象路径下的 ADAM ADSI 树：
`cd=vdi,dc=vmware,dc=int,ou=Properties,ou=Global,cn=Common Attributes`。
- 3 选择**操作 > 属性**，然后在 **pae-NameValuePair** 属性下，添加新条目 **pae-SAMLProxyName** 和 **pae-SAMLProxyPort**。

在连接服务器上更改服务提供程序元数据的过期时间

如果未更改过期时间，连接服务器将在 24 小时后停止接受来自 SAML 身份验证器（如 Unified Access Gateway 或第三方身份提供程序）的 SAML 断言，并且必须重新执行元数据交换过程。

此过程用于指定在连接服务器停止接受来自身份提供程序的 SAML 断言之前可经过的天数。此数值将在当前过期时间结束时使用。例如，如果当前过期时间为 1 天，而您指定的是 90 天，那么经过 1 天后，连接服务器会生成过期时间为 90 天的元数据。

前提条件

请参阅 Microsoft TechNet 网站，了解如何在您的 Windows 操作系统版本上使用“ADSI 编辑”实用程序。

步骤

- 1 在您的连接服务器主机上启动“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“计算机”窗格中，选择或键入 **localhost:389** 或者连接服务器主机的完全限定域名 (Fully Qualified Domain Name, FQDN) 后跟端口 389。
例如：**localhost:389** 或 **mycomputer.example.com:389**。
- 5 展开“ADSI 编辑”树，展开 **OU=Properties**，选择 **OU=Global**，然后在右侧窗格中双击 **CN=Common**。

- 6 在“属性”对话框中，编辑 **pae-NameValuePair** 属性以添加以下值：

```
cs-samlencryptionkeyvaliditydays=number-of-days
cs-samlsigningkeyvaliditydays=number-of-days
```

在此示例中，*number-of-days* 是在远程连接服务器停止接受 SAML 断言之前经过的天数。在这段时间过后，必须重新执行 SAML 元数据交换过程。

生成 SAML 元数据以便连接服务器可用作服务提供程序

在为要使用的身份提供程序创建并启用 SAML 身份验证器后，可能需要生成连接服务器元数据。您可以使用此元数据在作为身份提供程序的 Unified Access Gateway 设备或第三方负载平衡器上创建服务提供程序。

前提条件

确认您已为以下身份提供程序创建 SAML 身份验证器：Unified Access Gateway 或者第三方负载平衡器或网关。在 Horizon Administrator 仪表板上的“系统运行状况”部分，可以选择其他组件 > SAML 2.0 身份验证器，然后选择您之前添加的 SAML 身份验证器并验证详细信息。

步骤

- 1 打开新的浏览器选项卡，然后输入用于获取连接服务器 SAML 元数据的 URL。

```
https://connection-server.example.com/SAML/metadata/sp.xml
```

在此示例中，*connection-server.example.com* 是连接服务器主机的完全限定域名。

该页面显示连接服务器中的 SAML 元数据。

- 2 使用另存为命令将网页保存为 XML 文件。

例如，您可以将该页面保存到名为 **connection-server-metadata.xml** 的文件中。该文件的内容以下面的文本开头：

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

后续步骤

在身份提供程序上使用相应的过程复制连接服务器 SAML 元数据。请参阅 Unified Access Gateway 或者第三方负载平衡器或网关的相关文档。

多个动态 SAML 身份验证器的响应时间注意事项

如果在连接服务器实例上将 SAML 2.0 身份验证配置为可选或必需的身份验证，并将多个动态 SAML 身份验证器与连接服务器实例相关联，则当任何动态 SAML 身份验证器变得无法访问时，从其他动态 SAML 身份验证器中启动远程桌面的响应时间将会增加。

您可以使用 Horizon Administrator 禁用无法访问的动态 SAML 身份验证器，以缩短在其他动态 SAML 身份验证器上启动远程桌面的响应时间。有关禁用 SAML 身份验证器的信息，请参阅在 [Horizon Administrator 中配置 SAML 身份验证器](#)。

在 Horizon Administrator 中配置 Workspace ONE 访问策略

Workspace ONE 或 VMware Identity Manager (vIDM) 管理员可以在 Horizon 7 中配置访问策略，以限制对授权桌面和应用程序的访问。要强制实施在 vIDM 中创建的策略，您需将 Horizon Client 置于 Workspace ONE 模式，以便 Horizon Client 可以将用户推送到 Workspace ONE 客户端来启动授权。当您登录到 Horizon Client 时，访问策略会引导您通过 Workspace ONE 登录以访问已发布的桌面和应用程序。

前提条件

- 在 Workspace ONE 中配置应用程序的访问策略。有关设置访问策略的更多信息，请参阅《VMware Identity Manager 管理指南》。
- 在 Horizon Administrator 中授权用户使用已发布的桌面和应用程序。

步骤

- 1 在 Horizon Administrator 中，选择**配置 > 服务器**。
- 2 在**连接服务器**选项卡上，选择一个与 SAML 身份验证器关联的服务器实例，然后单击**编辑**。
- 3 在**身份验证**选项卡上，将**将身份验证委派给 VMware Horizon (SAML 2.0 身份验证器)**选项设置为**需要**。
“需要”选项将启用 SAML 身份验证。最终用户只能使用由 vIDM 或第三方身份提供程序提供的 SAML 令牌连接到 Horizon Server。无法从 Horizon Client 中手动启动桌面或应用程序。
- 4 选择**启用 Workspace ONE 模式**。
- 5 在 **Workspace ONE 服务器主机名**文本框中，输入 Workspace ONE 主机名 FQDN 值。
- 6 （可选）选择**阻止不支持 Workspace ONE 模式的客户端连接**以仅限支持 Workspace ONE 模式的 Horizon Client 访问应用程序。

版本低于 4.5 的 Horizon Client 不支持 Workspace ONE 模式功能。如果选择此选项，版本低于 4.5 的 Horizon Client 将无法访问 Workspace ONE 中的应用程序。如果 Workspace ONE 版本低于 2.9.1，则不会为高于 Horizon 7 版本 7.2 的版本启用 Workspace ONE 模式功能。

配置生物身份验证

您可以编辑 LDAP 数据库中的 `pae-ClientConfig` 属性以配置生物身份验证。

前提条件

有关如何在 Windows 服务器上使用“ADSI 编辑”实用程序的信息，请参阅 Microsoft TechNet 网站。

步骤

- 1 在连接服务器主机上启动“ADSI 编辑”实用程序。
- 2 在“连接设置”对话框中，选择或连接到 **DC=vdi,DC=vmware,DC=int**。
- 3 在“计算机”窗格中，选择或键入 **localhost:389** 或者连接服务器主机的完全限定域名 (Fully Qualified Domain Name, FQDN) 后跟端口 389。

例如：**localhost:389** 或 **mycomputer.mydomain.com:389**

- 4 在 **CN=Common, OU=Global, OU=Properties** 对象上，编辑 **pae-ClientConfig** 属性并添加 **BioMetricsTimeout=<integer>** 值。

以下 BioMetricsTimeout 值有效：

BioMetricsTimeout 值	说明
0	不支持生物身份验证。这是默认值。
-1	支持生物身份验证，并且没有任何时间限制。
任意正整数	支持生物身份验证，并且可以在指定的分钟数内使用。

新设置将立即生效。您无需重新启动连接服务器服务或客户端设备。

在不需要凭据的情况下对用户进行身份验证

在用户登录到客户端设备或 VMware Identity Manager 之后，他们可以在不被提示输入 Active Directory 凭据的情况下连接到已发布的应用程序或桌面。

管理员可以选择根据用户需求来设置配置。

- 为用户提供已发布的应用程序的未验证访问权限。管理员可以配置该设置，以使用户无需使用 Active Directory (AD) 凭据即可登录到 Horizon Client。
- 对于基于 Windows 的客户端，使用“以当前用户身份登录”。对于基于 Windows 的客户端，管理员可以配置相关设置，以使用户在使用 AD 凭据登录到基于 Windows 的客户端之后，无需提供其他凭据即可登录到 Horizon Server。
- 在移动和 Mac 客户端中保存凭据。对于移动和 Mac 客户端，管理员可以配置 Horizon Server 以保存凭据。通过使用该功能，在为移动或 Mac 客户端提供一次 AD 凭据后，用户无需记住这些凭据即可进行 SSO（单点登录）。
- 为 VMware Identity Manager 配置 True SSO。对于 VMware Identity Manager，管理员可以配置 True SSO，以便使用 AD 凭据以外的某种方法进行身份验证的用户也可以在不被提示输入 AD 凭据的情况下登录到发布的桌面或应用程序。

本章讨论了以下主题：

- [为已发布的应用程序提供未验证访问](#)
- [为用户配置混合登录](#)
- [使用基于 Windows 的 Horizon Client 所提供的“以当前用户身份登录”功能](#)
- [在移动和 Mac Horizon Client 中保存凭据](#)
- [设置 True SSO](#)

为已发布的应用程序提供未验证访问

管理员可以为未验证用户设置配置，以便这些用户无需 AD 凭据即可从 Horizon Client 访问其已发布的应用程序。如果您的用户需要访问具有安全和用户管理要求的无缝应用程序，可考虑设置未验证访问。

当用户启动配置为未验证访问的已发布的应用程序，RDS 主机会根据需要创建本地用户会话，并向用户分配会话。

该功能需要使用 Horizon Client 版本 4.4 或更高版本。对于 HTML Access 客户端，该功能则需要使用版本 4.5 或更高版本。

配置未验证用户的工作流

- 1 创建未验证访问用户。请参阅[创建未验证访问用户](#)。
- 2 对用户启用未验证访问和设置默认未验证用户。请参阅[启用用户未验证访问](#)。
- 3 授权未验证用户访问已发布的应用程序。请参阅[授权未验证访问用户访问已发布的应用程序](#)。
- 4 在 Horizon Client 中启用未验证访问。请参阅[从 Horizon Client 未验证访问](#)。

配置未验证用户的规则和指南

- 未验证访问不支持双因素身份验证（例如 RSA 和 RADIUS）和智能卡身份验证。
- 智能卡身份验证和未验证访问相互排斥。当连接服务器中的智能卡身份验证设置为**必需**时，将禁用未验证访问，即使之前已启用该功能也是如此。
- VMware Identity Manager 和 VMware App Volumes 不支持未验证访问。
- 该功能支持 PCoIP 和 VMware Blast 显示协议。
- 未验证访问功能不会验证 RDS 主机的许可证信息。管理员必须配置和使用设备许可证。
- 未验证访问功能不会保存任何用户特定数据。用户可以验证应用程序的数据存储要求。
- 您无法重新连接到未验证的应用程序会话。当用户与客户端断开连接时，RDS 主机自动注销本地用户会话。
- 仅已发布的应用程序支持未验证访问。
- 安全服务器或 Unified Access Gateway 设备不支持未验证访问。
- 不会保存未验证用户的用户首选项。
- 虚拟桌面不支持未验证用户。
- 如果连接服务器配置有 CA 签名的证书，并启用未验证访问，但默认未验证用户未配置，则 Horizon Administrator 会显示红色的连接服务器状态。
- 如果 RDS 主机上安装的 Horizon Agent 的 AllowSingleSignon 组策略设置被禁用，未验证访问功能将不可用。管理员也可以使用 Horizon Agent 的 UnAuthenticatedAccessEnabled 组策略设置控制是禁用还是启用未验证访问。Horizon Agent 组策略设置包含在 vdm_agent.admx 模板文件中。您必须重新引导 RDS 主机，才能使该策略生效。

创建未验证访问用户

管理员可以为已发布的应用程序创建未验证访问用户。管理员配置未验证访问用户后，用户仅可以使用未验证访问从 Horizon Client 登录连接服务器实例。

前提条件

- 验证您要为其配置未验证访问的 **Active Directory (AD)** 用户是否具有有效的 **UPN**。仅可以将一个 **AD** 用户配置为未验证访问用户。

注 管理员仅可以为每个 **AD** 帐户创建一个用户。管理员无法创建未验证用户组。如果您创建一个未验证访问用户，而该 **AD** 用户已存在客户端会话，您必须重新启动客户端会话，以使更改生效。

步骤

- 1 在 **Horizon Administrator** 中，选择**用户和组**。
- 2 在**未验证访问**选项卡上，单击**添加**。
- 3 在**添加未验证用户**向导中，选择一个或多个搜索条件，然后单击**查找**，根据搜索条件查找用户。
用户必须具有有效的 **UPN**。
- 4 选择一个用户，然后单击**下一步**。
重复该步骤添加多个用户。
- 5 （可选）输入用户别名。
默认的用户别名是已为 **AD** 帐户配置的用户名。最终用户可以使用用户别名，从 **Horizon Client** 登录连接服务器实例。
- 6 （可选）检查用户详细信息并添加备注。
- 7 单击**完成**。

连接服务器创建未验证访问用户，显示用户详细信息，包括用户别名、用户名、名字和姓氏、源容器的数量、应用程序授权和会话。您可以单击“源容器”列中的数字，显示容器信息。

后续步骤

在连接服务器中为用户启用未验证访问。请参阅[启用用户未验证访问](#)。

启用用户未验证访问

创建未验证访问用户后，您必须在连接服务器中启用未验证访问，以便用户可以连接和访问已发布的应用程序。

步骤

- 1 在 **Horizon Administrator** 中，选择 **View 配置 > 服务器**。
- 2 单击**连接服务器**选项卡。
- 3 选择连接服务器实例，然后单击**编辑**。
- 4 单击**身份验证**选项卡。
- 5 将**未验证访问**更改为**已启用**。

6 从默认未验证访问用户下拉菜单中选择一个用户作为默认用户。

默认用户必须在 Cloud Pod 架构 环境中的本地容器中存在。如果选择的默认用户来自其他容器，连接服务器会在本地容器中创建该用户，然后将其设置为默认用户。

7 （可选）为该用户输入默认会话超时。

默认会话超时是处于空闲状态后 10 分钟。

8 单击**确定**。

后续步骤

授权未验证用户访问已发布的应用程序。请参阅[授权未验证访问用户访问已发布的应用程序](#)。

授权未验证访问用户访问已发布的应用程序

创建未验证访问用户后，您必须授权该用户访问已发布的应用程序。

前提条件

- 根据 RDS 主机组创建场。请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档中的“创建场”。
- 为在 RDS 主机场上运行的已发布的应用程序创建应用程序池。请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档中的“创建应用程序池”。

步骤

- 1 在 Horizon Administrator 中，选择**目录 > 应用程序池**，然后单击应用程序池的名称。
- 2 从**授权**下拉菜单中选择**添加授权**。
- 3 单击**添加**，选择一个或多个搜索条件，然后单击**查找**，选中**未验证用户**复选框，根据搜索条件查找未验证访问用户。
- 4 选择池中获得应用程序授权的用户，然后单击**确定**。
- 5 单击**确定**保存更改。

完成授权过程后，未验证访问用户旁边会出现一个未验证访问图标。

后续步骤

使用未验证访问用户身份登录 Horizon Client。请参阅[从 Horizon Client 未验证访问](#)。

搜索未验证访问会话

使用 Horizon Administrator 列出或搜索未验证访问用户已连接到的应用程序会话。未验证访问用户图标出现在未验证访问用户已连接到的会话的旁边。

步骤

- 1 在 Horizon Administrator 中，选择**监视 > 会话**。
- 2 单击**应用程序**，搜索应用程序会话。

3 选择搜索条件，然后开始搜索。

搜索结果包含用户、会话类型（桌面或应用程序）、计算机、池或场、DNS 名称、客户端 ID 和安全网关。会话开始时间、持续时间、状态和最近的会话也显示在搜索结果中。

删除未验证访问用户

在删除未验证访问用户时，您必须同时移除该用户的应用程序池授权。您不能删除作为默认用户的未验证访问用户。

注 如果您删除一个未验证访问用户，而该 AD 用户已存在客户端会话，则您必须重新启动客户端会话，以使更改生效。

步骤

- 1 在 Horizon Administrator 中，选择**用户和组**。
- 2 在**未验证访问**选项卡上，单击**删除**。
- 3 单击**确定**。

后续步骤

移除用户的应用程序授权。请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档中的“移除桌面或应用程序池授权”。

从 Horizon Client 未验证访问

以未验证访问用户身份登录 Horizon Client，启动已发布的应用程序。

为确保获得更高安全性，未验证访问用户具有您可用于登录 Horizon Client 的用户别名。如果您选择用户别名，则无需提供该用户的 AD 凭据或 UPN。登录 Horizon Client 后，您可以单击已发布的应用程序，启动该应用程序。有关安装和设置 Horizon Client 的更多信息，请参阅 [VMware Horizon Client 文档](#) 网页中的 Horizon Client 文档。

前提条件

- 确认为 Horizon 7 7.1 版连接服务器配置了未验证访问。
- 确认已在 Horizon Administrator 中创建了未验证访问用户。如果默认未验证用户是唯一未验证访问用户，则 Horizon Client 使用默认用户连接到连接服务器实例。

步骤

- 1 启动 Horizon Client。
- 2 在 Horizon Client 中，选择**以未验证访问匿名登录**。
- 3 连接到连接服务器实例。
- 4 从下拉菜单中选择一个用户别名，然后单击**登录**。

默认用户的后缀为“default”。

- 5 双击已发布的应用程序，以启动该应用程序。

配置登录减速以对已发布应用程序进行未验证访问

由于用户在使用未验证访问时不需要输入凭据，因此，对已发布应用程序的请求可能会让 RDS 主机因不堪重负而崩溃。设置登录减速可缓解此问题。您可以调整减速的级别。还可以阻止不支持减速的客户端。

前提条件

- 确认已为用户启用未验证访问。
- 确认您使用的是 Horizon Client 版本 4.9 或更高版本。如果您使用的是 Horizon Client 版本 4.8，则当用户通过对 Horizon 7 版本 7.6 进行未验证访问来以匿名方式登录时，有时可能会失败，从而可能需要重试多次才能登录。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。
- 2 单击**连接服务器**选项卡。
- 3 单击**身份验证**选项卡。
- 4 从**登录减速级别**下拉菜单中，选择未验证访问登录的减速级别。

选项	说明
低	为未验证访问登录设置低减速级别。对于 Microsoft Internet Explorer 和 Microsoft Edge 等 Web 浏览器，建议设置为低减速级别。
中	为未验证访问登录设置中等减速级别。此为默认设置。如果您使用的是 Horizon Client 版本 4.8，请勿更改此设置。
高	为未验证访问登录设置高减速级别。设置高减速级别可能会增加登录时间，从而影响最终用户体验。

- 5 （可选）要阻止不支持登录减速的任何客户端通过未验证访问连接到 Horizon 7，请选择**阻止不合规的客户端**。

版本低于 4.8 的 Horizon Client 属于不合规的客户端。

- 6 单击**确定**。

后续步骤

以未验证访问用户身份登录 Horizon Client，启动已发布的应用程序。请参阅[从 Horizon Client 未验证访问](#)。

为用户配置混合登录

创建未验证访问用户后，您可以为该用户启用混合登录。通过启用混合登录，未验证访问用户可通过域访问文件共享或网络打印机等网络资源，而无需输入凭据。

注 对于配置了混合登录的给定未验证访问用户，混合登录功能会对所有登录用户使用相同的域用户。

注 如果您从 RDS 主机中使用用户配置文件选项卡将主目录设置为网络路径，则默认情况下 Windows 上的管理用户界面会移除对主目录文件夹的所有现有权限，并为管理员和具有完全控制权的本地用户添加相应的权限。可使用管理员帐户从权限列表中移除本地用户，然后添加域用户，并使该用户拥有需要为其设置的相应权限。

前提条件

- 确认当您在 RDS 主机上安装 Horizon Agent 时选择了“混合登录”自定义选项。有关 RDS 主机的 Horizon Agent 自定义设置选项的更多信息，请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档。
- 确认已创建未验证访问用户。
- 确认未在域中为此用户帐户启用 Kerberos DES 加密。混合登录功能不支持 Kerberos DES 加密。

步骤

- 1 在 Horizon Administrator 中，选择**用户和组**。
- 2 在**未验证访问**选项卡上，单击**添加**。
- 3 在**添加未验证用户**向导中，选择一个或多个搜索条件，然后单击**查找**以根据搜索条件查找未验证访问用户。用户必须具有有效的 UPN。
- 4 选择一个未验证访问用户，然后单击**下一步**。
重复该步骤添加多个用户。
- 5 （可选）输入用户别名。
默认的用户别名是已为 AD 帐户配置的用户名。最终用户可以使用用户别名，从 Horizon Client 登录连接服务器实例。
- 6 （可选）检查用户详细信息并添加备注。
- 7 选择**启用混合登录**。
默认情况下将选择**启用 True SSO** 选项。您必须已经为 Horizon 7 环境启用了 True SSO。然后，启用了混合登录的未验证访问用户会使用 True SSO 从 Horizon Client 登录到连接服务器实例。

注 如果没有为连接服务器容器配置 True SSO，用户可以通过未验证访问启动授权的应用程序。但是，用户不具备网络访问权限，因为容器上未启用 True SSO。

- 8 （可选）要允许用户从 **Horizon Client** 登录到连接服务器实例，请选择**启用密码登录**，然后输入用户密码。

如果没有为 **Horizon 7** 环境配置 **True SSO**，可使用此设置。

在 **CPA** 环境中，混合登录用户功能只能在满足以下条件的连接服务器容器上使用：容器上的混合登录用户配置了**启用密码登录**设置并且有权访问已发布的应用程序。

例如，在一个包含容器 **A** 和容器 **B** 的 **CPA** 环境中，混合登录用户在容器 **A** 上配置了**启用密码登录**设置，并且有权访问容器上的应用程序。该用户可以从连接到容器 **A** 或容器 **B** 的客户端查看并启动该应用程序。但是，如果随后将容器 **B** 上的另一应用程序授权给同一用户，此用户将无法从连接到容器 **B** 的客户端查看和启动此应用程序。要使混合登录功能在容器 **B** 上能够正常使用，您必须创建另一个混合登录用户，为其配置**启用密码登录**设置，并将应用程序授权给该用户。有关如何设置 **CPA** 环境的详细信息，请参阅《在 **Horizon 7** 中管理 **Cloud Pod 架构**》文档。

- 9 单击**完成**。

后续步骤

授权用户访问已发布的应用程序。请参阅[授权未验证访问用户访问已发布的应用程序](#)。

使用基于 Windows 的 Horizon Client 所提供的“以当前用户身份登录”功能

在适用于 Windows 的 **Horizon Client** 中，当用户选择**以当前用户身份登录**复选框时，用户登录客户端系统时提供的凭据将被用于 **Horizon** 连接服务器实例和远程桌面的身份验证。无需进行其他用户身份验证。

为支持此功能，用户凭据将会存储在连接服务器实例和客户端系统中。

- 在连接服务器实例中，用户凭据经过加密并与用户名、域和可选 **UPN** 一同存储在用户会话中。这些凭据会在进行身份验证时添加，并在会话对象被破坏时清除。用户注销、会话超时或身份验证失败时，会话对象都会被破坏。会话对象位于易失性内存中，而不是存储在 **Horizon LDAP** 或磁盘文件中。
- 在客户端系统中，用户凭据经过加密存储在身份验证包（**Horizon Client** 的一个组件）内的一个表中。用户登录时这些凭据会被添加到表中，用户注销时则会从表中移除。该表位于易失性内存中。

管理员可以使用 **Horizon Client** 组策略设置控制**以当前用户身份登录**复选框的可用性，并指定其默认值。管理员还可以使用组策略指定当用户在 **Horizon Client** 中选中**以当前用户身份登录**复选框时，由哪个连接服务器实例接受所传送的用户身份和凭据信息。

用户使用“以当前用户身份登录”功能登录到连接服务器后，将启用递归解锁功能。在解锁客户端计算机后，递归解锁功能解锁所有远程会话。管理员可以在 **Horizon Client** 中使用**解锁客户端计算机后解锁远程会话**全局策略设置来控制递归解锁功能。有关 **Horizon Client** 的全局策略设置的更多信息，请参阅 [VMware Horizon Client 文档](#) 网页上的 **Horizon Client** 文档。

“以当前用户身份登录”功能存在以下限制和要求：

- 当在连接服务器实例中将智能卡身份验证设置为“需要”时，如果用户连接到连接服务器实例时选中**以当前用户身份登录**复选框，则用户的身份验证将失败。这些用户登录到连接服务器时必须用智能卡和 **PIN** 码重新进行身份验证。
- 客户端登录的系统上的时间必须与连接服务器主机上的时间同步。

- 如果在客户端系统上修改默认的[通过网络访问此计算机](#)用户权限分配，必须按照 VMware 知识库 (KB) 文章 1025691 中所述进行修改。
- 客户端计算机必须能够与公司的 Active Directory 服务器通信，并且不使用缓存的凭据进行身份验证。例如，如果用户从公司网络外部登录其客户端计算机，则会使用缓存的凭据进行身份验证。如果用户没有先建立 VPN 连接就尝试连接安全服务器或连接服务器实例，则系统将提示用户提供凭据，而“以当前用户身份登录”功能将不起作用。

在移动和 Mac Horizon Client 中保存凭据

管理员可以配置连接服务器，以使移动和 Mac Horizon Client 能够记住用户的用户名、密码和域信息。

对于适用于移动设备的 Horizon Client，该功能导致在登录对话框中显示**保存密码**复选框。对于适用于 Mac 的 Horizon Client，该功能导致在登录对话框中显示**记住此密码**复选框。

如果用户选择保存其凭据，后续进行连接时会将这些凭据添加到 Horizon Client 中的登录字段。

要启用该功能，必须设置 View LDAP 中的值，以指示在客户端中保存凭据信息的时长。对于适用于 Mac 的 Horizon Client，仅在 4.1 或更高版本中支持该功能。

注 在基于 Windows 的 Horizon Client 上，以当前用户身份登录的功能可避免多次要求用户提供凭据。

配置保存 Horizon Client 凭据的超时限制

您可以在 View LDAP 中设置一个值以配置超时限制，以便指定将 Horizon Client 凭据信息在移动设备和 Mac 客户端系统上保存多长时间。超时限制的单位为分钟。在连接服务器实例上更改 View LDAP 时，所做的更改会传播给所有连接服务器副本实例。

前提条件

请参阅 Microsoft TechNet 网站，了解如何在您的 Windows 操作系统版本上使用“ADSI 编辑”实用程序。

步骤

- 1 在您的连接服务器主机上启动“ADSI 编辑”实用程序。
- 2 在“连接设置”对话框中，选择或连接到 **DC=vdi,DC=vmware,DC=int**。
- 3 在“计算机”窗格中，选择或键入 **localhost:389** 或者连接服务器主机的完全限定域名 (Fully Qualified Domain Name, FQDN) 后跟端口 389。

例如：**localhost:389** 或 **mycomputer.mydomain.com:389**

- 4 在对象 **CN=Common, OU=Global, OU=Properties** 中，编辑 **clientCredentialCacheTimeout** 属性值。

如果未设置 **clientCredentialCacheTimeout** 或将其设置为 **0**，则会禁用该功能。要启用该功能，您可以设置保留凭据信息的分钟数，或设置 **-1** 值以表示无超时。

在连接服务器上，新的设置将立即生效。您无需重新启动连接服务器服务或客户端计算机。

设置 True SSO

通过 True SSO（单点登录）功能，在用户使用智能卡、RSA SecurID 或 RADIUS 身份验证登录到 VMware Identity Manager 后，用户无需再输入 Active Directory 凭据即可使用虚拟桌面或发布的桌面或应用程序。

如果用户使用 Active Directory 凭据进行身份验证，则不需要 True SSO 功能，但即使在这种情况下，也可以配置 True SSO 以供使用，从而忽略用户提供的 AD 凭据，转而使用 True SSO。

在连接到虚拟桌面或发布的应用程序时，用户可以选择使用本机 Horizon Client 或 HTML Access。

此功能存在以下限制：

- 此功能不适用于使用 View Agent Direct Connection 插件提供的虚拟桌面。
- 此功能仅在 IPv4 环境中受支持。

以下是为 True SSO 设置环境时必须执行的任务列表：

- 1 确定 True SSO 的架构
- 2 设置企业证书颁发机构
- 3 创建用于 True SSO 的证书模板
- 4 安装并设置注册服务器
- 5 导出注册服务客户端证书
- 6 配置 SAML 身份验证以使用 True SSO
- 7 配置 Horizon 连接服务器以使用 True SSO

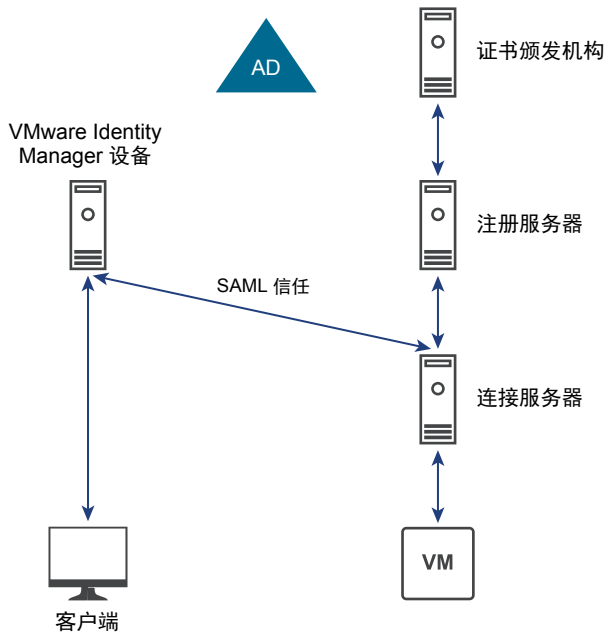
确定 True SSO 的架构

要使用 True SSO，您必须拥有或添加一个证书颁发机构，并创建一个注册服务器。这两个服务器可进行通信以创建短期 Horizon 虚拟证书，通过该证书可实现免密码的 Windows 登录。您可以在单个域中，具有多个域的单林中，以及多林多域设置中使用 True SSO。

VMware 建议部署两个 CA 和两个 ES 以使用 True SSO。以下示例说明了不同架构中的 True SSO。

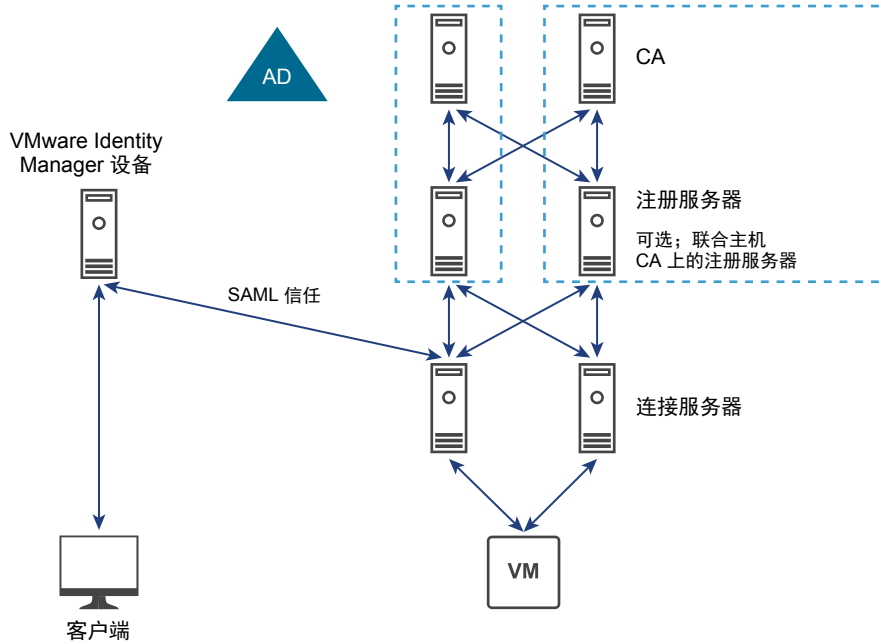
下图说明了简单的 True SSO 架构。

非常简单的 True SSO 架构



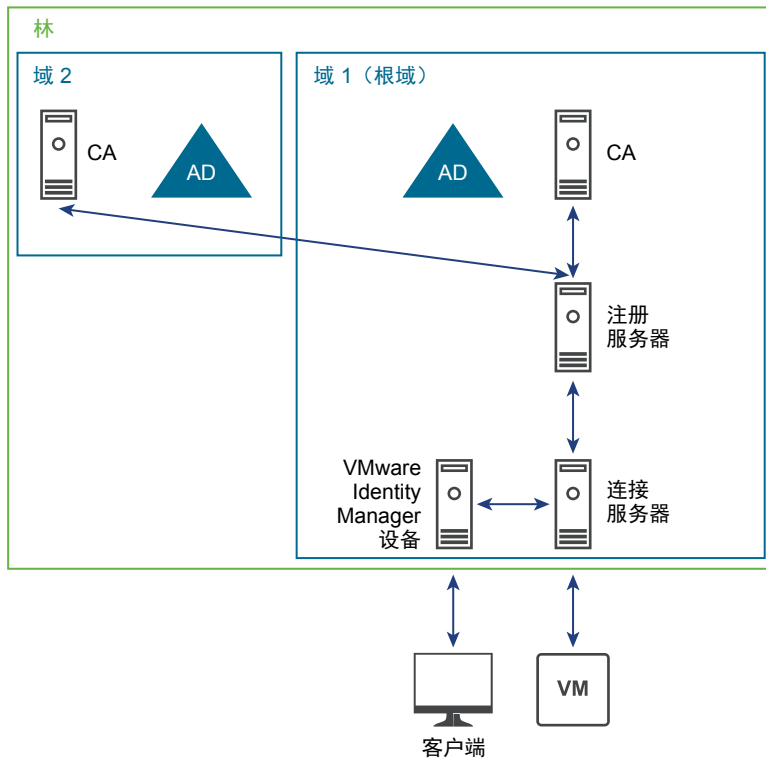
下图说明了单域架构中的 True SSO。

典型 HA True SSO 架构（单域）



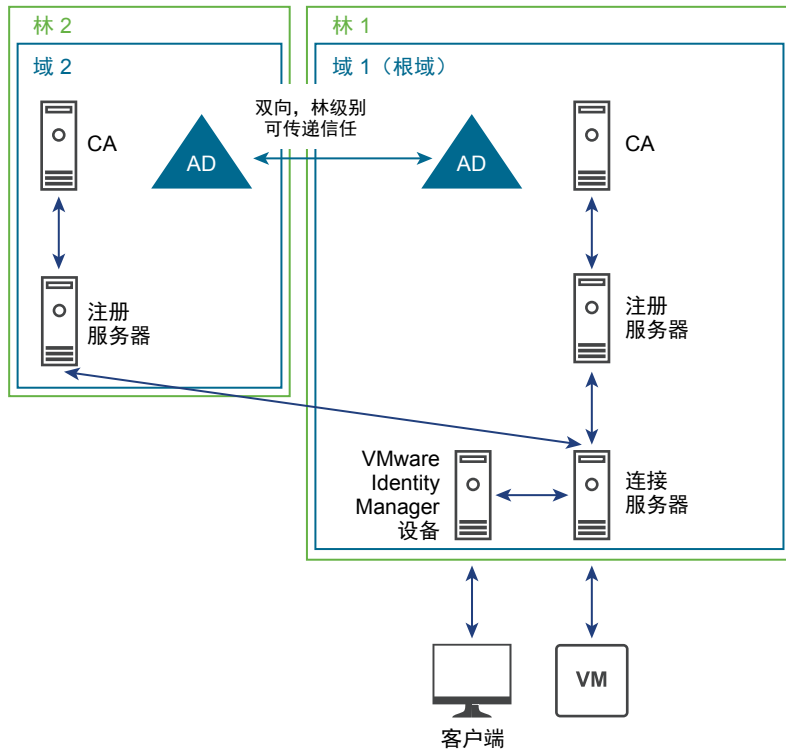
下图说明了具有多个域的单林架构中的 True SSO。

True SSO 单林多域架构（非 HA）



下图说明了多林架构中的 True SSO。

True SSO 多林架构（非 HA）



设置企业证书颁发机构

如果尚未设置证书颁发机构，则必须将 **Active Directory 证书服务 (Active Directory Certificate Service, AD CS)** 角色添加到 **Windows 服务器**，并将该服务器配置为企业 CA。

如果尚未设置企业 CA，请确认您使用的是此过程中所述的设置。

您必须至少拥有一个企业 CA，VMware 建议您拥有两个企业 CA 以用于故障切换和负载平衡。要为 **True SSO** 创建的注册服务器将与该企业 CA 进行通信。如果将注册服务器配置为使用多个企业 CA，则注册服务器将交替与可用的 CA 通信。如果将注册服务器安装在托管企业 CA 的同一台计算机上，则可以将注册服务器配置为首选使用本地 CA。建议使用此配置以获取最佳性能。

此过程包括启用非永久证书处理。默认情况下，证书处理包括在 CA 数据库中存储每个证书请求和已颁发证书的记录。持续大量的请求会提高 CA 数据库的增长率，如果不加以监视，可能会消耗所有可用的磁盘空间。启用非永久证书处理可以帮助降低 CA 数据库的增长率以及数据库管理任务的频率。

前提条件

- 创建 **Windows Server 2008 R2** 或 **Windows Server 2012 R2** 虚拟机。
- 确认虚拟机是 **Horizon 7** 部署的 **Active Directory** 域的一部分。
- 确认您使用的是 **IPv4** 环境。**IPv6** 环境当前不支持此功能。
- 确认系统具有静态 IP 地址。

步骤

- 1 以管理员身份登录到虚拟机操作系统，并启动服务器管理器。
- 2 选择用于添加角色的设置。

操作系统	选择项
Windows Server 2012 R2	a 选择 添加角色和功能 。 b 在“选择安装类型”页面上，选择 基于角色或基于功能的安装 。 c 在“选择目标服务器”页面上，选择一个服务器。
Windows Server 2008 R2	a 在导航树中选择 角色 。 b 单击 添加角色 启动 添加角色 向导。

- 3 在“选择服务器角色”页面上，选择 **Active Directory 证书服务**。
- 4 在“添加角色和功能”向导中，单击**添加功能**，并保留选中**包括管理工具**复选框。
- 5 在“选择功能”页面上，接受默认值。
- 6 在“选择角色服务”页面上，选择**证书颁发机构**。
- 7 按照提示完成安装。
- 8 安装完成后，在“安装进度”页面上，单击**在目标服务器上配置 Active Directory 证书服务**链接以打开“AD CS 配置”向导。

- 9 在“凭据”页面上，单击**下一步**，然后按照下表中所述的内容完成“AD CS 配置”向导页面。

选项	操作
角色服务	选择 证书颁发机构 ，然后单击 下一步 （而不是 配置 ）。
安装类型	选择 企业 CA 。
CA 类型	选择 根 CA 或 从属 CA 。某些企业首选双层 PKI 部署。有关更多信息，请访问 http://social.technet.microsoft.com/wiki/contents/articles/15037.ad-cs-step-by-step-guide-two-tier-pki-hierarchy-deployment.aspx 。
私钥	选择 创建新私钥 。
CA 的加密	对于哈希算法，可以选择 SHA1 、 SHA256 、 SHA384 或 SHA512 。对于密钥长度，可以选择 1024 、 2048 、 3072 或 4096 。 VMware 建议至少选择 SHA256 和 2048 密钥。
CA 名称	接受默认值或更改该名称。
有效期	接受默认值 5 年。
证书数据库	接受默认值。

- 10 在“确认”页面上，单击**配置**，当向导报告配置成功时，关闭该向导。

- 11 打开命令提示符，然后输入以下命令以针对非永久证书处理配置 CA：

```
certutil -setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
```

- 12 输入以下命令以忽略 CA 上的脱机 CRL（证书吊销列表）错误：

```
certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE
```

之所以需要此标记，是因为 True SSO 使用的根证书通常处于脱机状态，因此吊销检查将失败，这是预期的结果。

- 13 输入以下命令以重新启动该服务：

```
sc stop certsvc
sc start certsvc
```

后续步骤

创建证书模板。请参阅[创建用于 True SSO 的证书模板](#)。

创建用于 True SSO 的证书模板

您必须创建一个可用于颁发短期证书的证书模板，并指定域中的哪些计算机可请求获取此类型的证书。

您可以创建多个证书模板。针对每个域只能配置一个模板，但可以在多个域之间共享模板。例如，如果一个 Active Directory 林中包含三个域，您希望针对所有这三个域使用 True SSO，则可以选择配置一个、两个或三个模板。所有域可以共享同一个模板，您也可以针对每个域配置不同的模板。

前提条件

- 确认您拥有一个企业 CA，以用于创建此过程中所述的模板。请参阅[设置企业证书颁发机构](#)。

- 确认您准备了 **Active Directory** 以进行智能卡身份验证。有关更多信息，请参阅《**Horizon 7 安装指南**》文档。
- 在注册服务器的域和林中创建安全组，并将注册服务器的计算机帐户添加到该组。

步骤

- 1 要配置 **True SSO**，在用于证书颁发机构的计算机上，以管理员身份登录到操作系统，并转到**管理工具 > 证书颁发机构**。
 - a 展开左侧窗格中的树，右键单击**证书模板**，并选择**管理**。
 - b 右键单击**智能卡登录模板**，并选择**复制**。
 - c 在以下选项卡中进行如下更改：

选项卡	操作
“兼容性”选项卡	<ul style="list-style-type: none"> ■ 对于证书颁发机构，选择 Windows Server 2008 R2。 ■ 对于证书接收方，选择 Windows 7/Windows Server 2008 R2。
“常规”选项卡	<ul style="list-style-type: none"> ■ 将模板显示名称更改为 True SSO。 ■ 将有效期更改为一个典型工作日的时长；也就是用户可能在系统中保持登录的时间长度。 <p>这样，用户便不会在处于登录状态时失去对网络资源的访问；有限期必须长于用户域中的 Kerberos TGT 续订时间。</p> <p>（票证的默认最大生命周期为 10 小时。要查找默认的域策略，您可以转到计算机配置 > 策略 > Windows 设置 > 安全设置 > 帐户策略 > Kerberos 策略: 用户票证最长寿命。）</p> <ul style="list-style-type: none"> ■ 将续订期限更改为有效期的 50%-75%。
“请求处理”选项卡	<ul style="list-style-type: none"> ■ 对于用途，选择签名和智能卡登录。 ■ 选择对于智能卡的自动续订，...
“加密”选项卡	<ul style="list-style-type: none"> ■ 对于提供程序类别，选择密钥存储提供程序。 ■ 对于算法名称，选择 RSA。
“服务器”选项卡	<p>选择在 CA 数据库中不存储证书和请求。</p> <p>重要 确保取消选择在颁发的证书中不包含吊销信息。（在您选择第一个选项时，此框也会被随之选中，您必须取消选择（清除）它。）</p>
“发布要求”选项卡	<ul style="list-style-type: none"> ■ 选择授权签名的数量，并在该框中键入 1。 ■ 对于策略类型，选择应用程序策略，并将策略设置为证书申请代理。 ■ 对于要重新注册，要求下列项目，选择有效的现存证书。
“安全”选项卡	<p>对于为注册服务器计算机帐户创建的安全组（如“前提条件”中所述），提供以下权限：读取、注册。</p> <ol style="list-style-type: none"> 1 单击添加。 2 指定哪些计算机允许注册证书。 3 对于这些计算机，选中相应的复选框，以向计算机提供以下权限：读取、注册。

- d 在“新模板的属性”对话框中，单击**确定**。
- e 关闭“证书模板控制台”窗口。

- f 右键单击**证书模板**，并选择**新建 > 要颁发的证书模板**。

注 所有基于此模板颁发证书的证书颁发机构都需要执行此步骤。

- g 在“启用证书模板”窗口中，选择刚创建的模板（例如，**True SSO 模板**），并单击**确定**。
- 2** 要配置注册代理计算机，在用于证书颁发机构的计算机上，以管理员身份登录到操作系统，并转到**管理工具 > 证书颁发机构**。

- a 展开左侧窗格中的树，右键单击**证书模板**，并选择**管理**。

- b 找到并打开注册代理计算机模板，然后在**安全**选项卡中进行以下更改：

对于为注册服务器计算机帐户创建的安全组（如“前提条件”中所述），提供以下权限：读取、注册。

- 1 单击**添加**。
- 2 指定哪些计算机允许注册证书。
- 3 对于这些计算机，选中相应的复选框，以向计算机提供以下权限：读取、注册。

- c 右键单击**证书模板**，并选择**新建 > 要颁发的证书模板**。

注 所有基于此模板颁发证书的证书颁发机构都需要执行此步骤。

- d 在“启用证书模板”窗口中，选择**注册代理计算机**，并单击**确定**。

后续步骤

创建注册服务。请参阅[安装并设置注册服务器](#)。

安装并设置注册服务器

您可以运行连接服务器安装程序并选择 **Horizon 7 注册服务器** 选项来安装注册服务器。注册服务器将代表您指定的用户请求获取短期证书。这些短期证书即是 **True SSO** 用来进行身份验证的机制，这样可以避免提示用户提供 **Active Directory** 凭据。

您必须至少安装并设置一个注册服务器，并且注册服务器不能与 **View** 连接服务器安装在同一主机上。**VMware** 建议您拥有两个注册服务器，以用于故障切换和负载平衡。如果有两个注册服务器，则默认将首选其中一个注册服务器，而另一个则用于故障切换。但您可以更改此默认设置，以便连接服务器将证书请求交替发送到这两个注册服务器。

如果将注册服务器安装在托管企业 **CA** 的同一台计算机上，则可以将注册服务器配置为首选使用本地 **CA**。为了获取最佳性能，**VMware** 建议将首选使用本地 **CA** 的配置与平衡注册服务器负载的配置结合起来。因此，当收到证书请求时，连接服务器将使用备用注册服务器，并且每个注册服务器都将使用本地 **CA** 来为请求提供服务。有关要使用的配置设置的信息，请参阅[注册服务器配置设置](#)和[连接服务器配置设置](#)。

前提条件

- 创建至少具有 4 GB 内存的 Windows Server 2008 R2、Windows Server 2012 R2 或 Windows Server 2016 虚拟机，或者使用托管企业 **CA** 的虚拟机。请勿使用作为域控制器的计算机。
- 确认虚拟机上未安装其他 **View** 组件，包括 **View** 连接服务器、**View Composer**、安全服务器、**Horizon Client**、**View Agent** 或 **Horizon Agent**。

- 确认虚拟机是 Horizon 7 部署的 Active Directory 域的一部分。
- 确认您使用的是 IPv4 环境。IPv6 环境当前不支持此功能。
- VMware 建议系统必须具有静态 IP 地址。
- 确认您能够以具有管理员特权的域用户身份登录到操作系统。您必须以管理员身份登录才能运行此安装程序。

步骤

1 在要用于注册服务器的计算机上，将“证书”管理单元添加到 MMC：

- a 打开 MMC 控制台，然后选择**文件 > 添加/删除管理单元**。
- b 在**可用的管理单元**下，选择**证书**并单击**添加**。
- c 在“证书”管理单元窗口中，选择**计算机帐户**，单击**下一步**，然后单击**完成**。
- d 在“添加或删除管理单元”窗口中，单击**确定**。

2 颁发注册代理证书：

- a 在“证书”控制台中，展开控制台根树，右键单击**个人文件夹**，然后选择**所有任务 > 请求新证书**。
- b 在“证书注册”向导中，接受默认设置，直至到达“请求证书”页面。
- c 在“请求证书”页面上，选中**注册代理 (计算机)**复选框，然后单击**注册**。
- d 接受其他向导页面上的默认设置，然后单击最后一页上的**完成**。

如果在 MMC 控制台的左侧窗格中，展开**个人文件夹**并选择**证书**，您将会发现新证书就列在右侧窗格中。

3 安装注册服务器：

- a 从 VMware 下载页面下载 View 连接服务器安装程序文件，网址为 <https://my.vmware.com/web/vmware/downloads>。
在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 View 连接服务器。
安装程序文件名为 VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe，其中 xxxxxx 为内部版本号，y.y.y 为版本号。
- b 双击安装程序文件以启动向导，然后按照提示进行操作，直至到达“安装选项”页面。
- c 在“安装选项”页上，选择 **Horizon 7 注册服务器**，选择注册服务器实例的身份验证模式，然后单击**下一步**。

选项	说明
Horizon 7	为 Horizon 7 环境配置身份验证模式。
Horizon Cloud	为 Horizon Cloud 环境配置身份验证模式。

- d 按照提示完成安装。

您必须在端口 32111 (TCP) 上启用传入连接以使注册服务器正常工作。默认情况下，安装程序在安装期间打开该端口。

后续步骤

- 如果将注册服务器安装在托管企业 CA 的同一台计算机上，则将注册服务器配置为首选使用本地 CA。请参阅[注册服务器配置设置](#)。（可选）如果安装并设置多个注册服务器，则配置连接服务器，以便在注册服务器之间启用负载均衡。请参阅[连接服务器配置设置](#)。
- 将连接服务器与注册服务器配对。请参阅[导出注册服务客户端证书](#)。

导出注册服务客户端证书

要完成配对，您可以使用 MMC 证书管理单元，从群集中的某个连接服务器导出自动生成的自签名注册服务客户端证书。此证书之所以称为客户端证书，是因为连接服务器是注册服务器提供的注册服务的客户端。

在提示注册服务器为 Active Directory 用户颁发短期证书时，注册服务必须信任 VMware Horizon 连接服务器。因此，VMware Horizon 连接服务器群集或容器必须与注册服务器配对使用。

在安装 Horizon 7 或更高版本的连接服务器并启动 VMware Horizon 连接服务器服务后，将会自动创建注册服务客户端证书。该证书将通过 View LDAP 分发给以后添加到群集中的其他 Horizon 7 连接服务器。之后，该证书会被存储在计算机上 Windows 证书存储区的自定义容器 (VMware Horizon View Certificates\Certificates) 中。

前提条件

确认您装有 Horizon 7 或更高版本的连接服务器。有关安装说明，请参阅《Horizon 7 安装指南》。有关升级说明，请参阅《Horizon 7 升级指南》。

重要 客户可以使用自己的证书来配对，而不使用由连接服务器创建的自生成证书。要执行此操作，需将首选证书（以及关联的私钥）放置在连接服务器计算机上 Windows 证书存储区的自定义容器 (VMware Horizon View Certificates\Certificates) 中。然后，您必须将证书的友好名称设置为 **vdm.ec.new**，并重新启动服务器。群集中的其他服务器将从 LDAP 获取此证书。之后，您便可以执行以下过程中的步骤。

步骤

- 1 在群集中的某台连接服务器计算机上，将“证书”管理单元添加到 MMC：
 - a 打开 MMC 控制台，然后选择**文件 > 添加/删除管理单元**。
 - b 在**可用的管理单元**下，选择**证书**并单击**添加**。
 - c 在“证书”管理单元窗口中，选择**计算机帐户**，单击**下一步**，然后单击**完成**。
 - d 在“添加或删除管理单元”窗口中，单击**确定**。
- 2 在 MMC 控制台的左侧窗格中，展开 **VMware Horizon View 证书** 文件夹，然后选择**证书** 文件夹。
- 3 在右侧窗格中，右键单击友好名称为 **vdm.ec** 的证书文件，然后选择**所有任务 > 导出**。
- 4 在“证书导出”向导中，接受默认设置，包括保持选中**不，不要导出私钥**单选按钮。
- 5 当系统提示您命名文件时，键入注册服务客户端证书的文件名（如 **EnrollClient**），然后按照提示完成证书导出过程。

后续步骤

将证书导入到注册服务器。请参阅[在注册服务器上导入注册服务客户端证书](#)。

在注册服务器上导入注册服务客户端证书

要完成配对过程，您可以使用 MMC 证书管理单元将注册服务客户端证书导入到注册服务器中。您必须在每个注册服务器上执行此过程。

前提条件

- 确认您装有 Horizon 7 或更高版本的注册服务器。请参阅[安装并设置注册服务器](#)。
- 确认您拥有正确的证书可供导入。您可以使用自己的证书，也可以使用从群集中的某个连接服务器自动生成的自签名注册服务客户端证书，如[导出注册服务客户端证书](#)中所述。

重要 要使用您自己的证书进行配对，请将首选证书（以及关联的私钥）放置在连接服务器计算机上 Windows 证书存储区的自定义容器 (VMware Horizon View Certificates\Certificates) 中。然后，您必须将证书的友好名称设置为 **vdm.ec.new**，并重新启动服务器。群集中的其他服务器将从 LDAP 获取此证书。之后，您便可以执行以下过程中的步骤。

如果您拥有自己的客户端证书，则必须将用于生成客户端证书的根证书复制到注册服务器中。

步骤

- 1 将相应的证书文件复制到注册服务器计算机中。

要使用自动生成的证书，请从连接服务器中复制注册服务客户端证书。要使用自己的证书，请复制用来生成客户端证书的根证书。

- 2 在注册服务器上，将“证书”管理单元添加到 MMC：

- a 打开 MMC 控制台，然后选择**文件 > 添加/删除管理单元**。
- b 在**可用的管理单元**下，选择**证书**并单击**添加**。
- c 在“证书”管理单元窗口中，选择**计算机帐户**，单击**下一步**，然后单击**完成**。
- d 在“添加或删除管理单元”窗口中，单击**确定**。

- 3 在 MMC 控制台的左侧窗格中，右键单击 **VMware Horizon View 注册服务器可信根** 文件夹，然后选择**所有任务 > 导入**。

- 4 在“证书导入”向导中，按照提示浏览到 **EnrollClient** 证书文件，并将其打开。

- 5 按照提示操作，并接受默认设置以完成证书导入过程。

- 6 右键单击导入的证书，并添加友好名称，如 **vdm.ec**（适用于注册客户端证书）。

VMware 建议使用可识别 Horizon 7 群集的友好名称，但您可以使用有助于您轻松识别客户端证书的任何名称。

后续步骤

配置用于将身份验证委派给 VMware Identity Manager 的 SAML 身份验证器。请参阅[配置 SAML 身份验证以使用 True SSO](#)。

配置 SAML 身份验证以使用 True SSO

通过 Horizon 7 中引入的 True SSO 功能，用户可以使用智能卡、RADIUS 或 RSA SecurID 身份验证登录到 VMware Identity Manager 2.6 及更高版本，并且系统将不再提示他们输入 Active Directory 凭据，即使他们首次启动远程桌面或应用程序时也是如此。

在早期的版本中，用户首次启动远程桌面或已发布的应用程序时，如果他们之前没有通过其 Active Directory 凭据进行身份验证，则 SSO（单点登录）会提示用户输入其 Active Directory 凭据。随后凭据会被缓存，这样，后续的启动就不需要用户重新输入其凭据。通过 True SSO，系统会创建并使用短期证书，而不是 AD 凭据。

尽管为 VMware Identity Manager 配置 SAML 身份验证的过程并未更改，但为 True SSO 添加了一个额外步骤。您必须配置 VMware Identity Manager，以便禁止密码弹出窗口。

注 如果您的部署包括多个连接服务器实例，则必须将 SAML 身份验证器与每个实例都进行关联。

前提条件

- 确认已将单点登录作为全局设置启用。在 Horizon Administrator 中，选择**配置 > 全局设置**，并确认已将**单点登录 (SSO)** 设置为已启用。
- 确认已安装并配置了 VMware Identity Manager。请参阅 VMware Identity Manager 文档，网址为 <https://docs.vmware.com/cn/VMware-Identity-Manager/index.html>。
- 确认连接服务器主机上安装了 SAML 服务器证书的签名 CA 的根证书。VMware 建议不要配置 SAML 身份验证器使用自签名证书。请参阅《Horizon 7 安装指南》文档中“为 Horizon 7 Server 配置 SSL 证书”一章的“将根证书和中间证书导入 Windows 证书存储区”主题。
- 记下 VMware Identity Manager 服务器实例的 FQDN。

步骤

- 1 在 Horizon Administrator 中，选择**配置 > 服务器**。
- 2 在**连接服务器**选项卡上，选择一个要与 SAML 身份验证器关联的服务器实例，然后单击**编辑**。
- 3 在**身份验证**选项卡上的**将身份验证委派给 VMware Horizon (SAML 2.0 身份验证器)**下拉菜单中，选择**已允许或需要**。

您可以根据自己的需要，将部署中的每个连接服务器实例配置为使用不同的 SAML 身份验证设置。

- 4 单击**管理 SAML 身份验证器**，然后单击**添加**。

- 5 在“添加 SAML 2.0 身份验证器”对话框中配置 SAML 身份验证器。

选项	说明
标签	您可以使用 VMware Identity Manager 服务器实例的 FQDN。
说明	(可选) 您可以使用 VMware Identity Manager 服务器实例的 FQDN。
元数据 URL	此 URL 用于检索在 SAML 身份提供程序与 Horizon 连接服务器实例之间交换 SAML 信息所需的所有信息。在 URL <code>https://<Horizon Server 的名称>/SAAS/API/1.0/GET/metadata/idp.xml</code> 中, 单击 <Horizon Server 的名称> , 然后将其替换为 VMware Identity Manager 服务器实例的 FQDN。
管理 URL	此 URL 用于访问 SAML 身份提供程序 (VMware Identity Manager 实例) 的管理控制台。此 URL 的格式为 <code>https://<Identity-Manager-FQDN>:8443</code> 。

- 6 单击**确定**保存 SAML 身份验证器的配置。

如果您提供了有效信息, 必须接受自签名证书 (不建议) 或为 Horizon 7 和 VMware Identity Manager 使用可信证书。

SAML 2.0 身份验证器下拉菜单会显示新创建的身份验证器, 该身份验证器此时已被设为选中的身份验证器。

- 7 在 Horizon Administrator 仪表板上的“系统运行状况”部分, 选择**其他组件 > SAML 2.0 身份验证器**, 然后选择您之前添加的 SAML 身份验证器并验证详细信息。

如果配置成功, 身份验证器的运行状况将显示为绿色。如果证书不可信、VMware Identity Manager 服务不可用或者元数据 URL 无效, 身份验证器的运行状况可能会显示红色。如果证书不可信, 您或许可以单击**验证**来验证和接受该证书。

- 8 登录到 VMware Identity Manager 管理控制台, 转到“View 池”页面, 然后选中**禁止密码弹出窗口**复选框。

后续步骤

- 延长连接服务器元数据的过期时间, 以免远程会话在 24 小时后就终止。请参阅[在连接服务器上更改服务提供程序元数据的过期时间](#)。
- 使用 `vdmutil` 命令行界面配置连接服务器上的 True SSO。请参阅[配置 Horizon 连接服务器以使用 True SSO](#)。

有关 SAML 身份验证如何工作的详细信息, 请参阅[使用 SAML 身份验证](#)。

配置 Horizon 连接服务器以使用 True SSO

您可以使用 `vdmutil` 命令行界面进行配置, 以启用或禁用 True SSO。

只需在群集中的一个连接服务器上执行此过程。

重要 此过程仅使用启用 True SSO 时所必需的命令。有关可用于管理 True SSO 配置的所有配置选项列表以及每个选项的描述, 请参阅[用于配置 True SSO 的命令行参考](#)。

前提条件

- 确认您能够以具有管理员角色的用户身份运行命令。可以使用 **Horizon Administrator** 将管理员角色分配给用户。请参阅第 6 章，[配置基于角色的委托管理](#)。
- 确认您拥有以下服务器的完全限定域名 (Fully Qualified Domain Name, FQDN):
 - 连接服务器
 - 注册服务器

有关更多信息，请参阅[安装并设置注册服务器](#)。
 - 企业证书颁发机构

有关更多信息，请参阅[设置企业证书颁发机构](#)。
- 确认您拥有域的 **Netbios** 名称或 FQDN。
- 确认您已创建证书模板。请参阅[创建用于 True SSO 的证书模板](#)。
- 确认您已创建 **SAML** 身份验证器，以将身份验证委派给 VMware Identity Manager。请参阅[配置 SAML 身份验证以使用 True SSO](#)。

步骤

- 1 在群集中的某个连接服务器上，打开命令提示符，然后输入相应命令以添加注册服务器。

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truessso --environment --add --enrollmentServer enroll-server-fqdn
```

此时已将注册服务器添加到全局列表中。

- 2 输入相应命令，以列出该注册服务器的信息。

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truessso --environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn
```

输出会显示林名称，注册服务器的证书是否有效，您可使用的证书模板的名称和详细信息，以及证书颁发机构的公用名。要配置注册服务器可连接到哪些域，您可以在注册服务器上使用 **Windows** 注册表设置。默认为连接到所有信任域。

重要 您将需要在下一步中指定证书颁发机构的公用名。

- 3 输入相应命令以创建一个用于保存配置信息的 True SSO 连接器，并启用该连接器。

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --create --connector --domain domain-fqdn --template TrueSSO-template-name --
primaryEnrollmentServer enroll-server-fqdn --certificateServer ca-common-name --mode enabled
```

在此命令中，*TrueSSO-template-name* 是在上一步的输出中显示的模板名称，*ca-common-name* 是在该输出中显示的企业证书颁发机构的公用名。

将在指定的域的池或群集上启用 True SSO 连接器。要在池级别禁用 True SSO，请运行 `vdmUtil --certsso --edit --connector <domain> --mode disabled`。要为单个虚拟机禁用 True SSO，您可以使用 GPO (`vdm_agent.adm`)。

- 4 输入相应命令，以发现有哪些 SAML 身份验证器可用。

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --list --authenticator
```

身份验证器是在您使用 Horizon Administrator 配置 VMware Identity Manager 和连接服务器之间的 SAML 身份验证时创建的。

输出会显示身份验证器的名称以及是否已启用 True SSO。

重要 您将需要在下一步中指定身份验证器名称。

- 5 输入相应命令，以允许身份验证器使用 True SSO 模式。

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --
truesso --authenticator --edit --name authenticator-fqdn --truessoMode {ENABLED|ALWAYS}
```

对于 `--truessoMode`，如果您希望仅当用户不提供任何密码便登录到 VMware Identity Manager 时使用 True SSO，请使用 `ENABLED`。在这种情况下，如果使用并缓存了密码，则系统将使用该密码。如果您希望使用 True SSO，即使用户在登录到 VMware Identity Manager 时提供了密码的情况下也是如此，请将 `--truessoMode` 设置为 `ALWAYS`。

后续步骤

在 Horizon Administrator 中，确认 True SSO 配置的运行状况。有关更多信息，请参阅[使用系统运行状况控制板排除与 True SSO 相关的问题](#)。

要配置高级选项，请使用相应系统中的 Windows 高级设置。请参阅[True SSO 的高级配置设置](#)。

用于配置 True SSO 的命令行参考

您可以使用 `vdmutil` 命令行界面配置和管理 True SSO 功能。

该实用程序的位置

默认情况下，`vdmutil` 命令可执行文件的路径为 `C:\Program Files\VMware\VMware View\Server\tools\bin`。为避免在命令行中输入此路径，可以将此路径添加到 `PATH` 环境变量中。

语法和身份验证

在 Windows 命令提示符下，使用以下 `vdmutil` 命令格式。

```
vdmutil 身份验证选项 --truesso 其他选项和参数
```

您可以使用的附加选项取决于命令选项。本主题重点介绍用于配置 True SSO (`--truesso`) 的选项。以下是一个命令示例，该命令用于列出已针对 True SSO 进行配置的连接器：

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --list --connector
```

`vdmutil` 命令包括一些身份验证选项，用于指定进行身份验证时所使用的用户名、域和密码。

表 5-1. vdmutil 命令身份验证选项

选项	描述
<code>--authAs</code>	Horizon 7 管理员用户的名称。请勿使用域/用户名或用户主体名称 (UPN) 格式。
<code>--authDomain</code>	<code>--authAs</code> 选项中指定的 Horizon 7 管理员用户所在域的完全限定域名或 Netbios 名称。
<code>--authPassword</code>	<code>--authAs</code> 选项中指定的 Horizon 7 管理员用户的密码。在命令行中输入 "*" 来代替密码会导致 <code>vdmutil</code> 命令提示输入密码，并且不会在命令历史记录中保留敏感密码。

必须将身份验证选项与除了 `--help` `--verbose` 之外的所有 `vdmutil` 命令选项结合使用。

命令输出

操作成功时，`vdmutil` 命令将返回 0；操作失败时，将返回故障特定的非零代码。`vdmutil` 命令会将错误消息写入标准错误。当某个操作生成输出时，或通过使用 `--verbose` 选项启用了详细日志记录时，`vdmutil` 命令会使用美国英语将输出写入标准输出。

用于管理注册服务器的命令

您必须为每个域添加一个注册服务器。您还可以添加一个辅助注册服务器，并稍后指定该服务器用作备份。

下表中显示的选项并不表示您要输入的完整命令，其目的只是为了方便您查看。只有特定于特殊任务的选项才会包含在内。例如，有一行显示 `--environment --list --enrollmentServers` 选项，但您要实际输入的 `vdmUtil` 命令还包含用于身份验证的选项，以及用于指定您正在配置 True SSO 的选项：

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --truesso --environment --list --enrollmentServers
```

有关身份验证选项的详细信息，请参阅[用于配置 True SSO 的命令行参考](#)。

表 5-2. 用于管理注册服务器的 `vdmutil truesso` 命令选项

命令和选项	说明
<code>--environment --add --enrollmentServer enroll-server-fqdn</code>	将指定的注册服务器添加到环境中，其中 <i>enroll-server-fqdn</i> 是注册服务器的 FQDN。如果已经添加该注册服务器，则当您运行此命令时，不会发生任何操作。
<code>--environment --remove --enrollmentServer enroll-server-fqdn</code>	从环境中移除指定的注册服务器，其中 <i>enroll-server-fqdn</i> 是注册服务器的 FQDN。如果已经移除该注册服务器，则当您运行此命令时，不会发生任何操作。
<code>--environment --list --enrollmentServers</code>	列出环境中所有注册服务器的 FQDN。
<code>--environment --list --enrollmentServer enroll-server-fqdn</code>	<p>列出受注册服务器所属的域和林信任的域和林的 FQDN，以及注册证书的状态（可以为 VALID 或 INVALID）。VALID 表示注册服务器已安装注册代理证书。状态为 INVALID 可能是由于以下任意原因所致：</p> <ul style="list-style-type: none"> ■ 未安装证书。 ■ 证书尚未生效，或已过期。 ■ 证书不是由可信的企业 CA 颁发。 ■ 私钥不可用。 ■ 证书已损坏。 <p>注册服务器上的日志文件可提供状态为 INVALID 的原因。</p>
<code>--environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn</code>	对于指定域中的注册服务器，列出可用证书颁发机构的 CN（公用名），并提供有关每个可用于 True SSO 的证书模板的以下信息：名称、最小密钥长度和哈希算法。

用于管理连接器的命令

您可为每个域创建一个连接器。连接器可定义用于 True SSO 的参数。

下表中显示的选项并不表示您要输入的完整命令，其目的只是为了方便您查看。只有特定于特殊任务的选项才会包含在内。例如，有一行显示 `--list --connector` 选项，但您要实际输入的 `vdmUtil` 命令还包含用于身份验证的选项，以及用于指定您正在配置 True SSO 的选项：

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --truesso
--list --connector
```

有关身份验证选项的详细信息，请参阅[用于配置 True SSO 的命令行参考](#)。

表 5-3. 用于管理连接器的 vdmutil truesso 命令选项

选项	说明
<code>--create --connector --domain domain-fqdn</code> <code>--template template-name</code> <code>--primaryEnrollmentServer enroll-server1-fqdn</code> <code>[--secondaryEnrollmentServer enroll-server2-fqdn]</code> <code>--certificateServer CA-common-name</code> <code>--mode {enabled disabled}</code>	<p>为指定的域创建连接器，并配置该连接器以使用以下设置：</p> <ul style="list-style-type: none"> ■ template-name 是要使用的证书模板的名称。 ■ enroll-server1-fqdn 是要使用的主要注册服务器的 FQDN。 ■ enroll-server2-fqdn 是要使用的辅助注册服务器的 FQDN。此设置是可选的。 ■ CA-common-name 是要使用的证书颁发机构的公用名。这可以是一个以逗号分隔的 CA 列表。 <p>要确定哪些证书模板和证书颁发机构可用于特定的注册服务器，您可以运行 <code>vdmutil</code> 命令，并在命令中包含 <code>--truesso --environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn</code> 选项。</p>
<code>--list --connector</code>	列出已创建连接器的域的 FQDN。
<code>--list --connector --verbose</code>	<p>列出具有连接器的所有域，并且对于每个连接器，还提供以下信息：</p> <ul style="list-style-type: none"> ■ 主要注册服务器 ■ 辅助注册服务器（如果有） ■ 证书模板的名称 ■ 连接器处于启用状态还是禁用状态 ■ 证书颁发机构服务器（如果有多个服务器，则列出多个）的公用名
<code>--edit --connector domain-fqdn [--template template-name]</code> <code>[--mode {enabled disabled}]</code> <code>[--primaryEnrollmentServer enroll-server1-fqdn]</code> <code>[--secondaryEnrollmentServer enroll-server2-fqdn]</code> <code>[--certificateServer CA-common-name]</code>	<p>对于为 domain-fqdn 指定的域创建的连接器，允许您更改以下任何设置：</p> <ul style="list-style-type: none"> ■ template-name 是要使用的证书模板的名称。 ■ 其模式可以为 enabled 或 disabled。 ■ enroll-server1-fqdn 是要使用的主要注册服务器的 FQDN。 ■ enroll-server2-fqdn 是要使用的辅助注册服务器的 FQDN。此设置是可选的。 ■ CA-common-name 是要使用的证书颁发机构的公用名。这可以是一个以逗号分隔的 CA 列表。
<code>--delete --connector domain-fqdn</code>	删除已为 domain-fqdn 指定的域创建的连接器。

用于管理身份验证器的命令

身份验证器是在您配置 VMware Identity Manager Horizon 7 和连接服务器之间的 SAML 身份验证时创建的。唯一的管理任务是为身份验证器启用或禁用 True SSO。

下表中显示的选项并不表示您要输入的完整命令，其目的只是为了方便您查看。只有特定于特殊任务的选项才会包含在内。例如，有一行显示 `--list --authenticator` 选项，但您要实际输入的 `vdmUtil` 命令还包含用于身份验证的选项，以及用于指定您正在配置 True SSO 的选项：

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --truesso
--list --authenticator
```

有关身份验证选项的详细信息，请参阅[用于配置 True SSO 的命令行参考](#)。

表 5-4. 用于管理身份验证器的 vdmutil truesso 命令选项

命令和选项	说明
<code>--list --authenticator [--verbose]</code>	列出在域中找到的所有 SAML 身份验证器的完全限定域名 (Fully Qualified Domain Name, FQDN)。对于其中的每个身份验证器，指定是否已启用 True SSO。如果您使用 <code>--verbose</code> 选项，则还会列出关联的连接服务器的 FQDN。
<code>--list --authenticator --name label</code>	对于指定的身份验证器，列出是否已启用 True SSO，并且还列出关联的连接服务器的 FQDN。对于 <i>label</i> ，在您使用 <code>--authenticator</code> 选项而不使用 <code>--name</code> 选项时，使用所列出的名称之一。
<code>--edit --authenticator --name label</code> <code>--truessoMode mode-value</code>	对于指定的身份验证器，将 True SSO 模式设置为您指定的值，其中 <i>mode-value</i> 可以为下列值之一： <ul style="list-style-type: none"> ■ ENABLED。只有在用户的 Active Directory 凭据不可用时，才会使用 True SSO。 ■ ALWAYS。即使 vIDM 具有用户的 AD 凭据，也始终使用 True SSO。 ■ DISABLED。禁用 True SSO。 对于 <i>label</i> ，在您使用 <code>--authenticator</code> 选项而不使用 <code>--name</code> 选项时，使用所列出的名称之一。

True SSO 的高级配置设置

您可以使用 Horizon Agent 计算机上的 GPO 模板、注册服务器上的注册表设置以及连接服务器上的 LDAP 条目管理 True SSO 高级设置。这些设置包括默认超时，配置负载平衡，指定要包含的域，等等。

Horizon Agent 配置设置

您可以使用代理操作系统上的 GPO 模板在池级别关闭 True SSO，或更改证书设置（如密钥大小和计数）及重新连接尝试设置的默认值。

注 下表显示用于配置各个虚拟机上的代理的设置，但您也可以选择使用 Horizon Agent 配置模板文件。ADMX 模板文件名为 (vdm_agent.admx)。使用模板文件将这些策略设置应用于桌面或应用程序池中的所有虚拟机。如果设置了策略，则策略优先于注册表设置。

ADMX 文件包含在 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 中，您可以从 VMware 下载站点下载该文件，网址为 <https://my.vmware.com/web/vmware/downloads>。在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 ZIP 文件。

表 5-5. 用于在 Horizon Agent 上配置 True SSO 的项

项	最小值和最大值	说明
Disable True SSO	N/A	如果将此注册表项设置为 true ，则会在代理上禁用该功能。在组策略中使用此设置可在池级别禁用 True SSO。默认值为 false 。
Certificate wait timeout	10 - 120	指定证书到达代理的超时时限（以秒为单位）。默认值为 40 。
Minimum key size	1024 - 8192	允许的最小密钥大小。默认值为 1024 ，这表示在默认情况下，如果密钥大小低于 1024，则无法使用该密钥。

表 5-5. 用于在 Horizon Agent 上配置 True SSO 的项（续）

项	最小值和最大值	说明
All key sizes	N/A	可使用的密钥大小列表（以逗号分隔）。最多可以指定 5 个大小；例如： 1024,2048,3072,4096 。默认值为 2048 。
Number of keys to pre-create	1-100	要在提供远程桌面和托管 Windows 应用程序的 RDS 服务器上预先创建的密钥数。默认值为 5 。
Minimum validity period required for a certificate	N/A	证书被重复使用以重新连接用户时所需的最短有效期（以分钟为单位）。默认值为 5 。

注册服务器配置设置

您可以使用注册服务器操作系统上的 Windows 注册表设置来配置要连接到的域、各种超时时限、轮询周期、重试次数，以及是否首选使用同一本地服务器上安装的证书颁发机构（建议使用）。

要更改高级配置设置，您可以在注册服务器计算机上打开 Windows 注册表编辑器 (**regedit.exe**)，然后导航至以下注册表项：

```
HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Enrollment Service
```

表 5-6. 用于在注册服务器上配置 True SSO 的注册表项

注册表项	最小值和最大值	类型	说明
ConnectToDomains	N/A	REG_MULTI_SZ	注册服务器尝试自动连接的域列表。对于这种多字符串注册表类型，将列出每个域的 DNS 完全限定域名 (Fully Qualified Domain Name, FQDN)，其中每个 FQDN 占一行。 默认将信任所有域。
ExcludeDomains	N/A	REG_MULTI_SZ	注册服务器不自动连接的域列表。如果连接服务器提供了包含任何域的配置集，则注册服务器将尝试连接该域或这些域。对于这种多字符串注册表类型，将列出每个域的 DNS FQDN，其中每个 FQDN 占一行。 默认将不排除任何域。
ConnectToDomainsInForest	N/A	REG_SZ	指定是否连接并使用注册服务器所属林中的所有域。默认值为 TRUE 。 使用以下值之一： <ul style="list-style-type: none"> ■ 0 表示 false；即不连接所用林中的域。 ■ !=0 表示 true。
ConnectToTrustingDomains	N/A	REG_SZ	指定是否显式连接信任/入站域。默认值为 TRUE 。 使用以下值之一： <ul style="list-style-type: none"> ■ 0 表示 false；即不显式连接信任/入站域。 ■ !=0 表示 true。

表 5-6. 用于在注册服务器上配置 True SSO 的注册表项（续）

注册表项	最小值和最大值	类型	说明
PreferLocalCa	N/A	REG_SZ	指定是否首选本地安装的 CA（如果有）以提高性能。如果设置为 TRUE ，则注册服务器会将请求发送至本地 CA。如果连接本地 CA 失败，则注册服务器会尝试将证书请求发送至备用 CA。默认值为 FALSE 。 使用以下值之一： <ul style="list-style-type: none"> ■ 0 表示 false。 ■ !=0 表示 true。
MaxSubmitRetryTime	9500-59000	DWORD	在重新尝试提交证书签名请求之前等待的时间长度（以毫秒为单位）。默认值为 25000 。
SubmitLatencyWarningTime	500 - 5000	DWORD	接口被标记为“已降级”时的提交延迟警告时间（以毫秒为单位）。默认值为 1500 。 注册服务器使用此设置来确定是否应将 CA 视为处于已降级状态。如果完成最近三次证书请求所用的毫秒数多于此设置所指定的毫秒数，则 CA 即被视为已降级，并且此状态会显示在 Horizon Administrator 运行状况控制板上。 CA 通常会在 20 毫秒内颁发证书，但如果该 CA 空闲了几个小时，则任何首次请求都可能会花费较长时间才能完成。管理员可以使用此设置来了解某个 CA 是否缓慢，从而不必将该 CA 标记为缓慢。使用此设置可配置用于将该 CA 标记为缓慢的阈值。
WarnForLonglivedCert	N/A	REG_SZ	针对长久 True SSO 证书（模板）禁用警告。默认值是 True 。 如果证书的寿命设置为 14 天以上，注册服务器会在 Horizon Administrator 运行状况控制板中显示一个警告状态，同时报告 True SSO 模板处于已降级或者非最佳状态。注册服务器使用此设置禁用警告。 必须重新启动注册服务器才能使此设置生效。

连接服务器配置设置

您可以编辑连接服务器上的 **View LDAP**，以配置证书生成超时，以及是否在注册服务器之间启用负载均衡证书请求（建议启用）。

要更改高级配置设置，您必须在连接服务器主机上使用“**ADSI 编辑**”。您可以通过以下方法进行连接：键入标识名 **DC=vdi**，**DC=vmware**，**DC=int** 作为连接点，并键入计算机的服务器名称和端口 **localhost:389**。展开 **OU=Properties**，选择 **OU=Global**，然后在右侧窗格中双击 **CN=Common**。

之后，您可以编辑 **pae-NameValuePair** 属性，以添加下表中列出的一个或多个值。在添加值时，必须使用语法 **name=value**。

表 5-7. 连接服务器的高级 True SSO 设置

注册表项	说明
<code>cs-view-certsso-enable-es-loadbalance=[true false]</code>	指定是否在两个注册服务器之间启用负载均衡 CSR 请求。默认值为 false 。 例如，可添加 <code>cs-view-certsso-enable-es-loadbalance=true</code> 以启用负载均衡，这样当收到证书请求时，连接服务器将使用备用注册服务器。如果您的注册服务器和 CA 位于同一主机上，则每个注册服务器均可使用本地 CA 为请求提供服务。
<code>cs-view-certsso-certgen-timeout-sec=number</code>	在收到 CSR 后等待证书生成的时间长度（以秒为单位）。默认值为 35 。

识别没有 AD UPN 的 AD 用户

您可以为连接服务器配置 LDAP URL 筛选器以识别没有 AD UPN 的 AD 用户。

您必须在连接服务器主机上使用 ADAM ADSI 编辑。您可以通过键入标识名 **DC=vdi**，**DC=vmware**，**DC=int** 进行连接。展开 **OU=Properties**，并选择 **OU=Authenticator**。

然后，您可以编辑 **pae-LDAPURLList** 属性以添加 LDAP URL 筛选器。

例如，添加以下筛选器：

```
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=ldap:///???(telephoneNumber=$NAMEID)
```

连接服务器使用以下默认 LDAP URL 筛选器：

```
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=ldap:///???(
(&(objectCategory=user)(objectclass=user)(sAMAccountName=$NAMEID)) ldap:///???(
(&(objectCategory=group)(objectclass=group)(sAMAccountName=$NAMEID))
```

```
urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified=ldap:///???(
(&(objectCategory=user)(objectclass=user)(sAMAccountName=$NAMEID)) ldap:///???(
(&(objectCategory=group)(objectclass=group)(sAMAccountName=$NAMEID))
```

如果您配置了 LDAP URL 筛选器，则连接服务器便会使用此 LDAP URL 筛选器识别用户，而不会使用默认 LDAP URL 筛选器。

可用于对没有 AD UPN 的 AD 用户进行 SAML 身份验证的标识符示例：

- "cn"
- "mail"
- "description"
- "givenName"
- "sn"
- "canonicalName"
- "sAMAccountName"
- "member"

- "memberOf"
- "distinguishedName"
- "telephoneNumber"
- "primaryGroupID"

使用系统运行状况控制板排除与 True SSO 相关的问题

您可以使用 Horizon Administrator 中的系统运行状况仪表板快速查看可能影响 True SSO 功能运行的问题。

对于最终用户，如果 True SSO 停止工作，则当系统尝试将用户登录到远程桌面或应用程序时，用户会看到以下消息：“用户名或密码不正确 (The user name or password is incorrect)”。用户单击**确定**后，会进入登录屏幕。在 Windows 登录屏幕上，用户会看到一个标签为 **VMware SSO 用户** 的额外图块。如果用户拥有授权用户的 Active Directory 凭据，则可以使用 AD 凭据登录。

Horizon Administrator 显示屏幕左上方的系统运行状况仪表板包含几个与 True SSO 有关的项目。

注 True SSO 功能每分钟仅向控制板提供一次信息。单击右上角的刷新图标可立即刷新信息。

- 单击以展开 **View 组件 > True SSO** 可查看使用 True SSO 的域列表。

您可以单击域名来查看以下信息：为该域配置的注册服务器列表、企业证书颁发机构列表、所用证书模板的名称以及状态。如果存在问题，“状态”字段会对问题做出说明。

要更改“True SSO 域详细信息”对话框中显示的任何配置设置，请使用 vdmutil 命令行界面编辑 True SSO 连接器。有关更多信息，请参阅[用于管理连接器的命令](#)。

- 单击以展开**其他组件 > SAML 2.0 身份验证器**可查看为将身份验证委派给 VMware Identity Manager 实例而创建的 SAML 身份验证器列表。您可以单击身份验证器名称来查看其详细信息和状态。

注 为了使 True SSO 能够使用，必须为 SSO 启用全局设置。在 Horizon Administrator 中，选择**配置 > 全局设置**，并确认已将**单点登录 (SSO)** 设置为已启用。

表 5-8. 连接服务器到注册服务器的连接状态

状态文本	说明
未能获取 True SSO 运行状况信息。	仪表板无法从连接服务器实例中检索运行状况信息。
True SSO 配置服务无法访问 <FQDN> 注册服务器。	在容器中，将会选择其中一个连接服务器实例，用来将配置信息发送给该容器使用的所有注册服务器。此连接服务器实例将每分钟刷新一次注册服务器配置。如果配置任务无法更新注册服务器，便会显示此消息。有关其他信息，请参阅“注册服务器连接”表。
无法访问 <FQDN> 注册服务器以管理此连接服务器上的会话。	当前连接服务器实例无法连接到注册服务器。只有您的浏览器所指向的连接服务器实例才会显示此状态。如果容器中有多个连接服务器实例，您需要更改浏览器以使其指向其他连接服务器实例，这样才能查看这些实例的状态。有关其他信息，请参阅“注册服务器连接”表。

表 5-9. 注册服务器连接

状态文本	说明
<FQDN> 注册服务器上不存在此域 <Domain Name>。	True SSO 连接器已配置为对此域使用此注册服务器，但该注册服务器尚未配置为连接到此域。如果这种状态保持超过一分钟，则需要检查当前负责刷新注册配置的连接服务器状态。
仍在建立 <FQDN> 注册服务器与域 <Domain Name> 的连接。	注册服务器无法连接到此域中的域控制器。如果这种状态保持超过一分钟，则可能需要确认从注册服务器到域的名称解析正确无误，以及注册服务器和域之间存在网络连接。
<FQDN> 注册服务器与域 <Domain Name> 的连接正在停止或存在问题。	注册服务器已连接到域中的域控制器，但无法从该域控制器中读取 PKI 信息。如果发生这种情况，则说明实际域控制器可能存在问题。如果 DNS 的配置不正确，也可能发生此问题。请检查注册服务器上的日志文件，以查看注册服务器尝试使用的域控制器，然后确认该域控制器完全可操作。
<FQDN> 注册服务器尚未从域控制器中读取注册属性。	这是一种过渡状态，只有在注册服务器启动期间或在向环境中添加了新域时才会显示。这种状态的持续时间通常少于一分钟。如果这种状态的持续时间超过一分钟，则说明网速极慢，或者存在导致域控制器无法访问的问题。
<FQDN> 注册服务器已读取注册属性至少一次，但在一段时间内无法访问域控制器。	只要注册服务器从域控制器中读取 PKI 配置，它就会保持每两分钟轮询一次更改。如果域控制器 (Domain Controller, DC) 在短时间内无法访问，则将会设置这种状态。通常，这种无法访问 DC 的情况可能表示注册服务器检测不到 PKI 配置中的任何更改。只要证书服务器仍能够访问域控制器，便仍可以颁发证书。
<FQDN> 注册服务器已读取注册属性至少一次，但在较长时间内无法访问域控制器，或者存在其他问题。	如果注册服务器在较长时间内无法访问域控制器，则会显示这种状态。然后，注册服务器将尝试发现此域的备用域控制器。如果证书服务器仍能够访问域控制器，便仍可以颁发证书，但如果这种状态保持超过一分钟，则表示注册服务器已失去对该域的所有域控制器的访问权限，且可能再也无法颁发证书。

表 5-10. 注册证书状态

状态文本	说明
<FQDN> 注册服务器上没有为此域的 <domain name> 林安装有效的注册证书，或者证书可能已过期。	没有为此域安装注册证书，或者证书无效或已过期。注册证书必须由此域所属林信任的企业 CA 颁发。请确认您已完成《Horizon 7 管理指南》文档中的步骤，此文档介绍了如何在注册服务器上安装注册证书。您也可以依次打开 MMC 和证书管理单元，从而打开本地计算机存储区。然后，打开“个人”证书容器，并确认证书已经安装且有效。您还可以打开注册服务器日志文件。注册服务器会针对它所找到的任何证书，记录其他一些有关这些证书状态的信息。

表 5-11. 证书模板状态

状态文本	说明
<FQDN> 注册服务器域中不存在模板 <name>。	请检查指定的模板名称是否正确。
无法使用此模板生成的证书登录到 Windows。	此模板不支持使用智能卡，并且未启用数据签名。请检查指定的模板名称是否正确。此外，还请确认您已完成 创建用于 True SSO 的证书模板 中所述的步骤。
模板 <name> 启用了智能卡登录，但无法使用。	此模板启用了智能卡登录，但无法用于 True SSO。请检查指定的模板名称是否正确，并确认您已完成 创建用于 True SSO 的证书模板 中所述的步骤。您还可以查看注册服务器日志文件，因为它会记录模板中阻止将该模板用于 True SSO 的设置。

表 5-12. 证书服务器配置状态

状态文本	说明
域中不存在证书服务器 <CN of CA>。	请确认您为 CA 指定了正确的名称。必须指定公用名 (Common Name, CN)。
证书不在 NTAAuth (企业) 存储中。	此 CA 不是企业 CA，或者其 CA 证书尚未添加到 NTAUTH 存储。如果此 CA 不是林的成员，则必须手动将 CA 证书添加到此林的 NTAUTH 存储。

表 5-13. 证书服务器连接状态

状态文本	说明
<FQDN> 注册服务器未连接到证书服务器 <CN of CA>。	注册服务器未连接到证书服务器。如果注册服务器刚刚启动，或者如果 CA 最近才添加到 True SSO 连接器，则这可能是一种过渡状态。如果这种状态保持超过一分钟，则表示注册服务器无法连接到 CA。请验证名称解析正常工作，您具有到 CA 的网络连接，且注册服务器的系统帐户拥有访问 CA 的权限。
<FQDN> 注册服务器已连接到证书服务器 <CN of CA>，但该证书服务器处于降级状态。	如果 CA 颁发证书的速度缓慢，则会显示这种状态。如果 CA 一直保持这种状态，请检查 CA 的负载或 CA 使用的域控制器。 注 如果 CA 已标记为缓慢，则它会一直保持这种状态，直到至少成功完成了一个证书请求，并且在正常的时间范围内颁发了该证书。
<FQDN> 注册服务器可以连接到证书服务器 <CN of CA>，但该服务不可用。	如果注册服务器与 CA 之间存在有效的连接，但无法颁发证书，则会出现这种状态。这通常是一种过渡状态。如果 CA 没有快速变得可用，则此状态会更改为已断开。

配置基于角色的委托管理

Horizon 7 环境中的一项关键管理任务是确定哪些用户能够使用 **Horizon Administrator**，以及这些用户有执行哪些任务的权限。通过基于角色的委托管理，您可以将管理员角色分配给特定 **Active Directory** 用户和组，从而选择性地分配管理权限。

本章讨论了以下主题：

- [了解角色和特权](#)
- [使用访问组委派池和场的管理权](#)
- [了解权限](#)
- [对管理员进行管理](#)
- [管理和查看权限](#)
- [管理和查看访问组](#)
- [管理自定义角色](#)
- [预定义的角色和特权](#)
- [执行常见任务所需的特权](#)
- [针对管理员用户和组的最佳实践](#)

了解角色和特权

在 **Horizon Administrator** 中执行任务的能力由一个访问控制系统掌控，该系统由管理员角色和特权组成。该系统类似于 **vCenter Server** 访问控制系统。

管理员角色就是一组特权的集合。特权可授予执行特定操作的能力，例如授予用户对桌面池的权限。特权还控制管理员可在 **Horizon Administrator** 中查看的内容。例如，如果某个管理员不具有查看或修改全局策略的特权，那么该管理员登录到 **Horizon Administrator** 时将看不到导航面板中的**全局策略**设置。

管理员特权可以针对全局或特定对象。全局特权控制整个系统的操作，例如查看和更改全局设置。特定于对象的特权则控制对特定对象类型的操作。

管理员角色通常具有执行较高级别管理任务所需的各种特权。**Horizon Administrator** 中包含的预定义角色具有执行常规管理任务所需的特权。您可以将这些预定义角色分配给管理员用户和组，也可以通过组合特定特权来自行创建角色。您无法修改预定义角色。

要创建管理员，可以从 **Active Directory** 用户和组中选择用户和组并分配管理员角色。管理员通过其角色分配获取特权。您无法将特权直接分配给管理员。具有多个角色的管理员拥有这些角色中包含的所有特权。

使用访问组委派池和场的管理权

默认情况下，自动桌面池、手动桌面池和场在根访问组中创建，在 **Horizon Administrator** 中显示为 / 或 **Root(/)**。已发布的桌面池和应用程序池将继承其场的访问组。您可以在根访问组下创建访问组，然后将特定池或场的管理权委托给不同的管理员。

注 您无法直接更改已发布桌面池或应用程序池的访问组。您必须更改已发布桌面池或应用程序池所属的场的访问组。

虚拟机或物理机从其桌面池继承访问组。连接的永久磁盘从其计算机继承访问组。包括根访问组在内，最多可以有 **100** 个访问组。

通过在访问组上为管理员分配角色，就可以为管理员配置对该访问组中资源的访问权限。管理员只能访问为其分配了相应角色的访问组中的资源。管理员在访问组上的角色决定了其对该访问组中资源所具有的访问权限级别。

由于角色可从根访问组继承而来，因此在根访问组上具有某个角色的管理员在所有访问组上都具有该角色。在根访问组上具有管理员角色的管理员是超级管理员，因为他们对系统中的所有对象具有完全访问权限。

角色必须包含至少一个特定于对象的特权才能应用于访问组。只包含全局特权的角色不能应用于访问组。

您可以使用 **Horizon Administrator** 创建访问组，并将现有桌面池移到访问组中。创建自动桌面池、手动池或场时，您可以接受默认根访问组，也可以选择其他访问组。

注 如果您想要通过 **VMware Identity Manager** 提供对桌面和应用程序的访问，请确认您在 **Horizon Administrator** 中以拥有根访问组的管理员角色的用户身份来创建桌面和应用程序池。如果您向用户提供根访问组以外的其他访问组的管理员角色，**VMware Identity Manager** 将不会识别您在 **Horizon 7** 中配置的 **SAML** 身份验证器，并且您也将无法在 **VMware Identity Manager** 中配置池。

- **为不同访问组配置不同管理员**

您可以创建不同的管理员来管理配置中的每个访问组。

- **为同一访问组配置不同管理员**

您可以创建不同的管理员来管理同一访问组。

为不同访问组配置不同管理员

您可以创建不同的管理员来管理配置中的每个访问组。

例如，如果您的企业桌面池位于一个访问组中，而软件开发人员的桌面池位于另一个访问组中，那么您可以创建不同的管理员来管理每个访问组中的资源。

表 6-1 显示了这种配置的示例。

表 6-1. 为不同访问组配置不同管理员

管理员	角色	访问组
view-domain.com\Admin1	清单管理员	/CorporateDesktops
view-domain.com\Admin2	清单管理员	/DeveloperDesktops

在此示例中，名为 **Admin1** 的管理员在名为 **CorporateDesktops** 的访问组中具有 **Inventory Administrators** 角色，名为 **Admin2** 的管理员在名为 **DeveloperDesktops** 的访问组上具有 **Inventory Administrators** 角色。

为同一访问组配置不同管理员

您可以创建不同的管理员来管理同一访问组。

例如，如果您的企业桌面池位于一个访问组中，您可以创建一名可以查看和修改这些池的管理员，另外再创建一名只能查看这些池的管理员。

表 6-2 显示了这种配置的示例。

表 6-2. 为同一访问组配置不同管理员

管理员	角色	访问组
view-domain.com\Admin1	清单管理员	/CorporateDesktops
view-domain.com\Admin2	清单管理员 (只读)	/CorporateDesktops

在此示例中，名为 **Admin1** 的管理员在名为 **CorporateDesktops** 的访问组上拥有“清单管理员”角色，名为 **Admin2** 的管理员在同一访问组上拥有“清单管理员 (只读)”角色。

了解权限

Horizon Administrator 提供角色、管理员用户或组以及访问组的组合作为权限。角色定义了可以执行的操作，用户或组指明了谁可以执行操作，访问组则包含操作的目标对象。

根据您的选择的是管理员用户或组、访问组还是角色，Horizon Administrator 中将显示不同的权限。

下表显示了当您选择管理员用户或组时，权限在 Horizon Administrator 中的显示方式。管理员用户名为 **Admin 1**，具有两个权限。

表 6-3. “管理员和组”选项卡上显示的 Admin 1 权限

角色	访问组
清单管理员	MarketingDesktops
管理员 (只读)	/

第一个权限表示 **Admin 1** 在名为 **MarketingDesktops** 的访问组上具有 **Inventory Administrators** 角色。第二个权限表示 **Admin 1** 在根访问组上具有管理员 (**Read only**) 角色。

下表显示了当您选择 **MarketingDesktops** 访问组时，Horizon Administrator 中如何显示同样的权限。

表 6-4. “文件夹”选项卡上显示的 MarketingDesktops 权限

Admin	角色	已继承
view-domain.com\Admin1	清单管理员	
view-domain.com\Admin1	管理员 (只读)	是

第一个权限与 表 6-3 中显示的第一个权限相同。第二个权限是从 表 6-3 中显示的第二个权限继承而来。因为访问组从根访问组继承权限，因此 Admin1 在 MarketingDesktops 访问组上具有管理员 (Read only) 角色。如果权限是继承而来，那么“是否为继承”列中就会显示“是”。

下表显示了当您选择 Inventory Administrators 角色时，表 6-3 中的第一个权限如何在 Horizon Administrator 中显示。

表 6-5. “角色”选项卡上显示的清单管理员权限

Administrator	访问组
view-domain.com\Admin1	/MarketingDesktops

对管理员进行管理

具有 Administrators 角色的用户可以使用 Horizon Administrator 来添加和移除管理员用户和组。

Administrators 角色是 Horizon Administrator 中权限最高的角色。最初，Horizon Administrators 帐户的成员会被授予 Administrators 角色。当您安装连接服务器时，可以指定 Administrators 帐户。管理员帐户可以是连接服务器计算机上的本地 Administrators 组 (BUILTIN\Administrators)，也可以是域用户或组帐户。

注 默认情况下，Domain Admins（域管理员）组是本地管理员组的成员。如果指定 Administrators 帐户作为本地管理员组，并且不想使域管理员拥有对清单对象和 Horizon 7 配置设置的完全访问权限，您必须从本地管理员组中删除 Domain Admins（域管理员）组。

■ 创建管理员

要创建管理员，您需要在 Horizon Administrator 中从 Active Directory 用户和组内选择一个用户或组，然后分配管理员角色。

■ 移除管理员

您可以移除管理员用户或组，但无法移除系统中的最后一个超级管理员。超级管理员是在根访问组上具有管理员角色的管理员。

创建管理员

要创建管理员，您需要在 Horizon Administrator 中从 Active Directory 用户和组内选择一个用户或组，然后分配管理员角色。

前提条件

- 熟悉预定义的管理员角色。请参阅[预定义的角色和特权](#)。
- 熟悉创建管理员用户和组的最佳实践。请参阅[针对管理员用户和组的最佳实践](#)。

- 如果要为管理员分配自定义角色，请创建自定义角色。请参阅[添加自定义角色](#)。
- 要创建可以管理特定桌面池的管理员，请创建一个访问组并将桌面池移到该访问组中。请参阅[管理和查看访问组](#)。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 管理员**。
- 2 在**管理员和组**选项卡中，单击**添加用户或用户组**。
- 3 单击**添加**，选择一个或多个搜索条件，然后单击**查找**，根据您的搜索条件来筛选 Active Directory 用户或用户组。
- 4 选择您希望将其设为管理员用户或组的 Active Directory 用户或用户组，然后依次单击**确定**和**下一步**。
您可以按 **Ctrl** 和 **Shift** 键来选择多个用户和组。
- 5 选择一个要分配给管理员用户或用户组的角色。

“应用于访问组”列指示了角色是否应用于访问组。只有包含特定于对象的特权的角色才可以应用于访问组。只包含全局特权的角色不能应用于访问组。

选项	操作
将您所选的角色应用于访问组	选择一个或多个访问组，然后单击 下一步 。
您希望将该角色应用于所有访问组	选择根访问组，然后单击 下一步 。

- 6 单击**完成**创建管理员用户或组。

新的管理员用户或组将显示在**管理员和组**选项卡上的左侧窗格中，您选择的角色和访问组显示在右侧窗格中。

移除管理员

您可以移除管理员用户或组，但无法移除系统中的最后一个超级管理员。超级管理员是在根访问组上具有管理员角色的管理员。

步骤

- 1 在 View Administrator 中，选择 **View 配置 > 管理员**。
- 2 在**管理员和组**选项卡上，选择所需的管理员或组，然后依次单击**移除用户或用户组**和**确定**。

管理员和组选项卡上将不再显示该管理员用户或组。

管理和查看权限

您可以使用 Horizon Administrator 来添加、删除和查看特定管理员用户和组、特定角色以及特定访问组的权限。

■ 添加权限

您可以添加包含特定管理员用户或组、特定角色或特定访问组的权限。

■ 删除权限

可以删除包含特定管理员用户或组、特定角色或特定访问组的权限。

■ 查看权限

您可以查看包含特定管理员或组、特定角色或特定访问组的权限。

添加权限

您可以添加包含特定管理员用户或组、特定角色或特定访问组的权限。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 管理员**。
- 2 创建权限。

选项	操作
创建包含特定管理员用户或组的权限	<ol style="list-style-type: none"> a 在管理员和组选项卡上，选择所需的用户或组，然后单击添加权限。 b 选择一个角色。 c 如果该角色不适用于访问组，单击完成。 d 如果该角色适用于访问组，单击下一步，选择一个或多个访问组，然后单击完成。角色必须包含至少一个特定于对象的特权才能应用于访问组。
创建包含特定角色的权限	<ol style="list-style-type: none"> a 在角色选项卡上，选择所需的角色，单击权限，然后单击添加权限。 b 单击添加，选择一个或多个搜索条件，然后单击查找来查找符合搜索条件的管理员用户或组。 c 选择要包含在权限中的管理员用户或组，然后单击确定。您可以按 Ctrl 和 Shift 键来选择多个用户和组。 d 如果该角色不适用于访问组，单击完成。 e 如果该角色适用于访问组，单击下一步，选择一个或多个访问组，然后单击完成。角色必须包含至少一个特定于对象的特权才能应用于访问组。
创建包含特定访问组的权限	<ol style="list-style-type: none"> a 在访问组选项卡上，选择访问组并单击添加权限。 b 单击添加，选择一个或多个搜索条件，然后单击查找来查找符合搜索条件的管理员用户或组。 c 选择要包含在权限中的管理员用户或组，然后单击确定。您可以按 Ctrl 和 Shift 键来选择多个用户和组。 d 单击下一步选择一个角色，然后单击完成。角色必须包含至少一个特定于对象的特权才能应用于访问组。

删除权限

可以删除包含特定管理员用户或组、特定角色或特定访问组的权限。

移除管理员用户或组的最后一个权限后，该管理员用户或组也随之被移除。由于至少有一个管理员必须在根访问组上具有管理员角色，因此您无法删除会导致管理员被删除的权限。您无法删除继承而来的权限。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 管理员**。

2 选择要删除的权限。

选项	操作
删除应用于特定管理员或组的权限	在 管理员和组 选项卡上选择管理员或组。
删除应用于特定角色的权限	在 角色 选项卡上选择角色。
删除应用到特定访问组的权限	在 访问组 选项卡上选择文件夹。

3 选择所需的权限，然后单击**删除权限**。

查看权限

您可以查看包含特定管理员或组、特定角色或特定访问组的权限。

步骤

- 1 选择 **View 配置 > 管理员**。
- 2 查看权限。

选项	操作
查看包含特定管理员或组的权限	在 管理员和组 选项卡上选择管理员或组。
查看包含特定角色的权限	在 角色 选项卡上选择角色，然后单击 权限 。
查看包含特定访问组的权限	在 访问组 选项卡上选择文件夹。

管理和查看访问组

您可以使用 Horizon Administrator 添加和删除访问组，以及查看特定访问组中的桌面池和计算机。

- **添加访问组**
您可以通过创建访问组，将特定计算机、桌面池或场的管理权委托给不同的管理员。默认情况下，桌面池、应用程序池和场驻留在根访问组中。
- **将桌面池或场移至不同的访问组**
创建访问组后，您可以将自动桌面池、手动池或场移至新的访问组。
- **移除访问组**
当访问组不包含任何对象时，您可以移除该访问组。但是，您无法移除根访问组。
- **查看访问组中的桌面池、应用程序池或场**
您可以查看 Horizon Administrator 中特殊访问组内的桌面池、应用程序池或者场。
- **查看访问组中的 vCenter 虚拟机**
您可以在 Horizon Administrator 中查看特定访问组中的 vCenter 虚拟机。vCenter 虚拟机从其池中继承访问组。

添加访问组

您可以通过创建访问组，将特定计算机、桌面池或场的管理权委托给不同的管理员。默认情况下，桌面池、应用程序池和场驻留在根访问组中。

包括根访问组在内，最多可以有 100 个访问组。

步骤

- 1 在 Horizon Administrator 中，导航到“添加访问组”对话框。

选项	操作
从目录	<ul style="list-style-type: none"> ■ 选择 目录 > 桌面池。 ■ 从顶部窗格的 访问组 下拉菜单中，选择 新建访问组。
从资源	<ul style="list-style-type: none"> ■ 选择 资源 > 场。 ■ 从顶部窗格的 访问组 下拉菜单中，选择 新建访问组。
从 View 配置	<ul style="list-style-type: none"> ■ 选择 View 配置 > 管理员。 ■ 从 访问组 选项卡中，选择 添加访问组。

- 2 为访问组键入名称和描述，然后单击 **确定**。

描述是可选项。

后续步骤

将一个或多个对象移至该访问组。

将桌面池或场移至不同的访问组

创建访问组后，您可以将自动桌面池、手动池或场移至新的访问组。

步骤

- 1 在 Horizon Administrator 中，选择 **目录 > 桌面池** 或 **资源 > 场**。
- 2 选择一个池或场。
- 3 从顶部窗格中的 **访问组** 下拉菜单中选择 **更改访问组**。
- 4 选择访问组并单击 **确定**。

Horizon Administrator 会将池移至选定的访问组。

移除访问组

当访问组不包含任何对象时，您可以移除该访问组。但是，您无法移除根访问组。

前提条件

如果访问组包含对象，请将这些对象移动到另一访问组或根访问组中。请参阅[将桌面池或场移至不同的访问组](#)。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 管理员**。
- 2 在 **访问组** 选项卡上，选择访问组并单击 **移除访问组**。
- 3 单击 **确定** 移除访问组。

查看访问组中的桌面池、应用程序池或场

您可以查看 Horizon Administrator 中特殊访问组内的桌面池、应用程序池或者场。

步骤

- 1 在 Horizon Administrator 中，导航到对象的主页。

对象	操作
桌面池	选择目录 > 桌面池。
应用程序池	选择目录 > 应用程序池。
场	选择资源 > 场。

默认情况下显示所有访问组中的对象。

- 2 从主窗口窗格的访问组下拉菜单中选择访问组。

将显示访问组中您所选择的对象。

查看访问组中的 vCenter 虚拟机

您可以在 Horizon Administrator 中查看特定访问组中的 vCenter 虚拟机。vCenter 虚拟机从其池中继承访问组。

步骤

- 1 在 Horizon Administrator 中，选择资源 > 计算机。

- 2 选择 **vCenter 虚拟机** 选项卡。

默认情况下，将显示所有访问组中的 vCenter 虚拟机。

- 3 从访问组下拉菜单中选择一个访问组。

将显示您选择的访问组中的 vCenter 虚拟机。

管理自定义角色

您可以使用 Horizon Administrator 来添加、修改和删除自定义角色。

■ 添加自定义角色

如果预定义的管理员角色不符合您的要求，您可以在 Horizon Administrator 中组合特定特权以自行创建角色。

■ 修改自定义角色中的特权

您可以修改自定义角色中的特权，**pactara**。但无法修改预定义的管理员角色。

■ 移除自定义角色

如果自定义角色不包含在权限中时，您可以移除该角色，但您无法移除预定义的管理员角色。

添加自定义角色

如果预定义的管理员角色不符合您的要求，您可以在 **Horizon Administrator** 中组合特定特权以自行创建角色。

前提条件

熟悉可用于创建自定义角色的管理员特权。请参阅[预定义的角色和特权](#)。

注 创建自定义管理员角色时，自定义管理员用户没有全局权限。只有预定义的管理员角色才具有全局权限，能够管理 **Cloud Pod 架构** 环境中的全局授权。

步骤

- 1 在 **Horizon Administrator** 中，选择 **View 配置 > 管理员**。
- 2 在**角色**选项卡上，单击**添加角色**。
- 3 为新角色输入名称和描述，选择一个或多个特权，然后单击**确定**。
新角色将显示在左侧窗格中。

修改自定义角色中的特权

您可以修改自定义角色中的特权，**pactara**。但无法修改预定义的管理员角色。

前提条件

熟悉可用于创建自定义角色的管理员特权。请参阅[预定义的角色和特权](#)。

步骤

- 1 在 **Horizon Administrator** 中，选择 **View 配置 > 管理员**。
- 2 在**角色**选项卡上，选择所需的角色。
- 3 单击**特权**以显示该角色中的特权，然后单击**编辑**。
- 4 选择或取消选择特权。
- 5 单击**确定**保存更改。

移除自定义角色

如果自定义角色不包含在权限中时，您可以移除该角色，但您无法移除预定义的管理员角色。

前提条件

如果角色包含在权限中，请删除该权限。请参阅[删除权限](#)。

步骤

- 1 在 **Horizon Administrator** 中，选择 **View 配置 > 管理员**。

- 2 在**角色**选项卡上，选择所需的角色，然后单击**移除角色**。

对于预定义角色或者包含在权限中的自定义角色，**移除角色**按钮不可用。

- 3 单击**确定**移除角色。

预定义的角色和特权

Horizon Administrator 中包含预定义的角色，您可以将这些角色分配给管理员用户和组。您也可以组合特定的特权，自行创建管理员角色。

- **预定义的管理员角色**

预定义的管理员角色具有执行常见管理任务所需的所有特权。您无法修改预定义角色。

- **全局特权**

全局特权控制整个系统的操作，例如查看和更改全局设置。只包含全局特权的角色不能应用于访问组。

- **特定于对象的特权**

针对特定对象的特权可控制在特定清单对象类型上的操作。包含特定于对象的特权的角色可以应用于访问组。

- **内部特权**

某些预定义的管理员角色包含内部特权。您在创建自定义角色时无法选择内部特权。

预定义的管理员角色

预定义的管理员角色具有执行常见管理任务所需的所有特权。您无法修改预定义角色。

注 通过为用户分配预定义角色或自定义角色组合，可授权用户执行那些单独具有某个预定义角色或自定义角色时无法完成的操作。

下表说明了预定义角色，并指出了角色是否可以应用于访问组。

表 6-6. Horizon Administrator 中的预定义角色

角色	用户能力	应用于访问组
管理员	<p>执行所有管理员操作，包括创建其他管理员用户和组。在 Cloud Pod 架构环境中，拥有此角色的管理员可以配置和管理容器联合，以及管理远程容器会话。</p> <p>在根访问组上拥有“管理员”角色的管理员是超级用户，因为他们对系统中的所有清单对象拥有完全访问权限。由于管理员角色包含所有特权，您应该将其分配给一组有限的用户。最初，将在根访问组上为连接服务器主机上的本地 Administrators 组成员授予此角色。</p> <p>重要 管理员必须在根访问组上拥有“管理员”角色才能执行以下任务：</p> <ul style="list-style-type: none"> ■ 添加和删除访问组。 ■ 在 Horizon Administrator 中管理 ThinApp 应用程序和配置设置。 ■ 使用 vdmadmin、vdmimport 和 lmvutil 命令。 	是
管理员 (只读)	<ul style="list-style-type: none"> ■ 查看但不能修改全局设置和清单对象。 ■ 查看但不能修改 ThinApp 应用程序和设置。 ■ 运行所有 PowerShell 命令和命令行实用程序（包括 vdmexport，但不包括 vdmadmin、vdmimport 和 lmvutil）。 <p>在 Cloud Pod 架构环境中，拥有此角色的管理员可以查看全局数据层中的清单对象和设置。</p> <p>当管理员在某个访问组上拥有此角色时，他们只能查看该访问组中的清单对象。</p>	是
代理注册管理员	注册未受管的计算机（如物理系统、独立的虚拟机和 RDS 主机）。	否
全局配置和策略管理员	查看和修改除管理员角色和权限以外的全局策略和配置设置，以及 ThinApp 应用程序和设置。	否
全局配置和策略管理员 (只读)	查看但不能修改除管理员角色和权限以外的全局策略和配置设置，以及 ThinApp 应用程序和设置。	否
技术支持管理员	<p>执行桌面和应用程序操作（如关闭、重置和重新启动），以及远程协助操作（如结束用户桌面或应用程序的进程）。管理员必须具有根访问组权限才能访问 Horizon Help Desk Tool。</p> <ul style="list-style-type: none"> ■ 对 Horizon Help Desk Tool 进行只读访问。 ■ 管理全局会话。 ■ 可以登录到 Horizon Administrator。 ■ 执行所有计算机命令和会话相关命令。 ■ 管理远程进程和应用程序。 ■ 对虚拟桌面或已发布的桌面进行远程协助。 	否
技术支持管理员 (只读)	<p>查看用户和会话信息，以及深入了解会话详细信息。管理员必须具有根访问组权限才能访问 Horizon Help Desk Tool。</p> <ul style="list-style-type: none"> ■ 对 Horizon Help Desk Tool 进行只读访问。 ■ 可以登录到 Horizon Administrator。 	否
清单管理员	<ul style="list-style-type: none"> ■ 执行所有与计算机、会话和池相关的操作。 ■ 管理永久磁盘。 ■ 对链接克隆桌面进行重新同步、刷新和重新平衡，以及更改默认池映像。 <p>当管理员在某个访问组上拥有此角色时，他们只能对该访问组中的清单对象执行这些操作。</p>	是

表 6-6. Horizon Administrator 中的预定义角色（续）

角色	用户能力	应用于访问组
清单管理员 (只读)	查看但不能修改清单对象。 当管理员在某个访问组上拥有此角色时，他们只能查看该访问组中的清单对象。	是
本地管理员	执行除创建其他管理员用户和组以外的所有本地管理员操作。在 Cloud Pod 架构环境中，拥有此角色的管理员不能对全局数据层执行操作或管理远程容器上的会话。 注 拥有“本地管理员”角色的管理员不能访问 Horizon Help Desk Tool 。非 CPA 环境中的管理员不具有“管理全局会话”特权，而这是在 Horizon Help Desk Tool 中执行任务所必需的。	是
本地管理员 (只读)	除了不能查看全局数据层中的清单对象和设置外，其他都与“管理员 (只读)”角色相同。拥有此角色的管理员只对本地容器具有只读权限。 注 拥有“本地管理员 (只读)”角色的管理员不能访问 Horizon Help Desk Tool 。非 CPA 环境中的管理员不具有“管理全局会话”特权，而这是在 Horizon Help Desk Tool 中执行任务所必需的。	是

全局特权

全局特权控制整个系统的操作，例如查看和更改全局设置。只包含全局特权的角色不能应用于访问组。

下表介绍了全局特权，并列出了包含各个特权的预定义角色。

表 6-7. 全局特权

特权	用户能力	预定义角色
控制台交互	登录到和使用 Horizon Administrator。	管理员 管理员 (只读) 清单管理员 清单管理员 (只读) 全局配置和策略管理员 全局配置和策略管理员 (只读) 技术支持管理员 技术支持管理员 (只读) 本地管理员 本地管理员 (只读)
直接交互	运行所有 PowerShell 命令和命令行实用程序（vdmadmin 和 vdmimport 除外）。 管理员必须在根访问组上具有管理员角色才能使用 vdmadmin、vdmimport 和 lmvutil 命令。	管理员 管理员 (只读)
管理全局配置和策略	查看和修改全局策略与配置设置（针对管理员角色和权限的设置除外）。	管理员 全局配置和策略管理员
管理全局会话	在 Cloud Pod 架构环境中管理全局会话。	管理员

表 6-7. 全局特权（续）

特权	用户能力	预定义角色
管理角色和权限	创建、修改和删除管理员角色和权限。	管理员
注册代理	在未受管的计算机（如物理系统、独立的虚拟机和 RDS 主机）上安装 Horizon Agent。 在 Horizon Agent 安装过程中，您必须提供管理员登录凭据，才能在连接服务器实例上注册未受管理的计算机。	管理员 代理注册管理员

特定于对象的特权

针对特定对象的特权可控制在特定清单对象类型上的操作。包含特定于对象的特权的角色可以应用于访问组。

下表介绍了特定于对象的特权。预定义角色 **Administrators** 和 **Inventory Administrators** 中包含所有这些特权。

表 6-8. 特定于对象的特权

特权	用户能力	对象
启用场和桌面池	启用和禁用桌面池。	桌面池、场
授权桌面和应用程序池	添加和移除用户授权。	桌面池、应用程序池
管理 Composer 桌面池映像	对链接克隆池进行重新同步、刷新和重新平衡，以及更改默认池映像。	桌面池
管理计算机	执行与计算机和会话相关的所有操作。	计算机
管理永久磁盘	执行所有 View Composer 永久磁盘操作，包括附加、分离和导入永久磁盘。	永久磁盘
管理场以及桌面和应用程序池	添加、修改和删除场。添加、修改、删除和授权桌面及应用程序池。添加和移除计算机。	桌面池、应用程序池、场
管理会话	断开连接并注销会话，然后向用户发送消息。	会话
管理重新引导操作	重置虚拟机或重新启动虚拟桌面。	计算机

内部特权

某些预定义的管理员角色包含内部特权。您在创建自定义角色时无法选择内部特权。

下表介绍了内部特权，并列出了包含各个特权的预定义角色。

表 6-9. 内部特权

特权	说明	预定义角色
完整 (只读)	授予对所有设置的只读访问权限。	管理员 (只读)
管理清单 (只读)	授予对清单对象的只读访问权限。	清单管理员 (只读)
管理全局配置和策略 (只读)	授予只读访问配置设置和全局策略的权限，管理员和角色除外。	全局配置和策略管理员 (只读)

执行常见任务所需的特权

许多常见管理任务需要使用一组相互配合的特权。某些操作除了需要访问所操作对象的权限外，还需要根访问组的权限。

管理池所需的特权

管理员必须拥有某些特权才能在 Horizon Administrator 中管理池。

下表列出了常见的池管理任务，并显示了执行每项任务所需的特权。

表 6-10. 池管理任务和特权

任务	所需特权
启用或禁用桌面池	启用场和桌面池
将用户授权给池或取消授权	授权桌面和应用程序池
添加池	管理场以及桌面和应用程序池
修改或删除池	管理场以及桌面和应用程序池
从池添加或移除桌面	管理场以及桌面和应用程序池
刷新、重构、重新平衡或更改默认的 View Composer 映像	管理 Composer 桌面池映像
更改访问组	同时对源和目标访问组拥有管理场以及桌面和应用程序池特权。

管理计算机所需的特权

管理员必须拥有某些特权才能在 Horizon Administrator 中管理计算机。

下表列出了常见的计算机管理任务，并显示了执行每项任务所需的特权。

表 6-11. 计算机管理任务和特权

任务	所需特权
移除虚拟机	管理计算机
重置虚拟机	管理重新引导操作
重新启动虚拟桌面	管理重新引导操作
分配或移除用户所有权	管理计算机
进入或退出维护模式	管理计算机
断开会话连接或注销会话	管理会话

管理永久磁盘所需的特权

管理员必须拥有某些特权才能在 Horizon Administrator 中管理永久磁盘。

下表列出了常见的永久磁盘管理任务，并显示了执行每项任务所需的特权。您可在 Horizon Administrator 的“永久磁盘”页面执行这些任务。

表 6-12. 永久磁盘管理任务和特权

任务	所需特权
分离磁盘	对磁盘拥有 管理永久磁盘 特权，对池拥有 管理场以及桌面和应用程序池 特权。
附加磁盘	对磁盘拥有 管理永久磁盘 特权，对计算机拥有 管理场以及桌面和应用程序池 特权。
编辑磁盘	对磁盘拥有 管理永久磁盘 特权，对选定的池拥有 管理场以及桌面和应用程序池 特权。
更改访问组	对源和目标访问组拥有 管理永久磁盘 特权。
重新创建桌面	对磁盘拥有 管理永久磁盘 特权，对最后一个池拥有 管理场以及桌面和应用程序池 特权。
从 vCenter 导入	对文件夹拥有 管理永久磁盘 特权，对池拥有 管理池 特权。
删除磁盘	对磁盘拥有 管理永久磁盘 特权。

管理用户和管理员所需的特权

管理员必须拥有某些特权才能在 Horizon Administrator 中管理用户和管理员。

下表列出了常见的用户和管理员管理任务，并显示了执行每项任务所需的特权。您可在 Horizon Administrator 的“用户和组”页面管理用户，在 Horizon Administrator 的“全局管理员视图”页面管理管理员。

表 6-13. 用户和管理员管理任务和特权

任务	所需特权
更新常规用户信息	管理全局配置和策略
向用户发送消息	计算机上的 管理远程会话 。
添加管理员用户或组	管理角色和权限
添加、修改或删除管理员权限	管理角色和权限
添加、修改或删除管理员角色	管理角色和权限

Horizon Help Desk Tool 任务所需的特权

Horizon Help Desk Tool 管理员必须拥有某些特权才能在 Horizon Administrator 中执行故障排除任务。

下表列出了 Horizon Help Desk Tool 管理员可以执行的常见任务，并显示了执行每项任务所需的特权。

表 6-14. Horizon Help Desk Tool 任务和特权

任务	所需特权
对 Horizon Help Desk Tool 进行只读访问。	管理技术支持门户 (只读)
管理全局会话。	管理全局会话
可以登录到 Horizon Administrator。	控制台交互
执行所有计算机命令和会话相关命令。	管理计算机
重置或重新启动计算机。	管理重新引导操作
断开会话连接和注销会话。	管理会话
管理远程进程和应用程序。	管理远程进程和应用程序

表 6-14. Horizon Help Desk Tool 任务和特权（续）

任务	所需特权
对虚拟桌面或已发布的桌面进行远程协助。	远程协助
全局会话的断开连接、注销、重置和重新启动操作。	管理技术支持门户 (只读) 以及管理全局会话
本地会话的重置和重新启动操作。	管理技术支持门户 (只读) 以及管理重新引导操作
远程协助操作。	管理技术支持门户 (只读) 以及远程协助
结束远程进程和应用程序。	管理技术支持门户 (只读) 以及管理远程进程和应用程序
在 Horizon Help Desk Tool 中执行所有任务。	管理技术支持门户 (只读)、管理全局会话、管理重新引导操作、远程协助以及管理远程进程和应用程序
远程协助操作，以及结束远程进程和应用程序。	管理技术支持门户 (只读)、远程协助以及管理远程进程和应用程序
本地会话的断开连接和注销操作。	管理技术支持门户 (只读) 以及管理会话

执行常规管理任务和命令所需的特权

管理员必须具有某些特权才能执行常规管理任务和运行命令行实用程序。

下表显示了执行常规管理任务和运行命令行实用程序所需的特权。

表 6-15. 执行常规管理任务和命令所需的特权

任务	所需特权
添加或删除访问组	必须在根访问组上具有管理员角色。
在 Horizon Administrator 中管理 ThinApp 应用程序和设置	必须在根访问组上具有管理员角色。
在未受管的计算机（如物理系统、独立虚拟机或 RDS 主机）上安装 Horizon Agent	注册代理
查看或修改 Horizon Administrator 中的配置设置（针对管理员的设置除外）	管理全局配置和策略
运行所有 PowerShell 命令和命令行实用程序（vdmadmin 和 vdmimport 除外）。	直接交互
使用 vdmadmin 和 vdmimport 命令	必须在根访问组上具有管理员角色。
使用 vdmexport 命令	必须在根访问组上具有管理员角色或管理员 (Read only) 角色。

针对管理员用户和组的最佳实践

要增加您的 Horizon 7 环境的安全性和可管理性，在管理管理员用户和组时应该遵循以下最佳实践。

- 在 Active Directory 中创建新用户组并向这些组分配管理角色。避免使用 Windows 内置组或其他可能包含不需要或不应该具有 Horizon 7 特权的用户的现有组。
- 使具有 Horizon 7 管理特权的用户数量最少。
- 由于管理员角色具有所有特权，因此该角色不应当用于日常管理。
- 由于名称 Administrator 太过明显而且很容易猜到，因此在创建管理员用户和组时要避免使用该名称。
- 创建访问组以隔离敏感的桌面和场。将这些访问组的管理权委托给一组有限的用户。

- 创建可以修改全局策略和 Horizon 7 配置设置的单独管理员。

在 Horizon Administrator 和 Active Directory 中配置策略

7

您可以使用 Horizon Administrator 设置客户端会话策略。您可以将 Active Directory 组策略设置配置为控制 View 连接服务器、PCoIP 显示协议以及 Horizon 7 日志记录和性能警报的行为。

您还可以将 Active Directory 组策略设置配置为控制 Horizon Agent、适用于 Windows 的 Horizon Client、Horizon Persona Management 以及某些功能的行为。有关这些策略设置的信息，请参阅《在 Horizon 7 中配置远程桌面功能》文档。

本章讨论了以下主题：

- 在 Horizon Administrator 中设置策略
- 使用 Horizon 7 组策略管理模板文件

在 Horizon Administrator 中设置策略

您可以使用 Horizon Administrator 配置客户端会话策略。

您可以将这些策略设置为影响特定用户、特定桌面池或所有客户端会话用户。影响特定用户和桌面池的策略称为用户级别策略和桌面池级别策略。影响所有会话和用户的策略称为全局策略。

用户级别策略将从等效的桌面池级别策略设置继承设置。同样，桌面池级别策略将从等效的全局策略设置继承设置。桌面池级别策略设置优先于等效的全局策略设置。用户级别策略设置优先于等效的全局和池级别策略设置。

低级别策略设置可能比等效的高级别设置或多或少地要严格。例如，您可以将某个全局策略设置为**拒绝**，并将等效的桌面池级别策略设置为**允许**，反之亦然。

注 仅全局策略适用于已发布的桌面和应用程序池。无法为已发布的桌面和应用程序池设置用户级别的策略或池级别的策略。

■ 配置全局策略设置

您可以配置全局策略以控制所有客户端会话用户的行为。

■ 配置桌面池策略

您可以配置桌面级策略以影响特定桌面池。桌面级策略设置优先于等效的全局策略设置。

■ 配置用户策略

您可以配置用户级别策略以影响特定用户。用户级别策略设置始终优先于等效的全局和桌面池级别策略设置。

■ Horizon 7 策略

您可以将 Horizon 7 策略配置为影响所有客户端会话，或者只影响特定桌面池或用户。

配置全局策略设置

您可以配置全局策略以控制所有客户端会话用户的行为。

前提条件

请熟悉策略描述。请参阅 [Horizon 7 策略](#)。

步骤

- 1 在 Horizon Administrator 中，选择**策略 > 全局策略**。
- 2 单击**查看策略**窗格中的 **View 策略**。
- 3 单击**确定**保存更改。

配置桌面池策略

您可以配置桌面级策略以影响特定桌面池。桌面级策略设置优先于等效的全局策略设置。

前提条件

请熟悉策略描述。请参阅 [Horizon 7 策略](#)。

步骤

- 1 在 Horizon Administrator 中，选择**目录 > 桌面池**。
- 2 双击所需桌面池的 ID，然后单击**策略**选项卡。

策略选项卡将显示当前的池策略设置。如果设置是从等效的全局策略继承而来，**桌面池策略**列中会显示**继承**。

- 3 单击**查看策略**窗格中的 **View 策略**。
- 4 单击**确定**保存更改。

配置用户策略

您可以配置用户级别策略以影响特定用户。用户级别策略设置始终优先于等效的全局和桌面池级别策略设置。

前提条件

请熟悉策略描述。请参阅 [Horizon 7 策略](#)。

步骤

- 1 在 Horizon Administrator 中，选择**目录 > 桌面池**。

- 2 双击所需桌面池的 ID，然后单击**策略**选项卡。

策略选项卡将显示当前的池策略设置。如果设置是从等效的全局策略继承而来，**桌面池策略**列中会显示**继承**。

- 3 单击**用户覆盖**，然后单击**添加用户**。
- 4 要查找用户，请单击**添加**，键入用户的名称和描述，然后单击**查找**。
- 5 从列表中选择一个或多个用户，单击**确定**，然后单击**下一步**。

屏幕上将显示“添加单个策略”对话框。

- 6 配置 Horizon 策略并单击**完成**保存更改。

Horizon 7 策略

您可以将 Horizon 7 策略配置为影响所有客户端会话，或者只影响特定桌面池或用户。

下表介绍了每项 Horizon 7 策略设置。

表 7-1. Horizon 策略

策略	说明
多媒体重定向 (MMR)	<p>确定是否为客户端系统启用 MMR。</p> <p>MMR 是一种 Windows Media Foundation 过滤器，可直接通过 TCP 套接字将多媒体数据从远程桌面中的特定编解码器转发至客户端系统。随后，直接在播放数据的客户端系统中解码数据。</p> <p>默认值为拒绝。</p> <p>如果客户端系统没有足够的资源来处理本地多媒体解码，请将设置保留为拒绝。</p> <p>多媒体重定向 (MMR) 数据在不采用应用程序加密的情况下跨网络传输，其中可能包含敏感数据，具体取决于被重定向的内容。为确保无法在网络上监视此数据，请仅在安全网络中使用 MMR。</p>
USB 访问	<p>确定远程桌面是否可以使用 USB 设备连接客户端系统。</p> <p>默认值为允许。如果出于安全因素阻止使用外部设备，请将设置更改为拒绝。</p>
PCoIP 硬件加速	<p>确定是否启用 PCoIP 显示协议的硬件加速，指定分配给 PCoIP 用户会话的加速优先级。</p> <p>仅在托管远程桌面的物理机中装有 PCoIP 硬件加速设备时，此设置才有效。</p> <p>默认值为允许，优先级为中。</p>

使用 Horizon 7 组策略管理模板文件

Horizon 7 提供了多个特定于组件的组策略管理 ADMX 模板文件。您可以将这些 ADMX 模板文件中的策略设置添加到 Active Directory 中的新 GPO 或现有 GPO，从而优化和保护远程桌面和应用程序。

为 Horizon 7 提供组策略设置的所有 ADMX 文件包含在 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 中，其中 x.x.x 是版本，yyyyyyy 是内部版本号。您可以从 VMware 下载站点中下载该文件，网址为 <https://my.vmware.com/web/vmware/downloads>。在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 ZIP 文件。

Horizon 7 ADMX 模板文件同时包含计算机配置组策略和用户配置组策略。

- 计算机配置策略将设置应用于所有远程桌面的策略（无论哪个用户连接到桌面）。

- 用户配置策略将设置应用于所有用户的策略（无论他们连接到哪个远程桌面或应用程序）。用户配置策略覆盖等效的计算机配置策略。

Microsoft Windows 在桌面启动时和用户登录时应用策略。

Horizon 7 ADMX 模板文件

Horizon 7 ADMX 模板文件提供了组策略设置，让您可以控制和优化 Horizon 7 组件。

ADMX 文件包含在 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 中，您可以从 VMware 下载站点下载该文件，网址为 <https://my.vmware.com/web/vmware/downloads>。在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 ZIP 文件。

表 7-2. Horizon ADMX 模板文件

模板名称	模板文件	说明
VMware View Agent 配置	vdm_agent.admx	包含与 Horizon Agent 的身份验证和环境组件相关的策略设置。 请参阅《在 Horizon 7 中配置远程桌面功能》文档。
VMware Horizon Client 配置	vdm_client.admx	包含与 Horizon Client for Windows 相关的策略设置。 从连接服务器主机域外部连接的客户端不受应用于 Horizon Client 的策略的影响。 请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。
VMware Horizon URL 重定向	urlRedirection.admx	包含与 URL 内容重定向功能相关的策略设置。如果您将此模板添加到远程桌面池或应用程序池的 GPO，则在远程桌面或应用程序内单击的某些 URL 链接会被重定向到基于 Windows 的客户端，并在客户端浏览器中将其打开。 如果您将此模板添加到客户端 GPO，则当用户在基于 Windows 的客户端系统中单击某些 URL 链接时，会在远程桌面或应用程序中打开该 URL。 请参阅《在 Horizon 7 中配置远程桌面功能》文档和《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。
VMware View Server 配置	vdm_server.admx	包含与连接服务器相关的策略设置。
VMware View 公共配置	vdm_common.admx	包含所有 Horizon 组件中的常见策略设置。
PCoIP 会话变量	pcoip.admx	包含与 PCoIP 显示协议相关的策略设置。 请参阅《在 Horizon 7 中配置远程桌面功能》文档。
PCoIP 客户端会话变量	pcoip.client.admx	包含与影响 Horizon Client for Windows 的 PCoIP 显示协议相关的策略设置。 请参阅《适用于 Windows 的 VMware Horizon Client 安装和设置指南》文档。
用户配置管理	ViewPM.admx	包含与 Horizon Persona Management 相关的策略设置。 请参阅《在 Horizon 7 中设置虚拟桌面》文档。

表 7-2. Horizon ADMX 模板文件（续）

模板名称	模板文件	说明
VMware 虚拟打印重定向	printerRedirection.admx	包含执行以下操作的策略设置：禁用基于位置的打印、禁用打印设置持久性和为重定向的客户端打印机选择打印机驱动程序。
基于位置的打印	LBP.xml	用于为每个基于位置的打印机定义 VMware 虚拟打印的转换规则的模板。
远程桌面服务	vmware_rdsh_server.admx	包含与远程桌面服务相关的策略设置。 请参阅《在 Horizon 7 中配置远程桌面功能》文档。
查看 RTAV 配置	vdm_agent_rtav.admx	包含与实时音频-视频功能配合使用的网络摄像头相关的策略设置。 请参阅《在 Horizon 7 中配置远程桌面功能》文档。
扫描仪重定向	vdm_agent_scanner.admx	包含与被重定向以用于已发布桌面和应用程序的扫描设备相关的策略设置。 请参阅《在 Horizon 7 中配置远程桌面功能》文档。
Serial COM	vdm_agent_serialport.admx	包含与被重定向以用于虚拟桌面的串行 (COM) 端口相关的策略设置。 请参阅《在 Horizon 7 中配置远程桌面功能》文档。
VMware Horizon 打印机重定向	vdm_agent_printing.admx	包含与筛选重定向的打印机相关的策略设置。 请参阅《在 Horizon 7 中配置远程桌面功能》文档。
View Agent Direct-Connection	view_agent_direct_connection.admx	包含与 View Agent Direct-Connection 插件相关的策略设置。请参阅《View Agent Direct-Connection 插件管理指南》文档。
VMware Horizon 性能跟踪器	perf_tracker.admx	包含与 VMware Horizon 性能跟踪器功能相关的策略设置。 请参阅 使用 VMware Horizon 性能跟踪器 。

Horizon 连接服务器配置 ADMX 模板设置

View Server 配置 ADMX (vdm_server.admx) 模板文件包含与所有 Horizon 连接服务器有关的策略设置。

下表介绍了连接服务器配置 ADMX 模板文件中的各个策略设置。该模板仅包含“计算机配置”设置。所有设置均位于组策略管理编辑器中的 **Computer Configuration > Policies > Administrative Templates > VMware View Server Configuration** 文件夹中。

表 7-3. Horizon Server 配置模板设置

设置	属性
Enumerate Forest Trust Child Domains	<p>确定是否枚举服务器所在域信任的每个域。要建立完整的信任链，系统还将枚举每个受信任域所信任的域。该进程会继续递归，直到发现所有受信任的域为止。此信息将传送到连接服务器，以确保客户端登录后可使用所有受信任的域。默认情况下启用此属性。如果禁用此属性，将只枚举直接受信任的域，且不会连接到远程域控制器。</p> <p>注 在域关系复杂的环境中（如在林中的多个域之间使用多个受信任的林结构），此过程需要几分钟才能完成。</p>
Recursive Enumeration of Trusted Domains	<p>确定是否枚举服务器所在域信任的每个域。要建立完整的信任链，系统还将枚举每个受信任域所信任的域。该进程会继续递归，直到发现所有受信任的域为止。此信息将传送到 View 连接服务器，以确保客户端登录后可使用所有受信任的域。</p> <p>默认情况下启用此设置。如果禁用此设置，将只枚举直接受信任的域，且不会连接到远程域控制器。</p> <p>在域关系复杂的环境中（如在林中的多个域之间使用多个受信任的林结构），此过程需要几分钟才能完成。</p>
Windows Password Authentication Mode	<p>选择 Windows 密码身份验证模式。</p> <ul style="list-style-type: none"> ■ KerberosOnly。使用 Kerberos 进行身份验证。 ■ KerberosWithFallbackToNTLM。使用 Kerberos 进行身份验证，但在失败时回退至使用 NTLM。 ■ Legacy。使用 NTLM 进行身份验证，但在失败时回退至使用 Kerberos。用于支持旧版 NT 域控制器。 <p>默认设置为 KerberosOnly。</p>

Horizon 7 公共配置 ADMX 模板设置

Horizon 7 公共配置 ADMX (vdm_common.admx) 模板文件包含所有 Horizon 组件通用的策略设置。此类模板仅包含“计算机配置”设置。

日志配置设置

下表介绍了 Horizon 公共配置 ADMX 模板文件中的日志配置策略设置。所有设置均位于组策略管理编辑器中的 **Computer Configuration > Policies > Administrative Templates > VMware View Common Configuration > Log Configuration** 文件夹中。

表 7-4. View 公共配置模板：日志配置设置

设置	属性
Number of days to keep production logs	指定日志文件在系统中保留的天数。如果未设置任何值，将应用默认值，日志文件将保留 7 天。
Maximum number of debug logs	指定系统中可保留的最大调试日志文件数目。当日志文件达到最大大小时，系统将不再添加更多条目，而是创建一个新的日志文件。当先前的日志文件数量达到此值时，最早的日志文件将被删除。
Maximum debug log size in Megabytes	指定调试日志可以达到的最大大小（以 MB 为单位），达到此大小后系统将关闭该日志文件，并创建一个新的日志文件。

表 7-4. View 公共配置模板：日志配置设置（续）

设置	属性
Log Directory	指定日志文件目录的完整路径。如果该位置不可写，将使用默认位置。对于客户端日志文件，将额外创建一个带客户端名称的目录。
Send logs to a Syslog server	<p>允许将 View server 日志发送到 Syslog 服务器（如 VMware vCenter Log Insight）。将从配置此 GPO 的组织单位 (OU) 或域中的所有 View server 发送日志。</p> <p>您可以在与包含您桌面的 OU 链接的 GPO 中启用此设置，通过这种方法将 Horizon Agent 日志发送到 Syslog 服务器。</p> <p>要将日志数据发送到 Syslog 服务器，请启用此设置，并指定日志级别和服务器的完全限定域名 (FQDN) 或 IP 地址。如果您不想使用默认端口 514，可以指定一个替代端口。使用竖线 () 分隔规范中的每个元素。使用以下语法：</p> <p>日志级别 服务器 FQDN 或 IP [端口号（默认值为 514）]</p> <p>例如，Debug 192.0.2.2。</p> <p>重要 Syslog 数据将在不采用软件加密的情况下跨网络进行发送。由于 View server 日志可能包含敏感数据，因此请避免在不安全的网络中发送 Syslog 数据。如果可能，请使用链路层安全功能（例如 IPsec）来防止此类数据在网络中受到监视。</p>

性能警报设置

表 7-5 介绍了 Horizon 公共配置 ADMX 模板文件中的性能警报设置。所有设置均位于组策略管理编辑器中的 **Computer Configuration > Policies > Administrative Templates > VMware View Common Configuration > Performance Alarms** 文件夹中。

表 7-5. View 公共配置模板：性能警报设置

设置	属性
CPU and Memory Sampling Interval in Seconds	指定 CPU 和内存轮询间隔。低采样间隔会导致高日志输出级别。
Overall CPU usage percentage to issue log info	指定开始记录系统总体 CPU 使用率的阈值。如果有多个处理器可用，此百分比即表示综合使用率。
Overall memory usage percentage to issue log info	指定开始记录提交的总体系统内存使用率的阈值。提交的系统内存是进程分配的内存，操作系统已向其提交物理内存或页面文件中的页槽。
Process CPU usage percentage to issue log info	指定开始记录任意单个进程 CPU 使用率的阈值。

表 7-5. View 公共配置模板：性能警报设置（续）

设置	属性
Process memory usage percentage to issue log info	指定开始记录任意单个进程的内存使用率的阈值。
Process to check, comma separated name list allowing wild cards and exclusion	<p>指定一个用逗号分隔的查询列表，这些查询对应于要检查的一个或多个进程的名称。在每个查询内，您可以使用通配符来筛选列表。</p> <ul style="list-style-type: none"> ■ 星号 (*) 可匹配零个或多个字符。 ■ 问号 (?) 则严格匹配一个字符。 ■ 在查询开头添加叹号 (!) 可将该查询生成的任何结果排除在外。 <p>例如，以下查询将选择以 ws 开头的所有进程，并排除以 sys 结尾的所有进程： '! *sys,ws'</p>

注 性能警报设置仅适用于 Horizon 连接服务器和 Horizon Agent 系统，它们不适用于 Horizon Client 系统。

安全性设置

表 7-6 介绍了 Horizon 公共配置 ADMX 模板文件中的安全性设置。所有设置均位于组策略管理编辑器中的 **Computer Configuration > Policies > Administrative Templates > VMware View Common Configuration > Security Settings** 文件夹中。

表 7-6. View 公共配置模板：安全性设置

设置	属性
Only use cached revocation URLs	<p>证书吊销检查将仅访问缓存 URL。</p> <p>如果未配置，默认为 False。</p>
Revocation URL check timeout milliseconds	<p>所有吊销 URL Wire 检索之间的累积超时（单位：毫秒）。</p> <p>未配置或值设置为 0，意味着使用 Microsoft 默认处理方式。</p>
Type of certificate revocation check	<p>选择要执行的证书吊销检查类型：</p> <ul style="list-style-type: none"> ■ 无 ■ EndCertificateOnly ■ WholeChain ■ WholeChain <p>默认为 WholeChainButRoot。</p>

常规设置

表 7-7 介绍了 Horizon 公共配置 ADMX 模板文件中的常规设置。所有设置均位于组策略管理编辑器中的 **Computer Configuration > Policies > Administrative Templates > VMware View Common Configuration** 文件夹中。

表 7-7. View 公共配置模板：常规设置

设置	属性
Disk threshold for log and events in Megabytes	指定日志和事件的最小剩余磁盘空间阈值。如果不指定任何值，将使用默认值 200。达到指定的值后，事件记录将停止。
Enable extended logging	确定是否将跟踪和调试事件包含在日志文件中。
Override the default View Windows event generation	支持以下值： <ul style="list-style-type: none">■ 0 = 仅生成视图事件的事件日志条目（不会生成日志消息的事件日志条目）■ 1 = 在 4.5（及更低版本）兼容模式下生成事件日志条目。不会生成标准视图事件的事件日志条目。事件日志条目仅基于日志文件文本。■ 2 = 在 4.5（及更低版本）兼容模式下生成事件日志条目，同时包含视图事件。

维护 Horizon 7 组件

为保持 Horizon 7 组件可用并正常运行，您可以执行多种维护任务。

本章讨论了以下主题：

- 备份和还原 Horizon 7 配置数据
- 监控 Horizon 7 组件
- 监视计算机状态
- 了解 Horizon 7 服务
- 更改产品许可证密钥
- 监视产品许可证使用情况
- 从 Active Directory 更新常规用户信息
- 将 View Composer 迁移至另一台计算机
- 更新连接服务器实例、安全服务器或 View Composer 上的证书
- 客户体验改进计划

备份和还原 Horizon 7 配置数据

通过在 Horizon Administrator 中计划或运行自动备份，您可以备份 Horizon 7 和 View Composer 配置数据。通过手动导入备份的 View LDAP 文件和 View Composer 数据库文件，可以还原 Horizon 7 配置。

您可以使用备份和还原功能保留和迁移 Horizon 7 配置数据。

备份 Horizon 连接服务器和 View Composer 数据

完成对连接服务器的初始配置后，您应当计划对 Horizon 7 和 View Composer 配置数据进行定期备份。您可以使用 Horizon Administrator 来保留 Horizon 7 和 View Composer 数据。

Horizon 7 将连接服务器配置数据存储在 View LDAP 存储库中。View Composer 将链接克隆桌面的配置数据存储在 View Composer 数据库中。

当您使用 Horizon Administrator 执行备份时，Horizon 7 会备份 View LDAP 配置数据和 View Composer 数据库。两个备份文件集都存储在同一位置。View LDAP 数据将以加密的 LDAP 数据交换格式 (LDIF) 导出。有关 View LDAP 的说明，请参阅 [View LDAP 目录](#)。

您可以通过多种方式来执行备份。

- 使用 Horizon 7 配置备份功能可计划自动备份。
- 使用 Horizon Administrator 中的**立即备份**功能可即刻开始备份。
- 使用 `vdmexport` 实用程序手动导出 View LDAP 数据。每个连接服务器实例均附带了此实用程序。

`vdmexport` 实用程序可将 View LDAP 数据导出为加密 LDIF 数据、纯文本或移除了密码和其他敏感数据的纯文本。

注 `vdmexport` 工具仅备份 View LDAP 数据。此工具不会备份 View Composer 数据库信息。

有关 `vdmexport` 的更多信息，请参阅[从 Horizon 连接服务器中导出配置数据](#)。

以下指导原则适用于 Horizon 7 配置数据备份：

- Horizon 7 可以从任何连接服务器实例中导出配置数据。
- 如果您的副本实例组中有多个连接服务器实例，则只需从一个实例中导出数据。所有副本实例均包含相同的配置数据。
- 不要将连接服务器副本实例作为备份机制。如果 Horizon 7 将各个连接服务器副本实例中的数据同步，那么一个实例中的任何数据丢失可能会导致所有组成员中均丢失相应数据。
- 如果连接服务器结合使用多个 vCenter Server 实例和多种 Composer 服务，那么 Horizon 7 会备份与 vCenter Server 实例关联的所有 View Composer 数据库。

计划 Horizon 7 配置备份

您可计划定期备份 Horizon 7 配置数据。Horizon 7 将备份 View LDAP 存储库（连接服务器实例用其存储配置数据）的内容。

选择连接服务器实例并单击**立即备份**，即可立即备份配置。

前提条件

熟悉备份设置。请参阅[Horizon 7 配置备份设置](#)。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。
- 2 在**连接服务器**选项卡中，选择要备份的连接服务器实例，然后单击**编辑**。
- 3 在**备份**选项卡上，指定 Horizon 7 配置备份设置以配置备份频率、最大备份数以及备份文件所在的文件夹位置。
- 4 （可选）更改数据恢复密码。
 - a 单击**更改数据恢复密码**。
 - b 键入并再次键入新的密码。
 - c （可选）键入密码提醒。
 - d 单击**确定**。

5 单击确定。

Horizon 7 配置备份设置

Horizon 7 可以定期备份连接服务器和 View Composer 的配置数据。您可以在 Horizon Administrator 中设置备份操作的频率和其他设置。

表 8-1. Horizon 7 配置备份设置

设置	说明
自动备份频率	<p>每小时：每小时整点进行备份。</p> <p>每 6 小时：在零点、上午 6 点、中午 12 点和下午 6 点进行备份。</p> <p>每 12 小时：在零点和中午 12 点进行备份。</p> <p>每天：每天零点进行备份。</p> <p>每 2 天：在星期六、星期一、星期三和星期五的零点进行备份。</p> <p>每周：在每周星期六的零点进行备份。</p> <p>每 2 周：在每隔一周的星期六零点进行备份。</p> <p>从不：不自动进行备份。</p>
最大备份数量	<p>连接服务器实例上可以存储的最大备份文件数。该数必须是大于 0 的整数。</p> <p>达到最大数量时，Horizon 7 会删除最早的备份文件。</p> <p>此设置还适用于您使用立即备份功能创建的备份文件。</p>
文件夹位置	<p>运行连接服务器的计算机上的默认备份文件位置：C:\Programdata\VMware\VDM\backups</p> <p>当您使用立即备份时，Horizon 7 也会将备份文件存储在此位置。</p>

从 Horizon 连接服务器中导出配置数据

您可以通过导出 Horizon 连接服务器实例的 View LDAP 存储库内容来备份其配置数据。

使用 `vdmexport` 命令将 View LDAP 配置数据导出到加密的 LDIF 文件中。也可使用 `vdmexport -v`（逐字）选项将数据导出到纯文本 LDIF 文件中，或使用 `vdmexport -c`（已清除）选项将数据以纯文本形式导出，并移除密码和其他敏感数据。

您可以在任意连接服务器实例上运行 `vdmexport` 命令。如果您的副本实例组中有多个连接服务器实例，则只需从一个实例中导出数据。所有副本实例均包含相同的配置数据。

注 `vdmexport` 命令仅备份 View LDAP 数据。此命令不会备份 View Composer 数据库信息。

前提条件

- 从以下默认路径中找出随连接服务器安装的 `vdmexport.exe` 命令可执行文件。

`C:\Program Files\VMware\VMware View\Server\tools\bin`

- 以管理员或管理员 (只读) 用户角色登录到连接服务器实例。

步骤

- 1 选择开始 > 命令提示符。

- 2 在命令提示符下，键入 `vdmexport` 命令，并将输出重定向至文件。例如：

```
vdmexport > Myexport.LDF
```

默认情况下，导出数据是加密的。

您可以将输出文件的名称指定为 `-f` 选项的一个参数。例如：

```
vdmexport -f Myexport.LDF
```

您可以使用 `-v` 选项以纯文本的格式（逐字）导出数据。例如：

```
vdmexport -f Myexport.LDF -v
```

您可以使用 `-c` 选项以纯文本格式导出数据并移除密码和敏感数据（已清除）。例如：

```
vdmexport -f Myexport.LDF -c
```

注 不要使用清除过的备份数据来还原 View LDAP 配置。清除过的配置数据缺少密码和其他重要信息。

有关 `vdmexport` 命令的更多信息，请参阅《Horizon 7 集成指南》文档。

后续步骤

您可使用 `vdmimport` 命令来还原或传输连接服务器的配置信息。

有关导入 LDIF 文件的详细信息，请参阅[还原 Horizon 连接服务器和 View Composer 配置数据](#)。

还原 Horizon 连接服务器和 View Composer 配置数据

您可以手动还原由 Horizon 7 备份的连接服务器 LDAP 配置文件和 View Composer 数据库文件。

您需要手动运行单个实用程序来还原连接服务器和 View Composer 配置数据。

还原配置数据前，请确认您在 Horizon Administrator 中备份了配置数据。请参阅[备份 Horizon 连接服务器和 View Composer 数据](#)。

使用 `vdmimport` 实用程序将连接服务器数据从 LDIF 备份文件导入到连接服务器实例中的 View LDAP 存储库。

您可以使用 `SviConfig` 实用程序将 View Composer 数据从 `.svi` 备份文件导入到 View Composer SQL 数据库中。

注 在某些情况下，您可能需要安装当前版本的连接服务器实例，然后通过导入连接服务器 LDAP 配置文件来还原现有的 Horizon 7 配置。您可能需要将此过程纳入业务连续性和灾难恢复 (BC/DR) 计划中，也可能需要将其作为使用现有 Horizon 7 配置设置其他数据中心的一个步骤，或者出于其他原因需要执行此过程。有关更多信息，请参阅《Horizon 7 安装指南》文档。

将配置数据导入 Horizon 连接服务器中

您可以通过导入 LDIF 文件中存储的数据备份副本，来还原连接服务器实例的配置数据。

使用 `vdmimport` 命令将 LDIF 文件的数据导入到连接服务器实例中的 View LDAP 存储库。

如果您已通过使用 Horizon Administrator 或默认 `vdmexport` 命令备份了 View LDAP 配置，则导出的 LDIF 文件是加密的。在导入前您必须解密此 LDIF 文件。

如果导出的 LDIF 文件是纯文本格式的，则您无需解密该文件。

注 不要以清除过的格式（移除了密码和其他敏感数据的纯文本）导入 LDIF 文件。否则，重要配置信息将会从恢复的 View LDAP 存储库中丢失。

有关备份 View LDAP 存储库的信息，请参阅[备份 Horizon 连接服务器和 View Composer 数据](#)。

前提条件

- 从以下默认路径中找出随连接服务器安装的 `vdmimport` 命令可执行文件。
C:\Program Files\VMware\VMware View\Server\tools\bin
- 以具有管理员角色的用户身份登录到连接服务器实例。
- 确认您知道数据恢复密码。如果配置了密码提醒，则您可通过运行不含密码选项的 `vdmimport` 命令来显示提醒。

步骤

- 1 通过停止运行 View Composer 的服务器上的 Windows 服务 VMware Horizon View Composer，停止所有 View Composer 实例。
- 2 通过停止所有安全服务器上的 Windows 服务 VMware Horizon 安全服务器，停止所有安全服务器实例。
- 3 卸载所有 Horizon 连接服务器实例。
卸载 VMware Horizon 连接服务器和 AD LDS Instance VMwareVDMDS。
- 4 安装连接服务器的一个实例。
- 5 通过停止 Windows 服务 VMware Horizon 连接服务器停止连接服务器实例。
- 6 单击**开始 > 命令提示符**。
- 7 解密已加密的 LDIF 文件。

通过命令提示符键入 `vdmimport` 命令。指定 `-d` 选项、包含数据恢复密码的 `-p` 选项和包含现有加密 LDIF 文件的 `-f` 选项（后附已解密 LDIF 文件的名称）。例如：

```
vdmimport -d -p mypassword
-f MyEncryptedexport.LDF > MyDecryptedexport.LDF
```

如果您不记得数据恢复密码，则可键入不带 `-p` 选项的命令。实用程序显示密码提醒并提示您输入密码。

8 导入解密的 LDIF 文件还原 View LDAP 配置。

指定含有已解密的 LDIF 文件的 `-f` 选项。例如：

```
vdmimport -f MyDecryptedexport.LDF
```

9 卸载连接服务器。

仅卸载 VMware Horizon 连接服务器软件包。

10 重新安装连接服务器。**11 登录到 Horizon Administrator 并验证配置是否正确。****12 启动 View Composer 实例。****13 重新安装副本服务器实例。****14 启动安全服务器实例。**

如果安全服务器存在配置不一致的风险，应将其卸载而非停止，然后在该过程结束后重新进行安装。

`vdmimport` 命令将使用该 LDIF 文件中的配置数据更新连接服务器中的 View LDAP 存储库。有关 `vdmimport` 命令的更多信息，请参阅《Horizon 7 安装指南》文档。

注 确保要还原的配置与 vCenter Server 和 View Composer（如果在使用中）的已知虚拟机相匹配。必要时，请从备份还原 View Composer 配置。请参阅[还原 View Composer 数据库](#)。还原 View Composer 配置后，如果 vCenter Server 中的虚拟机自备份 View Composer 配置以来发生更改，则您可能需要手动解决此不一致问题。

还原 View Composer 数据库

您可以将备份的 View Composer 配置文件导入存储链接克隆信息的 View Composer 数据库中。

使用 `SviConfig restoredata` 命令，您可以在系统出现故障后还原 View Composer 数据库，或是将 View Composer 配置恢复到某个早期状态。

重要 只有经验丰富的 View Composer 管理员才可以使用 `SviConfig` 实用程序。该实用程序旨在解决 View Composer 服务的相关问题。

前提条件

确认 View Composer 数据库备份文件的位置。默认情况下，Horizon 7 将备份文件存储在连接服务器计算机的 C: 驱动器上，路径为 `C:\Programdata\VMware\VDM\backups`。

View Composer 备份文件采用带日期时间戳和 `.svi` 后缀的命名约定。

`Backup-YearMonthDayCount-vCenter Server Name_Domain Name.svi`

例如: `Backup-20090304000010-foobar_test_org.svi`

熟悉 `SviConfig restoredata` 参数：

- `DsnName` - 用于连接至数据库的 DSN。`DsnName` 参数是必填项，并且不能是空字符串。

- **Username** - 用于连接至数据库的用户名。如果未指定该参数，则使用 **Windows** 身份验证。
- **Password** - 连接至数据库的用户密码。如果未指定该参数且未使用 **Windows** 身份验证，系统会提示您稍后再输入密码。
- **BackupFilePath** - **View Composer** 备份文件的路径。

DsnName 和 **BackupFilePath** 参数是必填项，并且不能是空字符串。**Username** 和 **Password** 参数是可选项。

步骤

- 1 将 **View Composer** 备份文件从连接服务器计算机复制到可被安装有 **VMware Horizon View Composer** 服务的计算机访问的位置。
- 2 在安装了 **View Composer** 的计算机上，停止 **VMware Horizon View Composer** 服务。
- 3 打开 **Windows** 命令提示并导航到 **SviConfig** 可执行文件。

该文件与 **View Composer** 应用程序位于同一位置。默认路径为 **C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe**。

- 4 运行 **SviConfig restoredata** 命令。

```
sviconfig -operation=restoredata
          -DsnName=target_database_source_name_(DSN)
          -Username=database_administrator_username
          -Password=database_administrator_password
          -BackupFilePath=path_to_View_Composer_backup_file
```

例如：

```
sviconfig -operation=restoredata -dsname=LinkedClone
          -username=Admin -password=Pass
          -backupfilepath="C:\Program Files (x86)\VMware\VMware View
          Composer\Backup-20090304000010-foobar_test_org.SVI"
```

- 5 启动 **VMware Horizon View Composer** 服务。

后续步骤

有关 **SviConfig restoredata** 命令的输出结果代码，请参阅[还原 View Composer 数据库的结果代码](#)。

还原 View Composer 数据库的结果代码

还原 **View Composer** 数据库时，**SviConfig restoredata** 命令会返回一个结果代码。

表 8-2. Restoredata 结果代码

代码	描述
0	操作成功结束。
1	找不到所提供的 DSN。
2	提供的数据库管理员凭据无效。
3	数据库的驱动程序不受支持。

表 8-2. Restoredata 结果代码（续）

代码	描述
4	出现异常问题，命令无法完成。
14	另一个应用程序正在使用 VMware Horizon View Composer 服务。执行命令前，请关闭该服务。
15	还原过程中出现问题。屏幕日志输出中提供了详细信息。

导出 View Composer 数据库中的数据

您可以将 View Composer 数据库中的数据导出到文件。

重要 只有经验丰富的 View Composer 管理员才能使用 SviConfig 实用程序。

前提条件

默认情况下，Horizon 7 将备份文件存储在 View 连接服务器计算机的 C:驱动器上：
C:\Programdata\VMware\VDM\backups。

熟悉 SviConfig exportdata 参数：

- DsnName - 用于连接至数据库的 DSN。如果未指定，DSN 名称、用户名和密码将从服务器配置文件中检索。
- Username - 用于连接至数据库的用户名。如果未指定该参数，则使用 Windows 身份验证。
- Password - 连接至数据库的用户密码。如果未指定该参数且未使用 Windows 身份验证，系统会提示您稍后再输入密码。
- OutputFilePath - 输出文件路径。

步骤

- 1 在安装了 View Composer 的计算机上，停止 VMware Horizon View Composer 服务。
- 2 打开 Windows 命令提示并导航到 SviConfig 可执行文件。

该文件与 View Composer 应用程序位于同一位置。

View-Composer-installation-directory\sviconfig.exe

3 运行 SviConfig exportdata 命令。

```
sviconfig -operation=exportdata
          -DsnName=target_database_source_name_(DSN)
          -Username=database_administrator_username
          -Password=database_administrator_password
          -OutputFilePath=path_to_View_Composer_output_file
```

例如：

```
sviconfig -operation=exportdata -dsnname=LinkedClone
          -username=Admin -password=Pass
          -outputfilepath="C:\Program Files\VMware\VMware View
          Composer\Export-20090304000010-foobar_test_org.SVI"
```

后续步骤

有关 SviConfig exportdata 命令的导出结果代码，请参阅[导出 View Composer 数据库的结果代码](#)。

导出 View Composer 数据库的结果代码

导出 View Composer 数据库时，SviConfig exportdata 命令会显示一个退出代码。

表 8-3. Exportdata ExitStatus 代码

代码	描述
0	数据导出成功结束。
1	无法找到提供的 DSN 名称。
2	所提供的凭据无效。
3	所提供数据库不支持的驱动程序。
4	出现异常问题。
18	无法连接到数据库服务器。
24	无法打开输出文件。

监控 Horizon 7 组件

使用 Horizon Administrator 仪表板可以快速浏览 Horizon 7 部署中 Horizon 7 和 vSphere 组件的状态。

Horizon Administrator 显示有关连接服务器实例、事件数据库、网关、安全服务器、View Composer 服务、数据存储、vCenter Server 实例和域的监视信息。

注 Horizon 7 不能确定 Kerberos 域的状态信息。即使配置了 Kerberos 域且其可以正常运行，Horizon Administrator 也会将 Kerberos 域的状态显示为未知。

步骤

- 1 在 Horizon Administrator 中，单击**仪表板**。

2 在“系统运行状况”窗格中，展开 **View 组件**、**vSphere 组件**或者其他组件。

- 绿色向上箭头表明组件没有问题。
- 红色向下箭头表明组件不可用或未运行。
- 黄色双箭头表明组件处于警告状态。
- 问号表明组件状态未知。

3 单击组件的名称。

将出现一个对话框显示名称、版本、状态和其他组件信息。

后续步骤

使用 vCenter Server 监控所有 vSAN 群集以及加入 vSAN 数据存储的磁盘。有关在 vSphere 5.5 Update 1 中监控 vSAN 的更多信息，请参阅《vSphere 存储》文档和《vSphere 监控和性能》文档。有关在 vSphere 6 或更高版本中监控 vSAN 的更多信息，请参阅《管理 VMware vSAN》文档。

监视计算机状态

使用 Horizon Administrator 仪表板可以快速浏览 Horizon 7 部署中计算机的状态。例如，您可以显示所有断开连接的计算机或处于维护模式下的计算机。

前提条件

熟悉虚拟机状态值。有关虚拟机状态的更多信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“vCenter Server 虚拟机的状态”。

步骤

1 在 Horizon Administrator 中，单击**仪表板**。

2 在“计算机状态”窗格中，展开一个状态文件夹。

选项	说明
正在准备	列出当计算机处于置备、删除或维护模式时的状态。
问题计算机	列出错误状态。
已准备好供使用	列出当计算机可供使用时的状态。

3 定位计算机状态，并单击旁边带超链接的数字。

计算机页面将显示所有处于选定状态的计算机。

后续步骤

您可以单击某个计算机名称查看有关该计算机的详细信息，也可以单击 Horizon Administrator 后退箭头返回到“仪表板”页面。

了解 Horizon 7 服务

连接服务器实例和安全服务器的运行依赖于系统上运行的若干服务。这些系统是自动启动和停止的，但您有时需要手动调整这些服务的运行。

您可以使用 **Microsoft Windows** 服务工具来停止或启动 **Horizon 7** 服务。如果您停止连接服务器主机或安全服务器上的 **Horizon 7** 服务，最终用户将无法访问他们的远程桌面或应用程序，直到您重新启动服务。如果服务停止运行，或者它所控制的 **Horizon 7** 功能不响应，可能也要重新启动服务。

停止和启动 Horizon 7 服务

连接服务器实例和安全服务器的运行依赖于系统上运行的若干服务。排除 **Horizon 7** 运行故障时，有时可能需要手动停止和启动这些服务。

当您停止 **Horizon 7** 服务时，最终用户无法连接到其远程桌面和应用程序。您应该在计划的系统维护时间执行这种操作，或者警告最终用户其桌面和应用程序会暂时不可用。

注 仅停止连接服务器主机上的 **VMware Horizon View** 连接服务器服务或安全服务器上的 **VMware Horizon View** 安全服务器服务。不要停止任何其他组件服务。

前提条件

熟悉连接服务器主机和安全服务器上运行的服务，请分别参阅以下两个主题：[连接服务器主机上的服务](#)和[安全服务器上的服务](#)。

步骤

- 1 在命令提示符中输入 **services.msc**，启动 **Windows Services** 工具。
- 2 选择连接服务器主机上的 **VMware Horizon View** 连接服务器服务或安全服务器上的 **VMware Horizon View** 安全服务器服务，然后根据需要单击**停止**、**重新启动**或**启动**。
- 3 确认所列服务的状态按预期发生了更改。

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 8-4. 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 VMware VDMDS 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。

表 8-4. Horizon 连接服务器主机服务（续）

服务名称	启动类型	说明
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 8-5. 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。

更改产品许可证密钥

如果系统中当前的许可证到期，或者您要访问当前未经许可的 Horizon 7 功能，则可以使用 Horizon Administrator 更改产品许可证密钥。

Horizon 7 正在运行时，您可以向 Horizon 7 添加许可证。无需重新引导系统，对桌面和应用程序的访问也不会中断。

前提条件

要成功操作 Horizon 7 及其加载功能（如 View Composer 和发布的应用程序），请获取有效的产品许可证密钥。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 产品许可和使用情况**。

将在许可面板中显示当前许可证密钥的第一个和最后五个字符。

- 2 单击 **编辑许可证**。

- 3 输入许可证序列号，然后单击 **确定**。

产品许可窗口将显示更新的许可信息。

- 4 验证许可证的过期日期。

- 5 根据产品许可证授权您使用的 VMware Horizon 7 版本，验证是启用还是禁用了桌面、应用程序远程处理和 View Composer 许可证。

并非所有版本都提供 VMware Horizon 7 的所有特性和功能。有关各个版本中的功能集的比较，请参阅 <http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>。

- 6 验证许可使用模式是否与产品许可证中使用的模式匹配。

使用情况是按照命名用户或并发用户数计算的，具体取决于产品许可证的版本和使用协议。

监视产品许可证使用情况

在 Horizon 7 Administrator 中，您可以监视同时连接到 Horizon 的活动用户。**产品许可和使用情况**页显示当前和最高历史使用用户数。您可以通过这些数字跟踪产品许可证的使用情况。另外，还可以重置历史使用情况数据并重新开始当前数据。

Horizon 提供了两种许可使用模式，一种模式用于命名用户，另一种模式用于并发用户。Horizon 计算环境中的命名用户和并发用户，而无论使用哪种产品许可证版本或使用模式协议。

对于命名用户，Horizon 计算已访问 Horizon 环境的唯一用户数。如果命名用户运行多个单用户桌面、已发布的桌面和已发布的应用程序，则将该用户计入一次。

对于命名用户，**产品许可和使用情况**页上的**当前**列显示在首次配置 Horizon 部署或上次重置**命名用户计数**后的用户数。**最高**列不适用于命名用户。

对于并发用户，Horizon 计算每个会话的单用户桌面连接数。如果并发用户运行多个单用户桌面，将单独计算每个连接的桌面会话。

对于并发用户，将计算每个用户的已发布桌面和应用程序连接数。如果并发用户运行多个已发布的桌面会话和应用程序，则仅将该用户计入一次，即使在不同的 RDS 主机上托管了不同的已发布桌面或应用程序也是如此。如果并发用户运行一个单用户桌面以及其他已发布的桌面和应用程序，则仅将该用户计入一次。

对于并发用户，**产品许可和使用情况**页面上的**最高**列会显示在首次配置 Horizon 部署或上次重置**最大计数**后的最高并发桌面会话以及已发布的桌面和应用程序用户数。

您可以监视协作会话的数量以及连接到会话的会话协作者数量。

- “活动 - 协作会话”：会话所有者邀请了一个或多个用户加入会话的会话数量。示例：John 邀请了一个人加入他的会话，Mary 邀请了一个人加入她的会话。此行的值为 2，而不管是否有任何受邀者加入了会话。
- “活动 - 协作者总数”：连接到协作会话的用户总数，包括会话所有者和任何协作者。示例：John 邀请了一个人，但只有一个人加入了会话。Mary 邀请了一个人，但此人没有加入会话。此行的值为 3：John 的协作会话有一个主协作者和一个辅助协作者，而 Mary 的协作会话有一个主协作者和零个辅助协作者。由于计入了会话所有者，因此可以确保协作者的总数始终大于或等于协作会话的总数。

重置产品许可证使用情况数据

在 Horizon Administrator 中，您可以重置历史产品使用情况数据并使用当前数据重新开始。

具有**管理全局配置和策略**特权的管理人员可以选择**重置最大计数**和**重置已命名用户计数**设置。要限制访问这些设置，请仅为指定的管理员授予该特权。

前提条件

熟悉产品许可证使用情况。请参阅[监视产品许可证使用情况](#)。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 产品许可和使用情况**。
- 2 （可选）在**使用情况**窗格中，选择**重置最大计数**。
并发连接的最高历史数量将重置为当前数量。
- 3 （可选）在**使用情况**窗格中，选择**重置已命名用户计数**。
最高历史命名用户数将重置为 0。

注 如果在**用户和组**页上选择**更新常规用户信息**，也会将最高历史命名用户数重置为 0。

从 Active Directory 更新常规用户信息

您可以使用 Active Directory 中存储的当前用户信息来更新 Horizon 7。此功能将更新 Horizon 7 用户的姓名、电话、电子邮件、用户名和默认的 Windows 域。还会更新受信任的外部域。

当您要修改 Active Directory 中的受信任外部域的列表时，尤其是域之间的信任关系改变会影响 Horizon 7 中的用户权限时，请使用此功能。

此功能会扫描 Active Directory 中的最新用户信息并刷新 Horizon 7 配置。

在更新常规用户信息时，也会将命名用户数重置为 0。该数字显示在 Horizon Administrator 的**产品许可和使用情况**页上。请参阅[重置产品许可证使用情况数据](#)。

您也可以使用 `vdmadmin` 命令更新用户和域信息。请参阅[使用 -F 选项更新外部安全主体](#)。

前提条件

确认您能以具有**管理全局配置和策略**特权的管理人员身份登录到 Horizon Administrator。

步骤

- 1 在 Horizon Administrator 中，单击**用户和组**。
- 2 选择要更新所有用户的信息还是单个用户的信息。

选项	操作
针对所有用户	单击 更新常规用户信息 。 更新所有用户和组可能需要较长时间。
针对单个用户	<ol style="list-style-type: none"> a 单击要更新的用户名。 b 单击更新常规用户信息。

将 View Composer 迁移至另一台计算机

在某些情况下，您可能需要将 VMware Horizon View Composer 服务迁移到新的 Windows Server 虚拟机或物理机。例如，您可以将 View Composer 和 vCenter Server 迁移到新的 ESXi 主机或群集上以扩展您的 Horizon 7 部署。此外，View Composer 和 vCenter Server 无需安装在相同的 Windows Server 计算机上。

您可以将 View Composer 从 vCenter Server 计算机迁移到独立计算机，或从独立计算机迁移到 vCenter Server 计算机。

- **View Composer 迁移指南**

迁移 VMware Horizon View Composer 服务所采用的步骤取决于是否打算保留现有链接克隆虚拟机。

- **迁移使用现有数据库的 View Composer**

将 View Composer 迁移到另一台物理或虚拟机时，如果您想保留当前的链接克隆虚拟机，则新的 VMware Horizon View Composer 服务必须继续使用现有的 View Composer 数据库。

- **迁移不包含链接克隆虚拟机的 View Composer**

如果当前的 VMware Horizon View Composer 服务不管理任何链接克隆虚拟机，您可将 View Composer 迁移到一台新的物理机或虚拟机，而无需将 RSA 密钥迁移到此新计算机。已迁移的 VMware Horizon View Composer 服务可连接到原始的 View Composer 数据库，或者您可以为 View Composer 准备新的数据库。

- **准备 Microsoft .NET Framework 以迁移 RSA 密钥**

要使用现有的 View Composer 数据库，就必须在计算机之间迁移 RSA 密钥容器。您可以使用 Microsoft .NET Framework 提供的 ASP.NET IIS 注册工具迁移 RSA 密钥容器。

- **将 RSA 密钥容器迁移至新的 View Composer 服务**

要使用现有的 View Composer 数据库，您必须将 RSA 密钥容器从现有 VMware Horizon View Composer 服务所在的源物理机或虚拟机迁移到要安装新的 VMware Horizon View Composer 服务的计算机上。

View Composer 迁移指南

迁移 VMware Horizon View Composer 服务所采用的步骤取决于是否打算保留现有链接克隆虚拟机。

要保留您部署中的链接克隆虚拟机，安装在新虚拟机或物理机上的 VMware Horizon View Composer 服务必须继续使用现有 View Composer 数据库。View Composer 数据库包含创建、置备、维护及删除链接克隆所需的数据。

迁移 VMware Horizon View Composer 服务时，也可将 View Composer 数据库迁移到新计算机。

无论是否迁移 View Composer 数据库，都必须在与安装 VMware Horizon View Composer 服务的新计算机处于同一个域或受信任域中的某个可用计算机上配置该数据库。

View Composer 会创建 RSA 密钥对来加密和解密 View Composer 数据库中存储的身份验证信息。要使该数据源与新的 VMware Horizon View Composer 服务兼容，必须迁移由原来的 VMware Horizon View Composer 服务创建的 RSA 密钥容器。您必须将 RSA 密钥容器导入到安装新服务的计算机上。

如果当前的 VMware Horizon View Composer 服务未管理任何链接克隆虚拟机，则可以在不使用现有 View Composer 数据库的情况下迁移该服务。无论是否使用现有数据库，都没有必要迁移 RSA 密钥。

注 每个 VMware Horizon View Composer 服务实例必须具有各自的 View Composer 数据库。多个 VMware Horizon View Composer 服务不能共享一个 View Composer 数据库。

迁移使用现有数据库的 View Composer

将 View Composer 迁移到另一台物理或虚拟机时，如果您想保留当前的链接克隆虚拟机，则新的 VMware Horizon View Composer 服务必须继续使用现有的 View Composer 数据库。

按以下任何方式迁移 View Composer 时，请遵循此过程中的步骤：

- 从 vCenter Server 计算机到独立计算机
- 从独立计算机到 vCenter Server 计算机
- 从一台独立计算机到另一台独立计算机
- 从一台 vCenter Server 计算机到另一台 vCenter Server 计算机

迁移 VMware Horizon View Composer 服务时，也可将 View Composer 数据库迁移到新位置。例如，如果当前的数据库位于您正要迁移的 vCenter Server 计算机上，则您可能也需要迁移 View Composer 数据库。

在新计算机上安装 VMware Horizon View Composer 服务时，您必须将服务配置为连接到 View Composer 数据库。

前提条件

- 熟悉 View Composer 迁移要求。请参阅 [View Composer 迁移指南](#)。
- 熟悉将 RSA 密钥容器迁移到新的 VMware Horizon View Composer 服务的步骤。请参阅[准备 Microsoft .NET Framework 以迁移 RSA 密钥和将 RSA 密钥容器迁移至新的 View Composer 服务](#)。
- 熟悉《Horizon 7 安装指南》文档中有关安装 VMware Horizon View Composer 服务的内容。
- 熟悉《Horizon 7 安装指南》文档中有关为 View Composer 配置 TLS 证书的内容。
- 熟悉如何在 Horizon Administrator 中配置 View Composer。请参阅[配置 View Composer 设置和配置 View Composer 域](#)。
- 最佳做法是，确认您用于迁移 View Composer 的源计算机和目标计算机完全相同，并且共享相同的管理员凭据。在将 View Composer 从一个独立的计算机迁移到已装有 View Composer 的 vCenter Server 计算机时，如果两台计算机上所使用的凭据不一样，则配置 View Composer 可能会失败。

步骤

- 1 禁用与 VMware Horizon View Composer 服务相关联的 vCenter Server 实例中的虚拟机置备。

- a 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。
- b 在 **vCenter Servers** 选项卡上，选择 vCenter Server 实例并单击**禁用置备**。

- 2 （可选）将 View Composer 数据库迁移到新位置。

如果需要采取此步骤，请向您的数据库管理员咨询迁移说明。

- 3 从当前的计算机中卸载 VMware Horizon View Composer 服务。

- 4 （可选）将 RSA 密钥容器迁移到新的计算机上。

- 5 在新计算机上安装 VMware Horizon View Composer 服务。

在安装过程中，请指定原始 VMware Horizon View Composer 服务所使用的数据库的 DSN。还要指定为此数据库的 ODBC 数据源所提供的域管理员用户名和密码。

如果您已迁移了数据库，则 DSN 和数据源信息必须指向数据库的新位置。无论数据库是否已被迁移，新的 VMware Horizon View Composer 服务都必须能访问有关链接克隆的原始数据库信息。

- 6 在新计算机上为 View Composer 配置 SSL 服务器证书。

您可以复制在原始计算机上为 View Composer 安装的证书，或安装新的证书。

- 7 在 Horizon Administrator 中，配置新的 View Composer 设置。

- a 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。
- b 在 **vCenter Server** 选项卡上，选择与此 View Composer 服务关联的 vCenter Server 实例，然后单击**编辑**。
- c 在“View Composer Server 设置”窗格中，单击**编辑**并提供新的 View Composer 设置。

如果您在新的计算机上同时安装 View Composer 与 vCenter Server，请选择 **View Composer 与 vCenter Server 一同安装**。

如果您在独立的计算机上安装 View Composer，请选择**独立的 View Composer Server**，并提供 View Composer 计算机的 FQDN 和 View Composer 用户的用户名与密码。

- d 在“域”窗格中，单击**验证服务器信息**并根据需要添加或编辑 View Composer 域。
- e 单击**确定**。

迁移不包含链接克隆虚拟机的 View Composer

如果当前的 VMware Horizon View Composer 服务不管理任何链接克隆虚拟机，您可将 View Composer 迁移到一台新的物理机或虚拟机，而无需将 RSA 密钥迁移到此新计算机。已迁移的 VMware Horizon View Composer 服务可连接到原始的 View Composer 数据库，或者您可以为 View Composer 准备新的数据库。

前提条件

- 熟悉《Horizon 7 安装指南》文档中有关安装 VMware Horizon View Composer 服务的内容。

- 熟悉《Horizon 7 安装指南》文档中有关为 View Composer 配置 TLS 证书的内容。
- 熟悉从 Horizon Administrator 中移除 View Composer 的步骤。请参阅[从 Horizon 7 中移除 View Composer](#)。

移除 View Composer 之前，请确认 View Composer 不再管理任何链接克隆桌面。如果仍存在链接克隆，必须将其删除。

- 熟悉如何在 Horizon Administrator 中配置 View Composer。请参阅[配置 View Composer 设置](#)和[配置 View Composer 域](#)。

步骤

- 1 在 Horizon Administrator 中，从 Horizon Administrator 中移除 View Composer。

- a 选择 **View 配置 > 服务器**。
- b 在 **vCenter Server** 选项卡上，选择与 View Composer 服务关联的 vCenter Server 实例，然后单击 **编辑**。
- c 在“View Composer Server 设置”窗格中，单击 **编辑**。
- d 选择**不使用 View Composer**，然后单击**确定**。

- 2 从当前的计算机中卸载 VMware Horizon View Composer 服务。

- 3 在新计算机上安装 VMware Horizon View Composer 服务。

在安装过程中，配置 View Composer 以连接到原始的或新的 View Composer 数据库的 DSN。

- 4 在新计算机上为 View Composer 配置 TLS 服务器证书。

您可以复制在原始计算机上为 View Composer 安装的证书，或安装新的证书。

- 5 在 Horizon Administrator 中，配置新的 View Composer 设置。

- a 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。
- b 在 **vCenter Server** 选项卡上，选择与此 View Composer 服务关联的 vCenter Server 实例，然后单击 **编辑**。
- c 在“View Composer Server 设置”窗格中，单击 **编辑**。
- d 提供新的 View Composer 设置。

如果您在新的计算机上同时安装 View Composer 与 vCenter Server，请选择 **View Composer 与 vCenter Server 一同安装**。

如果您在独立的计算机上安装 View Composer，请选择**独立的 View Composer Server**，并提供 View Composer 计算机的 FQDN 和 View Composer 用户的用户名与密码。

- e 在“域”窗格中，单击**验证服务器信息**并根据需要添加或编辑 View Composer 域。
- f 单击**确定**。

准备 Microsoft .NET Framework 以迁移 RSA 密钥

要使用现有的 View Composer 数据库，就必须在计算机之间迁移 RSA 密钥容器。您可以使用 Microsoft .NET Framework 提供的 ASP.NET IIS 注册工具迁移 RSA 密钥容器。

前提条件

下载 .NET Framework，了解 ASP.NET IIS 注册工具。请访问 <http://www.microsoft.com/net>。

步骤

- 1 在安装了与现有数据库关联的 VMware Horizon View Composer 服务的物理机或虚拟机上安装 .NET Framework。
- 2 在您要安装新 VMware Horizon View Composer 服务的目标计算机上安装 .NET Framework。

后续步骤

将 RSA 密钥容器迁移到目标计算机上。请参阅[将 RSA 密钥容器迁移至新的 View Composer 服务](#)。

将 RSA 密钥容器迁移至新的 View Composer 服务

要使用现有的 View Composer 数据库，您必须将 RSA 密钥容器从现有 VMware Horizon View Composer 服务所在的源物理机或虚拟机迁移到要安装新的 VMware Horizon View Composer 服务的计算机上。

您必须在安装新的 VMware Horizon View Composer 服务之前执行此操作。

前提条件

确认 Microsoft .NET Framework 和 ASP.NET IIS 注册工具已安装在源计算机和目标计算机上。请参阅[准备 Microsoft .NET Framework 以迁移 RSA 密钥](#)。

步骤

- 1 在现有 VMware Horizon View Composer 服务所在的源计算机中打开一个命令提示符，并导航至 %windir%\Microsoft.NET\Framework\v2.0xxxxx 目录。
- 2 键入 aspnet_regiis 命令以将 RSA 密钥对保存在本地文件中。

```
aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri
```

ASP.NET IIS 注册工具会将 RSA 公-私密钥对从 SviKeyContainer 容器导出到 keys.xml 文件，并在本地保存该文件。

- 3 将 keys.xml 文件复制到要安装新 VMware Horizon View Composer 服务的目标计算机中。
- 4 在目标计算机上打开一个命令提示符并导航至 %windir%\Microsoft.NET\Framework\v2.0xxxxx 目录。

5 键入 `aspnet_regiis` 命令迁移 RSA 密钥对数据。

```
aspnet_regiis -pi "SviKeyContainer" "路径\keys.xml" -exp
```

其中，*path* 是导出文件的路径。

`-exp` 选项可创建可导出的密钥对。如果以后需要迁移，可将这些密钥从此台计算机导出然后再导入到另一台计算机。如果您以前未使用 `-exp` 选项便将密钥迁移到这台计算机上，则您可以使用 `-exp` 选项再次导入这些密钥，以便您以后可以导出这些密钥。

注册工具会将密钥对数据导入本地密钥容器。

后续步骤

在目标计算机上安装新的 VMware Horizon View Composer 服务。提供 DSN 和 ODBC 数据源信息，允许 View Composer 连接到原始 VMware Horizon View Composer 服务所使用的相同数据库信息。有关安装说明，请参阅《Horizon 7 安装指南》文档中的“安装 View Composer”。

完成将 View Composer 迁移到新计算机的步骤，并使用相同的数据库。请参阅[迁移使用现有数据库的 View Composer](#)。

更新连接服务器实例、安全服务器或 View Composer 上的证书

接收更新的服务器 TLS 证书或中间证书时，请将证书导入到每个连接服务器、安全服务器或 View Composer 主机上的 Windows 本地计算机证书存储区中。

通常情况下，服务器证书在 12 个月之后过期，根证书和中间证书会在 5 或 10 年后过期。

有关导入服务器和中间证书的详细信息，请参阅《Horizon 7 安装指南》文档中的“配置 Horizon 连接服务器、安全服务器或 View Composer 以使用新的 TLS 证书”。

前提条件

- 在当前有效证书过期之前从 CA 获取更新的服务器和中间证书。
- 确认证书插件已添加至 Windows Server 上的 MMC，Windows Server 上安装了连接服务器实例、安全服务器或 VMware Horizon View Composer 服务。

步骤

- 1 将已签发的 TLS 服务器证书导入 Windows Server 主机上的 Windows 本地计算机证书存储区。
 - a 在证书插件中，将服务器证书导入到**证书(本地计算机) > 个人 > 证书**文件夹。
 - b 选择**将此密钥标记为可导出**。
 - c 单击**下一步**，然后单击**完成**。
- 2 对于连接服务器或安全服务器，从签发给 Horizon 7 Server 的旧证书中删除证书的友好名称 **vdm**。
 - a 右键单击旧证书，然后单击**属性**
 - b 在“常规”选项卡上，删除友好名称文本 **vdm**。

- 3 对于连接服务器或安全服务器，将证书的友好名称 **vdm** 添加到用于替换原有证书的新证书。
 - a 右键单击新证书，然后单击**属性**
 - b 在“常规”选项卡上，在友好名称字段，键入 **vdm**。
 - c 单击**应用**，然后单击**确定**。
- 4 有关发放给 View Composer 的服务器证书，请运行 SviConfig ReplaceCertificate 实用程序以将新证书绑定到 View Composer 所用的端口。
此实用程序将旧证书绑定替换为新证书绑定。
 - a 停止 VMware Horizon View Composer 服务。
 - b 打开 Windows 命令提示并导航到 SviConfig 可执行文件。
该文件与 View Composer 应用程序位于同一位置。默认路径为 C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe。
 - c 键入 SviConfig ReplaceCertificate 命令。例如：


```
sviconfig -operation=ReplaceCertificate
          -delete=false
```

 实用程序显示 Windows 本地计算机证书存储区中可使用的 TLS 证书编号列表。
 - d 要选择证书，请键入证书的编号，然后按 Enter。
- 5 如果中间证书签发给连接服务器、安全服务器或 View Composer 主机，则将中间证书的最新更新导入到 Windows 证书存储区中的**证书(本地计算机) > 中间证书颁发机构 > 证书文件夹**。
- 6 重新启动 VMware Horizon View 连接服务器服务、VMware View 安全服务器服务或 VMware Horizon View Composer 服务，使所做的更改生效。

客户体验改进计划

此产品参与 VMware 客户体验改进计划 (Customer Experience Improvement Program, CEIP)。您可以选择将此产品加入或退出 CEIP。

“信任与保证中心”（网址为 <http://www.vmware.com/trustvmware/ceip.html>）详细阐述了通过 CEIP 收集的数据以及 VMware 将此数据用于何种用途。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 产品许可和使用情况**。
- 2 在**客户体验计划**面板中，单击**编辑设置**。
- 3 选择**加入 VMware 客户体验改进计划**以加入 CEIP。
如果不选择此选项，您就不能加入 CEIP。
- 4 单击**确定**。

在 Horizon Administrator 中管理 ThinApp 应用程序

9

您可以使用 Horizon Administrator 分发和管理用 VMware ThinApp 打包的应用程序。在 Horizon Administrator 中管理 ThinApp 应用程序的任务包括：捕获和存储应用程序包、将 ThinApp 应用程序添加到 Horizon Administrator 以及将 ThinApp 应用程序分配到计算机和桌面池。

您必须拥有在 Horizon Administrator 中使用 ThinApp 管理功能的许可。

重要 如果您更想将 ThinApp 分配至 Active Directory 用户和组，而不是分配至计算机和桌面池，那么您可以使用 VMware Identity Manager。

本章讨论了以下主题：

- [Horizon 7 对 ThinApp 应用程序的要求](#)
- [捕获和存储应用程序包](#)
- [将 ThinApp 应用程序分配到计算机和桌面池](#)
- [在 Horizon Administrator 中维护 ThinApp 应用程序](#)
- [在 Horizon Administrator 中监视 ThinApp 应用程序并进行故障排除](#)
- [ThinApp 配置示例](#)

Horizon 7 对 ThinApp 应用程序的要求

在 Horizon Administrator 中捕获和存储将要分发到远程桌面的 ThinApp 应用程序时，必须满足某些要求。

- 必须将应用程序打包为 Microsoft Installation (MSI) 包。
- 必须使用 ThinApp 4.6 或更高版本来创建 MSI 包或重新打包。
- 必须将 MSI 包存储在 Windows 网络共享上，该网络共享必须位于连接服务器主机和远程桌面均可访问的 Active Directory 域中。文件服务器必须支持基于计算机帐户的身份验证和文件权限。
- 必须在托管 MSI 包的网络共享位置上配置文件和共享权限，为内置 Active Directory 组 "Domain Computers" 授予读访问权限。如果您打算将 ThinApp 应用程序分发给域控制器，还必须为内置 Active Directory 组 "Domain Controllers" 授予读访问权限。
- 要允许用户访问流式传输 ThinApp 应用程序包，必须针对相应用户将托管 ThinApp 程序包的网络共享的 NTFS 权限设置为读取和执行。

- 确保非连续命名空间不会阻止域成员计算机访问托管 MSI 包的网络共享位置。当 Active Directory 域名和该域中计算机使用的 DNS 命名空间不同时，将会出现非连续命名空间。有关更多信息，请参阅 VMware 知识库 (KB) 文章 1023309。
- 要在远程桌面上运行流式 ThinApp 应用程序，用户必须对托管 MSI 包的网络共享拥有访问权限。

捕获和存储应用程序包

ThinApp 通过可将应用程序从底层操作系统及其库和框架中分离，并将应用程序捆绑到一个可执行文件（称为应用程序包）来提供应用程序虚拟化。

要在 Horizon Administrator 中管理 ThinApp 应用程序，您必须使用 ThinApp 安装捕获向导以 MSI 格式捕获并打包应用程序，并且将 MSI 程序包存储在应用程序存储库中。

应用程序存储库是一个 Windows 网络共享位置。您可以使用 Horizon Administrator 将网络共享位置注册为应用程序存储库。您可以注册多个应用程序存储库。

注 如果您拥有多个应用程序存储库，则可使用第三方解决方案来管理负载平衡和可用性。Horizon 7 中不包含负载平衡或可用性解决方案。

有关 ThinApp 功能以及如何使用 ThinApp 安装捕获向导的完整信息，请参阅《VMware ThinApp 简介》和《ThinApp 用户指南》。

1 将应用程序打包

您可以使用 ThinApp 安装捕获向导来捕获和打包应用程序。

2 创建 Windows 网络共享位置

您必须创建一个 Windows 网络共享，以托管在 Horizon Administrator 中分发到远程桌面和池的 MSI 包。

3 注册应用程序存储库

您必须在 Horizon Administrator 中将用来托管 MSI 包的 Windows 网络共享位置注册为应用程序存储库。

4 将 ThinApp 应用程序添加到 Horizon Administrator

您可以通过扫描应用程序存储库并选择 ThinApp 应用程序将 ThinApp 应用程序添加到 Horizon Administrator 中。将 ThinApp 应用程序添加到 Horizon Administrator 之后，您可以将其分配到计算机和桌面池。

5 创建 ThinApp 模板

您可以在 Horizon Administrator 中创建一个模板以指定一组 ThinApp 应用程序。您可以使用模板并按照功能、供应商或其他任何适合您组织的逻辑分组方式对应用程序进行整体分组。

将应用程序打包

您可以使用 ThinApp 安装捕获向导来捕获和打包应用程序。

前提条件

- 从 <http://www.vmware.com/products/thinapp> 下载 ThinApp 软件，并将其安装到干净的计算机上。View 支持 ThinApp 4.6 及更高版本。

- 熟悉《ThinApp 用户指南》中的 ThinApp 软件要求和应用程序打包说明。

步骤

- 1 启动 ThinApp 安装捕获向导，按照向导中的提示操作。
- 2 当 ThinApp 安装捕获向导提示您指定项目位置时，请选择生成 MSI 包。
- 3 如果您计划以流式方式将应用程序提供给远程桌面，请将 `package.ini` 文件中的 `MSIStreaming` 属性设为 1。

```
MSIStreaming=1
```

ThinApp 安装捕获向导会将应用程序、运行该应用程序所需的全部必需组件以及应用程序本身封装到一个 MSI 包中。

后续步骤

创建一个用于存储 MSI 包的 Windows 网络共享位置。

创建 Windows 网络共享位置

您必须创建一个 Windows 网络共享，以托管在 Horizon Administrator 中分发到远程桌面和池的 MSI 包。

前提条件

- 使用 ThinApp 安装捕获向导来打包应用程序。
- 确认网络共享满足 Horizon 7 对于存储 ThinApp 应用程序的要求。请参阅 [Horizon 7 对 ThinApp 应用程序的要求](#) 了解更多信息。

步骤

- 1 在连接服务器主机和远程桌面均可访问的 Active Directory 域中的某个计算机上创建一个共享文件夹。
- 2 在共享文件夹上配置文件和共享权限，为内置 Active Directory 组 "Domain Computers" 授予读访问权限。
- 3 如果您打算将 ThinApp 应用程序分配到域控制器，必须为内置 Active Directory 组 "Domain Controllers" 授予读访问权限。
- 4 如果计划使用流式传输 ThinApp 应用程序包，针对相应用户将托管 ThinApp 包的共享的 NTFS 权限设置为读取和执行。
- 5 将 MSI 包复制到共享文件夹中。

后续步骤

在 Horizon Administrator 中将 Windows 网络共享位置注册为应用程序存储库。

注册应用程序存储库

您必须在 Horizon Administrator 中将用来托管 MSI 包的 Windows 网络共享位置注册为应用程序存储库。

您可以注册多个应用程序存储库。

前提条件

创建 Windows 网络共享。

步骤

1 在 Horizon Administrator 中，选择 **View 配置 > ThinApp 配置**，然后单击**添加存储库**。

2 在**显示名称**文本框中键入应用程序存储库的显示名称。

3 在**共享路径**文本框中键入托管应用程序包的 Windows 网络共享位置的路径。

网络共享位置的路径必须是 \\服务器计算机名\共享名称格式，其中服务器计算机名是服务器计算机的 DNS 名称。不要指定 IP 地址。

例如：\\server.domain.com\MSIPackages

4 单击**保存**以在 Horizon Administrator 中注册应用程序存储库。

将 ThinApp 应用程序添加到 Horizon Administrator

您可以通过扫描应用程序存储库并选择 ThinApp 应用程序将 ThinApp 应用程序添加到 Horizon Administrator 中。将 ThinApp 应用程序添加到 Horizon Administrator 之后，您可以将其分配到计算机和桌面池。

前提条件

在 Horizon Administrator 中注册应用程序存储库。

步骤

1 在 Horizon Administrator 中，选择**目录 > ThinApp**。

2 在**摘要**选项卡上，单击**扫描新 ThinApp**。

3 选择要扫描的应用程序存储库和文件夹并单击**下一步**。

如果应用程序存储库包含子文件夹，可展开根文件夹并选择一个子文件夹。

4 选择您想添加到 Horizon Administrator 的 ThinApp 应用程序。

您可以使用按住 **Ctrl** 键并单击或按住 **Shift** 键并单击的方式选择多个 ThinApp 应用程序。

5 单击**扫描**开始扫描您选择的 MSI 包。

如果您需要停止扫描，请单击**停止扫描**。

Horizon Administrator 会报告每个扫描操作的状态以及添加到 Horizon Administrator 的 ThinApp 应用程序数量。如果您选择某个已存在于 Horizon Administrator 中的应用程序，则不会再次添加该程序。

6 单击**完成**。

新的 ThinApp 应用程序会显示在**摘要**选项卡上。

后续步骤

（可选）创建 ThinApp 模板。

创建 ThinApp 模板

您可以在 Horizon Administrator 中创建一个模板以指定一组 ThinApp 应用程序。您可以使用模板并按照功能、供应商或其他任何适合您组织的逻辑分组方式对应用程序进行整体分组。

ThinApp 模板可简化多个应用程序的分发。将 ThinApp 模板分配到计算机或桌面池时，Horizon Administrator 会安装模板中当前所有的应用程序。

创建 ThinApp 模板是可选操作。

注 如果您在将 ThinApp 模板分配到计算机或桌面池之后向该模板添加应用程序，Horizon Administrator 不会自动将新应用程序分配到计算机或桌面池。如果您从之前分配到计算机或桌面池的 ThinApp 模板中移除应用程序，则该应用程序仍会分配到该计算机或桌面池。

前提条件

将所选的 ThinApp 应用程序添加到 Horizon Administrator 中。

步骤

- 1 在 Horizon Administrator 中，选择**目录 > ThinApp**，然后单击**新建模板**。
- 2 键入模板的名称并单击**添加**。
所有可用的 ThinApp 应用程序都显示在该表中。
- 3 要查找一个特定的 ThinApp 应用程序，需要在**查找**文本框中键入应用程序名并单击**查找**。
- 4 选择您想在模板中包含的 ThinApp 应用程序并单击**添加**。
您可以使用按住 **Ctrl** 键并单击或按住 **Shift** 键并单击的方式选择多个应用程序。
- 5 单击**确定**保存模板。

将 ThinApp 应用程序分配到计算机和桌面池

要在远程桌面上安装 ThinApp 应用程序，您需要使用 Horizon Administrator 将 ThinApp 应用程序分配到计算机或桌面池。

在您将某个 ThinApp 应用程序分配到计算机时，Horizon Administrator 将在几分钟后开始在虚拟机上安装该应用程序。当您把某个 ThinApp 应用程序分配到桌面池时，Horizon Administrator 将在用户首次登录到池中的远程桌面时开始安装该应用程序。

流式

Horizon Administrator 在远程桌面上安装 ThinApp 应用程序的快捷方式。该快捷方式指向托管存储库的网络共享位置上的 ThinApp 应用程序。用户必须有权访问该网络共享位置才能运行流式 ThinApp 应用程序。

完整

Horizon Administrator 在本地文件系统中安装完整的 ThinApp 应用程序。

安装 ThinApp 应用程序所花费的时间取决于该应用程序的大小。

重要 您可以将 ThinApp 应用程序分配到基于虚拟机的桌面和自动桌面池或者包含 vCenter Server 虚拟机的手动池。无法将 ThinApp 应用程序分配到发布的桌面或传统 PC。

- **分配 ThinApp 应用程序的最佳实践**

将 ThinApp 应用程序分配到计算机和桌面池时，请遵循最佳做法。

- **将一个 ThinApp 应用程序分配到多个计算机**

您可以将某个特定的 ThinApp 分配到一个或多个计算机。

- **将多个 ThinApp 应用程序分配到一个计算机**

您可以将一个或多个 ThinApp 应用程序分配到某个特定的计算机。

- **将 ThinApp 应用程序分配到多个桌面池**

您可以将某个特定的 ThinApp 应用程序分配到一个或多个桌面池。

- **将多个 ThinApp 应用程序分配到一个桌面池**

您可以将一个或多个 ThinApp 应用程序分配到某个特定的桌面池。

- **向计算机或桌面池分配 ThinApp 模板**

通过向计算机或桌面池分配 ThinApp 模板，可以简化多个 ThinApp 应用程序的分配。

- **查看 ThinApp 应用程序分配**

您可以查看当前分配了某个特定 ThinApp 应用程序的所有计算机和桌面池。还可以查看分配到某个特定计算机或桌面池的所有 ThinApp 应用程序。

- **显示 MSI 包信息**

将 ThinApp 应用程序添加到 Horizon Administrator 后，您可以显示有关其 MSI 包的信息。

分配 ThinApp 应用程序的最佳实践

将 ThinApp 应用程序分配到计算机和桌面池时，请遵循最佳做法。

- 要在特殊远程桌面上安装 ThinApp 应用程序，可将该应用程序分配给托管桌面的虚拟机。如果您对计算机使用了通用命名约定，则可以根据计算机分配快速为使用该命名约定的所有计算机分发应用程序。
- 要在桌面池中的所有计算机上安装 ThinApp 应用程序，可将该应用程序分配给桌面池。如果您按部门或用户类型组织桌面池，则可以根据桌面池分配快速为特定部门或用户分发应用程序。例如，如果有一个用于会计部门用户的桌面池，则可以通过将应用程序分配给会计池的方式，将同一个应用程序分发给会计部门的所有用户。
- 要简化对多个 ThinApp 应用程序的分发，可以在 ThinApp 模板中包含这些应用程序。将 ThinApp 模板分配给计算机或桌面池时，Horizon Administrator 将安装当前模板中的所有应用程序。
- 如果 ThinApp 模板包含已分配给该计算机或桌面池的 ThinApp 应用程序，则不要将该模板分配给计算机或桌面池。此外，不要通过不同的安装类型将一个 ThinApp 模板多次分配给同一个计算机或桌面池。在这两种情况下，Horizon Administrator 将返回 ThinApp 分配错误。

将一个 ThinApp 应用程序分配到多个计算机

您可以将某个特定的 ThinApp 分配到一个或多个计算机。

前提条件

扫描应用程序存储库，将选定的 ThinApp 应用程序添加到 Horizon Administrator 中。请参阅[将 ThinApp 应用程序添加到 Horizon Administrator](#)。

步骤

- 1 在 Horizon Administrator 中，选择目录 > **ThinApp**，然后选择 ThinApp 应用程序。
- 2 从添加分配下拉菜单中选择分配计算机。

表中将显示尚未分配 ThinApp 应用程序的计算机。

选项	操作
查找特定计算机	在 查找 文本框中键入计算机名称，然后单击 查找 。
查找遵循同一命令约定的所有计算机	在 查找 文本框中键入部分计算机名称，然后单击 查找 。

- 3 选择要向其分配 ThinApp 应用程序的计算机并单击**添加**。

您可以使用按住 **Ctrl** 键并单击或按住 **Shift** 键并单击的方式选择多个计算机。

- 4 选择安装类型，然后单击**确定**。

选项	操作
流式	在计算机上安装应用程序的快捷方式。该快捷方式指向托管存储库的网络共享位置上的应用程序。用户必须有权访问该网络共享位置才能运行该应用程序。
完整	在计算机的本地文件系统中安装完整的应用程序。

某些 ThinApp 应用程序不支持这两种安装类型。应用程序包的创建方式决定可用的安装类型。

Horizon Administrator 在几分钟后开始安装 ThinApp 应用程序。安装完成后，应用程序将可供虚拟机托管的桌面的所有用户使用。

将多个 ThinApp 应用程序分配到一个计算机

您可以将一个或多个 ThinApp 应用程序分配到一个特定的计算机。

前提条件

扫描应用程序存储库，将选定的 ThinApp 应用程序添加到 Horizon Administrator 中。请参阅[将 ThinApp 应用程序添加到 Horizon Administrator](#)。

步骤

- 1 在 Horizon Administrator 中，选择资源 > 计算机，然后双击“计算机”列中的计算机名称。

- 2 在**摘要**选项卡上单击“ThinApps”窗格中的**添加分配**。

表中将显示尚未分配到计算机的 ThinApp 应用程序。

- 3 要查找一个特定的应用程序，请在**查找**文本框中键入应用程序名并单击**查找**。

- 4 选择一个要分配到计算机的 ThinApp 应用程序，然后单击**添加**。

重复该步骤添加多个应用程序。

- 5 选择安装类型，然后单击**确定**。

选项	操作
流式	在计算机上安装应用程序的快捷方式。该快捷方式指向托管存储库的网络共享位置上的应用程序。用户必须有权访问该网络共享位置才能运行该应用程序。
完整	在计算机的本地文件系统中安装完整的应用程序。

某些 ThinApp 应用程序不支持这两种安装类型。应用程序包的创建方式决定可用的安装类型。

Horizon Administrator 在几分钟后开始安装 ThinApp 应用程序。安装完成后，应用程序将可供虚拟机托管的桌面的所有用户使用。

将 ThinApp 应用程序分配到多个桌面池

您可以将某个特定的 ThinApp 应用程序分配到一个或多个桌面池。

将 ThinApp 应用程序分配到链接克隆池时，如果随后刷新、重构或重新平衡该池，则 Horizon Administrator 将重新安装该应用程序。您无需手动重新安装该应用程序。

前提条件

扫描应用程序存储库，将选定的 ThinApp 应用程序添加到 Horizon Administrator 中。请参阅[将 ThinApp 应用程序添加到 Horizon Administrator](#)。

步骤

- 1 在 Horizon Administrator 中，选择**目录 > ThinApp**，然后选择 ThinApp 应用程序。

- 2 从**添加分配**下拉菜单中，选择**分配桌面池**。

尚未分配 ThinApp 应用程序的桌面池会显示在表中。

选项	操作
查找特定桌面池	在 查找 文本框中键入桌面池名称，然后单击 查找 。
查找遵循同一命名约定的所有桌面池	在 查找 文本框中键入部分桌面池名称，然后单击 查找 。

- 3 选择您希望向其分配 ThinApp 应用程序的桌面池，然后单击**添加**。

您可以使用按住 **Ctrl** 键并单击或按住 **Shift** 键并单击的方式选择多个桌面池。

4 选择安装类型，然后单击**确定**。

选项	操作
流式	在计算机上安装应用程序的快捷方式。该快捷方式指向托管存储库的网络共享位置上的应用程序。用户必须有权访问该网络共享位置才能运行该应用程序。
完整	在计算机的本地文件系统中安装完整的应用程序。

某些 ThinApp 应用程序不支持这两种安装类型。应用程序包的创建方式决定可用的安装类型。

Horizon Administrator 会在用户首次登录到池中桌面时开始安装 ThinApp 应用程序。安装完成后，该应用程序即可供桌面池的所有用户使用。

将多个 ThinApp 应用程序分配到一个桌面池

您可以将一个或多个 ThinApp 应用程序分配到某个特定的桌面池。

将 ThinApp 应用程序分配到链接克隆池时，如果随后刷新、重构或重新平衡该池，则 Horizon Administrator 将重新安装该应用程序。您无需手动重新安装该应用程序。

前提条件

扫描应用程序存储库，将选定的 ThinApp 应用程序添加到 Horizon Administrator 中。请参阅[将 ThinApp 应用程序添加到 Horizon Administrator](#)。

步骤

1 在 Horizon Administrator 中，选择**目录 > 桌面池**并双击桌面池 ID。

2 在**清单**选项卡上，单击 **ThinApps**，然后单击**添加分配**。

尚未被分配到池的 ThinApp 应用程序将显示在表中。

3 要查找某个特定的应用程序，请在**查找**文本框中键入 ThinApp 应用程序名并单击**查找**。

4 选择一个要分配到池的 ThinApp 应用程序并单击**添加**。

重复该步骤可选择多个应用程序。

5 选择安装类型，然后单击**确定**。

选项	操作
流式	在计算机上安装应用程序的快捷方式。该快捷方式指向托管存储库的网络共享位置上的应用程序。用户必须有权访问该网络共享位置才能运行该应用程序。
完整	在计算机的本地文件系统中安装完整的应用程序。

某些 ThinApp 应用程序不支持这两种安装类型。应用程序包的创建方式决定可用的安装类型。

Horizon Administrator 会在用户首次登录到池中桌面时开始安装 ThinApp 应用程序。安装完成后，应用程序将可供该桌面池的所有用户使用。

向计算机或桌面池分配 ThinApp 模板

通过向计算机或桌面池分配 ThinApp 模板，可以简化多个 ThinApp 应用程序的分配。

向计算机或桌面池分配 ThinApp 模板后，Horizon Administrator 会安装模板中当前所包含的 ThinApp 应用程序。

前提条件

创建 ThinApp 模板。请参阅[创建 ThinApp 模板](#)。

步骤

- 1 在 Horizon Administrator 中，选择目录 > ThinApp。
- 2 选择 ThinApp 模板。
- 3 从添加分配下拉菜单中，选择分配计算机或分配桌面池。

表中显示了所有计算机或桌面池。

选项	操作
查找特定计算机或桌面池	在 查找 文本框中键入计算机或桌面池的名称，然后单击 查找 。
查找遵循同一命名约定的所有计算机或桌面池	在 查找 文本框中键入部分计算机或桌面池名称，然后单击 查找 。

- 4 选择您希望向其分配 ThinApp 模板的计算机或桌面池，然后单击**添加**。
重复此步骤可选择多个计算机或桌面池。
- 5 选择安装类型，然后单击**确定**。

选项	操作
流式	在计算机上安装应用程序的快捷方式。该快捷方式指向托管存储库的网络共享位置上的应用程序。用户必须有权访问该网络共享位置才能运行该应用程序。
完整	在计算机的本地文件系统中安装完整的应用程序。

某些 ThinApp 应用程序不支持这两种安装类型。应用程序包的创建方式决定可用的安装类型。

向计算机分配 ThinApp 模板几分钟后，Horizon Administrator 即会开始安装模板中的应用程序。向桌面池分配 ThinApp 模板后，Horizon Administrator 会在用户首次登录到该桌面池中的远程桌面时开始安装该模板中的应用程序。安装完成后，这些应用程序即可供计算机或桌面池的所有用户使用。

如果 ThinApp 模板包含已分配到计算机或桌面池的应用程序，Horizon Administrator 会返回一个应用程序分配错误。

查看 ThinApp 应用程序分配

您可以查看当前分配了某个特定 ThinApp 应用程序的所有计算机和桌面池。还可以查看分配到某个特定计算机或桌面池的所有 ThinApp 应用程序。

前提条件

熟悉[ThinApp 应用程序安装状态值](#)中介绍的 ThinApp 安装状态值。

步骤

- ◆ 选择您希望查看的 ThinApp 应用程序分配。

选项	操作
查看分配了某个特定 ThinApp 应用程序的所有计算机和桌面池	<p>选择目录 > ThinApp，然后双击 ThinApp 应用程序的名称。</p> <p>分配选项卡显示当前分配了该应用程序的计算机和桌面池，包括安装类型。</p> <p>计算机选项卡显示当前与该应用程序关联的计算机，包括安装状态信息。</p> <p>注 当您将某个 ThinApp 应用程序分配到池时，只有在安装该应用程序后，计算机选项卡上才会显示池中的计算机。</p>
查看分配到某个特定计算机的所有 ThinApp 应用程序	<p>选择资源 > 计算机，然后在“计算机”列中双击计算机的名称。</p> <p>摘要选项卡上的“ThinApp”窗格显示当前分配到该计算机的每个应用程序，包括安装状态。</p>
查看分配到某个特定桌面池的所有 ThinApp 应用程序	<p>选择目录 > 桌面池，双击池 ID，然后选择清单选项卡并单击 ThinApp。</p> <p>“ThinApp 分配”窗格显示当前分配到该桌面池的每个应用程序。</p>

ThinApp 应用程序安装状态值

将 ThinApp 应用程序分配到计算机或池后，Horizon Administrator 将指示安装的状态。

下表介绍了每个状态值。

表 9-1. ThinApp 应用程序安装状态

状态	说明
已分配	ThinApp 应用程序已分配到计算机。
安装错误	Horizon Administrator 尝试安装 ThinApp 应用程序时发生错误。
卸载错误	Horizon Administrator 尝试卸载 ThinApp 应用程序时发生错误。
已安装	ThinApp 应用程序已安装。
正在等待安装	<p>Horizon Administrator 正在尝试安装 ThinApp 应用程序。</p> <p>您不能取消分配处于此状态的应用程序。</p> <p>注 桌面池中的计算机不会显示此值。</p>
正在等待卸载	Horizon Administrator 正在尝试卸载 ThinApp 应用程序。

显示 MSI 包信息

将 ThinApp 应用程序添加到 Horizon Administrator 后，您可以显示有关其 MSI 包的信息。

步骤

- 1 在 Horizon Administrator 中，选择目录 > **ThinApp**。
摘要选项卡列出了当前可用的应用程序，并显示了完整分配和流式分配的数量。
- 2 在 ThinApp 列中双击应用程序名。
- 3 选择**摘要**选项卡查看有关 MSI 包的常规信息。

- 单击 **程序包信息** 查看有关 MSI 包的详细信息。

在 Horizon Administrator 中维护 ThinApp 应用程序

在 Horizon Administrator 中维护 ThinApp 应用程序时涉及的任务包括：移除 ThinApp 应用程序分配、移除 ThinApp 应用程序和应用程序存储库，以及修改和删除 ThinApp 模板。

注 要升级 ThinApp 应用程序，必须先取消分配并移除旧版应用程序，然后再添加并分配新版程序。

- **从多个计算机中移除一个 ThinApp 应用程序分配**
您可以从一个或多个计算机中移除某个特定的 ThinApp 应用程序分配。
- **从一个计算机中移除多个 ThinApp 应用程序分配**
您可以从某个特定的计算机中移除一个或多个 ThinApp 应用程序分配。
- **从多个桌面池中移除一个 ThinApp 应用程序分配**
您可以从一个或多个桌面池中移除某个特定的 ThinApp 应用程序分配。
- **从一个桌面池中移除多个 ThinApp 应用程序分配**
您可以从某个特定的桌面池中移除一个或多个 ThinApp 应用程序分配。
- **从 Horizon Administrator 中移除 ThinApp 应用程序**
从 Horizon Administrator 中移除 ThinApp 应用程序后，您将无法再将该应用程序分配到计算机和桌面池。
- **修改或删除 ThinApp 模板**
您可以从 ThinApp 模板添加和移除应用程序，也可以删除 ThinApp 模板。
- **移除应用程序存储库**
您可以从 Horizon Administrator 中移除应用程序存储库。

从多个计算机中移除一个 ThinApp 应用程序分配

您可以从一个或多个计算机中移除某个特定的 ThinApp 应用程序分配。

前提条件

通知由计算机托管的远程桌面的用户您要移除应用程序。

步骤

- 1 在 Horizon Administrator 中，选择 **目录 > ThinApp**，然后双击 ThinApp 应用程序的名称。
- 2 在 **分配** 选项卡上，选择一个计算机并单击 **移除分配**。
您可以使用按住 **Ctrl** 键并单击或按住 **Shift** 键并单击的方式选择多个计算机。

Horizon Administrator 在几分钟后卸载 ThinApp 应用程序。

重要 如果最终用户在 Horizon Administrator 尝试卸载 ThinApp 应用程序时使用该程序，卸载将失败且应用程序状态变为“卸载错误”。发生此错误时，必须首先手动从计算机中卸载 ThinApp 应用程序文件，然后单击 Horizon Administrator 中的**移除桌面的应用程序**状态。

从一个计算机中移除多个 ThinApp 应用程序分配

您可以从某个特定的计算机中移除一个或多个 ThinApp 应用程序分配。

前提条件

通知由计算机托管的远程桌面的用户您要移除应用程序。

步骤

- 1 在 Horizon Administrator 中，选择**资源 > 计算机**，然后双击“计算机”列中的计算机名称。
- 2 在**摘要**选项卡上单击“ThinApps”窗格中的**移除分配**。

重复该步骤移除其他应用程序分配。

Horizon Administrator 在几分钟后卸载 ThinApp 应用程序。

重要 如果最终用户在 Horizon Administrator 尝试卸载 ThinApp 应用程序时使用该程序，卸载将失败且应用程序状态变为“卸载错误”。发生此错误时，必须首先手动从计算机中卸载 ThinApp 应用程序文件，然后单击 Horizon Administrator 中的**移除桌面的应用程序**状态。

从多个桌面池中移除一个 ThinApp 应用程序分配

您可以从一个或多个桌面池中移除某个特定的 ThinApp 应用程序分配。

前提条件

通知相应池中的远程桌面用户您打算移除应用程序。

步骤

- 1 在 Horizon Administrator 中，选择**目录 > ThinApp**，然后双击 ThinApp 应用程序的名称。
- 2 在**分配**选项卡上，选择一个桌面池并单击**移除分配**。

您可以使用按住 **Ctrl** 键并单击或按住 **Shift** 键并单击的方式选择多个桌面池。

Horizon Administrator 会在用户首次登录到池中的远程桌面时卸载这些 ThinApp 应用程序。

从一个桌面池中移除多个 ThinApp 应用程序分配

您可以从某个特定的桌面池中移除一个或多个 ThinApp 应用程序分配。

前提条件

通知相应池中的远程桌面用户您打算移除应用程序。

步骤

- 1 在 Horizon Administrator 中，选择目录 > 桌面池并双击桌面池 ID。
- 2 在清单选项卡上，单击 **ThinApps**，选择 ThinApp 应用程序，然后**移除分配**。
重复该步骤移除多个应用程序。

Horizon Administrator 会在用户首次登录到池中的远程桌面时卸载这些 ThinApp 应用程序。

从 Horizon Administrator 中移除 ThinApp 应用程序

从 Horizon Administrator 中移除 ThinApp 应用程序后，您将无法再将该应用程序分配到计算机和桌面池。

如果您的组织决定用其他供应商的应用程序来取代某个 ThinApp 应用程序，您可能需要移除该 ThinApp 应用程序。

注 如果 ThinApp 应用程序已分配给计算机或桌面池，或者处于“正在等待卸载”状态，将无法移除该 ThinApp 应用程序。

前提条件

如果 ThinApp 应用程序当前已分配到某个计算机或桌面池，请从计算机或桌面池中移除该分配。

步骤

- 1 在 Horizon Administrator 中，选择目录 > **ThinApp**，然后选择 ThinApp 应用程序。
- 2 单击**移除 ThinApp**。
- 3 单击**确定**。

修改或删除 ThinApp 模板

您可以从 ThinApp 模板添加和移除应用程序，也可以删除 ThinApp 模板。

如果您在将 ThinApp 模板分配到计算机或桌面池之后向该模板添加应用程序，Horizon Administrator 不会自动将新应用程序分配到计算机或桌面池。如果您从之前分配到计算机或桌面池的 ThinApp 模板中移除应用程序，则该应用程序仍会分配到该计算机或桌面池。

步骤

- ◆ 在 Horizon Administrator 中，选择目录 > **ThinApp**，然后选择 ThinApp 模板。

选项	操作
从模板添加或移除 ThinApp 应用程序	单击 编辑模板 。
移除模板	单击 移除模板 。

移除应用程序存储库

您可以从 Horizon Administrator 中移除应用程序存储库。

如果不再需要应用程序存储库中包含的 MSI 包，或者需要将 MSI 包移到其他网络共享位置，您可能需要移除应用程序存储库。您无法在 Horizon Administrator 中编辑应用程序存储库的共享路径。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > ThinApp 配置**，然后选择应用程序存储库。
- 2 单击 **移除存储库**。

在 Horizon Administrator 中监视 ThinApp 应用程序并进行故障排除

Horizon Administrator 会将与 ThinApp 应用程序管理相关的事件记录到事件和报告数据库中。您可以在 Horizon Administrator 中的 **事件** 页面上查看这些事件。

出现以下情况时，**事件** 页面上会显示事件。

- 分配了 ThinApp 应用程序或移除了应用程序分配
- 在计算机上安装或卸载了 ThinApp 应用程序
- 无法安装或卸载 ThinApp 应用程序
- 在 Horizon Administrator 中注册、修改或移除了 ThinApp 应用程序存储库
- 将 ThinApp 应用程序添加到了 Horizon Administrator 中

故障排除提示可帮助您解决常见的 ThinApp 应用程序管理问题。

无法注册应用程序存储库

您无法在 Horizon Administrator 中注册应用程序存储库。

问题

尝试在 Horizon Administrator 中注册应用程序存储库时，收到一条错误消息。

原因

连接服务器主机无法访问托管应用程序存储库的网络共享。您在 **共享路径** 文本框中键入的网络共享路径可能不正确，托管应用程序存储库的网络共享位置位于连接服务器主机无法访问的域中，或者尚未正确设置网络共享位置的权限。

解决方案

- 如果网络共享路径不正确，则需要键入正确的网络共享路径。不支持包含 IP 地址的网络共享路径。
- 如果网络共享位置位于不可访问的域中，请将应用程序包复制到连接服务器主机可访问域中的网络共享位置。

- 确认在共享文件夹上的文件和共享权限中为内置 Active Directory 组 "Domain Computers" 授予了读访问权限。如果您打算将 ThinApp 分配到域控制器，请确认在文件和共享权限中为内置 Active Directory 组 "Domain Controllers" 授予了读访问权限。设置或更改权限后，可能需要等待 20 分钟才可以访问网络共享位置。

无法将 ThinApp 应用程序添加到 Horizon Administrator

Horizon Administrator 无法将 ThinApp 应用程序添加到 Horizon Administrator。

问题

在 Horizon Administrator 中单击扫描新 ThinApp 时，没有可用的 MSI 包。

原因

原因可能在于应用程序包不是 MSI 格式，或者连接服务器主机无法访问网络共享位置中的目录。

解决方案

- 确认应用程序存储库中的应用程序包采用了 MSI 格式。
- 确认网络共享满足 Horizon 7 对 ThinApp 应用程序的要求。请参阅 [Horizon 7 对 ThinApp 应用程序的要求](#) 了解更多信息。
- 确认网络共享位置中的目录具有正确的权限。请参阅[无法注册应用程序存储库](#)了解更多信息。

在扫描应用程序存储库时，连接服务器调试日志文件中会出现消息。连接服务器日志文件位于连接服务器主机上的 `drive:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` 目录中。

无法分配 ThinApp 模板

您无法将 ThinApp 模板分配到计算机或桌面池。

问题

尝试将 ThinApp 模板分配到计算机或桌面池时，Horizon Administrator 返回一个分配错误。

原因

这可能是由于 ThinApp 模板包含一个已分配到计算机或桌面池的应用程序，也可能是因为 ThinApp 模板之前已通过其他安装类型分配到计算机或桌面池。

解决方案

如果该模板中包含一个已分配到计算机或桌面池的 ThinApp 应用程序，则需要创建一个不包含该应用程序的新模板，或者编辑现有模板并移除该应用程序。将新的或修改后的模板分配到计算机或桌面池。

要更改 ThinApp 应用程序的安装类型，您必须从计算机或桌面池移除现有应用程序分配。卸载 ThinApp 应用程序之后，可通过其他安装类型将其分配到计算机或桌面池。

ThinApp 应用程序未安装

Horizon Administrator 无法安装 ThinApp 应用程序。

问题

ThinApp 应用程序的安装状态显示为“正在等待安装”或“安装错误”。

原因

此问题的常见原因包括：

- 计算机上没有足够的磁盘空间来安装 ThinApp 应用程序。
- 连接服务器主机与计算机之间，或连接服务器主机与应用程序存储库之间的网络连接丢失。
- 无法在网络共享位置访问 ThinApp 应用程序。
- ThinApp 应用程序之前已安装到计算机上，或者计算机上已存在相关目录或文件。

您可以查看 Horizon Agent 和连接服务器日志文件，了解有关问题原因的更多信息。

Horizon Agent 日志文件位于计算机上的 `drive:\ProgramData\VMware\VDM\logs` 中。

连接服务器日志文件位于连接服务器主机上的 `drive:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` 目录中。

解决方案

- 1 在 Horizon Administrator 中，选择目录 > ThinApp。
- 2 单击 ThinApp 应用程序的名称。
- 3 在计算机选项卡上，选择计算机并单击**重试安装**以重新安装 ThinApp 应用程序。

ThinApp 应用程序未卸载

Horizon Administrator 无法卸载 ThinApp 应用程序。

问题

ThinApp 应用程序的安装状态显示为“卸载错误”。

原因

此问题的常见原因包括：

- Horizon Administrator 尝试卸载 ThinApp 应用程序时，ThinApp 应用程序正忙。
- 连接服务器主机与计算机之间失去网络连接。

您可以查看 Horizon Agent 和连接服务器日志文件，了解有关问题原因的更多信息。

对于 Windows XP 系统，Horizon Agent 日志文件位于计算机上的 `drive:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` 中；对于 Windows 7 系统，该文件位于 `drive:\ProgramData\VMware\VDM\logs` 中。

连接服务器日志文件位于连接服务器主机上的 `drive:\Documents and Settings\All Users\Application Data\VMware\VDM\logs` 目录中。

解决方案

- 1 在 Horizon Administrator 中，选择目录 > ThinApp。
- 2 单击 ThinApp 应用程序的名称。
- 3 单击计算机选项卡，选择计算机并单击**重新尝试卸载**以重试卸载操作。
- 4 如果卸载操作仍然失败，请手动从该计算机中移除 ThinApp 应用程序，然后单击**移除桌面的应用程序状态**。

该命令会在 Horizon Administrator 中清除 ThinApp 应用程序分配，但不会移除该计算机中的任何文件或设置。

重要 请仅在从计算机手动移除 ThinApp 应用程序后使用该命令。

MSI 包无效

Horizon Administrator 报告应用程序存储库中存在无效的 MSI 包。

问题

Horizon Administrator 在扫描操作中报告有一个 MSI 包无效。

原因

此问题的常见原因包括：

- MSI 文件已损坏。
- MSI 文件不是用 ThinApp 创建的。
- MSI 文件是用不受支持的 ThinApp 版本创建或重新打包的。必须使用 ThinApp 4.6 或更高版本。

解决方案

有关排除 MSI 包问题的信息，请参阅《ThinApp 用户指南》。

ThinApp 配置示例

从捕获和打包应用程序到检查安装状态，ThinApp 配置示例将引导您逐步设置典型的 ThinApp 配置。

前提条件

请参阅以下主题全面了解如何在该示例中执行这些步骤。

- [捕获和存储应用程序包](#)
- [将 ThinApp 应用程序分配到计算机和桌面池](#)

步骤

- 1 从 <http://www.vmware.com/products/thinapp> 下载 ThinApp 软件，并将其安装到干净的计算机上。

Horizon 7 支持 ThinApp 4.6 及更高版本。

- 2 使用 ThinApp 安装捕获向导捕获并以 MSI 格式打包应用程序。
- 3 在连接服务器主机和远程桌面均可访问的 Active Directory 域中的某个计算机上创建一个共享文件夹，并在共享文件夹上配置文件和共享权限，为内置 Active Directory 组“Domain Computers”授予读取访问权限。

如果您打算将 ThinApp 应用程序分配到域控制器，还必须为内置 Active Directory 组 "Domain Controllers" 授予读访问权限。

- 4 将 MSI 包复制到共享文件夹中。
- 5 在 Horizon Administrator 中将该共享文件夹注册为应用程序存储库。
- 6 在 Horizon Administrator 中，在应用程序存储库中扫描 MSI 包并将选定的 ThinApp 应用程序添加到 Horizon Administrator。
- 7 确定将 ThinApp 应用程序分配到计算机还是分配到桌面池。

如果您对计算机使用了通用命名约定，则可以根据计算机分配快速为使用该命名约定的所有计算机分发应用程序。如果您按部门或用户类型组织桌面池，则可以根据桌面池分配快速为特定部门或用户分发应用程序。

- 8 在 Horizon Administrator 中，选择要分配到计算机或桌面池的 ThinApp 应用程序并指定安装方法。

选项	操作
流式	在计算机上安装应用程序的快捷方式。该快捷方式指向托管存储库的网络共享位置上的应用程序。用户必须有权访问该网络共享位置才能运行该应用程序。
完整	在计算机的本地文件系统中安装完整的应用程序。

- 9 在 Horizon Administrator 中，检查 ThinApp 应用程序的安装状态。

设置 Kiosk 模式的客户端

您可以设置能够从 Horizon 7 访问其桌面的无人参与运行的客户端。

Kiosk 模式的客户端是一种运行 Horizon Client 来连接连接服务器实例和启动会话的瘦客户端或锁定 PC。最终用户通常无需登录便可访问客户端设备，但是对于某些应用程序，发布的桌面可能会要求用户提供身份验证信息。具有代表性的应用程序包括医疗数据条目工作站、航空公司登记站、客户自助服务点和公共访问信息终端。

您应当确保：桌面应用程序可通过身份验证机制保证交易安全、物理网络不会被篡改和偷窃，以及连接到网络的所有设备都是受信任的。

Kiosk 模式的客户端支持远程访问的标准功能，例如将 USB 设备自动重定向到远程会话以及基于位置的打印功能。

Horizon 7 使用 Horizon 7 4.5 及更高版本中的灵活身份验证功能对 Kiosk 模式的客户端设备（而非最终用户）进行身份验证。您可以配置连接服务器实例，对以自身 MAC 地址为标识或以字符 "custom-"（或在 ADAM 中定义的备用前缀字符串）开头的用户名为标识的客户端进行身份验证。如果您将客户端配置为使用自动生成的密码，则无需指定密码即可在设备上运行 Horizon Client。如果您配置显式密码，则必须将此密码指定给 Horizon Client。由于您通常会从脚本运行 Horizon Client，而密码将以明文显示，因此应采取预防措施使无特权用户无法读取脚本。

只有您用来对 Kiosk 模式客户端进行身份验证的连接服务器实例才能接受以字符 "cm-" 开头并后接 MAC 地址（或以字符 "Custom-" 开头或定义的备用字符串）的帐户发出的连接。Horizon 7 4.5 及更高版本中的 Horizon Client 不允许手动输入这些格式的用户名。

最佳做法是使用专用的连接服务器实例处理 Kiosk 模式的客户端，并在 Active Directory 中为这些客户端的帐户创建专用的组织单位和组。这样不仅能防止这些系统遭受意外入侵，还会使客户端的配置和管理变得更加容易。

配置 Kiosk 模式的客户端

要配置 Active Directory 和 Horizon 7 来支持 Kiosk 模式的客户端，您必须按顺序执行若干任务。

前提条件

确认您有执行配置任务所需的特权。

- 拥有 Active Directory 中的域管理员或帐户操作员凭据，以便对域中的用户和组的帐户进行更改。
- 拥有管理员、清单管理员或等效角色，以使用 Horizon Administrator 授权用户或组访问远程桌面。

- 拥有**管理员**或等效角色，以运行 **vdmadmin** 命令。

步骤

1 为 Kiosk 模式客户端准备 Active Directory 和 Horizon 7

您必须配置 **Active Directory** 来接受您所创建的用来对客户端设备进行身份验证的帐户。无论何时创建组，都必须将该组授权给客户端访问的桌面池。您还可以准备客户端使用的桌面池。

2 为 Kiosk 模式客户端设置默认值

您可以使用 **vdmadmin** 命令在 **Active Directory** 中为 Kiosk 模式客户端的组织单位、密码到期项和组成员设置默认值。

3 显示客户端设备的 MAC 地址

如果您要为客户端创建基于其 **MAC** 地址的帐户，可以使用 **Horizon Client** 找出该客户端设备的 **MAC** 地址。

4 为 Kiosk 模式客户端添加帐户

您可以使用 **vdmadmin** 命令将客户端的帐户添加到连接服务器组的配置中。添加的客户端可在启用了客户端身份验证的连接服务器实例中使用。您还可以更新客户端的配置，或者从系统中移除其帐户。

5 启用 Kiosk 模式客户端的身份验证

您可以使用 **vdmadmin** 命令对尝试通过连接服务器实例连接远程桌面的客户端进行身份验证。

6 验证 Kiosk 模式客户端的配置

您可以使用 **vdmadmin** 命令显示 Kiosk 模式客户端以及对这些客户端进行身份验证而配置的连接服务器实例的信息。

7 从 Kiosk 模式下的客户端连接到远程桌面

您可以从命令行运行客户端或使用脚本将客户端连接到远程会话。

为 Kiosk 模式客户端准备 Active Directory 和 Horizon 7

您必须配置 **Active Directory** 来接受您所创建的用来对客户端设备进行身份验证的帐户。无论何时创建组，都必须将该组授权给客户端访问的桌面池。您还可以准备客户端使用的桌面池。

作为最佳实践，请创建一个单独的组织单位和组，尽可能减少管理 Kiosk 模式客户端的工作。您可以为不属于任何组的客户端添加单独的帐户，但如果您配置大量客户端，就会带来大量的管理开销。

步骤

1 在 Active Directory 中，创建一个单独的组织单位和组以供 Kiosk 模式客户端使用。

您必须为该组指定一个 **Windows 2000** 版本之前的名称。您需要使用此名称在 **vdmadmin** 命令中标识该组。

2 为客户虚拟机创建映像或模板。

您可以将 **vCenter Server** 管理的虚拟机用作自动池的模板、链接克隆池的父虚拟机或者手动桌面池中的虚拟机。您还可以在客户机操作系统上安装和配置应用程序。

- 3 配置客户机操作系统，以便客户端在无人参与状态下运行时不被锁定。

Horizon 7 禁止为以 Kiosk 模式连接的客户端显示登录前的消息。如果需要一个能够解锁屏幕和显示消息的事件，可以在客户机操作系统上配置一个合适的应用程序。

- 4 在 Horizon Administrator 中，创建客户端将使用的桌面池并将组授权给该池。

例如，您可以选择创建一个最能满足客户端应用程序要求的浮动分配链接克隆桌面池。您还可将一个或多个 ThinApp 应用程序关联到桌面池。

重要 不要将一个客户端或一个组授权给多个桌面池。这会使 Horizon 7 从已授权客户端的池随机分配远程桌面，并生成一个警告事件。

- 5 如果您想为客户端启用基于位置的打印功能，可以配置 Active Directory 组策略设置 AutoConnect Location-based Printing for VMware View，该设置位于 Microsoft 组策略对象编辑器计算机配置下的 软件设置文件夹中。
- 6 配置优化和保护客户端的远程桌面所需的其他策略。

例如，您可能希望覆盖在启动或插入本地 USB 设备时将其连接到远程桌面的策略。默认情况下，适用于 Windows 的 Horizon Client 会对 Kiosk 模式客户端启用这些策略。

示例：为 Kiosk 模式客户端准备 Active Directory

公司内网中包含域 MYORG，且它的组织单位具有标识名 OU=myorg-ou,DC=myorg,DC=com。在 Active Directory 中，您需要创建拥有标识名 OU=kiosk-ou,DC=myorg,DC=com 的组织单位 kiosk-ou 以及组 kc-grp，以供 Kiosk 模式客户端使用。

后续步骤

为客户端设置默认值。

为 Kiosk 模式客户端设置默认值

您可以使用 vdmadmin 命令在 Active Directory 中为 Kiosk 模式客户端的组织单位、密码到期项和组成员设置默认值。

您必须在客户端用来连接其发布的桌面的连接服务器实例所在组中的一个连接服务器实例上运行 vdmadmin 命令。

当您为密码到期项和 Active Directory 组成员关系配置默认值时，这些设置会由组中所有的连接服务器实例共享。

步骤

- ◆ 为客户端设置默认值。

```
vdmadmin -Q -clientauth -setdefaults [-b authentication_arguments] [-ou DN] [ -expirepassword |
-noexpirepassword ] [-group group_name | -nogroup]
```

选项	说明
-expirepassword	指定客户端帐户密码的到期时间与连接服务器组的到期时间相同。如果没有为该组定义到期时间，则密码不会失效。
-group group_name	指定客户端帐户所加入的默认组的名称。组名必须指定为 Windows 2000 之前版本的 Active Directory 组名。
-noexpirepassword	将客户端帐户的密码指定为从不过期。
-nogroup	清除默认组的设置。
-ou DN	指定客户端帐户所加入的默认组织单位的标识名。 例如：OU=kiosk-ou,DC=myorg,DC=com
注 您无法使用该命令更改组织单位的配置。	

该命令可更新连接服务器组中客户端的默认值。

示例：为 Kiosk 模式客户端设置默认值

为客户端的组织单位、密码到期项和组成员设置默认值。

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

后续步骤

找出使用自身 MAC 地址进行身份验证的客户端设备的 MAC 地址。

显示客户端设备的 MAC 地址

如果您要为客户端创建基于其 MAC 地址的帐户，可以使用 Horizon Client 找出该客户端设备的 MAC 地址。

前提条件

登录客户端控制台。

步骤

- ◆ 要显示 MAC 地址，请根据您所用的平台键入相应的命令。

选项	操作
Windows	<p>输入</p> <pre>C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -printEnvironmentInfo</pre> <p>客户端将使用您为其配置的默认连接服务器实例。如果您尚未配置默认值，客户端将提示您配置该值。</p> <p>该命令可显示客户端设备的 IP 地址、MAC 地址和计算机名称。</p>
Linux	<p>输入 <code>vmware-view --printEnvironmentInfo -s connection_server</code></p> <p>您必须指定客户端连接桌面时要使用的连接服务器实例的 IP 地址或完全限定域名 (FQDN)。</p> <p>该命令可显示 IP 地址、MAC 地址、计算机名称、域、任何登录用户的名称和域，以及客户端设备的时区。</p>

后续步骤

为客户端添加帐户。

为 Kiosk 模式客户端添加帐户

您可以使用 `vdadmin` 命令将客户端的帐户添加到连接服务器组的配置中。添加的客户端可在启用了客户端身份验证的连接服务器实例中使用。您还可以更新客户端的配置，或者从系统中移除其帐户。

您必须在客户端用来连接其发布的桌面的连接服务器实例所在组中的一个连接服务器实例上运行 `vdadmin` 命令。

添加 Kiosk 模式客户端时，Horizon 7 会在 Active Directory 中为该客户端创建一个用户帐户。如果为客户端指定名称，则该名称必须以可识别的前缀字符串（如：“`custom-`”）或在 ADAM 中定义的备用前缀字符串开头，而且名称长度不得超过 20 个字符。如果您不为客户端指定名称，Horizon 7 将使用您为客户端设备指定的 MAC 地址生成名称。例如，如果 MAC 地址是 `00:10:db:ee:76:80`，则相应的帐户名称为 `cm-00_10_db_ee_76_80`。您只能将这些帐户用于允许对客户端进行身份验证的连接服务器实例。

重要 不要将一个指定的名称用于多个客户端设备。今后的版本可能不支持该配置。

步骤

- ◆ 使用 `-domain` 和 `-clientid` 选项运行 `vdadmin` 命令，指定客户端所在的域及其名称或 MAC 地址。

```
vdadmin -Q -clientauth -add [-b authentication_arguments] -domain domain_name -clientid client_id
[-password "password" | -genpassword] [-ou DN] [-expirepassword | -noexpirepassword] [-group
group_name | -nogroup] [-description "description_text"]
```

选项	说明
<code>-clientid client_id</code>	指定客户端的名称或 MAC 地址。
<code>-description "description_text"</code>	在 Active Directory 中为客户端设备创建帐户描述。
<code>-domain domain_name</code>	指定客户端的域。

选项	说明
-expirepassword	指定客户端帐户密码的到期时间与连接服务器组的到期时间相同。如果没有为该组定义到期时间，则密码永远不会到期。
-genpassword	为客户端帐户生成密码。如果您未指定 -password 或 -genpassword ，则会执行此默认行为。 生成的密码长度是 16 位，至少包含一个大写字母、一个小写字母、一个符号和一个数字，可以包含重复字符。如果您需要一个更强的密码，请使用 -password 选项指定密码。
-group group_name	指定要添加客户端帐户的组的名称。组名必须指定为 Windows 2000 之前版本的 Active Directory 组名。如果您之前设置了默认组，则客户端帐户会被添加到该组。
-noexpirepassword	将客户端帐户的密码指定为永不过期。
-nogroup	指定不将客户端帐户添加到默认组。
-ou DN	指定要添加客户端帐户的组织单位的标识名。 例如：OU=kiosk-ou,DC=myorg,DC=com
-password "password"	为客户端帐户指定显式密码。

该命令会在 Active Directory 中为指定的域和组（如果存在）中的客户端创建一个用户帐户。

示例：为客户端添加帐户

使用组 **kc-grp** 的默认设置，将由 MAC 地址指定的客户端帐户添加到 **MYORG** 域。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

使用自动生成的密码，将由 MAC 地址指定的客户端帐户添加到 **MYORG** 域。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword
```

为已命名的客户端添加帐户，并为该客户端指定一个密码。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

使用自动生成的密码为命名的客户端添加帐户。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Kiosk11 -genpassword -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Kiosk 11"
```

后续步骤

启用客户端身份验证。

启用 Kiosk 模式客户端的身份验证

您可以使用 **vdmadmin** 命令对尝试通过连接服务器实例连接远程桌面的客户端进行身份验证。

您必须在客户端用来连接其远程桌面的连接服务器实例所在组中的一个连接服务器实例上运行 **vdmadmin** 命令。

即便为单个连接服务器实例启用身份验证，组中所有的连接服务器实例仍会共享客户端身份验证的所有其他设置。您仅需为每个客户端添加一个帐户。在连接服务器组中，任何启用的连接服务器实例都可对该客户端进行身份验证。

如果您计划在 RDS 主机上配合使用 **kiosk** 模式和基于会话的桌面，还必须将用户帐户添加到远程桌面用户组。

步骤

- 1 在连接服务器实例上启用客户端身份验证。

```
vdmadmin -Q -enable [-b authentication_arguments] -s connection_server [-requirepassword]
```

选项	说明
-requirepassword	指定该选项即表示您需要客户端提供密码。 重要 如果您指定该选项，连接服务器实例将无法对具有自动生成密码的客户端进行身份验证。如果您更改连接服务器实例的配置来指定该选项，此类客户端将无法对自身进行身份验证，而且会返回错误消息未知用户名或无效密码 (Unknown username or bad password)。
-s connection_server	指定要启用客户端身份验证的连接服务器实例的 NetBIOS 名称。

该命令可使指定的连接服务器实例对客户端进行身份验证。

- 2 如果发布的桌面是由 Microsoft RDS 主机提供的，请登录到 RDS 主机，并将用户帐户添加到远程桌面用户组。

例如，在 Horizon 7 Server 上，向用户帐户 **custom-11** 授予在 RDS 主机上使用基于会话的桌面的权限。然后，必须登录该 RDS 主机，并通过转到**控制面板 > 系统和安全 > 系统 > 远程设置 > 选择用户 > 添加**将用户 **custom-11** 添加到远程桌面用户组。

示例：启用 Kiosk 模式客户端的身份验证

为连接服务器实例 **csvr-2** 启用客户端身份验证。具有自动生成的密码的客户端可以自身进行身份验证，而无需提供密码。

```
vdmadmin -Q -enable -s csvr-2
```

为连接服务器实例 **csvr-3** 启用客户端身份验证，并要求客户端将其密码指定给 Horizon Client。具有自动生成密码的客户端无法对自身进行身份验证。

```
vdmadmin -Q -enable -s csvr-3 -requirepassword
```

后续步骤

确认连接服务器实例和客户端的配置。

验证 Kiosk 模式客户端的配置

您可以使用 **vdmadmin** 命令显示 Kiosk 模式客户端以及为对这些客户端进行身份验证而配置的连接服务器实例的信息。

您必须在客户端用来连接其远程桌面的连接服务器实例所在组中的一个连接服务器实例上运行 **vdmadmin** 命令。

步骤

- ◆ 显示有关 **Kiosk** 模式客户端和客户端身份验证的信息。

```
vdmadmin -Q -clientauth -list [-b authentication_arguments] [--xml]
```

该命令可显示有关 **Kiosk** 模式客户端以及启用了客户端身份验证的连接服务器实例的信息。

示例：显示 **Kiosk** 模式客户端的信息

以文本格式显示有关客户端的信息。客户端 **cm-00_0c_29_0d_a3_e6** 具有自动生成的密码，而且不需要最终用户或应用程序脚本将该密码指定给 **Horizon Client**。客户端 **cm-00_22_19_12_6d_cf** 具有显式指定的密码并需要最终用户提供该密码。连接服务器实例 **CONSVR2** 接受具有自动生成密码的客户端发出的身份验证请求。**CONSVR1** 不接受来自 **Kiosk** 模式客户端的身份验证请求。

```
C:\ vdmadmin -Q -clientauth -list
Client Authentication User List
=====
GUID                : 94be6344-0c9b-4a92-8d54-1brc1c2dc282
ClientID            : cm-00_0c_29_0d_a3_e6
Domain              : myorg.com
Password Generated: true

GUID                : 471d9d35-68b2-40ee-b693-56a7d92b2e25
ClientID            : cm-00_22_19_12_6d_cf
Domain              : myorg.com
Password Generated: false

Client Authentication Connection Servers
=====
Common Name          : CONSVR1
Client Authentication Enabled : false
Password Required    : false

Common Name          : CONSVR2
Client Authentication Enabled : true
Password Required    : false
```

后续步骤

确认客户端可以连接到其远程桌面。

从 **Kiosk** 模式下的客户端连接到远程桌面

您可以从命令行运行客户端或使用脚本将客户端连接到远程会话。

您通常会使用命令脚本在部署的客户端设备上运行 Horizon Client。

注 在 Windows 或 Mac 客户端上，在远程桌面会话启动时，如果另一个应用程序或服务正在使用客户端上的 USB 设备，则不会默认自动转发这些设备。在所有客户端上，默认情况下不转发人机接口设备 (HID) 和智能卡读卡器。

步骤

- ◆ 要连接到远程会话，请在您的平台上键入相应的命令。

选项	说明
Windows	<p>输入</p> <pre>C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended [-serverURL <i>连接服务器</i>] [-userName <i>用户名</i>] [-password <i>密码</i>]</pre> <p>-password <i>密码</i> 为客户端帐户指定密码。如果您为该帐户定义了密码，则必须指定该密码。</p> <p>-serverURL <i>connection_server</i> 指定 Horizon Client 连接其远程桌面时使用的连接服务器实例的 IP 地址或 FQDN。如果您不指定客户端连接其远程桌面时使用的连接服务器实例的 IP 地址或 FQDN，客户端将使用您为其配置的默认连接服务器实例。</p> <p>-userName <i>user_name</i> 指定客户端帐户名称。如果您希望客户端使用以可识别的前缀字符串（如 "Custom-"）开头的帐户名（而非 MAC 地址）对自身进行身份验证，则必须指定该名称。</p>
Linux	<p>输入</p> <pre>vmware-view --unattended -s <i>连接服务器</i> [--once] [-u <i>用户名</i>] [-p <i>密码</i>]</pre> <p>--once 指定不需要 Horizon Client 在发生错误时重新尝试连接。</p> <p>重要 通常情况下，您应该指定该选项，并利用退出代码来处理错误。否则，您将在远程终止 vmware-view 进程时遇到困难。</p> <p>-p <i>密码</i> 为客户端帐户指定密码。如果您为该帐户定义了密码，则必须指定该密码。</p> <p>-s <i>connection_server</i> 指定客户端在连接其桌面时使用的连接服务器实例的 IP 地址或 FQDN。</p> <p>-u <i>user_name</i> 指定客户端帐户名称。如果您希望客户端使用以可识别的前缀字符串（如 "Custom-"）开头的帐户名（而非 MAC 地址）对自身进行身份验证，则必须指定该名称。</p>

如果服务器对 Kiosk 客户端进行了身份验证，并且有远程桌面可用，命令会启动远程会话。

示例：在 Kiosk 模式下的客户端上运行 Horizon Client

在帐户名基于自身 MAC 地址且使用自动生成密码的 Windows 客户端上运行 Horizon Client。

```
C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended -serverURL  
consrv2.myorg.com
```

在使用分配的名称和密码的 Linux 客户端上运行 Horizon Client。

```
vmware-view -unattended -s 145.124.24.100 --once -u custom-Terminal21 -p "Secret1!"
```

对 Horizon 7 进行故障排除

您可以采取多种操作来诊断和修复在使用 Horizon 7 的过程中可能遇到的问题。您可以使用 Horizon Help Desk Tool 进行故障排除，使用其他故障排除过程调查并更正问题，或者从 VMware 技术支持部门获取帮助。

有关桌面和桌面池故障排除的信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档。

本章讨论了以下主题：

- 使用 [Horizon Help Desk Tool](#)
- 使用 [VMware](#) 登录监视器
- 使用 [VMware Horizon](#) 性能跟踪器
- 监视系统运行状况
- 在 [Horizon 7](#) 中监视事件
- 收集 [Horizon 7](#) 的诊断信息
- 更新支持请求
- 排除安全服务器与 [Horizon](#) 连接服务器配对失败的故障
- 排除 [Horizon 7 Server](#) 证书撤销检查中的故障
- 排除智能卡证书撤销检查中的故障
- 更多故障排除信息

使用 Horizon Help Desk Tool

Horizon Help Desk Tool 是一个 Web 应用程序，可用于获取 Horizon 7 用户会话的状态以及执行故障排除和维护操作。

在 Horizon Help Desk Tool 中，您可以查找要对问题进行故障排除的用户会话，还可以执行桌面维护操作，如重新启动或重置桌面。

要配置 Horizon Help Desk Tool，必须满足以下要求：

- Horizon 7 的 Horizon Enterprise 版许可证或 Horizon Apps Advanced 版许可证。要确认您具有正确的许可证，请参阅[验证 Horizon Help Desk Tool 许可证](#)。

- 用来存储 Horizon 7 组件相关信息的事件数据库。有关配置事件数据库的更多信息，请参阅《Horizon 7 安装指南》文档。
- 用来登录到 Horizon Help Desk Tool 的“技术支持管理员”角色或“技术支持管理员 (只读)”角色。有关这些角色的更多信息，请参阅[为 Horizon Help Desk Tool 配置基于角色的访问](#)。
- 在每个连接服务器实例上启用时间安排分析器，以查看登录分段。

使用以下 `vdadmin` 命令可在每个连接服务器实例上启用时间安排分析器：

```
vdadmin -I -timingProfiler -enable
```

使用以下 `vdadmin` 命令可在使用管理端口的连接服务器实例上启用时间安排分析器：

```
vdadmin -I -timingProfiler -enable -server {ip/server}
```

验证 Horizon Help Desk Tool 许可证

如果您没有有效的产品许可证密钥，就无法登录到 Horizon Help Desk Tool。您可以在 Horizon Administrator 中验证产品许可证密钥，并应用有效的许可证。

前提条件

- 获取 Horizon Enterprise 版许可证或 Horizon Apps Advanced 版许可证的有效产品许可证密钥。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 产品许可和使用情况**。

将在许可面板中显示当前许可证密钥的第一个和最后五个字符。

- 2 验证技术支持许可证字段的许可证状态。

选项	说明
已禁用	产品许可证密钥无效。您无法登录到 Horizon Help Desk Tool。
已启用	产品许可证密钥有效。您可以登录到 Horizon Help Desk Tool。

- 3 （可选）如果产品许可证密钥无效，请单击**编辑许可证**并输入有效的许可证序列号，然后单击**确定**并刷新 Horizon Administrator URL。

产品许可窗口将显示更新的许可信息。

后续步骤

登录到 Horizon Help Desk Tool。

为 Horizon Help Desk Tool 配置基于角色的访问

您可以将预定义的管理员角色分配给 Horizon Help Desk Tool 管理员，使其在管理员用户之间委派故障排除任务。此外，您还可以基于预定义的管理员角色创建自定义角色并添加特权。

您可以将以下预定义的管理员角色分配给 Horizon Help Desk Tool 管理员：

- 技术支持管理员
- 技术支持管理员 (只读)

如果为 Horizon Help Desk Tool 管理员创建自定义角色，您必须先分配“管理技术支持门户 (只读)”特权，以及任何其他基于“技术支持管理员”角色或“技术支持管理员 (只读)”角色的特权。

前提条件

熟悉可用于创建自定义角色的管理员特权。请参阅[预定义的角色和特权](#)。

步骤

- 1 在 Horizon Administrator 中，选择 **View 配置 > 管理员**，然后单击**角色**选项卡。
- 2 在**角色**选项卡中，单击**添加角色**，选择“技术支持管理员”角色或“技术支持管理员 (只读)”角色，然后单击**确定**。
 - a (可选) 要添加自定义角色，请在**角色**选项卡中，单击**添加角色**，选择“管理技术支持门户 (只读)”特权，再选择基于“技术支持管理员”角色或“技术支持管理员 (只读)”角色的任何特权，然后单击**确定**。

登录到 Horizon Help Desk Tool

Horizon Help Desk Tool 已集成到 Horizon Console 中。从 Horizon 7 版本 7.5 开始，您无法再使用 Horizon Help Desk Tool URL 登录到 Horizon Help Desk Tool。

步骤

- 1 要从 Horizon Administrator 登录到 Horizon Help Desk Tool，请单击右上方面板中的 **Horizon Console**。这是到 Horizon Console Web 界面的单点登录。
- 2 在 Horizon Console 的“用户搜索”字段中输入用户名。
Horizon Console 会在搜索结果中显示用户的列表。搜索最多可返回 100 个匹配结果。
- 3 选择一个用户名。
用户卡中将会显示相应的用户信息。

后续步骤

要对问题进行故障排除，请单击用户卡中的相关选项卡。

在 Horizon Help Desk Tool 中对用户进行故障排除

在 Horizon Help Desk Tool 中，您可以在用户卡中查看基本用户信息。您可以单击用户卡中的选项卡以获取有关特定组件的更多详细信息。

用户详细信息有时会显示在表中。您可以按表列对这些用户详细信息进行排序。

- 要按升序对某列进行排序，请单击该列一次。
- 要按降序对某列进行排序，请单击该列两次。

- 要不对该列进行排序，请单击该列三次。

基本用户信息

显示基本用户信息，例如用户的用户名、电话号码和电子邮件地址，以及用户的状态（已连接或已断开连接）。如果用户具有桌面或应用程序会话，则用户的状态为已连接。如果用户没有任何桌面或应用程序会话，则用户的状态为已断开连接。

您可以单击电话号码打开 **Skype for Business** 会话，以致电用户来与其协作完成故障排除任务。

您还可以单击电子邮件向用户发送消息。

会话

会话选项卡显示有关用户连接到的桌面或应用程序会话的信息。

您可以使用**筛选器**文本框筛选桌面或应用程序会话。

注 对于使用 **Microsoft RDP** 显示协议的会话，或者从 **vSphere Client** 或 **ESXi** 访问虚拟机的会话，**会话**选项卡不显示相应的会话信息。

会话选项卡包含以下信息：

表 11-1. “会话”选项卡

选项	说明
状态	<p>显示有关桌面或应用程序会话状态的信息。</p> <ul style="list-style-type: none"> ■ 如果会话已连接，则显示绿色。 ■ 如果会话是本地会话或在本地容器中运行的会话，则显示 L。 ■ 如果会话在容器联合内的其他容器中运行，则显示 G。
计算机名称	<p>桌面或应用程序会话的名称。单击该名称可在一个信息卡中打开会话信息。</p> <p>您可以单击会话信息卡中的选项卡以查看其他信息：</p> <ul style="list-style-type: none"> ■ 详细信息选项卡显示虚拟机信息、CPU 或内存使用情况等用户信息。请参阅 Horizon Help Desk Tool 的会话详细信息。 ■ 进程选项卡显示有关 CPU 和内存相关进程的信息。请参阅 Horizon Help Desk Tool 的会话进程。 ■ 应用程序选项卡显示有关正在运行的应用程序的详细信息。请参阅 Horizon Help Desk Tool 的应用程序状态。
协议	桌面或应用程序会话的显示协议。
类型	显示桌面是已发布的桌面、虚拟机桌面，还是应用程序。
连接时间	会话连接到连接服务器的时间。
会话持续时间	会话保持连接到连接服务器的时长。

桌面授权

桌面授权选项卡显示有关用户有权使用的已发布桌面或虚拟桌面的信息。

表 11-2. 桌面授权

选项	说明
状态	显示有关桌面会话状态的信息。 ■ 如果会话已连接，则显示绿色。
桌面池名称	会话的桌面池的名称。
桌面类型	显示桌面是已发布的桌面，还是虚拟机桌面。 注 如果会话在容器联合内的其他容器中运行，则不会显示任何信息。
类型	显示有关桌面授权类型的信息。 ■ 对于本地授权，显示“本地”。 ■ 对于全局授权，显示“全局”。
vCenter	显示 vCenter Server 中虚拟机的名称。 注 如果会话在容器联合内的其他容器中运行，则不会显示任何信息。
默认协议	桌面或应用程序会话的默认显示协议。

应用程序授权

应用程序授权选项卡显示有关用户有权使用的已发布应用程序的信息。

表 11-3. 应用程序授权

选项	说明
状态	显示有关应用程序会话状态的信息。 ■ 如果会话已连接，则显示绿色。
应用程序	显示应用程序池中已发布应用程序的名称。
场	会话连接到的 RDS 主机所在的场名称。 注 对于全局应用程序授权，此列显示全局应用程序授权中的场数量。
类型	显示有关应用程序授权类型的信息。 ■ 对于本地授权，显示“本地”。 ■ 对于全局授权，显示“全局”。
发布者	已发布的应用程序的软件制造商名称。

活动

活动选项卡显示有关用户活动的事件日志信息。您可以按时间范围（如过去 12 小时或过去 30 天）或按管理员名称筛选活动。单击**仅技术支持事件**可仅按 Horizon Help Desk Tool 活动进行筛选。单击刷新图标可刷新事件日志。单击导出图标可将事件日志导出为文件。

注 在 CPA 环境中，不会显示用户的事件日志信息。

表 11-4. 活动

选项	说明
时间	选择时间范围。默认值为过去 12 小时。 <ul style="list-style-type: none"> 过去 12 小时 过去 24 小时 过去 7 天 过去 30 天 全部
管理员	管理员用户的名称。
消息	向用户或管理员显示特定于用户或管理员所执行活动的消息。
资源名称	显示有关执行活动时所在的桌面池或虚拟机名称的信息。

Horizon Help Desk Tool 的会话详细信息

单击会话选项卡的计算机名称选项中的用户名时，会话用户详细信息会显示在详细信息选项卡中。您可以查看 Horizon Client、虚拟或已发布桌面以及 CPU 和内存的详细信息。

Horizon Client

显示的信息取决于 Horizon Client 的类型，这些信息包括用户名、Horizon Client 的版本、客户端计算机的 IP 地址和客户端计算机的操作系统等详细信息。

注 如果升级了 Horizon Agent，您还必须将 Horizon Client 升级到最新版本。否则，不会显示 Horizon Client 的版本。有关升级 Horizon Client 的更多信息，请参阅《Horizon 7 升级指南》文档。

虚拟机

显示有关虚拟桌面或已发布桌面的信息。

表 11-5. 虚拟机详细信息

选项	说明
计算机名称	桌面或应用程序会话的名称。
代理版本	Horizon Agent 版本。
会话状态	桌面或应用程序会话的状态。
状态持续时间	会话保持处于同一状态的时间。
登录时间	用户登录到会话的时间。
登录时长	用户保持登录到会话的时间。
会话持续时间	会话保持连接到连接服务器的时间。
连接服务器	会话连接到的连接服务器。
Unified Access Gateway 名称	Unified Access Gateway 设备的名称。此信息在连接到会话之后可能需要 30 到 60 秒才能显示。
Unified Access Gateway IP	Unified Access Gateway 设备的 IP 地址。此信息在连接到会话之后可能需要 30 到 60 秒才能显示。

表 11-5. 虚拟机详细信息（续）

选项	说明
池	桌面或应用程序池的名称。
场	已发布的桌面或应用程序会话的 RDS 主机的场。
vCenter	vCenter Server 的 IP 地址。

显示 Blast 衡量指标

显示使用 VMware Blast 显示协议的虚拟或已发布桌面会话的性能详细信息。要查看这些性能详细信息，请单击显示 **BLAST** 衡量指标。

表 11-6. Blast 显示协议详细信息

选项	说明
BLAST 会话计数器	<ul style="list-style-type: none"> ■ 估计的带宽 (上行链路)。上行链路信号的估计带宽。 ■ 数据包丢失 (上行链路)。上行链路信号的数据包丢失百分比。
BLAST 图像处理计数器	<ul style="list-style-type: none"> ■ 发送的字节数。为进行 Blast 会话而发送的图像处理数据的总字节数。 ■ 接收的字节数。为进行 Blast 会话而接收的图像处理数据的总字节数。
BLAST 音频计数器	<ul style="list-style-type: none"> ■ 发送的字节数。为进行 Blast 会话而发送的音频数据的总字节数。 ■ 接收的字节数。为进行 Blast 会话而接收的音频数据的总字节数。
BLAST CDR 计数器	<ul style="list-style-type: none"> ■ 发送的字节数。为进行 Blast 会话而发送的客户端驱动器重定向数据的总字节数。 ■ 接收的字节数。为进行 Blast 会话而接收的客户端驱动器重定向数据的总字节数。

CPU、内存和延迟

显示虚拟或已发布桌面或应用程序的 CPU 和内存使用情况图表，以及 PCoIP 或 Blast 显示协议的延迟图表。

表 11-7. CPU、内存和延迟详细信息

选项	说明
会话 CPU	当前会话的 CPU 使用情况。
主机 CPU	向其分配会话的虚拟机的 CPU 使用情况。
会话内存	当前会话的内存使用情况。

表 11-7. CPU、内存和延迟详细信息（续）

选项	说明
主机内存	向其分配会话的虚拟机的内存使用情况。
会话延迟	<p>显示 PCoIP 或 Blast 显示协议的延迟图表。</p> <p>对于 Blast 显示协议，延迟时间为往返时间（以毫秒为单位）。用于跟踪此延迟时间的性能计数器是 VMware Blast 会话计数器 > RTT。</p> <p>对于 PCoIP 显示协议，延迟时间为往返延迟时间（以毫秒为单位）。用于跟踪此延迟时间的性能计数器是 PCoIP 会话网络统计信息 > 往返延迟。</p>

会话登录分段

显示登录时长以及在登录过程中创建的使用情况分段。

表 11-8. 会话登录分段

选项	说明
登录时长	该时长从用户单击桌面或应用程序池时开始计算，直到 Windows 资源管理器启动时为止。
会话登录时间	用户登录到会话的时间长度。
登录部分	<p>显示在登录过程中创建的分段。</p> <ul style="list-style-type: none"> ■ 代理。连接服务器处理会话连接或重新连接的总时间。从用户单击桌面池时开始计算，直到设置了安全加密链路连接时为止。包括完成各项连接服务器任务（例如用户身份验证、计算机选择和为设置安全加密链路连接准备计算机）所用的时间。 ■ GPO 加载。处理 Windows 组策略的总时间。如果未配置全局策略，则显示 0。 ■ 配置文件加载。处理 Windows 用户配置文件的总时间。 ■ 交互式。Horizon Agent 处理会话连接或重新连接的总时间。从 PCoIP 或 Blast Extreme 使用安全加密链路连接时开始计算，直到 Windows 资源管理器启动时为止。 ■ 身份验证。连接服务器对会话进行身份验证的总时间。 ■ 虚拟机启动。启动虚拟机所用的总时间。该时间包括引导操作系统、恢复挂起的计算机的时间，以及 Horizon Agent 发出信号表明它已做好连接准备的时间。

在使用登录分段中的信息进行故障排除时，以下准则适用：

- 如果会话是新的虚拟桌面会话，将显示所有登录分段。如果未配置全局策略，**GPO 加载**登录分段时间为 0。
- 如果虚拟桌面会话是断开连接后重新连接的会话，将显示**登录时长**、**交互式**和**代理**登录分段。
- 如果会话是已发布的桌面会话，将显示**登录时长**、**GPO 加载**或**配置文件加载**登录分段。新会话应显示**GPO 加载**和**配置文件加载**登录分段。如果新会话没有显示这些登录分段，则必须重新启动 RDS 主机。

Horizon Help Desk Tool 的会话进程

单击会话选项卡的计算机名称选项中的用户名时，会话进程会显示在进程选项卡中。

进程

对于每个会话，您可以查看有关 CPU 和内存相关进程的其他详细信息。例如，如果您发现会话的 CPU 和内存使用情况异常高，则可以在进程选项卡中查看该进程的详细信息。

表 11-9. 会话进程详细信息

选项	说明
进程名称	会话进程的名称。例如， chrome.exe 。
CPU	进程的 CPU 使用情况，以百分比为单位。
内存	进程的内存使用情况，以 KB 为单位。
磁盘	内存磁盘 IOPS。使用以下公式进行计算： (当前时间的 I/O 总字节数) - (当前时间前一秒的 I/O 总字节数)。 如果任务管理器显示正值，此计算可以显示值为 0 KB/秒。
用户名	进程所属的用户的用户名。
主机 CPU	向其分配会话的虚拟机的 CPU 使用情况。
主机内存	向其分配会话的虚拟机的内存使用情况。
进程	虚拟机中的进程计数。
刷新	刷新图标可刷新进程列表。
结束进程	结束正在运行的进程。 注 您必须具有技术支持管理员角色才能结束进程。 要结束进程，请选择相应的进程，然后单击 结束进程 按钮。

Horizon Help Desk Tool 的应用程序状态

在会话选项卡上的计算机名称选项中单击某个用户名时，可以在应用程序选项卡中查看应用程序的状态和详细信息。

应用程序

对于每个应用程序，可以查看当前状态以及其他详细信息。

表 11-10. 应用程序详细信息

选项	说明
应用程序	应用程序的名称。
说明	应用程序的描述。
状态	应用程序的状态。显示应用程序是否正在运行。
主机 CPU	向其分配会话的虚拟机的 CPU 使用情况。

表 11-10. 应用程序详细信息（续）

选项	说明
主机内存	向其分配会话的虚拟机的内存使用情况。
应用程序	正在运行的应用程序列表。
刷新	刷新图标可刷新应用程序列表。

在 Horizon Help Desk Tool 中对桌面或应用程序会话进行故障排除

在 Horizon Help Desk Tool 中，您可以根据用户的连接状态对桌面或应用程序会话进行故障排除。

前提条件

- 启动 Horizon Help Desk Tool。

步骤

- 1 在用户卡上，单击**会话**选项卡。

此时将出现一个性能卡，其中显示了 CPU 和内存使用情况，并包含有关 Horizon Client 以及虚拟桌面或已发布的桌面的信息。

- 2 选择一个故障排除选项。

选项	操作
发送消息	向已发布的桌面或虚拟桌面上的用户发送消息。您可以选择消息的严重性以包含“警告”、“信息”或“错误”。单击 发送消息 ，输入严重性类型和消息详细信息，然后单击 提交 。
远程协助	<p>您可以为已连接的桌面或应用程序会话生成远程协助票证。管理员可以使用该远程协助票证控制用户的桌面并对问题进行故障排除。</p> <p>单击远程协助并下载技术支持票证文件。打开票证，并等待远程桌面上的用户接受该票证。您只能在 Windows 桌面上打开票证。用户接受票证之后，您可以与用户聊天并请求控制用户的桌面。</p> <p>注 技术支持远程协助功能基于 Microsoft 远程协助。您必须在已发布的桌面上安装 Microsoft 远程协助并启用远程协助功能。如果 Microsoft 远程协助存在连接或升级问题，技术支持远程协助可能无法启动。有关更多信息，请参阅 Microsoft 网站上的 Microsoft 远程协助文档。</p>
重新启动	<p>在虚拟桌面上启动 Windows 重新启动过程。此功能不适用于已发布的桌面或应用程序会话。</p> <p>单击重新启动 VDI。</p>
断开连接	<p>断开桌面或应用程序会话连接。</p> <p>单击更多 > 断开连接。</p>

选项	操作
注销	对已发布的桌面或虚拟桌面启动注销过程，或对应用程序会话启动注销过程。 单击 更多 > 注销 。
重置	启动虚拟机重置操作。此功能不适用于已发布的桌面或应用程序会话。 单击 更多 > 重置虚拟机 。
注 用户可能会丢失未保存的工作。	

使用 VMware 登录监视器

VMware 登录监视器监视 Windows 用户登录，并报告性能指标以帮助管理员、支持人员和开发人员对登录速度缓慢进行故障排除。

衡量指标包括登录时间、登录脚本时间、CPU/内存使用情况以及网络连接速度。登录监视器还可以从其他 VMware 产品接收衡量指标，以提供有关登录过程的更多信息。

支持的平台

登录监视器支持与 Horizon Agent 相同的 Windows 平台。

主要功能

登录监视器提供以下功能：

- 默认作为 Horizon Agent 的一部分安装并启用。
- 与 Horizon Help Desk Tool 时间安排分析器集成在一起。汇总与登录相关的衡量指标并发送到 Horizon Agent 事件数据库。
- 允许客户将日志上传到文件服务器以便于访问。
- 与其他 VMware 产品（如 Horizon Persona Management、App Volumes、UEM 以及 Horizon Agent）集成在一起，以便将登录相关事件发送到登录监视器。登录监视器记录发生的事件，以显示登录流中的事件以及这些事件的持续时间。
- 监控同一计算机上的并发登录。

日志

登录监视器写入服务状态消息和用户会话的日志文件。默认情况下，所有日志文件将写入到 C:\ProgramData\VMware\VMware Logon Monitor\Logs 中。

- **主日志：**主日志文件 `vmlm.txt` 包含监控登录前后写入的 `vmlm` 服务和会话事件的所有状态消息。可以检查该日志以确定登录监视器是否正常运行。
- **会话日志：**会话日志包含与用户登录会话相关的所有事件。在登录开始时，将在该日志中开始写入事件并仅适用于单个用户会话。在日志末尾写入的摘要简要说明了最重要的衡量指标。可以检查该日志以解决登录缓慢问题。在登录完成后，不会再将其他事件写入到会话日志中。

登录监视器衡量指标

登录监视器计算与登录、组策略、用户配置文件和性能相关的衡量指标。这些衡量指标为管理员提供登录期间的最终用户系统的详细视图，以帮助确定出现性能瓶颈的根本原因。

表 11-11. 登录监视器衡量指标

衡量指标	参数	说明
登录时间	<ul style="list-style-type: none"> 开始 结束 总时间 	衡量指标包括在客户机上开始登录、完成登录、加载配置文件和显示桌面的时间以及在客户机上处理登录所花的总时间。不包括在客户机外部所花的任何时间。
会话开始到登录开始时间	总时间	从 Windows 创建用户会话一直到开始登录的时间。
配置文件同步时间	总时间	在登录期间， Windows 在协调用户配置文件时所花的时间。
Shell 加载	<ul style="list-style-type: none"> 开始 结束 总时间 	Windows 提供用户 Shell 加载的开始时间。结束时间是创建资源管理器窗口的时间。
登录到配置单元加载时间	总时间	衡量指标提供从开始登录到加载用户注册表配置单元的总时间。
Windows 文件夹重定向	<ul style="list-style-type: none"> 开始 结束 总时间 	与开始并完全应用 Windows 文件夹重定向的时间以及启用 Windows 文件夹重定向的总时间相关的衡量指标。首次应用文件夹重定向或将新文件上传到重定向的共享时，该时间可能较长。
组策略时间	<ul style="list-style-type: none"> 用户组策略应用时间 计算机组策略应用时间 	与将组策略应用于客户机相关的衡量指标包括应用用户组策略和计算机组策略所花的时间。
配置文件衡量指标	<ul style="list-style-type: none"> 配置文件类型：本地、漫游、临时 配置文件大小：文件数、文件夹数、总 MB 数 	<p>与用户配置文件相关的衡量指标指示用户配置文件类型，以及是将其存储在本地计算机上、中心配置文件存储上还是在注销后删除。</p> <p>配置文件大小包括文件数、总文件夹数以及总用户配置文件大小 (MB) 衡量指标。</p>
配置文件大小分配	<ul style="list-style-type: none"> 0 到 1 MB 之间的文件数 1 MB 到 10 MB 之间的文件数 10MB 到 100MB 之间的文件数 100MB 到 1GB 之间的文件数 1GB 到 10GB 之间的文件数 	用户配置文件中具有不同大小范围的文件数。
在登录期间启动的进程	<ul style="list-style-type: none"> 名称 进程 ID 父进程 ID 会话 ID 	将为从会话开始到登录完成之间启动的每个进程记录这些值。
组策略登录脚本时间	总时间	与执行组策略登录脚本相关的衡量指标报告在执行组策略登录脚本时所花的总时间。

表 11-11. 登录监视器衡量指标（续）

衡量指标	参数	说明
组策略 PowerShell 脚本时间	总时间	与执行组策略 PowerShell 脚本相关的衡量指标指示在执行组策略 PowerShell 脚本时所花的时间。
内存使用情况	<ul style="list-style-type: none"> ■ 可用字节数：最小值、最大值、平均值 ■ 提交的字节数：最小值、最大值、平均值 ■ 分页池：最小值、最大值、平均值 	与登录期间的内存使用情况相关的 WMI 衡量指标。将一直进行采样，直到登录完成。默认情况下禁用。
CPU 使用情况	<ul style="list-style-type: none"> ■ 空闲 CPU：最小值、最大值、平均值 ■ 用户 CPU：最小值、最大值、平均值 ■ 内核 CPU：最小值、最大值、平均值 	与登录期间的 CPU 使用情况相关的 WMI 衡量指标。将一直进行采样，直到登录完成。默认情况下禁用。
登录脚本是否同步？		报告是将组策略登录脚本与登录同步还是异步执行。
网络连接状态	<ul style="list-style-type: none"> ■ 已中断 ■ 已恢复 	报告网络连接是处于活动还是断开连接状态。
组策略软件安装	<ul style="list-style-type: none"> ■ 异步：是/否 ■ 错误代码 ■ 总时间 	与组策略软件安装相关的衡量指标指示安装与登录同步还是异步，安装是成功还是失败以及在使用组策略安装软件时所花的总时间。
配置文件卷的磁盘使用情况	<ul style="list-style-type: none"> ■ 用户的可用磁盘空间 ■ 可用磁盘空间 ■ 总磁盘空间 	与存储用户配置文件的卷上的磁盘使用情况相关的衡量指标。
域控制器发现	<ul style="list-style-type: none"> ■ 错误代码 ■ 总时间 	与域控制器相关的衡量指标。错误代码指示域控制器是否发生故障。
估计的网络带宽	带宽	从事件 ID 5327 收集的值。
网络连接详细信息	<ul style="list-style-type: none"> ■ 带宽 ■ 慢速链路阈值 ■ 检测到慢速链路：是/否 	从事件 ID 5314 收集的值。

表 11-11. 登录监视器衡量指标（续）

衡量指标	参数	说明
可能影响登录时间的设置	<ul style="list-style-type: none"> 计算机\管理模板\登录\计算机启动和登录时总是等待网络 计算机\管理模板\登录\在用户登录时运行这些程序 计算机\管理模板\用户配置文件\等待漫游用户配置文件 计算机\管理模板\用户配置文件\设置用户有漫游用户配置文件或远程主目录时的网络最长等待时间 计算机\管理模板\组策略\配置登录脚本延迟 用户\管理模板\系统\登录\在用户登录时运行这些程序 用户\管理模板\系统\用户配置文件\指定仅在登录/注销时同步的网络目录 	
来自 Horizon Agent、Persona Management、App Volumes 的衡量指标		与登录监视器交互的 VMware 产品在登录监视器日志中报告自定义衡量指标。这些衡量指标可以帮助确定其中的某个产品是否可能会对登录时间造成不利影响。

登录监视器配置设置

您可以使用 Windows 注册表值配置登录监视器设置。

注册表设置

要更改配置设置，请导航到 HKLM\Software\VMware, Inc.\VMware Logon Monitor 注册表项。

表 11-12. 登录监视器配置值

注册表项	类型	说明
RemoteLogPath	REG_SZ	<p>要将日志上传到的远程共享的路径。在将日志复制到远程日志共享时，这些日志将放置在 RemoteLogPath 注册表项指定的文件夹中。示例：\\server\share\%username%.%userdomain%。登录监视器将根据需要创建文件夹。默认情况下禁用。</p> <ul style="list-style-type: none"> 远程日志文件夹的 UNC 路径 可选；如果未配置，则不上传日志。 支持可选的本地环境变量。
Flags	REG_DWORD	<p>该值是一个位掩码，它影响登录监视器的行为。</p> <ul style="list-style-type: none"> 要启用或禁用 CPU 和内存衡量指标而设置或移除的值为 0x4。默认情况下禁用。 要启用进程事件和登录脚本衡量指标而设置或移除的值为 0x8。默认情况下禁用。 要启用或禁用与 Horizon 7 的集成而设置的值为 0x2。默认情况下启用。 要禁用崩溃转储而设置的值为 0x1。转储将写入到 C:\ProgramData\VMware\VMware Logon Monitor\Data 中。默认情况下禁用。 要在远程路径中为每个用户创建文件夹而设置的值为 0x10。默认情况下禁用。

表 11-12. 登录监视器配置值（续）

注册表项	类型	说明
LogMaxSizeMB	REG_DWORD	主日志的最大大小 (MB)。默认为 100 MB。
LogKeepDays	REG_DWORD	在滚动之前保留主日志的最大天数。默认为 7 天。

时间安排分析器设置

登录监视器与 Horizon 技术支持时间安排分析器集成在一起。默认情况下，时间安排分析器处于关闭状态。

- 要允许登录监视器使用时间安排分析器将事件写入到事件数据库中，请运行 `vdmadmin -I -timingProfiler -enable`。
- 要禁止登录监视器使用时间安排分析器，请运行 `vdmadmin -I -timingProfiler -disable`。

使用 VMware Horizon 性能跟踪器

VMware Horizon 性能跟踪器是一个实用程序，它在远程桌面中运行，并监视显示协议性能和系统资源使用情况。您还可以创建一个应用程序池，并将 Horizon 性能跟踪器作为发布的应用程序运行。

配置 VMware Horizon 性能跟踪器

您可以在远程桌面中运行 Horizon 性能跟踪器。您还可以将 Horizon 性能跟踪器作为发布的应用程序运行。

Horizon 性能跟踪器功能

Horizon 性能跟踪器显示以下功能的重要数据：

表 11-13. Horizon 性能跟踪器功能

性能监控	详细信息
协议特定的数据	<ul style="list-style-type: none"> ■ 编码器名称：在显示协议中使用的编码器的名称 ■ 使用的带宽：在显示协议（PCoIP 或 Blast）的采样周期内的平均传入和传出带宽的总带宽 ■ 每秒帧速率：在 1 秒采样周期内编码的图像处理帧数 ■ 音频打开：是否打开了音频功能 ■ 音频已启动：是否启动了音频功能 ■ CPU 使用情况： <ul style="list-style-type: none"> ■ 编码器 CPU：当前用户会话中的显示协议编码器的 CPU 使用情况 ■ 系统 CPU：系统的总 CPU 使用量
传输类型	<ul style="list-style-type: none"> ■ 客户端到远程会话：从客户端传输到远程对等方时使用的 UDP 或 TCP 协议传输包 ■ 远程会话到客户端：从远程对等方传输到客户端时使用的 UDP 或 TCP 协议传输包 ■ Horizon Connection Server：用于连接到连接服务器实例的 UDP 或 TCP 协议传输包

表 11-13. Horizon 性能跟踪器功能（续）

性能监控	详细信息
系统运行状况	<ul style="list-style-type: none"> ■ 估计的带宽：Horizon Client 和 Horizon Agent 之间的总估计可用带宽 ■ 往返时间：Horizon Agent 和 Horizon Client 之间的往返延迟（毫秒）
会话上下文	<ul style="list-style-type: none"> ■ 服务器详细信息，例如，DNS 名称、域名、是否建立加密链路、URL、远程 IP 地址 ■ 客户端计算机详细信息，例如，显示器编号、IP 地址、键盘和鼠标布局、语言、时区
实时协议切换	

注 只有在虚拟桌面会话中运行 Horizon Agent 时，Horizon 性能跟踪器才会收集并显示数据。

Horizon 性能跟踪器的系统要求

Horizon 性能跟踪器支持以下配置。

表 11-14. Horizon 性能跟踪器系统要求

系统	要求
虚拟桌面操作系统	所有支持 Horizon Agent 的操作系统
客户端计算机操作系统	支持所有 Horizon Client 版本，但在作为发布的应用程序时不支持适用于 Linux 的 Horizon Client 和适用于 Windows 10 UWP 的 Horizon Client。
显示协议	VMware Blast 和 PCoIP

安装 Horizon 性能跟踪器

Horizon 性能跟踪器是 Horizon Agent 安装程序中的自定义安装选项。您必须选择该选项，因为不会默认选择该选项。Horizon 性能跟踪器适用于 IPv4 和 IPv6。

您可以将 Horizon 性能跟踪器安装在虚拟桌面或 RDS 主机上。如果将其安装在 RDS 主机上，您可以将其发布为发布的应用程序，并从 Horizon Client 中运行该发布的应用程序。请参阅《在 Horizon 7 中设置已发布的桌面和应用程序》文档。

安装将在桌面上创建一个快捷方式。

配置 Horizon 性能跟踪器组策略设置

您可以配置用于更改默认设置的组策略设置。请参阅[配置 Horizon 性能跟踪器组策略设置](#)。

配置 Horizon 性能跟踪器组策略设置

要配置 Horizon 性能跟踪器，请在代理计算机上安装 Horizon 性能跟踪器 ADMX 模板文件 (perf_tracker.admx)，然后使用本地组策略编辑器配置策略设置。

为 Horizon 7 提供组策略设置的所有 ADMX 文件包含在 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 中，其中 x.x.x 是版本，yyyyyyy 是内部版本号。您可以从 VMware 下载站点中下载该文件，网址为 <https://my.vmware.com/web/vmware/downloads>。在“桌面和最终用户计算”下，选择 VMware Horizon 7 下载，其中包含 ZIP 文件。

步骤

- 1 从 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 文件中提取 perf_tracker.admx 文件，并将该文件复制到代理计算机上的 %systemroot%\PolicyDefinitions 文件夹中。
- 2 从 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 文件中提取 perf_tracker.adml 文件，并将该文件复制到代理计算机上 %systemroot%\PolicyDefinitions\ 文件夹的相应语言子文件夹中。
例如，将 perf_tracker.adml 文件的 en_us 版本复制到 %systemroot%\PolicyDefinitions\en_us 子文件夹中。
- 3 启动本地组策略编辑器 (gpedit.msc)，然后导航到 **计算机配置 > 管理模板 > VMware Horizon 性能跟踪器**。
- 4 编辑组策略设置。

设置	说明
Horizon 性能跟踪器基本设置	如果启用，您可以设置 Horizon 性能跟踪器收集数据的频率（秒）。
在远程桌面连接中启用 Horizon 性能跟踪器自动启动。	如果启用，在用户登录到远程桌面连接时，将自动启动 Horizon 性能跟踪器。要清除该首选项 GPO 设置，请选择 禁用 。
在远程应用程序连接中启用 Horizon 性能跟踪器自动启动	如果启用，在用户登录到远程应用程序连接时，将自动启动 Horizon 性能跟踪器。要清除该首选项 GPO 设置，请选择 禁用 。

- 5 要使更改生效，请在代理计算机上重新启动 Horizon 性能跟踪器。

运行 Horizon 性能跟踪器

您可以使用 Horizon Client 在远程桌面中运行 Horizon 性能跟踪器，或者将其作为发布的应用程序运行。

如果使用的 Horizon Client 平台支持多个会话，您可以从不同的场中运行多个发布的 Horizon 性能跟踪器应用程序。在 Windows 和 Mac 客户端（支持多个会话）上，概述窗口中的计算机名称标识发布的应用程序来自的场。在 Android 和 iOS 客户端以及 HTML Access 中，每次仅支持一个打开的会话。如果从另一个场中打开第二个会话，则会关闭第一个会话。

前提条件

- 安装并配置 Horizon 性能跟踪器。请参阅[配置 VMware Horizon 性能跟踪器](#)。
- 配置 Horizon 性能跟踪器组策略设置。请参阅[配置 Horizon 性能跟踪器组策略设置](#)。

步骤

- 要在远程桌面中运行 Horizon 性能跟踪器，请使用 Horizon Client 或 HTML Access 连接到服务器并启动远程桌面。

如果在打开远程桌面时未自动启动 Horizon 性能跟踪器，您可以双击 Windows 桌面上的 **VMware Horizon 性能跟踪器** 快捷方式，或者使用与启动任何 Windows 应用程序相同的方式启动 Horizon 性能跟踪器。

要选择显示概述窗口或浮动栏以及退出应用程序的选项，请右键单击远程桌面上的系统托盘中的 VMware Horizon 性能跟踪器图标。

- 要将 Horizon 性能跟踪器作为发布的应用程序运行，请使用 Horizon Client 或 HTML Access 连接到服务器并启动发布的 Horizon 性能跟踪器应用程序。

使用发布的 Horizon 性能跟踪器应用程序的方式取决于使用的客户端类型。您无法使用适用于 Linux 的 Horizon Client 或适用于 Windows 10 UWP 的 Horizon Client 将 Horizon 性能跟踪器作为发布的应用程序运行。

- 在使用适用于 Windows 的 Horizon Client 时，将在 Windows 客户端系统上的系统托盘中显示 VMware Horizon 性能跟踪器图标。您可以双击该图标以在 Windows 客户端上打开 Horizon 性能跟踪器。您可以右键单击该图标以选择显示概述窗口或浮动栏以及退出应用程序的选项。
- 在使用适用于 Mac 的 Horizon Client 时，将在 Mac 客户端系统上的菜单栏中显示 VMware Horizon 性能跟踪器图标。您可以双击该图标以在 Mac 客户端上打开 Horizon 性能跟踪器。您还可以右键单击该图标以选择可显示概述窗口或浮动栏以及退出应用程序的选项。
- 在使用适用于 Android 的 Horizon Client 或适用于 iOS 的 Horizon Client 时，将在 Horizon Client 上的 Unity Touch 边栏中显示 VMware Horizon 性能跟踪器图标。您可以触摸并按住该图标，然后选择可显示概述窗口和浮动栏以及退出应用程序的选项。
- 在使用 HTML Access 时，将在 HTML Access 边栏中显示 VMware Horizon 性能跟踪器图标。您可以右键单击该图标，然后选择可显示概述窗口或浮动栏以及退出应用程序的选项。

后续步骤

有关 Horizon 性能跟踪器显示的数据的信息，请参阅[配置 VMware Horizon 性能跟踪器](#)。

监视系统运行状况

您可以使用 Horizon Administrator 中的系统运行状况仪表板来快速查看可能影响 Horizon 7 运行或最终用户远程桌面访问的问题。

位于 Horizon Administrator 屏幕左上角的系统运行状况仪表板提供了一些链接，您可以通过这些链接查看 Horizon 7 的运行报告：

会话	提供指向“会话”屏幕的链接，该屏幕会显示有关远程桌面和应用程序会话状态的信息。
问题 vCenter 虚拟机	提供指向“计算机”屏幕的链接，该屏幕显示有关 vCenter 虚拟机、RDS 主机、Horizon 7 标记为有问题的其他计算机的信息。

问题 RDS 主机	提供指向“计算机”屏幕上 RDS 主机 选项卡的链接，该屏幕显示有关 Horizon 7 已标记为有问题的 RDS 主机的信息。
事件	提供指向已过滤出错误事件和警告事件的“事件”屏幕的链接。
系统运行状况	提供指向“仪表板”屏幕的链接，该屏幕会显示 Horizon 7 组件、vSphere 组件、域和桌面的状态摘要，以及已注册 Unified Access Gateway 的详细信息（版本 3.4 或更高版本）和数据存储的使用情况。

系统运行状况仪表板将针对每个项目显示一个标有数字的链接。该值表示所链接的报告提供了多少个项目的详细信息。

在 Horizon 7 中监视事件

事件数据库存储了连接服务器主机或组、Horizon Agent 以及 Horizon Administrator 中所发生事件的相关信息，并在仪表板中显示事件数量。您可以在“事件”屏幕上查看事件的详细信息。

注 事件会在 Horizon Administrator 界面中持续显示一段有限的时间。在此之后，事件仅在历史数据库表中可见。您可使用 Microsoft SQL Server 或 Oracle 数据库报告工具检查数据库表中的事件。有关更多信息，请参阅《Horizon 7 集成指南》文档。

注 如果事件数据库变得不可用，Horizon 7 将保留在此不可用期间发生的事件的审计记录，待事件数据库变得可用后，再将这些记录保存到事件数据库。您必须重新启动事件数据库和连接服务器，才能在 Horizon Administrator 界面中查看这些事件。

除了监视 Horizon Administrator 中的事件外，还可以生成 Syslog 格式的 Horizon 7 事件，以便分析软件可以访问事件数据。请参阅[使用 -l 选项以 Syslog 格式生成 Horizon 7 事件日志消息](#)以及《Horizon 7 安装指南》文档中的“配置 Syslog 服务器的事件日志记录”。

前提条件

按照《Horizon 7 安装指南》文档中所述，创建并配置事件数据库。

步骤

- 1 在 Horizon Administrator 中，选择**监视 > 事件**。
- 2 （可选）在“事件”窗口中，您可以选择事件的时间范围，对事件应用过滤器，并在一个或多个栏中对列出的事件进行排序。

Horizon 7 事件消息

每当系统状态变化或者遇到问题时，Horizon 7 均会报告发生的事件。您可以根据事件消息中的信息来采取适当措施。

下表显示了 Horizon 7 报告的事件类型。

表 11-15. Horizon 7 所报告事件的类型

事件类型	说明
Audit Failure（审核失败）或 Audit Success（审核成功）	报告管理员或用户对 Horizon 7 的操作或配置所做的更改是否成功。
错误	报告 Horizon 7 所执行的错误操作。
信息	报告 Horizon 7 内的正常操作。
警告	报告在操作或配置设置中，今后有可能导致更严重问题的轻微问题。

如果您看到与“审核失败”、“错误”或“警告”事件相关的消息，则可能需要采取相应的措施。对于“审核成功”或“信息”事件，则不需要采取措施。

收集 Horizon 7 的诊断信息

您可以收集诊断信息以协助 VMware 技术支持部门诊断并解决 Horizon 7 存在的问题。

您可以收集 Horizon 7 中各个组件的诊断信息。此信息的具体收集方式取决于 Horizon 7 组件。

■ 为 Horizon Agent 创建数据收集工具捆绑包

为协助 VMware 技术支持部门对 Horizon Agent 进行故障排除，您可能需要使用 `vdmadmin` 命令来创建数据收集工具 (Data Collection Tool, DCT) 捆绑包。您也可手动获取 DCT 捆绑包，而无需使用 `vdmadmin`。

■ 保存 Horizon Client 的诊断信息

如果您在使用 Horizon Client 时遇到问题，并且采用常规的网络故障排除方法不能解决这些问题，可以保存一份日志文件和配置相关信息的副本。

■ 使用支持脚本收集 View Composer 的诊断信息

您可以使用 View Composer 支持脚本来收集 View Composer 的配置数据，并生成日志文件。这些信息有助于 VMware 客户支持部门诊断 View Composer 出现的问题。

■ 收集 Horizon 连接服务器的诊断信息

您可以使用支持工具设置 Horizon 连接服务器的日志级别并生成日志文件。

■ 从控制台收集 Horizon Agent、Horizon Client 或 Horizon 连接服务器的诊断信息

如果您能够直接访问控制台，可以使用支持脚本为连接服务器、Horizon Client 或运行 Horizon Agent 的远程桌面生成日志文件。这些信息有助于 VMware 技术支持部门诊断这些组件出现的问题。

为 Horizon Agent 创建数据收集工具捆绑包

为协助 VMware 技术支持部门对 Horizon Agent 进行故障排除，您可能需要使用 `vdmadmin` 命令来创建数据收集工具 (Data Collection Tool, DCT) 捆绑包。您也可手动获取 DCT 捆绑包，而无需使用 `vdmadmin`。

为方便起见，您可以在连接服务器实例上使用 `vdmadmin` 命令从远程桌面请求 DCT 捆绑包。捆绑包将返回到连接服务器。

或者您可以登录到特定的远程桌面，运行 `support` 命令，在此桌面上创建 DCT 捆绑包。如果启用了用户帐户控制 (User Account Control, UAC)，则必须按这种方式获取 DCT 捆绑包。

步骤

- 1 作为一个拥有所需特权的用户登录。

选项	操作
在 View 连接服务器中，使用 vdmadmin	以角色为 管理员 的用户身份登录连接服务器的标准或副本实例。
在远程桌面中	以拥有管理特权的用户身份登录远程桌面。

- 2 打开命令提示符，运行命令生成 DCT 捆绑包。

选项	操作
在 View 连接服务器中，使用 vdmadmin	要指定输出捆绑包文件、桌面池和计算机的名称，请使用 vdmadmin 命令并附带 <code>-outfile</code> 、 <code>-d</code> 和 <code>-m</code> 选项。 <pre>vdmadmin -A [-b authentication_arguments] -getDCT -outfile local_file -d desktop -m machine</pre>
在远程桌面中	将目录更改为 <code>c:\Program Files\VMware\VMware View\Agent\DCT</code> 并运行以下命令： <pre>support</pre>

此命令可将捆绑包写入指定的输出文件中。

示例：使用 vdmadmin 为 Horizon Agent 创建捆绑包文件

为桌面池 `dtpool2` 中的虚拟机 `machine1` 创建 DCT 捆绑包，并将其写入 zip 文件 `C:\myfile.zip` 中。

```
vdmadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\myfile.zip
```

后续步骤

如果您当前存在支持请求，可以通过附加 DCT 捆绑包文件来更新请求。

保存 Horizon Client 的诊断信息

如果您在使用 Horizon Client 时遇到问题，并且采用常规的网络故障排除方法不能解决这些问题，可以保存一份日志文件和配置相关信息的副本。

在保存诊断信息并联系 VMware 技术支持部门之前，您可以先尝试解决 Horizon Client 的连接问题。有关详细信息，请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“Horizon Client 和 Horizon 连接服务器之间的连接问题”。

步骤

- 1 在 Horizon Client 中，单击**支持信息**或者在远程桌面菜单上选择**选项 > 支持信息**。
- 2 在**支持信息**窗口中单击**收集支持数据**，在系统提示时单击**是**。

将出现一个命令窗口，其中显示了收集信息的进度。此过程可能需要几分钟时间。

- 3 在命令窗口中，按照提示输入要用来测试 Horizon Client 配置的 Horizon 连接服务器实例的 URL，并根据需要选择生成 Horizon 7 进程的诊断转储。

这些信息将写入客户机桌面文件夹下的 zip 文件中。

- 4 在 VMware 网站的支持页面中提交支持请求，并附加输出 zip 文件。

使用支持脚本收集 View Composer 的诊断信息

您可以使用 View Composer 支持脚本来收集 View Composer 的配置数据，并生成日志文件。这些信息有助于 VMware 客户支持部门诊断 View Composer 出现的问题。

前提条件

登录到安装有 View Composer 的计算机。

由于您必须使用 Windows 脚本宿主实用程序 (cscript) 运行支持脚本，因此需要熟悉 cscript 的使用方法。请参阅 <http://technet.microsoft.com/library/bb490887.aspx>。

步骤

- 1 打开命令提示符窗口，然后转到 C:\Program Files\VMware\VMware View Composer 目录。

如果您未将软件安装在默认目录中，请替换相应的驱动器盘符和路径。

- 2 键入命令以运行 svi-support 脚本。

```
cscript ".\svi-support.wsf" /zip
```

您可以使用 /? 选项显示脚本可用的其他命令选项的相关信息。

运行脚本后，系统将向您显示输出文件的名称和位置。

- 3 在 VMware 网站的支持页面中提交支持请求，并附加输出文件。

收集 Horizon 连接服务器的诊断信息

您可以使用支持工具设置 Horizon 连接服务器的日志级别并生成日志文件。

支持工具可用来收集连接服务器的日志数据。这些信息有助于 VMware 技术支持部门诊断连接服务器出现的问题。支持工具不可用于收集 Horizon Client 或 Horizon Agent 的诊断信息。您必须改为使用支持脚本。请参阅[从控制台收集 Horizon Agent、Horizon Client 或 Horizon 连接服务器的诊断信息](#)。

前提条件

以角色为**管理员**的用户身份登录连接服务器的标准或副本实例。

步骤

- 1 选择开始 > 所有程序 > VMware > 设置 View 连接服务器日志级别。

- 2 在**选项**文本框中键入一个数值以设置日志级别，然后按 **Enter** 键。

选项	说明
0	将日志级别重置为默认值。
1	选择常规日志级别。
2	选择调试日志级别（默认）。
3	选择完整日志级别。

系统将按您选择的详细信息级别开始记录日志信息。

- 3 如果您收集了与连接服务器的行为有关的充足信息，请选择**开始 > 所有程序 > VMware > 生成 View 连接服务器日志包**。

支持工具可将日志文件写入连接服务器实例桌面上名为 **vdm-sdct** 的文件夹中。

- 4 在 **VMware** 网站的支持页面中提交支持请求，并附加输出文件。

从控制台收集 Horizon Agent、Horizon Client 或 Horizon 连接服务器的诊断信息

如果您能够直接访问控制台，可以使用支持脚本为连接服务器、Horizon Client 或运行 Horizon Agent 的远程桌面生成日志文件。这些信息有助于 **VMware** 技术支持部门诊断这些组件出现的问题。

前提条件

登录到您希望收集信息的系统。您必须以具有管理员特权的用户身份登录。

- 对于 **Horizon Agent**，请登录到安装了 **Horizon Agent** 的虚拟机。
- 对于 **Horizon Client**，请登录安装有 **Horizon Client** 的系统。
- 对于连接服务器，请登录连接服务器主机。

步骤

- 1 打开一个命令提示符窗口，转到相应目录，找到您希望收集诊断信息的 **Horizon 7** 组件。

选项	说明
Horizon Agent	转到 C:\Program Files\VMware View\Agent\DCT 目录。
Horizon Client	转到 C:\Program Files\VMware View\Client\DCT 目录。
View 连接服务器	转到 C:\Program Files\VMware View\Server\DCT 目录。

如果您未将软件安装在默认目录中，请替换相应的驱动器盘符和路径。

2 键入命令运行支持脚本。

```
.\support.bat [loglevels]
```

如果您希望启用高级日志记录功能，请指定 **loglevels** 选项并在系统提示时输入日志级别对应的数值。

选项	说明
0	将日志级别重置为默认值。
1	选择常规日志级别。
2	选择调试日志级别（默认）。
3	选择完整日志级别。
4	选择 PCoIP 的信息日志级别（仅适用于 Horizon Agent 和 Horizon Client）。
5	选择 PCoIP 的调试日志级别（仅适用于 Horizon Agent 和 Horizon Client）。
6	选择虚拟通道的信息日志级别（仅适用于 Horizon Agent 和 Horizon Client）。
7	选择虚拟通道的调试日志级别（仅适用于 Horizon Agent 和 Horizon Client）。
8	选择虚拟通道的跟踪日志级别（仅适用于 Horizon Agent 和 Horizon Client）。

脚本会将压缩后的日志文件写入桌面上的 **vdm-sdct** 文件夹。

- 您可以在 **C:\Program Files\Common Files\VMware\View Composer Guest Agent svi-ga-support** 目录下找到 View Composer 客户代理日志。
- 在 VMware 网站的支持页面中提交支持请求，并附加输出文件。

更新支持请求

您可以在支持网站更新现有支持请求。

提交支持请求后，您可能会收到 VMware 技术支持部门发出的电子邮件请求，要求您提供 **support** 或 **svi-support** 脚本的输出文件。运行脚本后，您将看到输出文件的名称和位置。您需要回复电子邮件，并在回复中附加脚本输出文件。

如果输出文件过大（大于或等于 10 MB），请联系 VMware 技术支持部门，告之支持请求编号，请求提供 FTP 上传说明。或者，您也可以在支持网站将输出文件附加到现有支持请求中。

步骤

- 访问并登录 VMware 网站的支持页面。
- 单击**支持请求历史记录**，查找适当的支持请求编号。
- 更新支持请求，并附加通过运行 **support** 或 **svi-support** 脚本获得的输出文件。

排除安全服务器与 Horizon 连接服务器配对失败的故障

安全服务器如果未能与连接服务器实例成功配对，可能会无法工作。

问题

如果安全服务器与连接服务器配对失败，安全服务器可能会出现以下问题：

- 当您尝试再次安装安全服务器时，安全服务器无法连接到连接服务器。
- Horizon Client 无法连接到 Horizon 7。系统显示以下错误消息：**View 连接服务器身份验证失败。没有可用的网关能够提供与桌面的安全连接。请与网络管理员联系 (The View Connection Server authentication failed. No gateway is available to provide a secure connection to a desktop. Contact your network administrator)。**
- 安全服务器在 Horizon Administrator 仪表板中显示为停机 (Down)。

原因

当您开始安装安全服务器时，如果在输入安全服务器配对密码后取消或以其他方式中止了尝试，可能会发生此问题。

解决方案

如果您想要在 Horizon 7 环境中保留安全服务器，请执行以下步骤：

- 1 在 Horizon Administrator 中，选择 **View 配置 > 服务器**。
- 2 在**安全服务器**选项卡上，选择一个安全服务器，从**更多命令**下拉菜单中选择**准备升级或重新安装**，然后单击**确定**。
- 3 在**连接服务器**选项卡上，选择要与安全服务器配对的连接服务器实例，从**更多命令**下拉菜单中选择**指定安全服务器配对密码**，然后键入密码并单击**确定**。
- 4 再次安装安全服务器。

如果您想要从 Horizon 7 环境中移除安全服务器条目，请运行 `vdadmin -S` 命令。

例如：`vdadmin -S -r -s security_server_name`

排除 Horizon 7 Server 证书撤销检查中的故障

如果服务器的 TLS 证书不能执行证书撤销检查，则用于 Horizon Client 安全连接的安全服务器或连接服务器实例将在 View Administrator 中显示红色。

问题

安全服务器或连接服务器图标在 Horizon Administrator 仪表板上显示为红色。Horizon 7 服务器的状态显示以下消息：无法选中服务器证书 (Server's certificate cannot be checked)。

原因

如果您的组织使用代理服务器进行 Internet 访问，或如果连接服务器实例由于防火墙或其他控制的原因无法访问提供撤销检查的服务器，则证书撤销检查可能会失败。

连接服务器实例对自身的证书以及与其配对的安全服务器的证书执行证书撤销检查。默认情况下，VMware Horizon View 连接服务器服务以 LocalSystem 帐户身份启动。当以 LocalSystem 帐户运行时，连接服务器实例无法使用 Internet Explorer 中为访问 CRL DP URL 或 OCSP responder 而配置的代理设置来确定证书的撤销状态。

您可使用 Microsoft Netsh 命令将代理设置导入到连接服务器实例，从而服务器可以访问 Internet 上的证书撤销检查站点。

解决方案

- 1 在连接服务器计算机上，打开包含以管理员身份运行设置的命令行窗口。

例如，单击开始，键入 `cmd`，右键单击 `cmd.exe` 图标，然后选择以管理员身份运行。

- 2 键入 `netsh`，然后按 Enter。

- 3 键入 `winhttp`，然后按 Enter。

- 4 键入 `show proxy`，然后按 Enter。

Netsh 显示代理设置为直接连接。使用了此设置，如果您的组织正在使用代理，则连接服务器计算机无法连接到 Internet。

- 5 配置代理设置。

例如，在 `netsh winhttp>` 提示符中，键入 `import proxy source=ie`。

代理设置被导入到连接服务器计算机。

- 6 通过键入 `show proxy` 确认代理设置。

- 7 重新启动 VMware Horizon View 连接服务器服务。

- 8 在 Horizon Administrator 仪表板上，确认安全服务器或连接服务器图标为绿色。

排除智能卡证书撤销检查中的故障

已连接智能卡的连接服务器实例或安全服务器无法在服务器 TLS 证书上执行证书撤销检查，除非您已配置智能卡证书撤销检查。

问题

如果您的组织使用代理服务器进行 Internet 访问，或如果连接服务器实例或安全服务器由于防火墙或其他控制的原因无法连接执行撤销检查的服务器，则证书撤销检查可能会失败。

重要 确保 CRL 文件为最新版本。

原因

Horizon 7 支持通过证书撤销列表 (Certificate Revocation List, CRL) 和联机证书状态协议 (Online Certificate Status Protocol, OCSP) 进行证书撤销检查。CRL 是由颁发证书的 CA (证书颁发机构) 发布的已撤销证书列表。OCSP 是一种证书验证协议，用于获取 X.509 证书的撤销状态。CA 必须能够从连接服务器或安全服务器主机上访问。这一切的前提条件是已配置智能卡证书撤销检查。请参阅[使用智能卡证书撤销检查](#)。

解决方案

- 1 （手动）创建您自己的程序，从您所使用的 CA 网站上，将最新 CRL 下载到您的 Horizon 7 Server 路径中。
- 2 在连接服务器或安全服务器主机的 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\locked.properties`
- 3 将 `locked.properties` 文件中的 `enableRevocationChecking` 和 `crlLocation` 属性添加至存储 CRL 的本地路径中。
- 4 重新启动连接服务器服务或安全服务器服务，使所做的更改生效。

更多故障排除信息

您可以在 VMware 知识库文章中找到更多故障排除信息。

VMware 知识库 (Knowledge Base, KB) 经常更新，以纳入新的 VMware 产品故障排除信息。

有关对 Horizon 7 进行故障排除的更多信息，请参阅 VMware 知识库网站上提供的知识库文章：

<http://kb.vmware.com/selfservice/microsites/microsite.do>

使用 vdmadmin 命令

在连接服务器实例上，您可以使用 **vdmadmin** 命令行界面执行各种管理任务。

您可以使用 **vdmadmin** 命令执行那些在 **Horizon Administrator** 用户界面中无法执行的管理任务，或者执行需要通过脚本自动运行的管理任务。

有关 **Horizon Administrator**、**Horizon 7 cmdlet** 和 **vdmadmin** 所能执行的操作的对比，请参阅《**Horizon 7 集成指南**》文档。

- **vdmadmin 命令用法**

vdmadmin 命令的语法用于控制其操作。

- **使用 -A 选项在 Horizon Agent 中配置日志**

您可以使用带有 **-A** 选项的 **vdmadmin** 命令配置 **Horizon Agent** 生成的日志。

- **使用 -A 选项覆盖 IP 地址**

您可以使用带有 **-A** 选项的 **vdmadmin** 命令覆盖 **Horizon Agent** 报告的 IP 地址。

- **使用 -F 选项更新外部安全主体**

您可以使用 **vdmadmin** 命令和 **-F** 选项更新 **Active Directory** 中有权使用桌面的 **Windows** 用户的外部安全主体 (Foreign Security Principal, FSP)。

- **使用 -H 选项列出并显示运行状况监视器**

您可以使用 **vdmadmin** 命令 **-H** 列出现有的运行状况监视器，对 **Horizon 7** 组件的实例进行监视，并显示特定运行状况监视器或监视器实例的详细信息。

- **使用 -I 选项列出并显示 Horizon 7 运行报告**

您可以使用带 **vdmadmin** 选项的 **-I** 命令列出可用的 **Horizon 7** 运行报告，并显示运行其中任一报告的结果。

- **使用 -I 选项以 Syslog 格式生成 Horizon 7 事件日志消息**

您可以使用带 **-I** 选项的 **vdmadmin** 命令以 **Syslog** 格式在事件日志文件中记录 **Horizon 7** 事件消息。许多第三方分析产品要求使用平面文件 **Syslog** 数据作为输入内容来完成其分析操作。

- **使用 -L 选项分配专用计算机**

您可以使用带 **vdmadmin** 选项的 **-L** 命令从一个专用池中向用户分配计算机。

- **使用 -M 选项显示有关计算机的信息**

您可以使用带有 **-M** 选项的 **vdmadmin** 命令显示有关虚拟机或物理机配置的信息。

- **使用 -M 选项回收虚拟机上的磁盘空间**

您可使用含有 **-M** 选项的 **vdmadmin** 命令标记要进行磁盘空间回收的链接克隆虚拟机。Horizon 7 可以指示 ESXi 主机回收链接克隆操作系统磁盘上的磁盘空间，而无需等待操作系统磁盘上的未使用空间达到 Horizon Administrator 中指定的最小阈值。

- **使用 -N 选项配置域过滤器**

您可以使用带 **-N** 选项的 **vdmadmin** 命令控制 Horizon 7 允许最终用户访问的域。

- **配置域过滤器**

您可以配置域过滤器以限制连接服务器实例或安全服务器为最终用户提供的域。

- **使用 -O 和 -P 选项显示未授权用户的计算机和策略**

您可以使用带 **-O** 和 **-P** 选项的 **vdmadmin** 命令显示分配给那些不再具有系统使用授权的用户的虚拟机和策略。

- **使用 -Q 选项在 Kiosk 模式下配置客户端**

您可以使用带 **vdmadmin** 选项的 **-Q** 命令为处于 Kiosk 模式的客户端设置默认值及创建帐户，以及启用这些客户端的身份验证并显示其配置信息。

- **使用 -R 选项显示计算机的首个用户**

您可以使用带有 **-R** 选项的 **vdmadmin** 命令了解受管虚拟机的初始分配情况。例如，在 LDAP 数据丢失的情况下，您可能需要此信息，以便可以重新为用户分配虚拟机。

- **使用 -S 选项移除连接服务器实例或安全服务器条目**

您可以使用带 **-S** 选项的 **vdmadmin** 命令从 Horizon 7 配置中移除连接服务器实例或安全服务器条目。

- **使用 -T 选项为管理员提供辅助凭据**

可以使用具有 **-T** 选项的 **vdmadmin** 命令为管理员用户提供 Active Directory 辅助凭据。

- **使用 -U 选项显示用户信息**

您可以使用带 **-U** 选项的 **vdmadmin** 命令显示用户的详细信息。

- **使用 -V 选项解锁或锁定虚拟机**

您可以使用带 **-V** 选项的 **vdmadmin** 命令解锁或锁定数据中心的虚拟机。

- **使用 -X 选项检测和解决 LDAP 条目和模式冲突**

您可以使用带有 **-X** 选项的 **vdmadmin** 命令检测和解决某个组中的连接服务器副本实例存在的 LDAP 条目冲突和 LDAP 模式冲突。您还可以使用此选项检测和解决 Cloud Pod 架构环境中的 LDAP 模式冲突。

vdmadmin 命令用法

vdmadmin 命令的语法用于控制其操作。

在 Windows 命令提示符下，使用以下 **vdmadmin** 命令格式。

```
vdmadmin command_option [additional_option argument] ...
```

您可以使用的附加选项取决于命令选项。

默认情况下，vdmadmin 命令可执行文件的路径为 C:\Program Files\VMware\VMware View\Server\tools\bin。为避免在命令行中输入此路径，可以将此路径添加到 *PATH* 环境变量中。

■ vdmadmin 命令身份验证

为了成功运行指定操作，您必须以**管理员**角色运行 vdmadmin 命令。

■ vdmadmin 命令输出格式

您可以使用某些 vdmadmin 命令选项指定输出信息的格式。

■ vdmadmin 命令选项

您可以使用 vdmadmin 命令的选项来指定该命令执行的操作。

vdmadmin 命令身份验证

为了成功运行指定操作，您必须以**管理员**角色运行 vdmadmin 命令。

可以使用 Horizon Administrator 将**管理员**角色分配给用户。请参阅第 6 章，配置基于角色的委托管理。

如果您使用权限不足的用户身份登录，则可以使用 **-b** 选项以分配有**管理员**角色的用户身份运行该命令，前提是您知道用户密码。您可以指定 **-b** 选项，作为指定域的指定用户运行 vdmadmin 命令。下列形式的 **-b** 选项具有相同的效果。

```
-b username domain [password | *]
```

```
-b username@domain [password | *]
```

```
-b domain\username [password | *]
```

如果指定星号 (*) 而不是密码，将提示您输入密码，并且 vdmadmin 命令不会在命令行的命令历史记录中保留敏感密码。

-b 选项可以与除 **-R** 和 **-T** 选项以外的所有命令选项一起使用。

vdmadmin 命令输出格式

您可以使用某些 vdmadmin 命令选项指定输出信息的格式。

下表显示了某些 vdmadmin 命令选项为设置输出文本格式提供的选项。

表 12-1. 选择输出格式的选项

选项	说明
-csv	将输出格式设置为逗号分隔值格式。
-n	用 ASCII (UTF-8) 字符显示输出内容。这是逗号分隔值和纯文本格式输出的默认字符集。

表 12-1. 选择输出格式的选项（续）

选项	说明
-w	用 Unicode (UTF-16) 字符显示输出内容。这是 XML 输出的默认字符集。
-xml	以 XML 格式显示输出内容。

vdmadmin 命令选项

您可以使用 `vdmadmin` 命令的选项来指定该命令执行的操作。

下表显示了可与 `vdmadmin` 命令配合使用以控制和检验 Horizon 7 运行过程的命令选项。

表 12-2. vdmadmin 命令选项

选项	说明
-A	管理 Horizon Agent 在其日志文件中记录的信息。请参阅 使用 -A 选项在 Horizon Agent 中配置日志 。 覆盖 Horizon Agent 报告的 IP 地址。请参阅 使用 -A 选项覆盖 IP 地址 。
-C	为连接服务器组设置名称。请参阅 GUID-3AD7B00C-43C4-417E-A06B-7251805657D6#GUID-3AD7B00C-43C4-417E-A06B-7251805657D6 。
-F	为所有用户或指定用户更新 Active Directory 中的外部安全主体 (Foreign Security Principals, FSP)。请参阅 使用 -F 选项更新外部安全主体 。
-H	显示 Horizon 7 服务的运行状况信息。请参阅 使用 -H 选项列出并显示运行状况监视器 。
-I	生成有关 Horizon 7 运行情况的报告。请参阅 使用 -I 选项列出并显示 Horizon 7 运行报告 。
-L	为用户分配专用桌面或者删除所做的分配。请参阅 使用 -L 选项分配专用计算机 。
-M	显示关于某个虚拟机或物理机的信息。请参阅 使用 -M 选项显示有关计算机的信息 。
-N	配置连接服务器实例或组为 Horizon Client 提供的域。请参阅 使用 -N 选项配置域过滤器 。
-O	显示已分配给用户，但用户已不再具有其授权的远程桌面。请参阅 使用 -O 和 -P 选项显示未授权用户的计算机和策略 。
-P	显示与未授权用户的远程桌面相关联的用户策略。请参阅 使用 -O 和 -P 选项显示未授权用户的计算机和策略 。
-Q	在 Active Directory 帐户中配置帐户以及处于 kiosk 模式的客户端设备的 Horizon 7 配置。请参阅 使用 -Q 选项在 Kiosk 模式下配置客户端 。
-R	报告第一个访问远程桌面的用户。请参阅 使用 -R 选项显示计算机的首个用户 。
-S	从 Horizon 7 的配置中移除一个针对连接服务器实例的配置条目。请参阅 使用 -S 选项移除连接服务器实例或安全服务器条目 。
-T	向管理员用户提供 Active Directory 辅助凭据。请参阅 使用 -T 选项为管理员提供辅助凭据 。
-U	显示有关用户的信息，包括他们的远程桌面授权和 ThinApp 分配，以及管理员角色。请参阅 使用 -U 选项显示用户信息 。
-V	解锁或锁定虚拟机。请参阅 使用 -V 选项解锁或锁定虚拟机 。
-X	在连接服务器副本实例中检测和解决重复的 LDAP 条目。请参阅 使用 -X 选项检测和解决 LDAP 条目和模式冲突 。

使用 -A 选项在 Horizon Agent 中配置日志

您可以使用带有 `-A` 选项的 `vdmadmin` 命令配置 Horizon Agent 生成的日志。

语法

```
vdmadmin -A [-b authentication_arguments] -getDCT-outfile local_file -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -getlogfile logfile -outfile local_file -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -getloglevel [-xml] -d desktop [-m machine]
```

```
vdmadmin -A [-b authentication_arguments] -getstatus [-xml] -d desktop [-m machine]
```

```
vdmadmin -A [-b authentication_arguments] -getversion [-xml] -d desktop [-m machine]
```

```
vdmadmin -A [-b authentication_arguments] -list [-xml] [-w | -n] -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -setloglevel level -d desktop [-m machine]
```

用法说明

为了协助 VMware 技术支持部门排除 Horizon Agent 故障，您可以创建一个数据收集工具 (Data Collection Tool, DCT) 捆绑包。您还可以更改日志级别、显示 Horizon Agent 的版本和状态以及在本地磁盘上保存独立的日志文件。

选项

下表显示了可以在 Horizon Agent 中配置日志记录时指定的选项。

表 12-3. 用于在 Horizon Agent 中配置日志记录的选项

选项	说明
-d 桌面	指定桌面池。
-getDCT	创建一个数据收集工具 (Data Collection Tool, DCT) 捆绑包并将其保存在本地文件中。
-getlogfile 日志文件	指定要保存副本的日志文件的名称。
-getloglevel	显示 Horizon Agent 的当前日志记录级别。
-getstatus	显示 Horizon Agent 的状态。
-getversion	显示 Horizon Agent 的版本。
-list	列出 Horizon Agent 的日志文件。
-m 计算机	指定桌面池中的计算机。

表 12-3. 用于在 Horizon Agent 中配置日志记录的选项（续）

选项	说明
<code>-outfile</code> 本地文件	指定要保存 DCT 捆绑包或日志文件副本的本地文件的名称。
<code>-setloglevel</code> 级别	设置 Horizon Agent 的日志记录级别。
	debug 记录错误、警告和调试事件。
	normal 记录错误和警告事件。
	trace 记录错误、警告、信息和调试事件。

示例

显示桌面池 `dtpool2` 中虚拟机 `machine1` 的 Horizon Agent 日志级别。

```
vdadmin -A -d dtpool2 -m machine1 -getloglevel
```

将桌面池 `dtpool2` 中虚拟机 `machine1` 的 Horizon Agent 日志级别设为 `debug`。

```
vdadmin -A -d dtpool2 -m machine1 -setloglevel debug
```

显示桌面池 `dtpool2` 中虚拟机 `machine1` 的 Horizon Agent 日志文件列表。

```
vdadmin -A -d dtpool2 -m machine1 -list
```

将桌面池 `dtpool2` 中虚拟机 `machine1` 的 Horizon Agent 日志文件 `log-2009-01-02.txt` 另存为副本 `C:\mycopiedlog.txt`。

```
vdadmin -A -d dtpool2 -m machine1 -getlogfile log-2009-01-02.txt -outfile C:\mycopiedlog.txt
```

显示桌面池 `dtpool2` 中虚拟机 `machine1` 的 Horizon Agent 版本。

```
vdadmin -A -d dtpool2 -m machine1 -getversion
```

显示桌面池 `dtpool2` 中虚拟机 `machine1` 的 Horizon Agent 状态。

```
vdadmin -A -d dtpool2 -m machine1 -getstatus
```

为桌面池 `dtpool2` 中的虚拟机 `machine1` 创建 DCT 捆绑包，并将其写入 zip 文件 `C:\myfile.zip` 中。

```
vdadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\myfile.zip
```

使用 -A 选项覆盖 IP 地址

您可以使用带有 `-A` 选项的 `vdadmin` 命令覆盖 Horizon Agent 报告的 IP 地址。

语法

```
vdmadmin -A [-b authentication_arguments] -override -i ip_or_dns -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -override -list -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -override -r -d desktop [-m machine]
```

用法说明

Horizon Agent 可找出运行它的虚拟机的 IP 地址并报告给连接服务器实例。在安全性较高的配置中，连接服务器实例不会信任 Horizon Agent 所报告的值，您可以覆盖由 Horizon Agent 提供的值，并指定受管虚拟机应采用的 IP 地址。如果 Horizon Agent 报告的虚拟机地址与所定义的值不符，您就无法使用 Horizon Client 访问该虚拟机。

选项

下表显示了可以在覆盖 IP 地址时指定的选项。

表 12-4. 覆盖 IP 地址的选项

选项	说明
-d 桌面	指定桌面池。
-i ip_or_dns	指定 IP 地址或 DNS 中可解析的域名。
-m 计算机	指定桌面池中虚拟机的名称。
-override	指定一个覆盖 IP 地址的操作。
-r	移除被覆盖的 IP 地址。

示例

覆盖桌面池 dtpool2 中虚拟机 machine2 的 IP 地址。

```
vdmadmin -A -override -i 10.20.54.165 -d dtpool2 -m machine2
```

显示为桌面池 dtpool2 中的虚拟机 machine2 定义的 IP 地址。

```
vdmadmin -A -override -list -d dtpool2 -m machine2
```

移除为桌面池 dtpool2 中虚拟机 machine2 定义的 IP 地址。

```
vdmadmin -A -override -r -d dtpool2 -m machine2
```


移除为桌面池 **dtpool3** 中的桌面定义的 IP 地址。

```
vdmadmin -A -override -r -d dtpool3
```

使用 -F 选项更新外部安全主体

您可以使用 **vdmadmin** 命令和 **-F** 选项更新 Active Directory 中有权使用桌面的 Windows 用户的外部安全主体 (Foreign Security Principal, FSP)。

语法

```
vdmadmin -F [-b authentication_arguments] [-u domain\user]
```

用法说明

如果您信任本地域以外的域，就会允许外部域中的安全主体访问本地域的资源。Active Directory 用 FSP 来代表受信任的外部域中的安全主体。如果您修改受信任的外部域列表，则可能需要更新用户的 FSP。

选项

-u 选项可指定您希望更新 FSP 的用户的名称和域。如果您没有指定此选项，该命令会更新 Active Directory 中所有用户的 FSP。

示例

更新域 EXTERNAL 中用户 Jim 的 FSP。

```
vdmadmin -F -u EXTERNAL\Jim
```

更新 Active Directory 中所有用户的 FSP。

```
vdmadmin -F
```

使用 -H 选项列出并显示运行状况监视器

您可以使用 **vdmadmin** 命令 **-H** 列出现有的运行状况监视器，对 Horizon 7 组件的实例进行监视，并显示特定运行状况监视器或监视器实例的详细信息。

语法

```
vdmadmin -H [-b authentication_arguments] -list -xml [-w | -n]
```

```
vdmadmin -H [-b authentication_arguments] -list -monitorid monitor_id -xml [-w | -n]
```

```
vdmadmin -H [-b authentication_arguments] -monitorid monitor_id -instanceid instance_id -xml [-w | -n]
```

用法说明

下表显示了 Horizon 7 用来监视其组件运行状况的运行状况监视器。

表 12-5. 运行状况监视器

监视器	说明
CBMonitor	监视连接服务器实例的运行状况。
DBMonitor	监视事件数据库的运行状况。
DomainMonitor	监视连接服务器主机的本地域及所有信任域的运行状况。
SGMonitor	监视安全网关服务和安全服务器的运行状况。
VCMonitor	监视 vCenter 服务器的运行状况。

如果某个组件具有若干实例，Horizon 7 会创建单独的监视器实例来监视该组件的每个实例。

此命令会以 XML 格式输出关于运行状况监视器和监视器实例的所有信息。

选项

下表显示了可以在列出和显示运行状况监视器时指定的选项。

表 12-6. 列出并显示运行状况监视器的选项

选项	说明
-instanceid <i>instance_id</i>	指定一个运行状况监视器实例
-list	如果未指定运行状况监视器 ID，则显示现有的运行状况监视器。
-list -monitorid <i>monitor_id</i>	显示指定运行状况监视器 ID 的监视器实例。
-monitorid <i>monitor_id</i>	指定一个运行状况监视器 ID。

示例

以 XML 格式（使用 Unicode 字符）列出现有的所有运行状况监视器。

```
vdmadmin -H -list -xml
```

以 XML 格式（使用 ASCII 字符）列出 vCenter 监视器 (VCMonitor) 的所有实例。

```
vdmadmin -H -list -monitorid VCMonitor -xml -n
```

显示指定 vCenter 监视器实例的运行状况。

```
vdmadmin -H -monitorid VCMonitor -instanceid 4aec2c99-4879-96b2-de408064d035 -xml
```

使用 -I 选项列出并显示 Horizon 7 运行报告

您可以使用带 vdmadmin 选项的 -I 命令列出可用的 Horizon 7 运行报告，并显示运行其中任一报告的结果。

语法

```
vdmadmin -I [-b authentication_arguments] -list [-xml] [-w | -n]
```

```
vdmadmin -I [-b authentication_arguments] -report report -view view [-startdate yyyy-MM-dd-HH:mm:ss]
[-enddate yyyy-MM-dd-HH:mm:ss] [-w | -n] -xml | -csv
```

用法说明

您可以使用此命令显示可用的报告和视图，并显示 Horizon 7 为指定报告和视图记录的信息。

您可以使用带 vdmadmin 选项的 -I 命令来生成 Horizon 7syslog 格式的 日志消息。请参阅[使用 -I 选项以 Syslog 格式生成 Horizon 7 事件日志消息](#)。

选项

下表显示了可以在列出和显示报告和视图时指定的选项。

表 12-7. 列出并显示报告和视图的选项

选项	说明
-enddate yyyy-MM-dd-HH:mm:ss	指定显示信息的日期上限。
-list	列出可用的报告和视图。
-report 报告	指定一个报告。
-startdate yyyy-MM-dd-HH:mm:ss	指定要显示信息的日期下限。
-view 视图	指定一个视图。

示例

以 XML 格式（使用 Unicode 字符）列出可用的报告和视图。

```
vdmadmin -I -list -xml -w
```

以逗号分隔值格式（使用 ASCII 字符）显示自 2010 年 8 月 1 日以来发生的用户事件列表。

```
vdmadmin -I -report events -view user_events -startdate 2010-08-01-00:00:00 -csv -n
```

使用 -I 选项以 Syslog 格式生成 Horizon 7 事件日志消息

您可以使用带 `-I` 选项的 `vdmadmin` 命令以 Syslog 格式在事件日志文件中记录 Horizon 7 事件消息。许多第三方分析产品要求使用平面文件 Syslog 数据作为输入内容来完成其分析操作。

语法

```
vdmadmin -I -eventSyslog -disable
```

```
vdmadmin -I -eventSyslog -enable -localOnly
```

```
vdmadmin -I -eventSyslog -enable -path path
```

```
vdmadmin -I -eventSyslog -enable -path path  
-user DomainName\username -password password
```

用法说明

您可使用该命令以 Syslog 格式生成 Horizon 7 事件日志消息。在 Syslog 文件中，Horizon 7 事件日志消息的格式是键值对，便于分析软件访问日志数据。

您也可使用包含 `-I` 选项的 `vdmadmin` 命令来列出可用的报告和视图，并显示指定报告的内容。请参阅[使用 -I 选项列出并显示 Horizon 7 运行报告](#)。

选项

您可以禁用或启用 `eventSyslog` 选项。您可以将 Syslog 输出仅定向到本地系统，也可以定向到其他位置。Horizon 7 5.2 或更高版本支持通过 UDP 直接连接到 Syslog 服务器。请参阅《Horizon 7 安装指南》文档中的“为 Syslog 服务器配置事件日志记录”。

表 12-8. 以 Syslog 格式生成 Horizon 7 事件日志消息的选项

选项	说明
<code>-disable</code>	禁用 Syslog 日志记录。
<code>-e -enable</code>	启用 Syslog 日志记录。
<code>-eventSyslog</code>	指定 Horizon 7 事件以 Syslog 格式生成。
<code>-localOnly</code>	仅在本地系统中存储 Syslog 输出。使用 <code>-localOnly</code> 选项时，Syslog 输出的默认目标位置为 <code>%PROGRAMDATA%\VMware\VDM\events\</code> 。

表 12-8. 以 Syslog 格式生成 Horizon 7 事件日志消息的选项（续）

选项	说明
<code>-password 密码</code>	为用户指定密码，该用户可授予对 Syslog 输出的指定目标路径的访问权限。
<code>-path</code>	确定 Syslog 输出的目标 UNC 路径。
<code>-u -user 域名\用户名</code>	指定可访问 Syslog 输出的目标路径的域和用户名。

示例

禁用以 Syslog 格式生成 Horizon 7 事件。

```
vdadmin -I -eventSyslog -disable
```

将 Horizon 7 事件的 Syslog 输出仅定向到本地系统。

```
vdadmin -I -eventSyslog -enable -localOnly
```

将 Horizon 7 事件的 Syslog 输出定向到指定路径。

```
vdadmin -I -eventSyslog -enable -path path
```

将 Horizon 7 事件的 Syslog 输出定向到需要授权域用户访问的指定路径。

```
vdadmin -I -eventSyslog -enable -path \\logserver\share\ViewEvents -user mydomain\myuser  
-password mypassword
```

使用 -L 选项分配专用计算机

您可以使用带 `vdadmin` 选项的 `-L` 命令从一个专用池中向用户分配计算机。

语法

```
vdadmin -L [-b authentication_arguments] -d desktop -m machine -u domain\user
```

```
vdadmin -L [-b authentication_arguments] -d desktop [-m machine | -u domain\user] -r
```

用法说明

用户第一次连接到专用桌面池时，Horizon 7 会向用户分配计算机。在某些情况下，您可能需要向用户预分配计算机。例如，您可能需要他们在初次连接前准备好系统环境。当用户连接到 Horizon 7 从专用池分配的远程桌面后，在虚拟机的使用期限内，托管此桌面的虚拟机将始终分配给该用户。您可以将用户分配到专用池中的单个计算机。

您可以将计算机分配给任何经授权的用户。当您要恢复连接服务器实例上丢失的 **View LDAP** 数据，或者要更改特定计算机的所有权时，可能需要执行此操作。

当用户连接到 **Horizon 7** 从专用池分配的远程桌面后，在托管桌面的虚拟机的使用期限内，该远程桌面将始终分配给该用户。对于离开组织的用户、无需再访问桌面的用户或使用另一桌面池中桌面的用户，您可能需要移除这些用户的计算机分配。您还可以移除对访问桌面池的所有用户分配。

注 `vdmadmin -L` 命令不向 **View Composer** 永久磁盘分配所有权。要将具有永久磁盘的链接克隆桌面分配给用户，请使用 **Horizon Administrator** 中的**分配用户**菜单选项。

如果确实使用了 `vdmadmin -L` 向用户分配带有永久磁盘的链接克隆桌面，则在特定情况中可出现意外结果。例如，如果要分离永久磁盘并用它重新创建桌面，则重新创建的桌面不会分配给原始桌面的所有者。

选项

下表显示了可以在为用户分配桌面或移除分配时指定的选项。

表 12-9. 分配专用桌面的选项

选项	说明
<code>-d 桌面</code>	指定桌面池名称。
<code>-m 计算机</code>	指定托管远程桌面的虚拟机名称。
<code>-r</code>	移除授予指定用户的分配，或移除指定计算机上的所有分配。
<code>-u 域\用户</code>	指定用户的登录名和域。

示例

将桌面池 `dtpool1` 中的虚拟机 `machine2` 分配给域 `CORP` 中的用户 `Jo`。

```
vdmadmin -L -d dtpool1 -m machine2 -u CORP\Jo
```

移除桌面池 `dtpool1` 中对 `CORP` 域用户 `Jo` 的桌面分配。

```
vdmadmin -L -d dtpool1 -u Corp\Jo -r
```

移除对桌面池 `dtpool3` 中计算机 `machine1` 的所有用户分配。

```
vdmadmin -L -d dtpool3 -m machine1 -r
```

使用 -M 选项显示有关计算机的信息

您可以使用带有 `-M` 选项的 `vdmadmin` 命令显示有关虚拟机或物理机配置的信息。

语法

```
vdmadmin -M [-b authentication_arguments] [-m machine | [-u domain\user][-d desktop]] [-xml | -csv] [-w | -n]
```

用法说明

此命令可显示远程桌面的底层虚拟机或物理机的相关信息。

- 计算机的显示名称。
- 桌面池名称。
- 计算机状态。

计算机状态可以是以下值之一：UNDEFINED、PRE_PROVISIONED、CLONING、CLONINGERROR、CUSTOMIZING、READY、DELETING、MAINTENANCE、ERROR、LOGOUT。

此命令不会显示在 Horizon Administrator 中所显示的所有的动态计算机状态，例如 **Connected** 或 **Disconnected** 状态。

- 被分配的用户 SID。
- 被分配的用户帐户名。
- 被分配的用户域名。
- 虚拟机的详细目录（如果存在）。
- 虚拟机的创建日期。
- 虚拟机的模板路径（如果存在）。
- vCenter Server 的 URL（如果存在）。

选项

下表显示了可以在指定要显示详细信息的计算机时使用的选项。

表 12-10. 显示计算机信息的选项

选项	说明
-d 桌面	指定桌面池名称。
-m 计算机	指定虚拟机名称。
-u 域用户	指定用户的登录名和域。

示例

显示池 `dtpool2` 中分配给 `CORP` 域用户 `Jo` 的远程桌面的底层计算机相关信息，并将输出格式设为使用 ASCII 字符的 XML 格式。

```
vdadmin -M -u CORP\Jo -d dtpool2 -xml -n
```

显示计算机 `machine3` 的相关信息，并将输出格式设为逗号分隔值格式。

```
vdadmin -M -m machine3 -csv
```

使用 -M 选项回收虚拟机上的磁盘空间

您可使用含有 `-M` 选项的 `vdadmin` 命令标记要进行磁盘空间回收的链接克隆虚拟机。Horizon 7 可以指示 ESXi 主机回收链接克隆操作系统磁盘上的磁盘空间，而无需等待操作系统磁盘上的未使用空间达到 Horizon Administrator 中指定的最小阈值。

语法

```
vdadmin -M [-b authentication_arguments] -d desktop -m machine -markForSpaceReclamation
```

用法说明

通过此选项，您可以针对特定虚拟机启动磁盘空间回收，达到演示或排除故障的目的。

如果在中断期期间运行此命令，则不会执行空间回收操作。

使用包含 `-M` 选项的 `vdadmin` 命令回收磁盘空间时，必须先满足以下前提条件：

- 确认 Horizon 7 使用的是 vCenter Server 和 ESXi 5.1 版或更高版本。
- 确认适用于 vSphere 5.1 或更高版本的 VMware Tools 已安装在虚拟机上。
- 确认虚拟机为虚拟硬件版本 9 或更高版本。
- 在 Horizon Administrator 中，确认为 vCenter Server 选择了启用空间回收选项。请参阅[允许 vSphere 回收链接克隆虚拟机中的磁盘空间](#)。
- 在 Horizon Administrator 中，确认为桌面池选择了回收虚拟机磁盘空间选项。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“回收 View Composer 链接克隆上的磁盘空间”。
- 确认启动空间回收操作前虚拟机已开启。
- 确认不处于中断时期。请参阅《在 Horizon 7 中设置虚拟桌面》文档中的“为 View Composer 链接克隆设置 Storage Accelerator 和空间回收中断时间”。

选项

表 12-11. 回收虚拟机上磁盘空间的选项

选项	说明
<code>-d 桌面</code>	指定桌面池名称。
<code>-m 计算机</code>	指定虚拟机名称。
<code>-MarkForSpaceReclamation</code>	标记要进行磁盘空间回收的虚拟机。

示例

标记桌面池 `pool1` 中的虚拟机 `machine3`，以执行磁盘空间回收。

```
vdmadmin -M -d pool1 -m machine3 -markForSpaceReclamation
```

使用 -N 选项配置域过滤器

您可以使用带 `-N` 选项的 `vdmadmin` 命令控制 Horizon 7 允许最终用户访问的域。

语法

```
vdmadmin -N [-b authentication_arguments] -domains {-exclude | -include | -search} -domain domain -add [-s connsvr]
```

```
vdmadmin -N [-b authentication_arguments] -domains -list [-w | -n] [-xml]
```

```
vdmadmin -N [-b authentication_arguments] -domains -list -active [-w | -n] [-xml]
```

```
vdmadmin -N [-b authentication_arguments] -domains {-exclude | -include | -search} -domain domain -remove [-s connsvr]
```

```
vdmadmin -N [-b authentication_arguments] -domains {-exclude | -include | -search} -removeall [-s connsvr]
```

用法说明

指定 `-exclude`、`-include` 或 `-search` 中的一个选项，以将操作分别应用于排除列表、包含列表或搜索排除列表。

如果您将一个域添加到搜索排除列表，该域不会包含在自动域搜索中。

如果您将一个域添加到包含列表，该域会包含在搜索结果中。

如果您将一个域添加到排除列表，该域不会包含在搜索结果中。

选项

下表显示了可以在配置域过滤器时指定的选项。

表 12-12. 配置域过滤器的选项

选项	说明
<code>-add</code>	将域添加到列表中。
<code>-domain 域</code>	指定要过滤的域。 必须用域的 NetBIOS 名称而非 DNS 名称来指定域。
<code>-domains</code>	指定一个域过滤操作。
<code>-exclude</code>	在排除列表中指定操作。
<code>-include</code>	在包含列表中指定操作。
<code>-list</code>	显示每个连接服务器实例上和用于连接服务器组的搜索排除列表、排除列表以及包含列表中配置的域。
<code>-list -active</code>	显示运行该命令的连接服务器实例上可用的域。
<code>-remove</code>	从列表中移除域。
<code>-removeall</code>	从列表中移除所有域。
<code>-s connsvr</code>	指定应用于连接服务器实例上域过滤器的操作。您可以按照名称或 IP 地址指定连接服务器实例。 如果不指定该选项，您对搜索配置所做的任何更改都会应用于组中的所有连接服务器实例。
<code>-search</code>	在搜索排除列表中指定操作。

示例

将域 **FARDOM** 添加到连接服务器实例 **csvr1** 的搜索排除列表中。

```
vdmadmin -N -domains -search -domain FARDOM -add -s csvr1
```

将域 **NEARDOM** 添加到连接服务器组的排除列表中。

```
vdmadmin -N -domains -exclude -domain NEARDOM -add
```

显示组中连接服务器实例以及用于组的域搜索配置。

```
C:\ vdmadmin -N -domains -list

Domain Configuration
=====
Cluster Settings
  Include:
  Exclude:
  Search :
    FARDOM
```

```

DEPTX

Broker Settings: CONSVR-1
  Include:
  (*)Exclude:
    YOURDOM
  Search :

Broker Settings: CONSVR-2
  Include:
  Exclude:
  Search :
```

Horizon 7 会对组中每个连接服务器主机上的域搜索进行限制，以排除 FARDOM 和 DEPTX 域。CONSVR-1 的排除列表旁边的 (*) 字符表示 Horizon 7 会将 YOURDOM 域从 CONSVR-1 上的域搜索结果列表中排除。

以使用 ASCII 字符的 XML 格式显示域过滤器。

```
vdmadmin -N -domains -list -xml -n
```

显示本地连接服务器实例上当前对 Horizon 7 可用的域。

```

C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
=====
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS:fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

以使用 ASCII 字符的 XML 格式显示可用的域。

```
vdmadmin -N -domains -list -active -xml -n
```

从连接服务器组的排除列表中移除域 NEARDOM。

```
vdmadmin -N -domains -exclude -domain NEARDOM -remove
```

从连接服务器实例 csvr1 的包含列表中移除所有域。

```
vdmadmin -N -domains -include -removeall -s csvr1
```

配置域过滤器

您可以配置域过滤器以限制连接服务器实例或安全服务器为最终用户提供的域。

Horizon 7 通过遍历信任关系确定可以访问哪些域，从连接服务器实例或安全服务器所在的域开始。对于一组连接良好的小型域，Horizon 7 能够快速确定完整的域列表，但随着域数量的不断增多或域之间连通性能的逐渐降低，确定完整域列表所需的时间也会随之增加。Horizon 7 还可能在搜索结果中包含您不希望为用户登录桌面时为其提供的域。

如果您先前已将控制递归域枚举的 Windows 注册表项 (HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware VDM\RecursiveDomainEnum) 的值设为 **false**，则会禁用递归域搜索，连接服务器实例将仅搜索主域。要使用域过滤功能，需删除该注册表项，或者将其值设为 **true**，然后重新启动系统。您必须在设置了该注册表项的每个连接服务器实例上执行上述操作。

下表显示了可以在配置域过滤时指定的域列表类型。

表 12-13. 域列表类型

域列表类型	说明
搜索排除列表	指定 Horizon 7 在自动搜索过程中可以遍历的域。该搜索过程将忽略那些包含在搜索排除列表中的域，并且不会试图定位被排除的域所信任的域。您无法将主域排除在搜索过程以外。
排除列表	指定 Horizon 7 将从域搜索结果中排除的域。您无法排除主域。
包含列表	指定 Horizon 7 不从域搜索结果中排除的域。其他所有域（不包括主域）都将被排除。

自动域搜索会检索域列表，排除您在搜索排除列表中指定的域，以及被排除的域所信任的域。Horizon 7 将按以下顺序选择第一个非空排除列表或包含列表。

- 1 为连接服务器实例配置的排除列表。
- 2 为连接服务器组配置的排除列表。
- 3 为连接服务器实例配置的包含列表。
- 4 为连接服务器组配置的包含列表。

Horizon 7 仅应用它选择的第一个列表来生成搜索结果。

如果您指定包含某个域，而该域的控制当前无法访问，Horizon 7 将不把该域包含在活动域列表中。

您无法排除连接服务器实例或安全服务器所属的主域。

包含域的过滤操作示例

可以使用包含列表指定 Horizon 7 未从域搜索结果中排除的域。其他所有域（不包括主域）都将被移除。

一个连接服务器实例加入了 MYDOM 主域，并与 YOURDOM 域存在信任关系。YOURDOM 域与 DEPTX 具有信任关系。

对连接服务器实例显示当前活动的域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
=====
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS:fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

DEPTY 和 DEPTZ 域出现在列表中，因为它们是 DEPTX 域所信任的域。

指定连接服务器实例应只使 YOURDOM 和 DEPTX 域可用（除了主域 MYDOM 以外）。

```
vdmadmin -N -domains -include -domain YOURDOM -add
vdmadmin -N -domains -include -domain DEPTX -add
```

显示包含 YOURDOM 和 DEPTX 域之后当前活动的域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR)
=====
Primary Domain: MYDOM
Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
```

Horizon 7 将包含列表用于域搜索结果。如果域层次结构非常复杂，或是与某些域的网络连通性较差，那么域搜索速度可能会较慢。在这种情况下，可改用搜索排除。

排除域的过滤操作示例

您可以使用排除列表来指定 Horizon 7 将从域搜索结果中排除的域。

一个包含两个连接服务器实例（CONSVR-1 和 CONSVR-2）的组加入到了 MYDOM 主域中，并与 YOURDOM 域存在信任关系。YOURDOM 域与 DEPTX 和 FARDOM 域具有信任关系。

FARDOM 域在远程地理位置，与该域的网络连接速度缓慢且延迟较高。FARDOM 域中的用户不需要访问 MYDOM 域中的连接服务器组。

对连接服务器组中的成员显示当前活动的域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
=====
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS:fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

DEPTY 和 DEPTZ 域是 DEPTX 域所信任的域。

要改进 Horizon Client 的连接性能，请将 FARDOM 域从连接服务器组的搜索过程中排除。

```
vdmadmin -N -domains -search -domain FARDOM -add
```

此命令可显示将 FARDOM 域从搜索中排除后的活动域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
=====
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```

扩展搜索排除列表，以便将 DEPTX 域及其信任的所有域从组中所有连接服务器实例的域搜索中排除。同时，将 YOURDOM 域排除在 CONSVR-1 可访问的范围以外。

```
vdmadmin -N -domains -search -domain DEPTX -add
vdmadmin -N -domains -exclude -domain YOURDOM -add -s CONSVR-1
```

显示新的域搜索配置。

```
C:\ vdmadmin -N -domains -list

Domain Configuration
=====
Cluster Settings
  Include:
  Exclude:
  Search :
    FARDOM
    DEPTX

Broker Settings: CONSVR-1
  Include:
  (*)Exclude:
    YOURDOM
  Search :

Broker Settings: CONSVR-2
  Include:
  Exclude:
  Search :
```

Horizon 7 会对组中每个连接服务器主机上的域搜索进行限制，以排除 FARDOM 和 DEPTX 域。CONSVR-1 的排除列表旁边的 (*) 字符表示 Horizon 7 会将 YOURDOM 域从 CONSVR-1 上的域搜索结果列表中排除。

在 CONSVR-1 上，显示当前的活动域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-1)
=====
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
```

在 CONSVR-2 上，显示当前的活动域。

```
C:\ vdmadmin -N -domains -list -active

Domain Information (CONSVR-2)
=====
Primary Domain: MYDOM

Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
```

使用 -O 和 -P 选项显示未授权用户的计算机和策略

您可以使用带 -O 和 -P 选项的 vdmadmin 命令显示分配给那些不再具有系统使用授权的用户的虚拟机和策略。

语法

```
vdmadmin -O [-b authentication_arguments] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath path]]
```

```
vdmadmin -P [-b authentication_arguments] [-ld | -lu] [-w | -n] [-xml [-noxslt | -xsltpath path]]
```

用法说明

如果您撤消某个用户对永久虚拟机或物理系统的权限，并不会自动撤消相关联的远程桌面分配。如果您临时暂停了用户的帐户，或者用户正在休假，这种情况是可以接受的。当您重新启用授权后，用户可以像以前一样继续使用同一虚拟机。如果用户离开了组织，其他用户将无法访问该用户的虚拟机，该虚拟机会被视为孤立。您可能还希望检查分配给未授权用户的策略。

选项

下表显示了可以在显示未授权用户的虚拟机和策略时指定的选项。

表 12-14. 显示未授权用户的计算机和策略的选项

选项	说明
-ld	按计算机对输出条目排序。
-lu	按用户对输出条目排序。

表 12-14. 显示未授权用户的计算机和策略的选项（续）

选项	说明
<code>-noxslt</code>	指定输出的 XML 文件不应用默认样式表。
<code>-xsltpath <i>path</i></code>	指定用于转换 XML 输出的样式表的路径。

表 12-15 显示了可应用于 XML 输出以转换为 HTML 的样式表。该样式表位于 `C:\Program Files\VMware\VMware View\server\etc` 目录下。

表 12-15. XSL 样式表

样式表文件名	说明
<code>unentitled-machines.xsl</code>	转换那些包含当前分配给用户的未授权虚拟机（按用户或系统分组）列表的报告。这是默认的样式表。
<code>unentitled-policies.xsl</code>	转换那些包含其用户级别策略应用到未授权用户的虚拟机列表的报告。

示例

以文本格式显示分配给未授权用户（按虚拟机分组）的虚拟机。

```
vdmadmin -O -ld
```

以 XML 格式（使用 ASCII 字符）显示分配给未授权用户（按用户分组）的虚拟机。

```
vdmadmin -O -lu -xml -n
```

应用您自己的样式表（位于 `C:\tmp\unentitled-users.xsl`），将输出重定向至文件 `uu-output.html`。

```
vdmadmin -O -lu -xml -xsltpath "C:\tmp\unentitled-users.xsl" > uu-output.html
```

以 XML 格式（使用 Unicode 字符）显示与未授权用户的虚拟机（按桌面分组）相关联的用户策略。

```
vdmadmin -P -ld -xml -w
```

应用您自己的样式表（位于 `C:\tmp\unentitled-policies.xsl`），将输出重定向至文件 `up-output.html`。

```
vdmadmin -P -ld -xml -xsltpath "C:\tmp\unentitled-policies.xsl" > up-output.html
```

使用 -Q 选项在 Kiosk 模式下配置客户端

您可以使用带 `vdmadmin` 选项的 `-Q` 命令为处于 Kiosk 模式的客户端设置默认值及创建帐户，以及启用这些客户端的身份验证并显示其配置信息。

语法

```
vdmadmin -Q -clientauth -add [-b authentication_arguments] -domain domain_name-clientid client_id
[-password "password" | -genpassword] [-ou DN] [-expirepassword | -noexpirepassword] [-group group_name
| -nogroup] [-description "description_text"]
```

```
vdmadmin -Q -disable [-b authentication_arguments] -s connection_server
```

```
vdmadmin -Q -enable [-b authentication_arguments] -s connection_server [--requirepassword]
```

```
vdmadmin -Q -clientauth -getdefaults [-b authentication_arguments] [--xml]
```

```
vdmadmin -Q -clientauth -list [-b authentication_arguments] [--xml]
```

```
vdmadmin -Q -clientauth -remove [-b authentication_arguments] -domain domain_name-clientid client_id
```

```
vdmadmin -Q -clientauth -removeall [-b authentication_arguments] [--force]
```

```
vdmadmin -Q -clientauth -setdefaults [-b authentication_arguments] [-ou DN] [ -expirepassword |
-noexpirepassword ] [-group group_name | -nogroup]
```

```
vdmadmin -Q -clientauth -update [-b authentication_arguments] -domain domain_name-clientid client_id
[-password "password" | -genpassword] [-description "description_text"]
```

用法说明

您必须在客户端用来连接其远程桌面的连接服务器实例所在组中的一个连接服务器实例上运行 **vdmadmin** 命令。

当您为密码到期项和 **Active Directory** 组成员关系配置默认值时，这些设置会由组中所有的连接服务器实例共享。

添加 **Kiosk** 模式客户端时，**Horizon 7** 会在 **Active Directory** 中为该客户端创建一个用户帐户。如果为客户端指定名称，则该名称必须以 **"custom-"** 或可以在 **ADAM** 中定义的备用字符串开头，而且名称长度不得超过 20 个字符。每个指定名称只能用于一个客户端设备。

您可以在连接服务器实例的 **ADAM** 中的

cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int 下的 **pae-ClientAuthPrefix** 多值属性中，定义可替代 **"custom-"** 的前缀。请勿将普通用户帐户作为前缀使用。

如果您不为客户端指定名称，**Horizon 7** 将使用您为客户端设备指定的 **MAC** 地址生成名称。例如，如果 **MAC** 地址是 **00:10:db:ee:76:80**，则相应的帐户名称为 **cm-00_10_db_ee_76_80**。您只能将这些帐户用于允许对客户端进行身份验证的连接服务器实例。

一些瘦客户端仅允许在 **kiosk** 模式中使用以字符 **"custom-"** 或 **"cm-"** 开头的帐户名。

自动生成的密码长度是 **16** 位，包含至少一个大写字母、一个小写字母、一个符号和一个数字，可以包含重复的字符。如果您需要一个更强的密码，则必须使用 **-password** 选项指定密码。

如果您使用 **-group** 选项指定一个组，或者之前已设置了默认组，**Horizon 7** 会将客户端的帐户添加到该组。您可以指定 **-nogroup** 选项，以免将该帐户加入任何组中。

如果您启用一个连接服务器实例以对 **kiosk** 模式客户端进行身份验证，您可以指定客户端必须提供密码（可选）。如果禁用身份验证，客户端将无法连接到其远程桌面。

即便为单个连接服务器实例启用或禁用身份验证，组中所有的连接服务器实例仍会共享客户端身份验证的所有其他设置。您只需添加一次客户端，组中所有的连接服务器实例都将能够接受来自该客户端的请求。

如果您在启用身份验证时指定 **-requirepassword** 选项，连接服务器实例将无法对具有自动生成密码的客户端进行身份验证。如果您更改连接服务器实例的配置来指定该选项，此类客户端将无法对自身进行身份验证，而且会返回错误消息未知用户名或无效密码 (**Unknown username or bad password**)。

选项

下表显示了可以在配置 **kiosk** 模式客户端时指定的选项。

表 12-16. 配置 kiosk 模式客户端的选项

选项	说明
-add	为 kiosk 模式客户端添加一个帐户。
-clientauth	指定一个为 kiosk 模式客户端配置身份验证的操作。
-clientid <i>client_id</i>	指定客户端的名称或 MAC 地址。
-description " <i>description_text</i> "	在 Active Directory 中为客户端设备创建帐户描述。
-disable	在指定连接服务器实例中禁用 kiosk 模式客户端的身份验证。
-domain <i>domain_name</i>	指定客户端设备帐户的域。
-enable	在指定连接服务器实例中启用 kiosk 模式客户端的身份验证。
-expirepassword	指定客户端帐户密码的到期时间与连接服务器组帐户密码到期时间相同。如果没有为该组定义到期时间，则密码不会失效。
-force	禁用移除 kiosk 模式客户端帐户时的确认提示。
-genpassword	为客户端帐户生成密码。如果您未指定 -password 或 -genpassword ，则会执行此默认行为。
-getdefaults	获得添加客户端帐户使用的默认值。
-group <i>group_name</i>	指定客户端帐户所加入的默认组的名称。组名必须指定为 Windows 2000 之前版本的 Active Directory 组名。
-list	显示 kiosk 模式客户端以及已启用 kiosk 模式客户端身份验证的连接服务器实例的相关信息。
-noexpirepassword	指定帐户的密码不会失效。
-nogroup	为客户端添加帐户时，指定该客户端的帐户不会被添加到默认组。为客户端设置默认值时，清除默认组的设置。

表 12-16. 配置 kiosk 模式客户端的选项（续）

选项	说明
<code>-ou DN</code>	指定客户端帐户被添加到的组织单位的标识名。 例如：OU=kiosk-ou,DC=myorg,DC=com 注 您无法使用 <code>-setdefaults</code> 选项更改组织单位的配置。
<code>-password "password"</code>	为客户端帐户指定显式密码。
<code>-remove</code>	移除处于 kiosk 模式的客户端帐户。
<code>-removeall</code>	移除所有处于 kiosk 模式的客户端的帐户。
<code>-requirepassword</code>	指定处于 kiosk 模式的客户端必须提供密码。Horizon 7 不接受为新连接生成的密码。
<code>-s connection_server</code>	指定要启用或禁用 kiosk 模式客户端身份验证的连接服务器实例的 NetBIOS 名称。
<code>-setdefaults</code>	设置添加客户端帐户使用的默认值。
<code>-update</code>	为 kiosk 模式客户端更新一个帐户。

示例

为客户端的组织单位、密码到期项和组成员设置默认值。

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

获取纯文本格式的当前客户端默认值。

```
vdmadmin -Q -clientauth -getdefaults
```

获取 XML 格式的当前客户端默认值。

```
vdmadmin -Q -clientauth -getdefaults -xml
```

将其 MAC 地址指定的客户端的帐户添加到 MYORG 域，并将默认设置应用于组 kc-grp。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

将其 MAC 地址指定的客户端的帐户添加到 MYORG 域，并使用自动生成的密码。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword -ou "OU=kiosk-ou,DC=myorg,DC=com" -group kc-grp
```

为已命名的客户端添加帐户，并为该客户端指定一个密码。

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

更新客户端的帐户，指定一个新密码和描述文本。

```
vdmadmin -Q -clientauth -update -domain MYORG -clientid custom-Terminal21 -password "Secret1!" -
description "Foyer Entry Workstation"
```

从 MYORG 域中移除根据 MAC 地址指定的 kiosk 模式客户端的帐户。

```
vdmadmin -Q -clientauth -remove -domain MYORG -clientid 00:10:db:ee:54:12
```

在不提示确认移除的情况下直接移除所有客户端的帐户。

```
vdmadmin -Q -clientauth -removeall -force
```

为连接服务器实例 **csvr-2** 启用客户端身份验证。具有自动生成的密码的客户端可以对自身进行身份验证，而无需提供密码。

```
vdmadmin -Q -enable -s csvr-2
```

为连接服务器实例 **csvr-3** 启用客户端身份验证，并要求客户端将其密码指定给 **Horizon Client**。具有自动生成密码的客户端无法对自身进行身份验证。

```
vdmadmin -Q -enable -s csvr-3 -requirepassword
```

为连接服务器实例 **csvr-1** 禁用客户端身份验证。

```
vdmadmin -Q -disable -s csvr-1
```

以文本格式显示有关客户端的信息。客户端 **cm-00_0c_29_0d_a3_e6** 具有自动生成的密码，而且不需要最终用户或应用程序脚本将该密码指定给 **Horizon Client**。客户端 **cm-00_22_19_12_6d_cf** 具有显式指定的密码，并需要最终用户提供该密码。连接服务器实例 **CONSVR2** 接受具有自动生成密码的客户端发出的身份验证请求。**CONSVR1** 不接受来自 **Kiosk** 模式客户端的身份验证请求。

```
C:\ vdmadmin -Q -clientauth -list
Client Authentication User List
=====
GUID           : 94be6344-0c9b-4a92-8d54-1brc1c2dc282
ClientID       : cm-00_0c_29_0d_a3_e6
Domain        : myorg.com
Password Generated: true

GUID           : 471d9d35-68b2-40ee-b693-56a7d92b2e25
ClientID       : cm-00_22_19_12_6d_cf
Domain        : myorg.com
Password Generated: false

Client Authentication Connection Servers
=====
Common Name           : CONSVR1
Client Authentication Enabled : false
Password Required     : false
```

```
Common Name           : CONSVR2
Client Authentication Enabled : true
Password Required      : false
```

使用 -R 选项显示计算机的首个用户

您可以使用带有 `-R` 选项的 `vdadmin` 命令了解受管虚拟机的初始分配情况。例如，在 LDAP 数据丢失的情况下，您可能需要此信息，以便可以重新为用户分配虚拟机。

注 带有 `-R` 选项的 `vdadmin` 命令仅适用于早于 View Agent 5.1 的虚拟机。在运行 View Agent 5.1 和更高版本以及 Horizon Agent 7.0 和更高版本的虚拟机上，该选项无效。要查找虚拟机的首个用户，请使用事件数据库来确定哪些用户曾经登录过计算机。

语法

```
vdadmin -R -i network_address
```

用法说明

您不能使用 `-b` 选项以特权用户的身份运行此命令。您必须以**管理员**角色用户的身份登录。

选项

`-i` 选项指定虚拟机的 IP 地址。

示例

显示首个访问 IP 地址为 10.20.34.120 的虚拟机的用户。

```
vdadmin -R -i 10.20.34.120
```

使用 -S 选项移除连接服务器实例或安全服务器条目

您可以使用带 `-S` 选项的 `vdadmin` 命令从 Horizon 7 配置中移除连接服务器实例或安全服务器条目。

语法

```
vdadmin -S [-b authentication_arguments] -r -s server
```

用法说明

为确保高可用性，您可以利用 Horizon 7 在连接服务器组中配置一个或多个副本连接服务器实例。如果您禁用组中的一个连接服务器实例，该服务器条目仍会保留在 Horizon 7 配置中。

您也可使用带 **-S** 选项的 **vdadmin** 命令从 Horizon 7 环境中移除安全服务器。如果您想要升级或重新安装安全服务器而非永久移除，则您无需使用此选项。

要永久移除条目，请执行以下任务：

- 1 运行连接服务器安装程序，从 Windows Server 计算机中卸载连接服务器实例或安全服务器。
- 2 运行“添加或移除程序”工具，从 Windows Server 计算机中移除 Adam Instance VMwareVDMS 程序。
- 3 在另一个连接服务器实例上，使用 **vdadmin** 命令从配置中移除已卸载的连接服务器实例或安全服务器的条目。

如果您想在已移除的系统中重新安装 Horizon 7，但并不想复制原始组的 Horizon 7 配置，请在重新安装前重新启动原始组中的所有连接服务器主机。此操作可防止重新安装的连接服务器实例从原始组中接收配置更新。

选项

-s 选项指定了要移除的连接服务器实例或安全服务器的 NetBIOS 名称。

示例

移除连接服务器实例 **connsvr3** 的条目。

```
vdadmin -S -r -s connsvr3
```

使用 -T 选项为管理员提供辅助凭据

可以使用具有 **-T** 选项的 **vdadmin** 命令为管理员用户提供 Active Directory 辅助凭据。

语法

```
vdadmin -T [-b authentication_arguments] -domainauth  
{-add | -update | -remove | -removeall | -list} -owner domain\user -user domain\user [-password password]
```

用法说明

如果用户和组所在的域与连接服务器域具有单向信任关系，您必须在 Horizon Administrator 中为管理员用户提供辅助凭据。管理员必须具有辅助凭据才能访问单向信任域。单向信任域可以是外部域，也可以是具有可传递林信任关系的域。

仅 Horizon Administrator 会话需要使用辅助凭据，最终用户的桌面或应用程序会话则不需要使用该凭据。仅管理员用户需要使用辅助凭据。

通过使用 **vdadmin** 命令，您可以针对每个用户配置辅助凭据。您无法全局配置指定的辅助凭据。

对于林信任关系，通常只需为林根域配置辅助凭据。然后，连接服务器可以枚举具有林信任关系的子域。

仅当单向信任域中的用户首次登录时，才可执行 Active Directory 帐户锁定、禁用和登录时间检查。

单向信任域不支持对用户进行 PowerShell 管理和智能卡身份验证。不支持对单向信任域中的用户进行 SAML 身份验证。

辅助凭据帐户需要以下权限。标准用户帐户默认应拥有这些权限。

- 列出内容
- 读取全部属性
- 读取权限
- 读取 tokenGroupsGlobalAndUniversal（“读取全部属性”隐含的权限）

限制

- 不支持对单向信任域中的用户进行 PowerShell 管理和智能卡身份验证。
- 不支持对单向信任域中的用户进行 SAML 身份验证。

选项

表 12-17. 用于提供辅助凭据的选项

选项	说明
<code>-add</code>	为所有者帐户添加辅助凭据。 执行 Windows 登录以验证指定的凭据是否有效。在 View LDAP 中为用户创建外部安全主体 (Foreign Security Principal, FSP)。
<code>-update</code>	更新所有者帐户的辅助凭据。 执行 Windows 登录以验证更新的凭据是否有效。
<code>-list</code>	显示所有者帐户的安全凭据。不会显示密码。
<code>-remove</code>	移除所有者帐户的安全凭据。
<code>-removeall</code>	移除所有者帐户的所有安全凭据。

示例

为指定的所有者帐户添加辅助凭据。执行 Windows 登录以验证指定的凭据是否有效。

```
vdmadmin -T -domainauth -add -owner domain\user -user domain\user -password password
```

更新指定的所有者帐户的辅助凭据。执行 Windows 登录以验证更新的凭据是否有效。

```
vdmadmin -T -domainauth -update -owner domain\user -user domain\user -password password
```

移除指定的所有者帐户的辅助凭据。

```
vdmadmin -T -domainauth -remove -owner domain\user -user domain\user
```

移除指定的所有者帐户的所有辅助凭据。

```
vdmadmin -T -domainauth -removeall -owner domain\user
```

显示指定的所有者帐户的所有辅助凭据。不会显示密码。

```
vdmadmin -T -domainauth -list -owner domain\user
```

使用 -U 选项显示用户信息

您可以使用带 -U 选项的 vdmadmin 命令显示用户的详细信息。

语法

```
vdmadmin
-U [-b authentication_arguments] -u domain\user [-w | -n] [-xml]
```

用法说明

此命令显示从 Active Directory 和 Horizon 7 中获得的用户的信息。

- Active Directory 中用户帐户的详细信息。
- Active Directory 组的成员身份。
- 计算机授权，包括计算机 ID、显示名称、描述、文件夹，以及计算机是否被禁用。
- ThinApp 分配。
- Administrator 角色，包括用户的管理权限以及他们在哪些文件夹中具有这些权限。

选项

-u 选项可指定用户的名称和域。

示例

以 XML 格式（使用 ASCII 字符）显示域 CORP 中用户 Jo 的相关信息。

```
vdmadmin -U -u CORP\Jo -n -xml
```

使用 -V 选项解锁或锁定虚拟机

您可以使用带 -V 选项的 vdmadmin 命令解锁或锁定数据中心的虚拟机。

语法

```
vdmadmin -V [-b authentication_arguments] -e -d desktop -m machine [-m machine] ...
```

```
vdmadmin -V [-b authentication_arguments] -e -vcdn vCenter_dn -vmpath inventory_path
```

```
vdmadmin -V [-b authentication_arguments] -p -d desktop -m machine [-m machine] ...
```

```
vdmadmin -V [-b authentication_arguments] -p -vcdn vCenter_dn -vmpath inventory_path
```

用法说明

只有当遇到问题导致远程桌面处于错误状态时，您才能使用 **vdmadmin** 命令解锁或锁定虚拟机。请不要使用该命令管理正常运行的远程桌面。

如果一个远程桌面已锁定，而 **ADAM** 中已不存在其虚拟机的条目，请使用 **-vmpath** 和 **-vcdn** 选项指定虚拟机和 **vCenter Server** 的清单路径。您可以使用 **vCenter Client** 在 **Home/Inventory/VMs and Templates** 下找到远程桌面的虚拟机清单路径。您可以用 **ADAM ADSI Edit** 在 **OU=Properties** 标题下找到 **vCenter Server** 的标识名。

选项

下表显示了可以在解锁或锁定虚拟机时指定的选项。

表 12-18. 解锁或锁定虚拟机的选项

选项	说明
-d 桌面	指定桌面池。
-e	解锁虚拟机。
-m 计算机	指定虚拟机名称。
-p	锁定虚拟机。
-vcdn vCenter_dn	指定 vCenter Server 的标识名。
-vmpath inventory_path	指定虚拟机的详细目录。

示例

解锁桌面池 **dtpool3** 中的虚拟机 **machine1** 和 **machine2**。

```
vdmadmin -V -e -d dtpool3 -m machine1 -m machine2
```

锁定桌面池 **dtpool3** 中的虚拟机 **machine3**。

```
vdmadmin -V -p -d dtpool3 -m machine3
```

使用 -X 选项检测和解决 LDAP 条目和模式冲突

您可以使用带有 -X 选项的 `vdadmin` 命令检测和解决某个组中的连接服务器副本实例存在的 LDAP 条目冲突和 LDAP 模式冲突。您还可以使用此选项检测和解决 Cloud Pod 架构环境中的 LDAP 模式冲突。

语法

```
vdadmin -X [-b authentication_arguments] -collisions [-resolve]
vdadmin -X [-b authentication_arguments] -schemacollisions [-resolve] [-global]
```

用法说明

如果在两个或更多连接服务器实例上存在重复的 LDAP 条目，可能会破坏 Horizon 7 中 LDAP 数据的完整性。当 LDAP 复制无效时，升级期间可能会发生此情况。尽管 Horizon 7 会定期检查是否存在这种错误情况，但您也可以在组中的某个连接服务器实例上运行 `vdadmin` 命令，以手动检测和解决 LDAP 条目冲突。

当 LDAP 复制无效时，升级期间也可能发生 LDAP 模式冲突。由于 Horizon 7 不会检查是否存在这种错误情况，因此您必须运行 `vdadmin` 命令，以手动检测和解决 LDAP 模式冲突。

选项

下表显示了一些选项，您可以指定这些选项来检测和解决 LDAP 条目冲突。

表 12-19. 用于检测和解决 LDAP 条目冲突的选项

选项	说明
<code>-collisions</code>	指定一个用于检测连接服务器组中的 LDAP 条目冲突的操作。
<code>-resolve</code>	解决 LDAP 实例中的所有 LDAP 冲突。如果不指定此选项，命令只会列出它所发现的问题。

下表显示了一些选项，您可以指定这些选项来检测和解决 LDAP 模式冲突。

表 12-20. 用于检测和解决 LDAP 模式冲突的选项

选项	说明
<code>-schemacollisions</code>	指定一个用于检测连接服务器组或 Cloud Pod 架构环境中的 LDAP 模式冲突的操作。
<code>-resolve</code>	解决 LDAP 实例中的所有 LDAP 模式冲突。如果不指定此选项，命令只会列出它所发现的问题。
<code>-global</code>	对 Cloud Pod 架构环境中的全局 LDAP 实例应用检查和修复。如果不指定此选项，将会对本地 LDAP 实例运行检查。

示例

检测连接服务器组中的 LDAP 条目冲突。

```
vdmadmin -X -collisions
```

检测和解决本地 LDAP 实例中的 LDAP 条目冲突。

```
vdmadmin -X -collisions -resolve
```

检测和解决全局 LDAP 实例中的 LDAP 模式冲突。

```
vdmadmin -X -schemacollisions -resolve -global
```